TTC STANDARD

JJ-90.25

Technical Specifications on Inter-Carrier Interface between Managed Provider's SIP Networks

（English Edition）

Version 1.1

Aug. 25, 2005

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

Introduction

This document provides the TTC original Standard formulated by the TTC Signaling working group.

The working group translated JJ-90.25 Japanese Version 1.1 (August 25,2005) into English, and issued JJ-90.25 English Version on August 25, 2005.

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

August 25, 2005
TTC Signaling Working Group

CONTENTS

<Reference >

1. Relationship to international recommendations, etc.

There are no international recommendations relating to this standard.

2. Revision history

Revision	Date	Details of revision
Version 1.0	June 2nd 2005	Initial publication (Revised version 1 of TS-1007 (with the addition of section 5.5 Guidance/talkie services, and Annex b and c))
Version 1.1	August 25, 2005	Reference document is modified because “session timer” has been approved to be assigned an official RFC number in IETF

3. References

3.1. Normative References

[1] “SIP: Session Initiation Protocol”, TTC standard JF-IETF-RFC3261, version 1, The Telecommunication Technologies Committee), June 2005.

[2] “Reliability of Provisional Responses in the Session Initiation Protocol (SIP)”, TTC standard JF-IETF-RFC3262, version 1, The Telecommunication Technologies Committee, June 2005.

[3] “An Offer/Answer Model with the Session Description Protocol (SDP)”, TTC standard JF-IETF-RFC3264, version 1, The Telecommunication Technologies Committee, June 2005..

[4] “SDP: Session Description Protocol”, TTC standard JF-IETF-RFC2327, first edition, The Telecommunication Technologies Committee, June 2005.

[5] “A Privacy Mechanism for the Session Initiation Protocol (SIP)”, TTC standard JF-IETF-RFC3323, first edition, The Telecommunication Technologies Committee, June 2005.

[6] “Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks”, TTC standard JF-IETF-RFC3325, The Telecommunication Technologies Committee, June 2005.

[7] “The tel URI for Telephone Numbers)”, TTC standard JF-IETF-RFC3966, first edition, The Telecommunication Technologies Committee, June 2005.

[8] “The International Public Telecommunications Numbering Plan”, ITU-T Recommendation E.164, ITU-T, 1997.

[9] “Technical Specification on SIP to ISUP Interworking”, TTC standard JF-IETF-RFC3398, TTC, June 2005.

[10] “Technical Specification of the Framework on Provider’s SIP Networks”, TTC standard JJ-90.21, The Telecommunication Technologies Committee, June 2005.

[11] “Technical Specification on Network Asserted User Identity Information Transferring through Provider’s SIP Networks”, TTC standard JJ-90.22, The Telecommunication Technologies Committee), June 2005

[12] “Inter-Carrier Interface based on ISUP”, TTC standard JJ-90.10, 6th edition, The Telecommunication Technologies Committee, April 2003.

[13] “The Session Initiation Protocol UPDATE Method”, JF-IETF-RFC3311, The Telecommunication Technologies Committee, June 2005.

[14] “The Reason Header Field for the Session Initiation Protocol (SIP)”, TTC standard JF-IETF-RFC3326, The

Telecommunication Technologies Committee, June 2005.

[15] Session Timers in the Session Initiation Protcol(SIP) , JF-IETF-RFC4028, The Telecommunication Technologies Committee), 2005 mm/dd

3.2. Informative References

[16] Donovan, S. and J. Rosenberg, “Session Timers in the Session Initiation Protocol (SIP)”, draft-ietf-sip-session-timer-15 (work in progress), July 2004.

Informative reference [16] will be changed to a normative reference on becoming a Request for Comments (RFC).

4. Industrial property rights

Information regarding submittal of TTC’s “The Policy for the Handling of Industrial Property Rights” is available on TTC’s home page.

5. Contact

Signaling Working Group

1. Overview

1.1. Scope of this standard

This standard provides connection interface specifications that are necessary when using an E.164 number to specify and place a voice call to a destination by applying a connection interface (interface A) between interconnected providers' SIP networks in a network connection architecture conforming to JJ-90.21[10].

This standard is also intended to simplify network management while maintaining a high level of interconnectivity based on the premise that interconnected providers' SIP networks conform to this standard.

1.2. Purpose and provisions of this standard

This standard relates to the connection interface applied to interface A, and aims to achieve the following aims in relation to interconnections, including items relating to SIP and SDP:

- Produce a practical standard by ensuring that provisions relating to connection criteria are uniquely interpreted.
- Produce a standard that can be applied in common by both connecting parties when interconnections are made to another provider's SIP network.
- Produce a standard that includes connection criteria consisting of items necessary for achieving smooth interconnections at connection interfaces, in addition to signal criteria.

To achieve these aims, this standard prescribes the following items:

- Items relating to the use of SIP according to JF-IETF-RFC3261 [1] and extensions thereof as call control signal criteria.
- Items relating to SDP and media capability criteria based on G.711 μ-law audio as media-related criteria.
- Items relating to other behaviors associated with call establishment.

Items associated with operational criteria and the like related to interconnections are provided in the appendix of this standard by way of reference.

1.3. Content of this standard

Main body

The main body of this standard describes interfaces relating to interconnections between providers' SIP networks, and is mainly concerned with the following items:

- Prescribing a connection model for when interconnections are made (section 2)

- Prescribing a numbering system (section 3) and a signaling system (section 4) for SIP signals transmitted and received between providers' SIP networks.
- Prescribing the functional extensions and SDP formats needed to achieve interconnections (section 5).

Annex

Annex A relates to the control of session reservation during period of congestion when the upper limit on the number of simultaneous calls between providers' SIP networks is controlled, annex B relates to the necessary criteria for an RTP sent out by a network before call completion to be connected to the caller, and annex C relates to the criteria for connecting to a unallocated (unassigned) number talkie.

Appendices

By way of reference, the appendices describe connection test methods (Appendix i), connection sequences (Appendix ii) and call information (Appendix iii) to be implemented between providers.

1.4. Terminology

The terminology used in this standard conforms to JJ-90.21 [10] and TR-1007 [1]

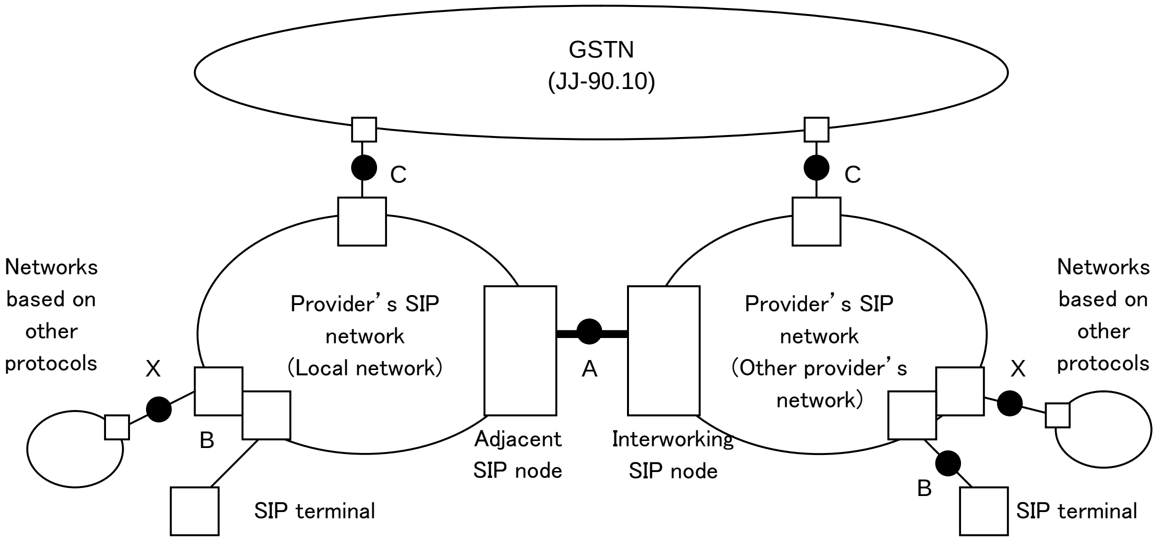
2. Connection modes

2.1. Basic connection modes

This standard shows the criteria to be fulfilled by interfaces connecting to managed providers' SIP networks that can be applied to the interface A specification of the provider's SIP network interconnection model according to JJ-90.21 [10] which is shown in Fig. 2-1.

In this standard, a provider's SIP network that has an interface capable of observing these interface provisions is referred to as a "managed provider's SIP network". In the following, where reference is made to a provider's SIP network, this should be assumed to mean a "managed provider's SIP network".

When a call is connected through an interface that conforms to this interface specification, it must be kept in mind that this standard does not show all the conditions that must be met by this connection. This standard assumes familiarity with the contents of JJ-90.21 [10] "Technical Specification of the Framework on Provider's SIP Networks" and JJ-90.22 [11] "Technical Specification on Network Asserted User Identity Information Transferring through Provider's SIP Networks".


GSTN
(JJ-90.10)
C
C
Networks based on other protocols
X
Provider' s SIP network (Local network)
A
Provider' s SIP network (Other provider' s network)
X
Networks based on other protocols
B
Adjacent SIP node
Interworking SIP node
B
SIP terminal
SIP terminal

* X represents an interface that might be subject to additional regulations in the future

Fig. 2-1/JJ-90.25: Provider's SIP network interconnection model

2.2. Scope of this standard

The connection patterns are shown in Table 2-1.

Table 2-1/JJ-90.25: Connection patterns

Message receiving side Message transmitting side	Provider’s network where this standard is supported	Provider’s network where this standard is not supported
Provider’s network where this standard is supported	○	–
Provider’s network where this standard is not supported	–	–

○: Connection pattern covered by this standard

－Connection pattern not covered by this standard

3. Numbering system

3.1. Basic callee number configuration

The callee number is set in the Request-URI of the Initial INVITE request as information used to route the call between the providers' SIP networks.

The Request-URI of the Initial INVITE request is assumed to be a SIP-URI, which is defined as follows:

3.1.1. user part

The callee number is set in the user part of the SIP-URI, which is set in the Request-URI of the Initial INVITE request. The basic format is the global-phone-number format of the tel URL defined by JF-IETF-RFC3966 [7], and uses no visual-separator. The format corresponding to a callee number as defined by JJ-90.10 [12] is shown in Table 3-1.

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

Table 3-1/JJ-90.25: Callee 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; C must not be 0	Mobile/PHS/wireless pager calls
+8150CDEFGHJK	C must not be 0	IP phone calls (category B)

Number formats other than those shown in Table 3-1 (e.g., national numbers without the "+81" prefix shown in Table 3-1) may be used by agreement between the connected providers.

3.1.2. hostport part

The hostport part of the SIP-URI set in the Request-URI of an Initial INVITE request is set to the name of the host or domain defined by the provider's SIP network to which the connection is made (including the IP address format). The specific information that is set is decided upon between the connecting providers.

3.1.3. Option URI parameter part

The option URI parameter of the SIP-URI set in the Request-URI of the Initial INVITE request is ignored during processing.

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

The calling provider's network should be able to register the valid number of received digits in the userinfo part of a valid Request-URI (which should be in the range between the minimum number of received digits and the maximum number of received digits), and if the minimum number of digits is not met, then a disconnection process should be performed inside the calling provider's network. When the maximum number of digits is exceeded, the behaviors related to the connection are not guaranteed. However, the minimum and maximum numbers of received digits should be determined based on discussions between providers.

4. Signal scheme

4.1. Signal scheme between connected providers' networks

Session Initiation Protocol (SIP) v2.0 (JF-IETF-RFC3261 [1]) based on an Internet Protocol (IP) Version 4 (IPv4) network is used as the signal scheme between connected providers' networks.

Attributes of the connection lines over which SIP signals propagate, such as their speed and bandwidth and the details of the physical layer and data link layer, are outside the scope of this standard. When an interconnection is made, these should be determined by agreement between the providers concerned.

4.1.1. Other connection requirements

The schemes used on connection lines for the transmission of media streams are outside the scope of this standard. When an interconnection is made, these should be determined by agreement between the providers concerned.

4.2. Network layer interface

The network layer interface associated with the transmission and reception of SIP signals conforms to Internet Protocol (IP) Version 4 (IPv4).

4.3. Transport layer interface

The transport layer interface associated with the transmission and reception of SIP signals conforms to the User Datagram Protocol (UDP).

It is RECOMMENDED that port 5060 is used to receive SIP signals, except when a port number is explicitly mentioned in the signal from the destination of a connection, e.g., in a Via header or Record-Route header.

When different port numbers are used, this should be agreed upon between the connecting providers after considering the status of equipment and the like.

4.4. Call processing signal specifications

Parts that are not mentioned in this standard should conform to the reference.

If any parts are restated differently by this standard, then the provisions of this standard should be applied.

4.5. Requirements relating to media streams

These are specified in section 5.3.

4.6. SIP messages

This section clarifies the data elements (messages, headers, and header parameters) of SIP messages exchanged in interconnections between providers' SIP networks.

4.6.1. Maximum message setting lengths

The maximum allowed lengths of SIP message elements are shown in Table 4-1.

