TTC標準
Standard

The difference between TTC JT-Q3401 and ITU-T Q.3401

NGN NNI Signalling Profile (Protocol Set 1)

(The English Edition)

Version 2.0

Published on March 2, 2011

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

TTC Telecommunication Technology Committee

Contents

Introduction

This document provides the English Edition.

In case of dispute, the original to be referred is the Japanese edition of the text.

This document provides the difference between TTC standard JT-Q3401 (Version 2.0, May 27, 2009) and ITU-T Recommendation Q.3401 (March 9, 2007) including Q.3401 Amendment. 1 (February 29, 2008).

・Change History

Version	Date	Outline
1.0	-	Missing Number
2.0	March 2, 2011	published.

・Industrial Property Rights

Information regarding submittal of TTC's "The Policy for the Handling of Industrial Property Rights" is available on TTC's website.

・Responsible working group

Signalling Working Group

TTC JT-Q3401 supplements ITU-T Q.3401 with the following items as annexes and appendices

(a) Clarification on the specifications, network options of the JT-Q3401 main body in order to improve the interoperability between domestic NGN carriers.
This annex shows the clarifications in tables with the corresponding clause number of the main body; follow the content of this annex in addition to the main body. (Annex a)

(b) Clarification of SIP message settings. (Annex b)

(c) Calling line identification presentation (Annex c)

(d) SDP non-transparency in early dialog. (Annex d)

(e) Unallocated number talkie as an example of a guidance/talkie service provided from an originating NGN (Annex e)

(f) Calling-party's category information (Annex f)

(g) Considerations on congestion control (Annex g)

(h) SIP-ISUP interworking rules for number-related information (Annex h)

(i) Fallback procedure on different IP version (Appendix i)

(j) Clarification of connection details when using TCP between NGNs (Appendix ii)

(k) ISUP-to-SIP interworking rules for number portability (Appendix iii)

(l) List of network options covering the whole parts: the main body, annexes and appendices. (Appendix iv)

(m) Signalling rule tables of SIP messages and headers (Appendix v)

(n) Examples of message flows (Appendix vi)

The difference of references between TTC JT-Q3401 and ITU-T Q.3401 is shown in:

Table 1-a/ JT-Q3401: Modifications of references (ITU and ISO/IEC references)

Table 1-b/ JT-Q3401: Modifications of references (IETF references / Service-level signalling specifcations)

Table 1-c/ JT-Q3401: Modifications of references (IETF references / Transport-level specifications)

See “TTC Standard Summary” in TTC Website (http://www.ttc.or.jp/e/) for the summary of difference between TTC standards and referred international standards (ex. ITU-T recommendations).

Table 1-a/ JT-Q3401: Modifications of references (ITU and ISO/IEC references)

Reference in ITU-T Q.3401		Modified reference in TTC JT-Q3401	
[Y.2012]	ITU-T Recommendation Y.2012, Functional requirements and architecture of the NGN release 1.	[TR-1014]	"General overview of NGN architecture", TTC technical report TR-1014, version 1, The Telecommunication Technology Committee, Jun 2006
[Q.761]	ITU-T Recommendation Q.761, Signalling System No. 7 – ISDN User Part functional description	[Q.761]	"ISUP functional description", TTC standard JT-Q761, version 7, The Telecommunication Technology Committee, Apr 2001
[Q.762]	ITU-T Recommendation Q.762, Signalling System No. 7 – ISDN User Part general functions of messages and signals	[Q.762]	"ISUP General Functions of Messages and Signals", TTC standard JT-Q762, version 20, The Telecommunication Technology Committee, May 2002
[Q.763]	ITU-T Recommendation Q.763, Signalling System No. 7 – ISDN User Part formats and codes	[Q.763]	"ISUP formats and codecs", TTC standard JT-Q763, version 21.1, The Telecommunication Technology Committee, Sep 2006
[Q.764]	ITU-T Recommendation Q.764, Signalling System No. 7 – ISDN User Part signaling procedures	[Q.764]	"ISUP Signalling Procedures", TTC standard JT-Q764, version 12, The Telecommunication Technology Committee, May 2002
[T.38]	ITU-T Recommendation T.38 (02/00), Procedures for real-time Group 3 facsimile communication over IP networks	[T.38]	"Procedures for real-time Group 3 facsimile communication over IP networks", TTC standard JT-T38, version 4, The Telecommunication Technology Committee, Jan 2006
[G.711]	ITU-T Recommendation G.711, "Pulse code modulation (PCM) of voice frequencies", 1988	[G.711]	"Pulse Code Modulation (PCM) of Voice Frequencies", TTC standard JT-G711, version 4, The Telecommunication Technology Committee, Apr 2001
[G.722]	ITU-T Recommendation G.722, "7kHz audio-coding within 64kbit/s", 1988	[G.722]	"7 kHz Audio Coding within 64 kbit/s", TTC standard JT-G722, version 2.2, The Telecommunication Technology Committee, Jun 2004
[G.722.1]	ITU-T Recommendation G.722.1, "Low-complexity coding at 24 and 32kbit/s for hands-free operation in systems with low frame loss", 2005	[G.722.1]	"7kHz Audio-coding at 24 and 32 kbit/s for Hands Free Operation in Systems with Low Frame Loss", TTC standard JT-G722.1, version 4, The Telecommunication Technology Committee, Nov 2005
[G.722.2]	ITU-T Recommendation G.722.2, "Wideband coding of speech at around 16kbit/s using Adaptive Multi-Rate Wideband (AMR-WB)", 2003	[G.722.2]	"WIDEBAND CODING OF SPEECH AT AROUND 16 KBIT/S USING ADAPTIVE MULTI-RATE WIDEBAND (AMR-WB))", TTC standard JT-G722.2, version 3.3, The Telecommunication Technology Committee, May 2007
[G.726]	ITU-T Recommendation ITU-T G.726, "40, 32, 24, 16kbit/s Adaptive Differential Pulse Code Modulation (ADPCM)", 1990	[G.726]	"40,32,24,16 kbit/s Adaptive Differential Pulse code Modulation (ADPCM)", TTC standard JT-G726, version 2.1, The Telecommunication Technology Committee, Jun 2005
[G.729]	ITU-T Recommendation G.729, "Coding of speech at 8kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)", 1996	[G.729]	"Coding of Speech at 8kbit/s using Conjugate-Structure Algebraic-Code-Excited Linear-Prediction (CS-ACELP)", TTC standard JT-G729, version 6.1, The Telecommunication Technology Committee, Nov 2006
[G.729A]	ITU-T Recommendation G.729 Annex A, "Reduced complexity 8 kbit/s CS-ACELP speech codec", 1996	[G.729A]	"Reduced complexity 8kbit/s CS-ACELP speech codec", TTC standard JT-G729 Annex A, version 6.1, The Telecommunication Technology Committee, Nov 2006

Table 1-b/ JT-Q3401: Modifications of references (IETF references / Service-level signalling specifcations)

Reference in ITU-T Q.3401		Modified reference in TTC JT-Q3401	
[RFC 2046]	IETF RFC 2046 (1996), Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types	[RFC2046]	"Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", TTC standard JF-IETF-RFC2046, version 1, The Telecommunication Technology Committee, Nov 2007
[RFC 2327]	IETF RFC 2327 (1998), SDP: Session Description Protocol	[RFC2327]	"Session Description Protocol", TTC standard JF-IETF-RFC2327, The Telecommunication Technology Committee, Jun 2005
[RFC 2976]	IETF RFC 2976 (2000), The SIP INFO Method	[RFC2976]	"The SIP INFO Method", TTC standard JF-IETF-RFC2976, The Telecommunication Technology Committee, Nov 2007
[RFC 3087]	IETF RFC 3087 (2001), Control of Service Context using SIP Request-URI	[RFC3087]	"Control of Service Context using SIP Request-URI", TTC standard JF-IETF-RFC3087, The Telecommunication Technology Committee, Nov 2007
[RFC 3204]	IETF RFC 3204 (2001), MIME media types for ISUP and QSIG Objects	[RFC3204]	"MIME media types for ISUP and QSIG Objects", TTC standard JF-IETF-RFC3204, The Telecommunication Technology Committee, Nov 2007
[RFC 3261]	IETF RFC 3261 (2002), SIP: Session Initiation Protocol	[RFC3261]	"Session Initiation Protocol", TTC standard JF-IETF-RFC3261, version 1, The Telecommunication Technology Committee, Jun 2005
[RFC 3262]	IETF RFC 3262 (2002), Reliability of Provisional Responses in the Session Initiation Protocol (SIP)	[RFC3262]	"Reliability of Provisional Responses in SIP", TTC standard JF-IETF-RFC3262, version 1, The Telecommunication Technology Committee, Jun 2005
[RFC 3264]	IETF RFC 3264 (2002), An Offer/Answer Model with the Session Description Protocol (SDP)	[RFC3264]	"An Offer/Answer model with SDP", TTC standard JF-IETF-RFC3264, version 1, The Telecommunication Technology Committee, Jun 2005
[RFC 3265]	IETF RFC 3265 (2002), Session Initiation Protocol (SIP)-Specific Event Notification	[RFC3265]	"Session Initiation Protocol (SIP)-Specific Event Notification", TTC standard JF-IETF-RFC3265, version 1, The Telecommunication Technology Committee, Mar 2007
[RFC 3311]	IETF RFC 3311 (2002), The Session Initiation Protocol (SIP) UPDATE Method	[RFC3311]	"The Session Initiation Protocol UPDATE Method", TTC standard JF-IETF-RFC3311, The Telecommunication Technology Committee, Jun 2005
[RFC 3312]	IETF RFC 3312 (2002), Integration of Resource Management and Session Initiation Protocol (SIP)	[RFC3312]	"Integration of Resource Management and Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3312, The Telecommunication Technology Committee, Nov 2007
[RFC 3323]	IETF RFC 3323 (2002), A Privacy Mechanism for the Session Initiation Protocol (SIP)	[RFC3323]	"A Privacy Mechanism for the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3323, The Telecommunication Technology Committee, Jun 2005
[RFC 3324]	IETF RFC 3324 (2002), Short Term Requirements for Network Asserted Identity	[RFC3324]	"Short Term Requirements for Network Asserted Identity", TTC standard JF-IETF-RFC 3324, version 1, The Telecommunication Technology Committee, Jun 2005
[RFC 3325]	IETF RFC 3325 (2002), Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks	[RFC3325]	"Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", TTC standard JF-IETF-RFC3325, The Telecommunication Technology Committee, Jun 2005
[RFC 3326]	IETF RFC 3326 (2002), The Reason Header Field for the Session Initiation Protocol (SIP)	[RFC3326]	"The Reason Header Field for the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3326, The Telecommunication Technology Committee, Jun 2005
[RFC 3398]	IETF RFC 3398 (2002), Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping	[RFC3398]	"Technical Specification on SIP to TTC ISUP Interworking", TTC standard JF-IETF-RFC3398, The Telecommunication Technology Committee, Jun 2005
[RFC 3420]	IETF RFC 3420 (2002), Internet Media Type message/sipfrag	[RFC3420]	"Internet Media Type message/sipfrag", TTC standard JF-IETF-RFC3420, The Telecommunication Technology Committee, Nov 2007
[RFC 3428]	IETF RFC 3428 (2002), Session Initiation Protocol (SIP) Extension for Instant Messaging	[RFC3428]	"Session Initiation Protocol (SIP) Extension for Instant Messaging, TTC standard JF-IETF-RFC3428, The Telecommunication Technology Committee, Sep 2006
[RFC 3455]	IETF RFC 3455 (2003), Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)	[RFC3455]	"Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)", TTC standard JF-IETF-RFC3455, The Telecommunication Technology Committee, Mar 2007
[RFC 3515]	IETF RFC 3515 (2003), The Session Initiation Protocol (SIP) Refer Method	[RFC3515]	"The Session Initiation Protocol (SIP) Refer Method", TTC standard JF-IETF-RFC3515, The Telecommunication Technology Committee, Mar 2007
[RFC 3824]	IETF RFC 3824 (2004), Using E.164 numbers with the Session Initiation Protocol (SIP)	[RFC3824]	"Using E.164 numbers with the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3824, The Telecommunication Technology Committee, Nov 2007
[RFC 3840]	IETF RFC 3840 (2004), Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)	[RFC3840]	"Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3840, The Telecommunication Technology Committee, Nov 2007

[RFC 3841]	IETF RFC 3841 (2004), Caller Preferences for the Session Initiation Protocol (SIP).	[RFC3841]	"Caller Preferences for the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3841, The Telecommunication Technology Committee, Nov 2007
[RFC 3891]	IETF RFC 3891 (2004), The Session Initiation Protocol (SIP) Replaces Header	[RFC3891]	"The Session Initiation Protocol (SIP) "Replaces" Header", TTC standard JF-IETF-RFC3891, The Telecommunication Technology Committee, Nov 2007
[RFC 3892]	IETF RFC 3892 (2004), The Session Initiation Protocol (SIP) Referred-By Mechanism	[RFC3892]	"The Session Initiation Protocol (SIP) Referred-By Mechanism", TTC standard JF-IETF-RFC3892, The Telecommunication Technology Committee, Mar 2007
[RFC 3893]	IETF RFC 3893 (2004), Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format	[RFC3893]	"Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format", TTC standard, JF-IETF-RFC3893, The Telecommunication Technology Committee, Nov 2007
[RFC 3911]	IETF RFC 3911 (2004), The Session Initiation Protocol (SIP) Join Header	[RFC3911]	"The Session Initiation Protocol (SIP) "Join" Header", TTC standard JF-IETF-RFC3911, The Telecommunication Technology Committee, Nov 2007
[RFC 3959]	IETF RFC 3959 (2004), The Early Session Disposition Type for the Session Initiation Protocol (SIP)	[RFC3959]	"The Early Session Disposition Type for the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3959, The Telecommunication Technology Committee, Nov 2007
[RFC 3960]	IETF RFC 3960 (2004), Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)	[RFC3960]	"Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3960, The Telecommunication Technology Committee, Aug 2006
[RFC 3966]	IETF RFC 3966 (2004), The tel URI for Telephone Numbers	[RFC3966]	"The tel URI for Telephone Numbers", TTC standard JF-IETF-RFC3966, The Telecommunication Technology Committee, Jun 2005
[RFC 4028]	IETF RFC 4028 (2005), Session Timers in the Session Initiation Protocol (SIP)	[RFC4028]	"Session Timers in the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC4028, The Telecommunication Technology Committee, Aug 2005
[RFC 4032]	IETF RFC 4032 (2005), Update to the Session Initiation Protocol (SIP) Preconditions Framework	[RFC4032]	"Update to the Session Initiation Protocol (SIP) Preconditions Framework", TTC standard JF-IETF-RFC4032, The Telecommunication Technology Committee, Nov 2007
[RFC 4035]	IETF RFC 4235 (2005), An INVITE Initiated Dialog Event Package for the Session Initiation Protocol (SIP)	[RFC4235]	"An INVITE Initiated Dialog Event Package for the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC4235, The Telecommunication Technology Committee, Nov 2007
[IETF RFC 4145]	IETF RFC 4145 (2005), TCP-Based Media Transport in the Session Description Protocol (SDP)	[RFC4145]	"TCP-Based Media Transport in the Session Description Protocol (SDP)", TTC standard JF-IETF-RFC4145, The Telecommunication Technology Committee, Mar 2007
[RFC 4244]	IETF RFC 4244 (2005), An Extension to the Session Initiation Protocol (SIP) for Request History Information	[RFC4244]	"An Extension to the Session Initiation Protocol (SIP) for Request History Information", TTC standard JF-IETF-RFC4244, The Telecommunication Technology Committee, Aug 2006
[RFC 4412]	IETF RFC 4412 (2006), Communications Resource Priority for the Session Initiation Protocol (SIP)	[RFC4412]	"Communications Resource Priority for the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC4412, The Telecommunication Technology Committee, Nov 2007
[RFC 4458]	IETF RFC 4458 (2006), Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)	[RFC4458]	"Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)", TTC standard JF-IETF-RFC4458, The Telecommunication Technology Committee, Aug 2006
[RFC 4483]	IETF RFC 4483 (2006), A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages	[RFC4483]	"A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages", TTC standard JF-IETF-RFC4483, The Telecommunication Technology Committee, Nov 2007
[RFC 4566]	IETF RFC 4566 (2006), SDP: Session Description Protocol	[RFC4566]	"SDP: Session Description Protocol", TTC standard JF-IETF-RFC4566, The Telecommunication Technology Committee, Mar 2007
[RFC 4694]	IETF RFC 4694 (2006), Number Portability Parameters for the "tel" URI	[RFC4694]	"Number Portability Parameters for the "tel" URI", TTC standard JF-IETF-RFC4694, The Telecommunication Technology Committee, Nov 2007

Table 1-c/ JT-Q3401: Modifications of references (IETF references / Transport-level specifications)

Reference in ITU-T Q.3401		Modified reference in TTC JT-Q3401	
[RFC 2833]	IETF RFC 2833 (2000), RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals	[RFC2833]	"RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals", TTC standard JF-IETF-RFC2833, The Telecommunication Technology Committee, Jun 2006
[IETF RFC 3016]	IETF RFC 3016 (2000), RTP Payload Format for MPEG-4 Audio/Visual Streams.	[RFC3016]	"RTP Payload Format for MPEG-4 Audio/Visual Streams", TTC standard JF-IETF-RFC3016, The Telecommunication Technology Committee, May 2009
[RFC 3267]	IETF RFC 3267 (2002), Real-time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Codecs	[RFC3267]	"Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs", JF-IETF-RFC3267, The Telecommunication Technology Committee, Nov 2007
[RFC 3389]	IETF RFC 3389 (2002), Real-time Transport Protocol (RTP) Payload for Comfort Noise (CN).	[RFC3389]	"RTP Payload for Comfort Noise", TTC standard JF-IETF-RFC3389, The Telecommunication Technology Committee, Nov 2007
[RFC 3550]	IETF RFC 3550 (2003), RTP: A Transport Protocol for Real-Time Applications.	[RFC3550]	"RTP: A Transport Protocol for Real-Time Applications", TTC standard JF-IETF-STD64, The Telecommunication Technology Committee, May 2005
[RFC 3551]	IETF RFC 3551 (2003), RTP Profile for Audio and Video Conferences with Minimal Control.	[RFC3551]	"RTP Profile for Audio and Video Conferences with Minimal Control", TTC standard JF-IETF-STD65, The Telecommunication Technology Committee, Jun 2005
[IETF RFC 3711]	IETF RFC 3711 (2004), The Secure Real-time Transport Protocol (SRTP).	[RFC3711]	"The Secure Real-time Transport Protocol (SRTP)", TTC standard JF-IETF-RFC3711, The Telecommunication Technology Committee, May 2009
[IETF RFC 3984]	IETF RFC 3984 (2005), RTP Payload Format for H.264 Video.	[RFC3984]	"RTP Payload Format for H.264 Video", TTC standard JF-IETF-RFC3984, The Telecommunication Technology Committee, May 2009
[RFC 4103]	IETF RFC 4103 (2005), RTP Payload for Text Conversation.	[RFC4103]	"RTP Payload for Text Conversation", TTC standard JF-IETF-RFC4103, The Telecommunication Technology Committee, Nov 2007
[IETF RFC 4629]	IETF RFC 4629 (2007), RTP Payload Format for ITU-T Rec. H.263 Video.	[RFC4629]	"RTP Payload Format for ITU-T Rec. H.263 Video", TTC standard JF-IETF-RFC4629, The Telecommunication Technology Committee, May 2009

Annex a. Clarification and option lists of JT-Q3401 main body

(This annex is a normative part of this standard.)

a.1. Overview

This annex provides clarification and option lists of the JT-Q3401 main body to improve the interoperability between domestic NGN carriers.

a.2. Clarification and option lists

Annex Table a-1 shows the clarification and option lists of TTC JT-Q3401. Clauses unmentioned in the table mean that specifications in the base document are applied as they are. Lists of options described in Annex b to Annex h and Appendix i to Appendix iii are not shown in Annex Table a-1. Refer to Appendix iv for lists of options including these annexes and appendices.

Annex Table a-1/ JT-Q3401: Clarification and option lists

Clause of JT-Q3401 main body		Clarifications	Options	Remarks
No.	Name of clause			
2.	References	References needed for this standard are described in each annex and appendix in addition to the base document.	–	
6.	Assumptions	6. MIME encapsulated ISUP information is not used.	–	
7.	Media availability in a SIP session	For SDP non-transparency in early dialog, follow Annex d b) Even in the case metered billing is used, when a *1xx* response to *INVITE* includes SDP answer, media packets from the originating network to the terminating network is allowed, and media packets from the terminating network to the originating network is also allowed as specified in Annex d.3.2.3.	–	
8.1	Codec list	The audio codec list shall contain G.711μ-law. Even when a codec in the codec list is set in an SDP offer, it may not be end-to-end negotiation, depending on a carrier's policy. A codec that is not contained in the codec list is not to be set in an SDP offer.	Codecs to be contained in the codec list other than G.711μ-law. (Appendix Table iv-8, Items 1 to 3)	
8.2	Packetization size	In the case there is no negotiation of packetization period using SDP, 20ms is used for the packetization period for G.711μ-law.	–	
9.	Routing and addressing	For the URI format in the case of using a global E.164 number, follow Annex b.3. For the subaddress, follow Annex b.5	Use of SIP-URI other than a global E.164 number in Request-URI outside existing dialogs. (Appendix Table iv-3, Item 1)	
10.1	RFCs to be supported	Follow the concept of Trust domain specified in RFC3324. RFC2976, RFC3204, RFC3398,	The followings are the list of options for each RFC. [RFC2046]	

		RFC3824, RFC3893, RFC3959, RFC3960, RFC4235, RFC4412, and RFC4483 are not to be used. Note: To support RFCs means to follow the contents described in the RFCs. It does not mean that their capabilities are used in all sessions.	Use of MIME Multipart (Appendix Table iv-13, Items 1 and 2) [RFC3265] Use of *SUBSCRIBE* method and *NOTIFY* method. (Appendix Table iv-2, Items 3 and 6) [RFC3311] SDP offer by *UPDATE* (Appendix Table iv-12, Item 2) Media modification in early dialog (Appendix Table iv-12, Item 3) [RFC3312, RFC4032] Use of function for reserving bandwidth before session establishment (*precondition*) (Appendix Table iv-9, Item 5) [RFC3428] Use of *MESSAGE* method (Appendix Table iv-2, Items 1 and 2) [RFC3455] Use of headers for inter-carrier charging (*P-Charging-Vector*, *P-Charging-Function-Addresses*) (Appendix Table iv-16, Item 1) [RFC3515, RFC3892] Use of *REFER* method (Appendix Table iv-2, Items 4 and 5) [RFC3840, RFC3841] Use of terminal capabilities notification function (*pref*) (Appendix Table iv-9, Item 6) [RFC3891] Use of dialog replacement function (*replaces*) (Appendix Table iv-9, Item 3) [RFC3911] Use of conference session participation function (*join*) (Appendix Table iv-9, Item	

			4) [RFC4028] Session update by *UPDATE* method (Appendix Table iv-10, Item 1) [RFC4244] Use of request history retention function (*histinfo*) (Appendix Table iv-9, Item 7) [RFC4694] Use of "*rn*" parameter and "*npdi*" parameter (Appendix Table iv-15, Item 1)	
10.2.1.7	SIP messages	For maximum length of SIP messages and its elements, follow Annex b.3	–	
10.2.1.7.1	Requests	*REGISTER* method and *OPTIONS* method are not used. SIPS-URI is not to be used.	–	
10.2.1.7.4.1	Message body types	Specifications in the base document are applied as they are.	SDP settings for *PRACK* and *200OK* to *PRACK*. (Appendix Table iv-12, Item 1)	
10.2.1.8.1.3.	Processing responses	Authentication procedures for a request outside existing dialogs are not used.	–	
10.2.1.8.3	Redirect servers	Specifications in the base document are applied as they are.	Use of redirect functions by *3xx* response (Appendix Table iv-14, Item 1)	
10.2.1.10	Registrations	Registrations are not supported.	–	
10.2.1.11	Querying for capabilities	Querying for capabilities is not supported.	–	
10.2.1.12.1	Creation of a dialog	SIPS-URI is not to be used.	–	
10.2.1.12.2	Requests within a dialog	SIPS-URI is not to be used.	–	
10.2.1.13	Initiating a session	Initial *INVITE* includes an SDP offer. (SDP negotiation using *2xx*/*ACK* is not to be used.) Follow Annex g for congestion control.	Use of early media when *100rel* is not used. (Appendix Table iv-11, Item 1)	
10.2.1.14	Modifying an existing session	In the case of using re-*INVITE*, SDP offer is set in *INVITE* request.	Media modification after a dialog is established. (Appendix Table iv-12, Item 4)	
10.2.1.19	Common message components	SIPS-URI is not to be used.	–	
10.2.1.20.10	Contact	When a new destination is a telephone number, the *Contact* header in *3xx* response has either SIP-URI or TEL-URI with the new destination number.	–	
10.2.1.20.11	Content-Disposition	Only the default value can be set in the parameter of *Content-Disposition* header. Early media by application server model is not provided.	–	

