International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3948

(06/2011)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN – Testing for next generation networks

---

Service testing framework for VoIP at the user-to-network interface of next generation networks

Recommendation ITU-T Q.3948

ITU-T

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3999
General	Q.3000–Q.3029
Network signalling and control functional architecture	Q.3030–Q.3099
Network data organization within the NGN	Q.3100–Q.3129
Bearer control signalling	Q.3130–Q.3179
Signalling and control requirements and protocols to support attachment in NGN environments	Q.3200–Q.3249
Resource control protocols	Q.3300–Q.3369
Service and session control protocols	Q.3400–Q.3499
Service and session control protocols – supplementary services	Q.3600–Q.3649
NGN applications	Q.3700–Q.3849
Testing for new generation networks	**Q.3900–Q.3999**

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

Recommendation ITU-T Q.3948

Service testing framework for VoIP at the user-to-network interface of next generation networks

Summary

Recommendation ITU-T Q.3948 describes the procedure, requirements, physical configuration and standard document sets for a service testing framework for VoIP at the user-to-network interface (UNI) of next generation networks (NGNs).

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Q.3948	2011-06-29	11

Keywords

NGN, service testing, UNI, VoIP.

FOREWORD

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

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

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

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

NOTE

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

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

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

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Page

Introduction

The World Telecommunication Standardization Assembly (WTSA-08) approved Resolution 76 (Johannesburg, 2008), *Studies related to conformance and interoperability testing, assistance to developing countries, and a possible future ITU Mark programme*, and assigned all ITU-T study groups with the responsibility of developing conformance and interoperability Recommendations to improve the interoperability of next generation networks (NGNs). This Recommendation provides the test specification framework to assure the interoperability of VoIP services at the user-to-network interface (UNI) of NGNs. This Recommendation encourages support of the testing of NGNs in multi-vendor environments.

Recommendation ITU-T Q.3948

Service testing framework for VoIP at the user-to-network interface of next generation networks

1 Scope

This Recommendation describes the procedure, requirements, physical configuration and standard document sets for the service testing framework for VoIP at the user-to-network interface (UNI) of next generation networks (NGNs). Other service tests await further study. The purpose of this Recommendation is to describe the service testing framework for VoIP at the UNI of NGNs in order to confirm conformity to the relevant ITU-T Recommendation and to assure the interoperability of NGN products at the specific interface.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T E.164] Recommendation ITU-T E.164 (2010), *The international public telecommunication numbering plan*.

[ITU-T G.711] Recommendation ITU-T G.711 (1984), *Pulse code modulation (PCM) of voice frequencies*.

[ITU-T H.264] Recommendation ITU-T H.264 (2009), *Advanced video coding for generic audiovisual services*.

[ITU-T Q.850] Recommendation ITU-T Q.850 (1998), *Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN User Part.*

[ITU-T Q.3402] Recommendation ITU-T Q.3402 (2008), *NGN UNI signalling profile (Protocol set 1).*

[ITU-T Y.1221] Recommendation ITU-T Y.1221 (2002), *Traffic control and congestion control in IP based networks*.

[ITU-T Y.1540] Recommendation ITU-T Y.1540 (2007), *Internet protocol data communication service – IP packet transfer and availability performance parameters*.

[ITU-T Y.1541] Recommendation ITU-T Y.1541 (2006), *Network performance objectives for IP-based services*.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks.*

[ISO/IEC 14496-2] ISO/IEC 14496-2:2004, *Information technology – Coding of audio-visual objects – Part 2: Visual*.

[ISO/IEC 14496-3] ISO/IEC 14496-3:2005, *Information technology – Coding of audio-visual objects – Part 3: Audio*.

[RFC 2046] IETF RFC 2046 (1996), Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types.

[RFC 2474] IETF RFC 2474 (2009), *Definition of Differentiated Services Field in the IPv4 and IPv6 Headers*.

[RFC 2475] IETF RFC 2476 (2009), *An Architecture for Differentiated Services*.

[RFC 2617] IETF RFC 2617 (1996), HTTP Authentication: Basic and Digest Access Authentication.

[RFC 3016] IETF RFC 3016 (2000), *RTP Payload Format for MPEG-4 Audio/Visual Streams.*

[RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

[RFC 3262] IETF RFC 3262 (2002), *Reliability of Provisional Responses in the Session Initiation Protocol (SIP).*

[RFC 3264] IETF RFC 3264 (2002), *An Offer/Answer Model with the Session Description Protocol (SDP).*

[RFC 3265] IETF RFC 3265 (2002), *Session Initiation Protocol (SIP)-Specific Event Notification*.

[RFC 3310] IETF RFC 3310 (2002), *Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA).*

[RFC 3311] IETF RFC 3311 (2002), *The Session Initiation Protocol (SIP) UPDATE Method*.

[RFC 3312] IETF RFC 3312 (2002), *Integration of Resource Management and Session Initiation Protocol (SIP).*

[RFC 3313] IETF RFC 3313 (2003), *Private Session Initiation Protocol (SIP) Extensions for Media Authorization.*

[RFC 3320] IETF RFC 3320 (2003), *Signaling Compression (SigComp).*

[RFC 3323] IETF RFC 3323 (2002), *A Privacy Mechanism for the Session Initiation Protocol (SIP).*

[RFC 3324] IETF RFC 3324 (2002), *Short Term Requirements for Network Asserted Identity*.

[RFC 3325] IETF RFC 3325 (2002), *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*.

[RFC 3326] IETF RFC 3326 (2002), *The Reason Header Field for the Session Initiation Protocol (SIP).*

[RFC 3327] IETF RFC 3327 (2002), *Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts*.

[RFC 3329] IETF RFC 3329 (2003), *Security Mechanism Agreement for the Session Initiation Protocol (SIP).*

[RFC 3388] IETF RFC 3388 (2002), *Grouping of Media Lines in the Session Description Protocol (SDP).*

[RFC 3428] IETF RFC 3428 (2002), *Session Initiation Protocol (SIP) Extension for Instant Messaging*.

[RFC 3455] IETF RFC 3455 (2003), *Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP).*

[RFC 3485] IETF RFC 3485 (2003), *The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Static Dictionary for Signaling Compression (SigComp).*

[RFC 3486] IETF RFC 3486 (2003), *Compressing the Session Initiation Protocol (SIP).*

[RFC 3515] IETF RFC 3515 (2003), *The Session Initiation Protocol (SIP) Refer Method.*

[RFC 3524] IETF RFC 3524 (2003), *Mapping of Media Streams to Resource Reservation Flows*.

[RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

[RFC 3551] IETF RFC 3551 (2003), *RTP Profile for Audio and Video Conferences with Minimal Control*.

[RFC 3556] IETF RFC 3556 (2003), *Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth*.

[RFC 3581] IETF RFC 3581 (2003), *An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing*.

[RFC 3608] IETF RFC 3608 (2003), *Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration*.

[RFC 3680] IETF RFC 3680 (2004), *A Session Initiation Protocol (SIP) Event Package for Registrations*.

[RFC 3840] IETF RFC 3840 (2004), *Indicating User Agent Capabilities in the Session Initiation Protocol (SIP).*

[RFC 3841] IETF RFC 3841 (2004), *Caller Preferences for the Session Initiation Protocol (SIP).*

[RFC 3891] IETF RFC 3891 (2004), *The Session Initiation Protocol (SIP) "Replaces" Header*.

[RFC 3892] IETF RFC 3892 (2004), *The Session Initiation Protocol (SIP) Referred-By Mechanism.*

[RFC 3903] IETF RFC 3903 (2004), *Session Initiation Protocol (SIP) Extension for Event State Publication.*

[RFC 3911] IETF RFC 3911 (2004), *The Session Initiation Protocol (SIP) "Join" Header*.

[RFC 3959] IETF RFC 3959 (2004), *The Early Session Disposition Type for the Session Initiation Protocol (SIP).*

[RFC 3984] IETF RFC 3984 (2005), *RTP Payload Format for H.264 Video*.

[RFC 4028] IETF RFC 4028 (2005), *Session Timers in the Session Initiation Protocol (SIP).*

[RFC 4032] IETF RFC 4032 (2005), *Update to the Session Initiation Protocol (SIP) Preconditions Framework.*

[RFC 4145] IETF RFC 4145 (2005), *TCP-Based Media Transport in the Session Description Protocol (SDP).*

[RFC 4566] IETF RFC 4566 (2006), *SDP: Session Description Protocol*.