Table 4-1/JJ-90.25: Maximum message setting lengths

Element	Maximum length
Maximum length of one line	255 bytes
Maximum repetitions of the same header	5 lines (see note 1)
Maximum length of message body	1000 bytes
Overall message length	1300 bytes or less (see note 2)
Note 1: The number of `Record-Route` elements is assumed to be 5 entries for a request, and 10 entries for a response. The `Route` and `Via` entries are assumed to be 5 entries. Note 2: Conforms to JJ-90.21 [10].	

4.7. Definitions in tables

Table 4-2 shows the definitions of prescribed types that are used in common in each table.

Table 4-2/JJ-90.25: Definitions of prescribed types in the tables

Code	Code name	Transmitting side	Receiving side
m	Mandatory	The capability conforming to the referenced provisions **must** be provided.	The capability conforming to the referenced provisions **must** be provided. Processing should not continue if required information is unavailable. (Suitable disconnection/release processing should be performed.) However, when a default value has been decided upon, processing is performed using the default value.
o	Optional	The capability may be available at the transmitting side, but the intended capability is not guaranteed.	If possible, perform the processing expected by the transmitting side. When the processing expected by the transmitting side cannot be performed, the received content should be ignored and processing should continue.
x	Prohibited (excluded)	The capability **must not** be provided.	Respond with an error, or ignore.
c <integer>	Conditional	Provision of the capability depends on condition <integer>. The capability **must not** be provided if this condition is not met.	Processing may be required depending on condition <integer>. Processing is not continued when the condition is not met.
o <integer>	Qualified optional	May be exclusively selected from options with the same condition <integer>.	Processing is performed according to the condition <integer>.

4.8. Request message classes

Table 4-3 lists the request messages exchanged between providers.

Table 4-3/JJ-90.25: List of supported request messages

Request signal	Reference	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
ACK	[1]	m	m	4.10.1
BYE	[1]	m	m	4.10.2
CANCEL	[1]	m	m	4.10.3
Initial INVITE	[1]	m	m	4.10.4
re-INVITE	[1]	m	m	4.10.5
REGISTER	[1]	x	x	
PRACK	[2]	c1	c1	4.10.6
UPDATE	[13]	c2	c2	4.10.7
Other requests		c3	c3	
c1: Set to “m” when 100rel is set in the Supported header, or to “x” otherwise. Providers will have to discuss among themselves if the use of 100rel is to be guaranteed. c2: Set to “m” when UPDATE is used to update a session, or to “x” otherwise. Providers will have to discuss among themselves if the use of UPDATE is to be guaranteed. c3: Set to “m” if used, or to “x” otherwise. Basically it cannot be used, but if it is then it must be arranged by discussion between providers, including negotiation based on Allow or Supported headers. When no negotiation is performed, a provider that receives such a request MAY respond to the provider that issued it with a 405 (Method Not Allowed) or 501 (Not Implemented) error response message.				

4.9. Response messages

The SIP response signals covered by these provisions with regard to each of the SIP requests shown in Table 4-3 are listed below.

SIP responses to other requests should be determined based on discussions between providers. Also, where an “o” appears in the receiving side column of this table, it means that the default values of each class (183 for 1xx, or x00 for x≠1) should at least be processed.

Table 4-4/JJ-90.25: List of SIP responses to INVITE requests

SIP response signal			Reference	Class (transmitting side)	Class (receiving side)	Notes
Class	Code	Phrase				
1xx	100	Trying	[1]	m	m	(Note 1)
	180	Ringing	[1]	m	m	(Note 2)
	181	Call Is Being Forwarded	[1]	o	o	
	182	Queued	[1]	o	o	
	183	Session Progress	[1]	m	m	(Note 3)
	Other			o	o	
2xx	200	OK	[1]	m	m	(Note 4)

SIP response signal			Reference	Class (transmitting side)	Class (receiving side)	Notes
Class	Code	Phrase				
	Other		[1]	o	o	
3xx	300	Multiple Choices	[1]	c2	o	
	301	Moved Permanently	[1]	c2	o	
	302	Moved Temporarily	[1]	c2	o	
	305	Use Proxy	[1]	c2	o	
	380	Alternative Service	[1]	c2	o	
	Other		[1]	o	o	
4xx	400	Bad Request	[1]	o	o	
	401	Unauthorized	[1]	x	x	
	402	Payment Required	[1]	o	o	
	403	Forbidden	[1]	o	o	
	404	Not Found	[1]	m	m	(Note 5)
	405	Method Not Allowed	[1]	x	x	
	406	Not Acceptable	[1]	o	o	
	407	Proxy Authentication Required	[1]	x	x	
	408	Request Timeout	[1]	o	m	(Note 6)
	410	Gone	[1]	o	o	
	413	Request Entity Too Large	[1]	o	o	
	414	Request-URI Too Long	[1]	o	o	
	415	Unsupported Media Type	[1]	o	o	
	416	Unsupported URI Scheme	[1]	o	o	
	420	Bad Extension	[1]	o	o	
	421	Extension Required	[1]	x	x	
	422	Session Interval Too Small	[15]	c1	c1	
	423	Interval Too Brief	[1]	x	x	
	480	Temporarily Unavailable	[1]	o	o	
	481	Call/Transaction Does Not Exist	[1]	o	m	(Note 6)
	482	Loop Detected	[1]	o	o	
	483	Too Many Hops	[1]	o	o	
	484	Address Incomplete	[1]	o	o	
	485	Ambiguous	[1]	o	o	
	486	Busy Here	[1]	o	m	(Note 7)
	487	Request Terminated	[1]	o	m	(Note 8)
	488	Not Acceptable Here	[1]	o	o	
	491	Request Pending	[1]	o	o	

SIP response signal			Reference	Class (transmitting side)	Class (receiving side)	Notes
Class	Code	Phrase				
	493	Undecipherable	[1]	o	o	
	Other		[1]	o	o	
5xx	500	Server Internal Error	[1]	o	o	
	501	Not Implemented	[1]	o	o	
	502	Bad Gateway	[1]	o	o	
	503	Service Unavailable	[1]	o	o	
	504	Server Time-out	[1]	o	o	
	505	Version Not Supported	[1]	o	o	
	513	Message Too Large	[1]	o	o	
	Other		[1]	o	o	
6xx	600	Busy Everywhere	[1]	o	o	
	603	Decline	[1]	o	o	
	604	Does Not Exist Anywhere	[1]	o	o	
	606	Not Acceptable	[1]	o	o	
	Other		[1]	o	o	

Note 1: MUST be sent when there is no response (including provisional responses) within 200 ms.

Note 2: Used when notifying the state of a call being made. A provider's SIP network that transmits a response MAY send additional SDP information only when the contents of the audio included in the RTP sent out to the provider that receives the response can be managed and guaranteed.

Note 3: Used when confirming early media by transmitting an SDP to the side that issued the INVITE request. A provider's SIP network that transmits a response MAY send additional SDP information only when the contents of the audio included in the RTP sent out to the provider that receives the response can be managed and guaranteed.

Note 4: Used when issuing a normal response.

Note 5: A Reason (Q.850; cause=1) header MAY be set only when the non-existence of the user is guaranteed by the provider at the transmitting side. At the receiving side, a unallocated (unassigned) number talkie MAY be sent out depending on the content of the Reason (Q.850; cause=1) header.

Note 6: Used when the call in question does not exist. The call is terminated at the receiving side.

Note 7: Used when a user is busy. The call is terminated at the receiving side.

Note 8: Used when disconnecting during call initiation. The call is terminated at the transmitting and receiving sides.

c1: "m" when using a JF-IETF-RFC4028 [16], or "x" otherwise.

c2: "m" when it can be used by agreement between providers, or "x" otherwise.

Table 4-5/JJ-90.25: SIP response signals to CANCEL, BYE and PRACK requests

SIP response signal			Reference	Class (transmitting side)	Class (receiving side)	Notes
Class	Code	Phrase				
1xx	100	Trying	[1][2]	x	x	

SIP response signal			Reference	Class (transmitting side)	Class (receiving side)	Notes
Class	Code	Phrase				
	180	Ringing	[1][2]	x	x	
	181	Call Is Being Forwarded	[1][2]	x	x	
	182	Queued	[1][2]	x	x	
	183	Session Progress	[1][2]	x	x	
	Other		[1][2]	x	x	
2xx	200	OK	[1][2]	m	m	(Note 1)
	Other		[1][2]	o	o	
3xx	300	Multiple Choices	[1][2]	x	x	
	301	Moved Permanently	[1][2]	x	x	
	302	Moved Temporarily	[1][2]	x	x	
	305	Use Proxy	[1][2]	x	x	
	380	Alternative Service	[1][2]	x	x	
	Other		[1][2]	x	x	
4xx	400	Bad Request	[1][2]	o	o	
	401	Unauthorized	[1][2]	x	x	
	402	Payment Required	[1][2]	o	o	
	403	Forbidden	[1][2]	o	o	
	404	Not Found	[1][2]	o	o	
	405	Method Not Allowed	[1][2]	c1	o	
	406	Not Acceptable	[1][2]	o	o	
	407	Proxy Authentication Required	[1][2]	x	x	
	408	Request Timeout	[1][2]	o	o	
	410	Gone	[1][2]	o	o	
	413	Request Entity Too Large	[1][2]	o	o	
	414	Request-URI Too Long	[1][2]	o	o	
	415	Unsupported Media Type	[1][2]	x	x	
	416	Unsupported URI Scheme	[1][2]	o	o	
	420	Bad Extension	[1][2]	o	o	
	421	Extension Required	[1][2]	x	x	
	422	Session Interval Too Small	[2][15]	x	x	
	423	Interval Too Brief	[1][2]	x	x	
	480	Temporarily Unavailable	[1][2]	o	o	
	481	Call/Transaction Does Not Exist	[1][2]	o	o	
	482	Loop Detected	[1][2]	o	o	
	483	Too Many Hops	[1][2]	o	o	

SIP response signal			Reference	Class (transmitting side)	Class (receiving side)	Notes
Class	Code	Phrase				
	484	Address Incomplete	[1][2]	o	o	
	485	Ambiguous	[1][2]	o	o	
	486	Busy Here	[1][2]	o	o	
	487	Request Terminated	[1][2]	o	o	
	488	Not Acceptable Here	[1][2]	o	o	
	491	Request Pending	[1][2]	o	o	
	493	Undecipherable	[1][2]	o	o	
	Other		[1][2]	o	o	
5xx	500	Server Internal Error	[1][2]	o	o	
	501	Not Implemented	[1][2]	o	o	
	502	Bad Gateway	[1][2]	o	o	
	503	Service Unavailable	[1][2]	o	o	
	504	Server Time-out	[1][2]	o	o	
	505	Version Not Supported	[1][2]	o	o	
	513	Message Too Large	[1][2]	o	o	
	Other		[1][2]	o	o	
6xx	600	Busy Everywhere	[1][2]	o	o	
	603	Decline	[1][2]	o	o	
	604	Does Not Exist Anywhere	[1][2]	o	o	
	606	Not Acceptable	[1][2]	o	o	
	Other		[1][2]	o	o	

Note 1: Used when issuing a normal response.

c1: “x” when using PRACK [2], or “m” otherwise. Whether or not PRACK can be used is basically determined by the Allow header of the message sent when establishing the dialog.

Table 4-6/JJ-90.25: List of SIP responses to UPDATE requests

SIP response signal			Reference	Class (transmitting side)	Class (receiving side)	Notes
Class	Code	Phrase				
1xx	100	Trying	[1][4]	x	x	
	180	Ringing	[1][4]	x	x	
	181	Call Is Being Forwarded	[1][4]	x	x	
	182	Queued	[1][4]	x	x	
	183	Session Progress	[1][4]	x	x	
	Other		[1][4]	x	x	
2xx	200	OK	[1][4]	m	m	(Note 1)

SIP response signal			Reference	Class (transmitting side)	Class (receiving side)	Notes
Class	Code	Phrase				
	Other		[1][4]	o	o	
3xx	300	Multiple Choices	[1][4]	x	x	
	301	Moved Permanently	[1][4]	x	x	
	302	Moved Temporarily	[1][4]	x	x	
	305	Use Proxy	[1][4]	x	x	
	380	Alternative Service	[1][4]	x	x	
	Other		[1][4]	x	x	
4xx	400	Bad Request	[1][4]	o	o	
	401	Unauthorized	[1][4]	x	x	
	402	Payment Required	[1][4]	o	o	
	403	Forbidden	[1][4]	o	o	
	404	Not Found	[1][4]	o	o	
	405	Method Not Allowed	[1][4]	c2	o	
	406	Not Acceptable	[1][4]	o	o	
	407	Proxy Authentication Required	[1][4]	x	x	
	408	Request Timeout	[1][4]	o	o	
	410	Gone	[1][4]	o	o	
	413	Request Entity Too Large	[1][4]	o	o	
	414	Request-URI Too Long	[1][4]	o	o	
	415	Unsupported Media Type	[1][4]	o	o	
	416	Unsupported URI Scheme	[1][4]	o	o	
	420	Bad Extension	[1][4]	o	o	
	421	Extension Required	[1][4]	x	x	
	422	Session Interval Too Small	[4][15]	c1	c1	
	423	Interval Too Brief	[1][4]	x	x	
	480	Temporarily Unavailable	[1][4]	o	o	
	481	Call/Transaction Does Not Exist	[1][4]	o	o	
	482	Loop Detected	[1][4]	o	o	
	483	Too Many Hops	[1][4]	o	o	
	484	Address Incomplete	[1][4]	o	o	
	485	Ambiguous	[1][4]	o	o	
	486	Busy Here	[1][4]	o	o	
	487	Request Terminated	[1][4]	o	o	
	488	Not Acceptable Here	[1][4]	o	o	
	491	Request Pending	[1][4]	o	o	

SIP response signal			Reference	Class (transmitting side)	Class (receiving side)	Notes
Class	Code	Phrase				
	493	Undecipherable	[1][4]	o	o	
	Other		[1][4]	o	o	
5xx	500	Server Internal Error	[1][4]	o	o	
	501	Not Implemented	[1][4]	o	o	
	502	Bad Gateway	[1][4]	o	o	
	503	Service Unavailable	[1][4]	o	o	
	504	Server Time-out	[1][4]	o	o	
	505	Version Not Supported	[1][4]	o	o	
	513	Message Too Large	[1][4]	o	o	
	Other		[1][4]	o	o	
6xx	600	Busy Everywhere	[1][4]	o	o	
	603	Decline	[1][4]	o	o	
	604	Does Not Exist Anywhere	[1][4]	o	o	
	606	Not Acceptable	[1][4]	o	o	
	Other		[1][4]	o	o	

Note 1: Used when issuing a normal response.

c1: “m” when using a JF-IETF-RFC4028 [16], or “x” otherwise.

c2: “x” when using UPDATE [13], or “m” otherwise. Whether or not UPDATE can be used is basically determined by the Allow header of the message sent when establishing the dialog.