10.2.1.20.15	Content-Type	Early media by application server model is not provided.	–	
10.2.1.20.24	MIME-Version	Only "1.0" is supported.	–	
10.2.1.20.32	Require	Early media by application server model is not provided.	Use of *timer*, *100rel*, and other SIP option tags (Appendix Table iv-9, Items 1 to 8)	
10.2.1.20.37	Supported	Early media by application server model is not provided.	–	
10.2.1.20.39	To	Either TEL-URI or SIP-URI is set for *To* header.	–	
10.2.1.22	Usage of HTTP authentication	HTTP Authentication is not supported.	–	
10.2.1.23	S/MIME	In the case of handling SDP information for call processing message related to *INVITE*, S/MIME is not used.	–	
10.2.2.2.2	P-Asserted-Identity	*P-Asserted-Identity* header is used only for requests and responses outside existing dialogs. For calling-party's category described in *P-Asserted-Identity* header, follow Annex f.	–	
10.2.2.2.4	Privacy	*Privacy* header is used only in requests and responses outside existing dialogs. Only "*id*" and "*none*" can be used for privacy options. For calling line identification presentation, follow Annex c.	–	
10.2.2.2.6	Reason	*Reason* header is supported for both directions, sending and receiving. When providing unallocated number talkie, follow Annex e.	–	
10.2.3	Summary of SIP methods and headers	*REGISTER* and *OPTIONS* are not to be used.	SIP methods to be used (Appendix Table iv-2, Items 1 to 7)	
10.3	SDP profile	Specifications in the base document are applied as they are.	SDP lines to be used (Appendix Table iv-6, Item 1) IP version to be used for media (Appendix Table iv-4, Item 2) Use of video (*m=video*) and data communication (*m=application*, *m=data*, etc.) (Appendix Table iv-7, Items 1 and 2) Use of TCP for media (Appendix Table iv-7, Item 3) Use of bandwidth control (Appendix Table iv-7, Item 4)	

12	Call control signalling transport	SCTP is not used. Refer to Appendix ii for a note of TCP connection.	Transport layer protocol type to be used (Appendix Table iv-5, Items 1 and 2)	
13	IP protocol version	Specifications in the base document are applied as they are. Refer to the Appendix i for a note of IPv4/IPv6 fallback.	Use of IPv6 in call control signals (Appendix Table iv-4, Item 1)	
Appendix A.	Call/signalling flows	1. For PSTN-IP-(NNI)-IP-PSTN connection, PSTN transit connection (a transit connection of a single call, except caused by the transfer of a call) is not applicable. For clause I.4.4, early media by application server model is not provided.	–	
Others		For SIP-ISUP interwork, refer to Annex h and Appendix iii.	–	

Annex b. SIP message settings

(This annex is a notmative part of this standard.)

b.1. Overview

This annex clarifies SIP message settings.

b.2. References

References used in this annex are as follows.

[TS-1008] "Technical Specification on ISDN Called Party Subaddress Information Transferring through Provider's SIP Networks", TTC standard TS-1008, version 1, The Telecommunication Technology Committee, Jun 2004.

[RFC4715] "The Integrated Services Digital Network (ISDN) Subaddress Encoding Type for tel URI", TTC standard JF-IETF-RFC4715, version 1, The Telecommunication Technology Committee, Mar 2007.

b.3. URI formats in the case of using global E.164 number

b.3.1. Format of destination number

The destination number using a global E.164 number is set in the *Request-URI* of a request outside existing dialogs as information used to route the call between NGNs. The URI format other than a global E.164 number can be used as well. [Appendix Table iv-3, Item 1]

The *Request-URI* of a request outside existing dialogs is a SIP-URI or TEL-URI, which is defined as follows:

b.3.1.1. telephone-subscriber part in Request-URI

When requesting the routing by the destination number using a global E.164 number for the request outside existing dialogs, either a SIP-URI of global-number format with the *telephone-subscriber* part or TEL-URI of *global-number* format with the *telephone-subscriber* part is set in a *Request-URI*. Note that *visual-separator* is not to be used for the description of *global-number*. On the basis of this, the format corresponding to a destination number as defined by JJ-90.10 is shown in Annex Table b-1.

When the global number includes a parameter part (anything preceded by a semicolon), the routing is processed according to the destination number even when the contents of this parameter part cannot be recognized.

It is RECOMMENDED to support "*npdi*" parameter and "*rn*" parameter defined in [RFC4694] for the purpose of number portability.

Annex Table b-1/JT-Q3401: Destination number representation format

Format	Conditions	Application
+ [Country code] [National number]	Any country code except 81, up to 15 digits	International network calls
+81ABCDEFGHJ	A and B must not be 0	Regional fixed-line phone calls, IP phone calls (Category A)
+81A0CDEFGHJK	A=2, 7, 8, 9, and C must not be 0	Mobile/PHS/wireless pager calls
+8150CDEFGHJK	C must not be 0	IP phone calls (Category B)

b.3.1.2. hostport part

The *hostport* part of the SIP-URI set in the *Request-URI* of a request outside existing dialogs is set to the name of the domain name or the host name (including the IP address format) defined by the NGN to which the connection is made. The specific settings of the *hostport* part is decided upon between the connecting carriers. [Appendix Table iv-3, Items 2 and 3]

b.3.1.3. Option URI parameter part

The terminating NGN ignores the option URI parameter of the SIP-URI set in the *Request URI* of a request message outside existing dialogs that the terminating NGN is unable to understand during the processing of it.

b.3.2. Functions relating to dialed numbers in the calling carrier's network

In the case that the calling carrier's network requests routing by the destination number in the request outside existing dialogs, it should be able to be configured with the valid number of received digits (which should be in the range between the minimum number of received digits and the maximum number of received digits) in the *telephone-subscriber* part of a valid *Request-URI*, and if the minimum number of digits is not met, then a disconnection process should be performed inside the calling carrier's network. When the maximum number of digits is exceeded, the behaviours related to the connection are not guaranteed. However, the minimum and maximum numbers of digits should be determined between carriers. [Appendix Table iv-3, Item 4]

b.4. Maximum SIP message string lengths

The maximum allowed lengths of SIP message elements transmitted between NGNs are shown in Annex Table b-2.

Annex Table b-2/JT-Q3401: Maximum message setting lengths

Element	Maximum length	
	When using UDP	When using TCP
Maximum length of one line	255 bytes (including CRLF)	(Note 3)
Maximum entries of the same header	5 lines (Note 1)	(Note 3)
Maximum length of message body	1000 bytes	(Note 3)
Overall message length	1300 bytes or less (Note 2)	(Note 3)

Note 1: The number of *Record-Route* elements is 5 entries for a request, and 10 entries for a response. The number of *Route* and *Via* elements is 5 entries.
Note 2: Conforms to [RFC3261].
Note 3: Follows the bilateral agreement. [Appendix Table iv-17]

b.5. Subaddress

NGN carriers may provide their users with services that are equivalent to services realized by the transfer of subaddress information that can be provided in the ISUP network through the interconnection interface as defined in JJ-90.10. [Appendix Table iv-18]

This clause and the following subclauses show the usage of subaddress information in SIP messages based on [TS-1008] and complement the standard. The network which handle subaddress information are required to follow this clause and its subclauses. As for [TS-1008], follow the specifications for Interface A in [TS-1008]. In referring to the specifications of [TS-1008], "called party subaddress" should be read as "calling and called subaddress", and "providers' SIP network" as "NGN".

b.5.1. Content of subaddress information

The subaddress is a numeric string of 19 digits or less using numbers 0 to 9. The details are based on [RFC4715] and [TS-1008].

b.5.2. Formats of subaddress information

Subaddress information is applied to all the requests and responses of SIP messages, and may be set in the headers that show the originating party (*From*, *P-Asserted-Identity*), the header that shows the terminating party (*To*), and *Request-URI*. Subaddress is expressed as a numeric string following a semicolon(;) and "isub=" of SIP URI or TEL URI.

Annex c. Calling line identification presentation

(This annex is a notmative part of this standard.)

c.1. Overview

This annex describes the procedures for calling line identification presentation.

c.2. Handling calling-party identity

Calling line identification presentation should be realized based on [RFC3323], [RFC3324], and [RFC3325] by transmitting network-asserted user identity information and presentation/restriction information as specified in this annex.

This annex defines terms, network-asserted user identity information, and presentation/restriction information used for calling line identification presentation as follows:

<Network-asserted user identity information>

In a trusted network, information describing the identity of a user that is asserted by the network through authentication or other means (or verified by the network if provided by the user). An example of network-asserted user identity information is an E.164 number that is reachable to the user. Note that subaddress information provided by SIP UA may be included.

<Presentation/Restriction information>

Information specifying whether a user is allowing or prohibiting the presentation of its network-asserted user identity information to another user receiving a signalling message.

(1) The calling-party identity is delivered in a request outside existing dialogs (*INVITE*, *MESSAGE*, *SUBSCRIBE*, or *REFER* request that is outside existing dialogs).

(2) The calling-party identity is set in each parameter value of the *P-Asserted-Identity header*. This header must always be set in a request outside existing dialogs.

(3) For data elements associated with the handling of the calling-party identity, use parameters defined in Annex Table c-1 and conform to the presentation conditions in Annex Table c-2.

Annex Table c-1/JT-Q3401: Information component associated with the handling of calling-party identity

1)	SIP_URI	Network-asserted user identity that is reachable from the NGN. The *addr-spec* part of the SIP_URI in the *P-Asserted-Identity* header of a request outside existing dialogs is taken as the "SIP_URI."
2)	SIP_DISPLAYNAME	Network-asserted user identity information component linked with the SIP_URI and consisting of information other than a number to be displayed to the called user. The display-name part of the SIP_URI in the *P-Asserted-Identity* header of a request outside existing dialogs, which is character strings composed only of UTF-8 code , is taken as the "SIP_DISPLAYNAME." When it is enclosed in quotation marks, the "SIP_DISPLAYNAME" is taken to be the text left after these quotation marks have been removed. Omission of the SIP_DISPLAYNAME information component indicates that a display format different from the SIP_URI is not particularly desired. This case must be interpreted as an indication that the SIP_URI character string SHOULD be used for display in the NGN as long as no special restrictions exist.
3)	TEL_URI	Network-asserted user identity information component consisting of a E.164 number reachable from the Global Switched Telephone Network (GSTN) The content of the telephone-subscriber part of TEL URI in the *P-Asserted-Identity* header of a request outside existing dialogs is taken as

		the "TEL_URI." Omission of the TEL_URI information component indicates that the calling user has no E.164 number for receiving incoming calls.
4)	TEL_DISPLAYNAME	Network-asserted user identity information component consisting of a dial number by which the calling user can be reached based on a numbering plan The display-name part of the TEL URI in the *P-Asserted-Identity* header of a request outside existing dialogs is taken as the "TEL_DISPLAYNAME." When it is enclosed in quotation marks, the "TEL_DISPLAYNAME" is taken to be the text left after these quotation marks have been removed. Omission of the TEL_DISPLAYNAME information component indicates that a dial number different from the number indicated by the TEL_URI information component is not particularly desired, or that accurate information pertaining to the dialing numbering plan that can be used by the terminating user is not held. In this case, the TEL_URI character string SHOULD be interpreted as the TEL_DISPLAYNAME information component as long as no special restrictions exist.
5)	Privacy	Presentation/restriction information that identifies the status of whether the network-asserted user identity information is presentable to the called user or not. The content of the *Privacy* header of a request outside existing dialogs is taken as the "Privacy."

Annex Table c-2/JT-Q3401: Conditions for notifying calling-party identity

Data item	Mapping condition	Notes
Calling-party's number (subscriber number)	TEL_URI	Used as a number identifying the originating user. Visual separator is not used. Specific setting contents are shown in Annex Table c-3.
Generic number (notified number)	TEL_DISPLAYNAME	Used when a number other than the calling-party identity is notified to the terminating user. Visual separator is not used. Specific setting contents are shown in Annex Table c-4.
Presentation/ restriction	Privacy	"*none*" = displayable, "*id*" = not displayable. Parameters other than "*none*" and "*id*" are not set. Assumed to be displayable when the *Privacy* header itself is not set. When the calling-party's number (subscriber number) and generic number (notified number) are both set, this item is handled as the displayable / hidden status of the general purpose number (notified number), and the calling number (subscriber number) is uniformly handled as hidden.
Cause of no ID	SIP_DISPLAYNAME	Character strings composed of only UTF-8 code. When the presentation/restriction information is restriction, character strings in Annex Table c-5 can be used to show the cause. If this item is not set, or if its contents are unidentified, the call is taken to be impossible for an undisclosed reason, which is taken to be equivalent to "Unavailable".

Annex Table c-3/JT-Q3401: TEL_URI format

TEL_URI	Condition	Number digit	Use
+country-code National-Number	Any country code except 81	Max. 15 digits	Originating call on international network (overseas)
+81ABCDEFGHJ	A and B are both non-zero	10 or 11 digits	Originating call on local fixed telephone network Originating call on IP phone (Category A)
+81A0CDEFGHJK	A is 7, 8, or 9, and C is non-zero.	12 digits	Originating call on mobile/PHS network
+8150CDEFGHJK	C is non-zero	12 digits	Originating call on IP phone (Category B)

Annex Table c-4/JT-Q3401: TEL_DISPLAYNAME format

TEL_DISPLAYNAME	Condition	No. of Digits	Use
010 country-code National-Number	Any country code except 81	Max. 18 digits	Originating call on international network (overseas)
0ABCDEFGHJ	A, B, and C are each non-zero	9 or 10 digits	Originating call on local fixed telephone network Originating call on IP phone (category A)
0A0CDEFGHJK	A is 7, 8, or 9	11 digits	Originating call on mobile/PHS network
0AB0~	A and B are both non-zero		Logical number
050CDEFGHJK	C is not 0	11 digits	Originating call on IP phone (category B)
Free Format			Operator-originating call, etc.

Annex Table c-5/JT-Q3401: Character strings indicating reason for Restriction of SIP_DISPLAYNAME

SIP_DISPLAYNAME	Meaning
Unavailable	No caller ID: service unavailable
Anonymous	No caller ID: rejected by user
Interaction with other service	No caller ID: service conflict
Coin line/payphone	No caller ID: call from public telephone

Annex d. SDP non-transparency in early dialog

(This annex is a notmative part of this standard.)

d.1. Overview

This annex defines SDP non-transparency in early dialog. This annex may not be applied depending on the results of what items of option lists to select (e.g., use of precondition, etc.).

d.2. Guidance/talkie services

Guidance/talkie services may be provided by the originating NGN or by the terminating NGN.

d.2.1. Guidance/talkie services from the terminating NGN

It is conceivable that guidance/talkie services might be provided from the terminating NGN through an early dialog or confirmed dialog.

Guidance/talkie services provided from the terminating NGN on the basis of an early dialog are realized by adding SDP information to a *18x* response. From the viewpoint of preventing illegally non-charged calls in the early dialog, the terminating NGN must manage and examine the SDP information of audio RTP source in *18x* responses and can return *18x* responses only when the SDP information is trusted. The terminating NGN must not return *18x* responses from the called terminal if the response contains SDP information.

Similarly, guidance/talkie services provided in a confirmed dialog from the terminating NGN are handled as normally connected calls (successful calls) at the calling carrier's side.

d.2.2. Guidance/talkie services from the calling NGN

To provide guidance/talkie services, the originating NGN may use the status codes of responses returned from the terminating NGN. When the terminating NGN sends back a response including a status code used in guidance/talkie services, the contents of this response must be guaranteed to avoid unexpected connections to guidance/talkie services. The status codes that are used should be agreed upon between the connecting carriers. [Appendix Table iv-19]

d.3. Connections for RTP audio sent out from the network before call establishment

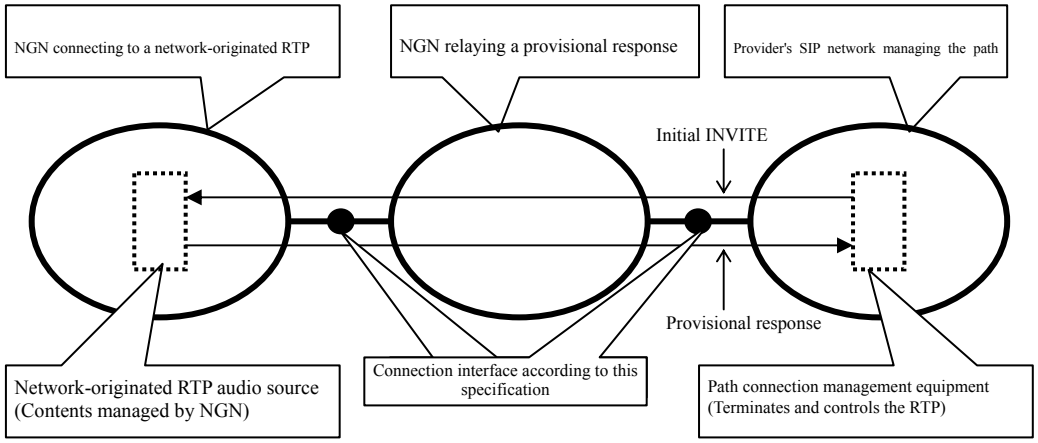
In the establishment of voice calls through existing GSTN, the network sometimes connects an unsuccessful call to an announcement service at the terminating network or at a transit network in order to provide the originating user with a voice message to notify why the call was unsuccessful. In a GSTN, a voice path from the terminating user to the originating user is normally connected before call establishment, so audio inserted by the network can be heard by the originating user even before the call is completed.

Since it may be possible to send out RTP audio from the terminal in connections between NGNs when the called user terminal is not controlled by the network, path connections are sometimes prohibited before normal call establishment, either in the calling network or a transit network, in order to prevent illegal use of the network. In this case, to establish announcement connections in the network, it is necessary to prepare some kind of mechanism whereby paths can still be connected before call establishment.

This clause states the requirements that NGNs must satisfy to allow network-originated RTP audio to be connected to the originating user before call establishment via a connection interface based on this annex.

d.3.1. A model of network-originated RTP audio

A connection model of an NGN related to network-originated RTP audio is shown in Fig. d.



* NGN relaying a provisional response may not exist in some connection systems.

* NGN relaying a provisional response may be Provider's SIP network managing the path connection before call establishment on the other hand.

Fig. d/JT-Q3401: Connection model of an NGN related to network-originated RTP audio

The classes of NGNs that play a role in network-originated RTP audio connections in the above model are described below. It should be pointed out that these are logical classes whose roles may change depending on the call being connected. Also, in calls that are actually connected, an NGN must be capable of undertaking multiple roles simultaneously, and the roles themselves may be omitted if not required.

<NGN connecting to a network-originated RTP>

An NGN that connects to a network-managed RTP audio source before call establishment with regard to an Initial *INVITE* request received via a connection interface conforming to this annex. Responsible for the content of the audio source connected before call establishment.

In practice, this corresponds to an NGN that performs connections according to conditions by preparing network-originated announcements such as congestion talkies.

<NGN that relays provisional responses>

An NGN that transmits a corresponding Initial *INVITE* request from a connection interface according to this annex in response to a call where an Initial *INVITE* request is received from a connection interface according to this annex.

<NGN that manages path connections before call establishment>

An NGN that manages a call where an Initial *INVITE* request is received from a connection interface according to this annex so that no audio path is connected from the terminating user to the originating user before call establishment. An NGN that manages path connections before call establishment must manage equipment that terminates RTP voice traffic from the terminating network. Equipment that can be used to manage these path connections includes MGs (media gateways) that connect with GSTNs, and SBCs (session border controllers) that terminate RTP packets in a network.

d.3.2. Overview of behaviours relating to network-originated RTP audio

This clause shows the behavioural provisions required of NGNs that have each of the roles of the behaviours of NGNs in relation to network-originated RTP audio. The NGN behaviours mentioned here are not applied to all the calls handled by an NGN, and whether or not they are applied to each call is judged according to conditions such as whether or not the path connection of the connected call is permitted.

d.3.2.1. Behaviours of originating NGN of network-originated RTP before call establishment

The following supplementary specification is applied to the *180 (Ringing)* and *183 (Session Progress)* responses:

An NGN that transmits a response can send additional SDP information only when the contents of the audio included in the RTP sent out to the carrier that receives the response can be managed and guaranteed.

Accordingly, when an NGN that has received an Initial *INVITE* request via an interface conforming to this annex establishes a network-originated RTP audio connection before call establishment, an SDP must be included in the *180 (Ringing)* or *183 (Session Progress)* response sent out in order to establish the RTP connection only when the contents of the audio included in the RTP sent out to the carrier that receives the response can be managed and guaranteed.

Also, when there is a possibility of receiving an SDP from an entity that is unable to guarantee the contents of a connected RTP due to the circumstances of the network configuration or terminal management[1], one of the following behaviours must be taken with messages received from such an entity.[2].

1. Delete the SDP and issue a corresponding response.
2. Issue a message including a corresponding response to the corresponding SDP, but make sure the RTP from the terminating user is not transferred to the originating user.

When adopting method (1), in cases where processing is performed based on a *100rel* extension an SDP may not be included in any *200 (OK)* response that might subsequently be issued. Accordingly, in an NGN that deletes the SDP, the contents of the deleted SDP must be recorded, and when there is no SDP included in *200 (OK)* response, it must be made possible to send a response that includes a corresponding SDP that would have been produced if the recorded SDP had been received.

When adopting method (2), it must be ensured that the terminating user is not made aware of the address and port information included in the SDP included in the received Initial *INVITE* request[3].

d.3.2.2. Behaviours of an NGN that relays provisional responses

In cases where an NGN receives an Initial *INVITE* request via an interface conforming to this annex, and a corresponding Initial *INVITE* request is sent via an interface conforming to this annex, when a *180 (Ringing)* or *183 (Session Progress)* response including an SDP is received, the *180 (Ringing)* or *183 (Session Progress)* response that is triggered by receiving a corresponding response and is sent out via the interface must include an SDP.

Note that an NGN that relays a provisional response may at the same time be an NGN that manages path connections before call establishment.

---

[1] This condition includes cases where it is possible for transmissions to be made by a subscriber who is performing unexpected actions (possibly with ill intent) outside the framework normally envisaged by the carrier.

[2] In an NGN that is the origin of requests (i.e., the destination of responses) as seen from an NGN, when it is guaranteed that there is no NGN managing the connection of paths before call completion, measures should be taken from the viewpoint of ensuring normality and expandability of connections between the NGNs even when the countermeasures mentioned here are not taken and there is no specific problem of illegal use or the like.

[3] In this case, it may be necessary for the NGN to have a function that terminates an RTP, such as an SBC (Session Border Controller).

d.3.2.3. Behaviours of an NGN that manages path connections before call establishment

When an NGN that has to prohibit audio path connections from terminating users before call establishment receives a *180 (Ringing)* or *183 (Session Progress)* response including an SDP in response to an Initial *INVITE* request transmitted via an interface conforming to this annex, it must judge that it contains no audio that is unsuitable for connection before call establishment, and establish a path connection from the terminating user to the originating user.

Annex e. Unallocated (unassigned) number talkie

(This annex is a notmative part of this standard.)

e.1. Overview

An unallocated (unassigned) number talkie is a guidance/talkie service provided from an originating NGN when establishing an interconnection between NGNs. This annex desccribes the functions and behaviours of the NGN that are required when providing a unallocated (unassigned) number talkie service.

e.2. Procedures for providing an unallocated (unassigned) number talkie service

As a rule, the following conditions should be observed when connecting to an unallocated (unassigned) number talkie.

