TTC STANDARDS

JJ-22.01

Technical Specifications on Inter-connection Interface between Private SIP Networks

Version 1.2

June 9, 2016

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

The copyright of this document is owned by the Telecommunication Technology Committee.
It is prohibited to duplicate, reprint, alter, or diversify all or part of the content, or deliver or distribute it through network without approval of the Telecommunication Technology Committee.

Table of Contents

<Reference> 5
1. Overview 7
1.1. Scope of this standard 7
1.2. Purpose and provisions of this standard 7
1.3. Contents of this standard 7
1.4. Terms 8
2. Connection Configurations 8
2.1. Basic connection configuration 8
2.2. Scope of this standard 8
3. Numbering System 8
3.1. Basic callee number configuration 8
3.1.1. user portion 8
3.1.2. hostport portion 9
3.1.3. Option URI parameter portion 9
3.2. Function for the dialing number of an originating server 9
4. Signalling System 9
4.1. Signalling system between servers in an operating agency 9
4.1.1. Other items required for connections 9
4.2. Network layer interface 9
4.3. Transport layer interface 9
4.4. Call processing signal specifications 9
4.5. Requirements for media streams 10
4.6. SIP messages 10
4.6.1. Maximum permissible lengths of elements in a message 10
4.7. Definitions of types in table 10
4.8. Request message types 11
4.9. Response messages 11
4.10. SIP messages and header information 18
4.10.1. ACK 18
4.10.2. BYE 18
4.10.3. CANCEL 20
4.10.4. Initial INVITE 22
4.10.5. re-INVITE 24
4.10.6. PRACK 27
4.10.7. UPDATE 28
4.11. Header information elements (header parameters) in each message 31
4.11.1. Basic format 31
4.11.2. Request-Line 31
4.11.3. Status-Line 31
4.11.4. Allow 32
4.11.5. Content-Type 32

4.11.6. CSeq 33
4.11.7. From 33
4.11.8. P-Asserted-Identity 33
4.11.9. Privacy 34
4.11.10. Record-Route 34
4.11.11. Route 35
4.11.12. Session-Expires 35
4.11.13. To 36
4.11.14. Via 36
4.12. URI specification system (addr-spec) 37
4.13. Other signal provisions 38
4.13.1. Handling of un-specified signals 38
4.13.2. Handling of calling line identifications 38
5. Connection conditions 40
5.1. Session timer 40
5.2. 100rel 40
5.3. Conditions for using bearers 40
5.3.1. SDP format 40
5.4. Session changes 41
5.5. Guidance/talkie services 41
5.5.1. Supply of guidance/talkie services from inside a called SIP private network 41
5.5.2. Supply of guidance/talkie services from an originating private SIP network 41
Annex a. Congestion Provisions 42
a.1. Basic rules 42
a.2. Control with a session reservation function 42
Annex b. Connections for RTP Audio Sent out from the Network before Call Completion 43
b.1. Purpose of this annex 43
b.2. Model for RTP audio sent out from the network 43
b.3. General description of the operations for RTP audio sent out from the network 44
b.3.1. Operation of the private SIP network that connects to RTP sent from the network 44
b.3.2. Operation of the private SIP network that relays temporary responses 45
b.3.3. Operation of the private SIP network that manages path connections before call completion 45

<Reference>

1. Introduction

The Private Network Interface Sub-Working Group of the Private Network Special Committee has implemented the standardization of the IP protocol based on private networks (circuit-switched networks) between PBXs (Private Branch eXchanges) and Qsig (Signalling information flows at the Q reference point). Considering recent trends in markets and international recommendations, it is necessary to study VoIP (Voice over Internet Protocol) technology based on SIP (Session Initiation Protocol) within private networks. It has been decided to implement standardization by focusing on the latest technical trends in the new technical field mentioned above and the status of the responses of carriers to them.

This standard makes it possible to promptly accommodate unique, additional services required in an operating agency by newly defining the SIP protocol in the operating agency.

It intends to increase connectivity by defining a light protocol for use in an operating agency, different from the one used in a carrier.

Because of the background and reason stated above, this standard summarizes technical specifications on inter-connection interface between private SIP networks.

2. Revision History

Version	Date of establishment	Description
First Version	August 24, 2006	Established.
Version 1.1	December 6,2007	Revision.
Version 1.2	June 9,2016	Revision (correction of Figure2-1)

3. Miscellaneous

(1) Recommendations, standards, etc., referenced

TTC standard: JJ-90.25 Technical Specifications on Inter-Connection Interface between Managed Carrier SIP Networks 1.1 Edition, August 25, 2005

* The contents of the number in [ ] in the “reference” of the each table is quoted from the JJ-90.25.

-Quoted Document-

[1] “Session Initiation Protocol”, JF-IETF-RFC3261 1st edition, The Telecommunication Technology Committee, 2005.6.

[2] “Reliability of Provisional Responses in SIP”, JF-IETF-RFC3262 1st edition, The Telecommunication Technology Committee, 2005.6.

[3] “An Offer/Answer model with SDP”, JF-IETF-RFC3264 1st edition, The Telecommunication Technology Committee, 2005.6.

[4] “Session Description Protocol”, JF-IETF-RFC2327, The Telecommunication Technology Committee, 2005.6.

[5] “A Privacy Mechanism for the Session Initiation Protocol (SIP)”, JF-IETF-RFC3323, The

Telecommunication Technology Committee, 2005.6.

[6] “Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks”, JF-IETF-RFC3325, The Telecommunication Technology Committee, 2005.6.

[7] “The tel URI for Telephone Numbers”, JF-IETF-RFC3966, The Telecommunication Technology Committee, 2005.6.

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

[9] “Technical Specification on SIP to ISUP Interworking”, JF-IETF-RFC3398, TTC, 2006.6.

[10] “Technical Specification of the Framework on Provider’s SIP Network”, JJ-90.21, The Telecommunication Technology Committee, 2005.6.

[11] “Technical Specification on Network Asserted User Identity Information Transferring through Provider’s SIP Networks”, JJ-90.22, The Telecommunication Technology Committee, 2005.6.

[12] “Inter-Carrier Interface based on ISUP”, JJ-90.10 6th edition, The Telecommunication Technology Committee, 2003.4.

[13] “The Session Initiation Protocol UPDATE Method”, JF-IETF-RFC3311, The Telecommunication Technology Committee, 2005.6.

[14] “The Reason Header Field for the Session Initiation Protocol (SIP)”, JF-IETF-RFC3326, The Telecommunication Technology Committee, 2005.6.

[15] “Session Timers in the Session Initiation Protocol (SIP)”, JF-IETF-RFC4028, The Telecommunication Technology Committee, 2005.8.

[16] “Technical Report on Session Initiation Protocol (SIP)”, TR-1007 1st edition 2003.3, The Telecommunication Technology Committee, 2003.3.

(2) Associations with other domestic standards

No associations with other domestic standards.

4. Organizational Unit Preparing Standards

First Version: Private Network Special Committee

Version 1.1: Private Network Special Committee

Version 1.2: Enterprise Network Working Group

1. Overview

1.1. Scope of this standard

This standard provides the connection interface specifications necessary for connecting a voice call by specifying the party to be connected with a private number, by applying a connection interface (interface C) between inter-connected private SIP networks in a network connection architecture specified in JJ-20.00.

Also, this standard is intended to ensure that in inter-connected private SIP networks, management in the private networks is facilitated while high interconnectivity is maintained, on the assumption that the private SIP networks conform to the provisions of this standard.

1.2. Purpose and provisions of this standard

This standard specifies the connection interface to be applied to interface C, and covers the items necessary for interconnections including items for SIP and SDP (Session Description Protocol). It aims to achieve the following purposes:

– Produce an implementable standard by ensuring that the provisions for connection conditions are uniquely interpreted.
– Produce a standard that can be applied universally to both operating agencies in interconnections to private SIP networks.
– Produce a standard that contains the items necessary for making smooth interconnections in connection interfaces as connection conditions other than signal conditions.

To achieve these purposes, this standard provides the provisions below.

- Items for the use of SIP specified in JF-IETF-RFC3261 and its extended provisions as call control signal conditions
- Values defined in RFC1890 as media conditions
- Other items for operations for call connections

Items associated with operating conditions and others for interconnections are described in the appendix of this standard as reference.