4.10. SIP messages and header information

This section describes the setting of header information in request messages and response messages in each SIP method.

4.10.1. ACK

This message is sent on in the forward direction when a final response is received to an INVITE request.

4.10.1.1. Request messages

Table 4-7/JJ-90.25: ACK request messages

Message class: request

Method: ACK

Data element	Reference	Class (transmitting side)	Class (receiving side)	Notes
Authorization	[1]20.7	x	x	
Call-ID	[1]20.8	m	m	
Contact	[1]20.8	o	m	
Content-Disposition	[1]20.11	x	x	
Content-Encoding	[1]20.12	x	x	
Content-Language	[1]20.13	x	x	
Content-Length	[1]20.14	m	m	(Note 1)
Content-Type	[1]20.15	x	x	4.11.5
CSeq	[1]20.16	m	m	4.11.6
Date	[1]20.17	o	o	
From	[1]20.20	m	m	4.11.7
Max-Forwards	[1]20.22	m	m	
MIME-Version	[1]20.24	x	x	
Privacy	[5]4.2	x	x	4.11.9
Proxy-Authorization	[1]20.27	x	x	
Record-Route	[1]20.30	o	o	4.11.10 (Note 2)
Route	[1]20.34	c1	m	4.11.11
Timestamp	[1]20.38	o	o	
To	[1]20.39	m	m	4.11.13
User-Agent	[1]20.41	o	o	
Via	[1]20.42	m	m	4.11.14
Message body	[1]7.4	x	x	5.3

Note 1: Set to “0” because the message body is not used.

Note 2: Even if this is set, its significance MAY be impossible to resolve at the called network side.

c1: Set to “m” when there is a route set established in the INITIAL response, or to “x” otherwise.

4.10.1.2. Response messages

Responses to ACK request messages are not prescribed.

4.10.2. BYE

This message is used when disconnecting a requested call after it has been started (after establishing a dialog or an early dialog).

4.10.2.1. Request messages

Table 4-8/JJ-90.25: BYE request messages

Message class: request

Method: BYE

Data element	Reference	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
Accept	[1]20.1	o	o	
Accept-Encoding	[1]20.2	o	o	
Accept-Language	[1]20.3	o	o	
Allow	[1]20.5	o	o	4.11.4
Authorization	[1]20.7	x	x	
Call-ID	[1]20.8	m	m	
Content-Disposition	[1]20.11	x	x	
Content-Encoding	[1]20.12	x	x	
Content-Language	[1]20.13	x	x	
Content-Length	[1]20.14	m	m	(Note 1)
Content-Type	[1]20.15	x	x	4.11.5
CSeq	[1]20.16	m	m	4.11.6
Date	[1]20.17	o	o	
From	[1]20.20	m	m	4.11.7
Max-Forwards	[1]20.22	m	m	
MIME-Version	[1]20.24	x	x	
P-Asserted-Identity	[3]9.1	x	x	4.11.8
P-Preferred-Identity	[6]9.2	x	x	
Privacy	[5]4.2	x	x	4.11.9
Proxy-Authorization	[1]20.28	x	x	
Proxy-Require	[1]20.29	o	m	
Record-Route	[1]20.30	o	o	4.11.10
Require	[1]20.32	x	m	
Route	[1]20.34	c1	m	4.11.11
Supported	[1]20.37	o	o	
Timestamp	[1]20.38	o	o	
To	[1]20.39	m	m	4.11.13
User-Agent	[1]20.41	o	o	
Via	[1]20.42	m	m	4.11.14
Message body	[1]7.4	x	x	

Note 1: Set to “0” because the message body is not used.

c1: Set to “m” when there is an entry for the other provider’s SIP network in the route set during transmission, or to “x” otherwise.

4.10.2.2. Response messages

Table 4-9/JJ-90.25: BYE response message

Message class: response

Method: BYE

Data element	Reference	Application	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
Accept	[1]20.1	415	x	x	
Accept-Encoding	[1]20.2	415	x	x	
Accept-Language	[1]20.3	415	x	x	
Allow	[1]20.5	2xx r	o	o	4.11.4
Allow	[1]20.5	405	x	x	4.11.4
Authentication-Info	[1]20.6	2xx	x	x	
Call-ID	[1]20.8	c	m	m	
Contact	[1]20.10	3xx 485	o	m	
Content-Disposition	[1]20.11	All codes	x	x	
Content-Encoding	[1]20.12	All codes	x	x	
Content-Language	[1]20.13	All codes	x	x	
Content-Length	[1]20.14	All codes	m	m	
Content-Type	[1]20.15	All codes	x	x	4.11.5
Cseq	[1]20.16	All codes	m	m	4.11.6
Date	[1]20.17	All codes	o	o	
Error-Info	[1]20.18	300- 699	o	o	
From	[1]20.20	All codes	m	m	4.11.7
MIME-Version	[1]20.24	All codes	x	x	
P-Asserted-Identity	[6]9.1	All codes	x	x	
P-Preferred-Identity	[6]9.2	All codes	x	x	
Privacy	[5]4.1	All codes	x	x	
Proxy-Authenticate	[1]20.27	401 407	x	x	
Record-Route	[1]20.30	18x 2xx	o	o	4.11.10
Require	[1]20.32	All codes	x	x	

Retry-After	[1]20.33	404 413 480 486 500 503 600 603	o	o	
Server	[1]20.35	All codes	o	o	
Supported	[1]20.37	2xx	o	o	
Timestamp	[1]20.38	All codes	o	o	
To	[1]20.39	All codes	m	m	4.11.13
Unsupported	[1]20.40	420	x	x	
User-Agent	[1]20.41	All codes	o	o	
Via	[1]20.42	All codes	m	m	4.11.14
Warning	[1]20.43	All codes	o	o	
WWW-Authenticate	[1]20.44	All codes	x	x	
Message body	[1]7.4	2xx	x	x	

4.10.3. CANCEL

This message is used when disconnecting a requested call from the caller before the call has been established.

4.10.3.1. Request messages

Table 4-10/JJ-90.25: `CANCEL` request messages

Message class: request

Method: `CANCEL`

Data element	Reference	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
`Authorization`	[1]20.7	x	x	
`Call-ID`	[1]20.8	m	m	
`Content-Length`	[1]20.14	m	m	(Note 1)
`CSeq`	[1]20.16	m	m	4.11.6
`Date`	[1]20.17	o	o	
`From`	[1]20.20	m	m	4.11.7
`Max-Forwards`	[1]20.22	m	m	
`Privacy`	[5]4.2	x	x	4.11.9
`Record-Route`	[1]20.30	o	o	4.11.10
`Route`	[1]20.32	x	x	4.11.11
`Supported`	[1]20.37	o	o	
`Timestamp`	[1]20.28	o	o	
`To`	[1]20.39	m	m	4.11.13
`User-Agent`	[1]20.41	o	o	
`Via`	[1]20.42	m	m	4.11.14
Note 1: Set to ”0”.				

4.10.3.2. Response messages

Table 4-11/JJ-90.25: CANCEL response messages

Message class: response

Method: CANCEL

Data element	Reference	Application	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
Call-ID	[1]20.8	All codes	m	m	
Content-Length	[1]20.14	All codes	m	m	(Note 1)
CSeq	[1]20.16	All codes	m	m	4.11.6
Date	[1]20.17	All codes	o	o	
Error-Info	[1]20.18	300- 699	o	o	
From	[1]20.20	All codes	m	m	4.11.7
Privacy		All codes	x	x	
Proxy-Authenticate	[1]20.27	401	x	x	
Record-Route	[1]20.30	18x 2xx	o	o	4.11.10
Retry-After	[1]20.33	404 413 480 486 500 503 600 603	o	o	
Server	[1]20.35	All codes	o	o	
Supported	[1]20.37	2xx	o	o	
Timestamp	[1]20.38	All codes	o	o	
To	[1]20.39	All codes	m	m	4.11.13
User-Agent	[1]20.42	All codes	o	o	
Via	[1]20.42	All codes	m	m	4.11.14
Warning	[1]20.43	All codes	o	o	
Note 1: Set to “0”.					

4.10.4. Initial INVITE

This message is used to initiate a call.

4.10.4.1. Request messages

Table 4-12/JJ-90.25: Initial INVITE request messages

Message class: request

Method: INVITE

Data element	Reference	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
Accept	[1]20.1	o	o	
Accept-Encoding	[1]20.2	o	o	
Accept-Language	[1]20.3	o	o	
Alert-Info	[1]20.4	o	o	
Allow	[1]20.5	o	o	4.11.4
Authorization	[1]20.7	x	x	
Call-ID	[1]20.8	m	m	
Call-Info	[1]20.9	o	o	
Contact	[1]20.10	m	m	
Content-Disposition	[1]20.11	o	o	
Content-Encoding	[1]20.12	o	o	
Content-Language	[1]20.13	o	o	
Content-Length	[1]20.14	m	m	
Content-Type	[1]20.15	m	m	4.11.5
CSeq	[1]20.16	m	m	4.11.6
Date	[1]20.17	o	o	
Expires	[1]20.19	o	m	
From	[1]20.20	m	m	4.11.7
In-Reply-To	[1]20.21	o	o	
Max-Forwards	[1]20.22	m	m	
MIME-Version	[1]20.24	o	o	
Min-SE	[15]5.	o	c1	
Organization	[1]20.25	o	o	
P-Asserted-Identity	[6]9.1	m	m	4.11.8
P-Preferred-Identity	[6]9.2	x	x	
Priority	[1]20.26	o	o	
Privacy	[5]4.2	m	m	4.11.9
Proxy-Authorization	[1]20.28	x	x	
Proxy-Require	[1]20.29	c2	m	
Record-Route	[1]20.30	o	m	4.11.10
Reply-To	[1]20.31	o	o	
Require	[1]20.32	c2	m	
Route	[1]20.34	x	x	4.11.11

Data element	Reference	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
`Session-Expires`	[15]4.	o	c1	4.11.12
`Subject`	[1]20.36	o	o	
`Supported`	[1]20.37	o	c3	
`Timestamp`	[1]20.38	o	o	
`To`	[1]20.39	m	m	4.11.13
`User-Agent`	[1]20.41	o	o	
`Via`	[1]20.42	m	m	4.11.14
Message body	[1]7.4	m	m	(Note 1)

Note 1: Message body MUST be set.

c1: “m” when using a JF-IETF-RFC4028 [16], or “o” otherwise.

c2: It is possible to set an option tag that can be used based on discussions between providers. When an option tag that has not been discussed is set, a `420 (Bad Extension)` response MUST be issued.

c3: “m” when using a JF-IETF-RFC4025 [16] and `100rel` [2], or “o” otherwise.