- The unallocated (unassigned) number talkie returns a response indicating the unallocated number from the terminating NGN to the originating NGN, and a connection to the unallocated (unassigned) number talkie is established inside the originating network.
- When the terminating NGN is unable to guarantee the notification of unallocated numbers, it notifies a status other than "unallocated number" in order to avoid a talkie connection at the originating network.

e.2.1. Required functions of the terminating NGN

When the destination number is an unallocated number, the terminating NGN sends back a *404* response with a *Reason* header. When a *404* response containing a *Reason* header is received from the called terminal, the terminating NGN must examine whether or not the response can be guaranteed as the terminating NGN and returns the response only when the destination number is really an unallocated number (i.e. the response can be guaranteed)..

When an unallocated number is detected, the *Reason* header should be configured as shown below:

```
Reason: Q.850;cause=1;text="unallocated number"
```

(The setting of text="unallocated number" is optional)

e.2.2. Required functions of an originating NGN

When an originating NGN has received a *404* response from the terminating NGN including a *Reason* header set with the above condition, it recognizes the unallocated number and connects to the unallocated (unassigned) number talkie.

Annex f. Calling-party's category

(This annex is a notmative part of this standard.)

f.1. Overview

Calling-party's category means subscriber's category that a call originator retains or network-asserted attribute to a call, and corresponds to the "calling subscriber with priority" indication or "test call" indication. This annex describes the formats that are used to exchange the calling-party's category information between NGNs.

Note that each NGN can send to other networks only the calling-party's category information that its own network or a trusted other carrier has verified

f.2. Format of Calling-party's category

In the case that the calling-party's category information is exchanged between NGNs, the calling-party's category is sent and received by asserting a cpc parameter value to the URI described in the *P-Asserted-Identity* header.

In the case that the URI is TEL-URI, a cpc parameter value is asserted to the *parameter* part of the TEL-URI. In the case that the URI is SIP-URI, a cpc parameter value is asserted to the *uri-parameter* part of the SIP-URI. In the case that more than one URIs are described in the *P-Asserted-Identity* header, the same cpc parameter value is asserted to all the URIs.

The cpc parameter format is shown below in ABNF syntax that conforms to [RFC3261].

```
cpc          = cpc-tag "=" cpc-value
cpc-tag      = "cpc"
cpc-value    = "operator" / "ordinary" / "priority" /
               "test" / "payphone" / genvalue
genvalue     = 1*(alphanum / "-" / ".")
```

Use of the calling-party's category is determined based on bilateral agreement between carriers. [Appendix Table iv-20]

f.3. Correspondence with ISUP calling-party's category

Allocation of the cpc parameter value for ISUP calling-party's category defined in [Q.763] is shown in Annex Table f. Each cpc parameter value should be handled in the same manner as its corresponding calling-party's category defined in [Q.763].

Annex Table f/JT-Q3401: Correspondence of cpc parameter value with calling-party's category defined in JT-Q763

cpc parameter value	calling-party's category defined in JT-Q763	
operator	00001001	national operator
ordinary	00001010	ordinary calling subscriber
priority	00001011	calling subscriber with priority
test	00001101	test call
payphone	00001111	payphone

f.4. Message examples

Message examples of calling-party's category information described in this clause are shown below.

1. Assertion of prioritized call indication to the *P-Asserted-Identity* header including SIP URI

```
P-Asserted-Identity: <sip:+81312345678@example.com;user=phone;cpc=priority>
```

2. Assertion of prioritized call indication to the *P-Asserted-Identity* header including TEL URI

```
P-Asserted-Identity: <tel:+81312345678;cpc=priority>
```

3. Assertion of prioritized call indication to the *P-Asserted-Identity* header including SIP URI and TEL URI

```
P-Asserted-Identity: <sip:+81312345678@example.com;user=phone;cpc=priority>,
                     <tel:+81312345678;cpc=priority>
```

Annex g. Congestion control

(This annex is a notmative part of this standard.)

g.1. Overview

This annex provides specification relating to congestion control.

g.2. Basic rule

When a maximum number of sessions has been agreed upon between providers, this may be controlled by a bidirectional session reservation function. [Appendix Table iv-21].

Note that when restriction is based on conditions other than the maximum number of sessions, the details are decided upon between connecting carriers.

g.3. Controlling traffic with a session reservation function

(1) The session hunting can be permitted or prohibited under the following conditions in Annex Table g by setting the number of sessions that can be used at both endpoints of a session group (the value used to judge whether or not to permit the use of sessions by two-way reserved session control during periods of busy two-way traffic) and the number of reserved sessions in both directions (the value used to judge whether or not to permit the number of sessions reserved for traffic from the other terminal during periods of busy one-way traffic):

Annex Table g/ JT-Q3401: Session hunting concept

Session hunting permitted or prohibited	
When the number of sessions used by calls initiated from this station during session hunting is larger than the number of sessions that can be used	When the number of free sessions resources is larger then the number of two-way reserved sessions, this station is allowed to perform session hunting.
	When the number of free sessions resources is less than or equal to the number of two-way reserved sessions, session hunting at this station is prohibited.

(2) The decision whether or not to control two-way reserved sessions should be made by arrangement between providers.

(3) The number of two-way reserved sessions and the number of sessions that can be used should be determined by arrangement between providers.

Annex h. SIP-ISUP interwork for number-related information

(This annex is a notmative part of this standard.)

h.1. SIP-ISUP interworking rules

This annex describes SIP-ISUP interworking rules, especially items regarding number information.

h.2. Transferring network-asserted user identity information between NGN and GSTN

This annex specifies the rules for exchanging presentation/restriction information and network-asserted user identity information between a SIP trust domain and TTC ISUP network.

Terms, network-asserted user identity information, presentation/restriction information, and anonymous URI used in this annex are defined in below:

<Network-asserted user identity information>

In a trusted network, information describing the identity of a user that is asserted by the network through authentication or other means (or verified by the network if provided by the user). An example of network-asserted user identity information is an E.164 number that is reachable to the user. Note that subaddress information provided by SIP UA may be included.

<Presentation/Restriction information>

Information specifying whether a user is allowing or prohibiting the presentation of its network-asserted user identity information to another user receiving a call control message.

<Anonymous URI>

URI used when one wants to make URI information anonymous. The specific format is as follows as recommended by [RFC3323]:

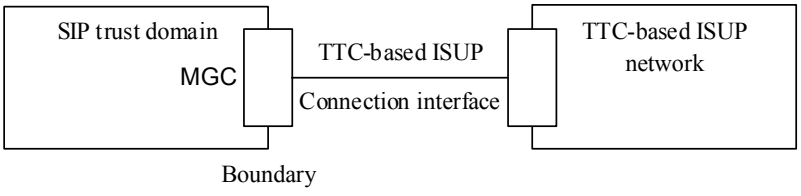
sip:anonymous@anonymous.invalid

h.3. Application model

Application model is shown in Annex Figure h-1.

Here, the processing at Media Gateway Controller (MGC) related to network-asserted user identity information conforms to the specifications of [RFC3398].

The connection interface is assumed to apply TTC-based ISUP protocol, and conforms in particular to JJ-90.10 in the case of different carriers. Interconnecting networks are assumed to be able to trust each other.



Annex Figure h-1/JT-Q3401: SIP trust domain and TTC ISUP interconnection model

h.3.1. SIP Messages to be applied

h.3.1.1. Inbound boundary

INVITE request mapped from an ISUP address message (IAM)

h.3.1.2. Outbound boundary

INVITE request mapped to an ISUP address message (IAM)

h.4. Behaviours particular to the interface

h.4.1. Inbound processing

h.4.1.1. Determining presentation/restriction information

If a valid generic number parameter (see clause h.4.1.2) exists in the IAM, the address presentation restricted indicator must be examined in this parameter. If its value is "presentation allowed," the value of presentation/restriction information is "presentation." All other values of the display indicator including "presentation restricted" means that the value of presentation/restriction information is "restriction."

If a valid generic number parameter does not exist in the IAM but a calling-party number parameter does exist in a valid IAM, the address presentation restricted indicator of this calling-party number parameter must be examined. If its value is "presentation allowed," the value of presentation/restriction information is "presentation." All other values including "presentation restricted" mean that the value of presentation/restriction information is "restriction."

If a calling-party number parameter does not exist in the IAM, the value of presentation/restriction information is "restriction."

h.4.1.2. Determining network-asserted user identity information

Valid generic number parameter:

The values listed in Annex Table h-1 constitute conditions for a valid generic number parameter, which provides the elements for generating network-asserted user identity information.

Annex Table h-1/JT-Q3401: Conditions for a valid generic number parameter

Field	Value	Meaning
Number Qualifier Indicator	00000110	Additional calling-party number
Nature of Address indicator	0000011	National-Number
Number incomplete indicator	0	Complete
Numbering plan indicator	001	ISDN (telephone) numbering plan (Recommendation E.164)
Address Presentation /Restriction indicator	00 or 01	presentation allowed or presentation restricted
Screening Indicator	01 or 11	User provided and network verification is passed, or network provided
Address signal	Max. 16 digits	

Valid calling-party number parameter:

The values listed in Annex Table h-2 constitute conditions for a valid calling-party number parameter, which provides the elements for generating network-asserted user identity information.

Annex Table h-2/JT-Q3401: Conditions for a valid calling-party number parameter

Field	Value	Meaning
Nature of Address indicator	0000011 0000100 1111110	National-Number International number Network specific number
Number incomplete indicator	0	Complete
Numbering plan indicator	001	ISDN (telephone) numbering plan (Recommendation E.164)
Address Presentation/ Restriction indicator	00 or 01	presentation allowed or presentation restricted
Screening Indicator	01 or 11	User provided, network verification is passed, or network provided
Address Signal	Max. 16 digits	

Main number:

This is a number determined in the following way.

If a valid generic number parameter exists, the main number is obtained from this parameter (Nature of Address indicator and address information). If it does not exist but a valid calling-party number parameter does, the main number is obtained from that parameter (Nature of Address indicator and address signal). If neither a valid generic number parameter nor valid calling-party number parameter exists, the main number is considered to be null4.

Mapping to various information components:

SIP_URI:

If the value of presentation/restriction information is "presentation," SIP_URI may be omitted. If the value is "restriction," the use of SIP_URI is essential.

When generating SIP_URI, the user part takes on a tel URI format by applying the conversion rules of Annex Table h-4 from the main number. The host part takes on a value unique to the SIP trust domain. The user=phone parameter may also be set at this time. A sip URI that can be achieved by application of the above rules is applied to SIP_URI, and if none can be achieved, either an anonymous URI should be applied or SIP_URI should be omitted.

If, however, the main number is null, a SIP_URI that requires no number information (such as an anonymous URI) must be set.

SIP_DISPLAYNAME:

If the value of presentation/restriction information is "restriction," the value of SIP_DISPLAYNAME is determined from the value of cause of no ID parameter as shown in Annex Table h-3 5. The value of SIP_DISPLAYNAME is case sensitive but is unaffected by the use of quotes.

---

[4] The case in which a valid generic number exists but a valid calling number does not exist is not normally considered. The processing to perform if such a case occurs depends on carrier policy.

[5] Same as the mapping method given in Section 12.1 of [RFC3398] from the cause of no ID parameter to the displayname part of the From header.

Annex Table h-3/JT-Q3401: Conversion rules from cause of no ID parameter to SIP_DISPLAYNAME

Parameter Value	Meaning	SIP_DISPLAYNAME
No parameter	-	Unavailable
0000001	No caller ID: rejected by user	Anonymous
0000010	No caller ID: service conflict	Interaction with other service
0000011	No caller ID: call from public telephone	Coin line/payphone

If the value of presentation/restriction information is "presentation," SIP_DISPLAYNAME may be omitted or the value of TEL_DISPLAYNAME may be applied.

TEL_URI:

If a calling-party number parameter exists, TEL_URI takes on the character string obtained by applying the conversion rules of Annex Table h-4. If a calling-party number parameter does not exist, TEL_URI is left to be null.

Annex Table h-4 lists the conversion rules to tel URI from the set format of address information in the calling-party number parameter specified 6.

Annex Table h-4/JT-Q3401: Conversion rules from ISUP nature of address indicator and address signal to tel URI

Use	Nature of Address indicator	Address Signal	tel URI
Originating call on international network (overseas)	International number	country-code + National-Number	tel:+country-code National-Number
Originating call on mobile/PHS network	National-Number	A0CDEFGHJK	tel:+81A0CDEFGHJK
Originating call on local fixed telephone network	National-Number	ABCDEFGHJ	tel:+81ABCDEFGHJ
Operator-originating call, etc.	Network specific number	Free Format	tel:<Free Format>;phone-context=+81

TEL_DISPLAYNAME:

If the value of presentation/restriction information is "restriction," TEL_DISPLAYNAME may be omitted or a value derived from the main number may be applied.

If the value of presentation/restriction information is "notification," TEL_DISPLAYNAME is derived from the main number. Here, if the SIP trust domain has enough information with regard to the dialing plan of the terminating user, that information is used to set a value. If it does not have enough information, TEL_DISPLAYNAME takes on the character string obtained by applying the conversion rules of Annex Table h-5.

Annex Table h-5 lists conversion rules based on standard dialing plans in GSTN.

[6] Equivalent to the rules supplemented in Section 12.1 of JF-IETF-RFC3398 with JJ-90.10 noted.

Annex Table h-5/JT-Q3401: Conversion rules from ISUP nature of address indicator and address signal to TEL_DISPLAYNAME

Use	Nature of Address indicator	Address Signal	TEL_DISPLAYNAME
Originating call on international network (overseas)	International number	country-code + National-Number	010 country -code National-Number
Originating call on mobile/PHS network	National-Number	A0CDEFGHJK	0A0CDEFGHJK
Originating call on local fixed telephone network	National-Number	ABCDEFGHJ	0ABCDEFGHJ
Logical number	National-Number	AB0~	0AB0~
Operator-originating call, etc.	Network specific number	Optional	Optional

Annex Table h-6 summarizes ISUP-to-SIP interworking conditions in inbound processing.

Annex Table h-6/JT-Q3401: ISUP-to-SIP interworking conditions in input processing

ISUP

Generic number		Calling-party number		Cause of no ID
Yes/No	Address Presentation Restriction indicator	Yes/No	Address Presentation Restriction indicator	Yes/No
Yes	Presentation Allowed	Yes	Presentation Allowed	Yes/No
			Other	
		No	-	
	Other	Yes	Presentation Allowed	Yes
				No
			Other	Yes
				No
		No	-	Yes/No
No	-	Yes	Presentation Allowed	Yes/No
			Other	Yes
				No
		No	-	Yes
				No

SIP

Notification/ Restriction	SIP		TEL	
	URI	DISPLAYNAME	URI	DISPLAYNAME
Notification	Generic number or omitted	Generic number or omitted	Calling-party number	Generic number
Not generally considered; configuration depends on carrier's policy.				
Restriction	Generic number	Cause of no ID	Calling-party number	Generic number or omitted
		"unavailable"		
		Cause of no ID		
		"unavailable"		
Not generally considered; configuration depends on carrier's policy.				
Notification	Calling-party number	Calling number	Calling-party number	Calling-party number
Restriction		Cause of no ID		Calling-party number or omitted
		"unavailable"		
	Anonymous URI, etc.	Cause of no ID	Not set	Not set
		"unavailable"		

h.4.2. Outbound processing

h.4.2.1. Outputting presentation/restriction information

If the value of presentation/restriction information is "restriction" and if a calling-party number parameter is to be output as a result of the processing described in clause h.4.2.2, the display indicator of the calling-party number parameter must be set to "presentation restricted."

If the value of presentation/restriction information is "presentation," the address presentation restriction indicator of the calling-party number parameter must be set to "presentation allowed."

Also, if a generic number parameter is to be output as a result of the processing described in clause h.4.2.2, the address presentation restriction indicator of the generic number parameter must be set to "presentation allowed" if the value of presentation/restriction information is "presentation", and to "presentation restricted" if that value is "restriction." Furthermore, for the case that the display indicator of the generic number parameter is equal to "presentation allowed," the display indicator of the calling-party number parameter must be set to "presentation restricted" regardless of the content of presentation/restriction information.

h.4.2.2. Outputting network-asserted user identity information

If TEL_URI is not null, the calling-party number parameter must be derived from the value of TEL_URI. The conversion rules from the value of TEL_URI to the calling-party number parameter follow Annex Table h-7. If TEL_URI begins with "+81", nature of address is set to "national" and address information to that number with "+81" removed. If it begins with "+" other than "+81", nature of address indicator is set to "international number" and address information to that number with "+" removed. If it begins with a character other than "+", nature of address is set to "network unique" and address information is unchanged. In addition, the Screening Indicator is set to "network provided." Setting of calling-party number parameter fields other than nature of address indicator, address signal, and Screening Indicator shall conform to the settings specified in JJ-90.10.

Annex Table h-7/JT-Q3401: Conversion rules from tel URI to nature of address and address signal of ISUP

tel URI	Use	Nature of Address indicator	Address Signal
tel:+country-code National-Number	Originating call on international network (overseas)	International number	country-code + National-Number
tel:+81A0CDEFGHJK	Originating call on mobile/PHS network	National-Number	A0CDEFGHJK
tel:+81ABCDEFGHJ	Originating call on local fixed telephone network	National-Number	ABCDEFGHJ
tel:optional;phone-context=+81	Operator-originating call, etc.	Network specific number	Optional

If TEL_DISPLAYNAME exists but differs from TEL_URI, a generic number parameter shall be output. The conversion rules from TEL_DISPLAYNAME to a generic number parameter state that, for a value beginning with "0" other than "010" or "00", nature of address indicator is set to national number and address signal to that number with "0" removed. For patterns other than the above, no mapping to a generic number is performed. In addition, the Screening Indicator is set to "network provided". Setting of generic number parameter fields other than nature of address indicator, address signal, and Screening Indicator shall conform to the settings specified in JJ-90.10.

This equivalency may follow rules particular to the SIP trust domain in question, but the equivalents listed in Annex Table h-8 are the same as those based on standard dialing plans in existing local fixed telephone networks and mobile and PHS networks.

Annex Table h-8/JT-Q3401: TEL_URI and TEL_DISPLAYNAME Equivalents

TEL_URI	TEL_DISPLAYNAME
tel:+81A0BCDEFGHJK	0A0CDEFGHJK
tel:+81ABCDEFGHJ	0ABCDEFGHJ
tel:+81ABCDEFGH	0ABCDEFGH

If the value of presentation/restriction information is "restriction" and if a calling-party number parameter or a generic number parameter has been derived, a cause of no ID parameter shall be output in accordance with the value of SIP_DISPLAYNAME. The values that can be set for the cause of no ID parameter follow the inverse of Annex Table h-3. However, if a value for SIP_DISPLAYNAME is not shown in the Annex Table h-3 column, the cause of no ID parameter shall be set to "rejected by user."

Annex Table h-9 summarizes SIP-to-ISUP interworking conditions in outbound processing.

Annex Table h-9/JT-Q3401: SIP-to-ISUP interworking conditions in output processing

SIP

Notification /Restriction	TEL			SIP
	URI	DISPLAYNAME		DISPLAYNAME
	Yes/No	Yes/No	Equivalency with URI	Yes/No
Notification	Yes	Yes	Equivalent	Yes/No
			Not equivalent	
		No	-	
	No	-	-	
Restriction	Yes	Yes	Equivalent	Yes
				No
			Not equivalent	Yes
				No
		No	-	Yes
				No
	No	-	-	Yes
				No

ISUP

Calling-party number		Generic number		Cause of no ID
Address signal, etc.	Address presentation restriction indicator	Address signal, etc.	Address presentation restriction indicator	
TEL_URI	Presentation allowed	Not set	-	Not set
	Presentation restricted	TEL_DISPLAYNAME	Presentation allowed	
	Presentation allowed	Not set	-	
Not set	-	Not set	-	
TEL_URI	Presentation restricted	Not set	-	SIP_DISPLAYNAME
				"Rejected by User" or omitted
		TEL_DISPLAYNAME	Presentation restricted	SIP_DISPLAYNAME
				"Rejected by User" or omitted
		Not set	-	SIP_DISPLAYNAME
				"Rejected by User" or omitted
Not set	-	Not set	-	Not set

Appendix i. Fallback connection

(This appendix does not form an integral part of this standard.)

This appendix describes IPv4/v6 fallback connection.

In the case that the NGN originates a call to the other NGN using IPv6 and the terminating NGN or the terminating terminal decides that the requested communication using IPv6 cannot be established, a *488* error response with *300 (Incompatible network protocol)* or *301 (Incompatible network address formats)* set to the value of *Warning* header should be sent back to the originating NGN.

When the originating NGN or the originating terminal receives the *488* error response with *300* or *301* set to the value of *Warning* header, it may interpret that the terminating side cannot establish communication using IPv6 then reoriginate a call using IPv4.

Appendix ii. TCP transport connection for NGN-to-NGN interface

(This appendix does not form an integral part of this standard.)

ii.1. Overview

[RFC3261] requires to use TCP transport when sending a SIP message with a size which may cause fragmentation over UDP transport.

This appendix describes the connection in the case of using TCP between NGNs, specifically the parts that are not clarified in the JT-Q3401 main body and [RFC3261], as an example of TCP transport connection.

ii.2. TCP transport connection

According to [RFC3261], the TCP connection established between gateway nodes is used for sending and receiving messages in a SIP transaction initiated by the client side of the established TCP connection. In sending and receiving messages in a SIP transaction initiated by each node, the established TCP connection originated by the each node is used. Therefore, in the case of sending and receiving SIP signals between gateway nodes, two TCP connections are normally established.

There is concern about the impact on performance caused by TCP connection establishment/release process at each gateway nodes of NGNs because establishing and releasing TCP connection on a per-call basis as specified in [RFC3261] require massive processing powers of SIP gateway nodes. Therefore, the TCP connection at the interface between NGNs, once established, may be retained for a long period, and be used for multiple calls. When the node is temporarily unable to use the established TCP connection while retaining the connection for a long period, the TCP connection which is originated by the opposite side can be used only to send SIP request messages inside existing dialogs, based on bilateral agreement between carriers. [Appendix Table iv-5, Item 4]

Other conditions on using the TCP transport between gateway nodes (port number, timer condition, maximum SIP message size when applying TCP, etc.) are decided based on bilateral agreement between carriers. [Appendix Table iv-5, Item 2]

ii.3. Long-period TCP connection establishment and release trigger

In the case that the long-period TCP connection is applied at the interface between NGNs, the TCP connection may be established prior to sending and receiving SIP messages between gateway nodes. In this case, procedures of TCP connection establishment/release between gateway nodes and the number of TCP connections established between them are decided based on bilateral agreement between carriers. [Appendix Table iv-5, Item 2]

It is recommended to apply keepalive processing for the purpose of monitoring the TCP connection when retaining a long-period TCP connection between gateway nodes. In the case of applying keepalive, a timeout value of keepalive is assumed to be small enough compared to SIP Timer B, and the basic behaviour is sending probe packets from both sides. Parameters of keepalive behaviour are decided based on bilateral agreement between carriers. [Appendix Table iv-5, Item 3]

Appendix iii. ISUP-to-SIP interworking rules for number portability

(This appendix does not form an integral part of this standard.)

iii.1. Overview

In order to realize number portability from PSTN to IP, ISUP-to-SIP interworking rules of directory number (DN and network routing number (NRN) specified between PSTNs are described. Specification regarding number portability for NNI between IP networks is outside the scope of this appendix.

iii.2. Signalling system

In redirection between PSTNs, IAM and REL are used to transfer the following address information

- NRN (network routing number)
- DN (called directory number)

In the case of receiving the above information by redirection IAM, *npdi* parameter and *rn* parameter are added to the par part of *Request-Line* of INVITE request, the user's DN is set to the phonedigit part, and NRN is set to rn.

In the case of receiving redirection REL, it is mapped to *3xx* response.

iii.3. Examples of SIP messages

SIP message examples at the time of number portability described in this appendix are shown below.