1.3. Contents of this standard

Main body: The main body of this standard specifies the interfaces for interconnections with private SIP networks, and mainly specifies the items below.

- Connection model (Chapter 2) for making interconnections.
- Numbering method (Chapter 3) and signalling system (Chapter 4) of the SIP signals to be transferred between private SIP networks.
- Function expansions and SDP format (Chapter 5) necessary for making interconnections.

Annexes: Annex a specifies the control of session reservation during congestion if the upper limit on the number of calls that can be connected between private SIP networks is managed, Annex b specifies the requirements necessary for an RTP sent out by a network before call completion (Real-time Transport Protocol) to be connected to the calling party, and Annex c specifies the requirements for connecting to an unallocated number talkie.

Appendix : For reference, a connection sequence to be implemented between servers in an operating agency is included (Appendix ii).

1.4. Terms

The terms used in this standard shall conform to TS survey material.

2. Connection Configurations

2.1. Basic connection configuration

This standard describes the conditions for connection interfaces to managed private SIP networks that are applicable to interface C specified in the private SIP network interconnection model shown in.Figure2-1.

In this standard, a private SIP network that has an interface that can observe the provisions for this interface is called a "managed private SIP network". It is assumed in the remainder of this standard that the term private SIP network refers to a "managed private SIP network".

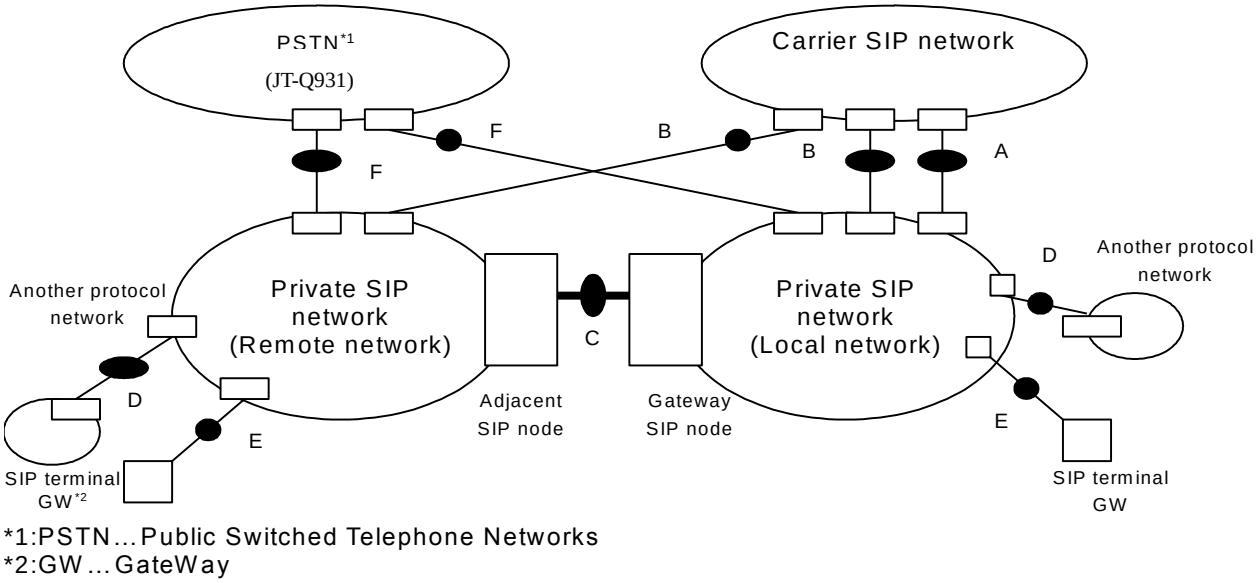


Figure 2-1/JJ-22.01 Private SIP network interconnection model

2.2. Scope of this standard

The scope of this standard is such that provisions for inter-server linkages (C) are defined.

3. Numbering System

3.1. Basic callee number configuration

In the Request-URI (Uniform Resource Identifier) of an Initial INVITE request, a callee number shall be set as information for use in the routing of a call between servers.

The setting in the Request-URI of an Initial INVITE request shall be a SIP-URI, and shall be specified as below.

3.1.1. user portion

In the user part of the SIP-URI to be set in the Request-URI of an Initial INVITE request, set a callee number.

As a basic format, use the format of the global-phone-number of the tel URL specified in JF-IETF-RFC3966. If the global-phone-number contains a parameter portion (portion subsequent to a semicolon (;)), routing is performed based on the destination number even if the contents of the portion cannot be recognized.

3.1.2. hostport portion

The hostport part of the SIP-URI to be set in the Request-URI of an Initial INVITE request shall be a domain name or host name (including that in IP address format) specified in the SIP network defined in an operating agency. Specific information to be set shall be determined with the number defined in the operating agency.

3.1.3. Option URI parameter portion

The option URI parameter in the SIP-URI to be set in the Request-URI of an Initial INVITE request shall be ignored during processing.

3.2. Function for the dialing number of an originating server

An originating server shall enable registration of the number of effective receive digits (in the range of the minimum number of receive digits to the maximum number of receive digits) in the userinfo portion of an effective Request-URI and, if the minimum number of digits is not satisfied, performs a clearing process in the originating server network. The numbering plan (for example, minimum number of receive digits and maximum number of receive digits) shall be decided through consultation between servers.

4. Signalling System

4.1. Signalling system between servers in an operating agency

For the signalling system between servers in an operating agency, the SIP v2.0 (JF-IETF-RFC3261) signalling system protocol is applied on the IP Version4 (IPv4) network.

The system for the connection line for transferring SIP signals, including the physical layer, data link layer, and band speed, are outside the scope of this standard. In interconnection case, decision shall be stipulated through consultation between servers in the operating agency.

4.1.1. Other items required for connections

The system for the connection line for transferring media streams is the outside the scope of this standard. In interconnections case, decisions shall be stipulated through consultation between servers in the operating agency.

4.2. Network layer interface

The network layer interface for sending and receiving of SIP signals shall conform to IPv4.

4.3. Transport layer interface

The transport layer interface for sending and receiving of SIP signals shall conform to UDP.

It is recommended that the receive port number for SIP signals is 5060. However, if a port number is explicitly indicated by Via header or Record-Route header on the signal of the destination side, this number shall be followed by indicated one.

And if different port numbers is used, in view of the facility and other factors, decision shall be stipulated between servers in the operating agency.

4.4. Call processing signal specifications

The contents are not covered by this standard shall conform to the reference document.

The contents are re-specified in this standard, the applicable provisions of this standard shall apply.

4.5. Requirements for media streams

Requirements are specified in Section 5.3.

4.6. SIP messages

This section defines each of the information elements (message, header, and parameters in the header) of SIP messages in the interconnection between private SIP networks.

4.6.1. Maximum permissible lengths of elements in a message

Maximum permissible lengths of elements in a SIP message are listed inTable4-1.

Table 4-1/JJ-22.01 Maximum permissible lengths of elements

Element	Maximum permissible length
Maximum permissible length per a line	255 bytes
The number of Maximum permissible iterations in the same header	5 lines (Note 1)
Maximum permissible length in the message body	1000 bytes
All message length	1300 bytes or less (Note 2)
Note 1: The number of Record-Route elements must be 5 entries for a request and 10 entries for a response. The number of Route and Via elements must be 5 entries. Note 2: Shall conform to carrier SIP recommendations.	

4.7. Definitions of types in table

The definitions of the specified types contained in each table that are used universally are listed in Table4-2.

Table 4-2/JJ-22.01 Definitions of specified types in the table

Code	Code name	Sender	Receiver
M	Mandatory	Need to have a capability that follows referenced provisions.	Need to have a capability that follows referenced provisions. Do not continue processing if it cannot get necessary informations. (It executes a disconnection and release process appropriately.) Execute default values if they have been decided.
O	Optional	The sender may have a capability, but it does not assure the intended capability.	Execute a processing expected by the sender, if it can. Ignore the received data and continue processing If it cannot execute the processing expected by the sender.
X	Prohibited (excluded)	Must not have the capability.	Send a return error or ignore it.
c <integer>	Conditional	It depends on the condition <integer> to have the capability. Must not have the capability without a condition.	Need to execute processing by the condition <integer>. Do not continue processing without a condition applied.
o<integer>	Qualified optional	It is exclusively selectable under the same conditions.	Execute processing by the condition <integer>.