[RFC 4585] IETF RFC 4585 (2008), *Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF).*

[RFC 5049] IETF RFC 5049 (2007), *Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP).*

[RFC 5079] IETF RFC 5079 (2007), *Rejecting Anonymous Requests in the Session Initiation Protocol (SIP).*

[RFC 5104] IETF RFC 5104 (2008), *Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF).*

[RFC 5407] IETF RFC 5407 (2009), *Example calls flows of race conditions in the Session Initiation Protocol (SIP).*

[TTC JJ-90.10] TTC JJ-90.10 (2005), *Inter-Carrier Interface for N-ISDN*, 7th English Edition.

[TTC TR-1014] TTC TR-1014 (2006), *Overview of the NGN architecture*, version 1.

[TTC TS-1008] TTC TS-1008 (2004), *Technical Specification on ISDN Called Party Subaddress Information Transferring through Provider's SIP Networks, version 1*.

[3GPP TS 24.229] 3GPP TS 24.229 (2002), *IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3.*

3 Definitions

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

MPEG Moving Picture Experts Group

NGN Next Generation Network

NIT Network Integration Test

NUT Network Under Test

PICS Protocol Implementation Conformance Statements

PIXIT Protocol Implementation Extra Information for Testing

QoS Quality of Service

RTC RTP Control Protocol

RTP Real-Time Transport Protocol

SCF Service Control Functions

SDP Session Description Protocol

SIP Session Initiation Protocol

TCP Transmission Control Protocol

UA User Agent

UDP User Datagram Protocol

UNI User-to-Network Interface

VoIP Voice over Internet Protocol

5 Conventions

None.

6 Preparation for testing

6.1 Test object

The test object of the VoIP service testing is specified in multiple Recommendations and relevant standards.

Figure 1 shows the block diagram of a session initiation protocol (SIP) multimedia communication terminal and the shaded parts are the test object of this Recommendation.

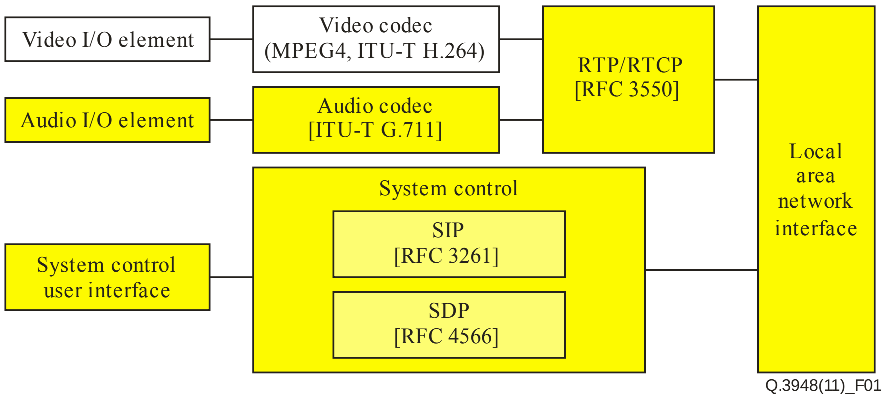

Figure 1 – SIP multimedia communication terminal

The test profile should include the list of the Recommendations related to the test object of VoIP service testing.

Table 1 shows the coding scheme and profiles of a SIP multimedia communication terminal.

Table 1 – Coding scheme and profiles

Item	VoIP	MPEG-4	ITU-T H.264
Session control	SIP [RFC 3261], SDP [RFC 4566]		
Capability exchange	[RFC 3264]	[RFC 3264], [RFC 3016]	[RFC 3264], [RFC 3984]
SIP extensions	[RFC 3262] (Reliability of provisional responses) [RFC 3311] (UPDATE) [RFC 4028] (Session Timers)		
Media transfer	RTP ([RFC 3550], [RFC 3551]), RTCP ([RFC 3550] Option)		
	[RFC 3551]	Packetization mode [RFC 3016]	Packetization mode [RFC 3984]
Video (high rate: CIF, low rate: QCIF)	None	High:MPEG-4 Visual SP@L3 Low:MPEG-4 Visual SP@L0	High: ITU-T H.264 (BP@L1.2) Low: ITU-T H.264 (BP@L1)
Audio	ITU-T G.711 μ/A-law		

6.2 Target interface

The UNI in Figure 2 is the target interface of this Recommendation.

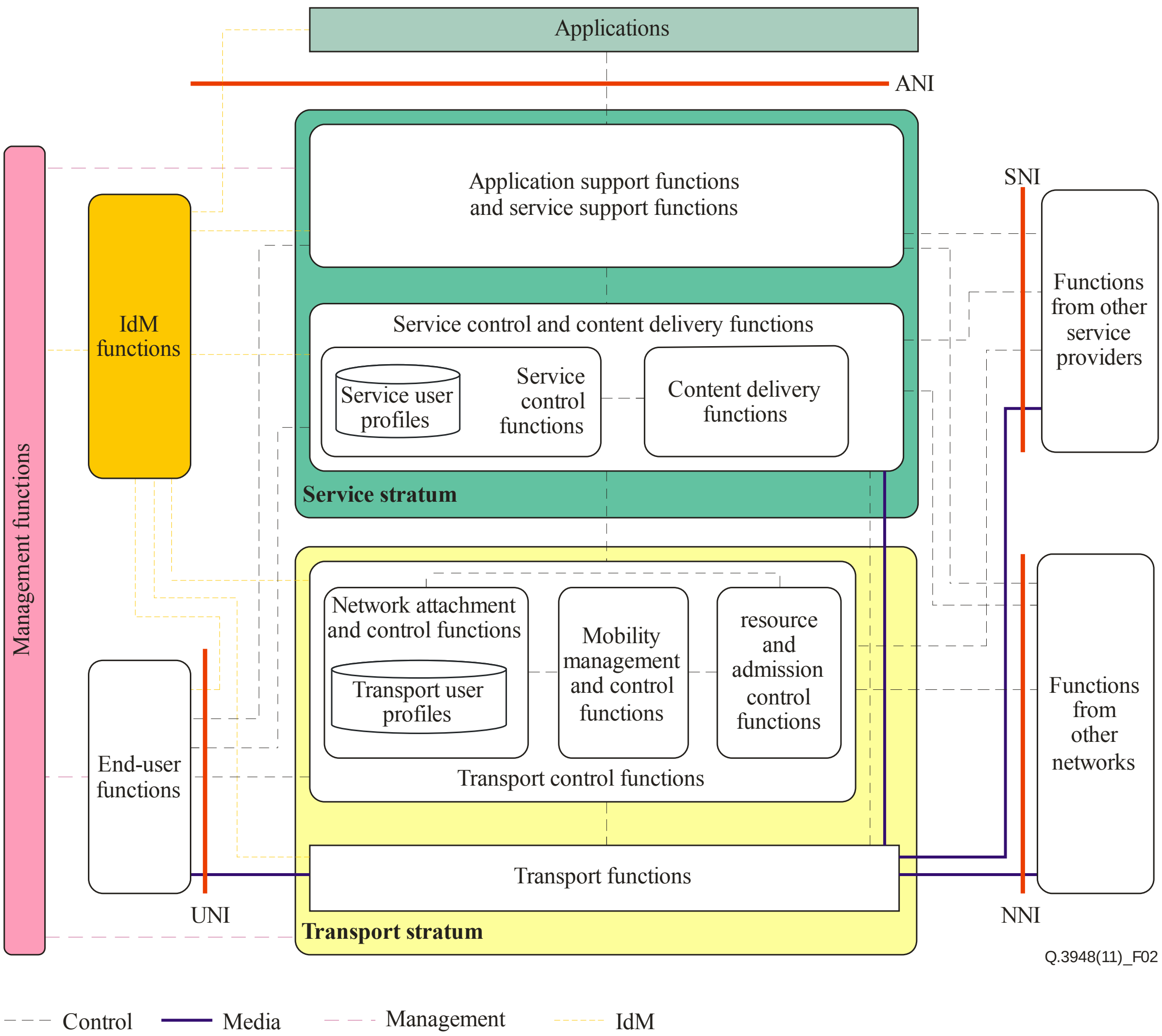

Figure 2 – UNI as the target interface (ITU-T Y.2012 NGN architecture overview)

6.3 Target Recommendation

[ITU-T Q.3402] is the target Recommendation.

6.4 Physical configuration

The physical configuration should define the functions which are needed for service testing. It may be depending on target protocol. This paragraph should show the items concerning conditions of the test configuration. There are two steps in a network under test (NUT), one is the network integration test (NIT), and the other is interoperability testing of the end-to-end service.

Figure 3 shows a sample of the general configuration of the NIT for the VoIP service testing at UNI. In this figure, the reference machine is similar to the network. Figure 4 shows a sample of the general configuration of VoIP interoperability testing of the end-to-end service.