4.10.4.2. Response messages

Table 4-13/JJ-90.25: Initial `INVITE` response messages

Message class: response

Method: `INVITE`

Data element	Reference	Application	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
`Accept`	[1]20.1	2xx	o	o	
`Accept`	[1]20.1	415	m	m	
`Accept-Encoding`	[1]20.2	2xx	o	o	
`Accept-Encoding`	[1]20.2	415	m	m	
`Accept-Language`	[1]20.3	2xx	o	o	
`Accept-Language`	[1]20.3	415	m	m	
`Alert-Info`	[1]20.4	180	o	o	
`Allow`	[1]20.5	2xx	m	m	4.11.4
`Allow`	[1]20.5	All codes	o	o	4.11.4
`Allow`	[1]20.5	405	x	x	4.11.4
`Authentication-Info`	[1]20.6	2xx	x	x	
`Call-ID`	[1]20.8	All codes	m	m	
`Call-Info`	[1]20.9	All codes	o	o	

Data element	Reference	Application	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
Contact	[1]20.10	1xx	o	m	
Contact	[1]20.10	2xx	m	m	
Contact	[1]20.10	3xx 485	o	m	
Content-Disposition	[1]20.11	All codes	o	o	
Content-Encoding	[1]20.12	All codes	o	o	
Content-Language	[1]20.13	All codes	o	o	
Content-Length	[1]20.14	All codes	m	m	
Content-Type	[1]20.15	All codes	c1	m	4.11.5
CSeq	[1]20.16	All codes	m	m	4.11.6
Date	[1]20.17	All codes	o	o	
Error-Info	[1]20.18	300- 699	o	o	
Expires	[1]20.19	All codes	o	m	
From	[1]20.20	All codes	m	m	4.11.7
MIME-Version	[1]20.24	All codes	o	o	
Min-SE	[15]5.	422	c3	m	
Organization	[1]20.25	All codes	o	o	
P-Asserted-Identity	[6]9.1	All codes	o	m	4.11.8
P-Preferred-Identity	[6]9.2	All codes	x	x	
Privacy	[5]4.2	All codes	o	m	
Proxy-Authenticate	[1]20.27	401 407	x	x	
Reason	[14]2.	404	c4	m	
Record-Route	[1]20.30	18x 2xx	o	m	4.11.10
Reply-To	[1]20.31	All codes	o	o	
Require	[1]20.32	18x	c2	m	
Require	[1]20.32	2xx	c3	m	
Retry-After	[1]20.33	404 413 480 486 500 503 600 603	o	o	

Data element	Reference	Application	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
`Rseq`	[2]7.1	`1xx`	o	o	
`Server`	[1]20.35	All codes	o	o	
`Session-Expires`	[15]4.	`2xx`	c3	m	4.11.12
`Supported`	[1]20.37	`2xx`	o	m	
`Timestamp`	[1]20.38	All codes	o	o	
`To`	[1]20.39	All codes	m	m	4.11.13
`Unsupported`	[1]20.40	`420`	m	m	
`User-Agent`	[1]20.41	All codes	o	o	
`Via`	[1]20.42	All codes	m	m	4.11.14
`Warning`	[1]20.43	All codes	o	o	
`WWW-Authenticate`	[1]20.44	All codes	x	x	

Message body	[1]7.4	`18x`
		`2xx`
			o	m	(Note 1)

Note 1: SDP information may be provided as a provisional response when `100rel` is not supported. 200 (OK) MUST include Message body. However, when SDP is provided as a provisional response with a confirmed response when `100rel` is supported, a `200 (OK)` response with no SDP may be given.

c1: “m” when SDP is used in the response, or “x” otherwise.

c2: “m” when `100rel` [2] is used, or “x” otherwise.

c3: “m” when JF-IETF-RFC4028 [16] is used, or “x” otherwise.

c4: “m” for an unallocated number, or “o” otherwise.

4.10.5. re-INVITE

This message is used to refresh a call (session timer) and to modify the media stream settings in the middle of a call.

4.10.5.1. Request messages

Table 4-14/JJ-90.25: re-`INVITE` request messages

Message class: request

Method: `INVITE`

Data element	Reference	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
`Accept`	[1]20.1	o	o	
`Accept-Encoding`	[1]20.2	o	o	
`Accept-Language`	[1]20.3	o	o	
`Alert-Info`	[1]20.4	o	o	
`Allow`	[1]20.5	o	o	4.11.4

Data element	Reference	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
`Authorization`	[1]20.7	x	x	
`Call-ID`	[1]20.8	m	m	
`Call-Info`	[1]20.9	o	o	
`Contact`	[1]20.10	m	m	
`Content-Disposition`	[1]20.11	o	o	
`Content-Encoding`	[1]20.12	o	o	
`Content-Language`	[1]20.13	o	o	
`Content-Length`	[1]20.14	m	m	
`Content-Type`	[1]20.15	m	m	4.11.5
`CSeq`	[1]20.16	m	m	4.11.6
`Date`	[1]20.17	o	o	
`Expires`	[1]20.19	o	o	
`From`	[1]20.20	m	m	4.11.7
`In-Reply-To`	[1]20.21	o	o	
`Max-Forwards`	[1]20.22	m	m	
`MIME-Version`	[1]20.24	o	o	
`Min-SE`	[15]5.	o	c1	
`Organization`	[1]20.25	o	o	
`P-Asserted-Identity`	[6]9.1	x	x	4.11.8
`P-Preferred-Identity`	[6]9.2	x	x	
`Priority`	[1]20.26	o	o	
`Privacy`	[5]4.2	x	x	4.11.9
`Proxy-Authorization`	[1]20.28	x	x	
`Proxy-Require`	[1]20.29	c2	m	
`Record-Route`	[1]20.30	x	x	4.11.10 (Note 1)
`Reply-To`	[1]20.31	o	o	
`Require`	[1]20.32	c2	m	
`Route`	[1]20.34	c3	m	4.11.11
`Session-Expires`	[15]4.	o	c1	4.11.12
`Subject`	[1]20.36	x	x	
`Supported`	[1]20.37	o	c1	
`Timestamp`	[1]20.38	o	o	
`To`	[1]20.39	m	m	4.11.13
`User-Agent`	[1]20.41	o	o	
`Via`	[1]20.42	m	m	4.11.14
Message body	[1]7.4	m	m	

Data element	Reference	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes

Note 1: In a re-INVITE request, the route set established in the Initial INVITE MUST NOT be modified.

c1: “m” when using a JF-IETF-RFC4028 [16], or “x” otherwise.

c2: It is possible to set an option tag that can be used based on discussions between providers. When an option tag that has not been discussed is set, a 420 (Bad Extension) response MUST be issued.

c3: “m” when there is a route set, or “x” otherwise.

4.10.5.2. Responses

Table 4-15/JJ-90.25: re-INVITE response messages

Message class: response

Method: INVITE

Data element	Reference	Application	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
Accept	[1]20.1	2xx	o	o	
Accept	[1]20.1	415	m	m	
Accept-Encoding	[1]20.2	2xx	o	o	
Accept-Encoding	[1]20.2	415	m	m	
Accept-Language	[1]20.3	2xx	o	o	
Accept-Language	[1]20.3	415	m	m	
Alert-Info	[1]20.4	180	o	o	
Allow	[1]20.5	2xx	m	m	4.11.4
Allow	[1]20.5	All codes	o	o	4.11.4
Allow	[1]20.5	405	m	m	4.11.4
Authentication-Info	[1]20.6	2xx	x	x	
Call-ID	[1]20.8	All codes	m	m	
Call-Info	[1]20.9	All codes	o	o	
Contact	[1]20.10	1xx	o	m	
Contact	[1]20.10	2xx	m	m	
Contact	[1]20.10	3xx, 485	o	m	
Content-Disposition	[1]20.11	All codes	o	o	
Content-Encoding	[1]20.12	All codes	o	o	
Content-Language	[1]20.13	All codes	o	o	

Data element	Reference	Application	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
Content-Length	[1]20.14	All codes	m	m	
Content-Type	[1]20.15	All codes	m	m	4.11.5
CSeq	[1]20.16	All codes	m	m	4.11.6
Date	[1]20.17	All codes	o	o	
Error-Info	[1]20.18	300- 699	o	o	
Expires	[1]20.19	All codes	o	o	
From	[1]20.20	All codes	m	m	4.11.7
MIME-Version	[1]20.24	All codes	o	o	
Min-SE	[15]5.	422	c1	m	
Organization	[1]20.25	All codes	o	o	
P-Asserted-Identity	[6]9.1	All codes	x	m	4.11.8
P-Preferred-Identity	[6]9.2	All codes	x	x	
Privacy	[5]4.2	All codes	x	x	
Proxy-Authenticate	[1]20.27	401 407	x	x	
Record-Route	[1]20.30	2xx 18x	x	x	4.11.10 (Note 2)
Reply-To	[1]20.31	All codes	o	o	
Require	[1]20.32	All codes	c1	m	
Retry-After	[1]20.33	404 413 480 486 500 503 600 603	o	o	
Rseq	[2]7.1	1xx	o	o	
Server	[1]20.35	All codes	o	o	
Session-Expires	[15]4.	2xx	c1	m	4.11.12
Supported	[1]20.37	2xx	c1	m	
Timestamp	[1]20.38	All codes	o	o	
To	[1]20.39	All codes	m	m	4.11.13
Unsupported	[1]20.40	420	m	m	
User-Agent	[1]20.41	All codes	o	o	
Via	[1]20.42	All codes	m	m	4.11.14

Data element	Reference	Application	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
Warning	[1]20.43	All codes	o	o	
WWW-Authenticate	[1]20.44	All codes	x	x	
Message body	[1]7.4	2xx	m	m	(Note 1)

Note 1: MUST be used when updating session timers and modifying media stream settings.

Note 2: The route set established in the Initial INVITE MUST NOT be modified.

c1: “m” when JF-IETF-RFC4028 [16] is used, or “x” otherwise.

4.10.6. PRACK

This message is used when providing a reliable provisional response message (100rel) in the process of establishing a call.

4.10.6.1. Request messages

Table 4-16/JJ-90.25: PRACK request messages

Message class: request

Method: PRACK

Data element	Reference	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
Accept	[1]20.1	o	o	
Accept-Encoding	[1]20.2	o	o	
Accept-Language	[1]20.3	o	o	
Allow	[1]20.5	o	o	4.11.4
Authorization	[1]20.7	x	x	
Call-ID	[1]20.8	m	m	
Content-Disposition	[1]20.11	o	o	
Content-Encoding	[1]20.12	o	o	
Content-Language	[1]20.13	o	o	
Content-Length	[1]20.14	m	m	
Content-Type	[1]20.15	c2	m	4.11.5
CSeq	[1]20.16	m	m	4.11.6
Date	[1]20.17	o	o	
From	[1]20.20	m	m	4.11.7

Data element	Reference	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
Max-Forwards	[1]20.22	m	m	
MIME-Version	[1]20.24	o	o	
Proxy-Authorization	[1]20.28	x	x	
Proxy-Require	[1]20.29	o	m	
RAck	[5]7.2	m	m	
Record-Route	[1]20.30	o	o	4.11.10
Require	[1]20.32	o	m	
Route	[1]20.34	c1	m	4.11.11
Supported	[1]20.37	o	o	
Timestamp	[1]20.38	o	o	
To	[1]20.39	m	m	4.11.13
User-Agent	[1]20.41	o	o	
Via	[1]20.42	m	m	4.11.14
Message body		o	m	
c1: "m" when there is a route set, or "x" otherwise. c2: "m" when setting is possible based on agreement between providers, or "x" otherwise.				

4.10.6.2. Responses

Table 4-17/JJ-90.25: PRACK response messages

Message class: response

Method: PRACK

Data element	Reference	Application	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
Accept	[1]20.1	415	m	m	
Accept-Encoding	[1]20.2	415	m	m	
Accept-Language	[1]20.3	415	m	m	
Allow	[1]20.5	2xx	o	o	4.11.4
Allow	[1]20.5	All codes	o	o	4.11.4
Allow	[1]20.5	405	m	m	4.11.4
Authentication-Info	[1]20.6	2xx	x	x	
Call-ID	[1]20.8	All codes	m	m	
Contact	[1]20.10	3xx 485	o	o	

Data element	Reference	Application	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
Content-Disposition	[1]20.11	All codes	o	o	
Content-Encoding	[1]20.12	All codes	o	o	
Content-Language	[1]20.13	All codes	o	o	
Content-Length	[1]20.14	All codes	m	m	
Content-Type	[1]20.15	All codes	c1	m	4.11.5
CSeq	[1]20.16	All codes	m	m	4.11.6
Date	[1]20.17	All codes	o	o	
Error-Info	[1]20.18	300- 699	o	o	
From	[1]20.20	All codes	m	m	4.11.7
MIME-Version	[1]20.24	All codes	o	o	
Proxy-Authenticate	[1]20.27	401 407	x	x	
Record-Route	[1]20.30	18x 2xx	o	o	4.11.10
Require	[1]20.32	All codes	c	c	
Retry-After	[1]20.33	404 413 480 486 500 503 600 603	o	o	
Server	[1]20.35	All codes	o	o	
Supported	[1]20.37	2xx	o	o	
Timestamp	[1]20.38	All codes	o	o	
To	[1]20.39	All codes	m	m	4.11.13
Unsupported	[1]20.40	420	m	o	
User-Agent	[1]20.41	All codes	o	o	
Via	[1]20.42	All codes	m	m	4.11.14
Warning	[1]20.43	All codes	o	o	
WWW-Authenticate	[1]20.44	401	x	m	
Message body	[1]7.4	2xx	o	m	(Note 1)

Note 1: MUST be used when modifying media stream settings.

c1: “m” when setting is possible based on agreement between providers, or “x” otherwise.

4.10.7. UPDATE

This message is used to refresh a call (session timer) and to modify the media stream settings in the middle of a call.