1. *Request-Line* of *INVITE* request in the case of receiving redirection IAM.

```
INVITE sip:+81312345678;npdi;rn=+8134512345@example.com SIP/2.0
```

Appendix iv. Option items

(This appendix does not form an integral part of this standard.)

iv.1. Introduction

The following tables show the option items of the main body, annexes, and appendices of JT-Q3401. The objective of this table is improvement of interoperability between NGN carriers.

The reader should consult the relevant clauses shown in "Relevant items" for more detailed information of each option item.

Note that any interaction among the options are not always described in these tables.

Note also that information given in the main document overrides that in this option item table in the event of any discrepancies.

iv.2. Option item extraction policy

Option items are extracted from a following viewpoint:

The option items are extracted to improve interoperability of domestic NGNs, and classified into different categories for ease of reference.

iv.3. Option item table format

Appendix Table iv-1 shows and explains the format of the option item table presented here.

Appendix Table iv-1/JT-Q3401: Format example

	Item	NNI condition	Relevant items	Special notes	Remarks
1	*MESSAGE* (outside existing dialogs)	Use	Clause 10.1 Table 10-12 / RFC3428		
		Not use			

Item: shows option items.
NNI condition: shows selectable patterns between networks.
Relevant items: shows, for each option item, relevant clauses of the JT-Q3401 main body, annex or appendix.
Special notes: shows option items that should be determined in addition to "Use conditions between networks"

iv.4. Option item table

Options item tables are shown in Appendix Table iv-2 to Appendix Table iv-21. Items specified that they shall be supported in the main body and annexes are not explicitly shown in each table.

Appendix Table iv-2/JT-Q3401: SIP method

	Item	NNI condition	Relevant items	Special notes	Remarks
1	*MESSAGE* (outside existing dialogs)	Use	Clause 10.1 Table 10-12 / RFC3428		
		Not use			
2	*MESSAGE* (inside an existing dialog)	Use	Clause 10.1 Table 10-12 / RFC3428		
		Not use			
3	*NOTIFY*	Use	Clause 10.1 Table 10-12 / RFC3265	[In the case of use, determine the event name.]	
		Not use			
4	*REFER* (outside existing dialogs)	Use	Clause 10.1 Table 10-12 / RFC3515		
		Not use			
5	*REFER* (inside an existing dialog)	Use	Clause 10.1 Table 10-12 / RFC3515		
		Not use			
6	*SUBSCRIBE*	Use	Clause 10.1 Table 10-12 / RFC3265	[In the case of use, determine the event name.]	
		Not use			
7	Other methods	Use		[In the case of use, determine the method name.]	
		Not use			

Appendix Table iv-3/JT-Q3401: Request-URI format of a request outside existing dialogs

	Item	NNI condition	Relevant items	Special notes	Remarks
1	Use of SIP-URI other than a global E.164 number	Use	Clause 9, Annex b.3.1	[Determine the SIP-URI format to use.]	
		Not use			
2	Use of IP address for the *hostport* part	Use*1	Annex b.3.1.2	[Determine the IP address to accept.]	
		Not use			
3	Use of domain name for the *hostport* part	Use*1	Annex b.3.1.2	[Determine the domain name to accept.]	
		Not use			
4	Constraints of the valid number of digits in the *telephone-subscriber* part	Use	Annex b.3.2	[In the case of use, determine the minimum and the maximum number of digits to receive.]	
		Not use			

*1 Use either or both of the formats.

Appendix Table iv-4/JT-Q3401: IP version type

	Item	NNI condition	Relevant items	Special notes	Remarks
1	IPv6	Use	Clause 13		
		Not use			
2	IP versions of call control signals and media	Use only the same IP version.	Clause 10.3 Table 810-7		
		Use the same or different IP version.			

Appendix Table iv-5/JT-Q3401: Layer 4 protocol for call control signals

	Item	NNI condition	Relevant items	Special notes	Remarks
1	UDP	Use	Clause 12	[Determine the port number in the case that a port number other than the default number (5060) is used for sending or receiving.]	
		Not use			
2	TCP	Use	Clause 12 Appendix ii.2 Appendix ii 3	[In the case of using TCP, determine conditions for TCP transport.] [In the case of establishing a TCP connection for a long period, determine the number of connections.] [Determine the port number in the case that a port number other than the default number (5060) is to be listened.]	
		Not use			
3	TCP keepalive option	Use	Appendix ii.3	[In the case of using keepalive options, determine parameters, such as timeout period, etc.]	
		Not use			
4	Sending a request inside an existing dialog, using a TCP connection established from the remote node side, when a TCP connection established from the local side is unavailable.	Use	Appendix ii.2		

		Not use			

Appendix Table iv-6/JT-Q3401: SDP

	Item	NNI condition	Relevant items	Special notes	Remarks
1	Optional SDP lines	Use	Clause 10.3 Table 10-78	[Determine the SDP lines to be used.]	
		Not use			

Appendix Table iv-7/JT-Q3401: Media

	Item	NNI condition	Relevant items	Special notes	Remarks
1	Video (*m=video*)	Use	Clause 10.3 Table 10-78		
		Not use			
2	Data communication (*m=application*, *m=data*, etc.)	Use	Clause 10.3 Table 10-78	[Determine the media type (*m=line* of SDP) to use.]	
		Not use			
3	Media TCP connection	Use	Clause 10.3 Table 10-78	[Determine the media type (*m=line* of SDP) that uses TCP.]	
		Not use			
4	Bandwidth control	Use	Clause 10.3 Table 10-78	[Determine the conditions of bandwidth control.]	
		Not use			

Appendix Table iv-8/JT-Q3401: Codecs to be included in a codec list

	Item	NNI condition	Relevant items	Special notes	Remarks
1	Voice band codec other than G.711 μ-law	Include	Clause 8	[Determine the name of codec.]	
		Not include			
2	Video codec	Include	Clause 8	[Determine the name of codec.]	
		Not include			
3	Data communication	Include	Clause 8	[Determine the name of protocol.]	
		Not include			

Appendix Table iv-9/JT-Q3401: SIP option tag

	Item	NNI condition	Relevant items	Special notes	Remarks
1	Session timer function (*timer*)	Use in all sessions Use in each session as necessary	Clause 10.2.1.20.32		
2	Provisional response reliability function (*100rel*)	Use in all sessions Use in each session as necessary	Clause 10.2.1.20.32		
3	Dialog replacement function (*replaces*)	Use in each session as necessary Not use	Clause 10.1 Table 10-12 / RFC3891		
4	Conference session participation function (*join*)	Use in each session as necessary Not use	Clause 10.1 Table 10-12 / RFC3911		
5	Bandwidth reservation function before establishment (*precondition*)	Use in each session as necessary Not use	Clause 10.1 Table 10-12 / RFC3312 Table 10-12 / RFC4032		
6	Terminal capabilities notification function (*pref*)	Use in each session as necessary Not use	Clause 10.1 Table 10-12 / RFC3840 Table 10-12 / RFC3841		
7	Request history notification function (*histinfo*)	Use in each session as necessary Not use	Clause 10.1 Table 10-12 / RFC4244		
8	Other SIP option tags	Use in each session as necessary Not use		[Determine the name of SIP option tag to use.]	

Appendix Table iv-10/JT-Q3401: timer

	Item	NNI condition	Relevant items	Special notes	Remarks
1	Session refresh by *UPDATE* method	Use Not use	Clause 10.1 Table 10-12 / RFC3311 Table 10-12 / RFC4028		

Appendix Table iv-11/JT-Q3401: 100rel

	Item	NNI condition	Relevant items	Special notes	Remarks
1	Early media when not using *100rel*	Use Not use	Clause 10.2.1.13		

Appendix Table iv-12/JT-Q3401: Media negotiation

	Item	NNI condition	Relevant items	Special notes	Remarks
1	SDP offer by *PRACK*	Use	Clause 10.2.1.7.4.1		
		Not use			
2	SDP offer by *UPDATE*	Use	Clause 10.1 Table 10-12 / RFC3311		
		Not use			
3	Media modification in early dialog	Use	Clause 10.1 Table 10-12 / RFC3311	[Determine items allowed to be modified.]	
		Not use			
4	Media modification after dialog establishment	Use	Clause 10.2.1.14	[Determine items allowed to be modified.]	
		Not use			

Appendix Table iv-13/JT-Q3401: Message body

	Item	NNI condition	Relevant items	Special notes	Remarks
1	Use of MIME Multipart in *INVITE* requests	Use	Clause 10.1 Table 10-12 / RFC2046		
		Not use			
2	Use of MIME Multipart in *MESSAGE* requests	Use	Clause 10.1 Table 10-12 / RFC2046		
		Not use			

Appendix Table iv-14/JT-Q3401: Redirection

	Item	NNI condition	Relevant items	Special notes	Remarks
1	Redirection by *3xx* response	Use	Clause 10.2.1.8.3	[In case of the use, determine the applicable method.]	
		Not use			

Appendix Table iv-15/JT-Q3401: Number portability

	Item	NNI condition	Relevant items	Special notes	Remarks
1	Parameters for number portability (*npdi* and *rn* parameters)	Use	Clause 10.1 Table 10-12 / RFC4694		
		Not use			

Appendix Table iv-16/JT-Q3401: Billing-related headers

	Item	NNI condition	Relevant items	Special notes	Remarks
1	Use of headers (*P-Charging-Vector*, *P-Charging-Function-Addresses*) for inter-carrier charging	Use	Clause 10.1 Table 10-12 / RFC3455		
		Not use			

Appendix Table iv-17/JT-Q3401: Maximum message length

	Item	NNI condition	Relevant items	Special notes	Remarks
1	Maximum length per one line of a SIP/SDP message	Use the same value as when using UDP.	Annex b.4	[In the case of using a value different from when using UDP, determine the value.]	
		Use a value different from when using UDP.			
2	Maximum entries of the same header for a SIP/SDP message	Use the same value as when using UDP.	Annex b.4	[In the case of using a value different from when using UDP, determine the value.]	
		Use a value different from when using UDP.			
3	Maximum message body length for a SIP/SDP message	Use the same value as when using UDP.	Annex b.4	[In the case of using a value different from when using UDP, determine the value.]	
		Use a value different from when using UDP.			
4	Overall message length for a SIP/SDP message	Use the same value as when using UDP.	Annex b.4	[In the case of using a value different from when using UDP, determine the value.]	
		Use a value different from when using UDP.			

Appendix Table iv-18/JT-Q3401: Subaddress

	Item	NNI condition	Relevant items	Special notes	Remarks
1	Originating subaddress	Use	Annex b.5		
		Not use			
2	Terminating subaddress	Use	Annex b.5		
		Not use			

Appendix Table iv-19/JT-Q3401: Guidance/talkie

	Item	NNI condition	Relevant items	Special notes	Remarks
1	Guidance/talkie services according to the status code in a received response	Use	Annex d.2.2	[In the case of use, determine specific status codes.]	
		Not use			
*1	For unallocated number talkie, Annex e is applied.				

Appendix Table iv-20/JT-Q3401: Calling-party's category

	Item	NNI condition	Relevant items	Special notes	Remarks
1	Calling-party's category (cpc parameter)	Use	Annex f.2	[In the case of using a calling-party's category other than defined "operator", "ordinary", "priority", "test", or "payphone", determine the name.]	
		Not use			

Appendix Table iv-21/JT-Q3401: Maximum number of sessions

	Item	NNI condition	Relevant items	Special notes	Remarks
1	Limitation of the maximum number of sessions at a time	Limit the number of originating sessions	Annex g.2	[In the case that bidirectional session reservation is performed as well as control of the number of originating sessions, determine the number of reserved sessions.]	
		Not limit			

Appendix v. Signalling rule of SIP messages and headers

(This appendix does not form an integral part of this standard.)

This appendix describes header information setting conditions for request and response messages for each SIP method by dynamic view.

v.1. Dynamic view and static view

v.1.1. Static view

Static view refers to the form which can be seen in Annex A of 3GPP TS24.229, where "sending" and "receiving" SIP entities' functional implementation is expressed as M (Mandatory), O (Optional), etc. in regard to application conditions of each header.

Functions are categorized into M (Mandatory) or O (Optional) in static view, from the standpoint of whether SIP entities at both ends of an interface reference point understand the header information or not, in other words, whether they recognize the contents and implement the functions to behave in accordance with specifications such as RFCs. Therefore, M (Mandatory) does not mean that the corresponding header always appears in a SIP message.

v.1.2. Dynamic view

Dynamic view refers to the header application condition table which can be seen in RFC3261, where it indicates M (Mandatory), O (Optional), etc. from the point of view that if the headers do appear and exist as information items for signalling over an interface between SIP entities, instead of using application categorization such as "sending" and "receiving" sides as in static view.

Dynamic view shows the possible appearance of information as regards whether certain headers exist on the involved interface reference point or not, and if M (Mandatory) is indicated, the header must be included in the corresponding message.

v.1.3. Adoption of dynamic view for this appendix

This appendix adopts dynamic view presentation for the purpose of the clarification of an interface specification.

v.1.4. Definition of notation codes in the tables in this appendix

The definition of the notation codes described in the columns of "RFC status" and "Status in this standard" for each table is identical to that of RFC3261.

Appendix Table v-1/JT-Q3401: Definition of notation codes

Notation code	Definition
m	The header field is mandatory. A mandatory header field MUST be present in a request, and MUST be understood by the UAS receiving the request message. Likewise, a mandatory response header field MUST be present in the response, and the header field MUST be understood by the UAC processing the response.
m*	The header field SHOULD be present, but clients or servers need to be prepared to receive messages without that header field.
t	The header field SHOULD be present, but clients or servers need to be prepared to receive messages without that header field. If TCP is used as a transport, then the header field is mandatory and MUST be sent.
o	The header field is optional. Optional means that the header field MAY be present in a request or response, and if present in the request or response, it MUST be understood by the receiving side, and the corresponding processing MUST be performed, according to the RFC. (Note) If specially specified, the header field present in the request or response MAY be allowed to be ignored. These specifications are noted in "Application conditions" and "Remarks" columns. In the case that option items regarding the header field are selected, the header field conforms to the specifications described in option items.
–	The header field is not applicable. The header field that is not applicable MUST NOT be present in a request or response.
c	Application of the header field depends on the context of the message. (Note) In this standard, conditions regarding the application of header fields are described in "Application conditions" column, but it does not affect the "c" classification in the RFC. "c" in this standard means that there are cases that the header field is necessary in the context of signallings. For the header fields which need to be set according to the conditions for the use of signallin, notes are included in "Application conditions" and "Remarks" columns with consideration to RFC specifications.
*	The header field is required if the message body is not empty.

v.2. ACK

This message is transferred in the forward direction in the case of receiving the final response to an *INVITE* request.

v.2.1. Supported headers in the ACK request

Appendix Table v-1/JT-Q3401: Supported headers in the ACK request

Message type: Request

Method: ACK

Header	Reference	RFC status	Status in this standard	Application conditions	Remarks
Accept-Contact	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Allow-Events	RFC3265	o	o	c2 (Appendix Table iv-2, Items 3 and 6)	
Authorization	RFC3261	o	–	c3	
Call-ID	RFC3261	m	m		
Contact	RFC3261	o	o		
Content-Disposition	RFC3261	o	–	c4	
Content-Encoding	RFC3261	o	–	c4	
Content-Language	RFC3261	o	–	c4	
Content-Length	RFC3261	t	t		
Content-Type	RFC3261	*	–	c4	
CSeq	RFC3261	m	m		
Date	RFC3261	o	o		(Note 1)
From	RFC3261	m	m		
Max-Forwards	RFC3261	m	m		
MIME-Version	RFC3261	o	–	c4	
Privacy	RFC3323	o	–	c5	
Proxy-Authorization	RFC3261	o	–	c3	
Reason	RFC3326	o	o		(Note 1)
Record-Route	RFC3261	o	o		(Note 1)
Reject-Contact	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Request-Disposition	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Route	RFC3261	c	c		
Timestamp	RFC3261	o	o		(Note 1)
To	RFC3261	m	m		
User-Agent	RFC3261	o	o		(Note 1)
Via	RFC3261	m	m		
Message body		o	–	c4	

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available between networks, the header information is handled as valid information. (Appendix Table iv-9, Item 6) (RFC3840 and RFC3841)

c2: In the case that *SUBSCRIBE*/*NOTIFY* is available between networks, the header information is handled as valid information. (Appendix Table iv-2, Items 3 and 6)

c3: Authentication procedures are not supported between networks, according to 10.2.1.8.1.3 of Annex Table a-1 in Annex a.3.

c4: Message body is not used since SDP negotiation by ACK is not performed, according to 10.2.1.13 of Annex Table a-1 in Annex a.3.

c5: *Privacy* header is applicable only to the request and response outside existing dialogs, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.

Note 1 When specified, whether expected behaviours are performed or the capabilities for the behaviours are provided is dependent on the policy of the connected carrier.

v.2.2. Supported headers in the ACK response

The response message to an *ACK* request message is not specified.

v.3. BYE

This message is used for releasing the call after a requested call started (either in early dialog or in confirmed dialog).

v.3.1. Supported header within the BYE request

Appendix Table v-2/JT-Q3401: Supported headers in the BYE request

Message type: Request

Method: BYE

Header	Reference	RFC status	Status in this standard	Application conditions	Remarks
Accept	RFC3261	o	o		
Accept-Contact	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Accept-Encoding	RFC3261	o	o		
Accept-Language	RFC3261	o	o		
Allow	RFC3261	o	o		
Allow-Events	RFC3265	o	o	c2 (Appendix Table iv-2, Items 3 and 6)	
Authorization	RFC3261	o	–	c3	
Call-ID	RFC3261	m	m		
Content-Disposition	RFC3261	o	o		(Note 1)
Content-Encoding	RFC3261	o	o		(Note 1)
Content-Language	RFC3261	o	o		(Note 1)
Content-Length	RFC3261	t	t		
Content-Type	RFC3261	*	*		
CSeq	RFC3261	m	m		
Date	RFC3261	o	o		(Note 1)
From	RFC3261	m	m		
Max-Forwards	RFC3261	m	m		
MIME-Version	RFC3261	o	o		(Note 1)
P-Access-Network-Info	RFC3455	o	o		(Note 1)
P-Asserted-Identity	RFC3325	o	–	c4	
P-Charging-Function-Addresses	RFC3455	o	o	c5 (when Appendix Table iv-16, Item 1 is stated "Use".)	(Note 1)
			–	c5 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
P-Charging-Vector	RFC3455	o	o	c5 (when Appendix Table iv-16, Item 1 is stated "Use".)	
			–	c5 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
P-Preferred-Identity	RFC3325	o	–	c6	
Privacy	RFC3323	o	–	c7	
Proxy-Authorization	RFC3261	o	–	c3	
Proxy-Require	RFC3261	o	o		
Reason	RFC3326	o	o		(Note 1)
Record-Route	RFC3261	o	o		(Note 1)
Referred-By	RFC3892	o	o	c8 (Appendix Table iv-2, Items 4 and 5)	
Reject-Contact	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Request-Disposition	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Require	RFC3261	c	c		
Route	RFC3261	c	c		
Supported	RFC3261	o	o		(Note 1)
Timestamp	RFC3261	o	o		(Note 1)
To	RFC3261	m	m		
User-Agent	RFC3261	o	o		(Note 1)
Via	RFC3261	m	m		
Message body		o	o		(Note 1)

c1:	In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available between networks, the header information is handled as valid information. (Appendix Table iv-9, Item 6) (RFC3840 and RFC3841)
c2:	In the case that *SUBSCRIBE*/*NOTIFY* is available between networks, the header information is handled as valid information. (Appendix Table iv-2, Items 3 and 6)
c3:	Authentication procedures are not supported between networks, according to 10.2.1.8.1.3 of Annex Table a-1 in Annex a.3.
c4:	*P-Asserted-Identity* header is applicable only to the request and response outside existing dialogs, according to 10.2.2.2.2 of Annex Table a-1 in Annex a.3.
c5:	Use of headers for inter-carrier charging (*P-Charging-Vector*, *P-Charging-Function-Address*) (Appendix Table iv-16, Item 1)
c6:	Use of *P-Preferred-Identity* header is not applicable, according to clause 10.2.2.2.3 in the main body.
c7:	*Privacy* header is applicable only to the request and response outside existing dialogs, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.
c8:	*Referred-By* header may be used as a result of using *REFER* (Appendix Table iv-2, Items 4 and 5). In the case that *REFER* is available between networks, the header information may be handled as valid information. It does not guarantee that the *Referred-By* header is used as a result of using *REFER*.
Note 1	When specified, whether expected behaviours are performed or the capabilities for the behaviours are provided is dependent on the policy of the connected carrier.

v.3.2. Supported headers in the BYE response

Appendix Table v-3/JT-Q3401: Supported headers in the BYE response

Message type: Response

Method: BYE

Header	Appli-cation	Reference	RFC status	Status in this standard	Application conditions	Remarks
Accept	415	RFC3261	c	c		
Accept-Encoding	415	RFC3261	c	c		
Accept-Language	415	RFC3261	c	c		
Allow	2xx	RFC3261	o	o		
Allow	405	RFC3261	m	m		
Allow		RFC3261	o	o		
Allow-Events	2xx	RFC3265	o	o	c1 (Appendix Table iv-2, Items 3 and 6)	
Authentication-Info	2xx	RFC3261	o	–	c2	
Call-ID		RFC3261	m	m		
Contact	3xx	RFC3261	o	o		
Contact	485	RFC3261	o	o		
Content-Disposition		RFC3261	o	o		(Note 1)
Content-Encoding		RFC3261	o	o		(Note 1)
Content-Language		RFC3261	o	o		(Note 1)
Content-Length		RFC3261	t	t		
Content-Type		RFC3261	*	*		(Note 1)
CSeq		RFC3261	m	m		
Date		RFC3261	o	o		(Note 1)
Error-Info	300-699	RFC3261	o	o		(Note 1)
From		RFC3261	m	m		
MIME-Version		RFC3261	o	o		(Note 1)
P-Access-Network-Info		RFC3455	o	o		(Note 1)
P-Asserted-Identity		RFC3325	o	–	c3	
P-Charging-Function-Addresses		RFC3455	o	o	c4 (when Appendix Table iv-16, Item 1 is stated "Use".)	(Note 1)
				–	c4 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
P-Charging-Vector		RFC3455	o	o	c4 (when Appendix Table iv-16, Item 1 is stated "Use".)	
				–	c4 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
P-Preferred-Identity		RFC3325	o	–	c5	
Privacy		RFC3323	o	–	c6	
Proxy-Authenticate	401	RFC3261	o	–	c2	
Proxy-Authenticate	407	RFC3261	m	–	c2	
Reason		RFC3326	o	o		(Note 1)
Record-Route	18x 2xx	RFC3261	o	o		(Note 1)
Require		RFC3261	c	c		(Note 1)
Retry-After	404 413 480 486	RFC3261	o	o		(Note 1)
Retry-After	500 503	RFC3261	o	o		(Note 1)
Retry-After	600 603	RFC3261	o	o		(Note 1)
Server		RFC3261	o	o		(Note 1)
Supported	2xx	RFC3261	o	o		
Timestamp		RFC3261	o	o		(Note 1)
To		RFC3261	m	m		
Unsupported	420	RFC3261	m	m		

User-Agent		RFC3261	o	o		(Note 1)
Via		RFC3261	m	m		
Warning		RFC3261	o	o		(Note 1)
WWW-Authenticate	401	RFC3261	m	–	c2	
WWW-Authenticate	407	RFC3261	o	–	c2	
Message body		RFC3261	o	o		(Note 1)

c1: In the case that *SUBSCRIBE*/*NOTIFY* is available between networks, the header information is handled as valid information. (Appendix Table iv-2, Items 3 and 6)

c2: Authentication procedures are not supported between networks, according to 10.2.1.8.1.3 of Annex Table a-1 in Annex a.3.

c3: *P-Asserted-Identity* header is applicable only to the request and response outside existing dialogs, according to 10.2.2.2.2 of Annex Table a-1 in Annex a.3.

c4: Use of headers for inter-carrier charging (P-Charging-Vector, P-Charging-Function-Address) (Appendix Table iv-16, Item 1)

c5: Use of this header is not applicable, according to clause 10.2.2.2.3 in the main body.

c6: *Privacy* header is applicable only to the request and response outside existing dialogs, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.

