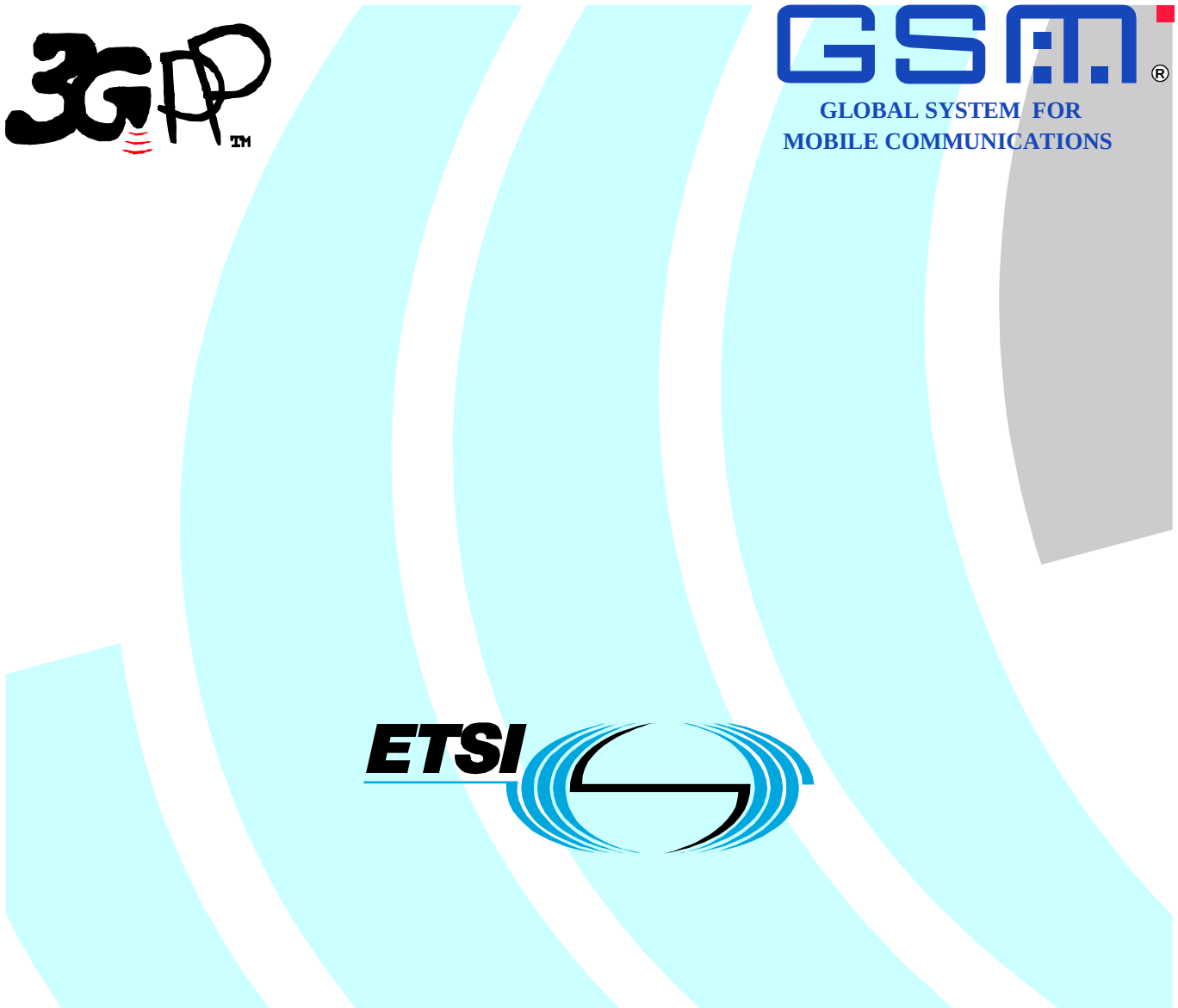
ETSI TS 124 229 V5.1.0 (2002-06)

Technical Specification

Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
IP Multimedia Call Control Protocol based on SIP and SDP;
Stage 3
(3GPP TS 24.229 version 5.1.0 Release 5)



Reference
DTS/TSGN-0124229v510

Keywords
GSM, UMTS

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

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 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under www.etsi.org/key .

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document defines a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP).

The present document is applicable to:

- the interface between the User Equipment (UE) and the Call Session Control Function (CSCF);
- the interface between the CSCF and any other CSCF;
- the interface between the CSCF and an Application Server (AS);
- the interface between the CSCF and the Media Gateway Control Function (MGCF);
- the interface between the S-CSCF and the Media Resource Function Controller (MRFC)
- the interface between the CSCF and the Breakout Gateway Control Function (BGCF);
- the interface between the BGCF and the MGCF;
- the interface between the BGCF and any other BGCF; and
- the interface between the CSCF and an external Multimedia IP network.

Where possible the present document specifies the requirements for this protocol by reference to specifications produced by the IETF within the scope of SIP and SDP. Where this is not possible, extensions to SIP and SDP are defined within the present document. The document has therefore been structured in order to allow both forms of specification.

NOTE: The present document covers only the usage of SIP and SDP to communicate with the enitities of the IM CN subsystem. It is perfectly possible, and not precluded, to use the capabilities of GPRS to allow a terminal containing a SIP UA to communicate with SIP servers outside the IM CN subsystem, and therefore utilise the services provided by those SIP servers. Such usage is outside the scope of the present document.

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, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.002: "Network architecture".

[3] 3GPP TS 23.003: "Numbering, addressing and identification".

[4] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[5] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IM call model".

[6] 3GPP TS 23.221: "Architectural requirements".

[7] 3GPP TS 23.228: "IP multimedia subsystem; Stage 2".

[8] 3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network protocols; Stage 3".

[9] 3GPP TS 25.304: "UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode".

[10] 3GPP TS 26.235: "Packet switched conversational multimedia applications; Default codecs".

[11] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)".

[12] 3GPP TS 29.207: "Policy control over Go interface".

[13] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".

[14] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".

[15] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol, Protocol details".

[16] 3GPP TS 32.200: "Telecommunication management; Charging management; Charging principles".

[17] 3GPP TS 32.225: "Telecommunication management; Charging management; Charging data description for the IP Multimedia subsystem".

[18] 3GPP TS 33.102: "3G Security; Security architecture".

[19] 3GPP TS 33.203: "Access security for IP based services".

[20] 3GPP TS 44.018: "Mobile radio interface layer 3 specification, Radio Resource Control Protocol".

[21] RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication".

[22] RFC 2806: "URLs for Telephone Calls".

[23] RFC 2833 (May 2000): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".

[24] RFC 2916: "E.164 number and DNS".

[25] RFC 2976 (October 2000): "The SIP INFO method".

[26] RFC 3261 (March 2002): "SIP: Session Initiation Protocol".

[27] RFC 3262 (March 2002): "Reliability of provisional responses in Session Initiation Protocol".

[28] RFC 3265 (March 2002): "Session Initiation Protocol Specific Event Notification".

[29] RFC 3311 (April 2002): "The SIP UPDATE method".

[30] RFC 3312 (May 2002): "Integration of resource management and SIP".

[31] RFC 3313 (February 2002): "SIP extensions for media authorization".

[32] RFC 3320 (March 2002): "Signaling Compression (SigComp)"

[33] RFC 3323 (May 2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[34] RFC 3325 (May 2002): "Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks".

[35] RFC 3327 (May 2002): "SIP Extension for Registering Non-Adjacent Contacts".

[36] draft-sparks-sip-refer-split-00 (April 2002): "The REFER method".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[37] draft-sparks-sip-mimetypes (April 2002): "Internet Media Type message/sipfrag".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[38] draft-willis-scvrtdisco-03 (May 2002): "SIP Extension Header for Service Route Discovery in Private Networks".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[39] draft-ietf-mmusic-sdp-new-04 (November 2001): "SDP: Session Description Protocol".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[40] draft-ietf-dhc-dhcpv6-23 (February 2002): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[41] draft-ietf-sip-dhcpv6-00 (April 2002): "DHCPv6 options for SIP servers".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[42] draft-ietf-sipping-sigcomp-sip-dictionary-00.txt (May 2002): "The SIP/SDP static dictionary for Signaling Compression".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[43] draft-beckmann-sip-reg-event-01 (May 2002): "Registration event package".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[44] draft-garcia-sip-visited-network-id-00 (March 2002): "Private SIP extension for Visited Network Identifier".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[45] draft-henrikson-sip-charging-information-01 (May 2002): "Private SIP Extension for Mobile Charging Information".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[46] draft-henrikson-sip-original-dialog-id-01 (May 2002): "Private SIP Extension for Original Dialog Identifier".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[47] draft-mills-sip-access-network-info-01.txt (April 2002): “SIP Access Network Information header”

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

3 Definitions and abbreviations

3.1 Definitions

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

For the purposes of the present document, the following terms and definitions given in RFC 3261 [26] apply (unless otherwise specified see clause 6).

Back-to-Back User Agent (B2BUA)
Client
Dialog
Final response

Header
Header field
Loose routeing
Method
Option-tag (see RFC 3261 [26] subclause 19.2)
Provisional response
Proxy, proxy server
Redirect server
Registrar
Request
Response
Server
Session
(SIP) transaction
Stateful proxy
Stateless proxy
Status-code (see RFC 3261 [26] subclause 7.2)
Tag (see RFC 3261 [26] subclause 19.3)
User agent client (UAC)
User agent server (UAS)
User agent (UA)

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.002 [2] subclause 4a.7 apply:

Breakout Gateway Control Function (BGCF)
Call Session Control Function (CSCF)
Media Gateway Control Function (MGCF)
Media Resource Function Controller (MRFC)
Subscription Locator Function (SLF)

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.218 [5] subclause 3.1 apply:

Filter criteria
Initial filter criteria

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.228 [7] subclause 4.3.3.1 and subclause 4.6 apply:

Interrogating-CSCF (I-CSCF)
Private user identity
Proxy-CSCF (P-CSCF)
Public user identity
Serving-CSCF (S-CSCF)

For the purposes of the present document, the following terms and definitions given in 3GPP TR 21.905 [1] apply:

User Equipment (UE)

3.2 Abbreviations

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

1xx	A status-code in the range 101 through 199, and excluding 100
2xx	A status-code in the range 200 through 299
AS	Application Server
APN	Access Point Name
AUTN	Authentication TokeN
B2BUA	Back-to-Back User Agent
BGCF	Breakout Gateway Control Function
c	conditional
CCF	Charging Collection Function

CDR	Charging Data Record
CK	Ciphering Key
CN	Core Network
CSCF	Call Session Control Function
DNS	Domain Name System
DTD	Document Type Definition
ECF	Event Charging Function
GCID	GPRS Charging Identifier
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
i	irrelevant
I-CSCF	Interrogating CSCF
ICID	IMS Charging Identifier
IK	Integrity Key
IM	IP Multimedia
IMSI	International Mobile Subscriber Identity
IOI	Inter Operator Identifier
IP	Internet Protocol
ISC	IP multimedia Subsystem Service Control
ISIM	IMS Suscriber Identity Module
m	mandatory
MAC	Message Authentication Code
MGCF	Media Gateway Control Function
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
PDP	Packet Data Protocol
n/a	not applicable
o	optional
P-CSCF	Proxy CSCF
PDU	Protocol Data Unit
RAND	RANDom challenge
RES	RESponse
RTP	Real-time Transport Protocol
S-CSCF	Serving CSCF
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
SQN	SeQuence Number
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UE	User Equipment
UICC	Universal Integrated Circuit Card
URI	Universal Resource Identifier
URL	Universal Resource Locator
USIM	UMTS Subscriber Identity Module
x	prohibited
XML	eXtensible Markup Language

4 General

4.1 Conformance of IM CN subsystem entities to SIP

SIP defines a number of roles which entities can implement in order to support capabilities. These roles are defined in annex A.

Each IM CN subsytem functional entity using an interface at the Gm reference point, the Mg reference point, the Mi reference point, the Mj reference point, the Mk reference point, the Mm reference point, the Mr reference point and the Mw reference point, and also using the IP multimedia Subsystem Service Control (ISC) Interface, shall implement SIP,

as defined by the referenced specifications in Annex A, and in accordance with the constraints and provisions specified in annex A, according to the following roles.

The Gm reference point, the Mg reference point, the Mi reference point, the Mj reference point, the Mk reference point, the Mm reference point and the Mw reference point are defined in 3GPP TS 23.002 [2].

The Mr reference point is defined in 3GPP TS 23.228 [7].

The ISC interface is defined in 3GPP TS 23.228 [7] subclause 4.2.4.

- The User Equipment (UE) shall provide the User Agent (UA) rolewith the exceptions and additional capabilities as described in subclause 5.1.

- The P-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.2. When acting as the subscriber to or the recipient of event information, the P-CSCF shall provide the UA role, again with the exceptions and additional capabilities as described in subclause 5.2.

- The I-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.3.

- The S-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.4. Under certain circumstances as described in subclause 5.4, the S-CSCF shall provide the UA role with the additional capabilities, as follows:

  a) the S-CSCF shall also act as a registrar. When acting as a registrar, or for the purposes of executing a third-party registration, the S-CSCF shall provide the UA role;

  b) as the notifier of event information the S-CSCF shall provide the UA role; and

  c) when performing S-CSCF initiated release the S-CSCF shall provide the UA role, even when acting as a proxy for the remainder of the dialog.

- The BGCF shall provided the proxy role, with the exceptions and additional capabilities as described in subclause 5.5.

- The MGCF shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.6.

- The AS, acting as terminating UA, or redirect server (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.1), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.2.

- The AS, acting as originating UA (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.2), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.3.

- The AS, acting as a SIP proxy (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.3), shall provided the proxy role, with the exceptions and additional capabilities as described in subclause 5.7.4.

- The AS, performing 3rd party call control (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.4), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.5.

- The AS, receiving third-party registration requests, shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.

- The MRFC shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.8.

NOTE: The allocated roles defined in this clause are the starting point of the requirements from the IETF SIP specifications, and are then the basis for the description of further requirements. Some of these extra requirements formally change the proxy role into a B2BUA. Thus, for example, a P-CSCF is a B2BUA in that it inspects and may modify SDP message bodies, and terminates Record-Route headers on behalf of the UA, but in all other respects other than those more completely described in subclause 5.2 it implements proxy requirements. Despite being a B2BUA a P-CSCF does not implement UA requirements from the IETF RFCs, except as indicated in this specification, e.g., relating to registration event subscription.

4.2 URL and address assignments

In order for SIP and SDP to operate, the following preconditions apply:

1) I-CSCFs used in registration are allocated SIP URLs. Other IM CN subsystem entities may be allocated SIP URLs. For example pcscf.home1.net and <impl-specific-info>@pcscf.home1.net are valid SIP URLIs. If the user part exists, it is an essential part of the address and shall not be omitted when copying or moving the address. How these addresses are assigned to the logical entities is up to the network operator. For example, a single SIP URL may be assigned to all I-CSCFs, and the load shared between various physical boxes by underlying IP capabilities, or separate SIP URLs may be assigned to each I-CSCF, and the load shared between various physical boxes using DNS SRV capabilities.

2) All IM CN subsystem entities are allocated IP addresses. Allocation of IPv6 and IPv4 addresses fulfils the requirements of of 3GPP TS 23.221 [6] subclause 5.1.

3) The subscriber is allocated a private user identity by the home network operator, and this is contained within the ISIM application, if present, on the UICC. Where no ISIM application is present, the private user identity is derived from the IMSI, which is contained on the USIM (see 3GPP TS 23.003 [3]). This private user identity is available to the SIP application within the UE.

NOTE: The SIP URLs may be resolved by using any of public DNSs, private DNSs, or peer-to-peer agreements.

4) The subscriber is allocated one or more public user identities by the home network operator. At least one of these is contained within the ISIM application, if present, on the UICC. Where no ISIM application is present, the UE shall derive a temporary public user identity from the IMSI contained on the USIM (see 3GPP TS 23.003 [3]). All registered public user identities are available to the SIP application within the UE, after registration.

5) The UE is dynamically assigned an IP version 6 address.

4.3 Routeing principles of IM CN subsystem entities

Each IM CN subsytem functional entity shall apply loose routeing policy as described in RFC 3261 [26], when processing a SIP request. In cases where the I-CSCF or the S-CSCFmay interact with strict routers in non IM CN subsystem networks, the routeing procedures defined in RFC 3261 [26] that ensure interoperability with strict routers shall be used by the I-CSCF and S-CSCF.

4.4 Trust domain for asserted identity

RFC 3325 [34] provides for the existence and trust of an asserted identity within a trust domain. For the IM CN subsystem, this trust domain consists of the P-CSCF, the I-CSCF, the S-CSCF, the BGCF. the MGCF, the MRFC, and all ASs that are not provided by third-party service providers. ASs provided by third-party service providers are outside the trust domain.

NOTE: In addition to the procedures specified in clause 5, procedures of RFC 3325 [34] in relation to transmission of P-Asserted-Identity headers and their contents outside the trust domain also apply.

4.5 Charging correlation principles for IM CN subsystems

4.5.1 Overview

This subclause describes charging correlation principles to aid with the readability of charging related procedures in subclause 5. See 3GPP TS 32.200 [16] and 3GPP TS 32.225 [17] for further information on charging.

IM CN subsystem generates and retrieves the following charging correlation information for later use with offline and online charging:

1. IMS Charging Identifier (ICID);

2. Access network information:

   a. GPRS Charging Information;

3. Inter Operator Identifier (IOI);
4. Charging function addresses:

   a. Charging Collection Function (CCF);

   b. Event Charging Function (ECF).

The charging correlation information is encoded in the P-Charging-Vector header as defined in subclause 7.2. The P-Charging-Vector header contains the following parameters: icid, access network information and ioi. The parameters are described further in the subclauses that follow. The GGSN provides the access network information to the IM CN subsystem, which is the common information used to correlate GGSN CDRs with IM CN subsystem CDRs.

The offline and online charging function addresses are encoded in the P-Charging-Function-Addresses as defined in subclause 7.2. The P-Charging-Function-Addresses header contains the following parameters: ccf and ecf.

4.5.2 IMS charging identifier (ICID)

The IMS Charging Identifier (ICID) is the session level data shared among the IMS network entities including ASs in both the calling and called IMS networks.

The first IMS network entity involved in a dialog (session) or standalone (non-session) message will generate the ICID and include it in the icid parameter of the P-Charging-Vector header in the SIP request. The P-CSCF will generate ICID for mobile originated calls. The I-CSCF will generate ICID for mobile terminated calls if there is no ICID received in the initial request (e.g. the calling party network is another SIP based network). The AS will generate ICID when acting as an originating UA. The MGCF will generate ICID for PSTN/PLMN originated calls. Each entity that processes the SIP request will extract the ICID for possible later use in a charging data records (CDR). The I-CSCF and S-CSCF are also allowed to generate a new ICID for mobile terminated calls received from another network.

There is also an ICID generated by the P-CSCF with a REGISTER request that is passed in a unique instance of P-Charging-Vector header. This ICID is valid for the duration of the registration and is associated with the signalling PDP context.

The icid parameter is included in any requests that include the P-Charging-Vector header. However, the P-Charging-Vector (and ICID) is not passed to the UE. It is also possible for the ICID to be passed to the GGSN and SGSN, but that is outside the scope of this specification.

The ICID is also passed from the P-CSCF to the GGSN, but the ICID is not passed to the SGSN. The interface supporting this operation is outside the scope of this document.

4.5.3 Access network information

4.5.3.1 General

The access network information are the media component level data shared among the IMS network entities for one side of the session (either the calling or called side). GPRS charging information (GGSN identifier and GCIDs) is an example of access network information.

4.5.3.2 GPRS charging information

The P-CSCF provides the GPRS charging information to the S-CSCF. The S-CSCF may also pass the information to an Application Server (AS), which may be needed for online pre-pay applications. The GPRS charging information for the originating network is used only within that network, and similarly the GPRS charging information for the terminating network is used only within that network. Thus the GPRS charging information are not shared between the calling and called networks. The GPRS charging information is not passed towards the external ASs from its own network.

The GPRS charging information is populated in the P-Charging-Vector using the gprs-charging-info parameter. The gprs-charging-info parameter contains further parameters: ggsn and gcid. The gcid parameter contains charging identifiers for one or more PDP contexts, or GCID. Each gcid parameter has an identifier assigned by the GGSN (pdp-id parameter), the authorization token used when PDP context was established (auth-token) and an index number

(pdpflow-index parameter) to correlate the PDP context with a media stream in the SDP from the SIP signalling. The numbering for the index shall start at 1 and is associated with the 'm' lines in the SDP, where the counting is done from top to bottom.

The GPRS charging information is passed at the first opportunity after the resources are allocated at the GGSN. GPRS charging information will be updated with new information during the session as media streams are added or removed.

4.5.4 Inter operator identifier (IOI)

The Inter Operator Identifier (IOI) is globally unique identifier to share between operator networks/service providers/content providers. There are two possible instances of IOI to be exchanged between networks/service providers/content providers: one for the originating side, ioi-originating, and one for the terminating side, ioi-terminating.

The originating network populates the ioi-originating parameter of the P-Charging-Vector header in the initial request, which identifies the operator network from which the request originated. Also in the initial request, the ioi-terminating parameter is left out of the P-Charging-Vector parameter. The originating network retrieves the teminating-ioi parameter from the P-Charging-Vector header within the message sent in response to the initial request, which identifies the operator network from which the response was sent. The MGCF takes responsibility for populating the ioi-originating on behalf of the PSTN/PLMN when a call/session is originated from the PSTN/PLMN.

The terminating network retrieves the ioi-originating parameter from the P-Charging-Vector header in the initial request, which identifies the operator network from which the request originated. The terminating network populates the ioi-terminating parameter of the P-Charging-Vector header in the response to the initial request, which identifies the operator network from which the response was sent. IOIs will not be passed along within network. However, IOIs will be sent to AS for accounting purposes.

4.5.5 Charging function addresses

Charging function addresses are distributed to each of the IMS network entities in the home network for one side of the session (either the calling or called side) and are to provide a common location for each entity to send charging information. Charging Collection Function (CCF) addresses are used for offline billing. Event Charging Function (ECF) addresses are used for online billing.

There may be two separate addresses for CCF and ECF addresses populated into the P-Charging-Function-Addresses header of the SIP request or response. The parameters are ccf-primary, ccf-secondary, ecf-primary and ecp-secondary. Only ccf-primary is required. The other parameters are optional. The secondary addresses may be included by each IMS network for redundancy purposes.

The CCF addresses and ECF addresses are retrieved from HSS via Cx interface and passed by the S-CSCF to subsequent entities. The charging function addresses are passed from the S-CSCF to IM CN subsystem entities in its home network, but are not passed to the visited network or the UE. When the P-CSCF is allocated in the visited network, then the charging function addresses are obtained by means outside the scope of this document. The AS receives the charging function addresses from the S-CSCF via the ISC interface.

5 Application usage of SIP

5.1 Procedures at the UE

5.1.1 Registration and authentication

5.1.1.1 General

The UE shall register public user identities (see table A.3/1 and dependencies on that major capability).

In case a UE registers several public user identities at different points in time, the procedures to re-register, deregister and subscribe to the registration-state event package for these public user identities can remain uncoordinated in time.

5.1.1.1A Parameters contained in the UICC

In case the UE is loaded with a UICC that contains the ISIM application, it will be preconfigured with all the necessary parameters to initiate the registration to the IM CN subsystem. These parameters include:

- the private user identity;
- one ore more public user identities; and
- the home network domain name used to address the SIP REGISTER request

In case the UE is loaded with a UICC that does not contain the ISIM application, the UE shall:

- generate a private user identity;
- generate a temporary public user identity; and
- generate a home network domain name to address the SIP REGISTER request to.

All these three parameters are derived from the IMSI parameter in the USIM, according to the procedures described in 3GPP TS 23.003 [3].

The temporary public user identity is only used in REGISTER requests. After a successful registration, the UE will get the associated public user identities, and any of them shall be used in subsequent non-REGISTER messages.

As the temporary public user identity may be barred, the UE shall not reveal the temporary public user identity to the user.

In the case the UE needs to derive the temporary public user identity, the procedure shall be executed every time the UICC is changed.

5.1.1.2 Initial registration

The UE can register a public user identity at any time that a valid PDP context exists. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

A REGISTER request may be integrity protected using IK, see 3GPP TS 33.203 [19], received in an earlier registration.

The public user identity to be registered can be extracted either from the ISIM application, if present, on the UICC or derived from the USIM, according to the procedures described in subclause 5.1.1.1A. A public user identity may be input by the end user. On sending a REGISTER request, the UE shall populate the header fields as follows:

a) the user ID field of the authentication protocol, carried in the Authorization header, shall contain the private user identity;

b) the From header shall contain the public user identity to be registered;

c) the To header shall contain the public user identity to be registered;

d) the Expires header, or the expires parameter within the Contact header, shall contain 600 000 seconds as the value desired for the duration of the registration; and

e) a Request-URI that contains the SIP URI of the domain name of the home network.

NOTE: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

The UE shall extract or derive from the UICC a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A.

The use of the Path header shall not be supported by the UE.

The UE shall also include the P-Access-Network-Info header in the REGISTER request. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2.3).

On receiving the 200 (OK) response to the REGISTER request, the UE shall store the expiration time of the registration for the public user identities found in the To header value. The UE shall also store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) too brief response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

5.1.1.3 Initial subscription to the registration-state event package

Upon receipt of a 2xx response to the initial registration, the UE shall subscribe to the users registration-state event package for the public user identity registered as described in subclause 5.1.1.2 at the users registrar (S-CSCF). The registration-state event package is described in draft-beckmann-sip-reg-event-01 [43]. Therefore the UE shall generate a SUBSCRIBE request with the following elements:

- a Request URI set to the resource to which the UE wants to be subscribed to, i.e. to a SIP URL that contains the public user identity;
- a From header set to a SIP URL that contains a public user identity;
- a To header, set to a SIP URL that contains a public user identity;
- an Event header set to the "registration-state" event package;
- an Expires header set to a value higher than the Expires header of the before sent REGISTER request.

The UE shall also include the P-Access-Network-Info header in the SUBSCRIBE request. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2.3).

Afterwards it shall send out the so generated SUBSCRIBE request.

Upon receipt of a 2xx response to the SUBSCRIBE request, the UE shall store the information for the established dialog and the expiration time as indicated in the Expires header of the received response.

The UE shall automatically resubscribe to the registration-state event package for a previously registered public user identity if the expiration time, as indicated in the Expires header of the 2xx response to the SUBSCRIBE request, has run out and the public user identity is still registered.

5.1.1.4 User-initiated re-registration

The UE can reregister a previously registered public user identity at any time.

The UE shall reregister the public user identity 600 seconds before the expiration time of a previous registration, unless either the user or the application within the UE has determined that a continued registration is not required. If the registration period indicated from the S-CSCF is less than 600 seconds, the UE shall reregister when half of the registration period has expired.

The REGISTER request may be integrity protected using IK, see 3GPP TS 33.203 [19], received in an earlier registration.

On sending a REGISTER request, the UE shall populate the header fields as follows:

a) the user ID field of the authentication protocol, carried in the Authorization header, shall contain the private user identity. This shall be extracted from the USIM;

b) the From header shall contain the public user identity to be registered;

c) the To header shall contain the public user identity to be registered;

d) the Expires header, or the expires parameter within the Contact header, should contain the same expiration timer as the expiration timer returned in the 200 (OK) response to the initial REGISTER request.

NOTE: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

The UE shall also include the P-Access-Network-Info header in the REGISTER request. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2.3).

On receiving the 200 (OK) response to the REGISTER request, the UE shall store the new expiration time of the registration for this public user identity found in the To header value. The UE shall also store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity.

The use of the Path header shall not be supported by the UE.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

5.1.1.5 Authentication

5.1.1.5.1 General

Authentication is achieved via the registration and re-registration procedures. When the network requires authentication or re-authentication of the UE, the UE will receive a 401 (Unauthorized) response to the REGISTER request.

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

- check the validity of a received authentication challenge, as described in 3GPP TS 33.102 [18] i.e. the locally calculated MAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range.

In the case that the 401 (Unauthorized) response to the REGISTER request is deemed to be valid the UE shall:

- extract the RAND and AUTN parameters, and use the derived keys (CK and IK) to protect future messages, see 3GPP TS 33.203 [19]; and

- send another REGISTER request using the derived IK to integrity protect the message. The header fields are populated as defined for the initial request, with the addition that the UE shall include an Authorization header containing the private user identity and the authentication challenge response (RES parameter).

In the case that the 401 (Unauthorized) response is deemed to be invalid then the UE shall behave as defined in subclause 5.1.1.5.3.

5.1.1.5.2 Network-initiated re-authentication

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the registration-state event package, which contains the registration state value "re-authenticate" for a public user identity, the UE shall start the re-authentication procedures by initiating a reregistration as described in subclause 5.1.1.4.

5.1.1.5.3 Abnormal cases

If, in a 401 (Unauthorized) response, either the MAC or SQN is incorrect the UE shall respond with a further REGISTER indicating to the S-CSCF that the challenge has been deemed invalid as follows:

- in the case where the UE deems the MAC parameter to be invalid the subsequent REGISTER request shall contain no response parameter (e.g. no RES or AUTS);

- in the case where the UE deems the SQN to be out of range, the subsequent REGISTER request shall contain the AUTS parameter (see 3GPP TS 33.102 [18]).

A UE shall only respond to two consecutive invalid challenges. The UE may attempt to register with the network again after an implementation specific time.

5.1.1.6 Mobile-initiated deregistration

The UE can deregister a previously registered public user identity at any time.

On sending a REGISTER request, the UE shall populate the header fields as follows:

a) the user ID field of the authentication protocol, carried in the Authorization header, shall contain the private user identity. This shall be extracted from the USIM;

b) the From header shall contain the public user identity to be deregistered;

c) the To header shall contain the public user identity to be deregistered;

d) the Expires header, or the expires parameter of the Contact header, shall contain a value of zero, appropriate to the deregistration requirements of the user.

The UE shall also include the P-Access-Network-Info header in the REGISTER request. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2.3).

On receiving the 200 (OK) response to the REGISTER request, the UE shall remove all registration details relating to this public user identity.

5.1.1.7 Network-initiated deregistration

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the registration-state event package as described in subclause 5.1.2.1, which contains the registration state value "closed", i.e. deregistered, for one or more public user identities that were previously stored as registered, the UE shall remove all registration details relating to these public user identities.

5.1.2 Subscription and notification

5.1.2.1 Notification about multiple registered public user identities

Upon receipt of a 2xx response to the SUBSCRIBE request the UE shall maintain the generated dialog (identified by the values of the Call-ID, To and From headers).

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the registration-state event package the UE shall perform the following actions:

- if a registration state value "open", i.e. registered is received for one or more public user identities, the UE shall store the indicated public user identities as registered;

- if a registration state value "closed", i.e. deregistered is received for one or more public user identities, the UE shall store the indicated public user identities as deregistered.

NOTE: There may be public user identities which are automatically registered within the registrar (S-CSCF) of the user upon registration of one public user identity. Usually these automatically or implicitly registered public user identities belong to the same service profile of the user and they might not be available within the UE, i.e. the UE does not know that they have been registered. The here-described procedures provide a mechanism to inform the UE about these automatically registered public user identities.

5.1.2.2 General SUBSCRIBE requirements

If the UA receives a 503 (Service Unavailable) response to an initial SUBSCRIBE request containing a Retry-After header, then the UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents.

5.1.2A Generic procedures applicable to all methods

5.1.2A.1 Mobile-originating case

In accordance with RFC 3325 [34] the UE may insert a P-Asserted-Identity header in any initial request for a dialog or request for a standalone transaction as a hint for creation of an asserted identity within the IM CN subsystem. The UE may include any of the following in the P-Asserted-Identity header:

- a public user identity stored in the USIM which has been registered by the user;
- a public user identity returned in a registration-state event package of a NOTIFY request as a result of an implict registration; or
- any other public user identity which the user has assumed by mechanisms outside the scope of this specification to have a current registration.

NOTE 1: The temporary public user identity specified in subclause 5.1.1.1 is not a public user identity suitable for use in the P-Asserted-Identity header.

Where privacy is required, in any initial request for a dialog or request for a standalone transaction, the UE shall set the From header to "Anonymous".

NOTE 2: It is a matter of network policy as to whether any of the contents of the From header are modified based on any privacy specified by the user either within the UE indication of privacy or by network subscription. Therefore the user could require to include the value "Anonymous" even on requests where privacy is not explicitly requested.

The UE can indicate privacy of the P-Asserted-Identity in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

5.1.2A.2 Mobile-terminating case

The UE can indicate privacy of the P-Asserted-Identity in accordance with RFC 3323 [33].

NOTE: In the mobile-terminating case, this version of the document makes no provision for the UE to provide an P-Asserted-Identity in the form of a hint.

5.1.3 Call initiation - mobile originating case

5.1.3.1 Initial INVITE

Upon generating an initial INVITE request, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism;
- indicate the requirement of precondition and specify it using the Require header mechanism.

If the UA receives a 503 (Service Unavailable) response to an initial INVITE request containing a Retry-After header, then the UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents.

5.1.4 Call initiation - mobile terminating case

5.1.4.1 Initial INVITE

Upon receiving an initial INVITE request without containing either Supported: precondition or Require: precondition header values, the UE shall generate a 421 (Extension Required) response indicating the required extension in the Require header field.

Upon generating the first response to the initial INVITE request, the UE shall indicate the requirement for reliable provisional responses and specify it using the Require header mechanism.The UE shall send the 200 (OK) response to the initial INVITE request only after the local resource reservation has been completed.

5.1.5 Call release

Void.

5.1.6 Emergency service

A UE shall not attempt to establish an emergency session via the IM CN Subsystem when the UE can detect that the number dialled is an emergency number. The UE shall use the CS domain as described in 3GPP TS 24.008 [8].

In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a XML body that includes an <alternative service> element with the <type> child element set to "emergency", the UE shall automatically:

- send an ACK request to the P-CSCF as per normal SIP procedures;
- attempt an emergency call setup according to the procedures described in 3GPP TS 24.008 [8].

The UE may also provide an indication to the user based on the text string contained in the <reason> element.

As a consequence of this, a UE operating in MS operation mode C cannot perform emergency calls.

5.2 Procedures at the P-CSCF

5.2.1 General

The P-CSCF shall support the Path and P-Service-Route headers.

NOTE 1: The Path header is only applicable to the REGISTER request and its 200 (OK) response. The P-Service-Route header is only applicable to the 200 (OK) response of REGISTER request.

When the P-CSCF sends any request or response to the UE, before sending the message the P-CSCF shall:

- remove the P-Charging-Function-Addresses and P-Charging-Vector headers, if present.

When the P-CSCF receives any request or response from the UE, the P-CSCF shall:

- remove the P-Charging-Function-Addresses and P-Charging-Vector headers, if present. Also, the P-CSCF shall ignore any data received in the P-Charging-Function-Addresses and P-Charging-Vector headers; and
- may insert previously saved values into the P-Charging-Function-Addresses and P-Charging-Vector headers before forwarding the message.

NOTE 2: When the P-CSCF is located in the visited network, then it will not receive the P-Charging-Function-Addresses header from the S-CSCF or I-CSCF. Instead, the P-CSCF discovers charging function addresses by other means not specified in this document.

5.2.2 Registration

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall:

1) insert a Path header in the request including an entry containing:
   - the SIP URL identifying the P-CSCF;
   - an indication that requests routed in this direction of the path (i.e. from the S-CSCF to the P-CSCF) shall be treated as for the mobile-terminating case. This indication may e.g. be in a Path header parameter, a character string in the user part or be a port number;

2) insert a Supported and a Require header both containing the option tag "path";

3) for the initial REGISTER request for a public user identity create a new, globally unique value for icid, save it locally and insert it into the icid parameter of the P-Charging-Vector header (see subclause 7.2.5). Also include the gprs-charging-info parameter in the P-Charging-Vector header (see subclause 5.2.7.4);

4) insert the parameter "integrity-protected" (described in subclause 7.2A.2) with a value “yes” into the Authorization header field in case the REGISTER request was received integrity protected, otherwise insert the parameter with the value “no”;

5) insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network; and

6) determine the I-CSCF of the home network and forward the request to that I-CSCF.

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

1) save the list of P-Service-Route headers preserving the order. This list shall be stored during the entire registration period of the respective public user identity. This list shall be used to preload the routeing information into the initial requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing list of P-Service-Route headers with the new list;

2) associate the P-Service-Route header information with the registered public user identity;

3) remove any Path and P-Service-Route headers from the 200 (OK) response before forwarding the response to the UE;

4) store the public user identities found in the P-Associated-URI header value, as those that are authorized to be used by the UE;

5) store the default public user identity for use with procedures for the P-Asserted-Identity. The default public user identity is specifically indicated in the Associated-URI header values.

Editor's note: The exact mechanism for indicating this value is for further discussion.

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall store the values received in the P-Charging-Function-Addresses header.

When the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall remove and store the CK and IK values contained in the 401 (Unauthorized) response. The 401 Unauthorized response shall be forwarded to the UE if and only if the CK and IK have been removed.

NOTE: The P-CSCF will maintain two Route lists. The first Route list - created during the registration procedure - is used only to pre-load the routeing information into the initial INVITE request that originated at the UE. This list is valid during the entire registration of the respective public user identity. The second Route list - constructed from the Record Route headers in the initial INVITE and associated response - is used during the duration of the call. Once the call is terminated, the second Route list is discarded.

5.2.3 Subscription to the users registration-state event package

Upon receipt of a 2xx response to the initial REGISTER request of an user, the P-CSCF shall subscribe to the users registration-state event package at the users registrar (S-CSCF) as described in draft-beckmann-sip-reg-event-01 [43]. Therefore the P-CSCF shall generate a SUBSCRIBE request with the following elements:

- a Request-URI set to the topmost entry of the path information that was obtained during the users registration;

- a From header set to the P-CSCF's SIP URL;

- a To header, set to a SIP URL that contains the public user identity that was previously registered;

- an Event header set to the "registration-state" event package;

- an Expires header set to a value higher then the Expires header of the before sent REGISTER request from the user; and

- a Route header according to the path information that was obtained during the users registration. Th S-CSCF shall set the last Route header entry to the resource to which it wants to subscribe to, i.e. to a SIP URL the public user identity that was previously registered.

Afterwards the P-CSCF shall send out the so generated SUBSCRIBE request.

Upon receipt of a 2xx response to the SUBSCRIBE request, the P-CSCF shall store the information for the so established dialog and the expiration time as indicated in the Expires header of the received response.

5.2.4 Registration of multiple public user identites

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the registration-state event package, the P-CSCF shall perform the following actions:

- if a registration state value "open", i.e. registered is received for one or more public user identities, the P-CSCF shall bind the indicated public user identities as registered to the contact information of the user;

- if a registration state value "closed", i.e. deregistered is received for one or more public user identities, the P-CSCF shall release all stored information for these public user identities.