4.8. Request message types

Request messages transferred between servers are listed in Table4-3.

Table 4-3/JJ-22.01 Supported request messages

Request signal	Reference	Specified type (Sender)	Specified type (Receiver)	Remarks
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 request		c3	c3	

c1: If "100rel" is set in "supported", it is "m". Otherwise it is "x". In addition, it needs to negotiate the assurance of "100rel" between servers in the operating agency.

c2: If UPDATE is used in a session update, it is "m". Otherwise it is "x". In addition, it needs to negotiate the assurance of "UPDATE" between servers in the operating agency.

c3: If it is used, it is "m". Otherwise it is "x". It basically cannot be used, but if it is used, it needs to negotiate the other request between servers in the operating agency, inclusive Allow or suppoted hedders negotiation. If it does not negotiate, the server in the operating agency that receives the request may send a 405 (Method Not Allowed) or 501 (Not Implemented) error response message to the server that sends the request.

4.9. Response messages

SIP response signals for the SIP requests in Table4-3 that are covered by this standard are listed below table.

SIP responses for other requests shall be decided through consultation between servers. About "o" in the "Type (Receiver)" column in the table, at least, process shall be executed a default value in each class (183 for 1xx and x00 for others).

Table 4-4/JJ-22.01 SIP response signals for the INVITE request (1/2)

SIP response signal			Recommended operation (Proposed)	Remarks
Type	Code	Phrase		
1xx	100	Trying	-	(Note 6)
	180	Ringing (Ringing)	-	(Note 1)
	181	Call Is Being Forwarded (The call is being forwarded.)	-	
	182	Queued (Placed in a queue.)	-	
	183	Session Progress (Session progress)	-	(Note 2)
	Other			
2xx	200	OK	-	(Note 3)
	Other			
3xx	300	Multiple Choices (There are multiple choices.)	-	
	301	Moved Permanently (Moved permanently.)	-	
	302	Moved Temporarily (Moved temporarily.)	-	
	305	Use Proxy (Use a proxy.)	-	
	380	Alternative Service (Alternative service)	-	
	Other			
4xx	400	Bad Request (Invalid request)	Barring/connection reject	
	401	Unauthorized (Unauthorized)	Barring/connection reject	
	402	Payment Required (Payment is required.)	Barring/connection reject	
	403	Forbidden (Forbidden.)	Barring/connection reject	
	404	Not Found (Not found.)	Barring/connection reject	
	405	Method Not Allowed (The method is not allowed.)	Barring/connection reject	
	406	Not Acceptable (Not acceptable.)	Barring/connection reject	
	407	Proxy Authentication Required (Proxy authentication is required.)	Barring/connection reject	
	408	Request Timeout (The request times out.)	Barring/connection reject	
	410	Gone (Resources no longer exist.)	Barring/connection reject	
	413	Request Entity Too Large (The request entity is too large.)	Barring/connection reject	
	414	Request-URI Too Long (The Request-URI is too long.)	Barring/connection reject	
	415	Unsupported Media Type (Unsupported media type)	Barring/connection reject	
	416	Unsupported URI Scheme (Unsupported URI scheme)	Barring/connection reject	
	420	Bad Extension (Invalid extension)	Barring/connection reject	
	421	Extension Required (Extension is required.)	Barring/connection reject	
	422	Session Interval Too Small (Session interval is too small)	Barring/connection reject	
	423	Interval Too Brief (The interval is too brief.)	Barring/connection reject	
	480	Temporarily Unavailable (Temporarily unavailable.)	Busy/failure/connection reject	
	481	Call/Transaction Does Not Exist (The calling or transaction does not exist.)	Barring/connection reject	
	482	Loop Detected (A loop was detected.)	Barring/connection reject	
	483	Too Many Hops (There are too many hops.)	Barring/connection reject	
	484	Address Incomplete (The address is incomplete.)	Barring/connection reject	
	485	Ambiguous (Ambiguous)	Barring/connection reject	
	486	Busy Here (Busy here.)	Busy	(Note 4)
	487	Request Terminated (The request was terminated.)	Barring/connection reject	(Note 5)
	488	Not Acceptable Here (Not acceptable here.)	Barring/connection reject	
	491	Request Pending (The request is pending.)	Barring/connection reject	
	493	Undecipherable (Undecipherable)	Barring/connection reject	
	Other		Barring/connection reject	

Table 4-4/JJ-22.01 SIP response signals for the INVITE request (2/2)

5xx	500	Server Internal Error (Internal server error)	Barring/connection reject	
	501	Not Implemented (Not implemented.)	Barring/connection reject	
	502	Bad Gateway (Invalid gateway)	Barring/connection reject	
	503	Service Unavailable (The service is unavailable.)	Barring/connection reject	
	504	Server Time-out (Server time-out)	Barring/connection reject	
	505	Version Not Supported (The SIP version is not supported.)	Barring/connection reject	
	513	Message Too Large (The message is too large.)	Barring/connection reject	
	Other		Barring/connection reject	
6xx	600	Busy Everywhere (Busy everywhere.)	Busy/congestion/barring	
	603	Decline (Decline)	Barring/connection reject	
	604	Does Not Exist Anywhere (Does not exist anywhere.)	Barring/connection reject	
	606	Not Acceptable (Not acceptable.)	Barring/connection reject	
	Other		Barring/connection reject	

Note 1: Used for indication of the calling state. When the sip server that sends a response can manage and assure the audio contents of the RTP, this server can send response that contains a message body with the SDP.

Note 2: Used for establishment of early media after sending SDP to the sender sends INVITE. When the SIP network in the operating agency that is to send a response can manage and assure the audio contents of the RTP, this network can send response that contains a message body with SDP.

Note 3: Used for the normal response.

Note 4: Used for the busy state when the user is in use. And after that, the receiver disconnects the call.

Note 5: Used for the call disconnection during calling process. And after that, The sender and the receiver disconnect the call.

Note 6: If no 100 responce of INVITE is received, the sender re-sends INVITE after waiting 500 ms that is a recommendation value.

Table 4-5/JJ-22.01 SIP response signals for the CANCEL, BYE, and PRACK requests (1/2)

SIP response signal			Reference	Type (Sender)	Type (Receiver)	Remarks
Type	Code	Phrase				
1xx	100	Trying	[1][2]	x	x	
	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][16]	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	
	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	

Table 4-5/JJ-22.01 SIP response signals for CANCEL, BYE, and PRACK requests (2/2)

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 for the normal response.
c1: If PRACK is used, it is "x". Otherwise it is "m". When a dialog finishes establishing, the case that PRACK is available or not is basically decided by Allow hedder.

Table 4-6/JJ-22.01 SIP response signals for UPDATE (1/2)

SIP response signal			Reference	Type (Sender)	Type (Receiver)	Remarks
Type	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)
	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][16]	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	
	493	Undecipherable	[1][4]	o	o	
	Other		[1][4]	o	o	

Table 4-6/JJ-22.01 SIP response signals for UPDATE (2/2)

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 for the normal response.
c1: if draft-ietf-session-timer is used, it is "m". Otherwise it is "x".
c2: if UPDATE is used, it is "x". Otherwise it is "m". When a dialog finishes establishing, the case that UPDATE is available or not is basically decided by Allow hedder.

4.10. SIP messages and header information

This section specifies the settings of header information in request messages and response messages for individual SIP methods.

4.10.1. ACK

This message is transferred in the forward direction if the last response to an INVITE request is obtained.

SDP implementation shall be decided through consultation between servers because this is an implement matter.

4.10.1.1. Request message

Table 4-7/JJ-22.01 ACK request message

Message type: Request

Method: ACK

Information element	Reference	Type (Sender)	Type (Receiver)	Remarks
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-Authorication	[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 "0" because the message body is not used.
Note 2: Even if it is set, the destination network may not be able to interpret its meaning.
c1: "m" if there is a route set established in the INVITE response and "x" otherwise.

4.10.1.2. Response message

No response message to the ACK request message is specified.

4.10.2. BYE

This message is used for clearing after a requested call is started (after early dialing or a dialog is established).