Figure 3 – General configuration of NIT for the VoIP service testing

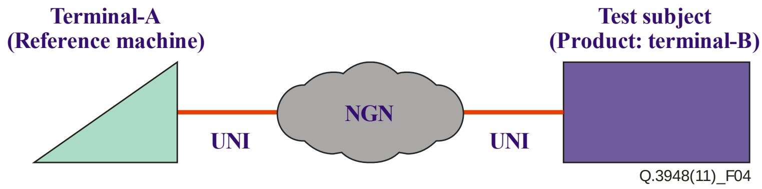

Figure 4 – General configuration of VoIP interoperability testing of the end-to-end service

6.5 Test scenarios of the network integration test (NIT)

The following is a sample of the network integration test (NIT) for VoIP service testing at UNI.

6.5.1 Test items

The sample of test items is as follows:

a) Terminal registration

b) Negotiating SIP capabilities

c) Audio terminal behaviour

For details, refer to the tables of "List of sequences".

Table 2 – List of sequences of the network integration test (NIT)

No.	Sequence Name	Corresponding clauses and figures of Table VII.1: List of sequence examples
1	Terminal registration (access-line based authentication)	Clause VII.1.1
2	Deletion of terminal registration (access-line based authentication)	Clause VII.1.3
3	Call origination to disconnection (IPv4, Use of `timer` and `100rel`, ITU-T G.711 μ-law)	Clause VII.1.4
4	Call termination to disconnection (IPv4, Use of `timer` and `100rel`, ITU-T G.711 μ-law)	Clause VII.1.6
5	Call cancellation	Clause VII.1.7
6	Busy on the terminating side	Clause VII.1.8

6.5.2 Execution flow

NGN service testing should be conducted in line with the following steps:

1) Set the test object, target interface and target Recommendations.

2) Set the physical configuration and target products.

3) Define the test scenarios.

4) Examine the service testing according to the test scenarios and analyse the test output.

Detail clauses are shown as follows.

6.5.2.1 Terminal registration (access-line based authentication)

This clause shows the message flow when a network requires a `REGISTER` from a terminal, and access-line based terminal authentication is performed. An IPv4 address and an IPv6 address are used as `Contact address`, and `REGISTER` is performed by IPv4 UDP. The network notifies the pre-existing route by a `Service-Route` header and notifies the available network-asserted user identity by a `P-Associated-URI` header.

In the terminal registration shown Figure 5 below, a SIP-URI composed of a telephone number is used as the URI to be specified in the `From` header and the `To` header at the time of terminal registration, like the caller number shown in Appendix VII.3. Note that there may be a case of using a SIP-URI which is not composed of the telephone number, according to the NGN carrier policy.

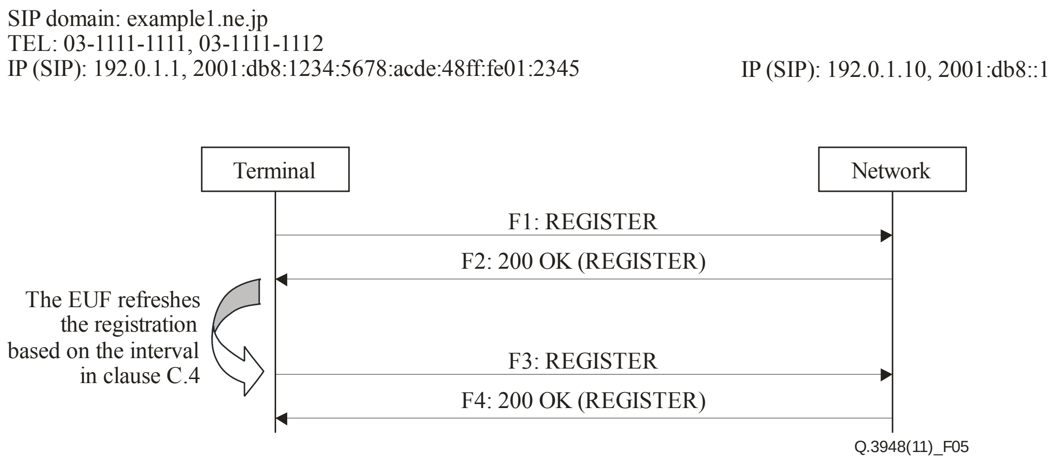

Figure 5 – Terminal registration (access-line based authentication)

F1: REGISTER

```
REGISTER sip:example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111111
Max-Forwards: 70
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111111
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 REGISTER
Contact:
<sip:qwertyui@192.0.1.1>,<sip:asdfghjk@[2001:db8:1234:5678:acde:48ff:fe01:2345]>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE
Expires: 3600
Supported: path
Content-Length: 0
```

F2: 200 OK (REGISTER)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111111
Path: <sip:192.0.1.10;lr>
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101010
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111111
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 REGISTER
Contact:
<sip:qwertyui@192.0.1.1>;expires=3600,<sip:asdfghjk@[2001:db8:1234:5678:48ff:fe0
1:2345]>;expires=3600
Supported: path
Service-Route: <sip:s-cscf.example1.ne.jp;lr>
P-Associated-URI:
<sip:0311111111@example1.ne.jp>,<sip:0311111112@example1.ne.jp>
Content-Length: 0
```

F3: REGISTER

```
REGISTER sip:example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Max-Forwards: 70
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Contact:
<sip:qwertyui@192.0.1.1>,<sip:asdfghjk@[2001:db8:1234:5678:acde:48ff:fe01:2345]>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE
Expires: 3600
Supported: path
Content-Length: 0
```

F4: 200 OK (REGISTER)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Path: <sip:192.0.1.10;lr>
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101011
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Contact:
<sip:qwertyui@192.0.1.1>;expires=3600,<sip:asdfghjk@[2001:db8:1234:5678:48ff:fe0
1:2345]>;expires=3600
Supported: path
Service-Route: <sip:s-cscf.example1.ne.jp;lr>
P-Associated-URI:
<sip:0311111111@example1.ne.jp>,<sip:0311111112@example1.ne.jp>
Content-Length: 0
```

6.5.2.2 Deletion of terminal registration (access line-based authentication)

This clause shows the message flow when terminal registration is deleted under the same condition of option item selection as in Table VII.1, assuming that the old registration of the terminal remains in the network when the power of the terminal turns on.

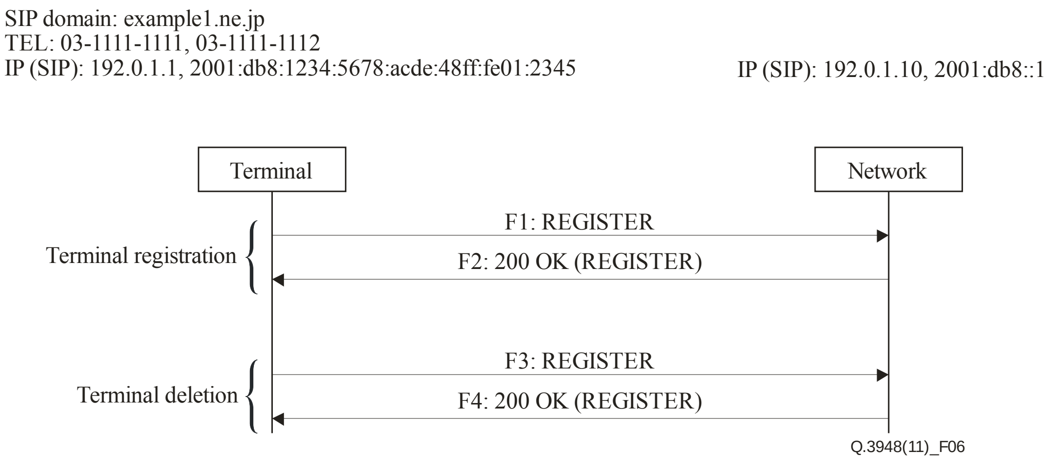

Figure 6 – Deletion of terminal registration (access-line based authentication)

F1 to F2 are omitted because they are the same as those of Table VII.1.