NOTE: There may be public user identities which are automatically registered within the registrar (S-CSCF) of the user upon registration of one public user identity. These automatically registered public user identities belong to the same service profile of the user and they are not available at the P-CSCF, i.e. P-CSCF does not know that they have been registered. The here-described procedures provide a mechanism to inform the UE about these automatically registered public user identities.

5.2.5 Deregistration

5.2.5.1 User-initiated deregistration

When the P-CSCF receives a 200 (OK) response to a REGISTER request (sent according to subclause 5.2.2), it shall check the value of the Expires header field and/or expires parameter in the Contact header field. When the value of the Expires header field or expires parameter equals zero, then the P-CSCF shall remove the public user identity found in the To header field, and all the associated public user identities, from the registered public user identities list and all related stored information.

NOTE: There is no requirement to distinguish a REGISTER request relating to a registration from that relating to a deregistration. For administration reasons the P-CSCF may distinguish such requests, however this has no impact on the SIP procedures.

5.2.5.2 Network-initiated deregistration

If the P-CSCF:

- has subscribed for the registration-state event package providing registration state information of a certain public identity and public user identities implicitly registered with it; and,

- an incoming NOTIFY request arrives on the dialog which was generated during subscription (as described in subclause 5.2.3) containing the registration state value “closed”, i.e. deregistered, for one or more public user identities;

the P-CSCF shall release all stored information for these public user identities which are indicated with registration state "closed".

5.2.6 General treatment for all dialogs and standalone transactions excluding the REGISTER method

5.2.6.1 Introduction

The procedures of subclause 5.2.6 and its subclauses are general to all requests and responses, except those for the REGISTER method. Procedures in subsequent clauses to subclause 5.2.6 apply in addition to the procedures of subclause 5.2.6.

5.2.6.2 Determination of mobile-originated or mobile-terminated case

Upon receipt of an initial request or a refresh request or a stand-alone transaction, the P-CSCF shall:

- perform the procedures for the mobile-terminating case as described in subclause 5.2.6.4 if the request makes use of the information for mobile-terminating calls, which was added to the Path header entry of the P-CSCF during registration (see subclause 5.2.2), e.g. the message is received at a certain port or the topmost Route header contains a specific user part or parameter;

- perform the procedures for the mobile-originating case as described in subclause 5.2.6.3 if this information is not used by the request.

5.2.6.3 Requests initiated by the UE

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains as P-Asserted-Identity header that matches one of the registered public user identities, the P-CSCF shall identify the initiator of the request by that public user identity.

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains as P-Asserted-Identity header that does not match one of the registered public user identities, or does not contain a P-Asserted-Identity header, the P-CSCF shall identify the initiator of the request by a default public user identity.

NOTE: The contents of the From header do not form any part of this decision process.

When the P-CSCF receives from the UE an initial request for a dialog, and a P-Service-Route header list exists for the initiator of the request, the P-CSCF shall:

- remove any Route header from the request;

- select the list of Route headers that was created during the registration or reregistration of the respective public user identity utilizing the P-Service-Route mechanism;

- pre-load the list of Route headers to the request;

- create a Record-Route header containing its own SIP URL;

- insert a P-Asserted-Identity header with a value representing the initiator of the request;

- create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header; and

- forward the request based on the topmost Route header.

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- store the values received in the P-Charging-Function-Addresses header;

- remove the list of Record-Route headers from the received response;

- create a new list of stored Route headers, with the newly received list of Record-Route headers. The Contact header received in the response shall not be appended to the bottom of the stored list of Route headers;

- store the dialog ID and associate it with the private user identity and public user identity involved in the session; and

- save the Contact header received in the response in order to release the dialog if needed.

When the P-CSCF receives any other response to the above request, the P-CSCF shall:

- remove any list of Record-Route headers, even though not allowed, from the received response and forward it to the UE.

When the P-CSCF receives from the UE a refresh request for a dialog, the P-CSCF shall:

- remove any Route header from the request;
- select the list of Route headers that was created during the exchange of the initial request and its associated response;
- pre-load the list of Route headers to the request;
- create a Record-Route header containing its own SIP URL;
- verify if the request relates to a dialog in which the originator of the request is involved. If the request does not relates to a dialog in which the originator is involved, then a 403 response shall be sent back to the originator; and
- forward the request based on the topmost Route header.

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- remove the list of Record-Route headers from the received response;
- overwrite any existing list of stored Route headers, or create a new list of stored Route headers, with the newly received list of Record-Route headers. The Contact header received in the response shall not be appended to the bottom of the stored list of Route headers; and
- save the Contact header received in the response in order to release the dialog if needed.

When the P-CSCF receives any other response to the above request, the P-CSCF shall:

- remove any list of Record-Route headers, even though not allowed, from the received response and forward it to the UE.

When the P-CSCF receives from the UE the request for a standalone transaction, and a P-Service-Route header list exists for the initiator of the request, the P-CSCF shall:

- remove any Route header from the request;
- select the list of Route headers that was created during the registration or reregistration of the respective public user identity utilizing the P-Service-Route mechanism;
- pre-load the list of Route headers to the request;
- insert a P-Asserted-Identity header with a value representing the initiator of the request;
- create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header; and
- forward the request based on the topmost Route header.

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- store the values received in the P-Charging-Function-Addresses header; and
- remove any list of Record-Route headers, even though not allowed, from the received response and forward it to the UE.

When the P-CSCF receives from the UE subsequent requests other than a refreshing request that pertains to an existing dialog, the P-CSCF shall:

- select the list of Route headers that was created during the exchange of the initial request and associated response for this call;

- pre-load the list of Route headers to the request;
- verify if the request relates to a dialog in which the originator of the request is involved. If the request does not relate to a dialog in which the originator is involved, then a 403 response shall be sent back to the originator; and
- forward the request based on the topmost Route header.

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- verify if the request relates to a dialog in which the originator of the request is involved.. If the request does not relates to a dialog in which the originator is involved, then a 403 response shall be sent back to the originator; and
- remove any list of Record-Route headers, valid or not, from the received response and forward it to the UE.

When the P-CSCF receives from the UE an initial request for a dialog, a refresh request for a dialog, or the request of a standalone transaction, and a P-Service-Route header list does not exist for the initiator of the request, the P-CSCF shall:

- send a 403 Forbidden response back to the UE containing a warning header.

Editor's Note: how to find out whether the user has a valid registration in the P-CSCF is FFS.

Editor's Note: The correct value for the warning code is yet to be assigned by IANA.

When the P-CSCF receives from the UE the request for an unknown method, and a P-Service-Route header list exists for the initiator of the request, the P-CSCF shall:

- select the list of Route headers that was created during the registration or reregistration of the respective public user identity utilizing the P-Service-Route mechanism;
- pre-load the list of Route headers to the request,
- insert an P-Asserted-Identity header with a value representing the initiator of the request; and
- forward the request based on the topmost Route header.

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- remove any list of Record-Route headers, even though invalid, from the received response and forward it to the UE.

When the P-CSCF receives any request or response from the UE, the P-CSCF shall:

- remove the <charging-vector> XML element (see subclause 7.6), if present, from the message body of the received request or response.

5.2.6.4 Requests terminated by the UE

When the P-CSCF receives a response to an initial request for a dialog or a response to a request for a standalone transaction, the P-CSCF shall identify responder by a public user identity that relates to the Request-URI used in the request.

NOTE: The contents of the To header do not form any part of this decision process.

When the P-CSCF receives, destined for the UE, an initial request for a dialog, or a refresh request for a dialog, prior to forwarding the request, the P-CSCF shall:

- remove its own SIP URL from the topmost Route header;
- remove the list of Record-Route headers, and shall convert it into a list of Route headers. The Contact header shall not be appended to the bottom of the list of Route headers. The P-CSCF shall save this list of Route headers and append this list to all UE originated requests for this dialog;
- save the Contact header received in the response in order to release the dialog if needed;

- add itself on the top of the removed list of Record-Route headers and save the list. The list will be appended to UE originated response to the SUBSCRIBE request;

- remove and store the list of received Via headers from the received request and shall place its own address in the Via header with locally unique token to identify the saved values as a branch parameter. The P-CSCF shall append the list of Via headers to the UE originated response for this request;

- store the values received in the P-Charging-Function-Addresses header; and

- remove and store the icid parameter received in the P-Charging-Vector header.

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- insert an P-Asserted-Identity header with a value representing the responder to the request;

- append the saved list of Record-Route headers to the response;

- append the saved list of Via headers to the response; and

- store the dialog ID and associate it with the private user identity and public user identity involved in the session.

When the P-CSCF receives any other response to the above request, the P-CSCF shall:

- append the saved list of Via headers to the response.

When the P-CSCF receives, destined for the UE, a request for a stand-alone transaction, prior to forwarding the request, the P-CSCF shall:

- insert an P-Asserted-Identity header with a value representing the responder to the request;

- remove and store the list of received Via headers from the received request and shall place its own address in the Via header with locally unique token to identify the saved values as a branch parameter. The P-CSCF shall append this list of Via headers to the UE originated response for this transaction;

- store the values received in the P-Charging-Function-Addresses header; and

- remove and store the icid parameter received in the P-Charging-Vector header.

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- append the saved list of Via headers to the response; and

- verify if the request relates to a dialog in which the originator of the request is involved. If the request does not relate to a dialog in which the originator is involved, then a 403 response shall be sent back to the originator.

When the P-CSCF receives, destined for the UE, a subsequent request for a dialog that is not a refresh request, prior to forwarding the request, the P-CSCF shall:

- remove and store the list of received Via headers from the received request and shall place its own address in the Via header with locally unique token to identify the saved values as a branch parameter. The P-CSCF shall append this list of Via headers to the UE originated response for this transaction; and

- remove and store the icid parameter from P-Charging-Identity header (see subclause 7.6).

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- append the saved list of Via headers to the response.

When the P-CSCF sends any request or response to the UE, the P-CSCF shall:

- remove the P-Charging-Vector header from the request or response.

5.2.7 Initial INVITE

5.2.7.1 Introduction

In addition to following the procedures for initial requests defined in subclause 5.2.6, initial INVITE requests also follow the procedures of this subclause.

5.2.7.2 Mobile-originating case

The P-CSCF shall respond to all INVITE requests with a 100 (Trying) provisional response.

Upon receiving a response (e.g. 183 (Session Progress), 200 (OK)) to the initial INVITE request, the P-CSCF:

- if a media authorization token is generated by the PCF as specified in RFC 3313 [31] (i.e. when service-based local policy control is applied), insert the P-Media-Authorization header containing that media authorization token.

When the P-CSCF sends the UPDATE request towards the S-CSCF, the P-CSCF shall also include the gprs-charging-info parameter in the P-Charging-Vector header. See subclause 5.2.7.4 for further information on the GPRS charging information.

5.2.7.3 Mobile-terminating case

When the P-CSCF receives an initial INVITE request destined for the UE, it will contain the URL of the UE in the Request-URI, and a single pre-loaded Route header. The received initial INVITE will also have a list of Record-Route headers. Prior to forwarding the initial INVITE to the URL found in the Request-URI, the P-CSCF shall:

- if a media authorization token is generated by the PCF as specified in RFC 3313 [31] (i.e. when service-based local policy control is applied), insert the P-Media-Authorization header containing that media authorization token.

In addition, the P-CSCF shall respond to all INVITE requests with a 100 (Trying) provisional response.

When the P-CSCF sends 180 (Ringing) or 200 (OK) (to INVITE) towards the S-CSCF, the P-CSCF shall also include the gprs-charging-info parameter in the P-Charging-Vector header. See subclause 5.2.7.4 for further information on the GPRS charging information.

5.2.7.4 GPRS charging identifier

The GPRS charging information shall be coded as the gprs-charging-info parameter within the P-Charging-Vector header as described in subclause 7.2.6.

The gprs-charging-info parameter shall contain one ggsn child parameter and one or more child gcid parameters. Each gcid child parameter within gprs-charging- info corresponds to a PDP context that was established at the GGSN for a UE. Each gcid parameter contains pdp-id, flow-index and auth-token child parameters. The pdp-id parameter shall be populated with the PDP context identifier that the P-CSCF obtained from the GGSN. The flow-index parameter shall be populated with the relative index to the media stream in the SDP for the PDP context. The auth-token parameter shall be populated with the authorization token that is associated with this PDP context for a media stream. For more information about the PDP contexts for media, see subclause 9.2.5. For the case of a PDP context that is used for signalling, the flow-index and auth-token parameters shall be set to 0.

5.2.8 Call release

5.2.8.1 P-CSCF-initiated call release

5.2.8.1.1 Cancellation of a session currently being established

Upon receipt of an indication that radio coverage is no longer available for a served user, for whom one ore more ongoing multimedia session are currently being established, the P-CSCF shall cancel the related dialogs by sending out a CANCEL request according to the procedures described in RFC 3261 [26].

5.2.8.1.2 Release of an existing session

Upon receipt of an indication that the radio interface resources are no longer available for a served user, for whom one or more ongoing session exists, the P-CSCF shall release each of the related dialogs by applying the following steps:

1) if the P-CSCF serves the calling user of a session it shall generate a BYE request based on the information saved for the related dialog, including:

   - a Request-URI, set to the stored Contact header provided by the called user;
   - a To header, set to the To header value as received in the 200 (OK) response for the initial INVITE request;
   - a From header, set to the From header value as received in the initial INVITE request;
   - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
   - a CSeq header, set to the CSeq value that was stored for the direction from the calling to the called user, incremented by one;
   - a Route header, set to the routeing information towards the called user as stored for the dialog;
   - further headers, based on local policy or the requested session release reason.

2) If the P-CSCF serves the called user of a session it shall generate a BYE request based on the information saved for the related dialog, including:

   - a Request-URI, set to the stored Contact header provided by the calling user;
   - a To header, set to the From header value as received in the initial INVITE request;
   - a From header, set to the To header value as received in the 200 (OK) response for the initial INVITE request;
   - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
   - a CSeq header, set to the CSeq value that was stored for the direction from the called to the calling user, incremented by one – if no CSeq value was stored for that session it shall generate and apply a random number within the valid range for CSeqs;
   - a Route header, set to the routeing information towards the calling user as stored for the dialog;
   - further headers, based on local policy or the requested session release reason.

3) send the so generated BYE request towards the indicated user.

4) upon receipt of the 2xx responses for the BYE request, shall delete all information related to the dialog and the related multimedia session.

5.2.8.1.3 Abnormal cases

Upon receipt of a request on a dialog for which the P-CSCF initiated session release, the P-CSCF shall terminate this received request and answer it with a 481 (Call/Transaction Does Not Exist) response.

5.2.8.2 Call release initiated by any other entity

When the P-CSCF receives a 2xx response for a BYE request matching an existing dialog, it shall delete all the stored information related to the dialog.

5.2.9 Subsequent requests

5.2.9.1 Mobile-originating case

For a reINVITE request from the UE, when the P-CSCF sends the UPDATE request towards the S-CSCF, the P-CSCF shall include the updated gprs-charging-info parameter in the P-Charging-Vector header. See subclause 5.2.7.4 for further information on the GPRS charging information.

5.2.9.2 Mobile-terminating case

For a reINVITE request destined towards the UE, when the P-CSCF sends 200 (OK) response (to the INVITE request) towards the S-CSCF, the P-CSCF shall include the updated gprs-charging-info parameter in the P-Charging-Vector header. See subclause 5.2.7.4 for further information on the GPRS charging information.

5.2.10 Emergency service

The P-CSCF shall inspect the Request URI of all INVITE requests for known emergency numbers and emergency URLs from a configurable list. If the P-CSCF detects that the Request-URI of the INVITE request matches one of the numbers in this list, the INVITE request shall not be forwarded. The P-CSCF shall answer the INVITE request with a 380 (Alternative Service) response.

The 380 (Alternative Service) response shall contain a Content-Type header field with the value set to associated MIME type of the 3GPP IMS XML body as described in subclause 7.6.1.

The 3GPP IMS XML body shall contain an <alternative-service> element that indicates the parameters of the alternative service. The <type> child element shall be set to "emergency" to indicate that it was an emergency call. An operator configurable <reason> child element shall be included with a reason phrase.

The P-CSCF shall have a configurable list of emergency numbers and emergency URLs (e.g. sos@domain). The list is used to determine whether the INVITE is destined for an emergency centre or not.

5.3 Procedures at the I-CSCF

5.3.1 Registration procedure

5.3.1.1 General

During the registration procedure the I-CSCF shall behave as a stateful proxy.

5.3.1.2 Normal procedures

When I-CSCF receives a REGISTER request, the I-CSCF starts the user registration status query procedure to the HSS as specified in 3GPP TS 29.228 [14].

Prior to performing the user registration query procedure to the HSS, the I-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14].

If the user registration status query response from the HSS includes a valid SIP URI, the I-CSCF shall:

1) replace the Request-URI of the received REGISTER request with the SIP URL received from the HSS in the Server-Name AVP;

2) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and

3) forward the REGISTER request to the indicated S-CSCF.

If the user registration status query response from the HSS includes a list of capabilities, the I-CSCF shall:

1) select a S-CSCF that fulfils the indicated mandatory capabilities – if more then one S-CSCFs fulfils the indicated mandatory capabilities the S-CSCF which fulfils most of the possibly additionally indicated optional capabilities;

2) replace the Request-URI of the received REGISTER request with the URI of the S-CSCF;

3) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and

4) forward the REGISTER request to the selected S-CSCF.

When the I-CSCF receives a 2xx response to a REGISTER request, the I-CSCF shall proxy the 2xx response to the P-CSCF.

5.3.1.3 Abnormal cases

In the case of SLF query, if the SLF does not send HSS address to the I-CSCF, the I-CSCF shall send back a 403 (Forbidden) response to the UE.

If the HSS sends a negative response to the user registration status query request, the I-CSCF shall send back a 403 (Forbidden) response.

If the the user registration status query procedure cannot be completed, e.g. due to time-out or incorrect information from the HSS, the I-CSCF shall send back a 480 (Temporarily Unavailable) response to the UE.

If a selected S-CSCF:

- does not respond to the REGISTER request and its retransmissions by the I-CSCF; or

- sends back a 3xx response or 480 (Temporarily Unavailable) response;

the I-CSCF shall select a new S-CSCF as described in subclause 5.3.1.2, based on the capabilities indicated from the HSS. The newly selected S-CSCF shall not be one of any S-CSCFs selected previously during this same registration procedure.

If the I-CSCF cannot select a S-CSCF which fulfils the mandatory capabilities indicated by the HSS, the I-CSCF shall send back a 600 (Busy Everywhere) response to the user.

5.3.2 Further initial requests

5.3.2.1 Normal procedures

The I-CSCF may behave as a stateful proxy for further initial requests.

When the I-CSCF receives an initial request, that either does not contain a Route header or contains a single Route header pointing to itself, the I-CSCF shall start the user location query procedure to the HSS as specified in 3GPP TS 29.228 [14] for the called user, indicated in the Request-URI. Prior to performing the user location query procedure to the HSS, the I-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14].

Upon successful user location query, when the response contains the URL of the assigned S-CSCF, the I-CSCF shall:

1) if present, remove its own SIP URL from the topmost Route header;

2) insert the URL received from the HSS as the topmost Route header;

3) store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header. If no icid parameter was found, then create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header;

4) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and

5) forward the request based on the topmost Route header.

Upon successful user location query, when the response contains information about the required S-CSCF capabilities, the I-CSCF shall:

1) select a S-CSCF according to the method described in 3GPP TS 29.228 [14];

2) insert the URL of the selected S-CSCF as the topmost Route header field value;

3) execute the procedure described in step 2 and 3 in the above paragraph (upon successful user location query, when the response contains the URL of the assigned S-CSCF); and

4) forward the request to the selected S-CSCF.

Upon an unsuccessful user location query when the response from the HSS indicates that the user does not exist, the I-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 404 (Not found) or 604 (Does not exist anywhere) in the case the user is not a user of the home network.

Upon an unsuccessful user location query when the response from the HSS indicates that the user is not registered and no services are provided for such a user, the I-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 480 (Temporarily unavailable) if the user is recognized as a valid user, but is not registered at the moment and it does not have services for unregistered users.

When the I-CSCF receives an initial request containing more than one Route header, the I-CSCF shall:

1) remove its own SIP URL from the topmost Route header;

2) apply the procedures as described in subclause 5.3.3; and

3) forward the request based on the topmost Route header if present, or based on the Request-URI, in case no topmost Route header is available.

NOTE: In accordance with SIP the I-CSCF can add its own routeable SIP URL to the top of the Record-Route header to any request, independently of whether it is an initial request, or whether topology hiding is performed. The P-CSCF will ignore any Record-Route header that is not in the initial request of a dialog.

When the I-CSCF receives a response to an initial request (e.g. 183 or 2xx), the I-CSCF shall store the values from the P-Charging-Function-Addresses header, if present. If the next hop is outside of the current network, then the I-CSCF shall remove the P-Charging-Function-Addresses header prior to forwarding the message.

5.3.2.2 Abnormal cases

In the case of SLF query, if the SLF does not send HSS address to the I-CSCF, the I-CSCF shall send back a 404 (Not Found) response to the UE.

If the HSS sends a negative response to the user location query, the I-CSCF shall send back a 404 (Not Found) response.

If the I-CSCF receives a CANCEL request and if the I-CSCF finds an internal state indicating a pending Cx transaction with the HSS, the I-CSCF:

- shall answer the CANCEL with a 200 OK;

- shall answer the original request with a 487 Request Terminated; and

- shall silently discard the later arriving (pending) Cx answer message from the HSS.

5.3.3 THIG functionality in the I-CSCF(THIG)

5.3.3.1 General

The following procedures shall only be applied if topology hiding is required by the network. The network requiring topology hiding is called the hiding network.

NOTE: Requests and responses are handled independently therefore no state information is needed for that purpose within an I-CSCF(THIG).

All headers which reveal topology information, such as Via, Route, Record-Route, P-Service-Route, shall be subject to topology hiding.

Upon receiving an incoming REGISTER request for which topology hiding has to be applied and which includes a Path header, the I-CSCF(THIG) shall add the routeable SIP URL of an I-CSCF(THIG) to the top of the Path header. The inserted SIP URL may include an indicator that identifies the direction of subsequent requests received by the I-CSCF.

This indicator may e.g., be a unique header parameter, a username or a dedicated port. Any subsequent request that includes this indicator (in the Route header) or arrives at the dedicated port indicates that the request was sent by the S-CSCF toward the P-CSCF.

Upon receiving an incoming initial request for which topology hiding has to be applied and which includes a Record-Route header, the I-CSCF(THIG) shall add its own routeable SIP URL to the top of the Record-Route header.

Upon receiving an outgoing initial request for which topology hiding has to be applied and which includes P-Charging-Function-Addresses header, the I-CSCF(THIG) shall remove the P-Charging-Function-Addresses header prior to forwarding the message.

5.3.3.2 Encryption for topology hiding

Upon receiving an outgoing request/response from the hiding network the I-CSCF(THIG) shall perform the encryption for topology hiding purposes, i.e. the I-CSCF(THIG) shall:

1) use the whole header values which were added by one or more specific entity of the hiding network as input to encryption, besides the UE entry;

2) not change the order of the headers subject to encryption when performing encryption;

3) use for one encrypted string all received consecutive header entries subject to encryption, regardless if they appear in separate consecutive headers or if they are consecutive entries in a comma separated list in one header;

4) construct an NAI in the form of 'username@realm',where the username part is the encrypted string, and the realm is the name of the encrypting network.

5) append a "tokenized-by=" tag and set it to the value of the encrypting network's name, after the constructed NAI;

6) form one valid entry for the specific header out of the resulting NAI, e.g. prepend "SIP/2.0/UDP" for Via headers or "sip:" for Route and Record-Route headers.

NOTE 1: Even if consecutive entries of the same network in a specific header are encrypted, they will result in only one encrypted header entry. For example:

```
Via: SIP/2.0/UDP icscf1_s.home1.net;lr,
     SIP/2.0/UDP Token( SIP/2.0/UDP scscf1.home1.net;lr,
                        SIP/2.0/UDP pcscf1.home1.net;lr)@home1.net;
                                    tokenized-by=home1.net,
     SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
```

NOTE 2: If multiple entries of the same network are within the same type of headers, but they are not consecutive, then these entries will be tokenized to different strings. For example:

```
Route:  sip:icscf1_s.home1.net;lr,
        sip:Token(sip:scscf1.home1.net;lr)@home1.net;tokenized-by=home1.net,
        sip:as1.foreign.net;lr,
        sip:Token(sip:scscf1.home1.net;lr,
                  sip:pcscf1.home1.net;lr)@home1.net;tokenized-by=home1.net,
        sip:[5555::aaa:bbb:ccc:ddd]
```

5.3.3.3 Decryption for Topology Hiding

Upon receiving and incoming requests/response to the hiding network the I-CSCF(THIG) shall perform the decryption for topology hiding purposes, i.e. the I-CSCF shall:

1) identify NAIs encrypted by the network this I-CSCF belongs to within all headers of the incoming message;

2) use the user part of those NAIs that carry the identification of the hiding network within the value of the tokenized-by tag as input to decryption;

3) use as encrypted string the user part of the NAI which follows the sent-protocol (for Via Headers, e.g. "SIP/2.0/UDP") or the URI scheme (for Route and Record-Route Headers, e.g. "sip:");

4) replace all content of the received header which carries encrypted information with the entries resulting from decryption.

EXAMPLE: An encrypted entry to a Via header that looks like:

```
Via:    SIP/2.0/UDP Token(SIP/2.0/UDP scscf1.home1.net;lr,
        SIP/2.0/UDP pcscf1.home1.net;lr)@home1.net;tokenized-by=home1.net
```

will be replaced with the following entries:

```
Via: SIP/2.0/UDP scscf1.home1.net;lr, SIP/2.0/UDP pcscf1.home1.net;lr
```

NOTE: Motivations for these decryption procedures are e.g. to allow the correct routeing of a response through the hiding network, to enable loop avoidance within the hiding network, or to allow the entities of the hiding network to change their entries within e.g. the Record-Route header.

5.4 Procedures at the S-CSCF

5.4.1 Registration and authentication

5.4.1.1 Introduction

The S-CSCF shall act as the SIP registrar for all UAs of the IM CN subsystem with public user identities.

The S-CSCF shall support the use of the Path and P-Service-Route header. The S-CSCF must also support the Require and Supported headers. The Path header is only applicable to the REGISTER request and its 200 (OK) response. The P-Service-Route header is only applicable to the 200 (OK) response of REGISTER.

The network operator defines minimum and maximum times for each registration. These values are provided within the S-CSCF.

The procedures for notification concerning automatically registered public user identities of a user are described in subclause 5.4.2.1.2.

5.4.1.2 Initial registration and user-initiated reregistration

5.4.1.2.1 Initial registration

Upon receipt of a REGISTER request for a user that is not registered and for which also no authentication is currently ongoing (i.e. timer reg-await-auth is not running), the S-CSCF shall:

1) identify the user by the public user identity as received in the To header and the private user identity as received in the username field in the Authorization header of the REGISTER request;

2) check if the P-Visited-Network header is included in the REGISTER request, and if it is included identify the visited network by the value of this header;

3) check the value of the Expires header. The S-CSCF shall only proceed with the following procedures if the Expires header is set to a value greater than zero;

4) select an authentication vector for the user. If no authentication vector for this user is available, after the S-CSCF has performed the Cx Multimedia Authentication procedure with the HSS, as described in 3GPP TS 29.229 [15], the S-CSCF shall select an authentication vector as described in 3GPP TS 33.203 [19].

   Prior to performing Cx Multimedia Authentication procedure with the HSS, the S-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14];

NOTE 1: At this point the S-CSCF informs the HSS, that the user currently registering will be served by the S-CSCF by passing its SIP URL to the HSS. This will be indicated by the HSS for all further incoming requests to this user, in order to direct all these requests directly to this S-CSCF.

5) store the icid parameter received in the P-Charging-Vector header;

6) remove the P-Access-Network-Info header and may act upon the contents accordingly;

7) challenge the user by generating a 401 (Unauthorized) response for the received REGISTER request, including a WWW-Authenticate header which transports:

   - the home network identification in the realm field;
   - the RAND and AUTN parameters and optional server specific data for the UE in the nonce field;
   - the security mechanism, which is AKAv1-MD5, in the algorithm field;
   - the IK (Integrity Key) parameter for the P-CSCF in the ik field (see subclause 7.2.3);
   - optionally the CK (Cipher Key) parameter for the P-CSCF in the ck field (see subclause 7.2.3);

8) send the so generated 401 (Unauthorized) response towards the UE; and,

9) start timer reg-await-auth which guards the receipt of the next REGISTER request.

While timer reg-await-auth is running, upon receipt of a REGISTER request, the S-CSCF shall:

1) identify the user by the public user identity as received in the To header and the private user identity as received in the username field in the Authorization header of the REGISTER request;

2) stop timer reg-await-auth;

3) check whether the P-CSCF included the Integrity-protection field of the Authorization header set to yes, indicating that the REGISTER request was received integrity protected. The S-CSCF shall only proceed with the following steps it the integrity check parameter is included;

4) check whether an Authorization header is included, containing:

   - the private user identity of the user in the username field;
   - the algorithm which is AKAv1-MD5 in the algorithm field; and
   - the RES parameter needed for the authentication procedure in the response field.

   The S-CSCF shall only proceed with the following steps in this paragraph if the RES parameter was included;

5) check whether the received RES parameter and the XRES parameter match. The XRES parameter was received from the HSS as part of the Authentication Vector. The S-CSCF shall only proceed with the following steps if RES and XRES are matching;

6) after performing the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.229 [15], store the following information in the local data:

   - the list of public user identities associated to the user, including the own public user identity under registration and the implicitly registered due to the received REGISTER request. Each public user identity is identified as either barred or non-barred; and,
   - the user profile of the user including initial Filter Criteria;

7) bind to each non-barred registered public user identity all registered contact information;

NOTE 2: There might be more then one contact information available for one public user identity.

NOTE 3: The barred public user identities are not bound to the contact information.

8) check whether a Path header was included in the REGISTER request and construct a list of preloaded Route headers from the list of entries in the Path header. The S-CSCF shall preserve the order of the preloaded Route headers and bind them to the contact information that was received in the REGISTER message;

NOTE 4: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

9) determine the duration of the registration by checking the value of the Expires header in the received REGISTER request. The S-CSCF may adjust the duration of the registration due to local policy;

10) store the icid parameter received in the P-Charging-Vector header;

11) remove the P-Access-Network-Info header and may act upon the contents accordingly;

12) create a 200 (OK) response for the REGISTER request, including:

- an expiration time in the Expires header, using one value provided within the S-CSCF, according to the local policy of the network, if this expiration time is shorter than the requested expiry time received from the UE; and,
- the list of received Path headers;
- a P-Associated-URI header containing the list of public user identities that the user is authorized to use. Such a collection of public user identities may or may not be implicitly registered by the network. Using information supplied by the HSS, the P-Associated-URI header will indicate the default public user identity to be used by the P-CSCF in conjunction with the procedures for the P-Asserted-Identity header;

Editor's note: The mechanism for indicating this default public user identity is yet to be agreed.

- a P-Service-Route header containing:
  - the SIP URL identifying the S-CSCF; and,
  - an indication that requests routed via the service route (i.e. from the P-CSCF to the S-CSCF) shall be treated as for the mobile-originating case. This indication may e.g. be in a URI parameter, a character string in the user part or be a port number;
  - if network topology hiding is required a SIP URL identifying an I-CSCF(THIG) as the topmost entry;

13) send the so created 200 (OK) response to the UE;

14) send a third-party REGISTER request, as described in subclause 5.4.1.7, to each Application Server that matches the Filter Criteria from the HSS for the REGISTER event; and,

NOTE 5: If this registration is a reregistration, the Filter Criteria already exists in the local data.

15) handle the user as registered for the duration indicated in the Expires header.

5.4.1.2.2 User-initiated reregistration

Upon receipt of a REGISTER request for an already registered user, the S-CSCF shall:

1) identify the user by the public user identity as received in the To header and the private user identity as received in the From header of the REGISTER request;

2) check whether the P-CSCF included the Integrity-protection field of the Authorization header set to yes, indicating that the REGISTER request was received integrity protected. The S-CSCF shall only proceed with the following steps if the field is set to yes;

3) check if the user needs to be reauthenticated.

   The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for registration requests received without integrity protection by the P-CSCF. The information that a REGISTER request was received integrity protected at the P-CSCF may be used as part of the decision to challenge the user.

   If the user needs to be reauthenticated, the S-CSCF shall proceed with the procedures as described for the initial REGISTER in subclause 5.4.1.2.1, beginning with step 4). If the user does not need to be reauthenticated, the S-CSCF shall proceed with the following steps in this paragraph;

4) check whether an Expires timer is included in the REGISTER request and its value. If the Expires header indicates a zero value, the S-CSCF shall perform the deregistration procedures as described in subclause 5.4.1.4. If the Expires header does not indicate zero, the S-CSCF shall proceed with the procedures as described for the second REGISTER in subclause 5.4.1.2, beginning with step 7); and

5) remove the P-Access-Network-Info header and may act upon the contents accordingly.

5.4.1.2.3 Abnormal cases

The S-CSCF need not challenge an unprotected REGISTER request for a private user identity that already has a registration in process, but instead return a 500 (Server Internal Error) response. The response shall contain a Retry-After header with a value indicating a time the UE shall wait before resending the request.

In the case that the authentication response (RES) from the UE does not match with XRES and the request was correctly integrity protected (it is indicated by the P-CSCF), or the S-CSCF determines that no response will be received from the UE (e.g. it may be unreachable due to loss of radio coverage), and the authentication response was triggered by an initial registration or a UE initiated reauthentication, the S-CSCF shall either:

- start a network initiated re-authentication procedure as defined in subclause 5.4.1.6; or
- send a further challenge 401 (Unauthorized) to the UE.

In the case that the authentication response (RES) from the UE does not match with XRES and the request was correctly integrity protected (it is indicated by the P-CSCF), or the S-CSCF determines that no response will be received from the UE (e.g. it may be unreachable due to loss of radio coverage), and the authentication response was triggered by a network initiated reauthentication the S-CSCF shall either:

- attempt a further authentication challenge; or
- deregister the user and terminate any ongoing sessions for all public user identities associated with the private user identity being authenticated, and release resources allocated to those sessions.

In the case that the REGISTER request from the UE containing an authentication response indicates that the authentication challenge was invalid and with no RES or AUTS parameter, the S-CSCF shall:

- respond with the relevant 4xx response (e.g. 401 (Unauthorized) to initiate a further authentication attempt, or 403 (Forbidden) if the authentication attempt is to be abandoned).

In the case that the REGISTER request from the UE containing an authentication response indicates that the authentication challenge was invalid but contains the AUTS parameter, the S-CSCF will fetch new authentication vectors from the HSS, including AUTS and RAND in the request to indicate a resynchronisation. On receipt of these vectors from the HSS, the S-CSCF shall:

- send a 401 Unauthorized to initiate a further authentication attempt, using these new vectors.

In the case that the expiration timer from the UE is too short to be accepted by the S-CSCF, the S-CSCF shall:

- reject the REGISTER request with a 423 (Interval Too Brief) response, containing a Min-Expires header with the minimum registration time the S-CSCF will accept.

On receiving a failure response to one of the third-party REGISTER requests, the S-CSCF may initiate network-initiated deregistration procedure based on the information in the Filter Criteria. If the Filter Criteria does not contain instruction to the S-CSCF regarding the failure of the contact to the Application Server, the S-CSCF shall not initiate network-initiated deregistration procedure.

5.4.1.3 Authentication and reauthentication

Authentication and reauthentication is performed by the registration procedures as described in subclause 5.4.1.2.

5.4.1.4 User-initiated deregistration

When S-CSCF receives a REGISTER request with the Expires header field containing the value zero, the S-CSCF shall:

- deregister the public user identity found in the To header field together with the implicitly registered public user identities;
- send a third-party REGISTER request, as described in subclause 5.4.1.7, to each Application Server that matches the Filter Criteria from the HSS for the REGISTER event.

Based on operators' policy the S-CSCF can request from HSS to either be kept or cleared as the S-CSCF allocated to this subscriber. In both cases the state of the subscriber identity is stored as unregistered in the HSS and the S-CSCF. Based on HSS decision, the S-CSCF may either keep all or only a part of the user profile or removes it.

5.4.1.5 Network-initiated deregistration

When a network-initiated deregistration event occurs for a public user identity, and the UE has subscribed for the registration-state event, the S-CSCF shall generate a NOTIFY request in order to inform the UE of the network-initiated deregistration event for that public user identity. The S-CSCF shall set the event header to the name of the event package, which provides information about the registration state of the UE.

When a network-initiated deregistration event occurs for a public user identity, and the P-CSCF has subscribed for registration events for that public user identity, the S-CSCF shall generate a NOTIFY request in order to inform the P-CSCF of the network initiated deregistration event for that public user identity. The S-CSCF shall set the event header to the name of the event package, which provides information about the registration state of the UE.

If the network-initiated deregistration is for a set of public user identities associated with the subscriber, the NOTIFY shall send the registration state of all public user identities of the subscriber.

Editor's note: The possible values of the event header are: presence, registration-state, a new subpackage of presence.

Also, the S-CSCF shall send a third-party REGISTER request, as described in subclause 5.4.1.7, to each Application Server that matches the Filter Criteria from the HSS for the REGISTER event.

The S-CSCF shall then deregister the public user identity together with the implicitly registered public user identities.

5.4.1.6 Network-initiated reauthentication

The S-CSCF may request a subscriber to reauthenticate at any time, based on a number of possible operator settable triggers as described in subclause 5.4.1.2.

If the S-CSCF is informed that a private user identity needs to be re-authenticated, the S-CSCF shall generate a NOTIFY request on all dialogs (i.e. the dialog between S-CSCF and the UE and additionally between S-CSCF and P-CSCF) which have been established due to subscription to the registration-state event package of that user. The S-CSCF shall populate the content of the NOTIFY request and additionally shall:

- set the Request-URI and Route header to the saved route information during subscription;
- set the Event header to the "registration-state" value; and
- indicate a public user identity of the user for which the private user identity needs to be re-authenticated in the body of the NOTIFY request with registration state "re-authenticate".

Afterwards the S-CSCF shall:

- wait for the user to reauthenticate (see subclause 5.4.1.2).

NOTE: Network initiated re-authentication might be requested from the HSS or may occur due to internal processing within the S-CSCF.

In case S-CSCF receives no data it can authenticate the subscriber from, the S-CSCF may as an implementation option try to request the UE by other means to re-authenticate, e.g. by sending a REFER method in order to request a REGISTER request.

When generating the NOTIFY request, the S-CSCF shall shorten the validity of subscriber's registration timer to an operator defined value that will allow the user to be re-authenticated. If user fails to reauthenticate while its registration is still valid, the S-CSCF shall deregister the private user identity as described in subclause 5.4.1.5 and terminate the ongoing sessions of that user.