Note 1 When specified, whether expected behaviours are performed or the capabilities for the behaviours are provided is dependent on the policy of the connected carrier.

v.4. CANCEL

This message is used for terminating the request from the originating side before the establishment of a requested call.

v.4.1. Supported headers in the CANCEL request

Appendix Table v-4/JT-Q3401: Supported headers in the CANCEL request

Message type: Request

Method: CANCEL

Header	Reference	RFC status	Status in this standard	Application conditions	Remarks
Accept-Contact	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Authorization	RFC3261	o	–	c2	
Call-ID	RFC3261	m	m		
Content-Length	RFC3261	t	t		
CSeq	RFC3261	m	m		
Date	RFC3261	o	o		(Note 1)
From	RFC3261	m	m		
Max-Forwards	RFC3261	m	m		
Privacy	RFC3323	o	–	c3	
Reason	RFC3326	o	o		(Note 1)
Record-Route	RFC3261	o	o		(Note 1)
Reject-Contact	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Request-Disposition	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Route	RFC3261	c	c		
Supported	RFC3261	o	o		(Note 1)
Timestamp	RFC3261	o	o		(Note 1)
To	RFC3261	m	m		
User-Agent	RFC3261	o	o		(Note 1)
Via	RFC3261	m	m		

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available between networks, the header information is handled as valid information. (Appendix Table iv-9, Item 6) (RFC3840 and RFC3841)

c2: Authentication procedures are not supported between networks, according to 10.2.1.8.1.3 of Annex Table a-1 in Annex a.3.

c3: *Privacy* header is applicable only to the request and response outside existing dialogs, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.

Note 1 When specified, whether expected behaviours are performed or the capabilities for the behaviours are provided is dependent on the policy of the connected carrier.

v.4.2. Supported headers in the CANCEL response

Appendix Table v-5/JT-Q3401: Supported headers in the CANCEL response

Message type: Response

Method: CANCEL

Header	Appli-cation	Reference	RFC status	Status in this standard	Application conditions	Remarks
Call-ID		RFC3261	m	m		
Content-Length		RFC3261	t	t		
CSeq		RFC3261	m	m		
Date		RFC3261	o	o		(Note 1)
Error-Info	300-699	RFC3261	o	o		(Note 1)
From		RFC3261	m	m		
Privacy		RFC3323	o	–	c1	(Note 1)
Proxy-Authenticate	401	RFC3261	o	–	c2	
Reason		RFC3326	o	o		(Note 1)
Record-Route	18x 2xx	RFC3261	o	o		(Note 1)
Retry-After	404 413 480 486	RFC3261	o	o		(Note 1)
Retry-After	500 503	RFC3261	o	o		(Note 1)
Retry-After	600 603	RFC3261	o	o		(Note 1)
Server		RFC3261	o	o		(Note 1)
Supported		RFC3261	o	o		(Note 1)
Timestamp		RFC3261	o	o		(Note 1)
To		RFC3261	m	m		
User-Agent		RFC3261	o	o		(Note 1)
Via		RFC3261	m	m		
Warning		RFC3261	o	o		(Note 1)

c1: *Privacy* header is applicable only to the request and response outside existing dialogs, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.

c2: Authentication procedures are not supported between networks, according to 10.2.1.8.1.3 of Annex Table a-1 in Annex a.3.

Note 1 When specified, whether expected behaviours are performed or the capabilities for the behaviours are provided is dependent on the policy of the connected carrier.

v.5. INVITE

This message is used for call initiation.

v.5.1. Supported headers in the INVITE request

Appendix Table v-6/JT-Q3401: Supported headers in the INVITE request

Message type: Request

Method: INVITE

Header	Reference	RFC status	Status in this standard	Application conditions	Remarks
Accept	RFC3261	o	o		
Accept-Contact	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Accept-Encoding	RFC3261	o	o		
Accept-Language	RFC3261	o	o		
Alert-Info	RFC3261	o	o		(Note 1)
Allow	RFC3261	o	m* / o	c2	c2
Allow-Events	RFC3265	o	o	c3 (Appendix Table iv-2, Items 3 and 6)	
Authorization	RFC3261	o	–	c4	
Call-ID	RFC3261	m	m		
Call-Info	RFC3261	o	o		(Note 1)
Contact	RFC3261	m	m		
Content-Disposition	RFC3261	o	o		
Content-Encoding	RFC3261	o	o		
Content-Language	RFC3261	o	o		
Content-Length	RFC3261	t	t		
Content-Type	RFC3261	*	*		
CSeq	RFC3261	m	m		
Date	RFC3261	o	o		(Note 1)
Expires	RFC3261	o	o		(Note 1)
From	RFC3261	m	m		
History-Info	RFC4244	o	o / –	c5 (when Appendix Table iv-9, Item 7 is stated "Used in each session as necessary ".)	
			–	c5 (when Appendix Table iv-9, Item 7 is stated "Not use".)	
In-Reply-To	RFC3261	o	o		(Note 1)
Join	RFC3911	o	o	c6 (when Appendix Table iv-9, Item 4 is stated "Use".)	
			–	c6 (when Appendix Table iv-9, Item 4 is stated "Not use".)	
Max-Forwards	RFC3261	m	m		
MIME-Version	RFC3261	o	o		
Min-SE	RFC4028	o	o	c7	
Organization	RFC3261	o	o		(Note 1)
P-Access-Network-Info	RFC3455	o	o		(Note 1)
P-Asserted-Identity	RFC3325	o	m / –	c8	
P-Called-Party-ID	RFC3455	o	o		(Note 1)
P-Charging-Function-Addresses	RFC3455	o	o	c9 (when Appendix Table iv-16, Item 1 is stated "Use".)	(Note 1)
			–	c9 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
P-Charging-Vector	RFC3455	o	o	c9 (when Appendix Table iv-16, Item 1 is stated "Use".)	
			–	c9 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
P-Preferred-Identity	RFC3325	o	-	c10	
P-Visited-Network-ID	RFC3455	o	o		(Note 1)
Priority	RFC3261	o	o		(Note 1)
Privacy	RFC3323	o	m* / –	c11	
Proxy-Authorization	RFC3261	o	–	c4	

Proxy-Require	RFC3261	o	o		
Reason	RFC3326	– / o	– / o	(Note 2)	(Note 1)
Record-Route	RFC3261	o	o		
Referred-By	RFC3892	o	o	c12 (Appendix Table iv-2, Items 4 and 5)	
Reject-Contact	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Replaces	RFC3891	o	o	c13 (when Appendix Table iv-9, Item 3 is stated "Used in each session as necessary ".)	
			–	c13 (when Appendix Table iv-9, Item 3 is stated "Not use".)	
Reply-To	RFC3261	o	o		(Note 1)
Request-Disposition	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Require	RFC3261	c	c	c14	
Route	RFC3261	c	c		
Session-Expires	RFC4028	o	m	c7 (when Appendix Table iv-9, Item 1 is stated "Used in all sessions".)	
			o	c7 (when Appendix Table iv-9, Item 1 is stated "Used in each session as necessary ".)	
Subject	RFC3261	o	o		(Note 1)
Supported	RFC3261	m*	m*	c14	
Timestamp	RFC3261	o	o		(Note 1)
To	RFC3261	m	m		
User-Agent	RFC3261	o	o		(Note 1)
Via	RFC3261	m	m		
Message body	RFC3261	o	m	c15	

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available between networks, the header information is handled as valid information. (Appendix Table iv-9, Item 6) (RFC3840 and RFC3841)

c2: The setting of *Allow* header is necessary for initial *INVITE*, according to clause 10.2.1.20.5. (Note that the initial INVITE without the setting is not handled as error when received.)

c3: In the case that *SUBSCRIBE*/*NOTIFY* is available between networks, the header information is handled as valid information. (Appendix Table iv-2, Items 3 and 6)

c4: Authentication procedures are not supported between networks, according to 10.2.1.8.1.3 of Annex Table a-1 in Annex a.3.

c5: In the case that the request history retention function (*histinfo*) is available between networks, the header can be used (Appendix Table iv-9, Item 7). Note that it is applicable only to the request outside existing dialogs which necessitates the recording of route information, and not applicable to the request inside an existing dialog.

c6: In the case that the conference session participation function (*join*) is available between networks, the header can be used. (Appendix Table iv-9, Item 4)

c7: The header must be used as specified in clause 10.2.2.2.1 and 10.2.2.2.8 in the main body. In the case that Session-Timer is used, at least the setting of value to the *Session-Expires* header (*delta-seconds*) is necessary.

c8: *P-Asserted-Identity* header needs to be set for a request outside dialogs (not to be used inside a dialog) and transmits the calling-party's information, according to 10.2.2.2.2 of Annex Table a-1 in Annex a.3 and Annex c. (The setting is necessary for initial-*INVITE*, but not necessary for re-*INVITE*.)

c9: Use of headers for inter-carrier charging (*P-Charging-Vector*, *P-Charging-Function-Address*) (Appendix Table iv-16, Item 1)

c10: Use of *P-Preferred-Identity* header is not applicable, according to clause 10.2.2.2.3 in the main body.

c11: *Privacy* header needs to be set for a request outside dialogs and transmits the presentation/restriction information of the calling-party, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3 and Annex c. (The setting is necessary for initial-*INVITE*, but not necessary for re-*INVITE*. In the case that this header is not present in initial *INVITE*, the calling-party's information is handled to be possible to be notified.)

c12: *Referred-By* header may be used as a result of using *REFER* (Appendix Table iv-2, Items 4 and 5). In the case that *REFER* is available between networks, the header information may be handled as valid information. It does not guarantee that the *Referred-By* header is used as a result of using *REFER*.

c13: In the case that the dialog replacement function (replaces) is available between networks, the header information can be used. (Appendix Table iv-9, Item 3)

c14: "*100rel*" and "*timer*" need to be set to the *Require* header and the *Supported* header in terms of the context, according to clause 10.2.1.20.32 and 10.2.1.20.37 in the main body. ("*100rel*" is contextually set to the *Supported* header of initial *INVITE*. "*timer*" should be contextually set to the *Supported* header of initial *INVITE* and re-*INVITE*.)

c15: SDP offer is described in the body part of an *INVITE* request, according to 10.2.1.13 and 10.2.1.14 of Annex Table a-1 in Annex a.3.

Note 1 When specified, whether expected behaviours are performed or the capabilities for the behaviours are provided is dependent on the policy of the connected carrier.

Note 2 *Reason* header is specified in RFC3326, and it is applicable to all the requests inside an existing dialog, *CANCEL*, and all the responses, according to the specifications. Therefore, it can be used in re-*INVITE*, but cannot be used in initial *INVITE*.

v.5.2. Supported headers in the INVITE response

Appendix Table v-7/JT-Q3401: Supported headers in the INVITE response

Message type: Response

Method: INVITE

Header	Appli-cation	Reference	RFC status	Status in this standard	Application conditions	Remarks
Accept	2xx	RFC3261	o	o		
Accept	415	RFC3261	c	c		
Accept-Encoding	2xx	RFC3261	o	o		
Accept-Encoding	415	RFC3261	c	c		
Accept-Language	2xx	RFC3261	o	o		
Accept-Language	415	RFC3261	c	c		
Alert-Info	180	RFC3261	o	o		(Note 1)
Allow	2xx	RFC3261	m*	m*		c1
Allow	405	RFC3261	m	m		
Allow	r	RFC3261	o	o		
Allow-Events	2xx	RFC3265	o	o	c2 (Appendix Table iv-2, Items 3 and 6)	
Authentication-Info	2xx	RFC3261	o	–	c3	
Call-ID		RFC3261	m	m		
Call-Info		RFC3261	o	o		(Note 1)
Contact	1xx	RFC3261	o	o	c9	
Contact	2xx	RFC3261	m	m		
Contact	3xx	RFC3261	o	o		(Note 2)
Contact	485	RFC3261	o	o		
Content-Disposition		RFC3261	o	o		
Content-Encoding		RFC3261	o	o		
Content-Language		RFC3261	o	o		
Content-Length		RFC3261	t	t		
Content-Type		RFC3261	*	*		
CSeq		RFC3261	m	m		
Date		RFC3261	o	o		(Note 1)
Error-Info	300-699	RFC3261	o	o		(Note 1)
Expires			o	o		(Note 1)
From		RFC3261	m	m		
History-Info		RFC4244	o	o / –	c4 (when Appendix Table iv-9, Item 7 is stated "Used in each session as necessary ".)	
				–	c4 (when Appendix Table iv-9, Item 7 is stated "Not use".)	
MIME-Version		RFC3261	o	o		
Min-SE	422	RFC4028	m	m	c10 (Appendix Table iv-9, Item 1)	
Organization		RFC3261	o	o		(Note 1)
P-Access-Network-Info		RFC3455	o	o		(Note 1)
P-Asserted-Identity		RFC3325	o	o / -	c7	(Note 1)
P-Charging-Function-Addresses		RFC3455	o	o	c5 (when Appendix Table iv-16, Item 1 is stated "Use".)	(Note 1)
				–	c5 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
P-Charging-Vector		RFC3455	o	o	c5 (when Appendix Table iv-16, Item 1 is stated "Use".)	
				–	c5 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
P-Preferred-Identity		RFC3325	o	–	c6	
Privacy		RFC3323	o	o / –	c7	(Note 1)
Proxy-Authenticate	401	RFC3261	o	–	c3	
Proxy-Authenticate	407	RFC3261	m	–	c3	
Reason	404	RFC3326	o	o	c8	
Reason	others	RFC3326	o	o		(Note 1)

Record-Route	18x 2xx	RFC3261	o	o	c9	
Reply-To		RFC3261	o	o		(Note 1)
Require		RFC3261	c	c	c9,c10	
Retry-After	404 413 480 486	RFC3261	o	o		(Note 1)
Retry-After	500 503	RFC3261	o	o		(Note 1)
Retry-After	600 603	RFC3261	o	o		(Note 1)
RSeq	1xx	RFC3262	o	o	c9	
Server		RFC3261	o	o		(Note 1)
Session-Expires	2xx	RFC4028	o	m	c10 (when Appendix Table iv-9, Item 1 is stated "Used in all sessions".)	
				o	c10 (when Appendix Table iv-9, Item 1 is stated "Used in each session as necessary ".)	
Supported	2xx	RFC3261	m*	m*		
Timestamp		RFC3261	o	o		(Note 1)
To		RFC3261	m	m		
Unsupported	420	RFC3261	m	m		
User-Agent		RFC3261	o	o		(Note 1)
Via		RFC3261	m	m		
Warning	488	RFC3261	o	o	c11	
Warning	others	RFC3261	o	o		(Note 1)
WWW-Authenticate	401	RFC3261	m	–	c3	
WWW-Authenticate	407	RFC3261	o	–	c3	
Message body		RFC3261	o	o		

c1: The setting of *Allow* header is necessary for *2xx* response of initial *INVITE*, according to clause 10.2.1.20.5 in the main body. (Note that the *2xx* response without the setting is not handled as error when received.)

c2: In the case that *SUBSCRIBE*/*NOTIFY* is available between networks, the header information is handled as valid information. (Appendix Table iv-2, Items 3 and 6)

c3: Authentication procedures are not supported between networks, according to 10.2.1.8.1.3 of Annex Table a-1 in Annex a.3.

c4: In the case that the request history retention function (*histinfo*) is available between networks, the header can be used (Appendix Table iv-9, Item 7). Note that it is applicable only to the response to a request outside existing dialogs which necessitates the recording of route information, and not applicable to the response to a re-*INVITE* request.

c5: Use of headers for inter-carrier charging (*P-Charging-Vector*, *P-Charging-Function-Address*) (Appendix Table iv-16, Item 1)

c6: Use of *P-Preferred-Identity* header is not applicable, according to clause 10.2.2.2.3 in the main body.

c7: *P-Asserted-Identity* and *Privacy* headers are applicable only to the request and response outside existing dialogs, according to 10.2.2.2.2 and 10.2.2.2.4 of Annex Table a-1 in Annex a.3. (The header is applicable only to the response to initial *INVITE*.)

c8: By setting the *Reason* header to a *404 (Not found)* response and using values of Annex e, it is possible when encountering an unallocated number to guarantee it is an unallocated number in the terminating network and to lead to the behaviour providing an unallocated number talkie etc. in the originating network, according to 10.2.2.2.6 of Annex Table a-1 in Annex a.3 and Annex e.

c9: In the case of providing a reliable provisional response, the setting of "*100rel*" to the *Require* header and the setting of *RSeq* header is necessary, according to clause 10.2.2.2.7 in the main body. The setting of *Contact* header is necessary to receive a subsequent *PRACK* request. In the case that *Record-Route* header is set to the *2xx* response of an *INVITE* request, the *Record-Route* header of the same content should be set to the reliable provisional response as well.

c10: The header must be used as specified in clause 10.2.1.20.32, 10.2.2.2.1 and 10.2.2.2.8 in the main body. In the case that Session-Timer is used, at least the setting of value to the *Session-Expires* header (*delta-seconds*) is necessary. In the case that the refresher is "*uac*", the setting of "*timer*" to the *Require* header is necessary. (Appendix Table iv-9, Item 1)

c11: It is possible to notify the IP version conflict from the terminating network to the originating network by setting the Warning header to the *488 (Not Acceptable Here)* response and using values of Appendix i, according to 13 of Annex Table a-1 in Annex a.3 and Appendix i.

Note 1 When specified, whether expected behaviours are performed or the capabilities for the behaviours are provided is dependent on the policy of the connected carrier.

Note 2 In the case that the redirection function of *3xx* response is available between networks, the header information is handlef as valid information, according to clause 10.2.1.8.3 in the main body. (Appendix Table iv-14, Item 1)

v.6. UPDATE

This message is used for refreshing a call (Session-Timer) and modifying media stream setting information during a call.

v.6.1. Supported headers in the UPDATE request

Appendix Table v- 8/JT-Q3401: Supported headers in the UPDATE request

Message type: Request

Method: UPDATE

Header	Reference	RFC status	Status in this standard	Application conditions	Remarks
Accept	RFC3261	o	o		
Accept-Contact	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Accept-Encoding	RFC3261	o	o		
Accept-Language	RFC3261	o	o		
Allow	RFC3261	o	o		
Authorization	RFC3261	o	-	c2	
Call-ID	RFC3261	m	m		
Call-Info	RFC3261	o	o		(Note 1)
Contact	RFC3261	m	m		
Content-Disposition	RFC3261	o	o		
Content-Encoding	RFC3261	o	o		
Content-Language	RFC3261	o	o		
Content-Length	RFC3261	t	t		
Content-Type	RFC3261	*	*		
CSeq	RFC3261	m	m		
Date	RFC3261	o	o		(Note 1)
From	RFC3261	m	m		
Max-Forwards	RFC3261	m	m		
MIME-Version	RFC3261	o	o		
Min-SE	RFC4028	o	o	c3	
Organization	RFC3261	o	o		(Note 1)
P-Access-Network-Info	RFC3455	o	o		(Note 1)
P-Charging-Function-Addresses	RFC3455	o	o	c4 (when Appendix Table iv-16, No. 1 is stated "Use".)	(Note 1)
			–	c4 (when Appendix Table iv-16, No. 1 is stated "Not use".)	
P-Charging-Vector	RFC3455	o	o	c4 (when Appendix Table iv-16, No. 1 is stated "Use".)	
			–	c4 (when Appendix Table iv-16, No. 1 is stated "Not use".)	
Privacy	RFC3323	o	–	c5	
Proxy-Authorization	RFC3261	o	–	c2	
Proxy-Require	RFC3261	o	o		
Reason	RFC3326	o	o		(Note 1)
Record-Route	RFC3261	o	o		(Note 1)
Referred-By	RFC3892		o	c6 (Appendix Table iv-2, Items 4 and 5)	
Reject-Contact	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Request-Disposition	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Require	RFC3261	c	c	c7	
Route	RFC3261	c	c		
Session-Expires	RFC4028	o	m	c3 (when Appendix Table iv-9, Item 1 is stated "Used in all sessions".)	
			o	c3 (when Appendix Table iv-9, Item 1 is stated "Used in each session as necessary ".)	
Supported	RFC3261	o	o	c7	
Timestamp	RFC3261	o	o		(Note 1)
To	RFC3261	m	m		
User-Agent	RFC3261	o	o		(Note 1)

Via	RFC3261	m	m		
Message body	RFC3261	o	o		

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available between networks, the header information is handled as valid information. (Appendix Table iv-9, Item 6) (RFC3840 and RFC3841)

c2: Authentication procedures are not supported between networks, according to 10.2.1.8.1.3 of Annex Table a-1 in Annex a.3.

c3: The header must be used as specified in clause 10.2.2.2.1 and 10.2.2.2.8 in the main body. In the case that Session-Timer is used, at least the setting of value to the *Session-Expires* header (*delta-seconds*) is necessary.

c4: Use of headers for inter-carrier charging (*P-Charging-Vector*, *P-Charging-Function-Address*) (Appendix Table iv-16, Item 1)

c5: *Privacy* header is applicable only to the request and response outside existing dialogs, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.

c6: *Referred-By* header may be used as a result of using *REFER* (Appendix Table iv-2, Items 4 and 5). In the case that *REFER* is available between networks, the header information may be handled as valid information. It does not guarantee that the *Referred-By* header is used as a result of using *REFER*.

c7: "*timer*" needs to be set to the *Require* header or the *Supported* header in terms of the context, according to clause 10.2.1.20.32 and 10.2.1.20.37 in the main body. ("*100rel*" is contextually set to the *Supported* header of initial *INVITE*. "*timer*" should be contextually set to the *Supported* header of initial *INVITE* and re-*INVITE*.)

Note 1 When specified, whether expected behaviours are performed or the capabilities for the behaviours are provided is dependent on the policy of the connected carrier.

v.6.2. Supported headers in the UPDATE response

Appendix Table v-9/JT-Q3401: Supported headers in the UPDATE response

Message type: Response

Method: UPDATE

Header	Appli-cation	Reference	RFC status	Status in this standard	Application conditions	Remarks
Accept	2xx	RFC3261	o	o		
Accept	415	RFC3261	c	c		
Accept-Encoding	2xx	RFC3261	o	o		
Accept-Encoding	415	RFC3261	c	c		
Accept-Language	2xx	RFC3261	o	o		
Accept-Language	415	RFC3261	c	c		
Allow	2xx	RFC3261	o	o		
Allow	405	RFC3261	m	m		
Allow	r	RFC3261	o	o		
Authentication-Info	2xx	RFC3261	o	–	c1	
Call-ID		RFC3261	m	m		
Call-Info		RFC3261	o	o		(Note 1)
Contact	1xx	RFC3261	o	o		
Contact	2xx	RFC3261	m	m		
Contact	3xx	RFC3261	o	o		
Contact	485	RFC3261	o	o		
Content-Disposition		RFC3261	o	o		
Content-Encoding		RFC3261	o	o		
Content-Language		RFC3261	o	o		
Content-Length		RFC3261	t	t		
Content-Type		RFC3261	*	*		
CSeq		RFC3261	m	m		
Date		RFC3261	o	o		(Note 1)
Error-Info	300-699	RFC3261	o	o		
From		RFC3261	m	m		
MIME-Version		RFC3261	o	o		
Min-SE	422	RFC4028	m	m	c2 (Appendix Table iv-9, Item 1)	
Organization		RFC3261	o	o		(Note 1)
P-Access-Network-Info		RFC3455	o	o		(Note 1)
P-Charging-Function-Addresses		RFC3455	o	o	c3 (when Appendix Table iv-16, Item 1 is stated "Use".)	(Note 1)
				–	c3 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
P-Charging-Vector		RFC3455	o	o	c3 (when Appendix Table iv-16, Item 1 is stated "Use".)	
				–	c3 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
Privacy		RFC3323	o	–	c4	
Proxy-Authenticate	401	RFC3261	o	–	c1	
Proxy-Authenticate	407	RFC3261	m	–	c1	
Reason		RFC3326	o	o		(Note 1)
Record-Route	18x 2xx	RFC3261	o	o		(Note 1)
Require		RFC3261	c	c	c2	
Retry-After	404 413 480 486	RFC3261	o	o		(Note 1)
Retry-After	500 503	RFC3261	o	o		(Note 1)
Retry-After	600 603	RFC3261	o	o		(Note 1)
Server		RFC3261	o	o		(Note 1)

Session-Expires	2xx	RFC4028	o	m	c2 (when Appendix Table iv-9, Item 1 is stated "Used in all sessions".)	
				o	c2 (when Appendix Table iv-9, Item 1 is stated "Used in each session as necessary ".)	
Supported	2xx	RFC3261	o	o		
Timestamp		RFC3261	o	o		(Note 1)
To		RFC3261	m	m		
Unsupported	420	RFC3261	m	m		
User-Agent		RFC3261	o	o		(Note 1)
Via		RFC3261	m	m		
Warning		RFC3261	o	o		(Note 1)
WWW-Authenticate	401	RFC3261	m	–	c1	
WWW-Authenticate	407	RFC3261	o	–	c1	
Message body		RFC3261	o	o		

c1: Authentication procedures are not supported between networks, according to 10.2.1.8.1.3 of Annex Table a-1 in Annex a.3.

c2: The header must be used as specified in clause 10.2.1.20.32, 10.2.2.2.1 and 10.2.2.2.8 in the main body. In the case that Session-Timer is used, at least the setting of value to the ***Session-Expires*** header (*delta-seconds*) is necessary. In the case that Refresher is "*uac*", the setting of "*timer*" to the ***Require*** header is necessary. (Appendix Table iv-9, Item 1)

c3: Use of headers for inter-carrier charging (*P-Charging-Vector*, *P-Charging-Function-Address*) (Appendix Table iv-16, Item 1)

c4: *Privacy* header is applicable only to the request and response outside existing dialogs, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.