F3: REGISTER

```
REGISTER sip:example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Max-Forwards: 70
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Contact: *
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE
Expires: 0
Supported: path
Content-Length: 0
```

F4: 200 OK (REGISTER)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Path: <sip:192.0.1.10;lr>
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101011
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Supported: path
Service-Route: <sip:s-cscf.example1.ne.jp;lr>
P-Associated-URI:
<sip:0311111111@example1.ne.jp>,<sip:0311111112@example1.ne.jp>
Content-Length: 0
```

6.5.2.3 Call origination to disconnection (IPv4, Use of timer and 100rel, ITU-T G.711 µ-law)

This clause shows the message flow of a call connection sequence on the originating side when the `timer` and `100rel` are enabled on both the originating and terminating sides. IPv4 is used for call control signals and media, UDP is used for call control, and ITU-T G.711 µ-law is used as audio media. Session refresh is performed by `UPDATE`, and disconnection (by the originating side) is finally performed by `BYE`.

This clause shows the message flow on the terminating side under the same condition of option item selections as those given in Table VII.1.

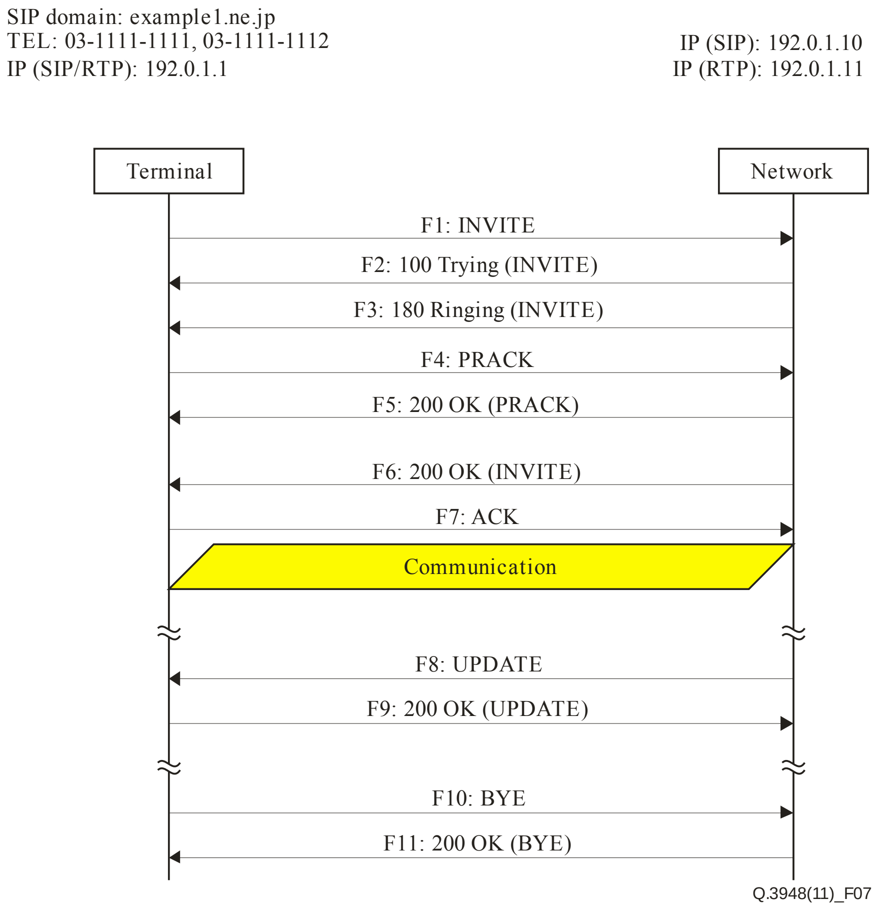

Figure 7 – Call origination to disconnection (IPv4, Use of timer and 100rel, ITU-T G.711 μ-law) (access-line based authentication)

F1: INVITE

```
INVITE tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>,<sip:s-cscf.example1.ne.jp;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:zxcvbnm@192.0.1.1>
P-Preferred-Identity: <sip:0311111112@example1.ne.jp>
Privacy: none
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: 100rel,timer
Session-Expires: 300
Content-Type: application/sdp
Content-Length: 195

v=0
o=- 82664419472 82664419472 IN IP4 192.0.1.1
s=-
c=IN IP4 192.0.1.1
t=0 0
m=audio 10000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F2: 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Content-Length: 0
```

F3: 180 Ringing

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Record-Route: <sip:192.0.1.10;lr>
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: 100rel
RSeq: 1
Content-Length: 0
```

F4: PRACK

```
PRACK sip:mnbvcxz@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111122
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 2 PRACK
RAck: 1 1 PRACK
Content-Length: 0
```

F5: 200 OK (PRACK)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111122
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 2 PRACK
Content-Length: 0
```

F6: 200 OK (INVITE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Record-Route: <sip:192.0.1.10;lr>
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uas
```

```
Content-Type: application/sdp
Content-Length: 197

v=0
o=- 82917391739 82917391739 IN IP4 192.0.1.11
s=-
c=IN IP4 192.0.1.11
t=0 0
m=audio 20000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F7: ACK

```
ACK sip:mnbvcxz@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111123
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

F8: UPDATE

```
UPDATE sip:zxcvbnm@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-22222222
Max-Forwards: 64
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 100 UPDATE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: timer,100rel
Session-Expires: 300;refresher=uac
Content-Length: 0
```

F9: 200 OK (UPDATE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-22222222
To: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111121
From: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 100 UPDATE
Contact: <sip:zxcvbnm@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uac
Content-Length: 0
```

F10: BYE

```
BYE sip:mnbvcxz@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK5678-11111124
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
```

```
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 3 BYE
Content-Length: 0
```

F11: 200 OK (BYE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK5678-11111124
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 3 BYE
Content-Length: 0
```

6.5.2.4 Call termination to disconnection (IPv4, Use of timer and 100rel, ITU-T G.711 µ-law)

This clause shows a message flow on the terminating side under the same condition of option item selections as in Table VII.1. After receiving a call from the network, session refresh is performed by `UPDATE`, and disconnection (by the terminating side) is performed by `BYE`. The network notifies the calling party's identity information by the `P-Asserted-Identity` header, and the called party's information by the `P-Called-Party-ID` header to the called terminal.

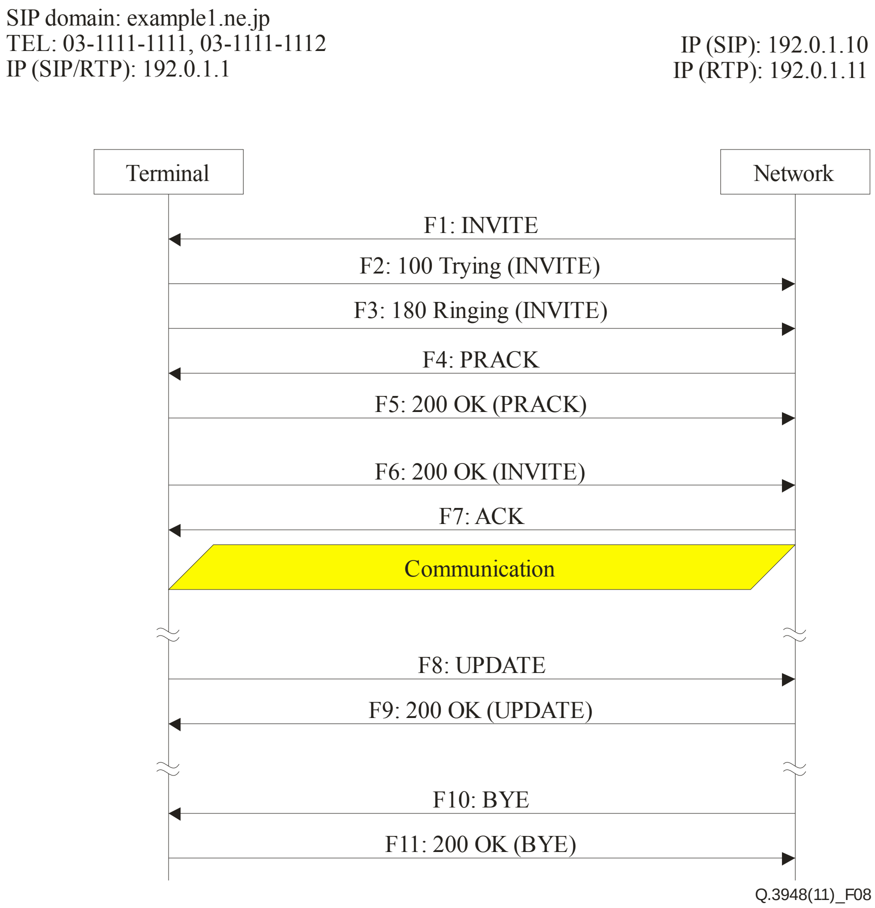

Figure 8 – Call termination to disconnection (IPv4, Use of timer and 100rel, ITU-T G.711 µ-law)