5.4.1.7 Notification of Application Servers about registration status

If the registration procedure described in subclauses 5.4.1.2, 5.4.1.4 or 5.4.1.5 (as appropriate) was successful, the S-CSCF shall send a third-party REGISTER request to each Application Server with the following information:

a) the Request-URI shall contain the AS's SIP URL;

b) the From header shall contain the S-CSCF's SIP URL;

c) the To header shall contain the public user identity as contained in the REGISTER request received form the UE;

d) the Contact header shall contain the S-CSCF's SIP URL;

e) for initial registration and user-initiated reregistration (subclause 5.4.1.2), the Expires header shall contain the same value that the S-CSCF returned in the 200 (OK) response for the REGISTER request received form the UE;

f) for user-initiated deregistration (subclause 5.4.1.4) and network-initiated deregistration (subclause 5.4.1.5), the Expires header shall contain the value zero;

g) for initial registration and user-initiated reregistration (subclause 5.4.1.2), a message body shall be included in the REGISTER request if there is Filter Criteria indicating the need to include HSS provided data for the REGISTER event (e.g. HSS may provide AS specific data to be included in the third-party REGISTER, such as IMSI to be delivered to IM SSF). If there is a service information XML element provided in the HSS Filter Criteria for an AS (see 3GPP TS 29.228 [14]), then it shall be included in the message body of the REGISTER request within the <service-info> XML element as described in subclause 7.6. For the messages including the 3GPP IMS XML body, set the value of the Content-Type header to include the MIME type specified in subclause 7.6;

h) for initial registration, the P-Charging-Vector header shall contain the same icid parameter that the S-CSCF received in the original REGISTER request from the UE;

i) for initial registration, a P-Charging-Function-Addresses header (see subclause 7.2.5) shall be populated with values received from the HSS if the message is forwarded within the S-CSCF home network.

5.4.2 Subscription and notification

5.4.2.1 Subscriptions to S-CSCF events

5.4.2.1.1 Subscription to the event providing registration state

When an incoming SUBSCRIBE request addressed to S-CSCF arrives containing the Event header with the registration-state event package, the S-CSCF shall generate a 2xx response acknowledging the SUBSCRIBE request and indicating that the subscription was successful. Furthermore, the response shall include:

- an Expires header which either contains the same or a decreased value as the Expires in SUBSCRIBE request; and

- a Contact header which is an identifier generated within the S-CSCF that will help to correlate refreshes for the SUBSCRIBE.

Afterwards the S-CSCF shall perform the procedures for notification about registration state as described in subclause 5.4.2.1.2.

5.4.2.1.2 Notification about registration state

Notification of the registration state shall affect the non-barred public user identities. The barred public user identities shall never be sent in a NOTIFY message.

If the registration state of one or more public user identities changes, the S-CSCF shall generate a NOTIFY request on all dialogs which have been established due to subscription to the registration-state event package of that user. For each NOTIFY request, the S-CSCF shall:

- set the Request-URI and Route header to the saved route information during subscription;

- set the Event header to the "registration-state" value;

- indicate registration state "open" for all public user identities which are currently registered;

- indicate registration state "closed" for all public user identities which are currently deregistered; and

- indicate within the "<note>" information of those public user identities which will be automatically reregistered the "automatically by" information, followed by the specific public user identity which will cover the reregistration.

EXAMPLE: If sip:user1_public1@home1.net is registered, the public user identity sip:user1_public2@home1.net can automatically be registered. Therefore the entries in the body of the NOTIFY request look like:

```
<tuple name="sip:user1_public1@home1.net">
  <status><basic>open</basic><<<</status>
</tuple>

<tuple name="sip:user1_public2@home1.net">
  <status> <basic>open</basic> </status>
  <note>automatically by sip:user1_public1@home1.net</note>
</tuple>
```

Afterwards the S-CSCF shall send the generated NOTIFY request on the dialog and await a 2xx response.

5.4.3 General treatment for all dialogs and standalone transactions excluding requests terminated by the S-CSCF

5.4.3.1 Determination of mobile-originated or mobile-terminated case

Upon receipt of an initial request or a refresh request or a stand-alone transaction, the S-CSCF shall:

- perform the procedures for the mobile-originating case as described in subclause 5.4.3.2 if the request makes use of the information for mobile-originating calls, which was added to the Path header entry of the S-CSCF during registration (see subclause 5.4.1.2), e.g. the message is received at a certain port or the topmost Route header contains a specific user part or parameter; or,

- perform the procedures for the mobile-terminating case as described in subclause 5.4.3.3 if this information is not used by the request.

5.4.3.2 Requests initiated by the served user

When the S-CSCF receives from the served user an initial request for a dialog or a request for a standalone transaction, prior to forwarding the request, the S-CSCF shall:

- determine whether the request contains a barred public user identity in the From or Remote-Party-ID header fields of the request or not. In case any of the said header fields contains a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 403 (Forbidden) response. Otherwise, continue with the rest of the steps;

- remove its own SIP URL from the topmost Route header;

- if the outgoing Request-URI is a TEL URL, the S-CSCF shall translate the E.164 address (see RFC 2806 [22]) to a globally routeable SIP URL using an ENUM/DNS translation mechanism with the format specified in RFC 2916 [24]. Databases aspects of ENUM are outside the scope of the present document. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or an appropriate SIP response shall be sent to the originator;

- check if P-Original-Dialog-ID header is present in the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request. The od-to-tag, od-from-tag and od-call-idparameter values from the P-Original-Dialog-ID header may be used as additional parameters when searching for existing dialogs. Local data shall be updated to indicate that this Application Server has been contacted for the initial request. The S-CSCF shall determine the next hop using initial filter criteria and local data on status of which Application Servers have been contacted. If the next hop is another Application Server, the S-CSCF shall retain the P-Original-Dialog-ID header in the request. If the next hop is not an Application Server, the S-CSCF shall remove the P-Original-Dialog-ID header from the request;

- check whether the initial request matches the initial filter criteria, the S-CSCF shall forward this request to that application server, then check for matching of the next following filter criteria of lower priority, and apply the filter criteria on the SIP method received from the previously contacted application server as described in 3GPP TS 23.218 [5] subclause 6.4. Depending on the result of the previous process, the S-CSCF may contact one or more application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:

  - insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL; and

  - populate the P-Original-Dialog-ID header in the message with the original To tag, From tag and Call-ID headers received in the request. See subclause 7.2.7 for further information on the original dialog identifier;

- store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header. Optionally, the S-CSCF may generate a new, globally unique icid and insert the new value in the icid parameter of the P-Charging-Vector header when forwarding the message. If the S-CSCF creates a new icid, then it is responsible for maintaining the two icid values in the subsequent messaging;

- insert an ioi-originating parameter into the P-Charging-Vector header if the next hop is an AS, I-CSCF or outside of the current network. The ioi-originating parameter shall be set to a value that identifies the sending network. The ioi-terminating parameter shall not be included;

- insert a P-Charging-Function-Addresses header (see subclause 7.2.5) populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

- in the case where the S-CSCF has knowledge of an associated tel-URI for a SIP URL contained in the received P-Asserted-Identity header, add a second P-Asserted-Identity header containing this tel-URI;

- in the case where the network operator has policy to provide privacy on From headers, and such privacy is required for this dialog, change the From header to "Anonymous". Network policy may also require the removal of the display field;

- determine the destination address (e.g. DNS access) using the URL placed in the topmost Route header if present, otherwise based on the Request-URI;

- if network hiding is needed due to local policy, put the address of the I-CSCF(THIG) to the topmost route header;

- in case of an initial request for a dialog the S-CSCF shall create a Record-Route header containing its own SIP URL and save the necessary Record-Route header fields and the Contact header from the request in order to release the dialog when needed;

- remove the P-Access-Network-Info header and act upon the contents accordingly; and

- route the request based on SIP routeing procedures.

When the S-CSCF receives any response to the above request, the S-CSCF may:

- apply any privacy required by RFC 3323 [33] to the P-Asserted-Identity header.

NOTE 1: This header would normally only be expected in 1xx or 2xx responses.

NOTE 2: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3323 [33].

When the S-CSCF receives a response to the initial request for a dialog, it shall save the necessary Record-Route header fields and the Contact header from the response in order to release the dialog if needed.

When the S-CSCF receives from the served user a refresh request for a dialog, prior to forwarding the request the S-CSCF shall:

- remove its own URL from the topmost Route header;

- create a Record-Route header containing its own SIP URL and save the Contact header from the request in order to release the dialog when needed;

- remove the P-Access-Network-Info header and act upon the contents accordingly; and

- route the request based on the topmost Route header.

When the S-CSCF receives a response to the refresh request for a dialog, it shall save the necessary Record-Route header fields and the Contact header from the response in order to release the dialog if needed.

When the S-CSCF receives from the served user a subsequent request other than refresh request for a dialog, prior to forwarding the request the S-CSCF shall:

- remove its own URL from the topmost Route header;
- remove the P-Access-Network-Info header and act upon the contents accordingly; and
- route the request based on the topmost Route header.

5.4.3.3 Requests terminated at the served user

When the S-CSCF receives, destined for a registered served user, an initial request for a dialog or a request for a standalone transaction, prior to forwarding the request, the S-CSCF shall:

1) remove its own URL from the topmost Route header;
2) check if P-Original-Dialog-ID header is present in the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request. The od-to-tag, od-from-tag and od-call-id parameter values from the P-Original-Dialog-ID header may be used as additional parameters when searching for existing dialogs. The S-CSCF shall determine the next hop using initial filter criteria. If the next hop is another Application Server, the S-CSCF shall retain the P-Original-Dialog-ID header in the message of the request. If the next hop is not an Application Server, the S-CSCF shall remove the P-Original-Dialog-ID header from the request;
3) check whether the initial request matches the initial filter criteria, the S-CSCF shall forward this request to that application server, then check for matching of the next following filter criteria of lower priority, and apply the filter criteria on the SIP method received from the previously contacted application server as described in 3GPP TS 23.218 [5] subclause 6.5. Depending on the result of the previous process, the S-CSCF may contact one or more application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:
   a) insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL; and
   b) populate the P-Original-Dialog-ID header in the message with the original To tag, From tag and Call-ID headers received in the request. See subclause 5.4.3.4 for further information on the original dialog identifier;
4) insert a P-Charging-Function-Addresses header (see subclause 7.2.4) populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;
5) store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header;
6) store the value of the ioi-originating parameter received in the P-Charging-Vector header, if present. The ioi-originating parameter identifies the sending network of the request message. The ioi-originating parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS;
7) in case there are no Route headers in the request, then determine, from the destination public user identity, the list of preloaded routes saved during registration or re-registration, as described in subclause 5.4.1.2;
8) build the Route header field with the values determined in the previous step;
9) determine, from the destination public user identity, the saved Contact URL where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2;
10) build a Request-URI with the contents of the saved Contact URL determined in the previous step;
11) insert a P-Called-Party-ID SIP header field including the Request-URI received in the INVITE;

12) in case of an initial request for a dialog create a Record-Route header containing its own SIP URL and save the necessary Record-Route header fields and the Contact header from the request in order to release the dialog when needed; and

13) optionally, apply any privacy required by RFC 3323 [33] to the P-Asserted-Identity header; and

NOTE: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3323 [33].

14) forward the request based on the topmost Route header.

When the S-CSCF receives, destined for an unregistered user, an initial request for a dialog or a request for a standalone transaction, the S-CSCF shall:

1) execute the procedures described in the steps 1 and 2 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction);

2) if the S-CSCF does not have the user profile, then initiate the S-CSCF Registration/deregistration notification with the purpose of downloading the relevant user profile (i.e. for unregistered user) and informing the HSS that the user is unregistered, but this S-CSCF will assess triggering of services for the unregistered user, as described in 3GPP TS 29.228 [14];

3) keep the user registration status as unregistered for the duration of the dialog. When the dialog expires, the S-CSCF shall inform appropriately the HSS according to the procedures described in 3GPP TS 29.228 [14];

4) execute the procedure described in step 3 and 4 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

   In case that no AS needs to be contacted, then S-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 480 (Temporarily unavailable) and terminate these procedures; and

5) execute the procedures described in the steps 5, 6, 11, 12, 13 and 14 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

When the S-CSCF receives a response to the initial request for a dialog (whether the user is registered or not), it shall save the necessary Record-Route header fields and the Contact header field from the response in order to release the dialog if needed. In the case where the S-CSCF has knowledge of an associated tel-URI for a SIP URL contained in the received P-Asserted-Identity header, the S-CSCF shall add a second P-Asserted-Identity header containing this tel-URI; in the case where the network operator has policy to provide privacy on To headers, and such privacy is required for this dialog, change the To header to "Anonymous". Network policy may also require the removal of the display field.

When the S-CSCF receives, destined for a served user, a refresh request for a dialog, prior to forwarding the request, the S-CSCF shall:

1) remove its own URL from the topmost Route header;

2) create a Record-Route header containing its own SIP URL and save the Contact header from the refresh request in order to release the dialog when needed;

3) remove the P-Access-Network-Info header, if it is present, and may act upon its contents accordingly; and

4) forward the request based on the topmost Route header.

When the S-CSCF receives a response to the refresh request for a dialog (whether the user is registered or not), it shall save the necessary Record-Route header fields and the Contact header field from the response in order to release the dialog if needed.

When the S-CSCF receives, destined for the served user, a subsequent request other than refresh request for a dialog, prior to forwarding the request, the S-CSCF shall:

1) remove its own URL from the topmost Route header; and

2) forward the request based on the topmost Route header.

When the S-CSCF receives a request destined for a barred public user identity, the S-CSCF shall return an appropriate unsuccessful SIP response. This response may be, e.g., a 404 (Not found) or 604 (Does not exist anywhere).

5.4.3.4 Original dialog identifier

The original dialog identifier is coded as the P-Original-Dialog-ID as described in subclause 7.2.7.

5.4.3.5 Abnormal cases

The S-CSCF shall, when contacting application servers based on the initial filter criteria, expect either a final response from the application server as the session terminates there, or the initial request message, that may be modified. In either case the message should be identified (using P-Original-Dialog-ID) as belonging to the original request forwarded by the S-CSCF.

If the S-CSCF receives a message including an P-Original-Dialog-ID that does not match any that it has forwarded to the application server it shall:

- respond to the application server with 481 Call Leg/Transaction Does Not Exist.

5.4.4 Call initiation

5.4.4.1 Initial INVITE

Void.

5.4.4.2 Subsequent requests

5.4.4.2.1 Mobile-originating case

When the S-CSCF receives the 183 response, the S-CSCF shall store the value of the received ioi-terminating parameter received in the P-Charging-Vector header, if present. The ioi-terminating parameter identifies the sending network of the response message. The ioi-terminating parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS.

When the S-CSCF receives the 183 response, the S-CSCF shall insert a P-Charging-Function-Addresses header (see subclause 7.2.5) populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS.

When the S-CSCF receives the UPDATE request, the S-CSCF shall store the gprs-charging-info parameter from the P-Charging-Vector header. The gprs-charging-info parameter shall be retained in the P-Charging-Vector header when the request is forwarded to an AS. However, the gprs-charging-info parameter shall not be included in the P-Charging-Vector header when the UPDATE request is forwarded outside the home network of the S-CSCF.

When the S-CSCF receives any request or response related to a mobile-originated dialog or standalone transaction, the S-CSCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before forwarding the message within the S-CSCF home network, including towards AS.

5.4.4.2.2 Mobile-terminating case

When the S-CSCF sends the 183 response, the S-CSCF shall insert an ioi-terminating parameter in the P-Charging-Vector header of the outgoing response if the response is sent to another network, an AS or an I-CSCF. The ioi-terminating parameter shall be set to a value that identifies the sending network of the response and the ioi-originating parameter is set to the previously received value of ioi-originating.

When the S-CSCF receives the 183 response, the S-CSCF shall insert a P-Charging-Function-Addresses header (see subclause 7.2.5) populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS.

When the S-CSCF receives 180 (Ringing) or 200 (OK) (to INVITE) responses, the S-CSCF shall store the gprs-charging-info parameter from the P-Charging-Vector header. The gprs-charging-info parameter shall be retained in the P-Charging-Vector header when the response is forwarded to an AS. However, the gprs-charging-info parameter shall

not be included in the P-Charging-Vector header when the response is forwarded outside the home network of the S-CSCF.

When the S-CSCF receives any request or response related to a mobile-originated dialog or standalone transaction, the S-CSCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before forwarding the message within the S-CSCF home network, including towards AS.

5.4.5 Call release

5.4.5.1 S-CSCF-initiated session release

5.4.5.1.1 Cancellation of a session currently being established

Upon receipt of an network internal indication to release a session which is currently being established, the S-CSCF shall cancel the related dialogs by sending the CANCEL request according to the procedures described in RFC 3261 [26].

5.4.5.1.2 Release of an existing session

Upon receipt of a network internal indication to release an existing multimedia session, the S-CSCF shall:

1) generate a first BYE request for the called user based on the information saved for the related dialog, including:
   - a Request-URI, set to the stored Contact header provided by the called user;
   - a To header, set to the To header value as received in the 200 OK response for the initial INVITE request;
   - a From header, set to the From header value as received in the initial INVITE request;
   - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
   - a CSeq header, set to the CSeq value that was stored for the direction from the calling to the called user, incremented by one;
   - a Route header, set to the routeing information towards the called user as stored for the dialog;
   - further headers, based on local policy or the requested session release reason.
2) generate a second BYE request for the calling user based on the information saved for the related dialog, including:
   - a Request-URI, set to the stored Contact header provided by the calling user;
   - a To header, set to the From header value as received in the initial INVITE request;
   - a From header, set to the To header value as received in the 200 OK response for the initial INVITE request;
   - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
   - a CSeq header, set to the CSeq value that was stored for the direction from the called to the calling user, incremented by one – if no CSeq value was stored for that session it shall generate and apply a random number within the valid range for CSeqs;
   - a Route header, set to the routeing information towards the calling user as stored for the dialog;
   - further headers, based on local policy or the requested session release reason.
3) if the S-CSCF serves the calling user, treat the first BYE request as if received directly from the calling user, i.e. send it to internal service control and based on the outcome further on towards the called user;
4) if the S-CSCF serves the calling user, send the second BYE request directly to the calling user.
5) if the S-CSCF serves the called user, send the first BYE request directly to the called user;

6) if the S-CSCF serves the called user, treat the second BYE request as if received directly from the called user, i.e. shall send it to internal service control and based on the outcome further on towards to the called user.

Upon receipt of the 2xx responses for both BYE requests, the S-CSCF shall release all information related to the dialog and the related multimedia session.

5.4.5.1.3 Abnormal cases

Upon receipt of a request on a dialog for which the S-CSCF initiated session release, the S-CSCF shall terminate the received request and answer it with a 481 (Call/Transaction Does Not Exist) response.

5.4.5.2 Session release initiated by any other entity

Upon receipt of a 2xx response for a BYE request matching an existing dialog, the S-CSCF shall delete all the stored information related to the dialog.

5.4.6 Call-related requests

5.4.6.1 ReINVITE

5.4.6.1.1 Determination of served user

Void.

5.4.6.1.2 Mobile-originating case

For a reINVITE request from the UE, when the S-CSCF receives the UPDATE request, the S-CSCF shall store the updated gprs-charging-info parameter from P-Charging-Vector header. The gprs-charging-info parameter shall be retained in the P-Charging-Vector header when the request is forwarded to an AS. However, the gprs-charging-info parameter shall not be included in the P-Charging-Vector header when the UPDATE request is forwarded outside the home network of the S-CSCF.

5.4.6.1.3 Mobile-terminating case

For a reINVITE request destined towards the UE, when the S-CSCF receives the 200 (OK) response (to the INVITE), the S-CSCF shall store the updated gprs-charging-info parameter from the P-Charging-Vector header. The gprs-charging-info parameter shall be retained in the P-Charging-Vector header when the response is forwarded to the AS. However, the gprs-charging-info parameter shall not be included in the P-Charging-Vector header when the 200 (OK) response is forwarded outside the home network of the S-CSCF.

5.5 Procedures at the MGCF

5.5.1 General

The MGCF, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem. Therefore the dependencies of table A.3/1 and table A.3/2 shall not apply.

The use of the Path and P-Service-Route headers shall not be supported by the MGCF.

When the MGCF sends any request or response related to a dialog or standalone transaction, the MGCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before sending the message.

5.5.2 Subscription and notification

Void.

5.5.3 Call initiation

5.5.3.1 Initial INVITE

5.5.3.1.1 Calls originated from circuit-switched networks

When the MGCF receives an indication of an incoming call from a circuit-switched network, the MGCF shall:

- generate and send an INVITE request to I-CSCF:
  - set the Request-URI to the "tel" format using an E.164 address;
  - set the Supported header to "100rel" (see RFC 3312 [30]);
  - include an P-Asserted-Identity header;
  - create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header; and
  - insert an ioi-originating parameter into the P-Charging-Vector header. The ioi-originating parameter shall be set to a value that identifies the sending circuit-switched network and the ioi-terminating parameter shall not be included.

5.5.3.1.2 Calls terminating in circuit-switched networks

When the MGCF receives an initial INVITE request with Supported header indicating "100rel", the MGCF shall:

- send 100 (Trying) response;
- after a matching codec is found at the MGW, send 183 "Session Progress" response:
  - set the Require header to the value of "100rel";
  - set the Content-Disposition header to the value of "precondition";
  - include an P-Asserted-Identity header; and
  - store the values received in the P-Charging-Function-Addresses header; and
  - store the value of the icid parameter received in the P-Charging-Vector header.

When the MGCF does not find an available matching codec at the MGW for the received initial INVITE request, the MGCF shall:

- send 503 (Service Unavailable) response if the type of codec was acceptable but none were available; or
- send 488 (Not Acceptable Here) response if the type of codec was not supported, and may include SDP in the message body to indicate the codecs supported by the MGCF/MGW.

5.5.3.2 Subsequent requests

5.5.3.2.1 Calls originating in circuit-switched networks

When the MGCF receives 183 response to an INVITE request, the MGCF shall:

- store the values received in the P-Charging-Function-Addresses header.

When the MGCF receives 200 (OK) response to a PRACK request and notification that bearer setup is complete, the MGCF shall:

- send an UPDATE request.

5.5.3.2.2 Calls terminating in circuit-switched networks

When the MGCF receives an indication of a ringing for the called party of outgoing call to a circuit-switched network, the MGCF shall:

- send 180 Ringing to the UE.

When the MGCF receives an indication of answer for the called party of outgoing call to a circuit-switched network, the MGCF shall:

- send 200 OK to the UE, including an P-Asserted-Identity header.

5.5.4 Call release

5.5.4.1 Call release initiated by a circuit-switched network

When the MGCF receives an indication of call release from a circuit-switched network, the MGCF shall:

- send a BYE request to the UE.

5.5.4.2 S-CSCF-initiated call release

5.5.4.3 MGW-initiated call release

When the MGCF receives an indication from the MGW that the bearer was lost, the MGCF shall:

- send a BYE request towards the UE; and
- may include Error-Info header witha pointer to additional information indicating that bearer was lost.

5.5.5 Call-related requests

5.5.5.1 ReINVITE

5.5.5.1.1 Calls originating from circuit-switched networks

Void.

5.5.5.1.2 Calls terminating in circuit-switched networks

When the MGCF receives a reINVITE request for hold/resume operation, the MGCF shall:

- send 100 (Trying) response;
- after performing interaction with MGW to hold/resume the media flow, send 200 (OK) response.

5.5.6 Further initial requests

When the MGCF responds to an OPTIONS request with a 200 (OK) response, the MGCF may include a message body with an indication of the DTMF capabilities and supported codecs of the MGCF/MGW.

NOTE: The detailed interface for requesting MGCF/MGW capabilities is not specified in this version of the document. Other solutions may be used in the interim.

5.6 Procedures at the BGCF

5.6.1 General

The use of the Path and P-Service-Route headers shall not be supported by the BGCF.

When the BGCF receives any request or response related to a dialog or standalone transaction, the BGCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before forwarding the message.

5.6.2 Session initiation transaction

When the BGCF receives an INVITE request, the BGCF shall forward the request either to an MGCF within its own network, or to another network containing an MGCF. The BGCF need not Record-Route the INVITE request. While the next entity may be a MGCF acting as a UA, the BGCF shall not apply the procedures of RFC 3323 [33] relating to privacy. The BGCF shall store the values received in the P-Charging-Function-Addresses header. The BGCF shall store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header.

NOTE: The means by which the decision is made to forward to an MGCF or to another network is outside the scope of the present document, but may be by means of a lookup to an external database, or may be by data held internally to the BGCF.

5.7 Procedures at the Application Server (AS)

NOTE: This subclause defines only the requirements on the application server that relate to SIP. Other requirements are defined in 3GPP TS 23.218 [5].

5.7.1 Common Application Server (AS) Procedures

5.7.1.1 Notification about registration status

The AS may support the REGISTER method in order to discover the registration status of the user. If a REGISTER request arrives containing information about the user's registration status and the AS supports the REGISTER method, the AS shall store the Expires parameter from the request and generate a 200 (OK) response or an appropriate failure response. For the success case, the 200 (OK) response shall contain Expires value equal to the value received in the REGISTER request. The AS shall store the values received in P-Charging-Function-Addresses header.Also, the AS shall store the values of the icid parameter in the P-Charging-Vector header from the REGISTER request.

5.7.1.2 Extracting charging correlation information

When an AS receives an initial request for a dialog or a request for a standalone transaction, the AS shall store the values received in the P-Charging-Vector header, e.g. icid parameter, and retain the P-Charging-Vector header in the message. The AS shall store the values received in the P-Charging-Function-Addresses header and retain the P-Charging-Function-Addresses header in the message.

When an AS sends any request or response related to a dialog or standalone transaction, the AS may insert previously saved values into the P-Charging-Vector and P-Charging-Function-Addresses headers before sending the message.

5.7.2 Application Server (AS) acting as terminating UA, or redirect server

When acting as a terminating UA the AS shall behave as defined for a UE in subclause 5.1.4, with the exceptions noted in this subclause.

The AS, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem.

The S-CSCF may forward received initial requests to the application server based on initial filter criteria being met. If the S-CSCF includes P-Original-Dialog-ID header in these requests, the AS shall include the same P-Original-Dialog-ID header in any responses and/or subsequent requests sent on this dialog.

An Application Server acting as redirect server shall propagate any received 3GPP message body in the redirected message.

5.7.3 Application Server (AS) acting as originating UA

When acting as an originating UA the AS shall behave as defined for a UE in subclause 5.1.3, with the exceptions noted in this subclause.

The AS, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem.

When an AS acting as an originating UA generates an initial request for a dialog or a request for a standalone transaction, the AS shall create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header.

Furthermore the AS shall insert a Route header pointing to the S-CSCF.

5.7.4 Application Server (AS) acting as a SIP proxy

The S-CSCF may forward received initial requests to the application server based on initial filter criteria being met. If the S-CSCF includes P-Original-Dialog-ID header in these requests, the AS shall include the same P-Original-Dialog-ID header in any responses and/or subsequent requests sent on this dialog.

When the AS acting as a SIP proxy receives a request from the S-CSCF, prior to forwarding the request it shall:

- remove its own URL from the topmost Route header; and
- after executing the required services, route the request based on the topmost Route header.

The AS may modify the SIP requests based on service logic, prior to forwarding the request back to the S-CSCF.

An Application Server acting as a SIP proxy shall propagate any received 3GPP message body in the forwarded message.

5.7.5 Application Server (AS) performing 3rd party call control

5.7.5.1 General

The AS performing 3rd party call control acts as a B2BUA. There are two kinds of 3rd party call control:

- Routeing B2BUA: an AS receives a request from S-CSCF, terminates it and generates a new request, which is based on the received request.
- Initiating B2BUA: an AS initiates two requests, which are logically connected together at the AS.

The B2BUA AS will internally map the message headers between the two dialogs that it manages. It is responsible for correlating the dialog identifiers and will decide when to simply translate a message from one dialog to the other, or when to perform other functions. These decisions are specific to each AS and are outside the scope of the present document.

The AS, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem.

5.7.5.2 Call initiation

5.7.5.2.1 Initial INVITE

When the AS acting as a Routeing B2BUA receives an initial INVITE request from the S-CSCF, the AS shall:

- remove its own SIP URL from the topmost Route header of the received INVITE request;
- perform the Application Server specific functions. See 3GPP TS 23.218 [5];
- if successful, generate and send a new INVITE request to the S-CSCF to establish a new dialog. The AS shall look for the presence of the P-Original-Dialog-ID header in the initial INVITE request and populate the same P-Original-Dialog-ID header in the new INVITE request;
- copy the remaining Route header(s) unchanged from the received INVITE request to the new INVITE request;
- route the new INVITE request based on the topmost Route header.

NOTE: The topmost Route header of the received INVITE request will contain the AS's SIP URI. The following Route header will contain the SIP URI of the S-CSCF.

When the AS acting as an Initiating B2BUA the AS shall apply the procedures described in subclause 5.7.3 for both requests. The AS shall either set the <icid> XML element to be the same as received or different.

5.7.5.2.2 Subsequent requests

Void.

5.7.5.3 Call release

5.7.5.4 Call-related requests

An Application Server may initiate a call release. See 3GPP TS 23.218 [5] for possible reasons. The BYE request shall be sent simultaneously for both dialogs managed by the B2BUA.

5.7.5.5 Further initial requests

Void.

5.8 Procedures at the MRFC

5.8.1 General

Although the MRFC is acting as a UA, it is outside the scope of this specification how the MRFC associated addresses are made known to other entities.

When the MRFC sends any request or response related to a dialog or standalone transaction, the MRFC may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before sending the message.

5.8.2 Call initiation

5.8.2.1 Initial INVITE

5.8.2.1.1 MRFC-terminating case

5.8.2.1.1.1 Introduction

The MRFC shall provide a P-Asserted-Identity header in a response to the initial request for a dialog, or any response for a standalone transaction. It is a matter of network policy whether the MRFC expresses privacy according to RFC 3323 [33] with such responses.

When the MRFC receives an initial INVITE request, the MRFC shall store the values received in the P-Charging-Vector header, e.g. icid parameter. The MRFC shall store the values received in the P-Charging-Function-Addresses header.

5.8.2.1.1.2 Tones and announcements

The MRFC can receive INVITE requests to set up a session to play tones and announcements. The MRFC acts as terminating UA in this case.

When the MRFC receives an INVITE request with an indicator for a tone or announcement, the MRFC shall:

- send 100 (Trying) response.

NOTE: The detailed interfaces for requesting tones and announcements are not specified in this version of the document. Other solutions may be used in the interim.

5.8.2.1.1.3 Ad-hoc conferences

The MRFC can receive INVITE requests to set up an ad-hoc conferencing session (e.g. Multiparty Call) or to add parties from the conference. The MRFC acts as terminating UA in this case.

When the MRFC receives an INVITE request with an indicator to initiate ad hoc conferencing, the MRFC shall:

- send 100 (Trying) response; and
- after the MRFP indicates that the conference resources are available, send 200 (OK) response with an MRFC conference identifier.If the MRFC chooses to send a 183 (Session Progress) response prior to the 200 (OK), then the conference identifier may also be included in the 183 (Session Progress) response.

When the MRFC receives an INVITE request with an indicator to add a party to an existing ad hoc conference (i.e. MRFC conference identifier), the MRFC shall:

- send 100 Trying response; and
- after the MRFP indicates that the conferencing request is granted, send 200 OK response with the MRFC conference identifier.If the MRFC chooses to send a 183 Session Progress response prior to the 200 OK, then the conference identifier may also be included in the 183 Session Progress response.

NOTE: The detailed interface for requesting ad-hoc conferencing sessions is not specified in this version of the document. Other solutions may be used in the interim.

5.8.2.1.1.4 Transcoding

The MRFC may receive INVITE requests to set up transcoding between endpoints with incompatible codecs. The MRFC acts as terminating UA in this case.

When the MRFC receives an INVITE request with an indicator for transcoding and a codec is supplied in SDP, the MRFC shall:

- send 100 (Trying) response; and
- after the MRFP indicates that the transcoding request is granted, send 200 (OK) response.

When the MRFC receives an INVITE request with an indicator for transcoding but no SDP, the MRFC shall:

- send 183 (Session Progress) response with list of codecs supported by the MRFC/MRFP.

5.8.2.1.2 MRFC-originating case

The MRFC shall provide a P-Asserted-Identity header in an initial request for a dialog, or any request for a standalone transaction. It is a matter of network policy whether the MRFC expresses privacy according to RFC 3323 [33] with such requests.

5.8.2.2 Subsequent requests

5.8.2.2.1 Tones and announcements

When the MRFC receives an ACK request for a session, this may be considered as an event to direct the MRFP to start the playing of a tone or announcement.

5.8.3 Call release

5.8.3.1 S-CSCF-initiated call release

5.8.3.1.1 Tones and announcements

When the MRFC receives a BYE request for a session, the MRFC directs the MRFP to stop the playing of a tone or announcement.

5.8.3.2 MRFC-initiated call release

5.8.3.2.1 Tones and announcements

When the MRFC has a timed session to play tones and announcements and the time expires, the MRFC shall:

- send a BYE request towards the UE.

When the MRFC is informed by the MRFP that tone or announcement resource has been released, the MRFC shall:

- send a BYE request towards the UE.

5.8.2.2.2 Transcoding

When the MRFC receives a PRACK request (in response to the 183 (Session Progress) response) with an indicator for transcoding and codec supplied in SDP, the MRFC shall:

- after the MRFP indicates that the transcoding request is granted, send 200 (OK) response.

5.8.4 Call-related requests

5.8.4.1 ReINVITE

5.8.4.1.1 MRFC-terminating case

5.8.4.1.1.1 Ad-hoc conferences

The MRFC can receive reINVITE requests to modify an ad-hoc conferencing session (e.g. Multiparty Call) for purposes of floor control and for parties to leave and rejoin the conference.

When the MRFC receives a reINVITE request, the MRFC shall:

- send 100 (Trying) response; and
- after the MRFP indicates that the conferencing request is granted, send 200 (OK) response with the MRFC conference identifier.If the MRFC chooses to send a 183 (Session Progress) response prior to the 200 OK, then the conference identifier may also be included in the 183 (Session Progress) response.

NOTE: The detailed interface for requesting ad-hoc conferencing sessions is not specified in this version of the document. Other solutions may be used in the interim.

5.8.4.1.2 MRFC-originating case

Void.

5.8.4.2 REFER

5.8.4.2.1 MRFC-terminating case

Void.

5.8.4.2.2 MRFC-originating case

Void.

5.8.4.2.3 REFER initiating a new session

Void.

5.8.4.2.4 REFER replacing an existing session

Void.

5.8.4.3 INFO

Void.

5.8.5 Further initial requests

When the MRFC responds to an OPTIONS request with a 200 (OK) response, the MRFC may include a message body with an indication of the supported tones/announcement packages, DTMF capabilities, supported codecs and conferencing options of the MRFC/MRFP.

NOTE: The detailed interface for requesting MRFC/MRFP capabilities is not specified in this version of the document. Other solutions may be used in the interim.

6 Application usage of SDP

6.1 Procedures at the UE

Usage of SDP by the UE:

1. In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect and possibly modify the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.

2. An INVITE request generated by a UE shall contain SDP payload. The SDP payload shall reflect the calling user's terminal capabilities and user preferences for the session. In addition, the calling user shall indicate the desired QoS for the session, using the segmented status type. In an initial INVITE the UE shall indicate that it mandates local QoS and that this precondition is not yet satisfied, i.e. the UE shall include the following preconditions:

   a=des: qos mandatory local sendrecv

   a=curr: qos local none

3. The first 183 (Session Progress) provisional response sent out shall contain the answer for the SDP received in the INVITE. The SDP payload shall reflect the called user's terminal capabilities and user preferences.

4. When UE sends out an 183 (Session Progress) response with SDP payload, it shall request confirmation for the result of the resource reservation at the originating end point.

5. During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description.

6. For "video" and "audio" media types that utilize the RTP/RTCP, the UE shall specify the proposed bandwidth for each media stream utilizing the "b=" media descriptor in the SDP. For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in 3GPP TS 29.208 [13].

7. The UE shall include the DTMF media format at the end of the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 2833 [23].

6.2 Procedures at the P-CSCF

When the P-CSCF receives an INVITE request or reINVITE request, the P-CSCF shall examine the media parameters in the received SDP, and remove those which are not allowed on the network by local policy. The P-CSCF will also remove those codecs from the approved media streams which are not allowed by local policy. If the P-CSCF modifies the SDP, it shall also revise the SDP to reflect the modified bandwidth requirements. For the rejected media streams, the P-CSCF should ignore the b= lines.

6.3 Procedures at the S-CSCF

When the S-CSCF receives an INVITE request or reINVITE request, the S-CSCF shall examine the media parameters in the received SDP, and remove those media streams which are not allowed based on the subscription. The S-CSCF will also remove those codecs from the approved media streams which are not allowed by the subscription. If the S-CSCF modifies the SDP, it shall also revise the SDP to reflect the modified bandwidth requirements. For the rejected media streams, the S-CSCF should ignore the b= lines.

6.4 Procedures at the MGCF

The usage of SDP by the MGCF is the same as its usage by the UE, as defined in the subclause 6.1 and A.3.2. When sending an SDP, the MGCF shall not include the "i", "u", "e", "p", "r", and "z" descriptors in the SDP, and it shall ignore them when received in the SDP.

6.4.1 Calls originating from circuit-switched networks

When the MGCF generates and sends an INVITE request for a call originating in a circuit-switched network, the MGCF shall:

- populate the SDP with the codecs supported by the associated MGW (see 3GPP TS 26.235 [10] for the supported codecs).

When the MGCF receives 183 (Session Progress) response to an INVITE request, the MGCF shall:

- check that a supported codec has been indicated in the SDP.

6.4.2 Calls terminating in circuit-switched networks

When the MGCF receives an initial INVITE request, the MGCF shall:

- check for a codec that matches the requested SDP, which may include DTMF support.

When the MGCF generates and sends a 183 (Session Progress) response to an initial INVITE request, the MGCF shall:

- set SDP indicating the selected codec, which may include DTMF support.

6.5 Procedures at the MRFC

Void.

7 Extensions within the present document

7.1 SIP methods defined within the present document

There are no SIP methods defined within the present document over and above those defined in the referenced IETF specifications.

7.2 SIP headers defined within the present document

7.2.1 Void

7.2.2 P-Called-Party-ID header

7.2.2.1 Introduction

The P-Called-Party-ID header is the mechanism whereby the terminating UE learns the dialled public user identity that triggered the current session initiation.

The S-CSCF inserts the header in all terminating INVITE and reINVITE requests. The header is not used in any other request or response.

7.2.2.2 Syntax

The P-Called-Party-ID header field has the syntax described in table 7.1.

Table 7.1: Syntax of P-Called-Party-ID header

```
P-Called-Party-ID = "P-Called-Party-ID" HCOLON 1#
                    (name-addr *( SEMI p-cdpid-param))

p-cdpid-param = generic-param
```

Table 7.2 is an extension of tables 2 and 3 in RFC 3261 [26] and table in subclause 7.5 in RFC 3265 [28].