Note 1 When specified, whether expected behaviours are performed or the capabilities for the behaviours are provided is dependent on the policy of the connected carrier.

v.7. PRACK

This message is used for providing a reliable provisional response message (*100rel*) in call establishment.

v.7.1. Supported headers in the PRACK request

Appendix Table v-10/JT-Q3401: Supported headers in the PRACK request

Message type: Request

Method: PRACK

Header	Reference	RFC status	Status in this standard	Application conditions	Remarks
Accept	RFC3261	o	o		
Accept-Contact	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Accept-Encoding	RFC3261	o	o		
Accept-Language	RFC3261	o	o		
Allow	RFC3261	o	o		
Allow-Events	RFC3265	o	o	c2 (Appendix Table iv-2, Items 3 and 6)	
Authorization	RFC3261	o	–	c3	
Call-ID	RFC3261	m	m		
Content-Disposition	RFC3261	o	o		
Content-Encoding	RFC3261	o	o		
Content-Language	RFC3261	o	o		
Content-Length	RFC3261	t	t		
Content-Type	RFC3261	*	*		
CSeq	RFC3261	m	m		
Date	RFC3261	o	o		(Note 1)
From	RFC3261	m	m		
Max-Forwards	RFC3261	m	m		
MIME-Version	RFC3261	o	o		
P-Access-Network-Info	RFC3455	o	o		(Note 1)
P-Charging-Function-Addresses	RFC3455	o	o	c4 (when Appendix Table iv-16, No. 1 is stated "Use".)	(Note 1)
			–	c4 (when Appendix Table iv-16, No. 1 is stated "Not use".)	
P-Charging-Vector	RFC3455	o	o	c4 (when Appendix Table iv-16, No. 1 is stated "Use".)	
			–	c4 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
Privacy	RFC3323	o	–	c5	
Proxy-Authorization	RFC3261	o	–	c3	
Proxy-Require	RFC3261	o	o		
RAck	RFC3262	m	m		
Reason	RFC3326	o	o		(Note 1)
Record-Route	RFC3261	o	o		(Note 1)
Referred-By	RFC3892		o	c6 (Appendix Table iv-2, Items 4 and 5)	
Reject-Contact	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Request-Disposition	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Require	RFC3261	c	c		
Route	RFC3261	c	c		
Supported	RFC3261	o	o		(Note 1)
Timestamp	RFC3261	o	o		(Note 1)
To	RFC3261	m	m		
User-Agent	RFC3261	o	o		(Note 1)
Via	RFC3261	m	m		
Message body	RFC3261	o	o	c7 (Appendix Table iv-12, Item 1)	

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available between networks, the header information is handled as valid information. (Appendix Table iv-9, Item 6) (RFC3840 and RFC3841)

c2: In the case that *SUBSCRIBE*/*NOTIFY* is available between networks, the header information is handled as valid information. (Appendix Table iv-2, Items 3 and 6)

c3:	Authentication procedures are not supported between networks, according to 10.2.1.8.1.3 of Annex Table a-1 in Annex a.3.
c4:	Use of headers for inter-carrier charging (*P-Charging-Vector*, *P-Charging-Function-Address*) (Appendix Table iv-16, Item 1)
c5:	*Privacy* header is applicable only to the request and response outside existing dialogs, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.
c6:	*Referred-By* header may be used as a result of using *REFER* (Appendix Table iv-2, Items 4 and 5). In the case that *REFER* is available between networks, the header information may be handled as valid information. It does not guarantee that the *Referred-By* header is used as a result of using *REFER*.
c7:	The message body part of *PRACK* should be supported, according to clause 10.2.1.7.4.1 in the main body. In the case that the SDP setting of the body part is available between networks, the message body information is handled as valid information. (Appendix Table iv-12, Item 1)
Note 1	When specified, whether expected behaviours are performed or the capabilities for the behaviours are provided is dependent on the policy of the connected carrier.

v.7.2. Supported headers in the PRACK response

Appendix Table v-11/JT-Q3401: Supported headers in the PRACK response

Message type: Response

Method: PRACK

Header	Appli-cation	Reference	RFC status	Status in this standard	Application conditions	Remarks
Accept	415	RFC3261	c	c		
Accept-Encoding	415	RFC3261	c	c		
Accept-Language	415	RFC3261	c	c		
Allow	2xx	RFC3261	o	o		
Allow	405	RFC3261	m	m		
Allow	r	RFC3261	o	o		
Allow-Events	2xx	RFC3265	o	o	c1 (Appendix Table iv-2, Items 3 and 6)	
Authentication-Info	2xx	RFC3261	o	–	c2	
Call-ID		RFC3261	m	m		
Contact	3xx	RFC3261	o	o		
Contact	485	RFC3261	o	o		
Content-Disposition		RFC3261	o	o		
Content-Encoding		RFC3261	o	o		
Content-Language		RFC3261	o	o		
Content-Length		RFC3261	t	t		
Content-Type		RFC3261	*	*		
CSeq		RFC3261	m	m		
Date		RFC3261	o	o		(Note 1)
Error-Info	300-699	RFC3261	o	o		(Note 1)
From		RFC3261	m	m		
MIME-Version		RFC3261	o	o		
P-Access-Network-Info		RFC3455	o	o		(Note 1)
P-Charging-Function-Addresses		RFC3455	o	o	c3 (when Appendix Table iv-16, Item 1 is stated "Use".)	(Note 1)
				–	c3 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
P-Charging-Vector		RFC3455	o	o	c3 (when Appendix Table iv-16, Item 1 is stated "Use".)	
				–	c3 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
Privacy		RFC3323	o	–	c4	
Proxy-Authenticate	401	RFC3261	o	–	c2	
Proxy-Authenticate	407	RFC3261	m	–	c2	
Reason		RFC3326	o	o		(Note 1)
Record-Route	18x 2xx	RFC3261	o	o		(Note 1)
Require		RFC3261	c	c		
Retry-After	404 413 480 486	RFC3261	o	o		(Note 1)
Retry-After	500 503	RFC3261	o	o		(Note 1)
Retry-After	600 603	RFC3261	o	o		(Note 1)
Server		RFC3261	o	o		(Note 1)
Supported	2xx	RFC3261	o	o		
Timestamp		RFC3261	o	o		(Note 1)
To		RFC3261	m	m		
Unsupported	420	RFC3261	m	m		
User-Agent		RFC3261	o	o		(note 1)
Via		RFC3261	m	m		
Warning		RFC3261	o	o		(Note 1)

WWW-Authenticate	401	RFC3261	m	–	c2	
Message body		RFC3261	o	o	c5	

c1: In the case that *SUBSCRIBE*/*NOTIFY* is available between networks, the header information is handled as valid information. (Appendix Table iv-2, Items 3 and 6)

c2: Authentication procedures are not supported between networks, according to 10.2.1.8.1.3 of Annex Table a-1 in Annex a.3.

c3 Use of headers for inter-carrier charging (*P-Charging-Vector*, *P-Charging-Function-Address*) (Appendix Table iv-16, Item 1)

c4: *Privacy* header is applicable only to the request and response outside existing dialogs, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.

c5: The message body part of *PRACK* should be supported, according to clause 10.2.1.7.4.1 in the main body. In the case that the SDP setting of the body part is available between networks, the message body information is handled as valid information. (Appendix Table iv-12, Item 1)

Note 1 When specified, whether expected behaviours are performed or the capabilities for the behaviours are provided is dependent on the policy of the connected carrier.

v.8. MESSAGE

This message is used for stateless short message services. *MESSAGE* can be used outside existing dialogs. The support for this method is optional and is used on bilateral agreement between carriers.

v.8.1. Supported headers in the MESSAGE request

Appendix Table v-12/JT-Q3401: Supported headers in the MESSAGE request

Message type: Request

Method: MESSAGE

Header	Reference	RFC status	Status in this standard	Application conditions	Remarks
Accept-Contact	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Allow	RFC3261	o	o		
Allow-Events	RFC3265		–		
Authorization	RFC3261	o	–	c2	
Call-ID	RFC3261	m	m		
Call-Info	RFC3261	o	o		(Note 1)
Content-Disposition	RFC3261	o	o		
Content-Encoding	RFC3261	o	o		
Content-Language	RFC3261	o	o		
Content-Length	RFC3261	t	t		
Content-Type	RFC3261	*	*		
CSeq	RFC3261	m	m		
Date	RFC3261	o	o		(Note 1)
Expires	RFC3261	o	o		(Note 1)
From	RFC3261	m	m		
History-Info	RFC4244	o	o / –	c3 (when Appendix Table iv-9, Item 7 is stated "Used in each session as necessary ".)	
			–	c3 (when Appendix Table iv-9, Item 7 is stated "Not use".)	
In-Reply-To	RFC3261	o	o		(Note 1)
Max-Forwards	RFC3261	m	m		
MIME-Version	RFC3261		o		
Organization	RFC3261	o	o		(Note 1)
P-Access-Network-Info	RFC3455	o	o		(Note 1)
P-Asserted-Identity	RFC3325		m / –	c4	
P-Called-Party-ID	RFC3455	o	o		(Note 1)
P-Charging-Function-Addresses	RFC3455	o	o	c5 (when Appendix Table iv-16, Item 1 is stated "Use".)	(Note 1)
			–	c5 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
P-Charging-Vector	RFC3455	o	o	c5 (when Appendix Table iv-16, Item 1 is stated "Use".)	
			–	c5 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
P-Preferred-Identity	RFC3325		–	c6	
P-Visited-Network-ID	RFC3455	o	o		(Note 1)
Priority	RFC3261	o	o		(Note 1)
Privacy	RFC3323		m* / –	c7	
Proxy-Authorization	RFC3261	o	–	c2	
Proxy-Require	RFC3261	o	o		
Reason	RFC3326	– / o	– / o	(Note 2)	(Note 1)
Referred-By	RFC3892		o	c8 (Appendix Table iv-2, Items 4 and 5)	
Reject-Contact	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Reply-To	RFC3261	o	o		(Note 1)
Request-Disposition	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Require	RFC3261	c	c		
Route	RFC3261	o	o		
Subject	RFC3261	o	o		(Note 1)

Supported	RFC3261		–		
Timestamp	RFC3261	o	o		(Note 1)
To	RFC3261	m	m		
User-Agent	RFC3261	o	o		(Note 1)
Via	RFC3261	m	m		
Message body	RFC3261	o	o		

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available between networks, the header information is handled as valid information. (Appendix Table iv-9, Item 6) (RFC3840 and RFC3841)

c2: Authentication procedures are not supported between networks, according to 10.2.1.8.1.3 of Annex Table a-1 in Annex a.3.

c3: In the case that the request history retention function (*histinfo*) is available between networks, the header can be used (Appendix Table iv-9, Item 7). Note that it is applicable only to the request outside existing dialogs which necessitates the recording of route information, and not applicable to the request inside an existing dialog.

c4: *P-Asserted-Identity* header needs to be set for a request outside existing dialogs and is not used inside a request, according to 10.2.2.2.2 of Annex Table a-1 in Annex a.3. It transmits the calling-party's information. (The setting is necessary for a *MESSAGE* request outside existing dialogs, but not necessary for a *MESSAGE* request inside an existing dialog.)

c5: Use of headers for inter-carrier charging (*P-Charging-Vector*, *P-Charging-Function-Address*) (Appendix Table iv-16, Item 1)

c6: Use of *P-Preferred-Identity* header is not applicable, according to clause 10.2.2.2.3 in the main body.

c7: *Privacy* header needs to be set for a request outside existing dialogs and transmits the presentation/restriction information of the calling-party, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3. (Use of the header in a *MESSAGE* request outside existing dialogs is necessary, but not necessary for a *MESSAGE* request inside an existing dialog. In the case that this header is not present in a *MESSAGE* request outside existing dialogs, the calling-party's information is handled to be possible to be notified.)

c8: *Referred-By* header may be used as a result of using *REFER* (Appendix Table iv-2, Items 4 and 5). In the case that *REFER* is available between networks, the header information may be handled as valid information. It does not guarantee that the *Referred-By* header is used as a result of using *REFER*.

Note 1 When specified, whether expected behaviours are performed or the capabilities for the behaviours are provided is dependent on the policy of the connected carrier.

Note 2 *Reason* header is specified in RFC3326, and it is applicable to all the requests inside an existing dialog, *CANCEL*, and all the responses, according to the specifications. Therefore, it can be used in a *MESSAGE* request inside an existing dialog, but cannot be used in a *MESSAGE* request outside existing dialogs.

v.8.2. Supported headers in the MESSAGE response

Appendix Table v-13/JT-Q3401: Supported headers in the MESSAGE response

Message type: Response

Method: MESSAGE

Header	Appli-cation	Reference	RFC status	Status in this standard	Application conditions	Remarks
Accept	415	RFC3261	m*	m*		
Accept-Encoding	415	RFC3261	m*	m*		
Accept-Language	415	RFC3261	m*	m*		
Allow	2xx	RFC3261	o	o		
Allow	405	RFC3261	m	m		
Allow	r	RFC3261	o	o		
Allow-Events				–		
Authentication-Info	2xx	RFC3261	o	–	c1	
Call-ID		RFC3261	m	m		
Call-Info		RFC3261	o	o		(Note 1)
Contact	3xx	RFC3261	o	o		(Note 2)
Contact	485	RFC3261	o	o		
Content-Disposition		RFC3261	o	o		
Content-Encoding		RFC3261	o	o		
Content-Language		RFC3261	o	o		
Content-Length		RFC3261	t	t		
Content-Type		RFC3261	*	*		
CSeq		RFC3261	m	m		
Date		RFC3261	o	o		(Note 1)
Error-Info	300-699	RFC3261	o	o		(Note 1)
Expires		RFC3261	o	o		(Note 1)
From		RFC3261	m	m		
History-Info		RFC4244	o	o / –	c2 (when Appendix Table iv-9, Item 7 is stated "Used in each session as necessary ".)	
				–	c2 (when Appendix Table iv-9, Item 7 is stated "Not use".)	
MIME-Version	4xx-6xx	RFC3261		o		
Organization		RFC3261	o	o		(Note 1)
P-Access-Network-Info		RFC3455	o	o		(Note 1)
P-Asserted-Identity		RFC3325		o / –	c3	(Note 1)
P-Charging-Function-Addresses		RFC3455	o	o	c4 (when Appendix Table iv-16, No. 1 is stated "Use".)	(Note 1)
				–	c4 (when Appendix Table iv-16, No. 1 is stated "Not use".)	
P-Charging-Vector		RFC3455	o	o	c4 (when Appendix Table iv-16, No. 1 is stated "Use".)	
				–	c4 (when Appendix Table iv-16, No. 1 is stated "Not use".)	
P-Preferred-Identity		RFC3325		–	c5	
Privacy		RFC3323		o / –	c3	(Note 1)
Proxy-Authenticate	401	RFC3261	o	–	c1	
Proxy-Authenticate	407	RFC3261	m	–	c1	
Reason		RFC3326	o	o		(Note 1)
Reply-To		RFC3261	o	o		(Note 1)
Require		RFC3261	c	c		(Note 1)
Retry-After	404 413 480 486	RFC3261	o	o		(Note 1)
Retry-After	500 503	RFC3261	o	o		(Note 1)

Retry-After	600 603	RFC3261	o	o		(Note 1)
Server		RFC3261	o	o		(Note 1)
Supported		RFC3261		–		(Note 1)
Timestamp		RFC3261	o	o		(Note 1)
To		RFC3261	m	m		
Unsupported	420	RFC3261	m	m		
User-Agent		RFC3261	o	o		(Note 1)
Via		RFC3261	m	m		
Warning		RFC3261	o	o		(Note 1)
WWW-Authenticate	401	RFC3261	m	–	c1	
WWW-Authenticate	407	RFC3261	o	–	c1	
Message body	2xx- 3xx	RFC3428	–	–		
Message body	4xx- 6xx	RFC3428	o	o		

c1:	Authentication procedures are not supported between networks, according to 10.2.1.8.1.3 of Annex Table a-1 in Annex a.3.
c2:	In the case that the request history retention function (*histinfo*) is available between networks, the header can be used (Appendix Table iv-9, Item 7). Note that it is applicable only to the response to a request outside existing dialogs which necessitates the recording of route information, and not applicable to the response to a request inside an existing dialog.
c3:	*P-Asserted-Identity* and *Privacy* headers are applicable only to the request and response outside existing dialogs, according to 10.2.2.2.2 and 10.2.2.2.4 of Annex Table a-1 in Annex a.3. (The header is applicable only to the *MESSAGE* response outside existing dialogs.)
c4:	Use of headers for inter-carrier charging (*P-Charging-Vector*, *P-Charging-Function-Address*) (Appendix Table iv-16, Item 1)
c5:	Use of *P-Preferred-Identity* header is not applicable, according to clause 10.2.2.2.3 in the main body.
Note 1	When specified, whether expected behaviours are performed or the capabilities for the behaviours are provided is dependent on the policy of the connected carrier.
Note 2	In the case that the redirection function of 3xx response is available between networks, the header information is handled as valid information, according to clause 10.2.1.8.3 in the main body. (Appendix Table iv-14, Item 1)

v.9. SUBSCRIBE

This message is used to establish an event subscription (event dialog).

v.9.1. Supported headers in the SUBSCRIBE request

Appendix Table v-14/JT-Q3401: Supported headers in the SUBSCRIBE request

Message type: Request

Method: SUBSCRIBE

Header	Reference	RFC status	Status in this standard	Application conditions	Remarks
Accept	RFC3261	o	o		
Accept-Contact	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Accept-Encoding	RFC3261	o	o		
Accept-Language	RFC3261	o	o		
Allow	RFC3261	o	o		
Allow-Events	RFC3265	o	o		
Authorization	RFC3261	o	–	c2	
Call-ID	RFC3261	m	m		
Call-Info	RFC3261		–	(Note 2)	
Contact	RFC3261	m	m		
Content-Disposition	RFC3261	o	o		
Content-Encoding	RFC3261	o	o		
Content-Language	RFC3261	o	o		
Content-Length	RFC3261	t	t		
Content-Type	RFC3261	*	*		
CSeq	RFC3261	m	m		
Date	RFC3261	o	o		(Note 1)
Event	RFC3265	m	m		
Expires	RFC3261	o	o		
From	RFC3261	m	m		
History-Info	RFC4244	o	o / –	c3 (when Appendix Table iv-9, Item 7 is stated "Used in each session as necessary ".)	
			–	c3 (when Appendix Table iv-9, Item 7 is stated "Not use".)	
Max-Forwards	RFC3261	m	m		
MIME-Version	RFC3261	o	o		
Organization	RFC3261	o	o		(Note 1)
P-Access-Network-Info	RFC3455	o	o		(Note 1)
P-Asserted-Identity	RFC3325	o	m / –	c4	
P-Called-Party-ID	RFC3455	o	o		(Note 1)
P-Charging-Function-Addresses	RFC3455	o	o	c5 (when Appendix Table iv-16, Item 1 is stated "Use".)	(Note 1)
			–	c5 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
P-Charging-Vector	RFC3455	o	o	c5 (when Appendix Table iv-16, Item 1 is stated "Use".)	
			–	c5 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
P-Preferred-Identity	RFC3325	o	–	c6	
P-Visited-Network-ID	RFC3455	o	o		(Note 1)
Priority	RFC3261	o	o		(Note 1)
Privacy	RFC3323	o	m* / –	c7	
Proxy-Authorization	RFC3261	o	–	c2	
Proxy-Require	RFC3261	o	o		
Reason	RFC3326	– / o	– / o	(Note 3)	(Note 1)
Record-Route	RFC3261	o	o		
Referred-By	RFC3892		o	c8 (Appendix Table iv-2, Items 4 and 5)	
Reject-Contact	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Request-Disposition	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Require	RFC3261	o	o		

Route	RFC3261	c	c		
Supported	RFC3261	o	o		
Timestamp	RFC3261	o	o		(Note 1)
To	RFC3261	m	m		
User-Agent	RFC3261	o	o		(Note 1)
Via	RFC3261	m	m		
Message body			o	(Note 4)	

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available between networks, the header information is handled as valid information. (Appendix Table iv-9, Item 6) (RFC3840 and RFC3841)

c2: Authentication procedures are not supported between networks, according to 10.2.1.8.1.3 of Annex Table a-1 in Annex a.3.

c3: In the case that the request history retention function (*histinfo*) is available between networks, the header can be used (Appendix Table iv-9, Item 7). Note that it is applicable only to the request outside existing dialogs which necessitates the recording of route information, and not applicable to the request inside an existing dialog.

c4: *P-Asserted-Identity* header needs to be set for a request outside existing dialogs (not to be used inside an existing dialog) and transmits the calling-party's information, according to 10.2.2.2.2 of Annex Table a-1 in Annex a.3 and Annex c. (The setting is necessary for initial *SUBSCRIBE*, but not necessary for re-*SUBSCRIBE*.)

c5: Use of headers for inter-carrier charging (*P-Charging-Vector*, *P-Charging-Function-Address*) (Appendix Table iv-16, Item 1)

c6: Use of *P-Preferred-Identity* header is not applicable, according to clause 10.2.2.2.3 in the main body.

c7: *Privacy* header needs to be set for a request outside existing dialogs and transmits the presentation/restriction information of the calling-party, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3 and Annex c. (The setting is necessary for initial *SUBSCRIBE*, but not necessary for re-*SUBSCRIBE*. In the case that this header is not present in initial *SUBSCRIBE*, the calling-party's information is handled to be possible to be notified.)

c8: *Referred-By* header may be used as a result of using *REFER* (Appendix Table iv-2, Items 4 and 5). In the case that *REFER* is available between networks, the header information may be handled as valid information. It does not guarantee that the *Referred-By* header is used as a result of using *REFER*.

Note 1 When specified, whether expected behaviours are performed or the capabilities for the behaviours are provided is dependent on the policy of the connected carrier.

Note 2 *Call-Info* shows additional information about the sender of the messages. There is no description of the application of the header into *SUBSCRIBE* in RFCs and other documents. Therefore, it is difficult to define its reaction in the case of using the header in *SUBSCRIBE*. Furthermore, security risks of *Call-Info* are noted in RFC3261. An ill-prepared use of the header should be avoided.

Note 3 *Reason* header is specified in RFC3326, and it is applicable to all the requests inside an existing dialog, *CANCEL*, and all the responses, according to the specifications. Therefore, it can be used in re-*SUBSCRIBE*, but cannot be used in initial *SUBSCRIBE*.