4.10.2.1. Request message

Table 4-8/JJ-22.01 BYE request message

Message type: Request

Method: BYE

Information element	Reference	Specified type (Sender)	Specified type (Receiver)	Remarks
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 "0" because the message body is not used.
c1: "m" if the destination's private SIP network entry exists in the route set during transmission and "x" otherwise.

4.10.2.2. Response message

Table 4-9/JJ-22.01 BYE response message

Message type: Response
Method: BYE

Information element	Reference	Application	Specified type (Sender)	Specified type (Receiver)	Remarks
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 to clear a requested call by the calling party before it is established.

4.10.3.1. Request message

Table 4-10/JJ-22.01 CANCEL request message

Message type: Request

Method: CANCEL

Information element	Reference	Specified type (Sender)	Specified type (Receiver)	Remarks
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 "0".				

4.10.3.2. Response message

Table 4-11/JJ-22.01 CANCEL response message

Message type: Response

Method: CANCEL

Information element	Reference	Application	Specified type (Sender)	Specified type (Receiver)	Remarks
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 "0".					

4.10.4. Initial INVITE

This message is used to start a dialog.

4.10.4.1. Request message

Table 4-12/JJ-22.01 Initial INVITE request message

Message type: Request

Method: INVITE

Information element	Reference	Specified type (Sender)	Specified type (Receiver)	Remarks
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	[16]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
Session-Expires	[16]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: A message body must be set.
c1: "m" if draft-ietf-session-timer is used, "o" otherwise.
c2: The option tag decided to be available through consultation between servers can be set. If an option tag does not decide available through consultation is set, a response is made with 420 (Bad Extension).
c3: "m" if draft-ietf-session-timer and 100rel are used and "o" otherwise.

4.10.4.2. Response message

Table 4-13/JJ-22.01 Initial INVITE response message (1/2)

Message type: Response

Method: INVITE

Information element	Reference	Application	Specified type (Sender)	Specified type (Receiver)	Remarks
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	
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	[16]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.	Note A:	c4	m	Note A: Used for interworking with a signalling system other than SIP.
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	
Rseq	[2]7.1	1xx	o	o	
Server	[1]20.35	All codes	o	o	
Session-Expires	[16]4.	2xx	c3	m	4.11.12

Table 4-13/JJ-22.01 Initial INVITE response message (2/2)

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: When 100rel is not supported, the temporary response may contain SDP information. Required for 200 (OK). For 100rel, however, if a temporary response with an acknowledge contains an SDP, 200 (OK) may not contain an SDP.

c1: "m" if an SDP is used for a response and "x" otherwise.
Whether there is an SDP in an INVITE shall be regarded as an implement matter.
c2: "m" if 100rel is used or "x" otherwise.
c3: "m" if draft-ietf-session-timer is used or "x" otherwise.
c4: "m" if the number is missing or "o" otherwise.

4.10.5. re-INVITE

This message is used to refresh a call (session timer) or to change the information set for a media stream during a dialog.

If the session refresh request transaction times out or generates a 408 (Request Timeout) or 481 (Call/Transaction Doe Not Exist) response,then the refresher SIP UA sends a BYE request as per Section 12.2.1.2 of JF-IETF-RFC3261. If the session refresh request does not generates 2xx and other than 408 or 481 response,it goes through procedure in accordance with the recepition of each response code in JF-IETF-RFC3261. However if the session refresh request generate 422 response,it operates in the same way as that when it receives a 422 response in an Initail-INVITE.

Alternatively,if the session refresh request transaction times out or generate 4xx response other than 422 response,the refresher SIP UA may,unless there is a clear indication from a user resource or a higher application,continue the session up to ten seconds before session timer expires,and then send a BYE request to that dialog and send a BUSY TONE to the user resource(or perform equivalent processing).

If the non-refresher SIP UA does not receive a session refresh request by 32 seconds before the session timer expires, or if a one-third of the session timer value is less than 32 seconds, by that time, the non-refresher SIP UA shall forcibly send a BYE request to that dialog at that point and send a BusyTone to the user resource (or perform equivalent processing). Alternatively, this operation may be performed by ten seconds before the session timer expires, or if a one-third of the session timer value is less than ten seconds, by that time.

4.10.5.1. Request message

Table 4-14/JJ-22.01 re-INVITE request message

Message type: Request

Method: INVITE

Information element	Reference	Specified type (Sender)	Specified type (Receiver)	Remarks
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	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	[16]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	[16]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	

Note 1: re-INVITE does not enable changing of the route set established with an Initial INIVTE.
c1: "m" when draft-ietf-session-timer is used or "x" otherwise.
c2: The option tag decided to be available through consultation between servers can be set. If an option tag does not decide available through consultation is set, a response is made with 420 (Bad Extension).
c3: "m" if a route set exists or "x" otherwise.

4.10.5.2. Response

Table 4-15/JJ-22.01 re-INVITE response message (1/2)

Message type: Response

Method: INVITE

Information element	Reference	Application	Specified type (Sender)	Specified type (Receiver)	Remarks
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	
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	[16]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	[16]4.	2xx	c1	m	4.11.12
Supported	[1]20.37	2xx	c1	m	

Table 4-15/JJ-22.01 re-INVITE response message (2/2)

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	2xx	m	m	(Note 1)

Note 1: Used to update the session timer or to change the information set for a media stream.
Note 2: Does not enable changing of the route set established with an Initial INIVTE.
c 1 : "m" when draft-ietf-session-timer is used or "x" otherwise.

4.10.6. PRACK

This message is used to supply a reliable temporary response message (100rel) in establishing a dialog.

4.10.6.1. Request message

Table 4-16/JJ-22.01 PRACK request message

Message type: Request

Method: PRACK

Information element	Reference	Specified type (Sender)	Specified type (Receiver)	Remarks
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
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" if a route set exists or "x" otherwise.
c2: "m" if it is decided to be settable through consultation between servers or "x" otherwise.

4.10.6.2. Response

Table 4-17/JJ-22.01 PRACK response message

Message type: Response

Method: PRACK

Information element	Reference	Application	Specified type (Sender)	Specified type (Receiver)	Remarks
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	
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: Used to change the information set for a media stream.
c1: "m" if it is decided to be settable through consultation between servers or "x" otherwise.

4.10.7. UPDATE

This message is used to refresh a call (Session-Timer) or to change the information set for a media stream during a dialog.

4.10.7.1. Request message

Table 4-18/JJ-22.01 UPDATE request message

Message type: Request

Method: UPDATE

Information element	Reference	Specified type (Sender)	Specified type (Receiver)	Remarks
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	[16]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	[16]4.	o	c4	4.11.12
Supported	[1]20.37	o	c4	
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: Does not enable changing of the route set established with an Initial INIVTE.
Note 2: Used to change the information set for a media stream.
c1: "m" if SDP is used for a response and "x" otherwise.
c2: Set it if an enhancement is requested by the network in the enterprise.
c3: "m" if a route set exists and "x" otherwise.
c4: "m" if draft-ietf-session-timer is used and "x" otherwise.

4.10.7.2. Response

Table 4-19/JJ-22.01 UPDATE response message (1/2)

Message type: Response

Method: UPDATE

Information element	Reference	Application	Specified type (Sender)	Specified type (Receiver)	Remarks
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 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	
From	[1]20.20	All codes	m	m	4.11.7
MIME-Version	[1]20.24	All codes	c	c	
Min-SE	[16]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	[16]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)

Table 4-19/JJ-22.01 UPDATE response message (2/2)

Note 1: Used to set the information set for a media stream. Note 2: Does not enable changing of the route set established with an Initial INIVTE. c1: "m" if SDP is used for a response and "x" otherwise. c2: "m" if draft-ietf-session-timer is used and "x" otherwise.

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

4.11.1. Basic format

Call set-up and call control are performed by transferring SIP/UDP (User Datagram Protocol)/IP packets between networks.

There are two formats for SIP messages, request message and response message. Each of the header parameters used in these formats are specified here. The details shall conform to the reference document. Unless otherwise noted, the symbols for ABNF (Augmented Backus-Naur Form) shall conform to the provisions contained in Chapter 25 of JF-IETF-RFC3261.