4.10.7.1. Request messages

Table 4-18/JJ-90.25: UPDATE request messages

Message class: request

Method: UPDATE

Data element	Reference	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
Accept	[1]20.1	o	o	
Accept-Encoding	[1]20.2	o	o	
Accept-Language	[1]20.3	o	o	
Allow	[1]20.5	o	o	4.11.4
Authorization	[1]20.7	x	x	
Call-ID	[1]20.8	m	m	
Call-Info	[1]20.9	o	o	
Contact	[1]20.10	m	m	
Content-Disposition	[1]20.11	o	o	
Content-Encoding	[1]20.12	o	o	
Content-Language	[1]20.13	o	o	
Content-Length	[1]20.14	m	m	
Content-Type	[1]20.15	c1	m	4.11.5
CSeq	[1]20.16	m	m	4.11.6
Date	[1]20.17	o	o	
From	[1]20.20	m	m	4.11.7
Max-Forwards	[1]20.22	m	m	
MIME-Version	[1]20.24	o	o	
Min-SE	[15]5.	o	c4	
Organization	[1]20.25	o	o	
Proxy-Authorization	[1]20.28	x	x	
Proxy-Require	[1]20.29	o	m	
Record-Route	[1]20.30	x	x	4.11.10 (Note 1)
Require	[1]20.32	c2	m	
Route	[1]20.34	c3	m	4.11.11
Session-Expires	[15]4.	o	c4	4.11.12
Supported	[1]20.37	o	c4	

Data element	Reference	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
`Timestamp`	[1]20.38	o	o	
`To`	[1]20.39	m	m	4.11.13
`User-Agent`	[1]20.41	o	o	
`Via`	[1]20.42	m	m	4.11.14
Message body	[1]7.4	c1	m	(Note 2)

Note 1: The route set established in the Initial `INVITE` cannot be modified.

Note 2: Used when modifying media stream settings.

c1: “m” when SDP is set in the response, or “x” otherwise.

c2: Set when an extension is required by the provider’s SIP network.

c3: “m” when there is a route set, or “x” otherwise.

c4: “m” when using a JF-IETF-RFC4028 [16], or “x” otherwise.

4.10.7.2. Responses

Table 4-19/JJ-90.25: `UPDATE` response messages

Message class: Response

Method: `UPDATE`

Data element	Reference	Application	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
`Accept`	[1]20.1	`2xx`	o	o	
`Accept`	[1]20.1	`415`	m	m	
`Accept-Encoding`	[1]20.2	`2xx`	o	o	
`Accept-Encoding`	[1]20.2	`415`	m	m	
`Accept-Language`	[1]20.3	`2xx`	o	o	
`Accept-Language`	[1]20.3	`415`	m	m	
`Allow`	[1]20.5	`2xx`	o	o	4.11.4
`Allow`	[1]20.5	All codes	o	o	4.11.4
`Allow`	[1]20.5	`405`	m	m	4.11.4
`Authentication-Info`	[1]20.6	`2xx`	x	x	
`Call-ID`	[1]20.8	All codes	m	m	
`Call-Info`	[1]20.9	All codes	o	o	
`Contact`	[1]20.10	`1xx`	o	m	
`Contact`	[1]20.10	`2xx`	m	m	
`Contact`	[1]20.10	`3xx`	o	m	

Data element	Reference	Application	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
		485			
Content-Disposition	[1]20.11	All codes	o	o	
Content-Encoding	[1]20.12	All codes	o	o	
Content-Language	[1]20.13	All codes	o	o	
Content-Length	[1]20.14	All codes	m	m	
Content-Type	[1]20.15	All codes	c1	m	4.11.5
CSeq	[1]20.16	All codes	m	m	4.11.6
Date	[1]20.17	All codes	o	o	
Error-Info	[1]20.18	300- 699	o	o	
From	[1]20.20	All codes	m	m	4.11.7
MIME-Version	[1]20.24	All codes	c	c	
Min-SE	[15]5.	422	c2	m	
Organization	[1]20.25	All codes	o	o	
Proxy-Authenticate	[1]20.27	401 407	x	x	
Record-Route	[1]20.30	2xx	x	x	4.11.10 (Note 2)
Require	[1]20.32	All codes	c2	m	
Retry-After	[1]20.33	404 413 480 486 500 503 600 603	o	o	
Server	[1]20.35	All codes	o	o	
Session-Expires	[15]4.	2xx	c2	m	4.11.12
Supported	[1]20.37	2xx	c2	m	
Timestamp	[1]20.38	All codes	o	o	
To	[1]20.39	All codes	m	m	4.11.13
Unsupported	[1]20.40	420	x	x	
User-Agent	[1]20.41	All codes	o	o	
Via	[1]20.42	All codes	m	m	4.11.14
Warning	[1]20.43	All codes	o	o	
WWW-Authenticate	[1]20.44	All codes	x	x	
Message body	[1]7.4	2xx	o	m	(Note 1)

Data element	Reference	Application	Prescribed type (transmitting side)	Prescribed type (receiving side)	Notes
Note 1: Used when modifying media stream settings. Note 2: The route set established in the Initial `INVITE` cannot be modified. c1: "m" when SDP is used in the response, or "x" otherwise. c2: "m" when using a JF-IETF-RFC4028 [16], or "x" otherwise.					

4.11. Header data elements (header parameters) in each message

4.11.1. Basic format

Call settings and call control are performed by exchanging SIP/UDP/IP packets between networks.

SIP messages exist in two formats — request messages and response messages. Each of the header parameters used in these formats are prescribed here. Detailed discussions of these parameters can be found in the references. Where no specific ABNF codes are noted, the messages conform to the provisions of chapter 25 in JF-IETF-RFC3261 [1].

4.11.2. Request-Line

SIP requests are distinguished by having a Request-Line header in the first line of the message. The Request-Line header contains a method name, request-URI and protocol version information separated by white space (SP).
The Request-Line header is terminated with a line break (CRLF).

Table 4-20/JJ-90.25: `Request-Line` header data elements

Header: header data items		Type	Statement format	Notes
Request-Line			Method SP Request-URI SP SIP-Version CRLF	
	Method	m	INVITEm / ACKm / BYEm / CANCELm / UPDATEm / PRACKm / token	(Note 1)
	Request-URI	m	SIP-URI	See 4.12
	SIP-Version	m	"SIP/2.0"	
* Only one Request-Line header can be set. It is not possible to use more than one in the same message. Note 1: The use of PRACK and UPDATE differs between providers. The use of other requests (tokens) should be agreed upon between providers.				

4.11.3. Status-Line

SIP responses are distinguished by having a Status-Line header in the first line of the message. The Status-Line header contains protocol version information, a Status-Code and a Reason-Phase separated by white space (SP). The Status-Line header is terminated with a line break (CRLF).

Table 4-21/JJ-90.25: `Status-Line` header data elements

Header: header data items	Type	Statement format	Notes
Status-Line		SIP-Version SP Status-Code Reason-Phase CRLF	
SIP-Version	m	"SIP/2.0"	
Status-Code	m	3DIGIT	(Note 1)
Reason-Phase	m	Text string	
* Only one Status-Line header can be set. It is not possible to use more than one in the same message. Note 1: Only the Status-Code values shown in section 4.9 can be set.			

4.11.4. Allow

This header lists the combinations of methods supported by the UA that generated this message.

Table 4-22/JJ-90.25: `Allow` header data elements

Header: header data items	Type	Statement format	Notes
Allow		"Allow" HCOLON [Method *(COMMA Method)]	
Method	m	INVITEm / ACKm / BYEm / CANCELm / extension-method	(Note 1)
extension-method	c1	UPDATEm / PRACKm / token	(Note 1)
* This header can only be set once in a message. Note 1: Only the message classes shown in section 4.8 can be set. The methods are listed in no particular order. c1: “m” when the UA is capable of receiving this method, or “x” otherwise.			

4.11.5. Content-Type

Indicates the media type of the message body sent to the recipient.

Table 4-23/JJ-90.25: `Content-Type` header data elements

Header: header data items	Type	Statement format	Notes
Content-Type		("Content-Type" / "c") HCOLON media-type	
media-type	m	m-type SLASH m-subtype *(SEMI m-parameter)	(Note 1)
m-type	m	discrete-type / composite-type	
discrete-type	m	"application"	
composite-type	x	"message" / "multipart" / extension-token	
m-subtype	m	”sdp”	
m-parameter	x	m-attribute EQUAL m-value	
* This header can only be set once, and cannot be used more than once in the same message. Note 1: The use of multipart messages must be agreed upon between providers.			

4.11.6. CSeq

Used to uniquely identify a transaction.

Table 4-24/JJ-90.25: `CSeq` header data elements

Header: header data items	Type	Statement format	Notes
CSeq		"CSeq" HCOLON 1*DIGIT LWS Method	
1*DIGIT	m	"0" / "1" / "2" / "3" / "4" / "5" / "6" / "7" / "8" / "9"	
Method	m	INVITEm / ACKm / BYEm / CANCELm / PRACKm / UPDATEm / token	(Note 1)
* This header can only be set once, and cannot be used more than once in the same message. Note 1: The value of “token” should be agreed upon between providers.			

4.11.7. From

Indicates the initiator of a request. Specifies information from the caller.

Table 4-25/JJ-90.25: From header data elements

Header: header data items	Type	Statement format	Notes
From		("From" / "f") HCOLON from-spec	
from-spec	m	(name-addr / addr-spec) *(SEMI from-param)	
name-addr	o1	[display-name] LAQUOT addr-spec RAQUOT	
display-name	o	*(token LWS)/ quoted-string	
addr-spec	m		
addr-spec	o1		
from-param	m	tag-param / generic-param	
tag-param	m	"tag" EQUAL token	
generic-param	x	token [EQUAL gen-value]	
* This header can only be set once, and cannot be used more than once in the same message. o1: Depends on the selection of provider’s SIP network.			

4.11.8. P-Asserted-Identity

This header conforms to JJ-90.22 [11]. It is used to transfer authenticated user information inside each provider’s network. (See section 4.13.2.)

Table 4-26/JJ-90.25: P-Asserted-Identity header data elements

Header: header data items	Type	Statement format	Notes
P-Asserted-Identity		"P-Asserted-Identity" HCOLON PAssertedID-value *(COMMA PAssertedID-value)	
PAssertedID-value	m	name-addr / addr-spec	
name-addr	o1	[display-name] LAQUOT addr-spec RAQUOT	
display-name	o	*(token LWS)/ quoted-string	
addr-spec	m		See 4.12
addr-spec	o1		See 4.12
* Settings conform to JJ-90.22 [11]. o1: Depends on the selection of provider’s SIP network.			

4.11.9. Privacy

This header conforms to JJ-90.22 [11]. It is used to transfer authenticated user information inside each provider’s network. (See section 4.13.2.)

Table 4-27/JJ-90.25: `Privacy` header data elements

Header: header data items		Type	Statement format	Notes
Privacy			"Privacy" HCOLON priv-value	
	priv-value	m	"id" / "none"	

* This header can only be set once, and cannot be used more than once in the same message.

4.11.10. Record-Route

This header is inserted into a request by a proxy server so ensure that requests in the dialog pass through the same proxy server.

Table 4-28/JJ-90.25: `Record-Route` header data elements

Header: header data items				Type	Statement format	Notes
Record-Route					"Record-Route" HCOLON rec-route *(COMMA rec-route)	
	rec-route			m	name-addr *(SEMI rr-param)	
		name-addr		m	[display-name] LAQUOT addr-spec RAQUOT	
			display-name	x	*(token LWS)/ quoted-string	
			addr-spec	m		(Note 1)
		rr-param		o	generic-param	

* This header MAY be used more than once in the same message, up to a maximum of 5 lines and 10 entries. For details, see JJ-90.21 [10].

Note 1: Only SIP-URIs are acceptable.

4.11.11. Route

This header is used route request messages via listed proxies.

Table 4-29/JJ-90.25: `Route` header data elements

Header: header data items	Type	Statement format	Notes
Route		"Route" HCOLON route-param *(COMMA route-param)	
route-param	m	name-addr *(SEMI rr-param)	
name-addr	m	[display-name] LAQUOT addr-spec RAQUOT	
display-name	x	*(token LWS)/ quoted-string	
addr-spec	m		(Note 1)
rr-param	o	generic-param	
* This header MAY be used more than once in the same message, up to a maximum of 5 lines and 5 entries. Note 1: Only SIP-URIs are acceptable.			

4.11.12. Session-Expires

Specifies the valid duration of a session timer updated by a re-INVITE request.

Table 4-30/JJ-90.25: `Session-Expires` header data elements

Header: header data items	Type	Statement format	Notes
Session-Expires		("Session-Expires" / "x") HCOLON delta-seconds [refresher]	
delta-seconds	m	1*DIGIT	
refresher	o	SEMI "refresher" EQUAL "uas" / "uac"	
* This header can only be set once, and cannot be used more than once in the same message.			

4.11.13. To

Specifies the logical recipient of a request. Specifies information from the callee.

Table 4-31/JJ-90.25: To header data elements

Header: header data items	Type	Statement format	Notes
To		("To" / "t") HCOLON (name-addr / addr-spec) *(SEMI to-param)	
name-addr	o1	[display-name] LAQUOT addr-spec RAQUOT	
display-name	o	*(token LWS)/ quoted-string	
addr-spec	m		
addr-spec	o1		
to-param	o	tag-param / generic-param	
tag-param	m	"tag" EQUAL token	(Note 1)
generic-param	x	token [EQUAL gen-value]	
* This header can only be set once, and cannot be used more than once in the same message. Note 1: Not set in Initial INVITE or CANCEL requests. o1: Depends on the selection of provider's SIP network.			

4.11.14. Via

Indicates the transport used for a transaction.