F1: INVITE

```
INVITE sip:qwertyui@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101020
Record-Route: <sip:192.0.1.10;lr>
Max-Forwards: 64
To: <sip:0311111112@example1.ne.jp>
From: <sip:03122222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101020@192.0.1.10
CSeq: 101 INVITE
Contact: <sip:lkjhgfds@192.0.1.10>
P-Asserted-Identity: "0322222223" <sip:0322222223@example1.ne.jp>,"0322222223"
<tel:0322222223;phone-context=example1.ne.jp>
Privacy: none
P-Called-Party-ID: <sip:0311111112@example1.ne.jp>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: 100rel,timer
Session-Expires: 300
Content-Type: application/sdp
Content-Length: 197

v=0
o=- 82664482616 82664482616 IN IP4 192.0.1.11
s=-
c=IN IP4 192.0.1.11
t=0 0
m=audio 40000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F2: 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101020
To: <sip:0311111112@example1.ne.jp>
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101020@192.0.1.10
CSeq: 101 INVITE
Content-Length: 0
```

F3: 180 Ringing

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101020
Record-Route: <sip:192.0.1.10;lr>
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 101 INVITE
Contact: <sip:asdfghjk@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: 100rel
RSeq: 1
Content-Length: 0
```

F4: PRACK

```
PRACK sip:asdfghjk@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101021
Max-Forwards: 64
```

```
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 102 PRACK
RAck: 1 1 PRACK
Content-Length: 0
```

F5: 200 OK (PRACK)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101021
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 102 PRACK
Content-Length: 0
```

F6: 200 OK (INVITE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101020
Record-Route: <sip:192.0.1.10;lr>
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101020@192.0.1.10
CSeq: 101 INVITE
Contact: <sip:asdfghjk@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uas
Content-Type: application/sdp
Content-Length: 195

v=0
o=- 82917391739 82917391739 IN IP4 192.0.1.1
s=-
c=IN IP4 192.0.1.1
t=0 0
m=audio 30000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F7: ACK

```
ACK sip:asdfghjk@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101022
Max-Forwards: 70
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 101 ACK
Content-Length: 0
```

F8: UPDATE

```
UPDATE sip:lkjhgfds@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111125
Max-Forwards: 70
```

```
To: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 201 UPDATE
Contact: <sip:asdfghjk@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: timer,100rel
Session-Expires: 300;refresher=uac
Content-Length: 0
```

F9: 200 OK (UPDATE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111125
To: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 201 UPDATE
Contact: <sip:lkjhgfds@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uac
Content-Length: 0
```

F10: BYE

```
BYE sip:asdfghjk@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-11111124
Max-Forwards: 70
To: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-11111121
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 103 BYE
Content-Length: 0
```

F11: 200 OK (BYE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-11111124
To: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-11111121
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 103 BYE
Content-Length: 0
```

6.5.2.5 Call cancellation (disconnection while ringing)

This clause shows an example message flow for call cancellation by the originating side under the same condition of option item selections as in Table VII.1.

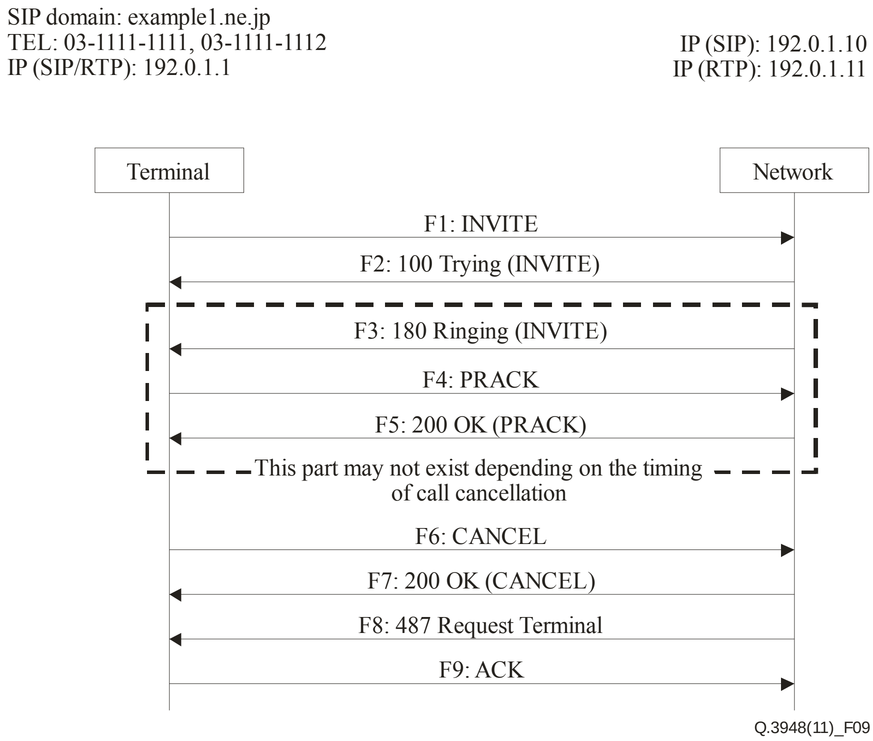

Figure 9 – Call cancellation (disconnection while ringing)

F1 to F5 are omitted because they are the same as those of Table VII.1.

F6: CANCEL

```
CANCEL tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>,<sip:s-cscf.example1.ne.jp;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 CANCEL
Content-Length: 0
```

F7: 200 OK (CANCEL)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 CANCEL
Content-Length: 0
```

F8: 487 Request Terminated

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 INVITE
Content-Length: 0
```

F9: ACK

```
ACK tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

6.5.2.6 Busy on the terminating side

This clause shows a message flow when the destination is busy (short of empty sessions) under the same condition of option item selections as in Table VII.1.

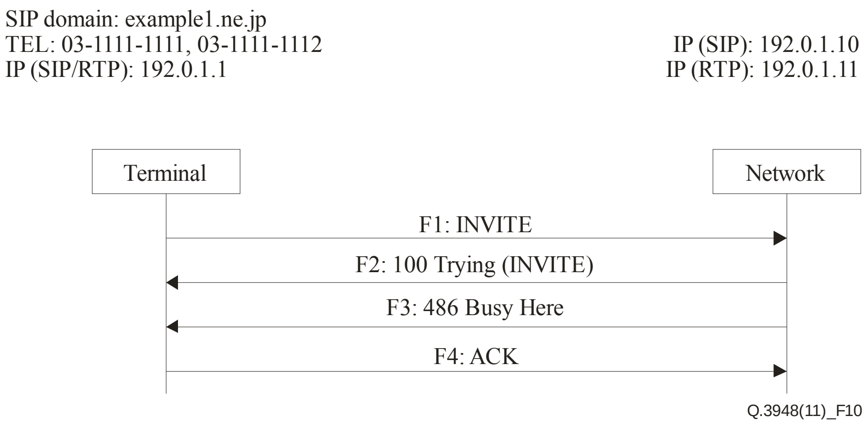

Figure 10 – Busy on the terminating side

F1 to F2 are omitted because they are the same as those of Table VII.1.

F3: 486 Busy Here

```
SIP/2.0 486 Busy Here
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 INVITE
Content-Length: 0
```

F4: ACK

```
ACK tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

6.6 Test scenario of VoIP interoperability testing of the end-to-end service

This paragraph shows the steps for each test to prevent the omission of VoIP interoperability testing of the end-to-end service. This step should be tested after NIT confirmation in 6.5.

Figure 11 shows a sample of the general configuration of VoIP interoperability testing of the end-to-end service, followed by a sample of test steps.

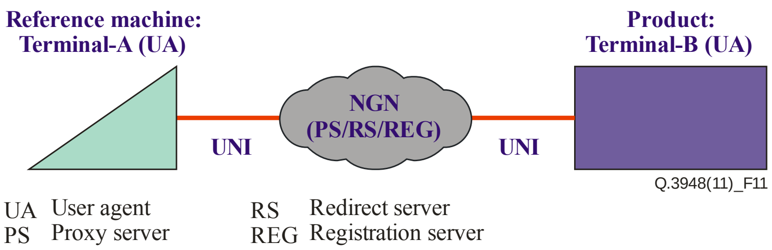

Figure 11 – General configuration of VoIP interoperability testing of the end-to-end service

6.6.1 Test items

Following is the sample of test items:

A) Register a UA in the server.

B) "Calling UA" calls "Receiving UA". Check PRACK request and OK response.

C) If the call is not received, try calling again up to three times. If the call is still not received, check the communication conditions, such as the registration information. If something is wrong with the conditions, then retry from (A). Otherwise, consider this as a communication error and conduct procedure (G).

D) After confirming the connection, the receiving UA checks that it can properly receive the audio, video (if required), and other test items from the other terminal in accordance with the items listed. In addition, the encoding mode that has executed the communication for the caller or the receiver must be recorded respectively for "Calling UA" or "Receiving UA".