4.11.2. Request-Line

A SIP request is identified by having a Request-Line on the first line of the message. A Request-Line can contain a Method name, Request-URI, protocol version information, each separated by a space (SP).

A Request-Line ends with a line feed (CRLF).

Table 4-20/JJ-22.01 Information elements in the Request-Line header

Header: header information item	Type	Coding format	Remarks
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 Section 4.12.
SIP-Version	m	"SIP/2.0"	

* A Request-Line can be set on a single line. It cannot be used more than once in the same message.
Note 1: The uses of PRACK and UPDATE differ depending on the server in the operating agency. The uses of other requests (tokens) shall be decided through consultation between servers.

4.11.3. Status-Line

A SIP response is identified by having a Status-Line on the first line of the message. A Status-Line can contain a protocol version information, Status-Code, and Reason-Phase, each separated by a space (SP).

A Status-Line ends with a line feed (CRLF).

Table 4-21/JJ-22.01 Information elements in the Status-Line header

Header: header information item	Type	Coding format	Remarks
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	Character string	
* A Status-Line can be set on a single line. It cannot be used more than once in the same message. Note 1: Only the Status-Codes described in Section 4.9 can be set.			

4.11.4. Allow

This header lists the set of methods supported by the UA (User Agent) generating the message.

Table 4-22/JJ-22.01 Information elements in the Allow header

Header: header information item	Type	Coding format	Remarks
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 be set on a single line only. Note 1: Only the message types described in Section 4.8can be set. Methods may be listed in any order. c1: "m" if the reception capability is provided and "x" otherwise.			

4.11.5. Content-Type

This header indicates the media type of the message-body sent to the recipient.

Table 4-23/JJ-22.01 Information elements in the Content-Type header

Header: header information item	Type	Coding format	Remarks
Content-Type		("Content-Type" / "c") HCOLON media-type	
media-type	m	m-type SLASH m-subtype *(SEMI m-parameter)	
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 be set only once. This header cannot be used more than once in the same message.			

4.11.6. CSeq

This header is used to uniquely identify a transaction.

Table 4-24/JJ-22.01 Information elements in the CSeq header

Header: header information item	Type	Coding format	Remarks
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 be set only once. This header cannot be used more than once in the same message. Note 1: Tokens shall be decided through consultation between servers.			

4.11.7. From

This header indicates the initiator of a request. It is used to specify the information for a calling party.

Table 4-25/JJ-22.01 Information elements in the From header

Header: header information item	Type	Coding format	Remarks
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 be set only once. This header cannot be used more than once in the same message. o1: Depends on the selection between the servers in the operating agency.			

4.11.8. P-Asserted-Identity

This header is used to transfer the user information authenticated on each server.

Because it is not clear whether PAI (P-Asserted-Identity) during an inter-server linkage on a private network is necessary or not, it shall be deleted.

Table 4-26/JJ-22.01 Information elements in the P-Asserted-Identity header

Header: header information item	Type	Coding format	Remarks
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 Section 4.12.
addr-spec	o1		See Section 4.12.

* Settings shall conform to the technical specifications for user ID transfer.
o1: Depends on the selection on each server.

4.11.9. Privacy

This header is used to transfer the user information authenticated on each server. (See Section 4.13.2.)

Table 4-27/JJ-22.01 Information elements in the Privacy header

Header: header information item	Type	Coding format	Remarks
Privacy		"Privacy" HCOLON priv-value	
priv-value	M	"id" / "none"	

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

4.11.10. Record-Route

To route a request in a dialog through the same proxy server, this header is inserted into the request by that proxy server.

Table 4-28/JJ-22.01 Information elements in the Record-Route header

Header: header information item	Type	Coding format	Remarks
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 can be used more than once in the same message. It can be used in up to ten entries on up to five lines. For details, refer to the carrier SIP recommendations.
Note 1: Only a SIP-URI is permitted.

4.11.11. Route

This header is used to route a request message via listed proxies.

Table 4-29/JJ-22.01 Information elements in the Route header

Header: header information item	Type	Coding format	Remarks
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 can be used more than once in the same message. It can be used in up to five entries on up to five lines.
Note 1: Only a SIP-URI is permitted.

4.11.12. Session-Expires

This header specifies the expiry time of the session timer to be updated with a re-INVITE.

Table 4-30/JJ-22.01 Information elements in the Session-Expires header

Header: header information item	Type	Coding format	Remarks
Session-Expires		("Session-Expires" / "x") HCOLON delta-seconds [refresher]	
delta-seconds	m	1*DIGIT	
Refresher	o	SEMI "refresher" EQUAL "uas" / "uac"	

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

4.11.13. To

This header specifies the logical recipient of a request. This information shall be considered not for use due to number dereferencing.

Table 4-31/JJ-22.01 Information elements the To header

Header: header information item	Type	Coding format	Remarks
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 be set only once. This header cannot be used more than once in the same message.
Note 1: Not set in an Initial INVITE or CANCEL.
o1: Depends on the selection on the server.

4.11.14. Via

This header indicates the transport used for a transaction.

Table 4-32/JJ-22.01 Information elements in the Via header

Header: header information item	Type	Coding format	Remarks
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 can be used more than once in the same message. It can be used in up to five entries on up to five lines. Constraint conditions are applied to only addresses that indicate adjacent SIP servers.

4.12. URI specification system (addr-spec)

This system supports both the SIP-URI and the TEL-URL (Uniform Resource Locator) formats.

Table 4-33/JJ-22.01 SIP-URI scheme

Header: header information item	Type	Coding format	Remarks
addr-spec			
SIP-URI	m	"sip:" anonymous-string / denote-string	Address starting with sip:.
Anonymous-string	o1	"anonymous@anonymous.invalid"	Used in the From header, etc. of a message if the number is not presented.
denote-string	o1	[userinfo] hostport uri-parameters	Normal URI specification format.
Userinfo	o	(user/telephone-subscriber) "@"	User distinguished name: User name, telephone number, etc. to be distinguished on the host.
Telephone-subscriber	o2	Private-phone-number	The telephone number is used as a user number. (Specified in JF-IETF-RFC3966.)
Private-phone-number	m	Not used.	Private network number defined on the private network.
phonedigit	x	DIGIT	Digits and delimiters, "-" / "." / "(" / ")", can be used.
User	o2	1*(unreserved / escaped / user-unreserved)	
"@"	m		If using userinfo, be sure to put a "@" as the separator for the host portion.
Hostport	m	host [":" port]	Specifies the host to provide resources.
Host	m	hostname / Ipv4address	Enter a host name as FQDN (Fully Qualified Domain Name) and an IPv4 address.
Port	o	1*DIGIT	Specifies the number of the port to provide resources.
Uri-parameters	o	*(";" uri-parameter)	Indicates the additional information for network access to the host.
uri-parameter	o	transport-param / user-param / maddr-param / lr-param	
transport-param	o	"transport=" ("udp" / "tcp")	Indicates the transport protocol for sending SIP messages. udp and tcp are defined.
user-param	o	"user=" ("phone")	Can be used to distinguish a user name similar to a telephone number from the telephone number. If User=phone, this is interpreted as requesting that it be handled as a telephone number.
maddr-param	o	"maddr=" host	Used to request to send a packet to the address specified with maddr. This address is given priority over other host addresses in the SIP-URI, etc.
lr-param	m	"lr"	Used in Route information such as Record-Route. Be sure to connect servers together with Loose-Router. (Strict is optional.)

Table 4-34/JJ-22.01 TEL-URI scheme

Header: header information item	Type	Coding format	Remarks
addr-spec			
TEL-URI	m	"tel:" telephone-subscriber	Address starting with tel:.
telephone-subscriber	m	global-phone-number / local-phone-number	The telephone number is used as a user number. (Specified in JF-IETF-RFC3966.)
Private-phone-number	o	Not used.	Private network number defined on the private network.
phonedigit	m	DIGIT	Digits can be used.
local-phone-number	o	Private-Number	Private network number defined on the private network.
phonedigit	m	DIGIT	Digits can be used.
area-specifier	m	";phone-context=" phone-context-ident	Used to add originating area information as additional dialing information.
phone-context-ident	m	Not used.	Private network number defined on the private network.
phonedigit	m	DIGIT	Digits can be used.