Table 4-32/JJ-90.25: `Via` header data elements

Header: header data items	Type	Statement format	Notes
Via		("Via" / "v") HCOLON via-parm *(COMMA via-parm)	
via-parm	m	sent-protocol LWS sent-by *(SEMI via-params)	
sent-protocol	m	protocol-name SLASH protocol-version SLASH transport	
protocol-name	m	SIP / token	
protocol-version	m	"2.0"	
transport	m	"UDP" / other-transport	
sent-by	m	host [COLON port]	
host	m	hostname / IPv4address	
port	o	1*DIGIT	
via-params	o	via-ttl / via-maddr / via-received / via-branch / via-extension	
via-ttl	x	"ttl" EQUAL ttl	
via-maddr	o	"maddr" EQUAL host	
via-received	x	"received" EQUAL (IPv4address)	
via-branch	o	"branch" EQUAL token	
via-extension	x	generic-param	
* This header MAY be used more than once in the same message, up to a maximum of 5 lines and 5 entries. Constraints are only applied to addresses that indicate interworking SIP nodes or adjacent SIP nodes.			

4.12. URI specification schemes (addr-spec)

SIP-URI and TEL-URL formats are supported.

Table 4-33/JJ-90.25: The SIP-URI scheme

Header: header data items	Type	Statement format	Notes
addr-spec			
SIP-URI	m	"sip:" anonymous-string / denote-string	Address starts with “sip:”
Anonymous-string	o1	"anonymous@anonymous.invalid"	Used in a message’s From header etc. when the number notification is restricted.
denote-string	o1	[userinfo] hostport uri-parameters	Normal URI specification format
Userinfo	o	(user/telephone-subscriber) "@"	User identifier: user name, phone number etc. identified in host.
Telephone-subscriber	o2	global-phone-number	Phone number used as user number. (Conforms to JF-IETF-RFC3966 [7].)
global-phone-number	m	"+" 1*phonedigit	Indicates an E.164 number starting with +country code (international public telephone number)
phonedigit	x	DIGIT	Numerical digits and delimiters "-" / "." / "(" / ")" may be used.
user	o2	1*(unreserved / escaped / user-unreserved)	
"@"	m		When userinfo is used, “@” must be inserted to separate it from the host part.
Hostport	m	host [":" port]	Specifies a host that provides a resource.
Host	m	hostname / IPv4address	Host name is inserted as a FQDN IPv4 address.
Port	o	1*DIGIT	Specifies the port number that provides a resource.
Uri-parameters	o	*(";" uri-parameter)	indicates additional information for gaining network access to a host.
uri-parameter	o	transport-param / user-param / maddr-param / lr-param	
transport-param	o	"transport=" ("udp" / "tcp")	Indicates the transport protocol used to send an SIP message. udp and tcp are defined.
user-param	o	"user=" ("phone")	MAY be used to distinguish between actual phone numbers and user names that look like phone numbers. Specifying user=phone requests that it should be treated as a phone number.
maddr-param	o	"maddr=" host	Used to request that packets are sent out to the address specified by maddr. This address is used in preference to other host addresses

			or the like in the SIP-URI.
lr-param	m	"lr"	Used in Route information such as Record-Route. A Loose-Router MUST be used to connect between providers' networks.

Table 4-34/JJ-90.25: The TEL-URI scheme

Header: header data items	Type	Statement format	Notes
addr-spec			
TEL-URI	m	"tel:" telephone-subscriber	Address starts with “tel:”
telephone-subscriber	m	global-phone-number / local-phone-number	Phone number used as user number. (Conforms to JF-IETF-RFC3966 [7].)
global-phone-number	o	"+" 1*phonedigit	Indicates an E.164 number starting with +country code (international public telephone number)
phonedigit	m	DIGIT	Numerical digits may be used.
local-phone-number	o	1*phonedigit area-specifier	E.164 national number
phonedigit	m	DIGIT	Numerical digits may be used.
area-specifier	m	";phone-context=" phone-context-ident	Call initiating area information is added as additional dialing information.
phone-context-ident	m	"+" 1*phonedigit	Starts with “+country code”, followed by a national number with the national dialing prefix omitted.
phonedigit	m	DIGIT	Numerical digits may be used.

4.13. Other signal provisions

4.13.1. Handling non-prescribed signals

When signals or information not covered by this standard are transmitted from a provider issuing a request, the provider that receives this request is not guaranteed to treat this information as meaningful.

To guarantee correct behavior, the content of signals should be agreed upon between providers.

4.13.2. Handling caller numbers

Caller numbers should be notified by employing a scheme conforming to JJ-90.22 [11].

(1) The caller number is delivered in the Initial INVITE request.

(2) The caller number is set in each parameter value of the P-Asserted-Identity header, and incorporated into the

Initial INVITE request. This header MUST always be set.

(3) For data elements associated with the handling of the caller number, the following parameters defined in JJ-90.22 [11] are used:

1) SIP_URI: The addr-spec part of the SIP_URI in the P-Asserted-Identity header of an Initial INVITE request is taken as the SIP_URI.

2) SIP_DISPLAYNAME: The displayname part of the SIP_URI in the P-Asserted-Identity header of an Initial INVITE request 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.

3) TEL_URI: The addr-spec part of the TEL URI in the P-Asserted-Identity header of an Initial INVITE request is taken as the TEL_URI.

4) TEL_DISPLAYNAME: The contents of the Displayname part of the TEL_ URI in the P-Asserted-Identity header of an Initial INVITE request 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.

5) Privacy: Treated as the Privacy information in the Privacy header of the Initial INVITE request.

Table 4-35/JJ-90.25: Conditions for notifying caller numbers

Data item	Mapping condition	Notes
Calling party's number (contractor number)	TEL_URI	Used as a number identifying the caller. Visual separators not used.
Generic number (notified number)	TEL_DISPLAYNAME	Used when a number other than the caller number is notified to the callee. Visual separators not used.
notification/restriction	Privacy	Basically, "none" = displayable, "id" = not displayable. Assumed to be displayable when "id" is not included, or when the `Privacy` header itself is not set. When the calling number (contractor number) and general purpose number (notified number) are both set, this item is treated as the displayable / hidden status of the general purpose number (notified number), and the calling number (contractor number) is uniformly treated as hidden.
cause of no ID	SIP_DISPLAYNAME	According to JJ-90.22 [11], the reason for cause of no ID can be expressed using the following classes (text strings): "Anonymous", "Unavailable", "Interaction with other service" or "Coin line/payphone". If this item is not set, or if its contents are unclear, the call is taken to be impossible for an undisclosed reason, which is taken to be equivalent to "Unavailable".
* When TEL_URI is not set, it is taken to mean that there is no caller number to notify back to.		

5. Connection criteria

5.1. Session timer

It is RECOMMENDED that a session timer function according to JF-IETF-RFC4028 [16] is provided in order to detect the release of a session in cases where a call has not been terminated normally, or has not been released by means of a BYE request.

5.2. 100rel

In each hop of an SIP signal route, including the interface sections defined by this standard, it is RECOMMENDED that JF-IETF-RFC3262 [2] is supported in cases where there is no means of securing reliable forwarding of provisional response messages, such as a mechanism in a lower layer.

5.3. Bearer usage criteria

5.3.1. SDP format

Table 5-1/JJ-90.25: SDP data elements

Item header: abbreviation			Prescribed type		Setting details	Notes
			(transmitting side)	(receiving side)		
Session description						
	protocol version	v=	m	m	SDP version number (currently set to v=0)	
	owner/creator and session identifier	o=	m	m	Session initiator and session identifier information	
	session name	s=	m	m	Session name (no constraints on format or contents)	
	connection information	c=	o	m	Connection information (indicates the location where session data is received)	(Note 1)
Time description						
	time the session is active	t=	m	m	Session start/end time	(Note 2)
Media description						
	media name and transport address	m =	m	m	Media class and transport address	
	connection information	c=	o	m	Connection information (indicates the location where session data is received)	(Note 1)
	media attribute line	a=	o	o	Media attributes	

* Requires G.711 µ-Law. A value of 0 must be used for PT (payload type). Other details should be arranged between providers.

Note 1: One of these MUST be set.

Note 2: If set to “0 0” when initiating a call, it must be ignored when receiving the call.

Media sessions in SIP (JF-IETF-RFC3261 [1]) are established and managed by means of SDP (Session Description Protocol) exchanges of SIP messages based on a so-called “offer/answer” model.

The use of lines not prescribed here is not guaranteed.

5.3.1.1. Multipart MIME body (offer or answer)

When a multipart/mixed MIME body is received, a 415 response is sent with an Accept header containing only the supported types.

5.3.1.2. SDP with multiple m= lines (offer)

When an SDP with multiple m= lines is received, an answer MUST be sent back in which the port number is set to 0 for all the m= lines except those that can be handled.

5.3.1.3. Receiving multiple payload types (answer)

When an offer is transmitted containing multiple compatible payload type values as payload types in an m= line, an answer may be received containing multiple payload type values in the m= line. This signifies that it is possible to freely switch between multiple payload types during a single session, so when switching is not possible a re-INVITE request or UPDATE request MUST be issued to re-offer an SDP containing only the payload type value that is actually desired to be used.

5.4. Session modification

When session modification is allowed by agreement between providers, modification of the a= line (sendonly, recvonly, inactive) is permitted, but this might be ignored when a provider is unable to support a requested session modification. Modification of the c= and m= lines is basically not possible.

Although session modifications can be requested, a session request may elicit a 488 error response. In this case, the recipient of the session modification request should not disconnect the call on the basis of the modification request rejection. Even the side that requested the session modification should not automatically disconnect the call if the modification request is rejected. In cases where a call is disconnected on the basis of a rejected modification request, the session should continue unless a BYE request is transmitted to explicitly disconnect the call.

When a provider’s network rejects a session modification that has been requested of it, it should issue a 488 error response.

5.5. Guidance/talkie services

Guidance/talkie services may be provided by the provider’s SIP network that initiates a call or by the provider’s SIP network that receives a call.

5.5.1. Provision of guidance/talkie services from the receiving provider’s SIP network

It is conceivable that guidance/talkie services might be provided from the receiving provider’s SIP network depending on the results of an early dialog or confirmed dialog.

Guidance/talkie services provided from the receiving provider’s SIP network on the basis of an early dialog are implemented by adding SDP information inside a 18X response. With regard to receiving provider’s SIP network, from the viewpoint of preventing illegal calls in the early dialog, the SDP information in the 18X response manages the content of audio signals included in the RTP in the receiving provider’s SIP network, and the SDP information can only be set and transmitted when this content can be guaranteed, while this response is not transparently forwarded when the SDP is set inside a 18X response from the called terminal.

Similarly, guidance/talkie services provided in a confirmed dialog from the receiving provider’s SIP network are treated as normally connected calls (successful calls) at the calling provider’s side. The status codes used for this purpose should be agreed upon between the connecting providers.

5.5.2. Provision of guidance/talkie services from the calling provider’s SIP network

To provide guidance/talkie services, the originating SIP network MAY use the status codes of responses obtained from the terminating SIP network. When the receiving provider’s SIP network sends back a response including a status code used in guidance/talkie services, the contents of this response must be guaranteed to avoid erroneous connections to guidance/talkie services. The status codes that are used should be agreed upon between the connecting providers.

Annex a. Provisions against congestion

a.1. Basic rule

When a maximum number of simultaneous connections of sessions has been agreed upon between providers, this is controlled by a bidirectional session reservation function.

a.2. Controlling traffic with a session reservation function

(1) The acquisition of sessions can be permitted or prohibited under the following conditions 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):

Table a/JJ-90.25: 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 b. Connections for RTP audio sent out from the network before call completion

b.1 Purpose of this annex

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

Since it is possible to send out RTP audio from the terminal in connections between provider's SIP networks when the called user terminal is not controlled by completion of the network, path connections are sometimes prohibited before normal call completion, 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 completion.

This annex states the requirements that providers' SIP networks must satisfy to allow network-originated RTP audio to be connected to the caller before call completion via a connection interface based on the provisions of this standard.

b.2 A model of network-originated RTP audio

A connection model of a provider's SIP network related to network-originated RTP audio is shown in Fig. b.

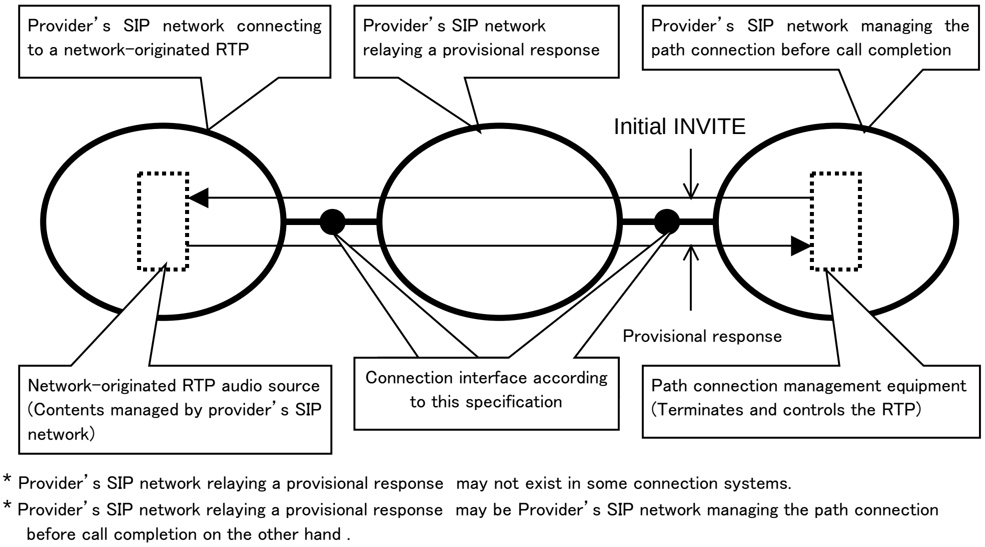

Provider's SIP network connecting to a network-originated RTP
Provider's SIP network relaying a provisional response
Provider's SIP network managing the path connection before call completion
Initial INVITE
Provisional response
Network-originated RTP audio source (Contents managed by provider's SIP network)
Connection interface according to this specification
Path connection management equipment (Terminates and controls the RTP)
* Provider's SIP network relaying a provisional response may not exist in some connection systems.
* Provider's SIP network relaying a provisional response may be Provider's SIP network managing the path connection before call completion on the other hand .