E) Continue the communication for at least three minutes and then check whether all the items have been tested. Check whether the session timer is updated by UPDATE request and OK response.

F) Both the caller and the receiver must confirm that the communication can be disconnected properly.

G) Switch the roles of the caller and the receiver, and repeat procedures (A) to (F).

The test criteria of each test item should be described to clarify the conformance test verifications.

Table 3 is a sample of test criteria.

Table 3 – Test criteria

No.	Item		Judging standard
1	Sending side (Terminal A)	Terminal registration	Confirm the communication of audio and the video in each mode for more than three minutes. Confirm `PRACK` request and `OK` response. Confirm that the session timer is updated by `UPDATE` request and `OK` response at least once.
2		Confirmation of audio communications	
3		Transmission rate of audio	Record the maximum transmission rate capability that was exchanged.
4		Other	If required.
5		Disconnection by network	Confirm that the terminal is disconnected properly when the disconnection is initiated by the network.
6		Disconnection by terminal	Confirm that the terminal is disconnected properly when the disconnection is initiated by the terminal.
1	Receiving side (Terminal B)	Terminal registration	Confirm the communication of audio and video in each mode for more than three minutes. Confirm the `PRACK` request and `OK` response. Confirm that the session timer is updated by `UPDATE` request and `OK` response at least once.
2		Confirmation of audio communications	
3		Transmission rate of audio	Record the maximum transmission rate capability that was exchanged.
4		Other	If required.
5		Disconnection by network	Confirm that the terminal is disconnected properly when the disconnection is initiated by the network.
6		Disconnection by terminal	Confirm that the terminal is disconnected properly when the disconnection is initiated by the terminal.

7 Analyse the test output

The test outcomes are assumed to include an identification of the test event, a log of the test event, and an indication of the state of the target device after the test event. The test outcomes in test campaigns are compared with the expected behaviour of the NGN service, to confirm the applicability of the device to the service.

The test outcomes (such as the output test event, test logs, and statement of the tested product) as service-testing results in test campaigns should be compared with the specifications of the Recommendations.

7.1 Test report production

This paragraph shows the methods to summarize the examinations for test result successes and failures, and shows the detailed items required for success of the tests in order to illustrate the results of the conformance test.

The test results will show two items about the network integration test (NIT) for service testing and VoIP interoperability testing of the end-to-end service.

Tables 4 and 5 show sample verification sheets.

Table 4 – Verification sheet of the network integration test

Item		Result	
		Success	**Failure**
(a)	Terminal registration (access-line based authentication)		
(b)	Deletion of terminal registration (access-line based authentication)		
(c)	Call origination to disconnection (IPv4, Use of `timer` and `100rel`, ITU-T G.711 μ-law)		
(d)	Call termination to disconnection (IPv4, Use of `timer` and `100rel`, ITU-T G.711 μ-law)		
(e)	Call cancellation		
(f)	Busy on the terminating side		

Table 5 – VoIP interoperability testing of the end-to-end service

Item			Result	
			Success	**Failure**
1	Sending side (Terminal A)	Terminal registration		
2		Confirmation of audio communications		
3		Transmission rate of audio		
4		Other (if required)		
5		Disconnection by network		
6		Disconnection by terminal		
1	Sending side (Terminal B)	Terminal registration		
2		Confirmation of audio communications		
3		Transmission rate of audio		
4		Other (if required)		
5		Disconnection by network		
6		Disconnection by terminal		

8 Guide to annexes and appendices

The annexes and appendices of this Recommendation provide additional specifications to Recommendation ITU-T Q.3402 in order to define more detailed protocol specifications, including clarifications on the specifications, network options, and terminal options of the ITU-T Q.3402 main body. This will improve the interoperability of SIP terminals connected to domestic NGN carriers through the UNI.

Annex A shows the clarifications in a table containing the corresponding clause number as given in the main body. The remaining annexes and appendices deal with the following topics:

Annex B: Calling line identification presentation.

Annex C: Terminal registration.

Annex D: Negotiating SIP capabilities.

Annex E: SDP setting and media handling.

Annex F: Considerations on congestion prevention and control.

Annex G: Bandwidth control.

Annex H: Limitations of SIP message settings.

Annex J: Audio terminal's behaviour.

Appendix I: List of network options and terminal options for this standard.

Appendix II: Guidelines for response code usage.

Appendix III: Mapping SDP description to QoS classes.

Appendix IV: Security considerations.

Appendix V: Discovery procedure of the SCF.

Appendix VI: Signalling rule tables of SIP messages and headers.

Appendix VII: Examples of message flows.

Annex A

Clarification and option lists of ITU-T Q.3402 main body

(This annex forms an integral part of this Recommendation.)

A.1 Overview

This annex provides clarification and option lists of the ITU-T Q.3402 main body to improve the interoperability of SIP terminals to the NGN connected through the UNI in the architecture defined in the ITU-T Q.3402 main body.

A.2 Clarification and option lists

Table A.1 shows the clarification and option lists for the main body of [ITU-T Q.3402]. Clauses unmentioned in the table mean that specifications in the base document are applied as they are. The lists of options described in Annexes A to J and in Appendices I to VI are not shown in Table A.1. Refer to Appendix I for the lists of options including these annexes and appendices.

Table A.1 – Clarification and option lists

ITU-T Q.3402 clause		Clarifications	Options	Remarks
No.	**Name of clause**			
5	Reference model	In the case that the EUF is an audio telephone terminal, follow Annex J.	–	
6	Assumptions	2. SRTP is not to be used for the transfer of audio and video	–	
7.1	Consideration related to media packets	Specifications in the base document are applied as they are.	Sending media packets from the originating terminal, in the case that a `1xx` response to `INVITE` includes SDP answer (Table I.25, Item 1). Handling of media packets before completion of SDP negotiation to an initial `INVITE` (Table I.25, Item 2, of Appendix I)	
8.1	Codec list	The audio codec list shall contain ITU-T G.711μ-law. Even when a codec in the codec list is set in an SDP offer, it may not be end-to-end negotiation, depending on a carrier's policy. A codec that is not contained in the codec list is not to be set in an SDP offer.	Codecs to be contained in the codec list other than ITU-T G.711 μ-law. (Table I.16, Items 1 to 3)	
8.2	Packetization size	For the packetization period in the case of using ITU-T G.711 μ-law, follow clause J.2.1.	–	
9	Routing and addressing	For the URI format in the case of using a national number, follow clause B.5. For the subaddress, follow clause B.6.	`Request-URI` format of SIP requests outside existing dialogues, except for `REGISTER` (Table I.20, Items 1 and 2).	

Table A.1 – Clarification and option lists

ITU-T Q.3402 clause		Clarifications	Options	Remarks
No.	**Name of clause**			
10.1	RFCs to be supported	[RFC 2976], [RFC 3388], [RFC 3725], [RFC 3824], [RFC 3853], RFC3861], [RFC 3959], [RFC 3960], [RFC 4168], [RFC 4244], [RFC 4412], [RFC 4458], and [RFC 5031] are not to be used. Support for the `P-Media-Authorization` header specified in [RFC 3313] is applicable only in the direction from the SCF to the EUF. For the handling of the `Reason` header specified in [RFC 3326], follow clause F.3.1. For the handling of the path extension function specified in [RFC 3327], follow clause C.3. Support for the `Path` header is applicable only to the response in the direction from the SCF to the EUF. Support for the `Security-Client` header and `Security-Verify` header specified in [RFC 3329] is applicable only to the request in the direction from the EUF to the SCF, and support for the `Security-Server` header is applicable only to the response in the direction from the SCF to the EUF. Of the headers specified in [RFC 3455], the `P-Associated-URI` header and the `P-Called-Party-ID` header are used, which conform to Annex B. The headers `P-Charging-Vector`, `P-Charging-Function-Addresses`, and `P-Visited-Network-ID` are not to be used. Support for the `P-Access-Network-Info` header is applicable only to the SIP messages in the direction from the EUF to the SCF. For the handling of the `Service-Route` header specified in [RFC 3608], follow clause C.3.	The followings are the list of options for each RFC. [RFC 2046] Use of MIME Multipart (Table I.10, Items 1 to 4) [RFC 3310], [RFC 2617], and [RFC 3329] Terminal authentication procedures (Table I.11, Items 1 and 2) Use of security capabilities exchange function (`sec-agree`) (Table I.7, Item 8) [RFC 3262] Use of provisional response reliability function (`100rel`) (Table I.7, Item 2) [RFC 3265] Use of `SUBSCRIBE` method and `NOTIFY` method. (Table I.2, Items 10 to 15) [RFC 3311] SDP offer by `UPDATE` (Table I.23, Items 1, 2, 5, and 6) Media modification in early dialogue (Table I.23, Items 1 and 2) [RFC 3312], [RFC 4032] Use of function for reserving bandwidth before session establishment (*precondition*) (Table I.7, Item 5) [RFC 3313] Use of `P-Media-Authorization` header (Table I.17, Item 1) [RFC 3320], [RFC 3485], [RFC 3486], [RFC 5049] Use of SigComp (Table I.5, Item 1)	