Table 7.2: P-Called-Party-ID header

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG	PRA	SUB	NOT
P-Called-Party-ID	R	am	-	-	-	o	-	-	-	-	-

7.2.2.3 Operation

The operation of this header is described in subclause 5.4.3.3.

7.2.3 P-Access-Network-Info header

7.2.3.1 Introduction

The P-Access-Network-Info header is the mechanism whereby the UE provides the S-CSCF with information relating to the access network it is using. This may include the cell ID.

The UE shall insert the P-Access-Network-Info header into all requests or responses it originates.

The S-CSCF shall remove the P-Access-Network-Info header from any message where it is present, before it forwards the message. The S-CSCS shall act accordingly upon the information received in the P-Access-Network-Info header.

7.2.3.2 Syntax

The syntax of the P-Access-Network-Info header is described in draft-mills-sip-access-network-info-02.txt [47].

7.2.3.3 Additional coding rules for P-Access-Network-Info header

In 3GPP systems, there are additional coding rules for the P-Access-Network-Info header:

If the *access type* field is equal to "3GPP-GERAN" the *access info* field shall contain a value for "3GPP-CGI". This value shall be the Cell Global Identity obtained from lower layers of the UE.

The Cell Global Identity is a concatenation of MCC, MNC, LAC and CI (as described in 3GPP TS23.003). The value of "3GPP-CGI" is therefore coded as a text string as follows:

Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and CI (fixed length code of 16 bits using a full hexadecimal representation).

If the *access type* field is equal to "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD" or "3GPP-CDMA2000" the *access info* field shall contain a value for "3GPP-UTRAN-CELL-ID". This value shall be made up of a concatenation of the MCC, MNC, LAC (as described in 3GPP TS 23.003) and the UMTS Cell Identity (as described in 3GPP TS 25.331), obtained from lower layers of the UE, and is coded as a text string as follows:

Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and UMTS Cell Identity (fixed length code of 28 bits).

7.2.4 P-Visited-Network-ID header

7.2.4.1 Introduction

The P-Visited-Network-ID header is used to allow the home network (e.g, the HSS) to discover, during the registration procedures, the network(s), other than the home network, that are utilised by the user. This allows the registration to be processed based on this, e.g. actions can be taken that are dependent on the roaming agreements between networks.

7.2.4.2 Syntax

The P-Visited-Network-ID header field has the syntax described in draft-garcia-sip-visited-network-id [44].

7.2.4.3 Operation

The header is inserted by the P-CSCF in every REGISTER request the UE sends. The I-CSCF sends the contents of the header to the HSS.

7.2.5 P-Charging-Function-Addresses header

7.2.5.1 Introduction

The P-Charging-Function-Addresses header is the mechanism whereby the S-CSCF may distribute a common set of addresses for charging functions to other network entities within the same network as the S-CSCF. The primary Charging Correlation Function (CCF) address is a required parameter for offline charging. The secondary CCF address is optional. Both the primary and secondary Event Charging Function (ECF) addresses for online charging are optional.

The S-CSCF inserts the header at the first opportunity when initialising dialogs and with standalone transactions. The header may be included in requests and responses.

7.2.5.2 Syntax

The P-Charging-Function-Addresses header field has the syntax described in draft-henrikson-sip-charging-information [45].

7.2.5.3 Operation

The operation of this header is described in subclauses 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 and 5.8.

7.2.6 P-Charging-Vector header

7.2.6.1 Introduction

The P-Charging-Vector header is the mechanism whereby the charging correlation information may be shared by IM CN subsystem functional entities. The charging correlation information consists of the following:

- IMS Charging Identifier (ICID), which is a globally unique identifier created per IMS dialog that is stored in all related CDRs.
- Inter Operator Identifier (IOI), which are globally unique identifiers for a particular network.
- Access Network Charging Information, where the GPRS is the initially supported access network. For GPRS there are the following components to track: GGSN address and one or more GPRS Charging Identifiers (GCID). Each GCID consists of an identifier of the PDP context assigned, the associated flow index into the SDP from the SIP signalling and the authorization token associated with the PDP context.

The first IM CN subsystem functional entity involved with a dialog or standalone transaction inserts the header with the icid parameter. Additional parameters are inserted into the P-Charging-Vector header by other entities as the processing continues. The header may be included in requests and responses.

7.2.6.2 Syntax

The P-Charging-Vector header field has the syntax described in table 7.3, which is extracted from draft-henrikson-sip-charging-information [45]. Table 7.3 describes extensions required for 3GPP.

Table 7.3: Syntax of extensions to P-Charging-Vector header

```
access-network-charging-info = (gprs-charging-info / gen-value)
gprs-charging-info = "gprs-charging-info" SEMI
                     "ggsn" EQUAL ggsn *(SEMI "gcid" EQUAL gcid)
                     [COMMA extension-param]
ggsn = gen-value
gcid = "pdp-id" EQUAL pdp-id COMMA "flow-index" EQUAL flow-index
       COMMA "auth-token" EQUAL auth-token
pdp-id = gen-value
flow-index = gen-value
auth-token = gen-value
extension-param = token [EQUAL (token | quoted-string)]
```

The gprs-charging-info parameter contains one ggsn child parameter and one or more child gcid parameters. Each gcid child parameter within gprs-charging-info corresponds to a PDP context that was established at the GGSN for a UE. Each gcid parameter contains pdp-id, flow-index and auth-token child parameters. The pdp-id parameter is the PDP context identifier that the P-CSCF obtained from the GGSN. The flow-index parameter is the relative index to the media stream in the SDP for the PDP context. The auth-token parameter is the authorization token associated with the PDP context. For more information about the PDP contexts for media, see subclause 9.2.5. For the case of a primary PDP context that is used for signalling, the flow-id and auth-token parameters are set to 0.

7.2.6.3 Operation

The operation of this header is described in subclauses 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 and 5.8.

7.2.7 P-Original-Dialog-ID header

7.2.7.1 Introduction

The P-Original-Dialog-ID header is the mechanism whereby the S-CSCF may associate dialogs related to the same initial request when traversing Application Servers specified in filter criteria.

The S-CSCF inserts the header in all INVITE and reINVITE requests. The header may also be used with standalone transactions and included in responses.

7.2.7.2 Syntax

The P-Original-Dialog-ID header field has the syntax described in draft-henrikson-sip-original-dialog-id [46].

7.2.7.3 Operation

The operation of this header is described in subclauses 5.4.3, 5.7.2, 5.7.4 and 5.7.5.

7.2.8 P-Service-Route header

The P-Service-Route header is defined in draft-willis-scvrtdisco [38].

7.2.9 P-Asserted-Identity header

7.2.9.1 Introduction

The P-Asserted-Identity header is the mechanism whereby the first element in the trust domain (see subclause 4.4) may assert a public user identity identifying the user. The P-Asserted-Identity header can also be used as a hint to the first element in the trust domain when it selects the asserted public user identity.

The header is inserted at the first opportunity when initialising dialogs and with standalone transactions. The header may be included in requests and responses.

7.2.9.2 Syntax

The P-Asserted-Identity header field has the syntax described in RFC 3325 [34].

7.2.9.3 Operation

The operation of this header is described in clause 5.

7.2A Extensions to SIP headers defined within the present document

7.2A.1 Extension to WWW-authenticate header

7.2A.1.1 Introduction

This extension defines a new authentication parameter (auth-param) for the WWW-Authenticate header used in a 401 (Unauthorized) response to the REGISTER request. For more information, see RFC 2617 [21] subclause 3.2.1.

7.2A.1.2 Syntax

The syntax for for auth-param is specified in table 7.4.

Table 7.4: Syntax of auth-param

```
auth-param      = 1#( integrity-key / cipher-key )
integrity-key   = "ik" EQUAL ik-value
cipher-key      = "ck" EQUAL ck-value
ik-value        = LDQUOT *(HEXDIG) RDQUOT
ck-value        = LDQUOT *(HEXDIG) RDQUOT
```

7.2A.1.3 Operation

This authentication parameter will be used in a 401 (Unauthorized) response in the WWW-authenticate header during UE authentication procedure as specified in subclause 5.4.1.

The S-CSCF appends the integrity-key parameter (directive) to the WWW.-Authenticate header in a 401 (Unauthorized) response. The P-CSCF stores the integrity-key value and removes the integrity-key parameter from the header prior to forwarding the response to the UE.

The S-CSCF appends the cipher-key parameter (directive) to the WWW-Authenticate header in a 401 (Unauthorized) response. The P-CSCF removes the cipher-key parameter from the header prior to forwarding the response to the UE. In the case ciphering is used, the P-CSCF stores the cipher-key value.

7.2A.2 integrity-protected parameter (directive)

7.2A.2.1 Introduction

The integrity-protected authentication parameter (auth-param) is an extension parameter defined for the Authorization header used in REGISTER requests. For more information, see RFC 2617 [21] subclause 3.2.2.

7.2A.2.2 Syntax

The syntax for for auth-param is specified in table 7.5.

Table 7.5: Syntax of auth-param

```
integrity-protected = “integrity-protected” EQUAL (“yes” / “no”)
```

7.2A.2.3 Operation

This authentication parameter is inserted by the P-CSCF in all the REGISTER requests received from the UE. The value of the parameter is set to “yes” in case the request was integrity protected, otherwise the value of it is set to “no”. This information is used by S-CSCF to decide whether to challenge the REGISTER request or not, as specified in subclause 5.4.1.

7.2A.3 Tokenized-by parameter definition

7.2A.3.1 Introduction

The tokenized-by parameter is an extension parameter appended to encrypted entries in various SIP headers as defined in subclause 5.3.3.1.

7.2A.3.2 Syntax

The syntax for the tokenized-by parameter is specified in table 7.6:

Table 7.6: Syntax of tokenized-by-param

```
uri-parameter =  transport-param / user-param / method-param
/ ttl-param / maddr-param / lr-param / tokenized-by-param / other-param
tokenized-by-param = “tokenized-by” EQUAL hostname
```

The BNF for uri-parameter is taken from IETF RFC 3261 [26] and modified accordingly.

7.2A.3.3 Operation

The tokenized-by parameter is appended by I-CSCF(THIG) after all encrypted strings within SIP headers when network configuration hiding is active. The value of the parameter is the domain name of the network which encrypts the information.

7.3 Option-tags defined within the present document

There are no option-tags defined within the present document over and above those defined in the referenced IETF specifications.

7.4 Status-codes defined within the present document

There are no status-codes defined within the present document over and above those defined in the referenced IETF specifications.

7.5 Session description types defined within the present document

There are no session description types defined within the present document over and above those defined in the referenced IETF specifications.

7.6 3GPP IM CN subsystem XML body, version 1

7.6.1 General

This subclause describes the Document Type Definition that is applicable for the 3GPP IM CN Subsystem XML body.

Any SIP User Agent or proxy may insert or remove the 3GPP IM CN subsystem XML body or parts of it, as required, in any SIP message. The 3GPP IM CN subsystem XML body shall not be forwarded outside a 3GPP network.

The associated MIME type with the 3GPP IMX XML body is "application/3gpp-ims+xml".

7.6.2 Document Type Definition

The Document Type Definition, according to XML syntax definitions, is defined in table 7.7.

Table 7.7: 3GPP IM CN subsystem XML body, version 1 DTD

```
<?xml version="1.0" ?>
<!-- Draft DTD for the 3GPP IMS XML body. -->

<!DOCTYPE ims-3gpp [
    <!-- ims-3gpp element: root element -->

    <!ELEMENT ims-3gpp (
        destination-public-user-id?,
        access?, service-info?)>
    <!ATTLIST ims-3gpp version CDATA #REQUIRED>

    <!-- public-user-id: public user ID -->
    <!ELEMENT destination-public-user-id    (#PCDATA)>

    <!-- service-info element: The transparent data received from HSS for AS -->
    <!ELEMENT service-info              (#CDATA)>

    <!-- alternative-service: alternative-service used in emergency sessions -->
    <!ELEMENT alternative-service   (type, reason)>
    <!ELEMENT type                  (emergency)>
    <!ELEMENT reason                (#PCDATA)>

]>
```

7.6.3 DTD description

This subclause describes the elements of the 3GPP IMS Document Type Definition as defined in table 7.7.

<ims-3gpp>: This is the root element of the 3GPP IMS XML body. It shall always be present. The version described in the present document is 1.

<destination-public-user-id>: The destination public-user-id URL of the current session.

<service-info>: the transparent element received from the HSS for a particular trigger point are placed within this optional element.

<alternative-service>: in the present document, the alternative service is used as a response for an attempt to establish an emergency session within the IM CN subsystem. The element describes an alternative service where the call should success. The alternative service is described by the type of service information. A possible reason cause why an alternative service is suggested may be included.

The <alternative-service> element contains a <type> element that indicates the type of alternative service. In the present document, the <type> element contains only the value "emergency".

The <reason> element contains an explanatory text with the reason why the session setup has been redirected. A UE may use this information to give an indication to the user.

7.7 SIP timers

The timers defined in RFC 3261 [26] need modification in some cases to accommodate the delays introduced by the air interface processing and transmission delays. Table 7.8 shows recommended values for 3GPP.

Table 7.8 lists in the first column, titled "SIP Timer" the timer names as defined in RFC 3261 [26].

The second column, titled "3GPP value to be applied between network elements" lists the values recommended for network elements e.g. P-CSCF, S-CSCF, MGCF, when communicating with each other i.e. when no air interface leg is included. These values are identical to those recommended by RFC 3261 [26].

The third column, titled "3GPP value to be applied at the UE" lists the values recommended for the UE. These are modified when compared to RFC 3261 [26] to accommodate the air interface delays.

The fourth column, titled "3GPP value to be applied at the P-CSCF toward a UE" lists the values recommended for the P-CSCF when an air interface leg is traversed. These are modified when compared to RFC 3261 [26].

The final column reflects the timer meaning as defined in RFC 3261 [26].

Table 7.8: SIP timers

SIP Timer	3GPP value to be applied between network elements	3GPP value to be applied at the UE	3GPP value to be applied at the P-CSCF toward a UE	Meaning
T1	500ms default	2s default	2s default	RTT estimate
T2	4s	16s	16s	The maximum retransmit interval for non-INVITE requests and INVITE responses
T4	5s	17s	17s	Maximum duration a message will remain in the network
Timer A	initially T1	initially T1	initially T1	INVITE request retransmit interval, for UDP only
Timer B	64*T1	64*T1	64*T1	INVITE transaction timeout timer
Timer C	> 3min	> 3 min	> 3 min	proxy INVITE transaction timeout
Timer D	> 32s for UDP	>128s	>128s	Wait time for response retransmits
	0s for TCP/SCTP	0s for TCP/SCTP	0s for TCP/SCTP	
Timer E	initially T1	initially T1	initially T1	non-INVITE request retransmit interval, UDP only
Timer F	64*T1	64*T1	64*T1	non-INVITE transaction timeout timer
Timer G	initially T1	initially T1	initially T1	INVITE response retransmit interval
Timer H	64*T1	64*T1	64*T1	Wait time for ACK receipt.
Timer I	T4 for UDP	T4 for UDP	T4 for UDP	Wait time for ACK retransmits
	0s for TCP/SCTP	0s for TCP/SCTP	0s for TCP/SCTP	
Timer J	64*T1 for UDP	64*T1 for UDP	64*T1 for UDP	Wait time for non-INVITE request retransmits
	0s for TCP/SCTP	0s for TCP/SCTP	0s for TCP/SCTP	
Timer K	T4 for UDP	T4 for UDP	T4 for UDP	Wait time for response retransmits
	0s for TCP/SCTP	0s for TCP/SCTP	0s for TCP/SCTP	

8 SIP compression

8.1 SIP compression procedures at the UE

8.1.1 SIP compression

The UE shall support SigComp as specified in RFC 3320 [32]. The compartment shall start when a SigComp message is received within a security association and shall finish when the UE is no longer registered. State creations and announcements shall be allowed only for messages received in a security association.

The UE shall support the SIP dictionary specified in draft-ietf-sipping-sigcomp-dictionary [42]. If compression is enabled, the UE shall use the dictionary to compress the first message.

8.1.2 Compression of SIP requests and responses transmitted to the P-CSCF

The UE should compress the requests and responses transmitted to the P-CSCF according to clause 8.1.1.

NOTE: Compression of SIP messages is an implementation option. However, compression is strongly recommended.

8.1.3 Decompression of SIP requests and responses received from the P-CSCF

The UE shall decompress the compressed requests and responses received from the P-CSCF according to clause 8.1.1.

8.2 SIP compression procedures at the P-CSCF

8.2.1 SIP compression

The P-CSCF shall support SigComp as specified in RFC 3320 [32]. The compartment shall start when a SigComp message is received within a security association and shall finish when the UE is no longer registered. State creations and announcements shall be allowed only for messages received in a security association.

The P-CSCF shall support the SIP dictionary specified in draft-ietf-sipping-sigcomp-dictionary [42]. If compression is enabled, the P-CSCF shall use the dictionary to compress the first message.

8.2.2 Compression of SIP requests and responses transmitted to the UE

The P-CSCF should compress the requests and responses transmitted to the UE according to clause 8.2.1.

NOTE: Compression of SIP messages is an implementation option. However, compression is strongly recommended.

8.2.3 Decompression of SIP requests and responses received from the UE

The P-CSCF shall decompress the compressed requests and responses received from the UE according to clause 8.2.1.

9 GPRS aspects when connected to the IM CN subsystem

9.1 Introduction

A UE accessing the IM CN subsystem, and the IM CN subsystem itself, utilise the services provided by GPRS to provide packet-mode communication between the UE and the IM CN subsystem.

Requirements for the UE on the use of these packet-mode services are specified in this clause. Requirements for the GGSN in support of this communication are specified in 3GPP TS 29.061 [11] and 3GPP TS 29.207 [12].

9.2 Procedures at the UE

9.2.1 PDP context activation and P-CSCF discovery

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a GPRS attach procedure;

b) establish a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4]. This PDP context shall remain active throughout the period the UE is connected to the IM

CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv6 address;

The UE shall choose one of the following options when performing establishment of this PDP context:

I. A dedicated PDP context for SIP signalling:

The UE shall indicate to the GGSN that this is a PDP context intended to carry IM CN subsystem-related signalling only by setting the IM CN Subsystem Signalling Flag within the Protocol Configuration Options IE at PDP Context activation. The UE may also use this PDP context for DNS and DHCP signalling according to the static packet filters described in 3GPP TS 29.207 [12];

II. A general-purpose PDP context:

The UE may decide to use a general purpose PDP Context to carry IM CN subsystem-related signaling. The UE shall indicate to the GGSN that this is a general-purpose PDP context by not setting the IM CN Subsystem Signalling Flag within the Protocol Configuration Options IE;

NOTE 1: A general purpose PDP Context is completely IM CN subsystem-unaware, and as such, it does not have any IM CN subsystem-specific mechanisms applied to it.

NOTE 2: A general purpose PDP Context may carry both IM CN subsystem signaling and media, in case the media does not need to be authorized by Service Based Local Policy mechanisms defined in 3GPP TS 29.207 [12] and the media component is not mandated by the P-CSCF to be carried in a separate PDP Context.

c) aquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

I. Employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) draft-ietf-dhc-dhcpv6 [40], the DHCPv6 options for SIP servers draft-ietf-sip-dhcpv6 [41] and if needed DNS after PDP context activation.

The UE shall either:

- in the DHCP query, request a list of SIP server domain names of P-CSCF(s) and the list of Domain Name Servers (DNS); or

- request a list of SIP server IPv6 addresses of P-CSCF(s).

II. Transfer P-CSCF address(es) within The PDP context activation procedure.

The UE shall indicate the request for a P-CSCF address to the GGSN within the Protocol Configuration Options IE of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message.

If the GGSN provides the UE with a list of P-CSCF IPv6 addresses in the ACTIVATE PDP CONTEXT ACCEPT message or ACTIVATE SECONDARY PDP CONTEXT ACCEPT message, the UE shall assume that the list is prioritised with the first address within the Protocol Configuration Options IE as the P-CSCF address with the highest priority.

The UE can freely select method I or II for P-CSCF discovery. In case several P-CSCF addresses are provided to the UE, the selection of P-CSCF address shall be performed according to the resolution of host name as indicated in RFC 3261 [26]. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

If the UE is designed to use I above, but receives P-CSCF address(es) according to II, then the UE shall either ignore the received address(es), or use the address(es) in accordance with II, and not proceed with the DHCP request according to I.

9.2.2 Session management procedures

The existing procedures for session management as described in 3GPP TS 24.008 [8] shall apply while the UE is connected to the IM CN subsystem.

9.2.3 Mobility management procedures

The existing procedures for mobility management as described in 3GPP TS 24.008 [8] shall apply while the UE is connected to the IM CN subsystem.

9.2.4 Cell selection and lack of coverage

The existing mechanisms and criteria for cell selection as described in 3GPP TS 25.304 [9] and 3GPP TS 44.018 [20] shall apply while the UE is connected to the IM CN subsystem.

9.2.5 PDP contexts for media

During establishment of a session, the UE establishes data streams(s) for media related to the session. Such data stream(s) may result in activation of additional PDP context(s). Such additional PDP context(s) shall be established as secondary PDP contexts associated to the PDP context used for signalling.

The P-CSCF shall indicate to the UE in SIP/SDP if a separate PDP Context is required for a media component as per procedures defined in 3GPP TS 23.228 [7]. The UE shall establish an additional PDP context for a media component if so indicated by the P-CSCF.

The UE shall pass the authorisation token received from the P-CSCF in the 183 (Session Progress) response to an INVITE request at originating setup or in the INVITE request at terminating setup to the GGSN by inserting it within the Traffic Flow Template IE at PDP Context activation/modification.

In order to identify to the GGSN which flow(s) (identified by m-lines within the SDP) are to be transferred within a particular PDP context, the UE shall set the flow identifier(s) within the Traffic Flow Template IE at PDP Context activation modification. Detailed description of how the flow identifiers are constructed is provided in 3GPP TS 29.207 [12].

Detailed description of how the authorization token and flow identifiers are carried in the Traffic Flow Template IE is provided in 3GPP TS 24.008 [8].

Annex A (normative): Profiles of IETF RFCs for 3GPP usage

A.1 Profiles

A.1.1 Relationship to other specifications

This annex contains a profile to the IETF specifications, and the PICS proformas underlying profiles do not add requirements to the specifications they are proformas for.

This annex provides a profile specification according to both the current IETF specifications for SIP, SDP and other protocols (as indicated by the "RFC status" column in the tables in this annex) and to the 3GPP specifications using SIP (as indicated by the "Profile status" column in the tables in this annex.

In the "RFC status" column the contents of the referenced specification takes precedence over the contents of the entry in the column. However, a number of the referenced specifications reference RFC 2543 rather than RFC 3261 [26], and therefore certain extensions (particularly new headers) have not been included in these referenced specifications. 3GPP apply the extensions of the bis draft to IETF specifications that reference RFC 2543, and where this consideration applies to the entry in the "RFC status" column, then the entry should apply and override the referenced IETF specification.

In the "Profile status" column, there are a number of differences from the "RFC status" column. Where these differences occur, these differences take precedence over any requirements of the IETF specifications. Where specification concerning these requirements exists in the main body of the present document, the main body of the present document takes precedence.

Where differences occur in the "Profile status" column, the "Profile status" normally gives more strength to a "RFC status" and is not be in contradiction with the "RFC status", e.g. it may change an optional "RFC status" to a mandatory "Profile status". If the "Profile status" weakens the strength of a "RFC status" then additionally this will be indicated by further textual description in the present document.

A.1.2 Introduction to methodology within this profile

This subclause does not reflect dynamic conformance requirements but static ones. In particular, an condition for support of a PDU parameter does not reflect requirements about the syntax of the PDU (i.e. the presence of a parameter) but the capability of the implementation to support the parameter.

In the sending direction, the support of a parameter means that the implementation is able to send this parameter (but it does not mean that the implementation always sends it).

In the receiving direction, it means that the implementation supports the whole semantic of the parameter.

As a consequence, PDU parameter tables in this subclause are not the same as the tables describing the syntax of a PDU in the reference specification, e.g. RFC 3261 [26] tables 2 and 3. It is not rare to see a parameter which is optional in the syntax but mandatory in subclause below.

The various statii used in this subclause are in accordance with the rules in table A.1.

Table A.1: Key to status codes

Status code	Status name	Meaning
m	mandatory	the capability shall be supported. It is a static view of the fact that the conformance requirements related to the capability in the reference specification are mandatory requirements. This does not mean that a given behaviour shall always be observed (this would be a dynamic view), but that it shall be observed when the implementation is placed in conditions where the conformance requirements from the reference specification compel it to do so. For instance, if the support for a parameter in a sent PDU is mandatory, it does not mean that it shall always be present, but that it shall be present according to the description of the behaviour in the reference specification (dynamic conformance requirement).
o	optional	the capability may or may not be supported. It is an implementation choice.
n/a	not applicable	it is impossible to use the capability. No answer in the support column is required.
x	prohibited (excluded)	It is not allowed to use the capability. This is more common for a profile.
c <integer>	conditional	the requirement on the capability ("m", "o", "n/a" or "x") depends on the support of other **optional or conditional** items. <integer> is the identifier of the conditional expression.
o.<integer>	qualified optional	for mutually exclusive or selectable options from a set. <integer> is the identifier of the group of options, and the logic of selection of the options.
i	irrelevant	capability outside the scope of the given specification. Normally, this notation should be used in a base specification ICS proforma only for transparent parameters in received PDUs. However, it may be useful in other cases, when the base specification is in fact based on another standard.

A.1.3 Roles

Table A.2: Roles

Item	Roles	Reference	RFC status	Profile status
1	User agent		o.1	o.1
2	Proxy		o.1	o.1
o.1:	It is mandatory to support exactly one of these items.			
NOTE:	For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role.			

Table A.3: Roles specific to this profile

Item	Roles	Reference	RFC status	Profile status
1	UE		n/a	o.1
2	P-CSCF		n/a	o.1
3	I-CSCF		n/a	o.1
4	S-CSCF		n/a	o.1
5	BGCF		n/a	o.1
6	MGCF		n/a	o.1
7	AS		n/a	o.1
8	MRFC		n/a	o.1
o.1:	It is mandatory to support exactly one of these items.			
NOTE:	For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role.			

A.2 Profile definition for the Session Initiation Protocol as used in the present document

A.2.1 User agent role

A.2.1.1 Introduction

This subclause contains the ICS proforma tables related to the user role. They need to be completed only for UA implementations:

Prerequisite: A.2/1 -- user agent role.

A.2.1.2 Major capabilities

Table A.4: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
	Capabilities within main protocol			
1	client behaviour for registration?	[26] subclause 10.2	m	c3
2	registrar?	[26] subclause 10.3	o	c4
3	client behaviour for session requests?	[26] subclause 13.2	m	o
4	server behaviour for session requests?	[26] subclause 13.3	m	o
5	session release?	[26] subclause 15.1	m	c1
6	timestamping of requests?	[26] subclause 8.2.6.1	o	o
7	authentication between UA and UA?	[26] subclause 22.2	o	o
8	authentication between UA and registrar?	[26] subclause 22.2	o	n/a
9	server handling of merged requests due to forking	[26] 8.2.2.2	m	m
10	client handling of multiple responses due to forking	[26] 13.2.2.4	m	m
11	insertion of date in requests and responses?	[26] subclause 20.17	o	o
12	downloading of alerting information?	[26] subclause 20.4	o	o
	Extensions			
13	The SIP INFO method?	[25]	o	n/a
14	Reliability of provisional responses in SIP?	[27]	o	m
15	the REFER method?	[36]	o	o
16	Integration of resource management and SIP?	[30]	o	m
17	the SIP UPDATE method	[29]	c5	m
18	SIP extensions for caller identity and privacy?	[34]	o	m
19	SIP extensions for media authorization?	[31]	o	m
20	SIP specific event notification	[28]	o	o
21	the use of NOTIFY to establish a dialog	[28] 4.2	o	n/a
22	acting as the notifier of event information	[28]	c2	c2
23	acting as the recipient of event information	[28]	c2	c2
24	Path Extension Header for Establishing Service Route with SIP REGISTER	[35]	o	c6
25	extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks	[34]	o	m
26	a Privacy Mechanism for the Session Initiation Protocol (SIP)	[33]	o	m

c1: IF A.4/3 OR A.4/4 THEN m ELSE o.
c2: IF A.4/20 THEN o.1 ELSE n/a.
c3: IF A.3/1 OR A.3/4 THEN m ELSE n/a - - UA or S-CSCF functional entity.
c4: IF A.3/4 OR A.3/7 THEN m ELSE n/a - - S-CSCF or AS functional entity.
c5: IF A.4/16 THEN m ELSE o - - integration of resource management and SIP.
c6: IF (A.150/3 AND A.150/4) THEN m ELSE n/a. - - S-CSCF acting as registrar.
o.1: At least one of these capabilities is supported.

A.2.1.3 PDUs

Table A.5: Supported methods

Item	PDU	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	ACK request	[26] 13	m	m	[26] 13	m	m
2	BYE request	[26] 15.1	o		[26] 15.1	o	
3	BYE response	[26] 15.1	o		[26] 15.1	o	
4	CANCEL request	[26] 9	o		[26] 9	o	
5	CANCEL response	[26] 9	o		[26] 9	o	
6	INFO request	[25] 2	c2	n/a	[25] 2	c2	n/a
7	INFO response	[25] 2	c2	n/a	[25] 2	c2	n/a
8	INVITE request	[26] 13	m	m	[26] 13	m	m
9	INVITE response	[26] 13	m	m	[26] 13	m	m
10	NOTIFY request	[28] 8.1.2	c4	c4	[28] 8.1.2	c3	c3
11	NOTIFY response	[28] 8.1.2	c3	c3	[28] 8.1.2	c4	c4
12	OPTIONS request	[26] 11	m	m	[26] 11	m	m
13	OPTIONS response	[26] 11	m	m	[26] 11	m	m
14	PRACK request	[27] 6	c5	c5	[27] 6	c5	c5
15	PRACK response	[27] 6	c5	c5	[27] 6	c5	c5
16	REFER request	[36] 3	c1	c1	[36] 3	c1	c1
17	REFER response	[36] 3	c1	c1	[36] 3	c1	c1
18	REGISTER request	[26] 10	o		[26] 10	n/a	
19	REGISTER response	[26] 10	n/a		[26] 10	m	
20	SUBSCRIBE request	[28] 8.1.1	c3	c3	[28] 8.1.1	c4	c4
21	SUBSCRIBE response	[28] 8.1.1	c4	c4	[28] 8.1.1	c3	c3
22	UPDATE request	[30] 6.1	c6	c6	[30] 6.2	c6	c6
23	UPDATE response	[30] 6.2	c6	c6	[30] 6.1	c6	c6
c1:	IF A.4/15 THEN m ELSE n/a.						
c2:	IF A.4/13 THEN m ELSE n/a.						
c3:	IF A.4/23 THEN m ELSE n/a.						
c4:	IF A.4/22 THEN m ELSE n/a.						
c5:	IF A.4/14 THEN m ELSE n/a - - reliability of provisional responses.						
c6:	IF A.4/17 THEN m ELSE n/a - - the SIP update method.						

Editor's note: Optional status of BYE in RFC status is given because RFC states SHOULD (client and server).

Editor's note: Optional status of REGISTER in RFC status is given because RFC states RECOMMENDED (client); for the UAS, not statement is made, but it is assumed that this therefore means n/a.

A.2.1.4 PDU parameters

A.2.1.4.1 Status-codes

Table A.6: Supported status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	100 (Trying)	[26] 21.1.1	n/a	n/a	[26] 21.1.1	m	m
2	180 (Ringing)	[26] 21.1.2	c2	c2	[26] 21.1.2	c1	c1
3	181 (Call Is Being Forwarded)	[26] 21.1.3	c2	c2	[26] 21.1.3	c1	c1
4	182 (Queued)	[26] 21.1.4	c2	c2	[26] 21.1.4	c1	c1
5	183 (Session Progress)	[26] 21.1.5	c1	c1	[26] 21.1.5	c1	c1
6	200 (OK)	[26] 21.2.1			[26] 21.2.1		
7	202 (Accepted)	[28] 8.3.1	c3	c3	[28] 8.3.1	c3	c3
8	300 (Multiple Choices)	[26] 21.3.1			[26] 21.3.1		
9	301 (Moved Permanently)	[26] 21.3.2			[26] 21.3.2		
10	302 (Moved Temporarily)	[26] 21.3.3			[26] 21.3.3		
11	305 (Use Proxy)	[26] 21.3.4			[26] 21.3.4		
12	380 (Alternative Service)	[26] 21.3.5			[26] 21.3.5		
13	400 (Bad Request)	[26] 21.4.1			[26] 21.4.1		
14	401 (Unauthorized)	[26] 21.4.2			[26] 21.4.2		
15	402 (Payment Required)	[26] 21.4.3			[26] 21.4.3		
16	403 (Forbidden)	[26] 21.4.4			[26] 21.4.4		
17	404 (Not Found)	[26] 21.4.5			[26] 21.4.5		
18	405 (Method Not Allowed)	[26] 21.4.6			[26] 21.4.6		
19	406 (Not Acceptable)	[26] 21.4.7			[26] 21.4.7		
20	407 (Proxy Authentication Required)	[26] 21.4.8			[26] 21.4.8		
21	408 (Request Timeout)	[26] 21.4.9			[26] 21.4.9		
22	410 (Gone)	[26] 21.4.10			[26] 21.4.10		
23	413 (Request Entity Too Large)	[26] 21.4.11			[26] 21.4.11		
24	414 (Request-URI Too Large)	[26] 21.4.12			[26] 21.4.12		
25	415 (Unsupported Media Type)	[26] 21.4.13			[26] 21.4.13		
26	416 (Unsupported URI Scheme)	[26] 21.4.14			[26] 21.4.14		
27	420 (Bad Extension)	[26] 21.4.15			[26] 21.4.15		
28	421 (Extension Required)	[26] 21.4.16			[26] 21.4.16		
29	423 (Registration Too Brief)	[26] 21.4.17	c4	c4	[26] 21.4.17	m	m
30	480 (Temporarily Unavailable)	[26] 21.4.18			[26] 21.4.18		
31	481 (Call Leg/Transaction Does Not Exist)	[26] 21.4.19			[26] 21.4.19		
32	482 (Loop Detected)	[26] 21.4.20			[26] 21.4.20		
33	483 (Too Many Hops)	[26] 21.4.21			[26] 21.4.21		
34	484 (Address Incomplete)	[26] 21.4.22			[26] 21.4.22		
35	485 (Ambiguous)	[26] 21.4.23			[26] 21.4.23		
36	486 (Busy Here)	[26] 21.4.24			[26] 21.4.24		
37	487 (Request Cancelled)	[26] 21.4.25			[26] 21.4.25		
38	488 (Not Acceptable Here)	[26] 21.4.26			[26] 21.4.26		
39	489 (Bad Events)	[28] 8.3.2	c3	c3	[28] 8.3.2	c3	c3
40	491 (Request Pending)	[26] 21.4.27			[26] 21.4.27		
41	493 (Undecipherable)	[26] 21.4.28			[26] 21.4.28		
42	500 (Internal Server Error)	[26] 21.5.1			[26] 21.5.1		
43	501 (Not Implemented)	[26] 21.5.2			[26] 21.5.2		
44	502 (Bad Gateway)	[26] 21.5.3			[26] 21.5.3		
45	503 (Service Unavailable)	[26] 21.5.4			[26] 21.5.4		
46	504 (Server Time-out)	[26] 21.5.5			[26] 21.5.5		
47	505 (SIP Version not	[26] 21.5.6			[26] 21.5.6		

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
	supported)						
48	513 (Message Too Large)	[26] 21.5.7			[26] 21.5.7		
49	580 (Precondition Failure)						
50	600 (Busy Everywhere)	[26] 21.6.1			[26] 21.6.1		
51	603 (Decline)	[26] 21.6.2			[26] 21.6.2		
52	604 (Does Not Exist Anywhere)	[26] 21.6.3			[26] 21.6.3		
53	606 (Not Acceptable)	[26] 21.6.4			[26] 21.6.4		
c1: IF A.5/9 THEN m ELSE n/a. c2: IF A.5/9 THEN o ELSE n/a. c3: IF A.4/20 THEN m ELSE n/a. c4: IF A.5/19 OR A.5/21 THEN m ELSE n/a - - REGISTER response or SUBSCRIBE response.							

A.2.1.4.2 ACK method

Prerequisite A.5/1 – ACK request

Table A.7: Supported headers within the ACK request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	o		[26] 20.5	o	
2	Allow-Events	[28] 8.2.2	c1	c1	[28] 8.2.2	c2	c2
3	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
4	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
5	Contact	[26] 20.10	o		[26] 20.10	o	
6	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
7	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
8	Content-Language	[26] 20.13	o		[26] 20.13	o	
9	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
10	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
11	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
12	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
13	From	[26] 20.20	m	m	[26] 20.20	m	m
14	Max-Forwards	[26] 20.22	o	o	[26] 20.22	n/a	n/a
15	MIME-Version	[26] 20.24	o		[26] 20.24	o	
16	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
17	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
18	Require	[26] 20.32	o	o	[26] 20.32	m	m
19	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
20	Timestamp	[26] 20.38	c7	c7	[26] 20.38	m	m
21	To	[26] 20.39	m	m	[26] 20.39	m	m
22	User-Agent	[26] 20.41	o		[26] 20.41	o	
23	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1: IF A.4/20 THEN o ELSE n/a. c2: IF A.4/20 THEN m ELSE n/a. c3: IF A.4/7 THEN m ELSE n/a. c4: IF A.4/11 THEN o ELSE n/a. c7: IF A.4/6 THEN o ELSE n/a.							

Editor's note: Is the following table a suitable way of showing the contents of message bodies.

Prerequisite A.5/1 – ACK request

Table A.8: Supported message bodies within the ACK request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.1.4.3 BYE method

Prerequisite A.5/2 – BYE request

Table A.9: Supported headers within the BYE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow-Events	[28] 8.2.2	c1	c1	[28] 8.2.2	c2	c2
5	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
8	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
9	Content-Language	[26] 20.13	o		[26] 20.13	o	
10	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
11	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
12	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
13	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
14	From	[26] 20.20	m	m	[26] 20.20	m	m
15	Max-Forwards	[26] 20.22	o	o	[26] 20.22	n/a	n/a
16	MIME-Version	[26] 20.24	o		[26] 20.24	o	
17	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
18	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
19	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a
20	Require	[26] 20.32	o	o	[26] 20.32	m	m
21	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
22	Supported	[26] 20.37	o	o	[26] 20.37	m	m
23	Timestamp	[26] 20.38	c8	c8	[26] 20.38	m	m
24	To	[26] 20.39	m	m	[26] 20.39	m	m
25	User-Agent	[26] 20.41	o		[26] 20.41	o	
26	Via	[26] 20.42	m	m	[20] 20.42	m	m
c1:	IF A.4/20 THEN o ELSE n/a.						
c2:	IF A.4/20 THEN m ELSE n/a.						
c3:	IF A.4/7 THEN m ELSE n/a.						
c4:	IF A.4/11 THEN o ELSE n/a.						
c8:	IF A.4/6 THEN o ELSE n/a.						