Fig. b/JJ-90.25: Connection model of a provider's SIP network related to network-originated RTP audio

The classes of providers' SIP networks 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, a single provider's SIP network must be capable of undertaking multiple roles simultaneously, and the roles themselves may be omitted if not required.

<Provider's SIP network connecting to a network-originated RTP>

A provider's SIP network that connects to a network-managed RTP audio source before call completion with regard to an Initial INVITE request received via a connection interface conforming to this standard. Responsible for the content of the audio source connected before call completion.

In practice, this corresponds to a provider's SIP network that performs connections according to conditions by preparing network-originated announcements such as congestion talkies.

<Provider's SIP network that relays provisional responses>

A provider's SIP network that transmits a corresponding Initial INVITE request from a connection interface according to this standard in response to a call where an Initial INVITE request is received from a connection interface according to this standard.

<Provider's SIP network that manages path connections before call completion>

A provider's SIP network that manages a call where an Initial INVITE request is received from a connection interface according to this standard so that no audio path is connected from the callee to the caller before call completion. A provider's SIP network that manages path connections before call completion must manage equipment that terminates RTP voice traffic from the callee 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.

b.3 Overview of behaviours relating to network-originated RTP audio

This section shows the behavioral provisions required of a providers' SIP networks that have each of the roles of the behaviors of providers' SIP networks in relation to network-originated RTP audio. The provider's SIP network behaviors mentioned here are not applied to all the calls handled by a provider's SIP network, 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.

b.3.1 Behaviours of a provider's SIP network connected to network-originated RTP

In Table 4-4: "List of SIP responses to INVITE requests" (Section 4.9), the following note is made in relation to the 180 (Ringing) and 183 (Session Progress) responses:

> A provider's SIP network that transmits a response can send additional SDP information only when the contents of the audio included in the RTP sent out to the provider that receives the response can be managed and guaranteed.

Accordingly, when a provider's SIP network that has received an Initial INVITE request via an interface conforming to this standard establishes a network-originated RTP audio connection before call completion, an SDP must be included in the 180 (Ringing) or 183 (Session Progress) response sent out in order to establish the RTP connection.

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 behaviors must be taken with messages received from such an entity.[2]

[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 provider.

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

(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 callee is not transferred to the caller.

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 a provider's SIP network 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 callee is not made aware of the address and port information included in the SDP included in the received Initial INVITE request[3]

b.3.2 Behaviours of a provider's SIP network that relays provisional responses

In cases where a provider's SIP network receives an Initial INVITE request via an interface conforming to this standard, and a corresponding Initial INVITE request is sent via an interface conforming to this standard, 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 the reception of corresponding response and is sent out via the interface must include an SDP.

Note that a provider's SIP network that relays a provisional response may at the same time be a provider's SIP network that manages path connections before call completion.

b.3.3 Behaviours of a provider's SIP network that manages path connections before call completion

When a provider's SIP network that has to prohibit audio path connections from callee users before call completion 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 standard, it must judge that it contains no audio that is unsuitable for connection before call completion, and establish a path connection from the callee to the caller.

Annex c Unallocated (unassigned) number talkie

c.1 Purpose of this annex

A Unallocated (unassigned) number talkie is an example of a guidance/talkie service provided from a originating SIP network when establishing an interconnection between provider's SIP networks. This annex discusses the functions and behaviors of a provider's SIP network that are required when providing a unallocated (unassigned) number talkie service.

c.2 Method for providing a unallocated (unassigned) number talkie service

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

- The unallocated (unassigned) number talkie issues a response indicating the unallocated number to the originating SIP network, and a connection to the unallocated (unassigned) number talkie is established by the

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

caller

- When the terminating SIP network is unable to guarantee the notifying of unallocated numbers, it notifies a status other than “unallocated number” in order to avoid a talkie connection at the caller.

c.2.1 Required functions of the terminating SIP network

When an unallocated number occurs, the terminating SIP network sends back a 404 response with a Reason header. When a 404 response containing a Reason header is received from the called terminal, it must be kept in mind that a response must be sent back to the originating SIP network after judging whether or not it can be guaranteed as the terminating SIP network.

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 text="unallocated number" is optional)

c.2.2 Required functions of a originating SIP network

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

Appendix i. Test schemes between interconnecting providers

It must be possible to perform audio connection tests by preparing terminals that can send out audio signal (e.g., audible tones) as automatic responses in each connection route.

Note that providers are free to set any test numbers to be used for this purpose. The connection routes (each server, each line, etc.) should be prescribed by agreement between providers.

Appendix ii. Connection sequences

ii.1. Basic concept

(1) This appendix prescribes the connection sequences to be employed between the caller network and callee network.

(2) The sequence between a terminal and the network is shown by dotted lines to assist the understanding of the sequence used between the networks.

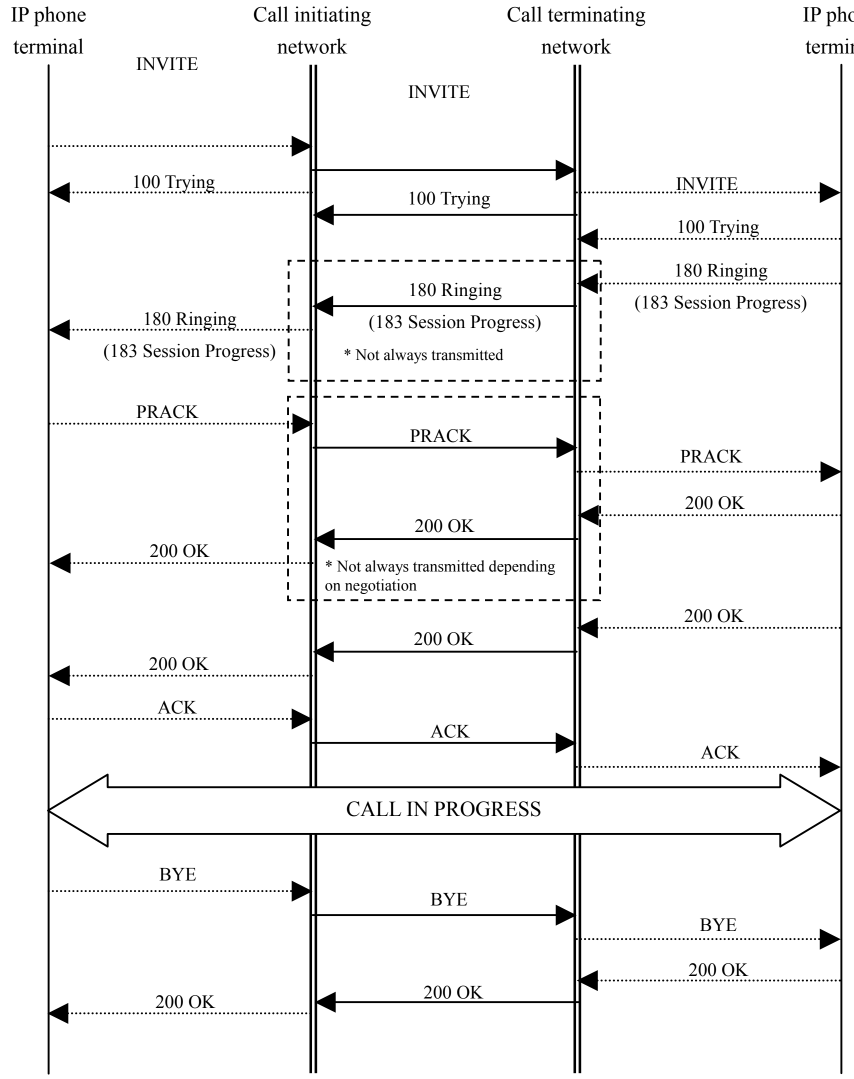
(3) Since unsuccessful and seminormal sequences exist in various different patterns, only partial examples are shown here.

ii.2. Various connection sequences

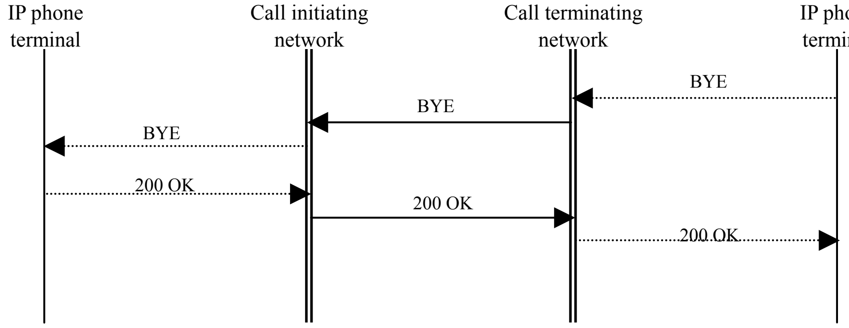
General connection sequences are shown here.

No	Sequence classification
1	Basic connection
2	Basic connection (abandoned during ringing)
3	Basic connection (unsuccessful example)
4	Basic connection (unsuccessful talkie example)
5	Basic connection (unallocated (unassigned) number talkie example)

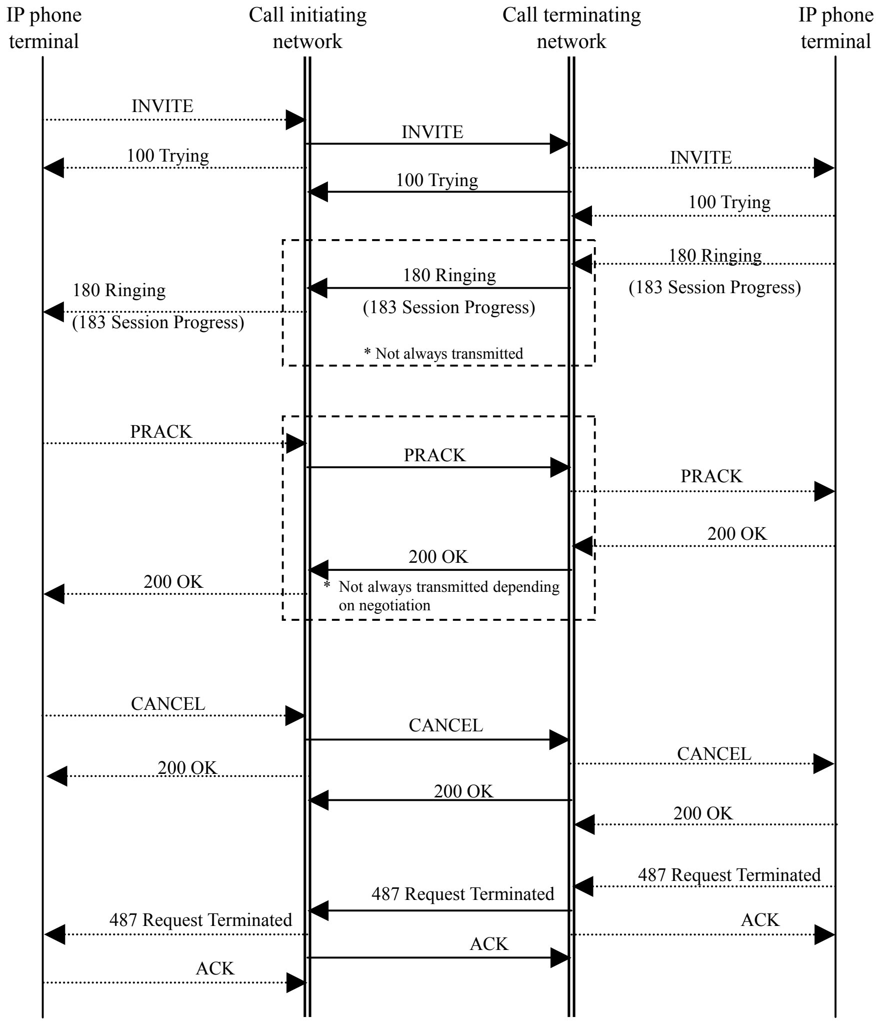
No	1	Class		Category	Basic connection



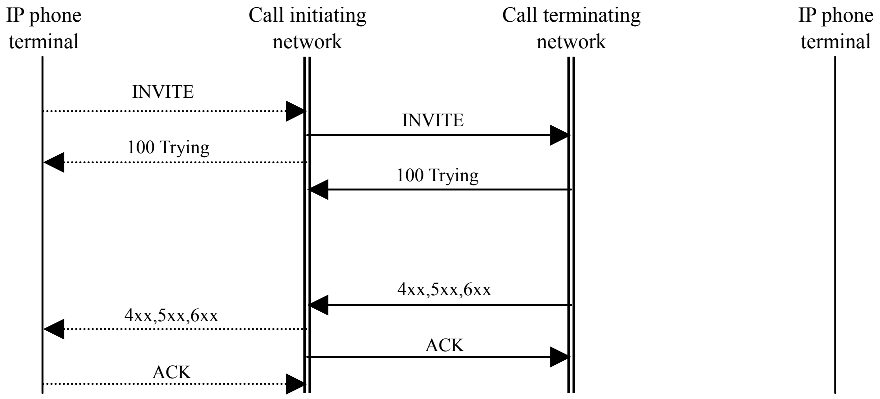
Disconnection sequence at call terminating end