4.13. Other signal provisions

4.13.1. Handling of un-specified signals

If a signal or information is not specified in this standard is sent from a private network from a request is sent, it is not assured that the signal or information is handled as significant information on the private network that receives the request.

If operation is to be assured, this shall be in accordance with the consultation between servers.

4.13.2. Handling of calling line identifications

Calling line identification presentation shall adopt a system conforming to the technical specifications for user ID transfer.

(1) A calling line identification is transferred with an Initial INVITE request.

(2) A calling line identification is set as each parameter value in a P-Asserted-Identity header, and is embedded in an Initial INVITE request. This header always needs to be set.

(3) As information elements regarding the handling of a calling line identification, the parameters below shall be used, which are defined in the technical specifications for user ID transfer.

1) SIP_URI : Set as SIP_URI the contents of the addr-spec section of the SIP_URI of the P-Asserted-Identity header of an Initial INVITE request.

2) SIP_DISPLAYNAME : Set as SIP_DISPLAYNAME the displayname portion of the SIP_URI of the P-Asserted-Identity header of an Initial INVITE request.
If the portion is enclosed with quotation marks, remove the quotation marks before setting it as SIP_DISPLAYNAME.

3) TEL_URI : Set as TEL_URI the contents of the addr-spec portion of the TEL URI of the P-Asserted-Identity header of an Initial INVITE request.

4) TEL_DISPLAYNAME : Set as TEL_DISPLAYNAME the contents of the Displayname portion of the TEL_ URI of the P-Asserted-Identity header of an Initial INVITE request.

If the portion is enclosed with quotation marks, remove the quotation marks before setting it as TEL_DISPLAYNAME.

5) Privacy : Handle the Privacy header of an Initial INVITE as Privacy information.

Table 4-35/JJ-22.01 Calling line identification presentation conditions

Information item	Mapping condition	Remarks
Calling line identification	TEL_URI	Handled as the number for identifying the originator. No visual separator is used. (Subscriber number approved by each server.)
Generic number (presented number)	TEL_DISPLAYNAME	Handled if a number different from a calling line identification is to be presented to the destination side. No visual separator is used.
Displayable /non-displayable	Privacy	Basically, "none" is displayable while "id" is non-displayable. If "id" is not contained and if the Privacy header itself is not set, it is treated as displayable. If both the calling party number (subscriber number) and the generic number (presented number) are set, the generic number (presented number) must be treated as displayable/non-displayable, while the calling party number (subscriber number) must be treated as non-displayable at all times.
Reason for non-presentation	SIP_DISPLAYNAME	As a reason for non presentation, the following type (character string) shall be made available in accordance with the technical specifications for user ID transfer: "Anonymous"
* If TEL_URI is not set, this is interpreted as the absence of the calling line identification to be presented.		

5. Connection conditions

5.1. Session timer

It is recommended to provide a session timer function specified for draft-ietf-session-timer to detect session release if a call is not terminated normally or if a call is not released with a BYE request.

5.2. 100rel

It is recommended to support JF-IETF-RFC3262 if there are no means for securing the reliable transfer of temporary response messages in each of the sections for SIP signal paths including the interface section defined in this standard, because of dependence on the mechanism in a lower layer, for example.

5.3. Conditions for using bearers

5.3.1. SDP format

Table 5-1/JJ-22.01 SDP information elements

Item Header:abbreviation		Specified type (Sender)	Specified type (Receiver)	Description	Remarks
Session description					
protocol version	v=	m	m	SDP version number (at present, always v = 0)	
owner/creator and session identifier	o=	m	m	Session starter and session identification information	
session name	s=	m	m	Session name. No constraints on the format and the description.	
connection information	c=	o	m	Connection information (indicating the location at which to receive data).	(Note 1)
Time description					
time the session is active	t=	m	m	Session start and end time.	(Note 2)
Media description					
media name and transport address	m=	m	m	Media type and transport address.	
connection information	c=	o	m	Connection information (indicating the location at which to receive data).	(Note 1)
media attribute line	a=	o	o	Media attribute.	

* The payload type and cycle shall conform to IETF-RFC. The payload types and the payload cycles must be identical on the two parties.
* A PT (payload type) of 0 must be used. Whether to use other values shall be decided through consultation between servers.
Note 1: It is required to set information in either of them.
Note 2: Must be "0 0" during origination and ignored during reception.

A media session in SIP (JF-IETF-RFC3261) is established and managed with the exchange of SDPs on SIP messages based on the models called offers and answers.
If unspecified lines are used, they are not assured.

5.3.1.1. Multipart MIME (Multipurpose Internet Mail Extensions) body (offer or answer)

When a multipart/mixed MIME body is received, only a type that can be supported is set in the Accept header and a 415 response is sent.

5.3.1.2. SDP with multiple m= lines (offer)

If an SDP containing multiple m= lines is received, it must be possible to return an answer with a port number being set to 0 except for those m= lines that can be supported.

5.3.1.3. Reception of multiple payload types (answer)

If an offer containing multiple payload type values on m= lines as supportable payload types is sent, there may be cases in which an answer containing multiple payload type values on m= lines is received. In such cases, this means that it is possible to freely switch among multiple payload types in a single session. If switching is not possible, therefore, it is necessary to offer again an SDP that contains only the payload type value whose use is desired in actual use, with a re-INVITE request or UPDATE request.

5.4. Session changes

If session changes are permitted through consultation between servers, a= line changes (sendonly, recvonly, and inactive) are permitted, but if the server that receives session change requests do not support them, the server may ignore the requests. Note that basically, it is not possible to change c= lines and m= lines.

Session change requests can be made, but 488 error responses may be sent in response to session requests. In such a case, the side that receives a session change request does not clear the call for the cause of change request reject. The session requester does not automatically clear the call with change request reject, either. If the call is to be cleared for the cause of change request reject, a BYE request must be sent to explicitly specify that the call should be cleared; otherwise, the session shall be continued.

> If a session change is to be rejected on the private network to the session change is requested, a 488 error response shall be sent.

5.5. Guidance/talkie services

Guidance/talkie services may be supplied by an originating SIP server or by a called SIP private network.

5.5.1. Supply of guidance/talkie services from inside a called SIP private network

As guidance/talkie services from inside a called SIP private network, those supplied from the Early dialog and those supplied on the confirm dialog can be considered.

Guidance/talkie services supplied on the Early dialog from inside a called SIP private network are achieved by providing SDP information in 18X responses. It is necessary for each server to match and verify the conditions for making a call on the Early dialog.

5.5.2. Supply of guidance/talkie services from an originating private SIP network

For the purpose of supplying guidance/talkie services, an originating private SIP network can use the status code in the response it has received from the called private SIP network. However, it is necessary to maintain compatibility in guidance connections with response codes between servers.

Annex a. Congestion Provisions

a.1. Basic rules

If the maximum number of calls that can be connected in a session is decided through the consultation between servers, control shall be performed with a bidirectional session reservation function.

a.2. Control with a session reservation function

(1) Set the number of sessions available at both ends of the session group (the value for deciding whether sessions can be used with bidirectional reserved-session control if there is a lot of bidirectional traffic) and the number of bidirectional sessions to be reserved (number of sessions to be reserved for the traffic of the other party if there is a lot of unidirectional traffic) and enable or disable the session seizure under the conditions below.

Attached Table a/JJ-22.01 Concept of session seizure

<table>
<tr><td colspan="2">Enabling or disabling the session seizure</td></tr>
<tr><td rowspan="2">If the number of sessions used due to the calls on the local station is equal to or greater than the maximum number of sessions available.</td><td>If the number of idle sessions is greater than the number of bidirectional reserved sessions, enable session seizure on the local station.</td></tr>
<tr><td>If the number of idle sessions is equal to or less than the number of bidirectional reserved sessions, disable session seizure on the local station.</td></tr>
</table>

(2) The implementation bidirectional reserved-session control shall be decided through the consultation between servers in the operating agency that make connections.

(3) The number of bidirectional reserved sessions and the number of available sessions shall be decided through the consultation between servers in the operating agency.