Prerequisite A.5/2 – BYE request

Table A.10: Supported message bodies within the BYE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.5/3 – BYE response

Prerequisite: A.6/1 – 100 Trying

Table A.11: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	n/a	n/a	[26] 20.8	m	m
2	Content-Length	[26] 20.14	n/a	n/a	[26] 20.14	m	m
3	Cseq	[26] 20.16	n/a	n/a	[26] 20.16	m	m
4	Date	[26] 20.17	n/a	n/a	[26] 20.17	m	m
5	From	[26] 20.20	n/a	n/a	[26] 20.20	m	m
6	To	[26] 20.39	n/a	n/a	[26] 20.39	m	m
7	Via	[26] 20.42	n/a	n/a	[26] 20.42	m	m

Prerequisite A.5/3 – BYE response

Table A.12: Supported headers within the BYE response - all remaining status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
3	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
4	Content-Language	[26] 20.13	o		[26] 20.13	o	
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o		[26] 20.24	o	
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
12	To	[26] 20.39	m	m	[26] 20.39	m	m
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/11 THEN o ELSE n/a.						
c2:	IF A.4/6 THEN m ELSE n/a.						

Prerequisite A.5/3 – BYE response

Prerequisite: A.6/6 – 2xx

Table A.13: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Authentication-Info	[26] 20.6	o		[26] 20.6	o	
2	Require	[26] 20.32	m	m	[26] 20.32	m	m
3	Server	[26] 20.35	o	o	[26] 20.35	o	o
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	User-Agent	[26] 20.41	o		[26] 20.41	o	
6	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/35 - - 3xx or 485 "Ambiguous"

Table A.14: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Require	[26] 20.32	m	m	[26] 20.32	m	m
3	Server	[26] 20.35	o	o	[26] 20.35	o	o
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	User-Agent	[26] 20.41	o		[26] 20.41	o	
6	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/3 – BYE response

Prerequisite: A.6/13 – 401

Table A.15: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
8	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	

Prerequisite A.5/3 – BYE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.16: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Require	[26] 20.32	m	m	[26] 20.32	m	m
3	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/3 – BYE response

Prerequisite: A.6/18 -- "405" Method Not Allowed

Table A.17: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m		[26] 20.5	m	
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/3 – BYE response

Prerequisite: A.6/19 – 407

Table A.18: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/3 – BYE response

Prerequisite A.6/25 -- "415" Unsupported Media Type

Table A.19: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/3 – BYE response

Prerequisite: A.6/27 – 420

Table A.20: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Require	[26] 20.32	m	m	[26] 20.32	m	m
3	Server	[26] 20.35	o	o	[26] 20.35	o	o
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/3 – BYE response

Prerequisite: A.6/34 – 484

Table A.21: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Require	[26] 20.32	m	m	[26] 20.32	m	m
3	Server	[26] 20.35	o	o	[26] 20.35	o	o
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	User-Agent	[26] 20.41	o		[26] 20.41	o	
6	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/3 – BYE response

Table A.22: Supported message bodies within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.1.4.4 CANCEL method

Prerequisite A.5/4 – CANCEL request

Table A.23: Supported headers within the CANCEL request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow-Events	[28] 8.2.2	c1	c1	[28] 8.2.2	c2	c2
5	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Content-Language	[26] 20.13	o		[26] 20.13	o	
8	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
9	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
10	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
11	From	[26] 20.20	m	m	[26] 20.20	m	m
12	Max-Forwards	[26] 20.22	o	o	[26] 20.22	n/a	n/a
13	MIME-Version	[26] 20.24	o		[26] 20.24	o	
14	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
15	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
16	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a
17	Require	[26] 20.32	o	o	[26] 20.32	m	m
18	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
19	Supported	[26] 20.37	o	o	[26] 20.37	m	m
20	Timestamp	[26] 20.38	c8	c8	[26] 20.38	m	m
21	To	[26] 20.39	m	m	[26] 20.39	m	m
22	User-Agent	[26] 20.41	o		[26] 20.41	o	
23	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/20 THEN o ELSE n/a.						
c2:	IF A.4/20 THEN m ELSE n/a.						
c3:	IF A.4/7 THEN m ELSE n/a.						
c4:	IF A.4/11 THEN o ELSE n/a.						
c8:	IF A.4/6 THEN o ELSE n/a.						

Prerequisite A.5/4 – CANCEL request

Table A.24: Supported message bodies within the CANCEL request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.5/5 – CANCEL response

Table A.25: Supported headers within the CANCEL response - all status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
5	From	[26] 20.20	m	m	[26] 20.20	m	m
6	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
7	To	[26] 20.39	m	m	[26] 20.39	m	m
8	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1: IF A.4/11 THEN o ELSE n/a. c2: IF A.4/6 THEN m ELSE n/a.							

Prerequisite A.5/5 – CANCEL response

Prerequisite: A.6/6 – 200

Table A.26: Supported headers within the CANCEL response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Content-Language	[26] 20.13	o		[26] 20.13	o	
2	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	User-Agent	[26] 20.41	o		[26] 20.41	o	
6	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/5 – CANCEL response

Prerequisite: A.6/13 – 401

Table A.27: Supported headers within the CANCEL response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Content-Language	[26] 20.13	o		[26] 20.13	o	
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
4	Require	[26] 20.32	m	m	[26] 20.32	m	m
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
8	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	

Prerequisite A.5/5 – CANCEL response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 – 404, 413, 480, 500, 503, 600, 603

Table A.28: Supported headers within the CANCEL response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Content-Language	[26] 20.13	o		[26] 20.13	o	
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	User-Agent	[26] 20.41	o		[26] 20.41	o	
6	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/5 – CANCEL response

Prerequisite: A.6/27 – 420

Table A.29: Supported headers within the CANCEL response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Content-Language	[26] 20.13	o		[26] 20.13	o	
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/5 – CANCEL response

Prerequisite: A.6/34 – 484

Table A.30: Supported headers within the CANCEL response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Content-Language	[26] 20.13	o		[26] 20.13	o	
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	User-Agent	[26] 20.41	o		[26] 20.41	o	
6	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/5 – CANCEL response

Table A.31: Supported message bodies within the CANCEL response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.1.4.5 COMET method

Void

A.2.1.4.6 INFO method

Prerequisite A.5/6 – INFO request

Table A.32: Supported headers within the INFO request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow-Events	[28] 8.2.2	c1	c1	[28] 8.2.2	c2	c2
5	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
6	Call-ID	[26] 20.8	m		[26] 20.8	m	
7	Contact	[26] 20.10	o		[26] 20.10	o	
8	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
9	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
10	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
11	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
12	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
13	Expires	[26] 20.19	o		[26] 20.19	o	
14	From	[26] 20.20	m	m	[26] 20.20	m	m
15	Max-Forwards	[26] 20.22	o	o	[26] 20.22	n/a	n/a
16	Organization	[26] 20.25	o		[26] 20.25	o	
17	Priority	[26] 20.26	o	o	[26] 20.26	o	o
18	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
19	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
20	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a
21	Require	[26] 20.32	o	o	[26] 20.32	m	m
22	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
23	Subject	[26] 24.38	o		[26] 24.38	o	
24	Supported	[26] 20.37	o	o	[26] 20.37	m	m
25	Timestamp	[26] 20.38	c8	c8	[26] 20.38	m	m
26	To	[26] 20.39	m	m	[26] 20.39	m	m
27	User-Agent	[26] 20.41	o		[26] 20.41	o	
28	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/20 THEN o ELSE n/a.						
c2:	IF A.4/20 THEN m ELSE n/a.						
c3:	IF A.4/7 THEN m ELSE n/a.						
c4:	IF A.4/11 THEN o ELSE n/a.						
c8:	IF A.4/6 THEN o ELSE n/a.						

Prerequisite A.5/6 – INFO request

Table A.33: Supported message bodies within the INFO request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.5/7 – INFO response

Prerequisite: A.6/1 – 100 Trying

Table A.34: Supported headers within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	n/a	n/a	[26] 20.8	m	m
2	Content-Length	[26] 20.14	n/a	n/a	[26] 20.14	m	m
3	Cseq	[26] 20.16	n/a	n/a	[26] 20.16	m	m
4	Date	[26] 20.17	n/a	n/a	[26] 20.17	m	m
5	From	[26] 20.20	n/a	n/a	[26] 20.20	m	m
6	To	[26] 20.39	n/a	n/a	[26] 20.39	m	m
7	Via	[26] 20.42	n/a	n/a	[26] 20.42	m	m

Prerequisite A.5/7 – INFO response

Table A.35: Supported headers within the INFO response - all remaining status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
3	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
4	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
5	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
6	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
7	From	[26] 20.20	m	m	[26] 20.20	m	m
8	Organization	[26] 20.25	o		[26] 20.25	o	
9	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
10	To	[26] 20.39	m	m	[26] 20.39	m	m
11	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/11 THEN o ELSE n/a.						
c2:	IF A.4/6 THEN m ELSE n/a.						

Prerequisite A.5/7 – INFO response

Prerequisite: A.6/6 – 2xx

Table A.36: Supported headers within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m		[26] 20.5	m	
2	Expires	[26] 20.19	o		[26] 20.19	o	
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/7 – INFO response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 – 3xx

Table A.37: Supported headers within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Expires	[26] 20.19	o		[26] 20.19	o	
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/7 – INFO response

Prerequisite: A.6/14 – 401

Table A.38: Supported headers within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Expires	[26] 20.19	o		[26] 20.19	o	
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
8	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	

Prerequisite A.5/7 – INFO response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 – 404, 413, 480, 486, 500, 503, 600, 603

Table A.39: Supported headers within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Expires	[26] 20.19	o		[26] 20.19	o	
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o
5	Server	[26] 20.35	o	o	[26] 20.35	o	o
6	Supported	[26] 20.37	m	m	[26] 20.37	m	m
7	User-Agent	[26] 20.41	o		[26] 20.41	o	
8	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/7 – INFO response

Prerequisite: A.6/18 -- "405" Method Not Allowed

Table A.40: Supported headers within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m		[26] 20.5	m	
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Expires	[26] 20.19	o		[26] 20.19	o	
4	Require	[26] 20.32	m	m	[26] 20.32	m	m
5	Server	[26] 20.35	o	o	[26] 20.35	o	o
6	Supported	[26] 20.37	m	m	[26] 20.37	m	m
7	User-Agent	[26] 20.41	o		[26] 20.41	o	
8	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/7 – INFO response

Prerequisite: A.6/25 -- "415" Unsupported Media Type @@@ combine

Table A.41: Supported headers within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Expires	[26] 20.19	o		[26] 20.19	o	
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/7 – INFO response

Prerequisite: A.6/27 – 420

Table A.42: Supported headers within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Expires	[26] 20.19	o		[26] 20.19	o	
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m
7	User-Agent	[26] 20.41	o		[26] 20.41	o	
8	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/7 - - INFO response

Prerequisite: A.6/34 - - 484

Table A.43: Supported headers within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Expires	[26] 20.19	o		[26] 20.19	o	
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/7 – INFO response

Prerequisite: A.6/35 - - 485 "Ambiguous" @@@ combine

Table A.44: Supported headers within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Expires	[26] 20.19	o		[26] 20.19	o	
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/7 – INFO response

Table A.45: Supported message bodies within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.1.4.7 INVITE method

Prerequisite A.5/8 – INVITE request

Table A.46: Supported headers within the INVITE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Alert-Info	[26] 20.4	o	o	[26] 20.4	c1	c1
5	Allow	[26] 20.5, [26] 5.1	o		[26] 20.5, [26] 5.1	o	
6	Allow-Events	[28] 8.2.2	c2	c2	[28] 8.2.2	c2	c2
7	Anonymity	[34] 5.2	o		[34] 5.2		
8	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
9	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
10	Call-Info	[26] 20.9	o		[26] 20.9	o	
11	Contact	[26] 20.10	m		[26] 20.10	m	
12	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
13	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
14	Content-Language	[26] 20.13	o		[26] 20.13	o	
15	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
16	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
17	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
18	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
19	Expires	[26] 20.19	o		[26] 20.19	o	
20	From	[26] 20.20	m	m	[26] 20.20	m	m
21	In-Reply-To	[26] 24.21	o	o	[26] 24.21	o	o
22	Max-Forwards	[26] 20.22	o	o	[26] 20.22	n/a	n/a
23	MIME-Version	[26] 20.24	o		[26] 20.24	o	
24	Organization	[26] 20.25	o		[26] 20.25	o	
25	P-Media-Authorization	[31] 6.1	n/a	n/a	[31] 6.1	c11	c12
26	Priority	[26] 20.26	o	o	[26] 20.26	o	o
27	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
28	Proxy-Require	[26] 20.29, [34] 4	c5	c5	[26] 20.29, [34] 4	n/a	n/a
29	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	m	m
30	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
31	Reply-To	[26] 20.31	o	o	[26] 20.31	o	o
32	Require	[26] 20.32	c8	o	[26] 20.32	m	m
33	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
34	Subject	[26] 24.38	o		[26] 24.38	o	
35	Supported	[26] 20.37	c9	m	[26] 20.37	m	m
36	Timestamp	[26] 20.38	c10	c10	[26] 20.38	m	m
37	To	[26] 20.39	m	m	[26] 20.39	m	m
38	User-Agent	[26] 20.41	o		[26] 20.41	o	
39	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/12 THEN m ELSE n/a.						
c2:	IF A.4/20 THEN m ELSE n/a.						
c3:	IF A.4/7 THEN m ELSE n/a.						
c4:	IF A.4/11 THEN o ELSE n/a.						
c5:	IF A.4/18 THEN m ELSE o -- (note).						
c8:	IF A.4/14 THEN o.1 ELSE o -- Reliable transport.						
c9:	IF IF A.4/14 THEN o.1 ELSE o -- support of reliable transport.						
c10:	IF A.4/6 THEN o ELSE n/a.						
c11:	IF A.4/19 THEN m ELSE n/a.						
c12:	IF A.3/1 THEN m ELSE n/a.						
o.1:	At least one of these shall be supported.						
NOTE:	No distinction has been made in these tables between first use of a request on a From/To/Call-ID combination, and the usage in a subsequent one. Therefore the use of "o" etc. above has been included from a viewpoint of first usage.						

Prerequisite A.5/8 – INVITE request

Table A.47: Supported message bodies within the INVITE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.5/9 – INVITE response

Prerequisite: A.6/1 – 100 Trying

Table A.48: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	n/a	n/a	[26] 20.8	m	m
2	Content-Length	[26] 20.14	n/a	n/a	[26] 20.14	m	m
3	Cseq	[26] 20.16	n/a	n/a	[26] 20.16	m	m
4	Date	[26] 20.17	n/a	n/a	[26] 20.17	m	m
5	From	[26] 20.20	n/a	n/a	[26] 20.20	m	m
6	To	[26] 20.39	n/a	n/a	[26] 20.39	m	m
7	Via	[26] 20.42	n/a	n/a	[26] 20.42	m	m

Prerequisite A.5/9 – INVITE response

Table A.49: Supported headers within the INVITE response - all remaining status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Disposition	[26] 20.11, [30] 8.3	o		[26] 20.11, [30] 8.3	o	
3	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
4	Content-Language	[26] 20.13	o		[26] 20.13	o	
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o		[26] 20.24	o	
11	Organization	[26] 20.25	o		[26] 20.25	o	
12	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
13	To	[26] 20.39	m	m	[26] 20.39	m	m
14	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1: IF A.4/11 THEN o ELSE n/a. c2: IF A.4/6 THEN m ELSE n/a.							

Prerequisite A.5/9 – INVITE response

Prerequisite: A.6/2 OR A.6/3 OR A.6/4 OR A.6/5 – 1xx

Table A.50: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Anonymity	[34] 5.2	o		[34] 5.2		
3	Call-Info	[26] 20.9	o		[26] 20.9	o	
4	Contact	[26] 20.10	o		[26] 20.10	o/m	
5	Expires	[26] 20.19	o		[26] 20.19	o	
6	P-Media-Authorization	[31] 6.1	n/a	n/a	[31] 6.1	c11	c12
7	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
8	Require	[26] 20.32	m	m	[26] 20.32	m	m
9	Rseq	[27] 7.1	c2	m	[27] 7.1	c3	m
10	Server	[26] 20.35	o	o	[26] 20.35	o	o
11	Supported	[26] 20.37	m	m	[26] 20.37	m	m
12	User-Agent	[26] 20.41	o		[26] 20.41	o	
13	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.4/14 THEN o ELSE n/a - - reliability of provisional responses.						
c3:	IF A.4/14 THEN m ELSE n/a - - reliability of provisional responses.						
c11:	IF A.4/19 THEN m ELSE n/a.						
c12:	IF A.3/1 THEN m ELSE n/a.						

Prerequisite A.5/9 – INVITE response

Prerequisite: A.6/6 – 2xx

Table A.51: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Allow	[26] 20.5	o		[26] 20.5	o	
3	Anonymity	[34] 5.2	o		[34] 5.2		
4	Authentication-Info	[26] 20.6	o		[26] 20.6	o	
5	Call-Info	[26] 20.9	o		[26] 20.9	o	
6	Contact	[26] 20.10	m		[26] 20.10	m	
7	Expires	[26] 20.19	o		[26] 20.19	o	
8	P-Media-Authorization	[31] 6.1	n/a	n/a	[31] 6.1	c11	c12
9	Record-Route	[26] 20.30	m	m	[26] 20.30	m	m
10	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
11	Require	[26] 20.32	m	m	[26] 20.32	m	m
12	Server	[26] 20.35	o	o	[26] 20.35	o	o
13	Supported	[26] 20.37	m	m	[26] 20.37	m	m
14	User-Agent	[26] 20.41	o		[26] 20.41	o	
15	Warning	[26] 20.43	o		[26] 20.43	o	
c11:	IF A.4/19 THEN m ELSE n/a.						
c12:	IF A.3/1 THEN m ELSE n/a.						

Prerequisite A.5/9 – INVITE response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/34 – 3xx or 485 "Ambiguous"

Table A.52: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Anonymity	[34] 5.2	o		[34] 5.2		
3	Call-Info	[26] 20.9	o		[26] 20.9	o	
4	Contact	[26] 20.10	o		[26] 20.10	o/m	
5	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
6	Expires	[26] 20.19	o		[26] 20.19	o	
7	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
8	Require	[26] 20.32	m	m	[26] 20.32	m	m
9	Server	[26] 20.35	o	o	[26] 20.35	o	o
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m
11	User-Agent	[26] 20.41	o		[26] 20.41	o	
12	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/9 – INVITE response

Prerequisite: A.6/14 – 401

Table A.53: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Anonymity	[34] 5.2	o		[34] 5.2		
3	Call-Info	[26] 20.9	o		[26] 20.9	o	
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Expires	[26] 20.19	o		[26] 20.19	o	
6	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
7	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
8	Require	[26] 20.32	m	m	[26] 20.32	m	m
9	Server	[26] 20.35	o	o	[26] 20.35	o	o
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m
11	User-Agent	[26] 20.41	o		[26] 20.41	o	
12	Warning	[26] 20.43	o		[26] 20.43	o	
13	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	
c1:	IF A.4/11 THEN o ELSE n/a.						
c2:	IF A.4/6 THEN m ELSE n/a.						

Prerequisite A.5/9 – INVITE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/50 OR A.6/51 - - 404, 413, 480, 486, 600, 603

Table A.54: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Anonymity	[34] 5.2	o		[34] 5.2		
3	Call-Info	[26] 20.9	o		[26] 20.9	o	
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Expires	[26] 20.19	o		[26] 20.19	o	
6	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
7	Require	[26] 20.32	m	m	[26] 20.32	m	m
8	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o
9	Server	[26] 20.35	o	o	[26] 20.35	o	o
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m
11	User-Agent	[26] 20.41	o		[26] 20.41	o	
12	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/9 – INVITE response

Prerequisite: A.6/18 -- "405" Method Not Allowed

Table A.55: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Allow	[26] 20.5	m		[26] 20.5	m/o	
3	Anonymity	[34] 5.2	o		[34] 5.2	o	
4	Call-Info	[26] 20.9	o		[26] 20.9	o	
5	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
6	Expires	[26] 20.19	o		[26] 20.19	o	
7	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
8	Require	[26] 20.32	m	m	[26] 20.32	m	m
9	Server	[26] 20.35	o	o	[26] 20.35	o	o
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m
11	User-Agent	[26] 20.41	o		[26] 20.41	o	
12	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/9 – INVITE response

Prerequisite: A.6/20 – 407

Table A.56: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Anonymity	[34] 5.2	o		[34] 5.2		
3	Call-Info	[26] 20.9	o		[26] 20.9	o	
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Expires	[26] 20.19	o		[26] 20.19	o	
6	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
7	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
8	Require	[26] 20.32	m	m	[26] 20.32	m	m
9	Server	[26] 20.35	o	o	[26] 20.35	o	o
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m
11	User-Agent	[26] 20.41	o		[26] 20.41	o	
12	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/9 – INVITE response

Prerequisite: A.6/25 -- "415" Unsupported Media Type

Table A.57: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Anonymity	[34] 5.2	o		[34] 5.2		
5	Call-Info	[26] 20.9	o		[26] 20.9	o	
6	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
7	Expires	[26] 20.19	o		[26] 20.19	o	
8	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
9	Require	[26] 20.32	m	m	[26] 20.32	m	m
10	Server	[26] 20.35	o	o	[26] 20.35	o	o
11	Supported	[26] 20.37	m	m	[26] 20.37	m	m
12	User-Agent	[26] 20.41	o		[26] 20.41	o	
13	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/9 – INVITE response

Prerequisite: A.6/27 – 420

Table A.58: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Anonymity	[34] 5.2	o		[34] 5.2		
3	Call-Info	[26] 20.9	o		[26] 20.9	o	
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Expires	[26] 20.19	o		[26] 20.19	o	
6	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
7	Require	[26] 20.32	m	m	[26] 20.32	m	m
8	Server	[26] 20.35	o	o	[26] 20.35	o	o
9	Supported	[26] 20.37	m	m	[26] 20.37	m	m
10	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m
11	User-Agent	[26] 20.41	o		[26] 20.41	o	
12	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/9 – INVITE response

Prerequisite: A.6/34 – 484

Table A.59: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Anonymity	[34] 5.2	o		[34] 5.2		
3	Call-Info	[26] 20.9	o		[26] 20.9	o	
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Expires	[26] 20.19	o		[26] 20.19	o	
6	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
7	Require	[26] 20.32	m	m	[26] 20.32	m	m
8	Server	[26] 20.35	o	o	[26] 20.35	o	o
9	Supported	[26] 20.37	m	m	[26] 20.37	m	m
10	User-Agent	[26] 20.41	o		[26] 20.41	o	
11	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/9 – INVITE response

Prerequisite: A.6/42 - - 500

Table A.60: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Anonymity	[34] 5.2	o		[34] 5.2		
3	Call-Info	[26] 20.9	o		[26] 20.9	o	
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Expires	[26] 20.19	o		[26] 20.19	o	
6	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
7	Require	[26] 20.32	m	m	[26] 20.32	m	m
8	Retry-After	[26] 20.33	m	m	[26] 20.33	o	o
9	Server	[26] 20.35	o	o	[26] 20.35	o	o
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m
11	User-Agent	[26] 20.41	o		[26] 20.41	o	
12	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/9 – INVITE response

Prerequisite: A.6/45 - - 503

Table A.61: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Anonymity	[34] 5.2	o		[34] 5.2		
3	Call-Info	[26] 20.9	o		[26] 20.9	o	
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Expires	[26] 20.19	o		[26] 20.19	o	
6	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
7	Require	[26] 20.32	m	m	[26] 20.32	m	m
8	Retry-After	[26] 20.33	o	o	[26] 20.33	o	m
9	Server	[26] 20.35	o	o	[26] 20.35	o	o
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m
11	User-Agent	[26] 20.41	o		[26] 20.41	o	
12	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/9 – INVITE response

Table A.62: Supported message bodies within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.1.4.8 NOTIFY method

Prerequisite A.5/10 - - NOTIFY request

Table A.63: Supported headers within the NOTIFY request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow-Events	[28] 8.2.2	c1	c1	[28] 8.2.2	c2	c2
5	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
8	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
9	Content-Language	[26] 20.13	o		[26] 20.13	o	
10	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
11	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
12	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
13	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
14	Event	[28] 8.2.1	m	m	[28] 8.2.1	m	m
15	From	[26] 20.20	m	m	[26] 20.20	m	m
16	Max-Forwards	[26] 20.22	o	o	[26] 20.22	n/a	n/a
17	MIME-Version	[26] 20.24	o		[26] 20.24	o	
18	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
19	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
20	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	c9	c9
21	Require	[26] 20.32	o	o	[26] 20.32	m	m
22	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
23	Subscription-State	[28] 8.2.3	m	m	[28] 8.2.3	m	m
24	Supported	[26] 20.37	o	o	[26] 20.37	m	m
25	Timestamp	[26] 20.38	c8	c8	[26] 20.38	m	m
26	To	[26] 20.39	m	m	[26] 20.39	m	m
27	User-Agent	[26] 20.41	o		[26] 20.41	o	
28	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/20 THEN o ELSE n/a.						
c2:	IF A.4/20 THEN m ELSE n/a.						
c3:	IF A.4/7 THEN m ELSE n/a.						
c4:	IF A.4/11 THEN o ELSE n/a.						
c8:	IF A.4/6 THEN o ELSE n/a.						
c9:	IF A.4/15 OR A.4/20 THEN m ELSE n/a - - the REFER method or SIP specific event notification.						

Prerequisite A.5/10 - - NOTIFY request

Table A.64: Supported message bodies within the NOTIFY request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	sipfrag	[37] 2	c1	c1	[37]	c1	c1
c1:	IF A.4/15 THEN m ELSE o						

Prerequisite A.5/11 - - NOTIFY response

Table A.65: Supported headers within the NOTIFY response - all status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
4	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
5	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
6	Content-Language	[26] 20.13	o		[26] 20.13	o	
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o		[26] 20.24	o	
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
12	To	[26] 20.39	m	m	[26] 20.39	m	m
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/11 THEN o ELSE n/a.						
c2:	IF A.4/6 THEN m ELSE n/a.						

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/6 and A.6/7 - - 2xx

Table A.66: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Authentication-Info	[26] 20.6	o		[26] 20.6	o	
2	Record-Route	[26] 20.30	c3	c3	[26] 20.30	c3	c3
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c3:	IF A.4/15 OR A.4/20 THEN m ELSE n/a - - the REFER method or SIP specific event notification.						

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/35 - - 3xx or 485 "Ambiguous"

Table A.67: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Contact	[26] 20.10	o		[26] 20.10	o	
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/14 - - 401

Table A.68: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
8	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.69: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Require	[26] 20.32	m	m	[26] 20.32	m	m
3	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/18 -- "405" Method Not Allowed

Table A.70: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m		[26] 20.5	m	
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/20 - - 407

Table A.71: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c1: IF A.4/11 THEN o ELSE n/a. c2: IF A.4/6 THEN m ELSE n/a.							

Prerequisite A.5/11 - - NOTIFY response

Prerequisite A.6/25 -- "415" Unsupported Media Type

Table A.72: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/27 - - 420

Table A.73: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Require	[26] 20.32	m	m	[26] 20.32	m	m
3	Server	[26] 20.35	o	o	[26] 20.35	o	o
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/34 - - 484

Table A.74: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Require	[26] 20.32	m	m	[26] 20.32	m	m
3	Server	[26] 20.35	o	o	[26] 20.35	o	o
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	User-Agent	[26] 20.41	o		[26] 20.41	o	
6	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/39 - - 489

Table A.75: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	m	m
2	Authentication-Info	[26] 20.6	o		[26] 20.6	o	
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Require	[26] 20.32	m	m	[26] 20.32	m	m
5	Server	[26] 20.35	o	o	[26] 20.35	o	o
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/11 - - NOTIFY response

Table A.76: Supported message bodies within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.1.4.9 OPTIONS method

Prerequisite A.5/12 – OPTIONS request

Table A.77: Supported headers within the OPTIONS request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow-Events	[28] 8.2.2	c1	c1	[28] 8.2.2	c1	c1
5	Authorization	[26] 20.7	c2	c2	[26] 20.7	c2	c2
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Call-Info	[26] 20.9	o		[26] 20.9	o	
8	Contact	[26] 20.10	m		[26] 20.10	m	
9	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
10	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
11	Content-Language	[26] 20.13	o		[26] 20.13	o	
12	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
13	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
14	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
15	Date	[26] 20.17	c3	c3	[26] 20.17	m	m
16	From	[26] 20.20	m	m	[26] 20.20	m	m
17	Max-Forwards	[26] 20.22	o	o	[26] 20.22	n/a	n/a
18	MIME-Version	[26] 20.24	o		[26] 20.24	o	
19	Organization	[26] 20.25	o		[26] 20.25	o	
20	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
21	Proxy-Require	[26] 20.29	o	o (note)	[26] 20.29	n/a	n/a
22	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a
23	Require	[26] 20.32	o	o	[26] 20.32	m	m
24	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
25	Supported	[26] 20.37	c6	c6	[26] 20.37	m	m
26	Timestamp	[26] 20.38	c7	c7	[26] 20.38	m	m
27	To	[26] 20.39	m	m	[26] 20.39	m	m
28	User-Agent	[26] 20.41	o		[26] 20.41	o	
29	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1: IF A.4/20 THEN m ELSE n/a. c2: IF A.4/7 THEN m ELSE n/a. c3: IF A.4/11 THEN o ELSE n/a. c7: IF A.4/6 THEN o ELSE n/a.							
NOTE: No distinction has been made in these tables between first use of a request on a From/To/Call-ID combination, and the usage in a subsequent one. Therefore the use of "o" etc. above has been included from a viewpoint of first usage.							

Prerequisite A.5/12 – OPTIONS request

Table A.78: Supported message bodies within the OPTIONS request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.5/13 – OPTIONS response

Prerequisite: A.6/1 – 100 Trying

Table A.79: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	n/a	n/a	[26] 20.8	m	m
2	Content-Length	[26] 20.14	n/a	n/a	[26] 20.14	m	m
3	Cseq	[26] 20.16	n/a	n/a	[26] 20.16	m	m
4	Date	[26] 20.17	n/a	n/a	[26] 20.17	m	m
5	From	[26] 20.20	n/a	n/a	[26] 20.20	m	m
6	To	[26] 20.39	n/a	n/a	[26] 20.39	m	m
7	Via	[26] 20.42	n/a	n/a	[26] 20.42	m	m
c1: IF A.4/11 THEN o ELSE n/a. c2: IF A.4/6 THEN m ELSE n/a.							

Prerequisite A.5/13 – OPTIONS response

Table A.80: Supported headers within the OPTIONS response - all remaining status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
3	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
4	Content-Language	[26] 20.13	o		[26] 20.13	o	
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o		[26] 20.24	o	
11	Organization	[26] 20.25	o		[26] 20.25	o	
12	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
13	To	[26] 20.39	m	m	[26] 20.39	m	m
14	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1: IF A.4/11 THEN o ELSE n/a. c2: IF A.4/6 THEN m ELSE n/a.							

Prerequisite A.5/13 – OPTIONS response

Prerequisite: A.6/6 – 2xx

Table A.81: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Allow	[26] 20.5	o		[26] 20.5	o/m	
3	Authentication-Info	[26] 20.6	o		[26] 20.6	o	
4	Call-Info	[26] 20.9	o		[26] 20.9	o	
5	Contact	[26] 20.10	o		[26] 20.10	o	
6	Require	[26] 20.32	m	m	[26] 20.32	m	m
7	Server	[26] 20.35	o	o	[26] 20.35	o	o
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/13 – OPTIONS response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/35 – 3xx or 485 "Ambiguous"

Table A.82: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Contact	[26] 20.10	o		[26] 20.10	o	
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/13 – OPTIONS response

Prerequisite: A.6/14 – 401

Table A.83: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
10	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.84: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Require	[26] 20.32	m	m	[26] 20.32	m	m
5	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/13 – OPTIONS response

Prerequisite: A.6/18 -- "405" Method Not Allowed

Table A.85: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Allow	[26] 20.5	m	m	[26] 20.5	m	m
3	Call-Info	[26] 20.9	o		[26] 20.9	o	
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/13 – OPTIONS response

Prerequisite: A.6/20 – 407

Table A.86: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/13 – OPTIONS response

Prerequisite: A.6/25 -- "415" Unsupported Media Type

Table A.87: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Call-Info	[26] 20.9	o		[26] 20.9	o	
5	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
6	Require	[26] 20.32	m	m	[26] 20.32	m	m
7	Server	[26] 20.35	o	o	[26] 20.35	o	o
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/13 – OPTIONS response

Prerequisite: A.6/27 – 420

Table A.88: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Require	[26] 20.32	m	m	[26] 20.32	m	m
5	Server	[26] 20.35	o	o	[26] 20.35	o	o
6	Supported	[26] 20.37	m	m	[26] 20.37	m	m
7	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/13 – OPTIONS response

Prerequisite: A.6/34 – 484

Table A.89: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Contact	[26] 20.10	o		[26] 20.10	o	
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/13 - - OPTIONS response

Table A.90: Supported message bodies within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.1.3.10 PRACK method

Prerequisite A.5/14 – PRACK request

Table A.91: Supported headers within the PRACK request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow-Events	[28] 8.2.2	c1	c1	[28] 8.2.2	c2	c2
5	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
8	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
9	Content-Language	[26] 20.13	o		[26] 20.13	o	
10	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
11	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
12	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
13	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
14	From	[26] 20.20	m	m	[26] 20.20	m	m
15	Max-Forwards	[26] 20.22	o	o	[26] 20.22	n/a	n/a
16	MIME-Version	[26] 20.24	o		[26] 20.24	o	
17	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
18	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
19	RAck	[27] 7.2	m	m	[27] 7.2	m	m
20	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a
21	Require	[26] 20.32	o	o	[26] 20.32	m	m
22	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
23	Supported	[26] 20.37	o	o	[26] 20.37	m	m
24	Timestamp	[26] 20.38	c8	c8	[26] 20.38	m	m
25	To	[26] 20.39	m	m	[26] 20.39	m	m
26	User-Agent	[26] 20.41	o		[26] 20.41	o	
27	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/20 THEN o ELSE n/a.						
c2:	IF A.4/20 THEN m ELSE n/a.						
c3:	IF A.4/7 THEN m ELSE n/a.						
c4:	IF A.4/11 THEN o ELSE n/a.						
c8:	IF A.4/6 THEN o ELSE n/a.						

Prerequisite A.5/14 – PRACK request

Table A.92: Supported message bodies within the PRACK request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.5/15 - PRACK response

Prerequisite: A.6/1 – 100 Trying

Table A.93: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	n/a	n/a	[26] 20.8	m	m
2	Content-Length	[26] 20.14	n/a	n/a	[26] 20.14	m	m
3	Cseq	[26] 20.16	n/a	n/a	[26] 20.16	m	m
4	Date	[26] 20.17	n/a	n/a	[26] 20.17	m	m
5	From	[26] 20.20	n/a	n/a	[26] 20.20	m	m
6	To	[26] 20.39	n/a	n/a	[26] 20.39	m	m
7	Via	[26] 20.42	n/a	n/a	[26] 20.42	m	m

Prerequisite A.5/15 – PRACK response

Table A.94: Supported headers within the PRACK response - all remaining status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
3	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
4	Content-Language	[26] 20.13	o		[26] 20.13	o	
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o		[26] 20.24	o	
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
12	To	[26] 20.39	m	m	[26] 20.39	m	m
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/11 THEN o ELSE n/a.						

Prerequisite A.5/15 – PRACK response

Prerequisite: A.6/6 – 2xx

Table A.95: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Require	[26] 20.32	m	m	[26] 20.32	m	m
2	Server	[26] 20.35	o	o	[26] 20.35	o	o
3	Supported	[26] 20.37	m	m	[26] 20.37	m	m
4	User-Agent	[26] 20.41	o		[26] 20.41	o	
5	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/35 - - 3xx or 485 "Ambiguous"

Table A.96: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Contact	[26] 20.10	o		[26] 20.10	o	
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/14 - - 401

Table A.97: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
8	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	

Prerequisite A.5/15 – PRACK response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.98: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Require	[26] 20.32	m	m	[26] 20.32	m	m
3	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/15 – PRACK response

Prerequisite: A.6/18 -- "405" Method Not Allowed

Table A.99: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m		[26] 20.5	m	
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/20 - - 407

Table A.100: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/15 – PRACK response

Prerequisite: A.6/25 -- "415" Unsupported Media Type

Table A.101: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/15 - PRACK response

Prerequisite: A.6/27 - 420@@@combine

Table A.102: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Require	[26] 20.32	m	m	[26] 20.32	m	m
3	Server	[26] 20.35	o	o	[26] 20.35	o	o
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	User-Agent	[26] 20.41	o		[26] 20.41	o	
6	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/15 – PRACK response

Prerequisite: A.6/34 – 484

Table A.103: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Require	[26] 20.32	m	m	[26] 20.32	m	m
3	Server	[26] 20.35	o	o	[26] 20.35	o	o
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	User-Agent	[26] 20.41	o		[26] 20.41	o	
6	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/15 – PRACK response

Table A.104: Supported message bodies within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.1.4.11 REFER method

Prerequisite A.5/16 – REFER request

Table A.105: Supported headers within the REFER request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Language	[26] 20.3	o		[26] 20.3	o	
2	Allow-Events	[28] 8.2.2	c1	c1	[28] 8.2.2	c2	c2
3	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
4	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
5	Contact	[26] 20.10	o		[26] 20.10	o	
6	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
7	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
8	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
9	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
10	Expires	[26] 20.19	o		[26] 20.19	o	
11	From	[26] 20.20	m	m	[26] 20.20	m	m
12	Max-Forwards	[26] 20.22	o	o	[26] 20.22	n/a	n/a
13	MIME-Version	[26] 20.24	o		[26] 20.24	o	
14	Organization	[26] 20.25	o		[26] 20.25	o	
15	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
16	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
17	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	m	m
18	Refer-To	[36] 3	m	m	[36] 3	m	m
19	Require	[26] 20.32	o	o	[26] 20.32	m	m
20	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
21	Supported	[26] 20.37, [26] 7.1	o	o	[26] 20.37, [26] 7.1	m	m
22	Timestamp	[26] 20.38	c6	c6	[26] 20.38	m	m
23	To	[26] 20.39	m	m	[26] 20.39	m	m
24	User-Agent	[26] 20.41	o		[26] 20.41	o	
25	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/20 THEN o ELSE n/a.						
c2:	IF A.4/20 THEN m ELSE n/a.						
c3:	IF A.4/7 THEN m ELSE n/a.						
c4:	IF A.4/11 THEN o ELSE n/a.						
c6:	IF A.4/6 THEN o ELSE n/a.						