Note 4 It is used when notification information is present. Formatting and other features depend on *Content-Type*.

v.9.2. Supported headers in the SUBSCRIBE response

Appendix Table v-15/JT-Q3401: Supported headers in the SUBSCRIBE response

Message type: Response

Method: SUBSCRIBE

Header	Appli-cation	Reference	RFC status	Status in this standard	Application conditions	Remarks
Accept	415	RFC3261	o	o		
Accept-Encoding	415	RFC3261	o	o		
Accept-Language	415	RFC3261	o	o		
Allow	2xx	RFC3261	o	o		
Allow	405	RFC3261	m	m		
Allow	r	RFC3261	o	o		
Allow-Events	2xx	RFC3265	o	o		
Allow-Events	489	RFC3265	m	m		
Authentication-Info	2xx	RFC3261	o	–	c1	
Call-ID		RFC3261	m	m		
Call-Info		RFC3261		–	(Note 2)	
Contact	1xx	RFC3261	o	o		
Contact	2xx	RFC3261	m	m		
Contact	3xx	RFC3261	m	m		
Contact	485	RFC3261	o	o		
Content-Disposition		RFC3261	o	o		
Content-Encoding		RFC3261	o	o		
Content-Language		RFC3261	o	o		
Content-Length		RFC3261	t	t		
Content-Type		RFC3261	*	*		
CSeq		RFC3261	m	m		
Date		RFC3261	o	o		(Note 1)
Error-Info	300-699	RFC3261	o	o		(Note 1)
Expires	2xx	RFC3261	m	m		
From		RFC3261	m	m		
History-Info		RFC4244	o	o / –	c2 (when Appendix Table iv-9, Item 7 is stated "Used in each session as necessary ".)	
				–	c2 (when Appendix Table iv-9, Item 7 is stated "Not use".)	
Min-Expires	423	RFC3261	m	m		
MIME-Version		RFC3261	o	o		
Organization		RFC3261	o	o		(Note 1)
P-Access-Network-Info		RFC3455	o	o		(Note 1)
P-Asserted-Identity		RFC3325	o	o / –	c3	
P-Charging-Function-Addresses		RFC3455	o	o	c4 (when Appendix Table iv-16, No. 1 is stated "Use".)	(Note 1)
				–	c4 (when Appendix Table iv-16, No. 1 is stated "Not use".)	
P-Charging-Vector		RFC3455	o	o	c4 (when Appendix Table iv-16, No. 1 is stated "Use".)	
				–	c4 (when Appendix Table iv-16, No. 1 is stated "Not use".)	
P-Preferred-Identity		RFC3325	o	–	c5	
Privacy		RFC3323	o	o / –	c3	
Proxy-Authenticate	401	RFC3261		–	c1	
Proxy-Authenticate	407	RFC3261	m	–	c1	
Reason		RFC3326	o	o		(Note 1)
Record-Route	2xx 401 484	RFC3261	o	o		
Require		RFC3261	o	o		

Retry-After	404 413 480 486	RFC3261	o	o		(Note 1)
Retry-After	500 503	RFC3261	o	o		
Retry-After	600 603	RFC3261	o	o		(Note 1)
RSeq	1xx	RFC3262	o	–	(Note 3)	
Server		RFC3261	o	o		(Note 1)
Supported	2xx	RFC3261	o	o		
Timestamp		RFC3261	o	o		(Note 1)
To		RFC3261	m	m		
Unsupported	420	RFC3261	o	o		
User-Agent		RFC3261	o	o		(Note 1)
Via		RFC3261	m	m		
Warning		RFC3261	o	o		(Note 1)
WWW-Authenticate	401	RFC3261	m	–	c1	
WWW-Authenticate	407	RFC3261		–	c1	
Message body				o	(Note 4)	

c1: Authentication procedures are not supported between networks, according to 10.2.1.8.1.3 of Annex Table a-1 in Annex a.3.

c2: In the case that the request history retention function (*histinfo*) is available between networks, the header can be used (Appendix Table iv-9, Item 7). Note that it is applicable only to the response to a request outside existing dialogs which necessitates the recording of route information, and not applicable to the response to a re-*SUBSCRIBE* request.

c3: *P-Asserted-Identity* and *Privacy* headers are applicable only to the request and response outside existing dialogs, according to 10.2.2.2.2 and 10.2.2.2.4 of Annex Table a-1 in Annex a.3. (The header is applicable only to the response to initial *SUBSCRIBE*.)

c4: Use of headers for inter-carrier charging (*P-Charging-Vector*, *P-Charging-Function-Address*) (Appendix Table iv-16, Item 1)

c5: Use of *P-Preferred-Identity* header is not applicable, according to clause 10.2.2.2.3 in the main body.

Note 1 When specified, whether expected behaviours are performed or the capabilities for the behaviours are provided is dependent on the policy of the connected carrier.

Note 2 *Call-Info* shows additional information about the sender of the messages. There is no description of the application of the header into *SUBSCRIBE* in RFCs and other documents. Therefore, it is difficult to define its reaction when using the header in *SUBSCRIBE*. Furthermore, security risks of *Call-Info* are noted in RFC3261. An ill-prepared use of the header should be avoided.

Note 3 The *100rel* option (*PRACK*) is not to be used in *SUBSCRIBE*.

Note 4 It is used when notification information is present. Formatting and other features depend on *Content-Type*.

v.10. NOTIFY

This message is used to notify event-related information within an event subscription (event dialog). *NOTIFY* is used in conjunction with a particular event subscription.

The event subscription is established based on the use of *SUBSCRIBE* method, *REFER* method, or other implicit subscriptions.

v.10.1. Supported headers in the NOTIFY request

Appendix Table v-16/JT-Q3401: Supported headers in the NOTIFY request

Message type: Request

Method: NOTIFY

Header	Reference	RFC status	Status in this standard	Application conditions	Remarks
Accept	RFC3261	o	o		
Accept-Contact	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Accept-Encoding	RFC3261	o	o		
Accept-Language	RFC3261	o	o		
Allow	RFC3261	o	o		
Allow-Events	RFC3265	o	o		
Authorization	RFC3261	o	–	c2	
Call-ID	RFC3261	m	m		
Call-Info	RFC3261		–	(Note 2)	
Contact	RFC3261	m	m		
Content-Disposition	RFC3261	o	o		
Content-Encoding	RFC3261	o	o		
Content-Language	RFC3261	o	o		
Content-Length	RFC3261	t	t		
Content-Type	RFC3261	*	*		
CSeq	RFC3261	m	m		
Date	RFC3261	o	o		(Note 1)
Event	RFC3265	m	m		
From	RFC3261	m	m		
History-Info	RFC4244	o	–	(Note 3)	
Max-Forwards	RFC3261	m	m		
MIME-Version	RFC3261	o	o		
P-Access-Network-Info	RFC3455	o	o		(Note 1)
P-Asserted-Identity	RFC3325	o	–	c3	
P-Charging-Function-Addresses	RFC3455	o	o	c4 (when Appendix Table iv-16, No. 1 is stated "Use".)	(Note 1)
			–	c4 (when Appendix Table iv-16, No. 1 is stated "Not use".)	
P-Charging-Vector	RFC3455	o	o	c4 (when Appendix Table iv-16, No. 1 is stated "Use".)	
			–	c4 (when Appendix Table iv-16, No. 1 is stated "Not use".)	
P-Preferred-Identity	RFC3325	o	–	c5	
Privacy	RFC3323	o	–	c3	
Proxy-Authorization	RFC3261	o	–	c2	
Proxy-Require	RFC3261	o	o		
Reason	RFC3326	o	o		(Note 1)
Record-Route	RFC3261	o	o		(Note 1)
Referred-By	RFC3892		o	c6 (Appendix Table iv-2, Items 4 and 5)	
Reject-Contact	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Request-Disposition	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Require	RFC3261	o	o		
Route	RFC3261	c	c		
Subscription-State	RFC3265	m	m		
Supported	RFC3261	o	o		
Timestamp	RFC3261	o	o		(Note 1)

To	RFC3261	m	m		
User-Agent	RFC3261	o	o		(Note 1)
Via	RFC3261	m	m		
Warning	RFC3261	o	o		(Note 1)
Message body			o	(Note 4)	

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available between networks, the header information is handled as valid information. (Appendix Table iv-9, Item 6) (RFC3840 and RFC3841)

c2: Authentication procedures are not supported between networks, according to 10.2.1.8.1.3 of Annex Table a-1 in Annex a.3.

c3: *P-Asserted-Identity* and *Privacy* headers are applicable only to the request and response outside existing dialogs, according to 10.2.2.2.2 and 10.2.2.2.4 of Annex Table a-1 in Annex a.3. (*NOTIFY* is used within a subscription (equivalent to a dialog). Therefore, the header is not applicable.)

c4: Use of headers for inter-carrier charging (*P-Charging-Vector*, *P-Charging-Function-Address*) (Appendix Table iv-16, Item 1)

c5: Use of *P-Preferred-Identity* header is not applicable, according to clause 10.2.2.2.3 in the main body.

c6: *Referred-By* header may be used as a result of using *REFER* (Appendix Table iv-2, Items 4 and 5). In the case that *REFER* is available between networks, the header information may be handled as valid information. It does not guarantee that the *Referred-By* header is used as a result of using *REFER*.

Note 1 When specified, whether expected behaviours are performed or the capabilities for the behaviours are provided is dependent on the policy of the connected carrier.

Note 2 *Call-Info* shows additional information about the sender of the messages. There is no description of the application of the header into *NOTIFY* in RFCs and other documents. Therefore, it is difficult to define its reaction when using the header in *NOTIFY*. Furthermore, security risks of *Call-Info* are noted in RFC3261. An ill-prepared use of the header should be avoided.

Note 3 It is not applicable due to the absence of a valid way to utilize the header in a message inside an existing dialog which does not record route information.

Note 4 It is used when notification information is present. Formatting and other features depend on *Content-Type*.

v.10.2. Supported headers in the NOTIFY response

Appendix Table v-17/JT-Q3401: Supported headers in the NOTIFY response

Message type: Response

Method: NOTIFY

Header	Appli-cation	Reference	RFC status	Status in this standard	Application conditions	Remarks
Accept	415	RFC3261	o	o		
Accept-Encoding	415	RFC3261	o	o		
Accept-Language	415	RFC3261	o	o		
Allow	2xx	RFC3261	o	o		
Allow	405	RFC3261	m	m		
Allow	r	RFC3261	o	o		
Allow-Events	2xx	RFC3265	o	o		
Allow-Events	489	RFC3265	m	m		
Authentication-Info	2xx	RFC3261	o	–	c1	
Call-ID		RFC3261	m	m		
Call-Info		RFC3261		–	(Note 2)	
Contact	1xx	RFC3261	o	o		
Contact	2xx	RFC3261	o	o		
Contact	3xx	RFC3261	m	m		
Contact	485	RFC3261	o	o		
Content-Disposition		RFC3261	o	o		
Content-Encoding		RFC3261	o	o		
Content-Language		RFC3261	o	o		
Content-Length		RFC3261	t	t		
Content-Type		RFC3261	*	*		
CSeq		RFC3261	m	m		
Date		RFC3261	o	o		(Note 1)
Error-Info	300-699	RFC3261	o	o		(Note 1)
From		RFC3261	m	m		
History-Info		RFC4244	o	–	(Note 3)	
MIME-Version		RFC3261	o	o		
P-Access-Network-Info		RFC3455	o	o		(Note 1)
P-Asserted-Identity		RFC3325	o	–	c2	
P-Charging-Function-Addresses		RFC3455	o	o	c3 (when Appendix Table iv-16, Item 1 is stated "Use".)	(Note 1)
				–	c3 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
P-Charging-Vector		RFC3455	o	o	c3 (when Appendix Table iv-16, Item 1 is stated "Use".)	
				–	c3 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
P-Preferred-Identity		RFC3325	o	–	c4	
Privacy		RFC3323	o	–	c2	
Proxy-Authenticate	401	RFC3261		–	c1	
Proxy-Authenticate	407	RFC3261	m	–	c1	
Reason		RFC3326	o	o		(Note 1)
Record-Route	2xx 401 484	RFC3261	o	o		(Note 1)
Require		RFC3261	o	o		
Retry-After	404 413 480 486	RFC3261	o	o		(Note 1)
Retry-After	500 503	RFC3261	o	o		(Note 1)
Retry-After	600 603	RFC3261	o	o		(Note 1)
RSeq	1xx	RFC3262	o	–	(Note 4)	

Server		RFC3261	o	o		(Note 1)
Supported	2xx	RFC3261	o	o		
Timestamp		RFC3261	o	o		(Note 1)
To		RFC3261	m	m		
Unsupported	420	RFC3261	o	o		
User-Agent		RFC3261	o	o		(Note 1)
Via		RFC3261	m	m		
Warning		RFC3261	o	o		(Note 1)
WWW-Authenticate	401	RFC3261	m	–	c1	
WWW-Authenticate	407	RFC3261		–	c1	
Message body				o	(Note 5)	

c1:	Authentication procedures are not supported between networks, according to 10.2.1.8.1.3 of Annex Table a-1 in Annex a.3.
c2:	*P-Asserted-Identity* and *Privacy* headers are applicable only to the request and response outside existing dialogs, according to 10.2.2.2.2 and 10.2.2.2.4 of Annex Table a-1 in Annex a.3. (*NOTIFY* is used within a subscription (equivalent to a dialog). Therefore, the header is not applicable.)
c3:	Use of headers for inter-carrier charging (*P-Charging-Vector*, *P-Charging-Function-Address*) (Appendix Table iv-16, Item 1)
c4:	Use of *P-Preferred-Identity* header is not applicable, according to clause 10.2.2.2.3 in the main body.
Note 1	When specified, whether expected behaviours are performed or the capabilities for the behaviours are provided is dependent on the policy of the connected carrier.
Note 2	*Call-Info* shows additional information about the sender of the messages. There is no description of the application of the header into *NOTIFY* in RFCs and other documents. Therefore, it is difficult to define its reaction when using the header in *NOTIFY*. Furthermore, security risks of *Call-Info* are noted in RFC3261. An ill-prepared use of the header should be avoided.
Note 3	It is not applicable due to the absence of a valid way to utilize the header in a message inside an existing dialog which does not record route information.
Note 4	The *100rel* option (*PRACK*) is not to be used in *NOTIFY*.
Note 5	It is used when notification information is present. Formatting and other features depend on *Content-Type*.

v.11. REFER

The message is used either inside or outside existing dialogs, and for requesting action to the recipient of the message, such as call origination specified in Refer-To.

v.11.1. Supported headers in the REFER request

Appendix Table v-18/JT-Q3401: Supported headers in the REFER request

Message type: Request

Method: REFER

Header	Reference	RFC status	Status in this standard	Application conditions	Remarks
Accept	RFC3261	o	o		
Accept-Contact	RFC3841	o	o	c1 (Appendix Table iv-9, Item 6)	
Accept-Encoding	RFC3261	o	o		
Accept-Language	RFC3261	o	o		
Allow	RFC3261	o	o		
Allow-Events	RFC3265		o	(Note 2)	
Authorization	RFC3261	o	–	c2	
Call-ID	RFC3261	m	m		
Contact	RFC3261	m	m		
Content-Disposition	RFC3261	o	o		
Content-Encoding	RFC3261	o	o		
Content-Language	RFC3261	o	o		
Content-Length	RFC3261	o	t	(Note 3)	
Content-Type	RFC3261	*	*		
CSeq	RFC3261	m	m		
Date	RFC3261	o	o		(Note 1)
Event	RFC3265		o	(Note 4)	(Note 1)
Expires	RFC3261	o	o		(Note 1)
From	RFC3261	m	m		
History-Info	RFC4244	o	o / –	c3 (when Appendix Table iv-9, Item 7 is stated "Used in each session as necessary ".)	
			–	c3 (when Appendix Table iv-9, Item 7 is stated "Not use".)	
Max-Forwards	RFC3261	m	m		
MIME-Version	RFC3261	o	o		
Organization	RFC3261	o	o		(Note 1)
P-Access-Network-Info	RFC3455	o	o		(Note 1)
P-Asserted-Identity	RFC3325	o	m / –	c4	
P-Called-Party-ID	RFC3455	o	o		(Note 1)
P-Charging-Function-Addresses	RFC3455	o	o	c5 (when Appendix Table iv-16, Item 1 is stated "Use".)	(Note 1)
			–	c5 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
P-Charging-Vector	RFC3455	o	o	c5 (when Appendix Table iv-16, Item 1 is stated "Use".)	
			–	c5 (when Appendix Table iv-16, Item 1 is stated "Not use".)	
P-Preferred-Identity	RFC3325	o	–	c6	
P-Visited-Network-ID	RFC3455	o	o		(Note 1)
Privacy	RFC3323		m / –	c7	
Proxy-Authorization	RFC3261	o	–	c2	
Proxy-Require	RFC3261	o	o		
RAck	RFC3262		–	(Note 5)	
Reason	RFC3326	– / o	– / o	(Note 6)	(Note 1)
Record-Route	RFC3261	o	o		
Refer-To	RFC3515	m	m		
Referred-By	RFC3892		o	c8 (Appendix Table iv-2, Items 4 and 5)	
Reject-Contact	RFC3841	o	o	c1	

Request-Disposition	RFC3841	o	o	c1	
Require	RFC3261	c	c		
Route	RFC3261	c	c		
Subscription-State	RFC3265		–	(Note 7)	
Supported	RFC3261	o	o		
Timestamp	RFC3261	o	o		(Note 1)
To	RFC3261	m	m		
User-Agent	RFC3261	o	o		(Note 1)
Via	RFC3261	m	m		
Message body			o	(Note 8)	

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available between networks, the header information is handled as valid information. (Appendix Table iv-9, Item 6) (RFC3840 and RFC3841)

c2: Authentication procedures are not supported between networks, according to 10.2.1.8.1.3 of Annex Table a-1 in Annex a.3.

c3: In the case that the request history retention function (*histinfo*) is available between networks, the header can be used (Appendix Table iv-9, Item 7). Note that it is applicable only to the request outside existing dialogs which necessitates the recording of route information, and not applicable to the request inside an existing dialog.

c4: *P-Asserted-Identity* header needs to be set for a request outside existing dialogs (not to be used inside an existing dialog) and transmits the calling-party's information, according to 10.2.2.2.2 of Annex Table a-1 in Annex a.3 and Annex c. (The setting is necessary for *REFER* outside existing dialogs, but not necessary for *REFER* inside an existing dialog.)

c5: Use of headers for inter-carrier charging (*P-Charging-Vector*, *P-Charging-Function-Address*) (Appendix Table iv-16, Item 1)

c6: Use of *P-Preferred-Identity* header is not applicable, according to clause 10.2.2.2.3 in the main body.

c7: *Privacy* header needs to be set for a request outside existing dialogs and transmits the presentation/restriction information of the calling-party, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3 and Annex c. (The setting is necessary for a message outside existing dialogs, but not necessary for a message inside an existing dialog. In the case that this header is not present in a message outside existing dialogs, the calling-party's information is handled to be possible to be notified.)

c8: *Referred-By* header may be used as a result of using *REFER* (Appendix Table iv-2, Items 4 and 5). In the case that *REFER* is available between networks, the header information may be handled as valid information. It does not guarantee that the *Referred-By* header is used as a result of using *REFER*.

Note 1 When specified, whether expected behaviours are performed or the capabilities for the behaviours are provided is dependent on the policy of the connected carrier.

Note 2 UA sending *REFER* is considered to support "*refer*" event option and there may be a possibility of related information being set. Therefore, although there are no RFC specifications, it is indicated as optional.

Note 3 Although specified as "o" in RFC3515, Content-Length is "t," which conforms to RFC3261.

Note 4 UA sending *REFER* is considered to be capable of requesting "refer" event establishment. Therefore, although there are no RFC specifications, it is indicated as optional.

Note 5 *RAck* is valid only for a *PRACK* request. There are no relevant RFC specifications, but it is indicated as not applicable (–).

Note 6 *Reason* header is specified in RFC3326, and it is applicable to all the requests inside an existing dialog, *CANCEL*, and all the responses, according to the specifications. Therefore, it can be used in *REFER* inside an existing dialog, but cannot be used in *REFER* outside existing dialogs.

Note 7 *Subscription-State* is valid when information is notified within a subscription. (That is, it is valid only for *NOTIFY*.) There are no relevant RFC specifications, but it is indicated as not applicable (-).

Note 8 It is used when notification information is present. Formatting and other features depend on *Content-Type*.

v.11.2. Supported headers in the REFER response

Appendix Table v-19/JT-Q3401: Supported headers in the REFER response

Message type: Response

Method: REFER

Header	Appli-cation	Reference	RFC status	Status in this standard	Application conditions	Remarks
Accept	415	RFC3261	c	c		
Accept-Encoding	415	RFC3261	c	c		
Accept-Language	415	RFC3261	c	c		
Allow	2xx	RFC3261	o	o		
Allow	405	RFC3261	m	m		
Allow	r	RFC3261	o	o		
Allow-Events		RFC3265		o	(Note 2)	
Authentication-Info	2xx	RFC3261	o	–	c1	
Call-ID		RFC3261	m	m		
Contact	2xx	RFC3261	m	m		
Contact	3xx-6xx	RFC3261	o	o		
Content-Disposition		RFC3261	o	o		
Content-Encoding		RFC3261	o	o		
Content-Language		RFC3261	o	o		
Content-Length		RFC3261	o	t	(Note 3)	
Content-Type		RFC3261	*	*		
CSeq		RFC3261	m	m		
Date		RFC3261	o	o		(Note 1)
Error-Info	300-699	RFC3261	o	o		(Note 1)
Expires		RFC3261	o	o		(Note 1)
From		RFC3261	m	m		
History-Info		RFC4244	o	o / –	c2 (when Appendix Table iv-9, Item 7 is stated "Used in each session as necessary ".)	
				–	c2 (when Appendix Table iv-9, Item 7 is stated "Not use".)	
MIME-Version		RFC3261	o	o		
Organization		RFC3261	o	o		(Note 1)
P-Access-Network-Info		RFC3455	o	o		(Note 1)
P-Asserted-Identity		RFC3325	o	o / –	c3	
P-Charging-Function-Addresses		RFC3455	o	o	c4 (when Appendix Table iv-16, No. 1 is stated "Use".)	(Note 1)
				–	c4 (when Appendix Table iv-16, No. 1 is stated "Not use".)	
P-Charging-Vector		RFC3455	o	o	c4 (when Appendix Table iv-16, No. 1 is stated "Use".)	
				–	c4 (when Appendix Table iv-16, No. 1 is stated "Not use".)	
P-Preferred-Identity		RFC3325	o	–	c5	
Privacy		RFC3323	o	o / –	c3	
Proxy-Authenticate	401	RFC3261	o	–	c1	
Proxy-Authenticate	407	RFC3261	m	–	c1	
Reason		RFC3326	o	o		(Note 1)
Record-Route	2xx 18x	RFC3261	o	o		
Require		RFC3261	c	c		
Retry-After	404 413 480 486	RFC3261	o	o		(Note 1)
Retry-After	500 503	RFC3261	o	o		(Note 1)

Retry-After	600 603	RFC3261	o	o		(Note 1)
RSeq	1xx	RFC3262		–	(Note 4)	
Server		RFC3261	o	o		(Note 1)
Supported	2xx	RFC3261	o	o		
Timestamp		RFC3261	o	o		(Note 1)
To		RFC3261	m	m		
Unsupported	420	RFC3261	o	o		
User-Agent		RFC3261	o	o		(Note 1)
Via		RFC3261	m	m		
Warning		RFC3261	o	o		(Note 1)
WWW-Authenticate	401	RFC3261	m	–	c1	
WWW-Authenticate	407	RFC3261	o	–	c1	
Message body				o	(Note 5)	

c1: Authentication procedures are not supported between networks, according to 10.2.1.8.1.3 of Annex Table a-1 in Annex a.3.

c2: In the case that the request history retention function (*histinfo*) is available between networks, the header can be used (Appendix Table iv-9, Item 7). Note that it is applicable only to the response to a request outside existing dialogs which necessitates the recording of route information, and not applicable to the response to a request inside an existing dialog.

c3: *P-Asserted-Identity* and *Privacy* headers are applicable only to the request and response outside existing dialogs, according to 10.2.2.2.2 and 10.2.2.2.4 of Annex Table a-1 in Annex a.3. (The header is applicable only to the response to initial *SUBSCRIBE*.)

c4: Use of headers for inter-carrier charging (*P-Charging-Vector*, *P-Charging-Function-Address*) (Appendix Table iv-16, Item 1)

c5: Use of *P-Preferred-Identity* header is not applicable, according to clause 10.2.2.2.3 in the main body.

Note 1 When specified, whether expected behaviours are performed or the capabilities for the behaviours are provided is dependent on the policy of the connected carrier.