Annex b. Connections for RTP Audio Sent out from the Network before Call Completion

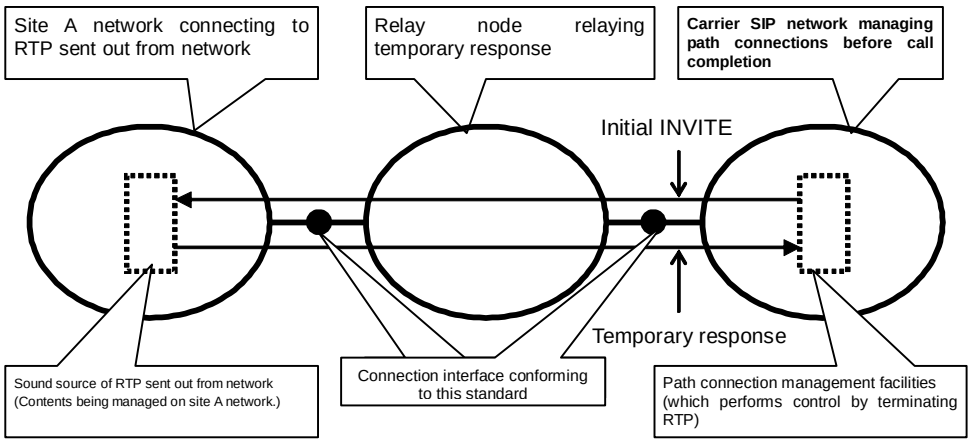
b.1. Purpose of this annex

For connections for RTP audio before the call completion, it is necessary to maintain the compatibility to provide linkages with individual servers on the private network and unify tones by sending announcements from the originating or terminating server.

A connection model configuration is shown below.

b.2. Model for RTP audio sent out from the network

Attached Figure b shows a connection model on a private SIP network for RTP audio sent out from the network.



* The node to relay temporary responses may not exist depending on the connection system.
* The node to relay temporary responses may also serve simultaneously as the node to manage path connections before call completion.

Attached Figure b-1/JJ-22.01 Connection model on a private network for RTP audio sent out from the network

The following shows the types of servers that play a role in RTP audio sent out from the network connections in the model above. It should be noted that these types are logical ones, and their roles may change depending on the call to be connected. It should also be noted that in a call actually connected, a single server (node) may play multiple roles at the same time and its roles are not required and omitted.

<Server to connect to RTP sent from the network>

Server which connects to the RTP sound source managed on the network before call completion, in response to the Initial INVITE request received via a connection interface specified in this standard, has responsibility for the contents of the sound source to be connected before call completion.

An example is a server that actually prepares announcements to be sent out from the network, such as congestion talkie services, and makes connections in accordance with conditions.

<Private SIP network that relays temporary responses>

A private SIP network (or a site) that sends a corresponding Initial INVITE request from a connection interface specified in this standard against the call that receives an Initial INVITE request from a connection interface specified in this standard.

<Private SIP network that manages path connections before call completion>

Private SIP network that conducts management so that in response to a call that sends an Initial INVITE request via a connection interface specified in this standard, an audio path is not connected from the called party to the calling party before call completion. The private SIP network that manages path connections before call completion needs to manage the facilities terminating RTP audio from the destination network. As the facilities for managing path connections there is a GW that is connected to a PSTN/PISN (Private Integrated Services Network) and an SBC (Session Border Controller) that temporarily terminates RTP packets between a carrier network and a private network.

b.3. General description of the operations for RTP audio sent out from the network

Regarding the operations of private SIP networks for RTP audio sent out from the network, operational provisions requested of the private SIP networks that have their respective roles are provided below. Note that the operations of the private SIP networks that are described below may be judged to determine if they are to be applied on a call-by-call basis under conditions such as whether a call can be connected to a path, rather than assuming that they apply to all calls handled by the private SIP networks.

b.3.1. Operation of the private SIP network that connects to RTP sent from the network

In Table 4-4, "SIP response signals for the INVITE request" (Section 4.9), the provisions below are described as annotations for 180 (Ringing) response and 183 (Session Progress) response.

The private SIP network to send a response can attached the SDP information and send it only if it can manage and assure the audio contents of the RTP to be sent to the private network that will receive the response.

Thus, if the private SIP network that receives an Initial INVITE request via an interface conforming to this standard is to connect RTP audio sent out from the network before call completion, it must include an SDP in the 180 (Ringing) response or 183 (Session Progress) response to be sent for an RTP connection.
If there is a possibility that an SDP is received from an entity that cannot assure the contents of the RTP to be connected because of the network configuration or terminal management conditions[1], either of the operations below must be performed on the message to be received from such an entity[2].

1. Delete the SDP and send a corresponding response.
2. Send a corresponding SDP by including it in a corresponding response, but ensure that the RTP from the called party is not transferred to the calling party.

If the method in 1. above is employed, if processing based on the 100rel expansion function is performed, the 200 (OK) response that may be sent subsequently may not include an SDP. Thus, on a private SIP network that deletes SDPs, it is necessary to record the contents of SDPs will deleted, and if no SDP is included in the 200 (OK) response, it is necessary to send a response containing a corresponding SDP, as the recorded SDP has been received.

---

[1] This includes a case that subscribers have malice and performe unexpected operations can transmit except the composition operation agencies assume usually.

[2] If in the private SIP network of the request source as seen from the private SIP network (that is, the response destination), it is assured that no private SIP network that manages path connections before call completion exists, though no specific problems such as unauthorized uses will occur even if the actions described here are not taken, but action should be taken to secure generality and expandability of connections between private SIP networks.

If the method in 2. above is employed, it is necessary to ensure that the address and port information included in the SDP included in the received Initial INVITE request is not known to the called party[3].

b.3.2. Operation of the private SIP network that relays temporary responses

If a private SIP network receives an Initial INVITE request via an interface conforming to this standard, and it sends a corresponding Initial INVITE request via an interface conforming to this standard, and if it then receives a 180 (Ringing) response or 183 (Session Progress) response containing an SDP, it must include an SDP in the 180 response or 183 response to be sent via the interface, in response to receiving the response.

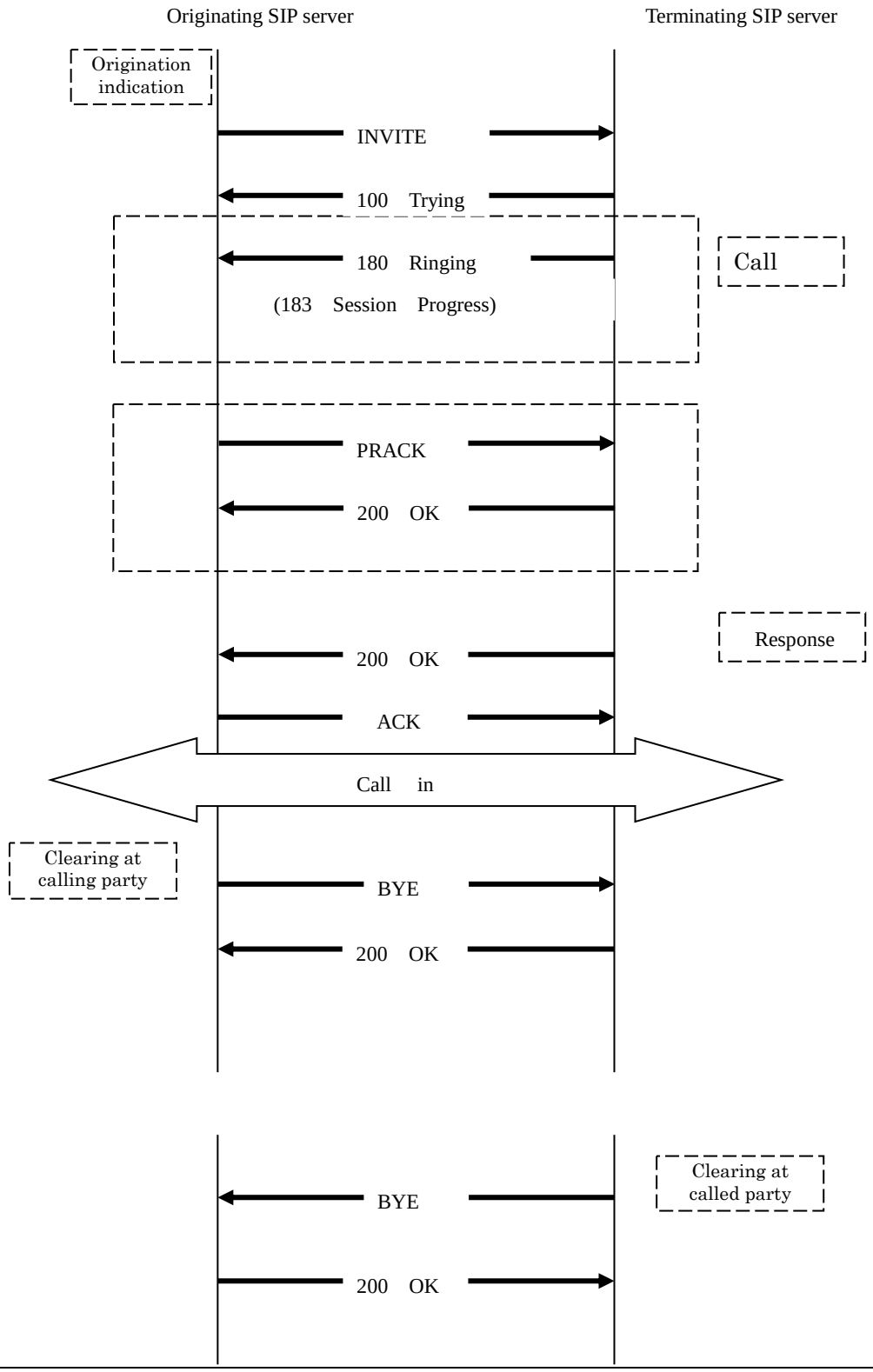
Note that the private SIP network that relays temporary responses may also serve simultaneously as a private SIP network that manages path connections before call completion.