Prerequisite A.5/16 – REFER request

Table A.106: Supported message bodies within the REFER request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.5/17 – REFER response

Prerequisite: A.6/1 – 100 Trying

Table A.107: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	n/a	n/a	[26] 20.8	m	m
2	Content-Length	[26] 20.14	n/a	n/a	[26] 20.14	m	m
3	Cseq	[26] 20.16	n/a	n/a	[26] 20.16	m	m
4	Date	[26] 20.17	n/a	n/a	[26] 20.17	m	m
5	From	[26] 20.20	n/a	n/a	[26] 20.20	m	m
6	To	[26] 20.39	n/a	n/a	[26] 20.39	m	m
7	Via	[26] 20.42	n/a	n/a	[26] 20.42	m	m

Prerequisite A.5/17 – REFER response

Table A.108: Supported headers within the REFER response - all remaining status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
3	Content-Language	[26] 20.13	o		[26] 20.13	o	
4	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
5	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
6	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
7	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
8	From	[26] 20.20	m	m	[26] 20.20	m	m
9	MIME-Version	[26] 20.24	o		[26] 20.24	o	
10	Organization	[26] 20.25	o		[26] 20.25	o	
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
12	To	[26] 20.39	m	m	[26] 20.39	m	m
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/11 THEN o ELSE n/a.						
c2:	IF A.4/6 THEN m ELSE n/a.						

Prerequisite A.5/17 – REFER response

Prerequisite: A.6/7 - - 202

Table A.109: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Authentication-Info	[26] 20.6	o		[26] 20.6	o	
3	Contact	[26] 20.10	o		[26] 20.10	o	
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Record-Route	[26] 20.30	m	m	[26] 20.30	m	m
6	Require	[26] 20.32	m	m	[26] 20.32	m	m
7	Server	[26] 20.35	o	o	[26] 20.35	o	o
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/35 - - 3xx or 485 "Ambiguous"@@@combine

Table A.110: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Contact	[26] 20.10	o		[26] 20.10	o	
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/17 – REFER response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11OR A.6/12 – 401

Table A.111: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Expires	[26] 20.19	o		[26] 20.19	o	
4	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
10	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.112: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Contact	[26] 20.10	o		[26] 20.10	o	
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o
7	Server	[26] 20.35	o	o	[26] 20.35	o	o
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/17 – REFER response

Prerequisite: A.6/18 -- "405" Method Not Allowed

Table A.113: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Allow	[26] 20.5	m	m	[26] 20.5	m	m
3	Expires	[26] 20.19	o		[26] 20.19	o	
4	Require	[26] 20.32	m	m	[26] 20.32	m	m
5	Server	[26] 20.35	o	o	[26] 20.35	o	o
6	Supported	[26] 20.37	m	m	[26] 20.37	m	m
7	User-Agent	[26] 20.41	o		[26] 20.41	o	
8	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/17 – REFER response

Prerequisite: A.6/20 – 407

Table A.114: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Contact	[26] 20.10	o		[26] 20.10	o	
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Expires	[26] 20.19	o		[26] 20.19	o	
4	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/17 – REFER response

Prerequisite: A.6/25 -- "415" Unsupported Media Type

Table A.115: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Expires	[26] 20.19	o		[26] 20.19	o	
6	Require	[26] 20.32	m	m	[26] 20.32	m	m
7	Server	[26] 20.35	o	o	[26] 20.35	o	o
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/17 – REFER response

Prerequisite: A.6/27 – 420

Table A.116: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Contact	[26] 20.10	o		[26] 20.10	o	
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/17 – REFER response

Prerequisite: A.6/34 – 484@@@combine

Table A.117: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Contact	[26] 20.10	o		[26] 20.10	o	
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/17 - - REFER response

Table A.118: Supported message bodies within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.1.4.12 REGISTER method

Prerequisite A.5/18 - - REGISTER request

Table A.119: Supported headers within the REGISTER request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow-Events	[28] 8.2.2	c1	c1	[28] 8.2.2	c1	c1
5	Authorization	[26] 20.7	c2	n/a	[26] 20.7	c2	n/a
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Call-Info	[26] 20.9	o		[26] 20.9	o	
8	Contact	[26] 20.10	m		[26] 20.10	m	
9	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
10	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
11	Content-Language	[26] 20.13	o		[26] 20.13	o	
12	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
13	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
14	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
15	Date	[26] 20.17	c3	c3	[26] 20.17	m	m
16	Expires	[26] 20.19	o		[26] 20.19	o	
17	From	[26] 20.20	m	m	[26] 20.20	m	m
18	Max-Forwards	[26] 20.22	o	o	[26] 20.22	n/a	n/a
19	MIME-Version	[26] 20.24	o		[26] 20.24	o	
20	Organization	[26] 20.25	o		[26] 20.25	o	
21	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
22	Proxy-Require	[26] 20.29	o	o (note)	[26] 20.29	n/a	n/a
23	Require	[26] 20.32	o	o	[26] 20.32	m	m
24	Route	[26] 20.34	o	n/a	[26] 20.34	n/a	n/a
25	Supported	[26] 20.37	o	o	[26] 20.37	m	m
26	Timestamp	[26] 20.38	m	m	[26] 20.38	c7	c7
27	To	[26] 20.39	m	m	[26] 20.39	m	m
28	User-Agent	[26] 20.41	o		[26] 20.41	o	
29	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1: IF A.4/20 THEN m ELSE n/a. c2: IF A.4/8 THEN m ELSE n/a. c3: IF A.4/11 THEN o ELSE n/a. c7: IF A.4/6 THEN m ELSE n/a.							
NOTE: No distinction has been made in these tables between first use of a request on a From/To/Call-ID combination, and the usage in a subsequent one. Therefore the use of "o" etc. above has been included from a viewpoint of first usage..							

Prerequisite A.5/18 - - REGISTER request

Table A.120: Supported message bodies within the REGISTER request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/1 - - 100 Trying

Table A.121: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	n/a	n/a	[26] 20.8	m	m
2	Content-Length	[26] 20.14	n/a	n/a	[26] 20.14	m	m
3	Cseq	[26] 20.16	n/a	n/a	[26] 20.16	m	m
4	Date	[26] 20.17	n/a	n/a	[26] 20.17	m	m
5	From	[26] 20.20	n/a	n/a	[26] 20.20	m	m
6	To	[26] 20.39	n/a	n/a	[26] 20.39	m	m
7	Via	[26] 20.42	n/a	n/a	[26] 20.42	m	m

Prerequisite A.5/19 – REGISTER response

Table A.122: Supported headers within the REGISTER response - all status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
3	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
4	Content-Language	[26] 20.13	o		[26] 20.13	o	
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o		[26] 20.24	o	
11	Organization	[26] 20.25	o		[26] 20.25	o	
12	Timestamp	[26] 20.38	c2	c2	[26] 20.38	m	m
13	To	[26] 20.39	m	m	[26] 20.39	m	m
14	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/11 THEN o ELSE n/a.						

Prerequisite A.5/19 – REGISTER response

Prerequisite: A.6/6 – 2xx

Table A.123: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Allow	[26] 20.5	o		[26] 20.5	o	
3	Authentication-Info	[26] 20.6	o		[26] 20.6	o	
4	Call-Info	[26] 20.9	o		[26] 20.9	o	
5	Contact	[26] 20.10	o		[26] 20.10	o	
6	Expires	[26] 20.19	o		[26] 20.19	o	
7	Require	[26] 20.32	m	m	[26] 20.32	m	m
8	Server	[26] 20.35	o	o	[26] 20.35	o	o
9	Supported	[26] 20.37	m	m	[26] 20.37	m	m
10	User-Agent	[26] 20.41	o		[26] 20.41	o	
11	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/35 - - 3xx or 485 "Ambiguous"

Table A.124: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Contact	[26] 20.10	o		[26] 20.10	o	
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Expires	[26] 20.19	o		[26] 20.19	o	
6	Require	[26] 20.32	m	m	[26] 20.32	m	m
7	Server	[26] 20.35	o	o	[26] 20.35	o	o
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/19 – REGISTER response

Prerequisite: A.6/14 – 401

Table A.125: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
10	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.126: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o
7	Server	[26] 20.35	o	o	[26] 20.35	o	o
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/19 – REGISTER response

Prerequisite: A.6/18 -- "405" Method Not Allowed

Table A.127: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Allow	[26] 20.5	m		[26] 20.5	m	
3	Call-Info	[26] 20.9	o		[26] 20.9	o	
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Expires	[26] 20.19	o		[26] 20.19	o	
6	Require	[26] 20.32	m	m	[26] 20.32	m	m
7	Server	[26] 20.35	o	o	[26] 20.35	o	o
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/19 – REGISTER response

Prerequisite: A.6/20 – 407

Table A.128: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
6	Require	[26] 20.32	m	m	[26] 20.32	m	m
7	Server	[26] 20.35	o	o	[26] 20.35	o	o
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/19 – REGISTER response

Prerequisite: A.6/25 -- "415" Unsupported Media Type

Table A.129: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Call-Info	[26] 20.9	o		[26] 20.9	o	
5	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
6	Expires	[26] 20.19	o	o	[26] 20.19	o	o
7	Require	[26] 20.32	m	m	[26] 20.32	m	m
8	Server	[26] 20.35	o	o	[26] 20.35	o	o
9	Supported	[26] 20.37	m	m	[26] 20.37	m	m
10	User-Agent	[26] 20.41	o		[26] 20.41	o	
11	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/27 - - 420

Table A.130: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/29 - - 423

Table A.131: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	o		[26] 20.18	o	
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Min-Expires	[26] 20.23	m	m	[26] 20.23	m	m
6	Require	[26] 20.32	m	m	[26] 20.32	m	m
7	Server	[26] 20.35	o		[26] 20.35	o	
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/34 - - 484

Table A.132: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1			[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/19 - - REGISTER response

Table A.133: Supported message bodies within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.1.4.13 SUBSCRIBE method

Prerequisite A.5/20 - - SUBSCRIBE request

Table A.134: Supported headers within the SUBSCRIBE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow-Events	[28] 8.2.2	c1	c1	[28] 8.2.2	c2	c2
5	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
8	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
9	Content-Language	[26] 20.13	o		[26] 20.13	o	
10	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
11	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
12	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
13	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
14	Event	[28] 8.2.1	m	m	[28] 8.2.1	m	m
15	Expires	[26] 20.19	m	m	[26] 20.19	m	m
16	From	[26] 20.20	m	m	[26] 20.20	m	m
17	Max-Forwards	[26] 20.22	o	o	[26] 20.22	n/a	n/a
18	MIME-Version	[26] 20.24	o		[26] 20.24	o	
19	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
20	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
21	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	m	m
22	Require	[26] 20.32	o	o	[26] 20.32	m	m
23	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
24	Supported	[26] 20.37	o	o	[26] 20.37	m	m
25	Timestamp	[26] 20.38	c8	c8	[26] 20.38	m	m
26	To	[26] 20.39	m	m	[26] 20.39	m	m
27	User-Agent	[26] 20.41	o		[26] 20.41	o	
28	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/20 THEN o ELSE n/a.						
c2:	IF A.4/20 THEN m ELSE n/a.						
c3:	IF A.4/7 THEN m ELSE n/a.						
c4:	IF A.4/11 THEN o ELSE n/a.						
c8:	IF A.4/6 THEN o ELSE n/a.						

Prerequisite A.5/20 - - SUBSCRIBE request

Table A.135: Supported message bodies within the SUBSCRIBE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.5/21 - - SUBSCRIBE response

Table A.136: Supported headers within the SUBSCRIBE response - all status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
3	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
4	Content-Language	[26] 20.13	o		[26] 20.13	o	
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o		[26] 20.24	o	
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
12	To	[26] 20.39	m	m	[26] 20.39	m	m
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/11 THEN o ELSE n/a.						
c2:	IF A.4/6 THEN m ELSE n/a.						

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/6 and A.6/7 - - 2xx

Table A.137: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Authentication-Info	[26] 20.6	o		[26] 20.6	o	
2	Expires	[26] 20.19	m	m	[26] 20.19	m	m
3	Record-Route	[26] 20.30	m	m	[26] 20.30	m	m
4	Require	[26] 20.32	m	m	[26] 20.32	m	m
5	Server	[26] 20.35	o	o	[26] 20.35	o	o
6	Supported	[26] 20.37	m	m	[26] 20.37	m	m
7	User-Agent	[26] 20.41	o		[26] 20.41	o	
8	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/35 - - 3xx or 485 "Ambiguous"

Table A.138: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Contact	[26] 20.10	o		[26] 20.10	o	
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/14 - - 401

Table A.139: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
8	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/50 OR A.6/51 - - 404, 413, 480, 486, 500, 600, 603

Table A.140: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Require	[26] 20.32	m	m	[26] 20.32	m	m
3	Retry-After	[26] 20.33	o		[26] 20.33	o	
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/18 -- "405" Method Not Allowed

Table A.141: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m		[26] 20.5	m	
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/20 - - 407

Table A.142: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite A.6/25 -- "415" Unsupported Media Type

Table A.143: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/27 - - 420

Table A.144: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Require	[26] 20.32	m	m	[26] 20.32	m	m
3	Server	[26] 20.35	o	o	[26] 20.35	o	o
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/29 - - 423

Table A. 145: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o		[26] 20.18	o	
2	Min-Expires	[26] 20.23	m	m	[26] 20.23	m	m
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Server	[26] 20.35	o		[26] 20.35	o	
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/34 - - 484

Table A.146: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Require	[26] 20.32	m	m	[26] 20.32	m	m
3	Server	[26] 20.35	o	o	[26] 20.35	o	o
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	User-Agent	[26] 20.41	o		[26] 20.41	o	
6	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/39 - - 489

Table A.147: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	m	m
2	Authentication-Info	[26] 20.6	o		[26] 20.6	o	
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Require	[26] 20.32	m	m	[26] 20.32	m	m
5	Server	[26] 20.35	o	o	[26] 20.35	o	o
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/45 - - 503

Table A.148: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Require	[26] 20.32	m	m	[26] 20.32	m	m
3	Retry-After	[26] 20.33	o	o	[26] 20.33	o	m
4	Server	[26] 20.35	o	o	[26] 20.35	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/21 - - SUBSCRIBE response

Table A.149: Supported message bodies within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.1.4.14 UPDATE method

Prerequisite A.5/22 – UPDATE request

Table A.150: Supported headers within the UPDATE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow	[26] 20.5	o		[26] 20.5	o	
5	Allow-Events	[28] 8.2.2	c2	c2	[28] 8.2.2	c3	c3
6	Authorization	[26] 20.7	c4	c4	[26] 20.7	c4	c4
7	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
8	Call-Info	[26] 20.9	o		[26] 20.9	o	
9	Contact	[26] 20.10	o		[26] 20.10	o	
10	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
11	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
12	Content-Language	[26] 20.13	o		[26] 20.13	o	
13	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
14	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
15	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
16	Date	[26] 20.17	c5	c5	[26] 20.17	m	m
17	From	[26] 20.20	m	m	[26] 20.20	m	m
18	Max-Forwards	[26] 20.22	o	o	[26] 20.22	n/a	n/a
19	MIME-Version	[26] 20.24	o		[26] 20.24	o	
20	Organization	[26] 20.25	o		[26] 20.25	o	
21	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
22	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
23	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a
24	Require	[26] 20.32	o	o	[26] 20.32	m	m
25	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
26	Supported	[26] 20.37	c8	c8	[26] 20.37	m	m
27	Timestamp	[26] 20.38	c9	c9	[26] 20.38	m	m
28	To	[26] 20.39	m	m	[26] 20.39	m	m
29	User-Agent	[26] 20.41	o		[26] 20.41	o	
30	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/12 THEN o ELSE n/a.						
c2:	IF A.4/20 THEN o ELSE n/a.						
c3:	IF A.4/20 THEN m ELSE n/a.						
c4:	IF A.4/7 THEN m ELSE n/a.						
c5:	IF A.4/11 THEN o ELSE n/a.						
c6:	IF A.4/15 THEN o ELSE n/a.						
c7:	IF A.4/15 THEN m ELSE n/a.						
c8:	IF A.4/16 THEN m ELSE o -- support of timer extension.						
c9:	IF A.4/6 THEN o ELSE n/a.						

Table A.151: Supported message bodies within the UPDATE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.5/23 – UPDATE response

Table A.152: Supported headers within the BYE response - all remaining status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
3	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
4	Content-Language	[26] 20.13	o		[26] 20.13	o	
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o		[26] 20.24	o	
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
12	To	[26] 20.39	m	m	[26] 20.39	m	m
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/11 THEN o ELSE n/a.						
c2:	IF A.4/6 THEN m ELSE n/a.						

Prerequisite A.5/23 – UPDATE response

Prerequisite: A.6/6 – 2xx

Table A.153: Supported headers within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m		[26] 20.5	m	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Organization	[26] 24.25	o		[26] 24.25	o	
4	Require	[26] 20.31	m	m	[26] 20.31	m	m
5	Server	[26] 20.35	o	o	[26] 20.35	o	o
6	Supported	[26] 20.37	m	m	[26] 20.37	m	m
7	User-Agent	[26] 20.41	o		[26] 20.41	o	
8	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/23 – UPDATE response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 – 3xx

Table A.154: Supported headers within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-Info	[26] 20.9	o		[26] 20.9	o	
2	Contact	[26] 20.10	o		[26] 20.10	o	
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Organization	[26] 20.25	o		[26] 20.25	o	
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/23 – UPDATE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.155: Supported headers within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-Info	[26] 20.9	o		[26] 20.9	o	
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Organization	[26] 20.25	o		[26] 20.25	o	
4	Require	[26] 20.32	m	m	[26] 20.32	m	m
5	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/23 – UPDATE response

Prerequisite: A.6/18 -- "405" Method Not Allowed

Table A.156: Supported headers within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m		[26] 20.5	m	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Organization	[26] 20.25	o		[26] 20.25	o	
5	Require	[26] 20.32	m	m	[26] 20.33	m	m
6	Server	[26] 20.35	o	o	[26] 20.37	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/23 – UPDATE response

Prerequisite: A.6/20 – 407

Table A.157: Supported headers within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-Info	[26] 20.9	o		[26] 20.9	o	
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Organization	[26] 20.25	o		[26] 20.25	o	
4	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
5	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/23 – UPDATE response

Prerequisite: A.6/25 -- "415" Unsupported Media Type

Table A.158: Supported headers within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow	[26] 20.5	o		[26] 20.5	o	
5	Call-Info	[26] 20.9	o		[26] 20.9	o	
6	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
7	Organization	[26] 20.25	o		[26] 20.25	o	
8	Require	[26] 20.32	m	m	[26] 20.32	m	m
9	Server	[26] 20.35	o	o	[26] 20.35	o	o
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m
11	User-Agent	[26] 20.41	o		[26] 20.41	o	
12	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/23 – UPDATE response

Prerequisite: A.6/27 – 420

Table A.159: Supported headers within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-Info	[26] 20.9	o		[26] 20.9	o	
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Organization	[26] 20.25	o		[26] 20.25	o	
4	Require	[26] 20.32	m	m	[26] 20.32	m	m
5	Server	[26] 20.35	o	o	[26] 20.35	o	o
6	Supported	[26] 20.37	m	m	[26] 20.37	m	m
7	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	

Prerequisite A.5/23 – UPDATE response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/35 – 3xx or 485 "Ambiguous"

Table A.160: Supported headers within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-Info	[26] 20.9	o		[26] 20.9	o	
2	Contact	[26] 20.10	o		[26] 20.10	o	
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Organization	[26] 20.25	o		[26] 20.25	o	
5	Require	[26] 20.32	m	m	[26] 20.33	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	

Table A.161: Supported message bodies within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.2 Proxy role

A.2.2.1 Introduction

This subclause contains the ICS proforma tables related to the proxy role. They need to be completed only for proxy implementations.

Prerequisite: A.2/2 -- proxy role

A.2.2.2 Major capabilities

Table A.162: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
	Capabilities within main protocol			
1	client behaviour for session requests?	[26] 16	m	m
2	server behaviour for session requests?	[26] 16	m	m
3	session release?	[26] 16	m	m
4	Stateless proxy behaviour?	[26] 16.11	o.1	
5	Stateful proxy behaviour?	[26] 16.2	o.1	
6	forking of initial requests	[26] 16.1	c1	n/a
7	support of TLS connections on the upstream side	[26] 16.7	o	n/a
8	support of TLS connections on the downstream side	[26] 16.7	o	n/a
9	insertion of date in requests and responses	[26] 20.17	o	o
10	suppression or modification of alerting information data	[26] 20.4	o	o
11	reading the contents of the Require header before proxying the request or response	[26] 20.32	o	o
12	adding or modifying the contents of the Require header before proxying the REGISTER request or response	[26] 20.32	o	m
13	adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER	[26] 20.32	o	o
14	the requirement to be able to insert itself in the subsequent transactions in a dialog	[26] 16.6	o	c2
15	the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing	[26] 16.7	c3	c3
16	reading the contents of the Supported header before proxying the response	[26] 20.37	o	o
17	reading the contents of the Unsupported header before proxying the 420 response to a REGISTER	[26] 20.40	o	m
18	reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER	[26] 20.40	o	o
19	the inclusion of the Error-Info header in 3xx - 6xx responses	[26] 20.18	o	o
	Extensions			
20	The SIP INFO method?	[25]	o	o
21	Reliability of provisional responses in SIP?	[27]	o	m
22	the REFER method?	[36]	o	o
23	Integration of resource management and SIP?	[30]	o	m
24	the SIP UPDATE method	[29]	c4	m
25	SIP extensions for caller identity and privacy?	[34]	o	m
26	SIP extensions for media authorization?	[31]	o	m
27	SIP specific event notification	[28]	o	o
28	the use of NOTIFY to establish a dialog	[28] 4.2	o	n/a
29	Path Extension Header for Establishing Service Route with SIP REGISTER	[35]	o	c5
30	extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks	[34]	o	m

31	a Privacy Mechanism for the Session Initiation Protocol (SIP)	[33]	o	m
c1:	IF A.162/5 THEN o ELSE n/a			
c2:	IF A.3/4 OR A.3/7 THEN m ELSE IF A.3/3 THEN o ELSE n/a - - S-CSCF or AS else I-CSCF			
c3:	IF (A.162/7 AND NOT A.162/8) OR (NOT A.162/7 AND A.162/8) THEN m ELSE IF A.162/14 THEN o ELSE n/a - - TLS interworking with non-TLS else proxy insertion			
c4:	IF A.162/23 THEN m ELSE o - - integration of resource management and SIP			
c5:	IF A.3/2 OR A.3/3 THEN m ELSE n/a. - - P-CSCF or I-CSCF.			
o.1:	It is mandatory to support at least one of these items.			

A.2.2.3 PDUs

Table A.163: Supported methods

Item	PDU	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	ACK request	[26] 13	m	m	[26] 13	m	m
2	BYE request	[26] 16	o	m	[26] 16	o	m
3	BYE response	[26] 16	o	m	[26] 16	o	m
4	CANCEL request	[26] 16.10	o	m	[26] 16.10	o	m
5	CANCEL response	[26] 16.10	o	m	[26] 16.10	o	m
6	INFO request	[25] 2	c2	c2	[25] 2	c2	c2
7	INFO response	[25] 2	c2	c2	[25] 2	c2	c2
8	INVITE request	[26] 16	m	m	[26] 16	m	m
9	INVITE response	[26] 16	m	m	[26] 16	m	m
10	NOTIFY request	[28] 8.1.2	c3	c3	[28] 8.1.2	c3	c3
11	NOTIFY response	[28] 8.1.2	c3	c3	[28] 8.1.2	c3	c3
12	OPTIONS request	[26] 16	m	m	[26] 16	m	m
13	OPTIONS response	[26] 16	m	m	[26] 16	m	m
14	PRACK request	[27] 6	m	m	[27] 6	m	m
15	PRACK response	[27] 6	m	m	[27] 6	m	m
16	REFER request	[36] 3	c1	c1	[36] 3	c1	c1
17	REFER response	[36] 3	c1	c1	[36] 3	c1	c1
18	REGISTER request	[26] 16	m	m	[26] 16	m	m
19	REGISTER response	[26] 16	m	m	[26] 16	m	m
20	SUBSCRIBE request	[28] 8.1.1	c3	c3	[28] 8.1.1	c3	c3
21	SUBSCRIBE response	[28] 8.1.1	c3	c3	[28] 8.1.1	c3	c3
22	UPDATE request	[30] 7	c4	c4	[30] 7	c4	c4
23	UPDATE response	[30] 7	c4	c4	[30] 7	c4	c4
c1:	IF A.162/22 THEN m ELSE n/a.						
c2:	IF A.162/20 THEN m ELSE n/a.						
c3	IF A.162/27 THEN m ELSE n/a.						
c4	IF A.162/24 THEN m ELSE n/a - - the SIP UPDATE method.						

A.2.2.4 PDU parameters

A.2.2.4.1 Status-codes

Table A.164: Supported-status codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	100 (Trying)	[26] 21.1.1	c1	c1	[26] 21.1.1	c2	c2
2	180 (Ringing)	[26] 21.1.2	c3	c3	[26] 21.1.2	c3	c3
3	181 (Call Is Being Forwarded)	[26] 21.1.3	c3	c3	[26] 21.1.3	c3	c3
4	182 (Queued)	[26] 21.1.4	c3	c3	[26] 21.1.4	c3	c3
5	183 (Session Progress)	[26] 21.1.5	c3	c3	[26] 21.1.5	c3	c3
6	200 (OK)	[26] 21.2.1			[26] 21.2.1		
7	202 (Accepted)	[28] 8.3.1	c4	c4	[28] 8.3.1	c4	c4
8	300 (Multiple Choices)	[26] 21.3.1			[26] 21.3.1		
9	301 (Moved Permanently)	[26] 21.3.2			[26] 21.3.2		
10	302 (Moved Temporarily)	[26] 21.3.3			[26] 21.3.3		
11	305 (Use Proxy)	[26] 21.3.4			[26] 21.3.4		
12	380 (Alternative Service)	[26] 21.3.5			[26] 21.3.5		
13	400 (Bad Request)	[26] 21.4.1			[26] 21.4.1		
14	401 (Unauthorized)	[26] 21.4.2			[26] 21.4.2		
15	402 (Payment Required)	[26] 21.4.3			[26] 21.4.3		
16	403 (Forbidden)	[26] 21.4.4			[26] 21.4.4		
17	404 (Not Found)	[26] 21.4.5			[26] 21.4.5		
18	405 (Method Not Allowed)	[26] 21.4.6			[26] 21.4.6		
19	406 (Not Acceptable)	[26] 21.4.7			[26] 21.4.7		
20	407 (Proxy Authentication Required)	[26] 21.4.8			[26] 21.4.8		
21	408 (Request Timeout)	[26] 21.4.9			[26] 21.4.9		
22	410 (Gone)	[26] 21.4.10			[26] 21.4.10		
23	413 (Request Entity Too Large)	[26] 21.4.11			[26] 21.4.11		
24	414 (Request-URI Too Large)	[26] 21.4.12			[26] 21.4.12		
25	415 (Unsupported Media Type)	[26] 21.4.13			[26] 21.4.13		
26	416 (Unsupported URI Scheme)	[26] 21.4.14			[26] 21.4.14		
27	420 (Bad Extension)	[26] 21.4.15			[26] 21.4.15		
28	421 (Extension Required)	[26] 21.4.16			[26] 21.4.16		
29	423 (Registration Too Brief)	[26] 21.4.17	c5	c5	[26] 21.4.17	c6	c6

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
30	480 (Temporarily not available)	[26] 21.4.18			[26] 21.4.18		
31	481 (Call Leg/Transaction Does Not Exist)	[26] 21.4.19			[26] 21.4.19		
32	482 (Loop Detected)	[26] 21.4.20			[26] 21.4.20		
33	483 (Too Many Hops)	[26] 21.4.21			[26] 21.4.21		
34	484 (Address Incomplete)	[26] 21.4.22			[26] 21.4.22		
35	485 (Ambiguous)	[26] 21.4.23			[26] 21.4.23		
36	486 (Busy Here)	[26] 21.4.24			[26] 21.4.24		
37	487 (Request Cancelled)	[26] 21.4.25			[26] 21.4.25		
38	488 (Not Acceptable Here)	[26] 21.4.26			[26] 21.4.26		
39	489 (Bad Events)	[28] 8.3.2	c4	c4	[28] 8.3.2	c4	c4
40	491 (Request Pending)	[26] 21.4.27			[26] 21.4.27		
41	493 (Undecipherable)	[26] 21.4.28			[26] 21.4.28		
42	500 (Internal Server Error)	[26] 21.5.1			[26] 21.5.1		
43	501 (Not Implemented)	[26] 21.5.2			[26] 21.5.2		
44	502 (Bad Gateway)	[26] 21.5.3			[26] 21.5.3		
45	503 (Service Unavailable)	[26] 21.5.4			[26] 21.5.4		
46	504 (Server Time-out)	[26] 21.5.5			[26] 21.5.5		
47	505 (SIP Version not supported)	[26] 21.5.6			[26] 21.5.6		
48	513 (Message Too Large)	[26] 21.5.7			[26] 21.5.7		
49	580 (Precondition Failure)						
50	600 (Busy Everywhere)	[26] 21.6.1			[26] 21.6.1		
51	603 (Decline)	[26] 21.6.2			[26] 21.6.2		
52	604 (Does Not Exist Anywhere)	[26] 21.6.3			[26] 21.6.3		
53	606 (Not Acceptable)	[26] 21.6.4			[26] 21.6.4		

c1: IF A.162/15 THEN m ELSE n/a.
c2: IF A.162/15 THEN m ELSE i.
c3: IF A.163/9 THEN m ELSE n/a.
c4: IF A.162/27 THEN m ELSE n/a.
c5: IF A.163/19 OR A.163/21 THEN m ELSE n/a - - REGISTER response or SUBSCRIBE response.
c6: IF A.163/19 OR A.163/21 THEN i ELSE n/a - - REGISTER response or SUBSCRIBE response.

A.2.2.4.2 ACK method

Prerequisite A.163/1 – ACK request

Table A.165: Supported headers within the ACK request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	o		[26] 20.5	o	
2	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	c1	c1
3	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
4	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
5	Contact	[26] 20.10	o		[26] 20.10	o	
6	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
7	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
8	Content-Language	[26] 20.13	o		[26] 20.13	o	
9	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
10	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
11	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
12	Date	[26] 20.17	m	m	[26] 20.17	c2	c2
13	From	[26] 20.20	m	m	[26] 20.20	m	m
14	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
15	MIME-Version	[26] 20.24	o		[26] 20.24	o	
16	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
17	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
18	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
19	Route	[26] 20.34	m	m	[26] 20.34	m	m
20	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
21	To	[26] 20.39	m	m	[26] 20.39	m	m
22	User-Agent	[26] 20.41	o		[26] 20.41	o	
23	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1: IF A.4/20 THEN m ELSE i. c2: IF A.162/9 THEN m ELSE i. c5: IF A.162/11 OR A.162/13 THEN m ELSE i.							
NOTE: c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.							

Editor's note: Is the following table a suitable way of showing the contents of message bodies.

Prerequisite A.163/1 – ACK request

Table A.166: Supported message bodies within the ACK request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.2.4.3 BYE method

Prerequisite A.163/2 – BYE request

Table A.167: Supported headers within the BYE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	c1	c1
5	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
8	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
9	Content-Language	[26] 20.13	o		[26] 20.13	o	
10	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
11	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
12	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
13	Date	[26] 20.17	m	m	[26] 20.17	c2	c2
14	From	[26] 20.20	m	m	[26] 20.20	m	m
15	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
16	MIME-Version	[26] 20.24	o		[26] 20.24	o	
17	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
18	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
19	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
20	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
21	Route	[26] 20.34	m	m	[26] 20.34	m	m
22	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
23	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
24	To	[26] 20.39	m	m	[26] 20.39	m	m
25	User-Agent	[26] 20.41	o		[26] 20.41	o	
26	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1: IF A.4/20 THEN m ELSE i. c2: IF A.162/9 THEN m ELSE i. c5: IF A.162/11 OR A.162/13 THEN m ELSE i. c6: IF A.162/16 THEN m ELSE i. c7: IF A.162/14 THEN o ELSE i.							
NOTE: c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.							

Prerequisite A.163/2 – BYE request

Table A.168: Supported message bodies within the BYE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/1 - - 100 Trying

Table A.169: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
5	From	[26] 20.20	m	m	[26] 20.20	m	m
6	To	[26] 20.39	m	m	[26] 20.39	m	m
c1:	IF A.162/9 THEN m ELSE i.						

Prerequisite A.163/3 – BYE response

Table A.170: Supported headers within the BYE response - all remaining status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
3	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
4	Content-Language	[26] 20.13	o		[26] 20.13	o	
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o		[26] 20.24	o	
11	Timestamp	[26] 20.38	o		[26] 20.38	o	
12	To	[26] 20.39	m	m	[26] 20.39	m	m
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.162/9 THEN m ELSE i.						

Prerequisite A.163/3 – BYE response

Prerequisite: A.164/6 – 2xx

Table A.171: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Authentication-Info	[26] 20.6	o		p	o	
2	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c3:	IF A.162/15 THEN o ELSE i.						

Prerequisite A.163/3 - BYE response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/35 - 3xx or 485 "Ambiguous"

Table A.172: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Contact	[26] 20.10	o		[26] 20.10	o	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/3 – BYE response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 - - 401

Table A.173: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
8	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.174: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
3	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/18 -- "405" Method Not Allowed

Table A.175: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m		[26] 20.5	m	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/3 – BYE response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 - - 407

Table A.176: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/3 – BYE response

Prerequisite: A.164/25 -- "415" Unsupported Media Type

Table A.177: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
6	Server	[26] 20.35	m	m	[26] 20.35	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/27 - - 420

Table A.178: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
3	Server	[26] 20.35	m	m	[26] 20.35	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
5	Unsupported	[26] 20.40	m	m	[26] 20.40	c3	c3
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2: IF A.162/11 OR A.162/13 THEN m ELSE i. c3: IF A.162/18 THEN m ELSE i.							

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/34 - - 484

Table A.179: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
3	Server	[26] 20.35	m	m	[26] 20.35	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
5	User-Agent	[26] 20.41	o		[26] 20.41	o	
6	Warning	[26] 20.43	o		[26] 20.43	o	
c2: IF A.162/11 OR A.162/13 THEN m ELSE i.							

Prerequisite A.163/3 - - BYE response

Table A.180: Supported message bodies within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.2.4.4 CANCEL method

Prerequisite A.163/4 – CANCEL request

Table A.181: Supported headers within the CANCEL request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	c1	c1
5	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Content-Language	[26] 20.13	o		[26] 20.13	o	
8	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
9	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
10	Date	[26] 20.17	m	m	[26] 20.17	c2	c2
11	From	[26] 20.20	m	m	[26] 20.20	m	m
12	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
13	MIME-Version	[26] 20.24	o		[26] 20.24	o	
14	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
15	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
16	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
17	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
18	Route	[26] 20.34	m	m	[26] 20.34	m	m
19	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
20	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
21	To	[26] 20.39	m	m	[26] 20.39	m	m
22	User-Agent	[26] 20.41	o		[26] 20.41	o	
23	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/20 THEN m ELSE i.						
c2:	IF A.162/9 THEN m ELSE i.						
c5:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c6:	IF A.162/16 THEN m ELSE i.						
c7:	IF A.162/14 THEN o ELSE i.						
NOTE:	c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.						

Prerequisite A.163/4 – CANCEL request

Table A.182: Supported message bodies within the CANCEL request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.163/5 - - CANCEL response

Table A.183: Supported headers within the CANCEL response - all status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
5	From	[26] 20.20	m	m	[26] 20.20	m	m
6	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
7	To	[26] 20.39	m	m	[26] 20.39	m	m
8	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.162/9 THEN m ELSE i.						

Prerequisite A.163/5 - - CANCEL response

Prerequisite: A.164/6 - - 200

Table A.184: Supported headers within the CANCEL response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Content-Language	[26] 20.13	o		[26] 20.13	o	
2	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
5	User-Agent	[26] 20.41	o		[26] 20.41	o	
6	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c3:	IF A.162/15 THEN o ELSE i.						

Prerequisite A.163/5 - - CANCEL response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 - - 401

Table A.185: Supported headers within the CANCEL response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Content-Language	[26] 20.13	o		[26] 20.13	o	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
4	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
8	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/5 - - CANCEL response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - 404, 413, 480, 500, 503, 600, 603

Table A.186: Supported headers within the CANCEL response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Content-Language	[26] 20.13	o		[26] 20.13	o	
2	Error-Info	[26] 2418	m	m	[26] 20.18	i	i
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/5 - - CANCEL response

Prerequisite: A.164/27 - - 420

Table A.187: Supported headers within the CANCEL response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Content-Language	[26] 20.13	o		[26] 20.13	o	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
5	Unsupported	[26] 20.40	m	m	[26] 20.40	c3	c3
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c3:	IF A.162/18 THEN m ELSE i.						

Prerequisite A.163/5 - - CANCEL response

Prerequisite: A.164/34 - - 484

Table A.188: Supported headers within the CANCEL response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Content-Language	[26] 20.13	o		[26] 20.13	o	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
5	User-Agent	[26] 20.41	o		[26] 20.41	o	
6	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/5 - - CANCEL response

Table A.189: Supported message bodies within the CANCEL response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.2.4.5 COMET method

Void

A.2.2.4.6 INFO method

Prerequisite A.163/6 - - INFO request

Table A.190: Supported headers within the INFO request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	c1	c1
5	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
6	Call-ID	[26] 20.8	m		[26] 20.8	m	
7	Contact	[26] 20.10	o		[26] 20.10	o	
8	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
9	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
10	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
11	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
12	Date	[26] 20.17	m	m	[26] 20.17	c2	c2
13	Expires	[26] 20.19	o		[26] 20.19	o	
14	From	[26] 20.20	m	m	[26] 20.20	m	m
15	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
16	Organization	[26] 20.25	o		[26] 20.25	o	
17	Priority	[26] 20.26	m	m	[26] 20.26	i	i
18	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
19	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
20	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
21	Require	[26] 20.32	m	m	[26] 20.32	c4	c5
22	Route	[26] 20.34	m	m	[26] 20.34	m	m
23	Subject	[26] 24.38	o		[26] 24.38	o	
24	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
25	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
26	To	[26] 20.39	m	m	[26] 20.39	m	m
27	User-Agent	[26] 20.41	o		[26] 20.41	o	
28	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/20 THEN m ELSE i.						
c2:	IF A.162/9 THEN m ELSE i.						
c5:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c6:	IF A.162/16 THEN m ELSE i.						
c7:	IF A.162/14 THEN o ELSE i.						
NOTE:	c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.						

Prerequisite A.163/6 - - INFO request

Table A.191: Supported message bodies within the INFO request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.163/7 – INFO response

Prerequisite: A.164/1 – 100 Trying

Table A.192: Supported headers within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
5	From	[26] 20.20	m	m	[26] 20.20	m	m
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.162/9 THEN m ELSE i.						