Note 2 UA receiving *REFER* is considered to support "*refer*" event options and there may be a possibility of the information being set. Therefore, although there are no RFC specifications, it is indicated as optional.

Note 3 Although specified as "o" in RFC3515, Content-Length is "t," which conforms to RFC3261.

Note 4 The *100rel* option (*PRACK*) is not to be used in *REFER*.

Note 5 It is used when notification information is present. Formatting and other features depend on *Content-Type*.

Appendix vi. Message examples

(This appendix does not form an integral part of this standard.)

This appendix provides examples of call sequences corresponding to typical call origination and termination in SIP call establishment.

Note that the sequence examples listed here are intended to be a help for system implementation, and behaviors different from sequences listed in this appendix may be needed due to actual service contents and/or terminal functions of each carrier. Note also that the content of these sequence examples do not guarantee call connectivity or quality.

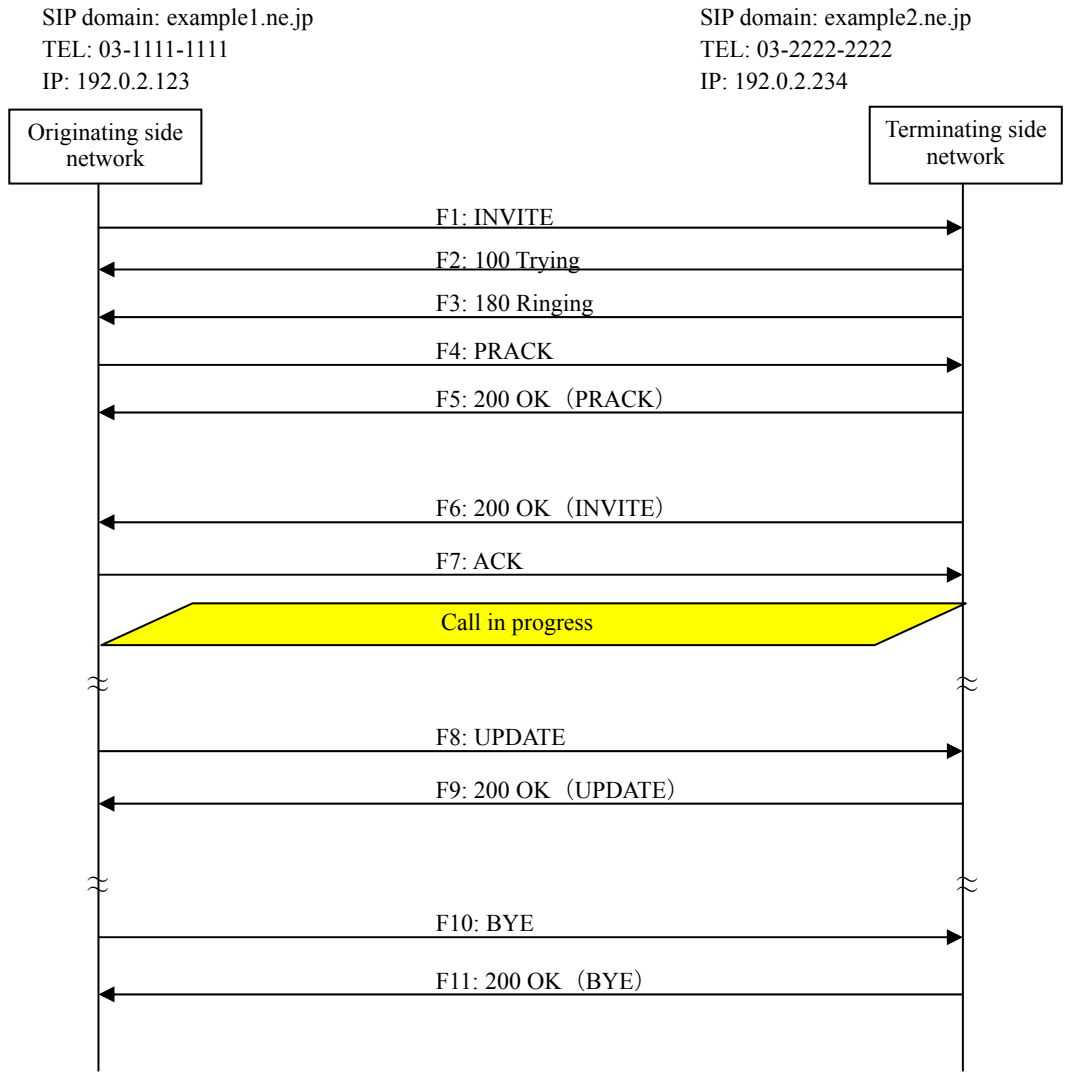
Appendix Table vi-1/JT-Q3401: List of sequence examples

No.	Sequence Name	Corresponding clauses and figures
1	Call origination and disconnection from the originating side (IPv4, Use of *timer*, *100rel* and cpc, G.711 μ-law)	Appendix vi.1.1
2	Call origination and disconnection from the terminating side (IPv4, Use of *timer*, *100rel* and cpc, G.711 μ-law)	Appendix vi.1.2
3	Call cancellation	Appendix vi.1.3
4	Unallocated number	Appendix vi.1.4

vi.1. Sequence examples

vi.1.1. Call origination and disconnection from the originating side (IPv4, Use of timer, 100rel and cpc, G.711 μ-law)

This clause shows an example message flow of a call connection sequence in the case that *timer* and *100rel* are enabled on both originating and terminating sides and calling-party's category (cpc) is specified. IPv4 is used for call control signals and media, TCP is used for call control, and for G.711 μ-law is used as audio media.



Appendix Figure vi-1/JT-Q3401: Call origination and disconnection from the originating side (IPv4, Use of timer, 100rel and cpc, G.711

F1: INVITE

```
INVITE sip:+81322222222@example2.ne.jp;user=phone SIP/2.0
Via: SIP/2.0/TCP 192.0.2.123:5060;branch=z9hG4bK12345678abcdefgh
Max-Forwards: 70
To: <sip:+81322222222@example2.ne.jp;user=phone>
From: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
Call-ID: qwertyuiop123456@192.0.2.123
```

```
CSeq: 1 INVITE
Contact: <sip:192.0.2.123:5060;transport=tcp>
Privacy: none
P-Asserted-Identity: "0311111111" <tel:+81311111111;cpc=ordinary>
P-Asserted-Identity: <sip:+81311111111@example1.ne.jp;user=phone;cpc=ordinary>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: 100rel,timer
Session-Expires: 300;refresher=uac
Min-SE: 300
Content-Type: application/sdp
Content-Length: 207

v=0
o=- 82664419472 82664419472 IN IP4 192.0.2.111
s=-
c=IN IP4 192.0.2.111
t=0 0
m=audio 10000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F2: 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/TCP 192.0.2.123:5060;branch=z9hG4bK12345678abcdefgh
To: <sip:+81322222222@example2.ne.jp;user=phone>
From: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
Call-ID: qwertyuiop123456@192.0.2.123
CSeq: 1 INVITE
Content-Length: 0
```

F3: 180 Ringing

```
SIP/2.0 180 Ringing
Via: SIP/2.0/TCP 192.0.2.123:5060;branch=z9hG4bK12345678abcdefgh
To: <sip:+81322222222@example2.ne.jp;user=phone>;tag=9876zyxw
From: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
Call-ID: qwertyuiop123456@192.0.2.123
CSeq: 1 INVITE
Contact: <sip:192.0.2.234:5060;transport=tcp>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: 100rel
RSeq: 1
Content-Length: 0
```

F4: PRACK

```
PRACK sip:192.0.2.234:5060 SIP/2.0
Via: SIP/2.0/TCP 192.0.2.123:5060;branch=z9hG4bK23456789bcdefghi
Max-Forwards: 70
To: <sip:+81322222222@example2.ne.jp;user=phone>;tag=9876zyxw
From: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
Call-ID: qwertyuiop123456@192.0.2.123
CSeq: 2 PRACK
RAck: 1 1 PRACK
Content-Length: 0
```

F5: 200 OK（PRACK）

```
SIP/2.0 200 OK
Via: SIP/2.0/TCP 192.0.2.123:5060;branch=z9hG4bK23456789bcdefghi
To: <sip:+81322222222@example2.ne.jp;user=phone>;tag=9876zyxw
From: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
Call-ID: qwertyuiop123456@192.0.2.123
CSeq; 2 PRACK
Content-Length: 0
```

F6: 200 OK（INVITE）

```
SIP/2.0 200 OK
Via: SIP/2.0/TCP 192.0.2.123:5060;branch=z9hG4bK12345678abcdefgh
To: <sip:+81322222222@example2.ne.jp;user=phone>;tag=9876zyxw
From: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
Call-ID: qwertyuiop123456@192.0.2.123
CSeq: 1 INVITE
Contact: <sip:192.0.2.234:5060;transport=tcp>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uac
Content-Type: application/sdp
Content-Length: 207

v=0
o=- 82917391739 82917391739 IN IP4 192.0.2.222
s=-
c=IN IP4 192.0.2.222
t=0 0
m=audio 20000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F7: ACK

```
ACK sip:192.0.2.234:5060 SIP/2.0
Via: SIP/2.0/TCP 192.0.2.123:5060;branch=z9hG4bK34567890cdefghij
Max-Forwards: 70
To: <sip:+81322222222@example2.ne.jp;user=phone>;tag=9876zyxw
From: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
Call-ID: qwertyuiop123456@192.0.2.123
CSeq: 1 ACK
Content-Length: 0
```

F8: UPDATE

```
UPDATE sip:192.0.2.234:5060 SIP/2.0
Via: SIP/2.0/TCP 192.0.2.123:5060;branch=z9hG4bK45678901defghijk
Max-Forwards: 70
To: <sip:+81322222222@example2.ne.jp;user=phone>;tag=9876zyxw
From: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
Call-ID: qwertyuiop123456@192.0.2.123
CSeq: 3 UPDATE
Contact: <sip:192.0.2.123:5060;transport=tcp>
Supported: timer
Session-Expires: 300;refresher=uac
```

```
Min-SE: 300
Content-Length: 0
```

F9: 200 OK（UPDATE）

```
SIP/2.0 200 OK
Via: SIP/2.0/TCP 192.0.2.123:5060;branch=z9hG4bK45678901defghijk
To: <sip:+81322222222@example2.ne.jp;user=phone>;tag=9876zyxw
From: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
Call-ID: qwertyuiop123456@192.0.2.123
CSeq: 3 UPDATE
Contact: <sip:192.0.2.234:5060;transport=tcp>
Require: timer
Session-Expires: 300;refresher=uac
Content-Length: 0
```

F10: BYE

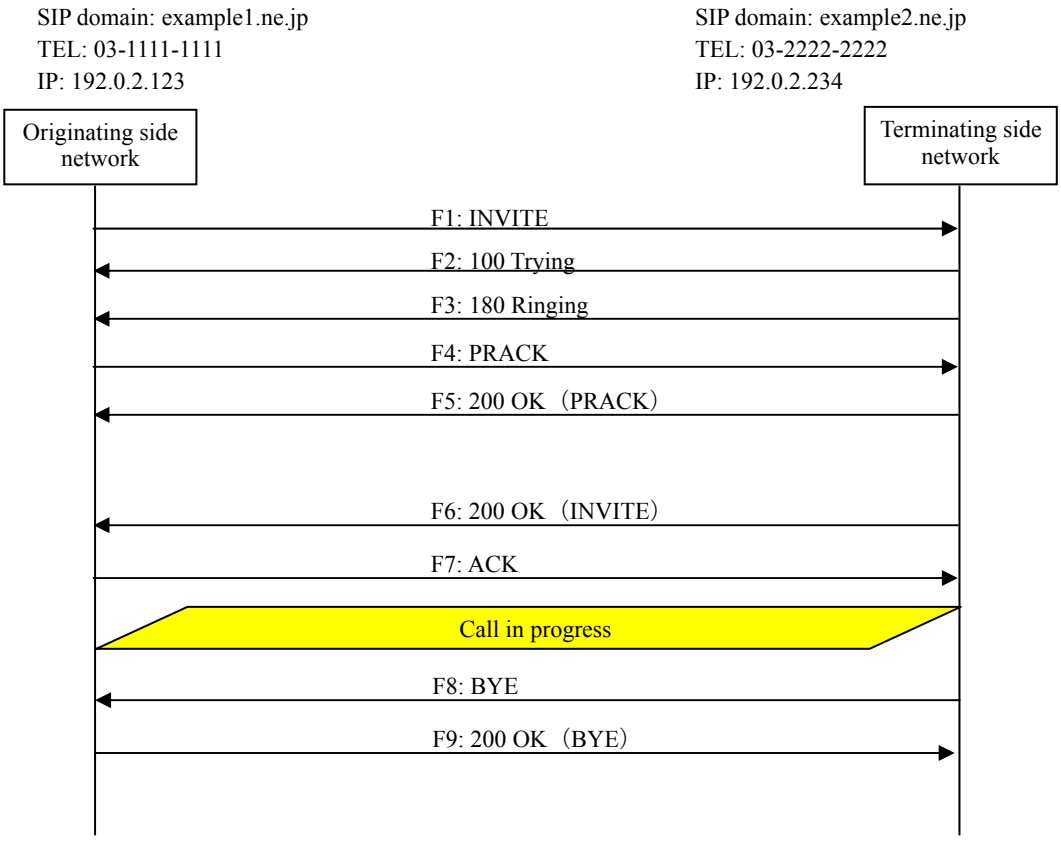
```
BYE sip:192.0.2.234:5060 SIP/2.0
Via: SIP/2.0/TCP 192.0.2.123:5060;branch=z9hG4bK56789012efghijkl
Max-Forwards: 70
To: <sip:+81322222222@example2.ne.jp;user=phone>;tag=9876zyxw
From: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
Call-ID: qwertyuiop123456@192.0.2.123
CSeq: 4 BYE
Content-Length: 0
```

F11: 200 OK（BYE）

```
SIP/2.0 200 OK
Via: SIP/2.0/TCP 192.0.2.123:5060;branch=z9hG4bK56789012efghijkl
To: <sip:+81322222222@example2.ne.jp;user=phone>;tag=9876zyxw
From: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
Call-ID: qwertyuiop123456@192.0.2.123
CSeq: 4 BYE
Content-Length: 0
```

vi.1.2. Call origination and disconnection from the terminating side (IPv4, Use of timer, 100rel and cpc, G.711 μ–law)

This clause shows an example message flow in the case that the call is disconnected by the terminating side under the same condition of option item selection as clause v.1.1.



Appendix Figure vi-2/JT-Q3401: Call origination and disconnection from the terminating side (IPv4, Use of timer, 100rel and cpc, G.711 μ–law)

F1 to F7 are omitted because they are the same as those of clause vi.1.1.

F8: BYE

```
BYE sip:192.0.2.123:5060 SIP/2.0
Via: SIP/2.0/TCP 192.0.2.234:5060;branch=z9hG4bK98765432stuvwxyz
Max-Forwards: 70
To: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
From: <sip:+81322222222@example2.ne.jp;user=phone>;tag=9876zyxw
Call-ID: qwertyuiop123456@192.0.2.123
CSeq: 100 BYE
Content-Length: 0
```

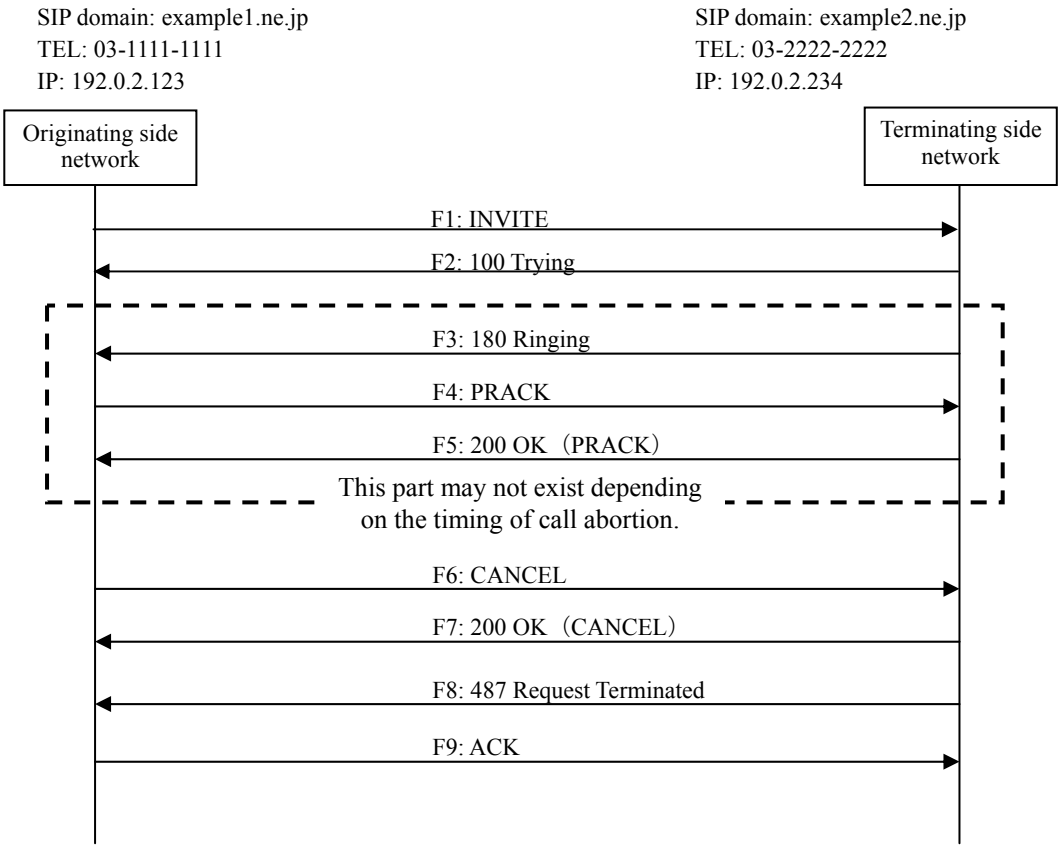
F9: 200 OK（BYE）

```
SIP/2.0 200 OK
Via: SIP/2.0/TCP 192.0.2.123:5060;branch=z9hG4bK98765432stuvwxyz
```

```
To: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
From: <sip:+81322222222@example2.ne.jp;user=phone>;tag=9876zyxw
Call-ID: qwertyuiop123456@192.0.2.123
CSeq: 100 BYE
Content-Length: 0
```

vi.1.3. Call cancellation (disconnection while ringing)

Below is an example message flow for call cancellation by the originating side under the same condition of option item selection as clause v.1.1



Appendix Figure vi-3/JT-Q3401: Call cancellation (disconnection while ringing)

F1 to F5 are omitted because they are the same as those of clause vi.1.1.

F6: CANCEL

```
CANCEL sip:+81322222222@example2.ne.jp;user=phone SIP/2.0
Via: SIP/2.0/TCP 192.0.2.123:5060;branch=z9hG4bK12345678abcdefgh
Max-Forwards: 70
To: <sip:+81322222222@example2.ne.jp;user=phone>
From: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
Call-ID: qwertyuiop123456@192.0.2.123
CSeq: 1 CANCEL
Content-Length: 0
```

F7: 200 OK（CANCEL）

```
SIP/2.0 200 OK
Via: SIP/2.0/TCP 192.0.2.123:5060;branch=z9hG4bK12345678abcdefgh
To: <sip:+81322222222@example2.ne.jp;user=phone>;tag=5555eeee
From: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
Call-ID: qwertyuiop123456@192.0.2.123
```

```
CSeq: 1 CANCEL
Content-Length: 0
```

F8: 487 Request Terminated

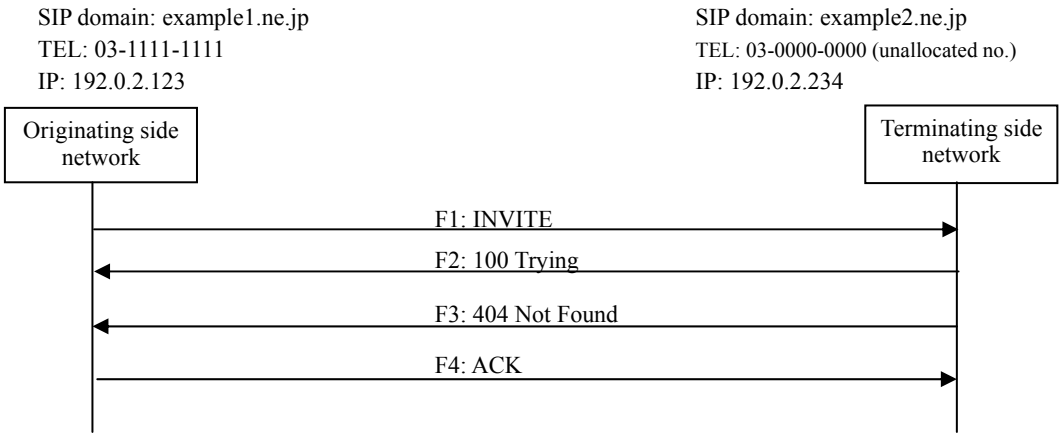
```
SIP/2.0 200 OK
Via: SIP/2.0/TCP 192.0.2.123:5060;branch=z9hG4bK12345678abcdefgh
To: <sip:+81322222222@example2.ne.jp;user=phone>;tag=5555eeee
From: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
Call-ID: qwertyuiop123456@192.0.2.123
CSeq: 1 INVITE
Content-Length: 0
```

F9: ACK

```
ACK sip:192.0.2.234:5060 SIP/2.0
Via: SIP/2.0/TCP 192.0.2.123:5060;branch=z9hG4bK12345678abcdefgh
Max-Forwards: 70
To: <sip:+81322222222@example2.ne.jp;user=phone>;tag=5555eeee
From: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
Call-ID: qwertyuiop123456@192.0.2.123
CSeq: 1 ACK
Content-Length: 0
```

vi.1.4. Unallocated number

Below is an example message flow when reaching an unallocated number on the terminating side under the same condition of option item selection as clause v.1.1.



Appendix Figure vi-4/JT-Q3401: Unallocated number

F1: INVITE

```
INVITE sip:+81300000000@example2.ne.jp SIP/2.0
Via: SIP/2.0/TCP 192.0.2.123:5060;branch=z9hG4bK12345678abcdefgh
Max-Forwards: 70
To: <sip:+81300000000@example2.ne.jp;user=phone>
From: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
Call-ID: qwertyuiop123456@192.0.2.123
CSeq: 1 INVITE
Contact: <sip:192.0.2.123:5060;transport=tcp>
Privacy: none
P-Asserted-Identity: "0311111111" <tel:+81311111111;cpc=ordinary>
P-Asserted-Identity: <sip:+81311111111@example1.ne.jp;user=phone;cpc=ordinary>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: 100rel,timer
Session-Expires: 300;refresher=uac
Min-SE: 300
Content-Type: application/sdp
Content-Length: 207

v=0
o=- 82664419472 82664419472 IN IP4 192.0.2.111
s=-
c=IN IP4 192.0.2.111
t=0 0
m=audio 10000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F2: 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/TCP 192.0.2.123:5060;branch=z9hG4bK12345678abcdefgh
To: <sip:+81300000000@example2.ne.jp;user=phone>
From: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
Call-ID: qwertyuiop123456@192.0.2.123
```

```
CSeq: 1 INVITE
Content-Length: 0
```

F3: 404 Not Found

```
SIP/2.0 404 Not Found
Via: SIP/2.0/TCP 192.0.2.123:5060;branch=z9hG4bK12345678abcdefgh
To: <sip:+81300000000@example2.ne.jp;user=phone>;tag=7777gggg
From: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
Call-ID: qwertyuiop123456@192.0.2.123
CSeq: 1 INVITE
Reason: Q.850 ;cause=1
Content-Length: 0
```

F4: ACK

```
ACK sip:192.0.2.234:5060 SIP/2.0
Via: SIP/2.0/TCP 192.0.2.123:5060;branch=z9hG4bK12345678abcdefgh
To: <sip:+81300000000@example2.ne.jp;user=phone>;tag=7777gggg
From: <sip:+81311111111@example1.ne.jp;user=phone>;tag=1234abcd
Call-ID: qwertyuiop123456@192.0.2.123
CSeq: 1 ACK
Content-Length: 0
```