Table A.1 – Clarification and option lists

ITU-T Q.3402 clause		Clarifications	Options	Remarks
No.	**Name of clause**			
		For the registration event specified in [RFC 3680], follow clause C.6. NOTE – To support RFCs means to follow the contents described in the RFCs. It does not mean that their capabilities are used in all sessions.	[RFC 3388], [RFC 3524] Use of Grouping of media (Table I.18, Item 1) [RFC 3428] Use of `MESSAGE` method (Table I.2, Items 2 to 5) [RFC 3515], [RFC 3892] Use of `REFER` method (Table I.2, Items 6 to 9) [RFC 3556] Use of SDP bandwidth modifier for RTCP bandwidth (Table I.13, Item 4) [RFC 3581] Allowing Hosted NAT in the lower part of UNI (Table I.6, Item 1) [RFC 3840], [RFC 3841] Use of terminal capabilities notification function (*pref*) (Table I.7, Item 6) [RFC 3891] Use of dialogue replacement function (*replaces*) (Annex Table I.7, Item 3) [RFC 3903] Use of `PUBLISH` method (Table I.2, Items 16 to 19) [RFC 3911] Use of conference session participation function (*join*) (Table I.7, Item 4) [RFC 4028] Session refresh by `UPDATE` method (Table I.8, Item 1)	
10.2.1.7	SIP Messages	For maximum length of SIP messages and its elements, follow Annex H.	–	

Table A.1 – Clarification and option lists

ITU-T Q.3402 clause		Clarifications	Options	Remarks
No.	**Name of clause**			
10.2.1.7.1	Requests	`OPTIONS` method is not to be used. SIPS-URI is not to be used.	–	
10.2.1.7.4.1	Message body types	Specifications in the base document are applied as they are.	SDP settings for `PRACK` and `200 OK` to `PRACK`. (Table I.22, Items 2 and 3)	
10.2.1.8.1.3	Processing responses	Specifications in the base document are applied as they are.	Terminal authentication procedures (Table I.11, Items 1 and 2)	
10.2.1.8.3	Redirect servers	Specifications in the base document are applied as they are. The `3xx` response is applicable to requests outside existing dialogues, except for `REGISTER`.	Use of redirect functions by *3xx* response (Table I.12, Items 1 and 2)	
10.2.1.10	Registrations	For the terminal registration procedures, follow Annex C. For the congestion control at the time of terminal registration, follow clause F.2.	Whether or not terminal registration needed and procedures (Table I.2, Item 1, Table I.11, Item 1, and Table I.24, Items 1 to 5)	
10.2.1.11	Querying for capabilities	Querying for capabilities is not supported.	–	
10.2.1.12.1	Creation of a dialogue	SIPS-URI is not to be used.	–	
10.2.1.12.2	Requests within a dialogue	SIPS-URI is not to be used.	–	
10.2.1.13	Initiating a session	Initial `INVITE` includes an SDP offer which contains valid media. (SDP negotiation using `2xx/ACK` is not to be used.) Follow Annex F.3 for congestion control at the time of call origination.	–	
10.2.1.14	Modifying an existing session	In the case of using re-`INVITE`, SDP offer is set in `INVITE` request.	Media modification after a dialogue is established (Table I.23, Items 3 to 6)	
10.2.1.17	Transactions	For the processing at race conditions triggered by SIP signalling crossover etc., conform to [RFC 5407]. Note that this standard lists a sequence between SIP-UAs, and when applying to the UNI, it should be read as sequence between network and terminal.	–	
10.2.1.19	Common message components	SIPS-URI is not to be used.	–	

Table A.1 – Clarification and option lists

ITU-T Q.3402 clause		Clarifications	Options	Remarks
No.	Name of clause			
10.2.1.20.7	Authorization	The Authorization header is used only when the SCF authenticates a `REGISTER` request from the EUF.	–	
10.2.1.20.11	Content-Disposition	Only the default value can be set in the parameter of the `Content-Disposition` header. Application server model as defined in [RFC 3959] is not to be used.	–	
10.2.1.20.27	Proxy-Authenticate	The `Proxy-Authenticate` header is used only in the `407` response when the SCF authenticates a request sent from the EUF outside existing dialogues except for `REGISTER`.	–	
10.2.1.20.28	Proxy-Authorization	The `Proxy-Authorization` header is used only when the SCF authenticates a request sent from the EUF outside existing dialogues except for `REGISTER`.	–	
10.2.1.20.29	Proxy-Require	The `Proxy-Require` header is applicable only in the direction from the EUF to the SCF.	–	
10.2.1.20.24	MIME-Version	Only "1.0" is supported	–	
10.2.1.20.32	Require	Application server model as defined in [RFC 3959] is not to be used.	Use of `timer`, `100rel`, and other SIP option tags (Table I.7, Items 1 to 9)	
10.2.1.20.33	Retry-After	For congestion control, the `Retry-After` header is utilized as described in clause F.2.1.	–	
10.2.1.20.34	Route	For the pre-existing route, follow clause C.3.	–	
10.2.1.20.44	WWW-Authenticate	The `WWW-Authenticate` header is used only in `401` responses when the SCF authenticates a `REGISTER` request from the EUF.	–	
10.2.1.23	S/MIME	S/MIME is not to be used for SDP with SIP messages related to `INVITE`.	–	
10.2.2.1	Extension method	For `UPDATE` and `PRACK` requests, follow Annex D.	–	
10.2.2.2.2	P-Asserted-Identity	The `P-Asserted-Identity` header is used only in requests outside existing dialogues except for `REGISTER`. For calling line identification presentation, follow Annex B.	–	

Table A.1 – Clarification and option lists

ITU-T Q.3402 clause		Clarifications	Options	Remarks
No.	**Name of clause**			
10.2.2.2.3	P-Preferred-Identity	The `P-Preferred-Identity` header is used only in requests outside existing dialogues except for `REGISTER`. For calling line identification presentation, follow Annex B.	–	
10.2.2.2.4	Privacy	The `Privacy` header is used only in requests outside existing dialogues except for `REGISTER`. Only "*id*" and "*none*" can be used for privacy options. For calling line identification presentation, follow Annex B.	–	
10.2.3	Summary of SIP methods and headers	`OPTIONS` method is not to be used.	SIP methods to be used (Table I.2, Items 1 to 21)	
10.3.1	SDP usage	For the handling of SDP, follow Annex E. For the values specified in *b=* line, follow Annex G.	SDP lines to be used (Table I.22, Items 4 and 5) IP version to be used for media (Table I.3, Item 3) Use of video (*m=video*) and data communication (*m=application*, *m=data*, etc.) (Table I.14, Items 1 and 2) Use of TCP for media [RFC 4145] (Table I.14, Item 3)	
11.1	Specifications to be supported	Specifications in the base document are applied as they are. Feedback function utilizing RTCP (RTP/AVPF)[RFC 4585] [RFC 5104] can be used.	Use of feedback function utilizing RTCP (Table I.19, Items 1 and 2)	
12	Call control signalling transport	UDP or TCP is used as transport protocol for sending and receiving SIP messages. TLS may be used for security.	Layer 4 protocol for call control signals (Table I.4, Items 1 to 3)	
13	IP protocol version	Specifications in the base document are applied as they are. Refer to clause E.4.1 for a note of IPv4/IPv6 fallback.	Layer 3 protocol for call control signals (Table I.3, Items 1 to 4)	

Annex B

Calling line identification presentation and related headers

(This annex forms an integral part of this Recommendation.)

B.1 Overview

This annex clarifies procedures for calling line identification presentation and notification of "cause of no ID", SIP headers used for them (`P-Preferred-Identity`, `P-Asserted-Identity`, `Privacy`, and `From`) and `Request-URI`, the SIP header used for relevant network-asserted user identity (`P-Associated-URI`), and the SIP header used for called party notification (`P-Called-Party-ID`).

B.2 Network-asserted user identity

The network-asserted user identity is the identity of a user that is asserted by the network through authentication or other means (verified by the network if provided by the terminal), and it is used for calling-party identity, etc. An example of network-asserted user identity information is a SIP-URI composed of an ITU-T E.164 number reachable to the terminal. As described in clause B.6, subaddress information may be provided by the calling terminal.