Prerequisite A.163/7 – INFO response

Table A.193: Supported headers within the INFO response - all remaining status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
3	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
4	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
5	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
6	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
7	From	[26] 20.20	m	m	[26] 20.20	m	m
8	Organization	[26] 20.25	o		[26] 20.25	o	
9	Timestamp	[26] 20.38	i	i	[26] 20.38	i	i
10	To	[26] 20.39	m	m	[26] 20.39	m	m
11	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.162/9 THEN m ELSE i.						

Prerequisite A.163/7 – INFO response

Prerequisite: A.164/6 - - 2xx

Table A.194: Supported headers within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m		[26] 20.5	m	
2	Expires	[26] 20.19	o		[26] 20.19	o	
3	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
4	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3
5	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
6	Server	[26] 20.35	m	m	[26] 20.35	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
10	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c3:	IF A.162/15 THEN o ELSE i.						

Prerequisite A.163/7 - - INFO response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 - - 3xx

Table A.195: Supported headers within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Expires	[26] 20.19	o		[26] 20.19	o	
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
8	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/7 - - INFO response

Prerequisite: A.164/14 - - 401

Table A.196: Supported headers within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 2418	m	m	[26] 20.18	i	i
2	Expires	[26] 20.19	o		[26] 20.19	o	
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
8	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/7 - - INFO response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.197: Supported headers within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Expires	[26] 20.19	o		[26] 20.19	o	
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
5	Server	[26] 20.35	m	m	[26] 20.35	i	i
6	Supported	[26] 20.37	m	m	[26] 20.37	i	i
7	User-Agent	[26] 20.41	o		[26] 20.41	o	
8	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/7 - - INFO response

Prerequisite: A.164/18 -- "405" Method Not Allowed

Table A.198: Supported headers within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m		[26] 20.5	m	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Expires	[26] 20.19	o		[26] 20.19	o	
4	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
5	Server	[26] 20.35	m	m	[26] 20.35	i	i
6	Supported	[26] 20.37	m	m	[26] 20.37	i	i
7	User-Agent	[26] 20.41	o		[26] 20.41	o	
8	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/7 – INFO response

Prerequisite: A.164/25 -- "415" Unsupported Media Type @@@ combine

Table A.199: Supported headers within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Expires	[26] 20.19	o		[26] 20.19	o	
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/7 - - INFO response

Prerequisite: A.164/27 - - 420

Table A.200: Supported headers within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Expires	[26] 20.19	o		[26] 20.19	o	
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	Unsupported	[26] 20.40	m	m	[26] 20.40	c3	c3
7	User-Agent	[26] 20.41	o		[26] 20.41	o	
8	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c3:	IF A.162/18 THEN m ELSE i.						

Prerequisite A.163/7 - - INFO response

Prerequisite: A.164/34 - - 484

Table A.201: Supported headers within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Expires	[26] 20.19	o		[26] 20.19	o	
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/7 - - INFO response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/35 - - 3xx or 485 "Ambiguous" @@@ combine

Table A.202: Supported headers within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Expires	[26] 20.19	o		[26] 20.19	o	
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/7 - - INFO response

Table A.203: Supported message bodies within the INFO response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.2.4.7 INVITE method

Prerequisite A.163/8 – INVITE request

Table A.204: Supported headers within the INVITE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	c1	c1
5	Alert-Info	[26] 20.4	c2	c2	[26] 20.4	c3	c3
6	Allow	[26] 20.5, [26] 13	o		[26] 20.5, [26] 13	o	
7	Anonymity	[34] 5.2	o		[34] 5.2		
8	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
9	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
10	Call-Info	[26] 20.9	o		[26] 20.9	o	
11	Contact	[26] 20.10	m		[26] 20.10	m	
12	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
13	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
14	Content-Language	[26] 20.13	o		[26] 20.13	o	
15	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
16	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
17	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
18	Date	[26] 20.17	m	m	[26] 20.17	c4	c4
19	Expires	[26] 20.19	o		[26] 20.19	o	
20	From	[26] 20.20	m	m	[26] 20.20	m	m
21	In-Reply-To	[26] 24.21	m	m	[26] 24.21	i	i
22	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
23	MIME-Version	[26] 20.24	o		[26] 20.24	o	
24	Organization	[26] 20.25	o		[26] 20.25	o	
25	P-Media-Authorization	[31] 6.1	c9	c10	[31] 6.1	n/a	n/a
26	Priority	[26] 20.26	m	m	[26] 20.26	i	i
27	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
28	Proxy-Require	[26] 20.29, [34] 4	m	m	[26] 20.29, [34] 4	m	m
29	Record-Route	[26] 20.30	m	m	[26] 20.30	c11	c11
30	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
31	Reply-To	[26] 20.31	m	m	[26] 20.31	i	i
32	Require	[26] 20.32	m	m	[26] 20.32	c7	c7
33	Route	[26] 20.34	m	m	[26] 20.34	m	m
34	Subject	[26] 24.38	o		[26] 24.38	o	
35	Supported	[26] 20.37	m	m	[26] 20.37	c8	c8
36	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
37	To	[26] 20.39	m	m	[26] 20.39	m	m
38	User-Agent	[26] 20.41	o		[26] 20.41	o	
39	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/20 THEN m ELSE i.						
c2:	IF A.162/10 THEN n/a ELSE m.						
c3:	IF A.162/10 THEN m ELSE i.						
c4:	IF A.162/9 THEN m ELSE i.						
c7:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c8:	IF A.162/16 THEN m ELSE i.						
c9:	IF A.162/26 THEN m ELSE n/a.						
c10:	IF A.3/2 THEN m ELSE n/a.						
c11:	IF A.162/14 THEN m ELSE i.						
NOTE:	c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.						

Prerequisite A.163/8 – INVITE request

Table A.205: Supported message bodies within the INVITE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/1 - - 100 Trying

Table A.206: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	c1	c1	[26] 20.17	c2	c2
5	From	[26] 20.20	m	m	[26] 20.20	m	m
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF (A.162/9 AND A.162/5) OR A.162/4 THEN m ELSE n/a - - Stateful proxies that insert date, or stateless proxies.						
c2:	IF A.162/4 THEN i ELSE m - - Stateless proxy passes on.						

Prerequisite A.163/9 – INVITE response

Table A.207: Supported headers within the INVITE response - all remaining status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Disposition	[26] 20.11, [30] 8.3	o		[26] 20.11, [30] 8.3	o	
3	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
4	Content-Language	[26] 20.13	o		[26] 20.13	o	
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o		[26] 20.24	o	
11	Organization	[26] 20.25	o		[26] 20.25	o	
12	Timestamp	[26] 20.38	i	i	[26] 20.38	i	i
13	To	[26] 20.39	m	m	[26] 20.39	m	m
14	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.162/9 THEN m ELSE i.						

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/2 OR A.164/3 OR A.164/4 OR A.164/5 – 1xx

Table A.208: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Anonymity	[34] 5.2	o		[34] 5.2		
3	Call-Info	[26] 20.9	o		[26] 20.9	o	
4	Contact	[26] 20.10	o		[26] 20.10	o/m	
5	Expires	[26] 20.19	o		[26] 20.19	o	
6	P-Media-Authorization	[31] 6.1	c9	c10	[31] 6.1	n/a	n/a
7	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
8	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
9	Rseq	[27] 7.1	m	m	[27] 7.1	i	i
10	Server	[26] 20.35	m	m	[26] 20.35	i	i
11	Supported	[26] 20.37	m	m	[26] 20.37	i	i
12	User-Agent	[26] 20.41	o		[26] 20.41	o	
13	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c9:	IF A.162/26 THEN m ELSE n/a.						
c10:	IF A.3/2 THEN m ELSE n/a.						

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/6 – 2xx

Table A.209: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Allow	[26] 20.5	o		[26] 20.5	o	
3	Anonymity	[34] 5.2	o		[34] 5.2		
4	Authentication-Info	[26] 20.6	o		[26] 20.6	o	
5	Call-Info	[26] 20.9	o		[26] 20.9	o	
6	Contact	[26] 20.10	m		[26] 20.10	m	
7	Expires	[26] 20.19	o		[26] 20.19	o	
8	P-Media-Authorization	[31] 6.1	c9	c10	[31] 6.1	n/a	n/a
9	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3
10	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
11	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
12	Server	[26] 20.35	m	m	[26] 20.35	i	i
13	Supported	[26] 20.37	m	m	[26] 20.37	i	i
14	User-Agent	[26] 20.41	o		[26] 20.41	o	
15	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c3:	IF A.162/14 THEN m ELSE i.						
c9:	IF A.162/26 THEN m ELSE n/a.						
c10:	IF A.3/2 THEN m ELSE n/a.						

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/35 - - 3xx or 485 "Ambiguous"

Table A.210: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Anonymity	[34] 5.2	o		[34] 5.2		
3	Call-Info	[26] 20.9	o		[26] 20.9	o	
4	Contact	[26] 20.10	o		[26] 20.10	o/m	
5	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
6	Expires	[26] 20.19	o		[26] 20.19	o	
7	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
8	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
9	Server	[26] 20.35	m	m	[26] 20.35	i	i
10	Supported	[26] 20.37	m	m	[26] 20.37	i	i
11	User-Agent	[26] 20.41	o		[26] 20.41	o	
12	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/14 - - 401

Table A.211: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Anonymity	[34] 5.2	o		[34] 5.2		
3	Call-Info	[26] 20.9	o		[26] 20.9	o	
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Expires	[26] 20.19	o		[26] 20.19	o	
6	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
7	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
8	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
9	Server	[26] 20.35	m	m	[26] 20.35	i	i
10	Supported	[26] 20.37	m	m	[26] 20.37	i	i
11	Timestamp	[26] 20.38	i	i	[26] 20.38	i	i
12	To	[26] 20.39	m	m	[26] 20.39	m	m
13	User-Agent	[26] 20.41	o		[26] 20.41	o	
14	Warning	[26] 20.43	o		[26] 20.43	o	
15	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.212: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Anonymity	[34] 5.2	o		[34] 5.2		
3	Call-Info	[26] 20.9	o		[26] 20.9	o	
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Expires	[26] 20.19	o		[26] 20.19	o	
6	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
7	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
8	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
9	Server	[26] 20.35	m	m	[26] 20.35	i	i
10	Supported	[26] 20.37	m	m	[26] 20.37	i	i
11	User-Agent	[26] 20.41	o		[26] 20.41	o	
12	Via	[26] 20.42	m	m	[26] 20.42	m	m
13	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/18 -- "405" Method Not Allowed

Table A.213: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Allow	[26] 20.5	m		[26] 20.5	m/o	
3	Anonymity	[34] 5.2	o		[34] 5.2	o	
4	Call-Info	[26] 20.9	o		[26] 20.9	o	
5	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
6	Expires	[26] 20.19	o		[26] 20.19	o	
7	From	[26] 20.20	m	m	[26] 20.20	m	m
8	MIME-Version	[26] 20.24	o		[26] 20.24	o	
9	Organization	[26] 20.25	o		[26] 20.25	o	
10	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
11	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
12	Server	[26] 20.35	m	m	[26] 20.35	i	i
13	Supported	[26] 20.37	m	m	[26] 20.37	i	i
14	User-Agent	[26] 20.41	o		[26] 20.41	o	
15	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/20 - - 407

Table A.214: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Anonymity	[34] 5.2	o		[34] 5.2		
3	Call-Info	[26] 20.9	o		[26] 20.9	o	
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Expires	[26] 20.19	o		[26] 20.19	o	
6	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
7	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
8	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
9	Server	[26] 20.35	m	m	[26] 20.35	i	i
10	Supported	[26] 20.37	m	m	[26] 20.37	i	i
11	User-Agent	[26] 20.41	o		[26] 20.41	o	
12	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/9 – INVITE response

Prerequisite: A.164/25 -- "415" Unsupported Media Type

Table A.215: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Anonymity	[34] 5.2	o		[34] 5.2		
5	Call-Info	[26] 20.9	o		[26] 20.9	o	
6	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
7	Expires	[26] 20.19	o		[26] 20.19	o	
8	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
9	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
10	Server	[26] 20.35	m	m	[26] 20.35	i	i
11	Supported	[26] 20.37	m	m	[26] 20.37	i	i
12	User-Agent	[26] 20.41	o		[26] 20.41	o	
13	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/27 - - 420

Table A.216: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Anonymity	[34] 5.2	o		[34] 5.2		
3	Call-Info	[26] 20.9	o		[26] 20.9	o	
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Expires	[26] 20.19	o		[26] 20.19	o	
6	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
7	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
8	Server	[26] 20.35	m	m	[26] 20.35	i	i
9	Supported	[26] 20.37	m	m	[26] 20.37	i	i
10	Unsupported	[26] 20.40	m	m	[26] 20.40	c3	c3
11	User-Agent	[26] 20.41	o		[26] 20.41	o	
12	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c3:	IF A.162/18 THEN m ELSE i.						

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/34 - - 484

Table A.217: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Anonymity	[34] 5.2	o		[34] 5.2		
3	Call-Info	[26] 20.9	o		[26] 20.9	o	
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Expires	[26] 20.19	o		[26] 20.19	o	
6	Remote-Party-ID	[34] 5.1	o		[34] 5.1	o	
7	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
8	Server	[26] 20.35	m	m	[26] 20.35	i	i
9	Supported	[26] 20.37	m	m	[26] 20.37	i	i
10	User-Agent	[26] 20.41	o		[26] 20.41	o	
11	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/9 - - INVITE response

Table A.218: Supported message bodies within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.2.4.8 NOTIFY method

Prerequisite A.163/10 - - NOTIFY request

Table A.219: Supported headers within the NOTIFY request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	c1	c1
5	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
8	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
9	Content-Language	[26] 20.13	o		[26] 20.13	o	
10	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
11	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
12	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
13	Date	[26] 20.17	m	m	[26] 20.17	c2	c2
14	Event	[28] 8.2.1	m	m	[28] 8.2.1	m	m
15	From	[26] 20.20	m	m	[26] 20.20	m	m
16	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
17	MIME-Version	[26] 20.24	o		[26] 20.24	o	
18	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
19	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
20	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
21	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
22	Route	[26] 20.34	m	m	[26] 20.34	m	m
23	Subscription-State	[28] 8.2.3	m	m	[28] 8.2.3	i	i
24	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
25	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
26	To	[26] 24.39	m	m	[26] 24.39	m	m
27	User-Agent	[26] 20.41	o		[26] 20.41	o	
28	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/20 THEN m ELSE i.						
c2:	IF A.162/9 THEN m ELSE i.						
c5:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c6:	IF A.162/16 THEN m ELSE i.						
c7:	IF A.162/14 THEN (IF A.162/22 OR A.162/27 THEN m ELSE o) ELSE i.						
NOTE:	c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.						

Prerequisite A.163/10 - - NOTIFY request

Table A.220: Supported message bodies within the NOTIFY request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	sipfrag	[37] 2	m	m	[37] 2	i	i

Prerequisite A.163/11 - - NOTIFY response

Table A.221: Supported headers within the NOTIFY response - all status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
3	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
4	Content-Language	[26] 20.13	o		[26] 20.13	o	
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o		[26] 20.24	o	
11	Timestamp	[26] 20.38	o		[26] 20.38	o	
12	To	[26] 20.39	m	m	[26] 20.39	m	m
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.162/9 THEN m ELSE i.						

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/6 AND A.164/7 - - 2xx

Table A.222: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Authentication-Info	[26] 20.6	o		[26] 20.6	o	
2	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c3:	IF A.162/15 THEN m ELSE i.						

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/35 - - 3xx or 485 "Ambiguous"

Table A.223: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Contact	[26] 20.10	o		[26] 20.10	o	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/14 - - 401

Table A.224: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
8	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.225: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
3	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/18 -- "405" Method Not Allowed

Table A.226: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m		[26] 20.5	m	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/20 - - 407

Table A.227: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/25 -- "415" Unsupported Media Type

Table A.228: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
6	Server	[26] 20.35	m	m	[26] 20.35	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/27 - - 420

Table A.229: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
3	Server	[26] 20.35	m	m	[26] 20.35	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
5	Unsupported	[26] 20.40	m	m	[26] 20.40	c3	c3
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c3:	IF A.162/18 THEN m ELSE i.						

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/34 - - 484

Table A.230: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
3	Server	[26] 20.35	m	m	[26] 20.35	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
5	User-Agent	[26] 20.41	o		[26] 20.41	o	
6	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/39 - - 489

Table A.231: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	c1	c1
2	Authentication-Info	[26] 20.6	o		[26] 20.6	o	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Require	[26] 20.32	m	m	[26] 20.32	c3	c3
5	Server	[26] 20.35	m	m	[26] 20.35	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c1:	IF A.4/20 THEN m ELSE i.						
c3:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
NOTE:	c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.						

Prerequisite A.163/11 - - NOTIFY response

Table A.232: Supported message bodies within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.2.4.9 OPTIONS method

Prerequisite A.163/12 – OPTIONS request

Table A.233: Supported headers within the OPTIONS request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	c1	c1
5	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Call-Info	[26] 20.9	o		[26] 20.9	o	
8	Contact	[26] 20.10	m		[26] 20.10	m	
9	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
10	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
11	Content-Language	[26] 20.13	o		[26] 20.13	o	
12	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
13	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
14	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
15	Date	[26] 20.17	m	m	[26] 20.17	c2	c2
16	From	[26] 20.20	m	m	[26] 20.20	m	m
17	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
18	MIME-Version	[26] 20.24	o		[26] 20.24	o	
19	Organization	[26] 20.25	o		[26] 20.25	o	
20	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
21	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
22	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
23	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
24	Route	[26] 20.34	m	m	[26] 20.34	m	m
25	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
26	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
27	To	[26] 20.39	m	m	[26] 20.39	m	m
28	User-Agent	[26] 20.41	o		[26] 20.41	o	
29	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1: IF A.4/20 THEN m ELSE i. c2: IF A.162/9 THEN m ELSE i. c5: IF A.162/11 OR A.162/13 THEN m ELSE i. c6: IF A.162/16 THEN m ELSE i. c7: IF A.162/14 THEN o ELSE i.							
NOTE: c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.							

Prerequisite A.163/12 – OPTIONS request

Table A.234: Supported message bodies within the OPTIONS request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.163/13 – OPTIONS response

Prerequisite: A.164/1 – 100 Trying

Table A.235: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
5	From	[26] 20.20	m	m	[26] 20.20	m	m
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.162/9 THEN m ELSE i.						

Prerequisite A.163/13 – OPTIONS response

Table A.236: Supported headers within the OPTIONS response - all remaining status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
3	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
4	Content-Language	[26] 20.13	o		[26] 20.13	o	
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o		[26] 20.24	o	
11	Organization	[26] 20.25	o		[26] 20.25	o	
12	Timestamp	[26] 20.38	i	i	[26] 20.38	i	i
13	To	[26] 20.39	m	m	[26] 20.39	m	m
14	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.162/9 THEN m ELSE i.						

Prerequisite A.163/13 – OPTIONS response

Prerequisite: A.164/6 – 2xx

Table A.237: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Allow	[26] 20.5	o		[26] 20.5	o/m	
3	Authentication-Info	[26] 20.6	o		[26] 20.6	o	
4	Call-Info	[26] 20.9	o		[26] 20.9	o	
5	Contact	[26] 20.10	o		[26] 20.10	o	
6	From	[26] 20.20	m	m	[26] 20.20	m	m
7	MIME-Version	[26] 20.24	o		[26] 20.24	o	
8	Organization	[26] 20.25	o		[26] 20.25	o	
9	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3
10	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
11	Server	[26] 20.35	m	m	[26] 20.35	i	i
12	Supported	[26] 20.37	m	m	[26] 20.37	i	i
13	User-Agent	[26] 20.41	o		[26] 20.41	o	
14	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c3:	IF A.162/15 THEN o ELSE i.						

Prerequisite A.163/13 – OPTIONS response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/35 - - 3xx or 485 "Ambiguous"

Table A.238: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Contact	[26] 20.10	o		[26] 20.10	o	
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
6	Server	[26] 20.35	m	m	[26] 20.35	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/13 – OPTIONS response

Prerequisite: A.164/14 – 401

Table A.239: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
5	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
6	Server	[26] 20.35	m	m	[26] 20.35	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
10	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/13 – OPTIONS response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.240: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
5	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
6	Server	[26] 20.35	m	m	[26] 20.35	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/13 – OPTIONS response

Prerequisite: A.164/18 -- "405" Method Not Allowed

Table A.241: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Allow	[26] 20.5	m	m	[26] 20.5	m	m
3	Call-Info	[26] 20.9	o		[26] 20.9	o	
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
6	Server	[26] 20.35	m	m	[26] 20.35	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/13 – OPTIONS response

Prerequisite: A.164/20 – 407

Table A.242: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
5	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
6	Server	[26] 20.35	m	m	[26] 20.35	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/13 – OPTIONS response

Prerequisite: A.164/25 -- "415" Unsupported Media Type

Table A.243: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Call-Info	[26] 20.9	o		[26] 20.9	o	
5	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
6	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
7	Server	[26] 20.35	m	m	[26] 20.35	i	i
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/13 – OPTIONS response

Prerequisite: A.164/27 – 420

Table A.244: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
5	Server	[26] 20.35	m	m	[26] 20.35	i	i
6	Supported	[26] 20.37	m	m	[26] 20.37	i	i
7	Unsupported	[26] 20.40	m	m	[26] 20.40	c3	c3
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c3:	IF A.162/18 THEN m ELSE i.						

Prerequisite A.163/13 – OPTIONS response

Prerequisite: A.164/34 – 484

Table A.245: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Contact	[26] 20.10	o		[26] 20.10	o	
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
6	Server	[26] 20.35	m	m	[26] 20.35	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/13 – OPTIONS response

Table A.246: Supported message bodies within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.2.4.10 PRACK method

Prerequisite A.163/14 – PRACK request

Table A.247: Supported headers within the PRACK request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	c1	c1
5	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
8	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
9	Content-Language	[26] 20.13	o		[26] 20.13	o	
10	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
11	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
12	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
13	Date	[26] 20.17	m	m	[26] 20.17	c2	c2
14	From	[26] 20.20	m	m	[26] 20.20	m	m
15	Max-Forwards	[26] 20.22	o	o	[26] 20.22	n/a	n/a
16	MIME-Version	[26] 20.24	o		[26] 20.24	o	
17	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
18	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
19	RAck	[27] 7.2	m	m	[27] 7.2	i	i
20	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
21	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
22	Route	[26] 20.34	m	m	[26] 20.34	m	m
23	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
24	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
25	To	[26] 20.39	m	m	[26] 20.39	m	m
26	User-Agent	[26] 20.41	o		[26] 20.41	o	
27	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1: IF A.4/20 THEN m ELSE i. c2: IF A.162/9 THEN m ELSE i. c5: IF A.162/11 OR A.162/13 THEN m ELSE i. c6: IF A.162/16 THEN m ELSE i. c7: IF A.162/14 THEN 0 ELSE i.							
NOTE: c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.							

Prerequisite A.163/14 – PRACK request

Table A.248: Supported message bodies within the PRACK request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.163/15 – PRACK response

Prerequisite: A.164/1 – 100 Trying

Table A.249: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
5	From	[26] 20.20	m	m	[26] 20.20	m	m
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.162/9 THEN m ELSE i.						

Prerequisite A.163/15 – PRACK response

Table A.250: Supported headers within the PRACK response - all remaining status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
3	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
4	Content-Language	[26] 20.13	o		[26] 20.13	o	
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o		[26] 20.24	o	
11	Timestamp	[26] 20.38	i	i	[26] 20.38	i	i
12	To	[26] 20.39	m	m	[26] 20.39	m	m
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.162/9 THEN m ELSE i.						

Prerequisite A.163/15 – PRACK response

Prerequisite: A.164/6 - - 2xx

Table A.251: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3
2	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
3	Server	[26] 20.35	m	m	[26] 20.35	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
5	User-Agent	[26] 20.41	o		[26] 20.41	o	
6	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c3:	IF A.162/15 THEN o ELSE i.						

Prerequisite A.163/15 – PRACK response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/35 - - 3xx or 485 "Ambiguous"

Table A.252: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Contact	[26] 20.10	o		[26] 20.10	o	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/15 – PRACK response

Prerequisite: A.164/14 – 401

Table A.253: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
8	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/15 – PRACK response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.254: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
3	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/15 – PRACK response

Prerequisite: A.164/18 -- "405" Method Not Allowed

Table A.255: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m		[26] 20.5	m	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/15 – PRACK response

Prerequisite: A.164/20 – 407

Table A.256: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/15 – PRACK response

Prerequisite: A.164/25 -- "415" Unsupported Media Type

Table A.257: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
6	Server	[26] 20.35	m	m	[26] 20.35	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/15 – PRACK response

Prerequisite: A.164/27 – 420@@@combine

Table A.258: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
3	Server	[26] 20.35	m	m	[26] 20.35	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
5	User-Agent	[26] 20.41	o		[26] 20.41	o	
6	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/34 - - 484

Table A.259: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
3	Server	[26] 20.35	m	m	[26] 20.35	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
5	User-Agent	[26] 20.41	o		[26] 20.41	o	
6	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/15 – PRACK response

Table A.260: Supported message bodies within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.2.4.11 REFER method

Prerequisite A.163/16 – REFER request

Table A.261: Supported headers within the REFER request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Language	[26] 20.3	o		[26] 20.3	o	
2	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	c1	c1
3	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
4	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
5	Contact	[26] 20.10	o		[26] 20.10	o	
6	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
7	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
8	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
9	Date	[26] 20.17	m	m	[26] 20.17	c2	c2
10	Expires	[26] 20.19	o		[26] 20.19	o	
11	From	[26] 20.20	m	m	[26] 20.20	m	m
12	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
13	MIME-Version	[26] 20.24	o		[26] 20.24	o	
14	Organization	[26] 20.25	o		[26] 20.25	o	
15	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
16	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
17	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
18	Refer-To	[36] 3	c3	c3	[36] 3	c4	c4
19	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
20	Route	[26] 20.34	m	m	[26] 20.34	m	m
21	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
22	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
23	To	[26] 20.39	m	m	[26] 20.39	m	m
24	User-Agent	[26] 20.41	o		[26] 20.41	o	
25	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1: IF A.4/20 THEN m ELSE i. c2: IF A.162/9 THEN m ELSE i. c5: IF A.162/11 OR A.162/13 THEN m ELSE i. c6: IF A.162/16 THEN m ELSE i. c7: IF A.162/14 THEN m ELSE i.							
NOTE: c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.							

Prerequisite A.163/16 – REFER request

Table A.262: Supported message bodies within the REFER request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.163/17 – REFER response

Prerequisite: A.164/1 – 100 Trying

Table A.263: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
5	From	[26] 20.20	m	m	[26] 20.20	m	m
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.162/9 THEN m ELSE i.						

Prerequisite A.163/17 – REFER response

Table A.264: Supported headers within the REFER response - all remaining status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
3	Content-Language	[26] 20.13	o		[26] 20.13	o	
4	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
5	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
6	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
7	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
8	From	[26] 20.20	m	m	[26] 20.20	m	m
9	MIME-Version	[26] 20.24	o		[26] 20.24	o	
10	Organization	[26] 20.25	o		[26] 20.25	o	
11	Timestamp	[26] 20.38	i	i	[26] 20.38	i	i
12	To	[26] 20.39	m	m	[26] 20.39	m	m
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.162/9 THEN m ELSE i.						

Prerequisite A.163/17 – REFER response

Prerequisite: A.164/7 - - 202

Table A.265: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Authentication-Info	[26] 20.6	o		[26] 20.6	o	
3	Contact	[26] 20.10	o		[26] 20.10	o	
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3
6	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
7	Server	[26] 20.35	m	m	[26] 20.35	i	i
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c3:	IF A.162/15 THEN m ELSE i.						

Prerequisite A.163/17 – REFER response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/35 - - 3xx or 485 "Ambiguous"@@@combine

Table A.266: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Contact	[26] 20.10	o		[26] 20.10	o	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
6	Server	[26] 20.35	m	m	[26] 20.35	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/17 – REFER response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 – 401

Table A.267: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Expires	[26] 20.19	o		[26] 20.19	o	
4	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
5	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
6	Server	[26] 20.35	m	m	[26] 20.35	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
10	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/17 – REFER response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.268: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Contact	[26] 20.10	o		[26] 20.10	o	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
6	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
7	Server	[26] 20.35	m	m	[26] 20.35	i	i
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/17 – REFER response

Prerequisite: A.164/18 -- "405" Method Not Allowed

Table A.269: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Allow	[26] 20.5	m	m	[26] 20.5	m	m
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
6	Server	[26] 20.35	m	m	[26] 20.35	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/17 – REFER response

Prerequisite: A.164/20 – 407

Table A.270: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Contact	[26] 20.10	o		[26] 20.10	o	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Expires	[26] 20.19	o		[26] 20.19	o	
4	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
5	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
6	Server	[26] 20.35	m	m	[26] 20.35	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/17 – REFER response

Prerequisite: A.164/25 -- "415" Unsupported Media Type

Table A.271: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Expires	[26] 20.19	o		[26] 20.19	o	
6	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
7	Server	[26] 20.35	m	m	[26] 20.35	i	i
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/17 – REFER response

Prerequisite: A.164/27 – 420

Table A.272: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Contact	[26] 20.10	o		[26] 20.10	o	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
6	Server	[26] 20.35	m	m	[26] 20.35	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	Unsupported	[26] 20.40	m	m	[26] 20.40	c3	c3
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	
c2: IF A.162/11 OR A.162/13 THEN m ELSE i. c3: IF A.162/18 THEN m ELSE i.							

Prerequisite A.163/17 – REFER response

Prerequisite: A.164/34 – 484@@@combine

Table A.273: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Contact	[26] 20.10	o		[26] 20.10	o	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
6	Server	[26] 20.35	m	m	[26] 20.35	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
c2: IF A.162/11 OR A.162/13 THEN m ELSE i.							

Prerequisite A.163/17 – REFER response

Table A.274: Supported message bodies within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.2.4.12 REGISTER method

Prerequisite A.163/18 – REGISTER request

Table A.275: Supported headers within the REGISTER request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	c1	c1
5	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Call-Info	[26] 20.9	o		[26] 20.9	o	
8	Contact	[26] 20.10	m		[26] 20.10	m	
9	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
10	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
11	Content-Language	[26] 20.13	o		[26] 20.13	o	
12	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
13	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
14	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
15	Date	[26] 20.17	m	m	[26] 20.17	m	m
16	Expires	[26] 20.19	o		[26] 20.19	o	
17	From	[26] 20.20	m	m	[26] 20.20	m	m
18	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
19	MIME-Version	[26] 20.24	o		[26] 20.24	o	
20	Organization	[26] 20.25	o		[26] 20.25	o	
21	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
22	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
23	Require	[26] 20.32	m	m	[26] 20.32	c4	c4
24	Route	[26] 20.34	m	m	[26] 20.34	m	m
25	Supported	[26] 20.37	m	m	[26] 20.37	c5	c5
26	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
27	To	[26] 20.39	m	m	[26] 20.39	m	m
28	User-Agent	[26] 20.41	o		[26] 20.41	o	
29	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1: IF A.4/20 THEN m ELSE i. c4: IF A.162/11 OR A.162/12 THEN m ELSE i. c5: IF A.162/16 THEN m ELSE i.							
NOTE: c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.							

Prerequisite A.163/18 – REGISTER request

Table A.276: Supported message bodies within the REGISTER request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.163/19 – REGISTER response

Prerequisite: A.164/1 – 100 Trying

Table A.277: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	m	m	[26] 20.17	m	m
5	From	[26] 20.20	m	m	[26] 20.20	m	m
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m

Prerequisite A.163/19 – REGISTER response

Table A.278: Supported headers within the REGISTER response - all remaining status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
3	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
4	Content-Language	[26] 20.13	o		[26] 20.13	o	
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	m	m	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o		[26] 20.24	o	
11	Organization	[26] 20.25	o		[26] 20.25	o	
12	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
13	To	[26] 20.39	m	m	[26] 20.39	m	m
14	Via	[26] 20.42	m	m	[26] 20.42	m	m

Prerequisite A.163/19 – REGISTER response

Prerequisite: A.164/6 – 2xx

Table A.279: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Allow	[26] 20.5	o		[26] 20.5	o	
3	Authentication-Info	[26] 20.6	o		[26] 20.6	o	
4	Call-Info	[26] 20.9	o		[26] 20.9	o	
5	Contact	[26] 20.10	o		[26] 20.10	o	
6	Expires	[26] 20.19	o		[26] 20.19	o	
7	Require	[26] 20.32	m	m	[26] 20.32	c1	c1
8	Server	[26] 20.35	m	m	[26] 20.35	i	i
9	Supported	[26] 20.37	m	m	[26] 20.37	i	i
10	User-Agent	[26] 20.41	o		[26] 20.41	o	
11	Warning	[26] 20.43	o		[26] 20.43	o	
c1:	IF A.162/11 OR A.162/12 THEN m ELSE i.						

Prerequisite A.163/19 – REGISTER response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/35 - - 3xx or 485 "Ambiguous"

Table A.280: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Contact	[26] 20.10	o		[26] 20.10	o	
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Expires	[26] 20.19	o		[26] 20.19	o	
6	Require	[26] 20.32	m	m	[26] 20.32	c1	c1
7	Server	[26] 20.35	m	m	[26] 20.35	i	i
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	
c1:	IF A.162/11 OR A.162/12 THEN m ELSE i.						

Prerequisite A.163/19 – REGISTER response

Prerequisite: A.164/14 – 401

Table A.281: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Require	[26] 20.32	m	m	[26] 20.32	c1	c1
6	Server	[26] 20.35	m	m	[26] 20.35	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
10	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	
c1:	IF A.162/11 OR A.162/12 THEN m ELSE i.						

Prerequisite A.163/19 – REGISTER response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.282: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Require	[26] 20.32	m	m	[26] 20.32	c1	c1
6	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
7	Server	[26] 20.35	m	m	[26] 20.35	i	i
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	
c1:	IF A.162/11 OR A.162/12 THEN m ELSE i.						

Prerequisite A.163/19 – REGISTER response

Prerequisite: A.164/18 -- "405" Method Not Allowed

Table A.283: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Allow	[26] 20.5	m		[26] 20.5	m	
3	Call-Info	[26] 20.9	o		[26] 20.9	o	
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Expires	[26] 20.19	o		[26] 20.19	o	
6	Require	[26] 20.32	m	m	[26] 20.32	c1	c1
7	Server	[26] 20.35	m	m	[26] 20.35	i	i
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	
c1:	IF A.162/11 OR A.162/12 THEN m ELSE i.						

Prerequisite A.163/19 – REGISTER response

Prerequisite: A.164/20 – 407

Table A.284: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
6	Require	[26] 20.32	m	m	[26] 20.32	c1	c1
7	Server	[26] 20.35	m	m	[26] 20.35	i	i
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	
c1:	IF A.162/11 OR A.162/12 THEN m ELSE i.						

Prerequisite A.163/19 – REGISTER response

Prerequisite: A.164/25 -- "415" Unsupported Media Type

Table A.285: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Call-Info	[26] 20.9	o		[26] 20.9	o	
5	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
6	Expires	[26] 20.19	o		[26] 20.19	o	
7	Require	[26] 20.32	m	m	[26] 20.32	c1	c1
8	Server	[26] 20.35	m	m	[26] 20.35	i	i
9	Supported	[26] 20.37	m	m	[26] 20.37	i	i
10	User-Agent	[26] 20.41	o		[26] 20.41	o	
11	Warning	[26] 20.43	o		[26] 20.43	o	
c1:	IF A.162/11 OR A.162/12 THEN m ELSE i.						

Prerequisite A.163/19 – REGISTER response

Prerequisite: A.164/27 – 420

Table A.286: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Require	[26] 20.32	m	m	[26] 20.32	c1	c1
6	Server	[26] 20.35	m	m	[26] 20.35	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	Unsupported	[26] 20.40	m	m	[26] 20.40	c3	c3
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	
c1:	IF A.162/11 OR A.162/12 THEN m ELSE i.						
c3:	IF A.162/17 THEN m ELSE.i						

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/29 - - 423

Table A.287: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	o		[26] 20.18	o	
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Min-Expires	[26] 20.23	m	m	[26] 20.23	i	i
6	Require	[26] 20.32	m	m	[26] 20.32	c1	c1
7	Server	[26] 20.35	o		[26] 20.35	o	
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i
9	User-Agent	[26] 20.41	o		[26] 20.41	o	
10	Warning	[26] 20.43	o		[26] 20.43	o	
c1:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/19 – REGISTER response

Prerequisite: A.164/34 – 484

Table A.288: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Call-Info	[26] 20.9	o		[26] 20.9	o	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Expires	[26] 20.19	o		[26] 20.19	o	
5	Require	[26] 20.32	m	m	[26] 20.32	c1	c1
6	Server	[26] 20.35	m	m	[26] 20.35	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
c1:	IF A.162/11 OR A.162/12 THEN m ELSE i.						

Prerequisite A.163/19 - - REGISTER response

Table A.289: Supported message bodies within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.2.4.13 SUBSCRIBE method

Prerequisite A.163/20 - - SUBSCRIBE request

Table A.290: Supported headers within the SUBSCRIBE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	c1	c1
5	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
8	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
9	Content-Language	[26] 20.13	o		[26] 20.13	o	
10	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
11	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
12	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
13	Date	[26] 20.17	m	m	[26] 20.17	c2	c2
14	Event	[28] 8.2.1	m	m	[28] 8.2.1	m	m
15	Expires	[26] 20.19	m	m	[26] 20.19	i	i
16	From	[26] 20.20	m	m	[26] 20.20	m	m
17	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
18	MIME-Version	[26] 20.24	o		[26] 20.24	o	
19	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
20	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
21	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
22	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
23	Route	[26] 20.34	m	m	[26] 20.34	m	m
24	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
25	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
26	To	[26] 20.39	m	m	[26] 20.39	m	m
27	User-Agent	[26] 20.41	o		[26] 20.41	o	
28	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1: IF A.4/20 THEN m ELSE i. c2: IF A.162/9 THEN m ELSE i. c5: IF A.162/11 OR A.162/13 THEN m ELSE i. c6: IF A.162/16 THEN m ELSE i. c7: IF A.162/14 THEN m ELSE i.							
NOTE: c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.							

Prerequisite A.163/20 - - SUBSCRIBE request

Table A.291: Supported message bodies within the SUBSCRIBE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.163/21 - - SUBSCRIBE response

Table A.292: Supported headers within the SUBSCRIBE response - all status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
3	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
4	Content-Language	[26] 20.13	o		[26] 20.13	o	
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o		[26] 20.24	o	
11	Timestamp	[26] 20.38	o		[26] 20.38	o	
12	To	[26] 20.39	m	m	[26] 20.39	m	m
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.162/9 THEN m ELSE i.						