b.3.3. Operation of the private SIP network that manages path connections before call completion

If a private SIP network that needs to prohibit audio path connections before call completion from a called user receives a 180 (Ringing) response or 183 (Session Progress) response containing an SDP in response to the Initial INVITE request sent via an interface conforming to this standard, it must be judged that the connection before call completion does not contain any improper audio and made a path connection from the called party to the calling party.

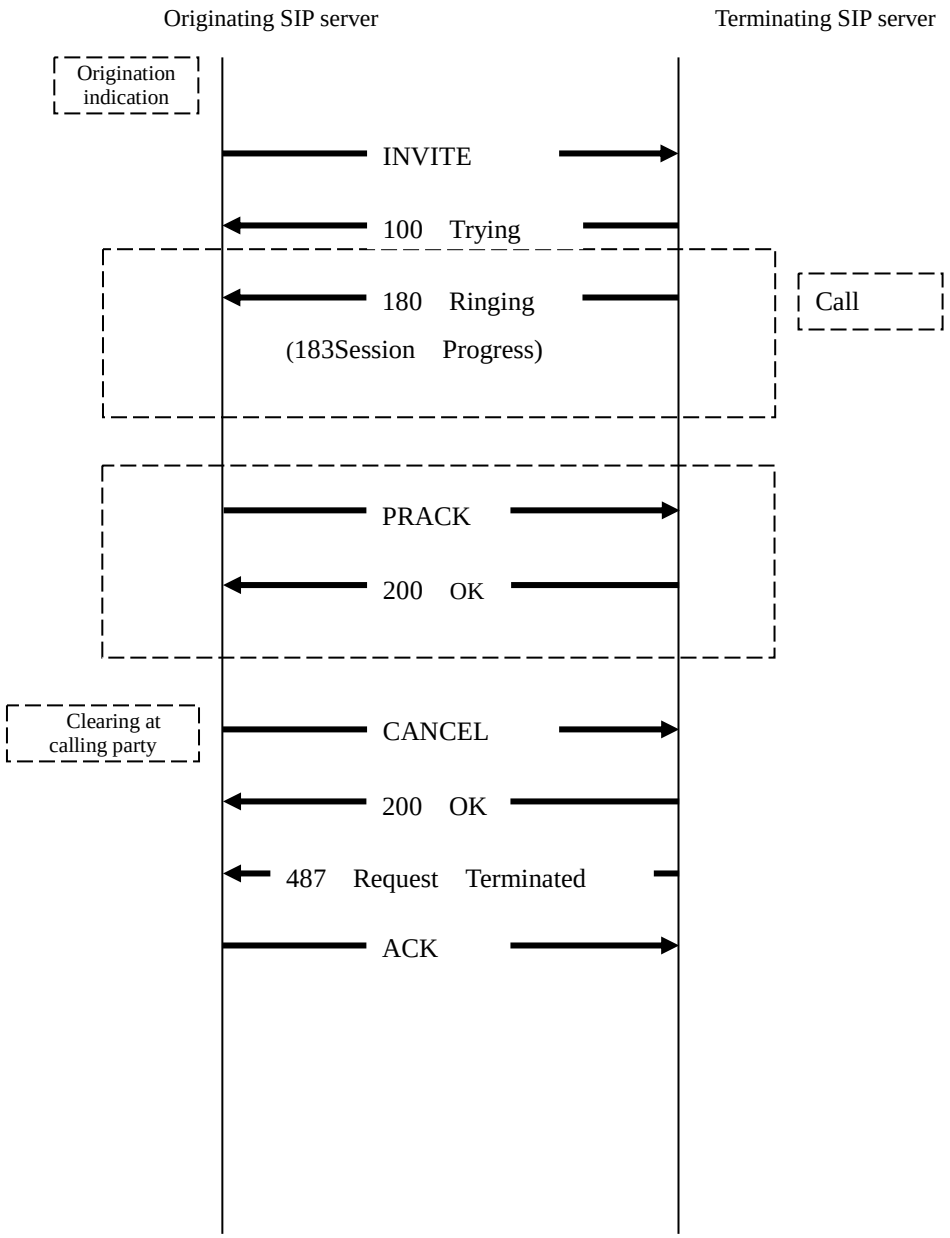
[3] In this case, the private SIP network may be required to have a function for terminating RTP, such as SBC.

No	1	Type		Classification	Basic connection



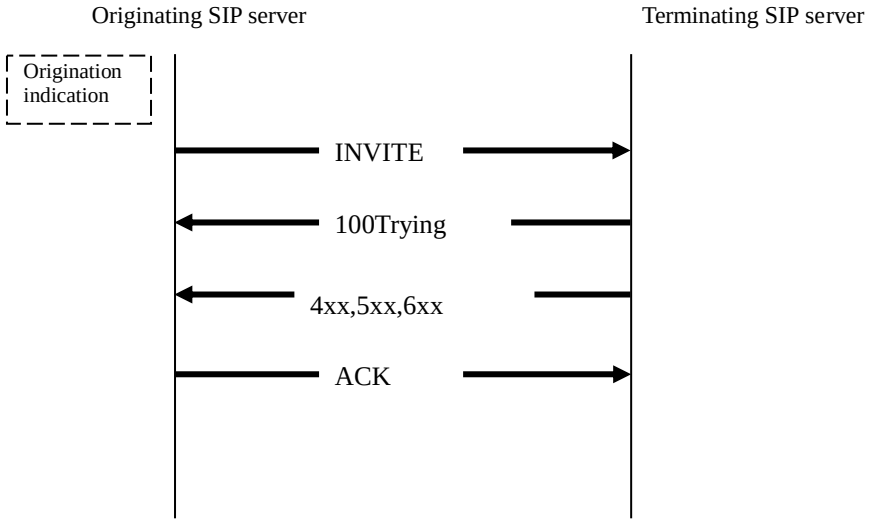
Attached Figure b-2/JJ-22.01 Basic connection

No	2	Type		Classification	Basic connection (call abort)



Attached Figure b-3/JJ-22.01 Basic connection (call abort)

No	3	Type		Classification	Basic connection (incomplete example)



Technical Specifications on Inter-connection Interface between Private SIP Networks

December 6, 2007

TTC Original Standards [JJ-22.01]

Copyright © 2007

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE (TTC)

All rights reserved.

Printed by HIFUMI SHOBO CO., Ltd.

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE (TTC)

Shiba kouen Denki Building 1-1-12, Shiba kouen, Minato-ku

Tokyo 105-0011, Japan

TEL ; ＋81 3 3432 1551　FAX ; ＋81 3 3432 1553

Printed in JAPAN