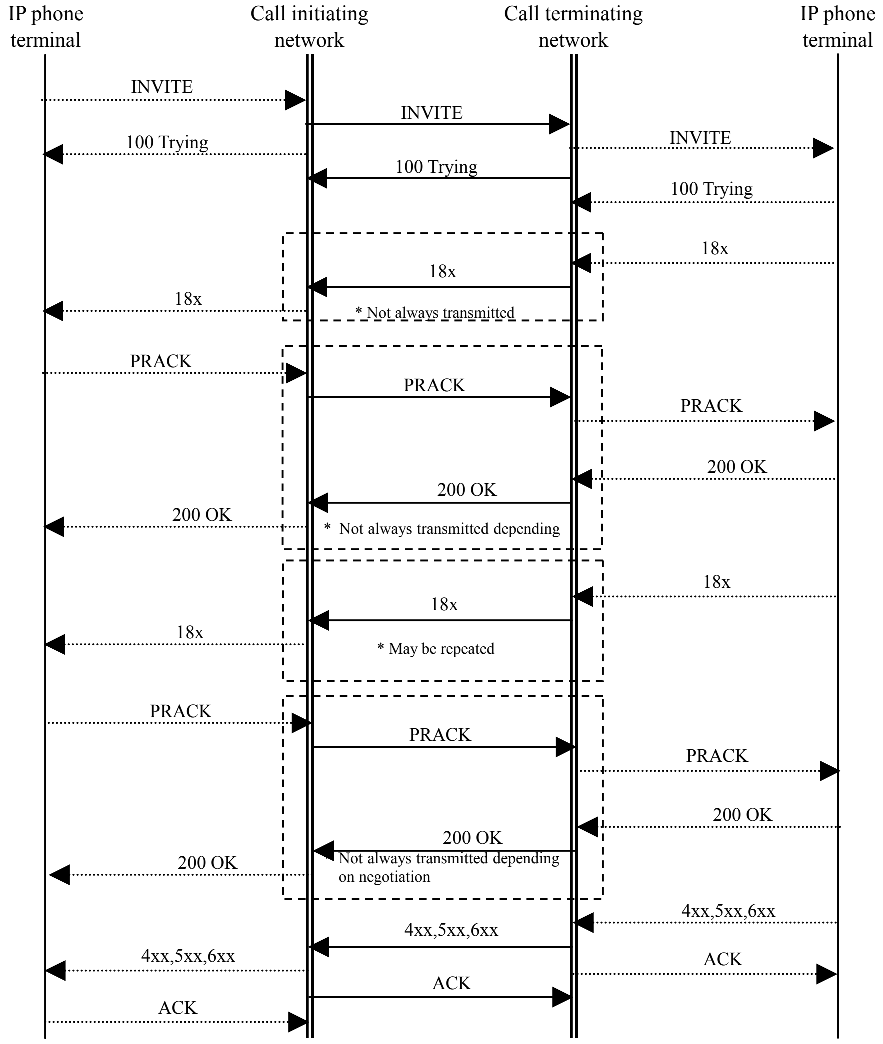


No	2	Class		Category	Basic connection (abandoned during ringing)

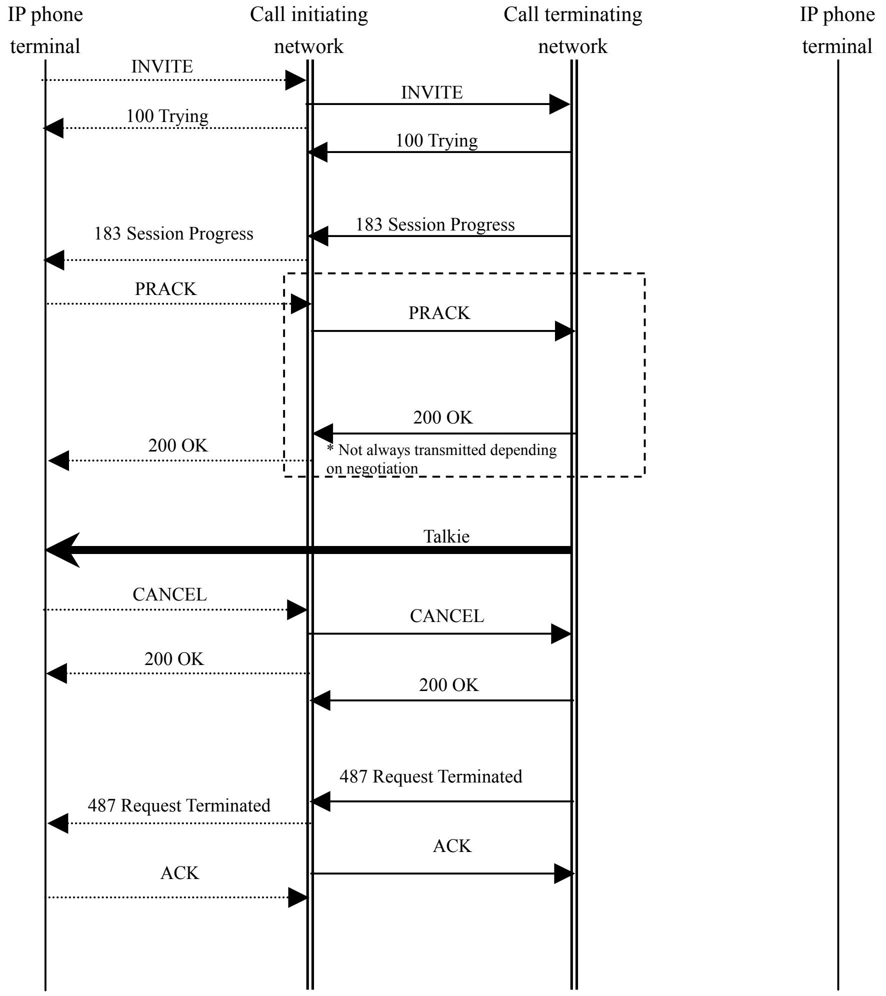


No	3	Class		Category	Basic connection (unsuccessful example)

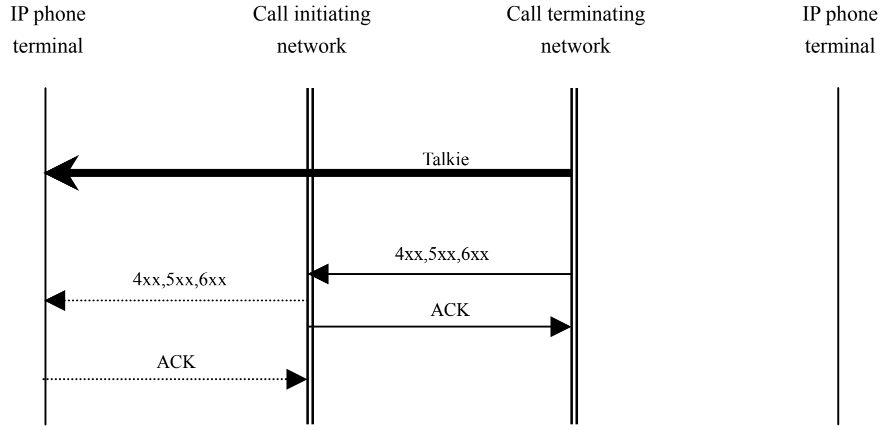




No	4	Class		Category	Basic connection (unsuccessful talkie example)

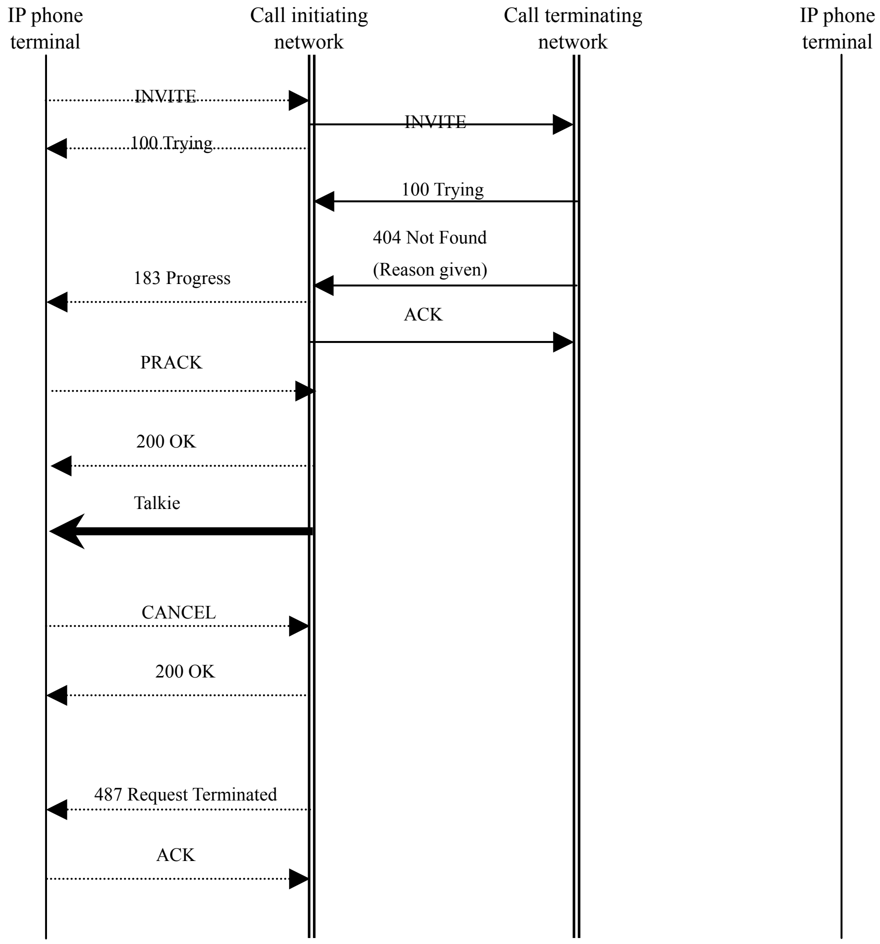


Disconnection sequence at call terminating end

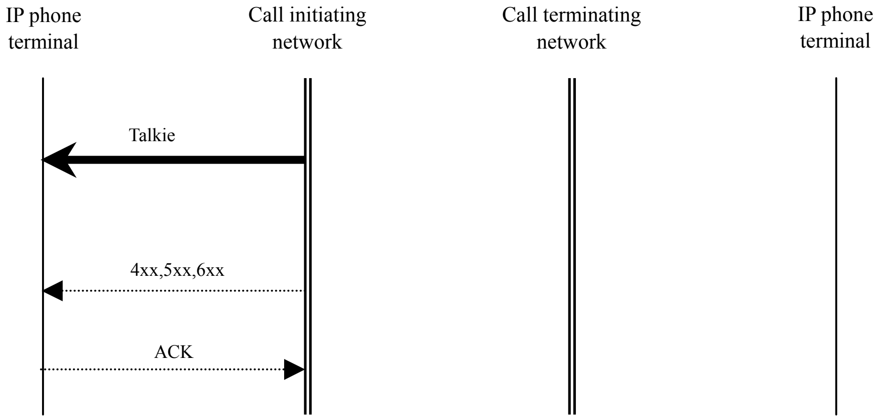


No	5	Class		Category	Basic connection (unallocated (unassigned) number talkie example)

Disconnection sequence at call initiating end



Disconnection sequence at call terminating end



Appendix iii.   Call information

Billing information and the like must be obtained by a technique such as CDR. The detailed nature of the call information should be determined based on agreement between providers.

It is essential that the following items of information are acquired.

- **Caller number:** The TEL-URI part of the P-Asserted-Identity header in an INVITE request
- **Called number:** The Request-URI part of an INVITE request
- **Call start time:** For a successful call, the call initiator should record the reception time of the 200 (OK) response to the Initial INVITE request, and the call recipient should record the transmission time of the 200 (OK) response. For an unsuccessful call, the caller should record the transmission time of the Initial INVITE request, and the callee should record the reception time of this Initial INVITE request.
- **Call end time:** For a successful call, the transmission time of the BYE request should be recorded by the side that hangs up first, and the time at which this request was received should be recorded by the side that hangs up second. For an unsuccessful call, the reception time of the 4XX/5XX/6XX response should be recorded by the caller, and the transmission time of this response should be recorded by the callee.
- **Response code:** The Status-Code part received in the error response.