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/6 AND A.164/7 - - 2xx

Table A.293: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Authentication-Info	[26] 20.6	o		[26] 20.6	o	
2	Expires	[26] 20.19	m	m	[26] 20.19	i	i
3	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3
4	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
5	Server	[26] 20.35	m	m	[26] 20.35	i	i
6	Supported	[26] 20.37	m	m	[26] 20.37	i	i
7	User-Agent	[26] 20.41	o		[26] 20.41	o	
8	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c3:	IF A.162/15 THEN m ELSE i.						

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/35 - - 3xx or 485 "Ambiguous"

Table A.294: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Contact	[26] 20.10	o		[26] 20.10	o	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/14 - - 401

Table A.295: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
8	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.296: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
3	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/18 -- "405" Method Not Allowed

Table A.297: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m		[26] 20.5	m	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/20 - - 407

Table A.298: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	m	m	[26] 20.35	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/25 -- "415" Unsupported Media Type

Table A.299: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
6	Server	[26] 20.35	m	m	[26] 20.35	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	User-Agent	[26] 20.41	o		[26] 20.41	o	
9	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/27 - - 420

Table A.300: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
3	Server	[26] 20.35	m	m	[26] 20.35	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
5	Unsupported	[26] 20.40	m	m	[26] 20.40	c3	c3
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c3:	IF A.162/18 THEN m ELSE i.						

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/29 -- 423

Table A.301: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o		[26] 20.18	o	
2	Min-Expires	[26] 20.23	m	m	[26] 20.23	i	i
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Server	[26] 20.35	o		[26] 20.35	o	
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/34 - - 484

Table A.302: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
3	Server	[26] 20.35	m	m	[26] 20.35	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
5	User-Agent	[26] 20.41	o		[26] 20.41	o	
6	Warning	[26] 20.43	o		[26] 20.43	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/39 - - 489

Table A.303: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	c1	c1
2	Authentication-Info	[26] 20.6	o		[26] 20.6	o	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Require	[26] 20.32	m	m	[26] 20.32	c3	c3
5	Server	[26] 20.35	m	m	[26] 20.35	i	i
6	User-Agent	[26] 20.41	o		[26] 20.41	o	
7	Warning	[26] 20.43	o		[26] 20.43	o	
c1:	IF A.4/20 THEN m ELSE i.						
c3:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
NOTE:	c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.						

Prerequisite A.163/21 - - SUBSCRIBE response

Table A.304: Supported message bodies within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.2.2.4.14 UPDATE method

Prerequisite A.163/22 - - UPDATE request

Table A.305: Supported headers within the UPDATE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow	[26] 20.5	o		[26] 20.5	o	
5	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	c1	c1
6	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
7	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
8	Call-Info	[26] 20.9	o		[26] 20.9	o	
9	Contact	[26] 20.10	o		[26] 20.10	o	
10	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
11	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
12	Content-Language	[26] 20.13	o		[26] 20.13	o	
13	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
14	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
15	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
16	Date	[26] 20.17	m	m	[26] 20.17	c2	c2
17	From	[26] 20.20	m	m	[26] 20.20	m	m
18	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
19	MIME-Version	[26] 20.24	o		[26] 20.24	o	
20	Organization	[26] 20.25	o		[26] 20.25	o	
21	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
22	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
23	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
24	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
25	Route	[26] 20.34	m	m	[26] 20.34	m	m
26	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
27	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
28	To	[26] 20.39	m	m	[26] 20.39	m	m
29	User-Agent	[26] 20.41	o		[26] 20.41	o	
30	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1: IF A.4/20 THEN m ELSE i. c2: IF A.162/9 THEN m ELSE i. c5: IF A.162/11 OR A.162/13 THEN m ELSE i. c6: IF A.162/16 THEN m ELSE i. c7: IF A.162/14 THEN o ELSE i.							
NOTE: c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.							

Table A.306: Supported message bodies within the UPDATE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.163/22 – INVITE response

Table A.307: Supported headers within the BYE response - all remaining status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
3	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
4	Content-Language	[26] 20.13	o		[26] 20.13	o	
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o		[26] 20.24	o	
11	Timestamp	[26] 20.38	o		[26] 20.38	o	
12	To	[26] 20.39	m	m	[26] 20.39	m	m
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.162/9 THEN m ELSE i.						

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/6 - - 2xx

Table A.308: Supported headers within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 24.5	m		[26] 24.5	m	
2	Call-Info	[26] 24.9	o		[26] 24.9	o	
3	Organization	[26] 24.25	o		[26] 24.25	o	
4	Require	[26] 24.33	m	m	[26] 24.33	c2	c2
5	Server	[26] 24.37	m	m	[26] 24.37	i	i
6	Supported	[26] 24.39	m	m	[26] 24.39	i	i
7	User-Agent	[26] 24.43	o		[26] 24.43	o	
8	Warning	[26] 24.45	o		[26] 24.45	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c3:	IF A.162/15 THEN o ELSE i.						

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 - - 3xx

Table A.309: Supported headers within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-Info	[26] 24.9	o		[26] 24.9	o	
2	Contact	[26] 24.10	o		[26] 24.10	o	
3	Error-Info	[26] 24.18	m	m	[26] 24.18	i	i
4	From	[26] 24.20	m	m	[26] 24.20	m	m
5	Require	[26] 24.33	m	m	[26] 24.33	c2	c2
6	Server	[26] 24.37	m	m	[26] 24.37	i	i
7	Supported	[26] 24.39	m	m	[26] 24.39	i	i
8	User-Agent	[26] 24.43	o		[26] 24.43	o	
9	Warning	[26] 24.45	o		[26] 24.45	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.310: Supported headers within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-Info	[26] 24.9	o		[26] 24.9	o	
2	Error-Info	[26] 24.18	m	m	[26] 24.18	i	i
3	Organization	[26] 24.25	o		[26] 24.25	o	
4	Require	[26] 24.33	m	m	[26] 24.33	c2	c2
5	Retry-After	[26] 24.34	m	m	[26] 24.34	i	i
6	Server	[26] 24.37	m	m	[26] 24.37	i	i
7	Supported	[26] 24.39	m	m	[26] 24.39	i	i
8	User-Agent	[26] 24.43	o		[26] 24.43	o	
9	Warning	[26] 24.45	o		[26] 24.45	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/18 -- "405" Method Not Allowed

Table A.311: Supported headers within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 24.5	m		[26] 24.5	m	
2	Call-Info	[26] 24.9	o		[26] 24.9	o	
3	Error-Info	[26] 24.18	m	m	[26] 24.18	i	i
4	Organization	[26] 24.25	o		[26] 24.25	o	
5	Require	[26] 24.33	m	m	[26] 24.33	c2	c2
6	Server	[26] 24.37	m	m	[26] 24.37	i	i
7	Supported	[26] 24.39	m	m	[26] 24.39	i	i
8	User-Agent	[26] 24.43	o		[26] 24.43	o	
9	Warning	[26] 24.45	o		[26] 24.45	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/20 - - 407

Table A.312: Supported headers within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-Info	[26] 24.9	o		[26] 24.9	o	
2	Error-Info	[26] 24.18	m	m	[26] 24.18	i	i
3	Organization	[26] 24.25	o		[26] 24.25	o	
4	Proxy-Authenticate	[26] 24.27	o		[26] 24.27	o	
5	Require	[26] 24.33	m	m	[26] 24.33	c2	c2
6	Server	[26] 24.37	m	m	[26] 24.37	i	i
7	Supported	[26] 24.39	m	m	[26] 24.39	i	i
8	User-Agent	[26] 24.43	o		[26] 24.43	o	
9	Warning	[26] 24.45	o		[26] 24.45	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/25 -- "415" Unsupported Media Type

Table A.313: Supported headers within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 24.1	o		[26] 24.1	o	
2	Accept-Encoding	[26] 24.2	o		[26] 24.2	o	
3	Accept-Language	[26] 24.3	o		[26] 24.3	o	
4	Allow	[26] 20.5	o		[26] 20.5	o	
5	Call-Info	[26] 24.9	o		[26] 24.9	o	
6	Error-Info	[26] 24.18	m	m	[26] 24.18	i	i
7	Organization	[26] 24.25	o		[26] 24.25	o	
8	Require	[26] 24.33	m	m	[26] 24.33	c2	c2
9	Server	[26] 24.37	m	m	[26] 24.37	i	i
10	Supported	[26] 24.39	m	m	[26] 24.39	i	i
11	User-Agent	[26] 24.43	o		[26] 24.43	o	
12	Warning	[26] 24.45	o		[26] 24.45	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/27 - - 420

Table A.314: Supported headers within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-Info	[26] 24.9	o		[26] 24.9	o	
2	Error-Info	[26] 24.18	m	m	[26] 24.18	i	i
3	Organization	[26] 24.25	o		[26] 24.25	o	
4	Require	[26] 24.33	m	m	[26] 24.33	c2	c2
5	Server	[26] 24.37	m	m	[26] 24.37	i	i
6	Supported	[26] 24.39	m	m	[26] 24.39	i	i
7	Unsupported	[26] 24.42	m	m	[26] 24.42	c3	c3
8	User-Agent	[26] 24.43	o		[26] 24.43	o	
9	Warning	[26] 24.45	o		[26] 24.45	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						
c3:	IF A.162/18 THEN m ELSE i.						

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/35 - - 3xx or 485 "Ambiguous"

Table A.315: Supported headers within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-Info	[26] 24.9	o		[26] 24.9	o	
2	Contact	[26] 24.10	o		[26] 24.10	o	
3	Error-Info	[26] 24.18	m	m	[26] 24.18	i	i
4	Organization	[26] 24.25	o		[26] 24.25	o	
5	Require	[26] 24.33	m	m	[26] 24.33	c2	c2
6	Server	[26] 24.37	m	m	[26] 24.37	i	i
7	Supported	[26] 24.39	m	m	[26] 24.39	i	i
8	User-Agent	[26] 24.43	o		[26] 24.43	o	
9	Warning	[26] 24.45	o		[26] 24.45	o	
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i.						

Table A.316: Supported message bodies within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

A.3 Profile definition for the Session Description Protocol as used in the present document

A.3.1 Introduction

Void.

A.3.2 User agent role

This subclause contains the ICS proforma tables related to the user role. They need to be completed only for UA implementations.

Prerequisite: A.2/1 -- user agent role

A.3.2.1 Major capabilities

Table A.317: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
	Capabilities within main protocol			
	Extensions			
22	Integration of resource management and SIP?	[30]	o	m

A.3.2.2 SDP types

Table A.318: SDP types

Item	Type	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
	Session level description						
1	v= (protocol version)	[39] 6	m	m	[39] 6	m	m
2	o= (owner/creator and session identifier)	[39] 6	m	m	[39] 6	m	m
3	s= (session name)	[39] 6	m	m	[39] 6	m	m
4	i= (session information)	[39] 6	o		[39] 6		
5	u= (URI of description)	[39] 6	o	n/a	[39] 6		n/a
6	e= (email address)	[39] 6	o	n/a	[39] 6		n/a
7	p= (phone number)	[39] 6	o	n/a	[39] 6		n/a
8	c= (connection information)	[39] 6	o		[39] 6		
9	b= (bandwidth information)	[39] 6	o	o (NOTE 1)	[39] 6		
	Time description (one or more per description)						
10	t= (time the session is active)	[39] 6	m	m	[39] 6	m	m
11	r= (zero or more repeat times)	[39] 6	o	n/a	[39] 6		n/a
	Session level description (continued)						
12	z= (time zone adjustments)	[39] 6	o	n/a	[39] 6		n/a
13	k= (encryption key)	[39] 6	o		[39] 6		
14	a= (zero or more session attribute lines)	[39] 6	o		[39] 6		
	Media description (zero or more per description)						
15	m= (media name and transport address)	[39] 6	o	o	[39] 6	m	m
16	i= (media title)	[39] 6	o		[39] 6		
17	c= (connection information)	[39] 6	c1	c1	[39] 6		
18	b= (bandwidth information)	[39] 6	o	o (NOTE 1)	[39] 6		
19	k= (encryption key)	[39] 6	o		[39] 6		
20	a= (zero or more media attribute lines)	[39] 6	o		[39] 6		
c1: IF A.318/15 THEN m ELSE n/a.							
NOTE 1: For "video" and "audio" media types that utilise RTP/RTCP, it shall be specified. For other media types, it may be specified.							

Prerequisite A.318/14 OR A.318/20 - - a= (zero or more session/media attribute lines)

Table A.319: zero or more session / media attribute lines (a=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	category (a=cat)	[39] 6			[39] 6		
2	keywords (a=keywds)	[39] 6			[39] 6		
3	name and version of tool (a=tool)	[39] 6			[39] 6		
4	packet time (a=ptime)	[39] 6			[39] 6		
5	maximum packet time (a=maxptime)	[39] 6			[39] 6		
6	receive-only mode (a=recvonly)	[39] 6			[39] 6		
7	send and receive mode (a=sendrecv)	[39] 6			[39] 6		
8	send-only mode (a=sendonly)	[39] 6			[39] 6		
9	whiteboard orientation (a=orient)	[39] 6			[39] 6		
10	conference type (a=type)	[39] 6			[39] 6		
11	character set (a=charset)	[39] 6			[39] 6		
12	language tag (a=sdplang)	[39] 6			[39] 6		
13	language tag (a=lang)	[39] 6			[39] 6		
14	frame rate (a=framerate)	[39] 6			[39] 6		
15	quality (a=quality)	[39] 6			[39] 6		
16	format specific parameters (a=fmtp)	[39] 6			[39] 6		
17	rtpmap attribute (a=rtpmap)	[39] 6			[39] 6		
18	qos-attribute (a=qos)	[30] 5	c1	c1	[30] 5	c2	c2
c1:	IF A.317/22 THEN o ELSE n/a.						
c2:	IF A.317/22 THEN m ELSE n/a.						

A.3.2.3 SDP types parameters

Prerequisite A.318/2 - - o= (owner/creator and session identifier)

Table A.320: owner/creator and session identifier type (o=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	username	[39] 6	m	m	[39] 6	m	n/a
2	session id	[39] 6	m	m	[39] 6	m	m
3	version	[39] 6	m	m	[39] 6	m	m
4	network type	[39] 6	m	m	[39] 6	m	n/a
5	address type	[39] 6	m	m	[39] 6	m	n/a
6	address	[39] 6	m	m	[39] 6	m	n/a

Prerequisite A.318/10 - - t= (time the session is active)

Table A.321: time the session is active type (t=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	start time	[39] 6	m	m	[39] 6	m	n/a
2	stop time	[39] 6	m	m	[39] 6	m	n/a

Prerequisite A.318/11 - - r= (zero or more repeat times)

Table A.322: zero or more repeat times (r=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	repeat interval	[39] 6		n/a	[39] 6		n/a
2	active duration	[39] 6		n/a	[39] 6		n/a
3	list of offsets from start-time	[39] 6		n/a	[39] 6		n/a

Prerquisite A.318/12 - - z= (time zone adjustments)

Table A.323: time zone adjustments type (z=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	adjustment time	[39] 6		n/a	[39] 6		n/a
2	offset	[39] 6		n/a	[39] 6		n/a
3	adjustment time	[39] 6		n/a	[39] 6		n/a
4	offset	[39] 6		n/a	[39] 6		n/a

Prerquisite A.318/13 - - k= (encryption key)

Table A.324: encryption key type (k=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	method	[39] 6			[39] 6		
2	encryption key	[39] 6			[39] 6		

Prerequisite A.318/15 - - m= (media name and transport address)

Table A.325: media name and transport address type (m=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	media - ``audio'' - ``video'' - ``application'' - ``data'' - ``control''	[39] 6			[39] 6		
2	port	[39] 6			[39] 6		
3	transport	[39] 6			[39] 6		
4	fmt list	[39] 6			[39] 6		

Editor's note: It is expected that this table will be expanded, as this is the principle table that will distinguish operation of different entities within the IM CN subsystem.

Prerequisite A.318/17 - - c= (connection information)

Table A.326: connection type (c=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	network type	[39] 6			[39] 6		
2	address type	[39] 6			[39] 6		
3	connection address	[39] 6			[39] 6		

Prerequisite A.318/18 - - b= (bandwidth information)

Table A.327: bandwidth information (b=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	modifier	[39] 6		o (NOTE 1)	[39] 6		
2	bandwidth-value	[39] 6		o (NOTE 2)	[39] 6		
NOTE 1: For "video" and "audio" media types that utilise RTP/RTCP, the value shall be AS. NOTE 2: For "video" and "audio" media types that utilise RTP/RTCP, it shall be specified. For other media types, it may be specified.							

A.3.3 Proxy role

This subclause contains the ICS proforma tables related to the user role. They need to be completed only for proxy implementations.

Prerequisite: A.2/2 -- proxy role

A.3.3.1 Major capabilities

Table A.328: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
	Capabilities within main protocol			
	Extensions			
1	Integration of resource management and SIP?	[30]	o	m

A.3.3.2 SDP types

Table A.329: SDP types

Item	Type	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
	Session level description						
1	v= (protocol version)	[39] 6	m	m	[39] 6	m	m
2	o= (owner/creator and session identifier).	[39] 6	m	m	[39] 6	i	i
3	s= (session name)	[39] 6	m	m	[39] 6	i	i
4	i= (session information)	[39] 6	m	m	[39] 6	i	i
5	u= (URI of description)	[39] 6	m	m	[39] 6	i	i
6	e= (email address)	[39] 6	m	m	[39] 6	i	i
7	p= (phone number)	[39] 6	m	m	[39] 6	i	i
8	c= (connection information)	[39] 6	m	m	[39] 6	i	i
9	b= (bandwidth information)	[39] 6	m	m	[39] 6	i	i
	Time description (one or more per description)						
10	t= (time the session is active)	[39] 6	m	m	[39] 6	i	i
11	r= (zero or more repeat times)	[39] 6	m	m	[39] 6	i	i
	Session level description (continued)						
12	z= (time zone adjustments)	[39] 6	m	m	[39] 6	i	i
13	k= (encryption key)	[39] 6	m	m	[39] 6	i	i
14	a= (zero or more session attribute lines)	[39] 6	m	m	[39] 6	i	i
	Media description (zero or more per description)						
15	m= (media name and transport address)	[39] 6	m	m	[39] 6	m	m
16	i= (media title)	[39] 6	o		[39] 6		
17	c= (connection information)	[39] 6	o		[39] 6		
18	b= (bandwidth information)	[39] 6	o		[39] 6		
19	k= (encryption key)	[39] 6	o		[39] 6		
20	a= (zero or more media attribute lines)	[39] 6	o		[39] 6		

Prerequisite A.329/14 OR A.329/20 - - a= (zero or more session/media attribute lines)

Table A.330: zero or more session / media attribute lines (a=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	category (a=cat)	[39] 6			[39] 6		
2	keywords (a=keywds)	[39] 6			[39] 6		
3	name and version of tool (a=tool)	[39] 6			[39] 6		
4	packet time (a=ptime)	[39] 6			[39] 6		
5	maximum packet time (a=maxptime)	[39] 6			[39] 6		
6	receive-only mode (a=recvonly)	[39] 6			[39] 6		
7	send and receive mode (a=sendrecv)	[39] 6			[39] 6		
8	send-only mode (a=sendonly)	[39] 6			[39] 6		
9	whiteboard orientation (a=orient)	[39] 6			[39] 6		
10	conference type (a=type)	[39] 6			[39] 6		
11	character set (a=charset)	[39] 6			[39] 6		
12	language tag (a=sdplang)	[39] 6			[39] 6		
13	language tag (a=lang)	[39] 6			[39] 6		
14	frame rate (a=framerate)	[39] 6			[39] 6		
15	quality (a=quality)	[39] 6			[39] 6		
16	format specific parameters (a=fmtp)	[39] 6			[39] 6		
17	rtpmap attribute (a=rtpmap)	[39] 6			[39] 6		
18	qos-attribute (a=qos)	[30] 5	m	m	[30] 5	c2	c2
c2:	IF A.328/1 THEN m ELSE i.						

A.3.2.3 SDP types parameters

Prerequisite A.329/2 - - o= (owner/creator and session identifier)

Table A.331: owner/creator and session identifier type (o=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	username	[39] 6	m	m	[39] 6	m	m
2	session id	[39] 6	m	m	[39] 6	m	m
3	version	[39] 6	m	m	[39] 6	m	m
4	network type	[39] 6	m	m	[39] 6	m	m
5	address type	[39] 6	m	m	[39] 6	m	m
6	address	[39] 6	m	m	[39] 6	m	m

Prerequisite A.329/10 - - t= (time the session is active)

Table A.332: time the session is active type (b=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	start time	[39] 6			[39] 6		
2	stop time	[39] 6			[39] 6		

Prerequisite A.329/11 - - r= (zero or more repeat times)

Table A.333: zero or more repeat times (r=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	repeat interval	[39] 6			[39] 6		
2	active duration	[39] 6			[39] 6		
3	list of offsets from start-time	[39] 6			[39] 6		

Prerequisite A.329/12 - - z= (time zone adjustments)

Table A.334: time zone adjustments type (z=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	adjustment time	[39] 6			[39] 6		
2	offset	[39] 6			[39] 6		
3	adjustment time	[39] 6			[39] 6		
4	offset	[39] 6			[39] 6		

Prerequisite A.329/13 - - k= (encryption key)

Table A.335: encryption key type (k=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	method	[39] 6			[39] 6		
2	encryption key	[39] 6			[39] 6		

Prerequisite A.329/15 - - m= (media name and transport address)

Table A.336: media name and transport address type (m=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	media - ``audio'' - ``video'' - ``application'' - ``data'' - ``control''	[39] 6			[39] 6		
2	port	[39] 6			[39] 6		
3	transport	[39] 6			[39] 6		
4	fmt list	[39] 6			[39] 6		

Editor's note: It is expected that this table will be expanded, as this is the principle table that will distinguish operation of different entities within the IM CN subsystem.

Prerequisite A.329/17 - - c= (connection information)

Table A.337: connection type (c=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	network type	[39] 6			[39] 6		
2	address type	[39] 6			[39] 6		
3	connection address	[39] 6			[39] 6		

Prerequisite A.329/18 - - b= (bandwidth information)

Table A.338: bandwidth information (b=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	modifier	[39] 6			[39] 6		
2	bandwidth-value	[39] 6			[39] 6		

A.4 Profile definition for other message bodies as used in the present document

Void.

Annex B (informative): Change history

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
					Version 0.0.0 Editor's internal draft			
					Version 0.0.1 Editor's internal draft			
					Version 0.0.2 Editor's internal draft			
		N1-001060			Version 0.0.3 Submitted to CN1 SIP adhoc #1			
19/10/00		N1-001109			Version 0.0.4 Reflecting results of initial CN1 discussion			
19/10/00		N1-001115			Version 0.0.5 Reflecting output of CN1 SIP adhoc#1 discussion			
09/11/00					Version 0.0.6 Revision to include latest template and styles			
		N1-010092			Version 0.0.7 Reflecting updates of some IETF drafts			
14/02/01		N1-010269			Version 0.0.8 Revision to include temporary annex B incorporating valuable source material			
18/03/01		N1-010378 rev			Version 0.1.0 incorporating results of CN1 discussion at CN1 #16			
12/04/01		N1-010737			Version 0.2.0 incorporating results of CN1 discussions at SIP adhoc #4			
11/06/01		N1-010935			Version 0.3.0 incorporating results of CN1 discussions at CN1 #16			
23/07/01		N1-011103			Version 0.4.0 incorporating results of CN1 discussions at CN1 #18 (agreed documents N1-011028, N1-011050, N1-011055, N1-011056)			
12/09/01		N1-011385			Version 0.5.0 incorporating results of CN1 discussions at CN1 #19 (agreed documents N1-011109, N1-011152, N1-011195, N1-011312, N1-011319, N1-011343)			
04/10/01		N1-011470			Version 0.6.0 incorporating results of CN1 discussions at CN1 #19bis (agreed documents N1-011346, N1-011373, N1-011389, N1-011390, N1-011392, N1-011393, N1-011394, N1-011408, N1-011410, N1-011426)			
19/10/01		N1-011643			Version 0.7.0 incorporating results of CN1 discussions at CN1 #20 (agreed documents N1-011477, N1-011479, N1-011498, N1-011523, N1-011548, N1-011585, N1-011586, N1-011592, N1-011611, N1-011629)			
16/11/01		N1-011821			Version 0.8.0 incorporating results of CN1 discussions at CN1 #20bis (agreed documents N1-011685, N1-011690, N1-011741, N1-011743, N1-011759, N1-011760, N1-011761, N1-011765c, N1-011767, N1-011769, N1-011770, N1-011771, N1-011774, N1-011777, N1-011779, N1-011780) N1-011712 was agreed but determined to have no impact on the specification at this time.			
30/11/01		N1-020010			Version 1.0.0 incorporating results of CN1 discussions at CN1 #21 (agreed documents N1-011828, N1-011829, N1-011836, N1-011899 [revision marks not used on moved text - additional change from chairman's report incorporated], implementation of subclause 3.1 editor's note based on discussion of N1-011900 [chairman's report], N1-011905, N1-011984, N1-011985, N1-011986, N1-011988, N1-011989, N1-012012 [excluding points 2 and 16], N1-012013, N1-012014 [excluding point 1], N1-012015, N1-012021, N1-012022, N1-012025, N1-012031, N1-012045, N1-012056, N1-012057) CN1 agreed for presentation for information to CN plenary.			
18/01/02		N1-020189			Version 1.1.0 incorporating results of CN1 discussions at CN1 SIP ad-hoc (agreed documents N1-020015, N1-020053, N1-020064, N1-020101, N1-020123, N1-020124, N1-020142, N1-020146, N1-020147, N1-020148, N1-020151, N1-020157, N1-020159, N1-020165). Also N1-012000 (agreed at previous meeting) required, subclause 5.2.6 to be deleted and this			

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
					change has been enacted			
01/02/02		N1-020459			Version 1.2.0 incorporating results of CN1 discussions at CN1 #22 (agreed documents N1-020198, N1-020396, N1-020398, N1-020399, N1-020408, N1-020417, N1-020418, N1-020419, N1-020421, N1-020422, N1-020436, N1-020437, N1-020449)			
01/02/02		N1-020569			Version 1.2.1 issues to correct cut and paste error in incorporation of Annex B into main document. Affected subclause 5.1.1.3. Change to clause 7 title that was incorrectly applied to subclause 7.2 also corrected.			
22/02/02					Advanced to version 2.0.0 based on agreement of N1-020515. Version 2.0.0 incorporating results of CN1 discussions at CN1 #22bis (agreed documents N1-020466, N1-020468, N1-020469, N1-020472, N1-020473, N1-020500, N1-020504, N1-020507, N1-020511, N1-020512, N1-020521, N1-020583, N1-020584, N1-020602, N1-020603, N1-020604, N1-020611, N1-020612, N1-020613, N1-020614, N1-020615, N1-020617, N1-020623, N1-020624, N1-020625, N1-020626, N1-020627, N1-020642, N1-020643, N1-020646, N1-020649, N1-020656, N1-020659, N1-020668, N1-020669, N1-020670, N1-020671). In addition N1-020409, agreed at CN1#22 but missed from the previous version, was also implemented. References have been resequenced.			
02/03/02					Editorial clean-up by ETSI/MCC.	2.0.0	2.0.1	
11/03/02	TSG CN#15	NP-020049			The draft was approved, and 3GPP TS 24.229 was then to be issued in Rel-5 under formal change control.	2.0.1	5.0.0	
2002-06	NP-16	NP-020230	004	1	S-CSCF Actions on Authentication Failure	5.0.0	5.1.0	N1-020903
2002-06	NP-16	NP-020230	005	2	Disallow Parallel Registrations	5.0.0	5.1.0	N1-020959
2002-06	NP-16	NP-020230	007	1	Hiding	5.0.0	5.1.0	N1-020910
2002-06	NP-16	NP-020312	008	8	Support for services for unregistered users	5.0.0	5.1.0	
2002-06			009	1	Not implemented nor implementable. In the meeting report CN1#24 under doc N1-021513 it is shown that CR095r2 supercedes 009r1 if 095r2 was to be approved in CN#16 (but unfortunately 009r1 was also approved in the the CN#16 draft minutes).			N1-020921
2002-06	NP-16	NP-020231	019		MGCF procedure clarification	5.0.0	5.1.0	N1-020788
2002-06	NP-16	NP-020231	020	2	MGCF procedure error cases	5.0.0	5.1.0	N1-020960
2002-06	NP-16	NP-020231	022	1	Abbreviations clean up	5.0.0	5.1.0	N1-020949
2002-06	NP-16	NP-020231	023		Clarification of SIP usage outside IM CN subsystem	5.0.0	5.1.0	N1-020792
2002-06	NP-16	NP-020314	024	3	Replacement of COMET by UPDATE	5.0.0	5.1.0	
2002-06	NP-16	NP-020231	025	3	Incorporation of current RFC numbers	5.0.0	5.1.0	N1-021091
2002-06	NP-16	NP-020231	026	1	Clarification of B2BUA usage in roles	5.0.0	5.1.0	N1-020941
2002-06	NP-16	NP-020231	028	4	Determination of MO / MT requests in I-CSCF(THIG)	5.0.0	5.1.0	N1-021248
2002-06	NP-16	NP-020231	030	2	P-CSCF release of an existing session	5.0.0	5.1.0	N1-021006
2002-06	NP-16	NP-020232	031	1	S-CSCF release of an existing session	5.0.0	5.1.0	N1-020939
2002-06	NP-16	NP-020232	033	3	SDP procedure at the UE	5.0.0	5.1.0	N1-020971
2002-06	NP-16	NP-020232	035	1	AS Procedures corrections	5.0.0	5.1.0	N1-020934
2002-06	NP-16	NP-020232	036	8	Corrections to SIP Compression	5.0.0	5.1.0	N1-021499
2002-06	NP-16	NP-020232	037	1	Enhancement of S-CSCF and I-CSCF Routing Procedures for interworking with external networks	5.0.0	5.1.0	N1-020928
2002-06	NP-16	NP-020232	041	2	Delivery of IMS security parameters from S-CSCF to the P-CSCF by using proprietary auth-param	5.0.0	5.1.0	N1-021003

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2002-06	NP-16	NP-020232	045		Cleanup of request / response terminology - clause 5	5.0.0	5.1.0	N1-020835
2002-06	NP-16	NP-020232	046		Cleanup of request / response terminology - clause 6	5.0.0	5.1.0	N1-020836
2002-06	NP-16	NP-020232	047	2	Simplification of profile tables	5.0.0	5.1.0	N1-021059
2002-06	NP-16	NP-020232	049		Forking options	5.0.0	5.1.0	N1-020839
2002-06	NP-16	NP-020315	050	1	Media-Authorization header corrections	5.0.0	5.1.0	
2002-06	NP-16	NP-020233	051	1	Clause 5.4 editorials (S-CSCF)	5.0.0	5.1.0	N1-020950
2002-06	NP-16	NP-020233	053	2	Integrity protection signalling from the P-CSCF to the S-CSCF	5.0.0	5.1.0	N1-021007
2002-06	NP-16	NP-020233	054		Representing IM CN subsystem functional entities in profile table roles	5.0.0	5.1.0	N1-020847
2002-06	NP-16	NP-020233	055		Clause 4 editorials	5.0.0	5.1.0	N1-020848
2002-06	NP-16	NP-020233	056		Clause 5.8 editorials (MRFC)	5.0.0	5.1.0	N1-020849
2002-06	NP-16	NP-020233	057	1	Annex A editorials, including precondition additions	5.0.0	5.1.0	N1-021001
2002-06	NP-16	NP-020233	058	2	Representing the registrar as a UA	5.0.0	5.1.0	N1-021054
2002-06	NP-16	NP-020233	059		Additional definitions	5.0.0	5.1.0	N1-020852
2002-06	NP-16	NP-020312	060	11	Restructuring of S-CSCF Registration Sections	5.0.0	5.1.0	
2002-06	NP-16	NP-020234	061	2	Determination of MOC / MTC at P-CSCF and S-CSCF	5.0.0	5.1.0	N1-021060
2002-06	NP-16	NP-020234	062		Correction to the terminating procedures	5.0.0	5.1.0	N1-020927
2002-06	NP-16	NP-020234	063		Loose Routing for Network Initiated Call Release Procedures	5.0.0	5.1.0	N1-020940
2002-06	NP-16	NP-020234	064		Incorporation of previously agreed corrections to clause 5.2.5.2 (N1-020416)	5.0.0	5.1.0	N1-021004
2002-06	NP-16	NP-020234	065		Clause 7.2 editorial corrections	5.0.0	5.1.0	N1-021005
2002-06	NP-16	NP-020234	067	2	S-CSCF routing of MO calls	5.0.0	5.1.0	N1-021097
2002-06	NP-16	NP-020234	068	1	I-CSCF routeing of dialog requests	5.0.0	5.1.0	N1-021078
2002-06	NP-16	NP-020234	069	2	Definition of the Tokanised-by parameter	5.0.0	5.1.0	N1-021096
2002-06	NP-16	NP-020235	070	3	SDP procedures at UE	5.0.0	5.1.0	N1-021453
2002-06	NP-16	NP-020235	073	2	Updates to the procedures involving the iFCs, following the Oulu iFC changes	5.0.0	5.1.0	N1-021440
2002-06	NP-16	NP-020235	074	1	Addition of DHCPv6 references to 24.229	5.0.0	5.1.0	N1-021086
2002-06	NP-16	NP-020235	075	1	Clarification to URL and address assignments	5.0.0	5.1.0	N1-021083
2002-06	NP-16	NP-020235	079	3	Downloading the implicitely registered public user identities from the S-CSCF to P-CSCF	5.0.0	5.1.0	N1-021510
2002-06	NP-16	NP-020235	080	3	Clarification of GPRS aspects	5.0.0	5.1.0	N1-021486
2002-06	NP-16	NP-020235	081	2	Introduction of Subscription Locator Function Interrogation at I-CSCF in 24.229	5.0.0	5.1.0	N1-021469
2002-06	NP-16	NP-020235	082	1	Introduction of Visited_Network_ID p-header	5.0.0	5.1.0	N1-021433
2002-06	NP-16	NP-020236	084	1	MRFC register addresses	5.0.0	5.1.0	N1-021434
2002-06	NP-16	NP-020236	085	1	MRFC INVITE interface editor's notes	5.0.0	5.1.0	N1-021470
2002-06	NP-16	NP-020236	086	1	MRFC OPTIONS interface editor's notes	5.0.0	5.1.0	N1-021471
2002-06	NP-16	NP-020236	087		MRFC PRACK & INFO editor's notes	5.0.0	5.1.0	N1-021159
2002-06	NP-16	NP-020236	088	1	MGCF OPTIONS interface editor's notes	5.0.0	5.1.0	N1-021472
2002-06	NP-16	NP-020236	089		MGCF reINVITE editor's notes	5.0.0	5.1.0	N1-021161

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2002-06	NP-16	NP-020237	090		3PCC AS editor's notes	5.0.0	5.1.0	N1-021162
2002-06	NP-16	NP-020237	091		AS acting as terminating UA editor's notes	5.0.0	5.1.0	N1-021163
2002-06	NP-16	NP-020237	092	1	AS acting as originating UA editor's notes	5.0.0	5.1.0	N1-021466
2002-06	NP-16	NP-020237	093	2	Charging overview clause	5.0.0	5.1.0	N1-021512
2002-06	NP-16	NP-020237	094	1	Procedures for original-dialog-id P-header	5.0.0	5.1.0	N1-021456
2002-06	NP-16	NP-020237	095	2	Procedures for charging-vector P-header	5.0.0	5.1.0	N1-021513
2002-06	NP-16	NP-020237	096	1	Procedures for charging-function-addresses P-header	5.0.0	5.1.0	N1-021458
2002-06	NP-16	NP-020237	097	1	SDP types	5.0.0	5.1.0	N1-021467
2002-06	NP-16	NP-020237	100		Removal of State from profile tables	5.0.0	5.1.0	N1-021173
2002-06	NP-16	NP-020238	101		Editor's note cleanup - clause 3	5.0.0	5.1.0	N1-021174
2002-06	NP-16	NP-020238	102		Editor's note cleanup - clause 4	5.0.0	5.1.0	N1-021175
2002-06	NP-16	NP-020238	103		Editor's note cleanup - clause 5.1 and deletion of void subclauses	5.0.0	5.1.0	N1-021176
2002-06	NP-16	NP-020238	104	1	Editor's note cleanup - clause 5.2 and deletion of void subclauses	5.0.0	5.1.0	N1-021487
2002-06	NP-16	NP-020238	105		Editor's note cleanup - clause 5.3	5.0.0	5.1.0	N1-021178
2002-06	NP-16	NP-020238	106		Editor's note cleanup - clause 5.4 and deletion of void subclauses	5.0.0	5.1.0	N1-021179
2002-06	NP-16	NP-020238	107		Editor's note cleanup - clause 5.5 and deletion of void subclauses	5.0.0	5.1.0	N1-021180
2002-06	NP-16	NP-020238	110		Editor's note cleanup - clause 6	5.0.0	5.1.0	N1-021183
2002-06	NP-16	NP-020238	111		Editor's note cleanup - clause 9	5.0.0	5.1.0	N1-021184
2002-06	NP-16	NP-020239	113	1	SIP Default Timers	5.0.0	5.1.0	N1-021465
2002-06	NP-16	NP-020239	114	1	Correction of the subscription to the registration event package	5.0.0	5.1.0	N1-021436
2002-06	NP-16	NP-020239	115	1	Support for ISIMless UICC	5.0.0	5.1.0	N1-021441
2002-06	NP-16	NP-020239	119	1	SIP procedures at UE	5.0.0	5.1.0	N1-021452
2002-06	NP-16	NP-020239	121	2	New requirements in the P-CSCF	5.0.0	5.1.0	N1-021509
2002-06	NP-16	NP-020239	122		SDP procedures at MGCF	5.0.0	5.1.0	N1-021264
2002-06	NP-16	NP-020239	124	1	S-CSCF allocation	5.0.0	5.1.0	N1-021443
2002-06	NP-16	NP-020240	129	1	Introduction of P-Access-Network-Info header	5.0.0	5.1.0	N1-021498
2002-06	NP-16	NP-020240	130	2	Usage of Path and P-Service Route	5.0.0	5.1.0	N1-021508
2002-06	NP-16	NP-020240	133		Removal of Referred-By header from specification	5.0.0	5.1.0	N1-021354
2002-06	NP-16	NP-020240	134		Handling of Record-Route header in profile tables	5.0.0	5.1.0	N1-021357
2002-06	NP-16	NP-020312	135	1	Asserted identities and privacy	5.0.0	5.1.0	
2002-06	NP-16	NP-020240	136		Removal of caller preferences from specification	5.0.0	5.1.0	N1-021359
2002-06	NP-16	NP-020240	137		Substitution of REFER references	5.0.0	5.1.0	N1-021360
2002-06	NP-16	NP-020240	138		Removal of session timer from specification	5.0.0	5.1.0	N1-021361

History

Document history		
V5.1.0	June 2002	Publication