Clause B.5 indicates a specific URI format for network-asserted user identity.

B.2.1 Notification when the terminal registers

In the case of using a `REGISTER` request for registration, the network may set a `P-Associated-URI` header [RFC 3455] in its `200 OK` response in order to notify a network-asserted user identity to the terminal (Table I.24, Item 3).

A `P-Associated-URI` header lists one or more URIs which indicate network-asserted user identities allocated to the terminal. In the case that multiple network-asserted user identities are listed, the terminal recognizes the first URI as the default network-asserted user identity.

B.3 Calling party numbers

Calling-party number (hereinafter referred to as calling-party identity) presentation should be realized based on [RFC 3323], [RFC 3324], and [RFC 3325] by notifying network-asserted user identity and presentation/restriction information. Calling-party identity presentation/restriction are applied to requests outside existing dialogues, except for `REGISTER` which can be sent and received over the UNI.

Calling-party identity information presentation is mainly performed by four steps as follows.

1) A calling terminal transmits the selected calling-party identity information (`P-Preferred-Identity`) and preference of presentation/restriction (`Privacy`) to a network, instructs a destination (`Request-URI`), and calls.
2) The network which has the calling party verifies and normalizes a calling-party identity that a terminal selected, takes into consideration the default presentation/restriction setting etc. regarding the subscriber, and determines a calling-party identity information transmitted in the network and through the NNI.
3) The network which has the called party takes into consideration the preference of presentation/restriction and the called party's subscription for calling-party identity presentation service, and determines a calling-party identity information to be notified to the called terminal.
4) The called terminal is notified of calling-party identity information from the network when receiving a call.

In this annex, clause B.3.1 describes steps 1 and 2 as procedures on originating a call, and clause B.3.2 describes steps 3 and 4 as procedures on terminating a call.

B.3.1 Procedures on originating a call

B.3.1.1 Selecting a calling-party identity

If a terminal desires to explicitly select a calling-party identity among the network-asserted identities, the terminal populates the selected network-asserted user identity in `P-Preferred-Identity` header in requests outside existing dialogues. If network-asserted user identities are notified as described in clause B.2.1, the terminal selects one of the URIs listed in a `P-Associated-URI` header and populates it in the `P-Preferred-Identity` header.

The network handles a SIP-URI set in the `P-Preferred-Identity` header as calling-party identity. Note that in the case the `P-Preferred-Identity` header is not set, or a URI set in the `P-Preferred-Identity` header is not a network-asserted user identity allocated to the calling terminal, it is h to be the same as when the default network-asserted user identity is set in the `P-Preferred-Identity` header.

B.3.1.2 Setting for presentation/restriction of calling-party identity

When a terminal sends requests outside existing dialogues, calling-party identity presentation/restriction is requested using two kinds of procedures, namely, `Privacy` header [RFC 3325] and `186/184` prefixes.

– Calling-party identity presentation can be requested by setting "*none*" in the `Privacy` header, and restricted by setting "*id*". The `Privacy` header is set only when the terminal has the user configuration option of calling-party identity presentation/restriction, and the user completes the setting.

– In the case that the `Request-URI` is a URI composed of a national telephone number, calling-party identity presentation is specified when the `186` prefix is set, and restriction is specified when the `184` prefix is set. The decision as to whether to set the 186/184 prefix must be left to the dialling user, and a terminal must not act on its own, such as automatically putting the prefix.

The settings of the `Privacy` header and those of the `186/184` prefix are independent of each other.

In the case that the terminal sets "*id*" in a `Privacy header`, `<sip:anonymous@anonymous.invalid>` is set to the SIP-URI of a `From` header. In other cases, a URI identical to that of a `P-Preferred-Identity` header is set.

Table B.1 describes the contents set in the headers above.

Table B.1 – Settings of headers for calling line identification presentation

Field	Privacy header		
	None	id	No header
The user part or telephone-subscriber part of a `Request-URI`	Number that a user dialled (includes 186/184 prefix if dialled)		
`P-Preferred-Identity` header	Calling-party's network-asserted user identity		
URI in `To` header	Same value as Request-URI		
`name-addr` in `From` header	Same value as the URI set in a `P-Preferred-Identity` header, if the header is set	`<sip:anonymous@anonymous.invalid>`	Same value as the URI set in a `P-Preferred-Identity` header, if the header is set

A network selects calling-party identity presentation/restriction based on the `Privacy` header and the `186/184` prefix setting, and the default calling-party identity presentation/restriction setting of a subscriber who originates a call.

– In the case that a 186/184 prefix is set at the beginning of the telephone number in the `Request-URI`, the call is treated as a calling-party identity presentation when 186 is set, and as a calling-party identity restriction when 184 is set, regardless of a `Privacy` header setting content.

– The default calling-party identity presentation setting of the subscriber who originates the call is applied when neither the `Privacy` header setting nor a 186/184 prefix setting exists.

– In the case that the 184 prefix is not set, it is treated to be calling-party identity presentation, regardless of a `Privacy` header setting content, at the time of emergency call.

Tables B.2 and B.3 describe the order of priority among the `Privacy` header settings, 186/184 prefix settings, and the default calling-party identity presentation/restriction setting above.

Table B.2 – Calling-party identity presentation/ restriction selection conditions for normal call

<table>
<tr><th colspan="2" rowspan="2"></th><th colspan="3">Prefix of destination number</th></tr>
<tr><th>186</th><th>184</th><th>No prefix</th></tr>
<tr><td rowspan="3">Privacy</td><td>none</td><td rowspan="3">Calling-party identity presentation</td><td rowspan="3">Calling-party identity restriction</td><td>Calling-party identity presentation</td></tr>
<tr><td>id</td><td>Calling-party identity restriction</td></tr>
<tr><td>No header</td><td>Follow the default value of the network managed for each calling user</td></tr>
</table>

Table B.3 – Network selected conditions of presentation/ restriction of calling-party identity for emergency call

<table>
<tr><th colspan="2" rowspan="2"></th><th colspan="3">Prefix of a destination number</th></tr>
<tr><th>186</th><th>184</th><th>No prefix</th></tr>
<tr><td rowspan="3">Privacy</td><td>none</td><td rowspan="3">Calling-party identity presentation</td><td rowspan="3">Calling-party identity restriction</td><td rowspan="3">Calling-party identity presentation</td></tr>
<tr><td>id</td></tr>
<tr><td>No header</td></tr>
</table>

In the case that the calling-party identity is restricted, "*Anonymous*" (No caller ID: rejected by user) is selected as cause of no ID out of causes described in Table B.4.

B.3.2 Procedures on receiving a call

The SIP headers on the terminating side are populated according to the called-party's subscription of calling-party identity presentation/restriction.

B.3.2.1 In the case that calling-party identity, cause of no ID, etc., are notified

The calling-party identity and cause of no ID, etc. are notified by setting a `Privacy` header in requests outside existing dialogues received from a network.

In the case that "*none*" is set in the `Privacy` header, calling-party identity is notified by a `P-Asserted-Identity` header. In the `P-Asserted-Identity` header, only a SIP-URI is set or both a SIP-URI and a TEL-URI are set.

In the case that "*id*" is set in the `Privacy` header, calling-party identity is not notified by the `P-Asserted-Identity` header. Instead, cause of no ID is set in *display-name* in a `From` header. In the case that calling-party identity is not notified, a displayed content (meaning) may be provided as cause of no ID in the form indicated in Table B.4. Note that the cause of no ID is not provided in the case that a format is not as shown in Table B.4.

Table B.4 – Cause of no ID

Received content (Notes 1, 2)	Display content (meaning)
Anonymous	No caller ID: rejected by user
Coin line/payphone	No caller ID: call from public telephone
Interaction with other service	No caller ID: service conflict
Unavailable	No caller ID: service unavailable
NOTE 1 – It may be enclosed with a pair of double quotation marks. NOTE 2 – A character string listed in this table may be followed by a given character string.	

B.3.2.1.1 Displaying calling-party identity

A terminal displays calling-party identity notified by a `P-Asserted-Identity` header according to the order of priority described below.

1) In the case that both a SIP-URI and a TEL-URI are set in a `P-Asserted-Identity` header, the TEL-URI is preferred for display.
2) In the case that display-name is set in the URI of a `P-Asserted-Identity` header, *display-name* is preferred for display rather than *addr-spec*.

In the case that *display-name* is not set, *user* part of a SIP-URI, *local-number-digits* part or *global-number-digits* part of a TEL-URI is displayed, and this part is a character string indicated in the display content in Table B.5, a display content (meaning) corresponding to each case is indicated.

Table B.5 – Content of caller number display

Received content (Note)	Display content (meaning)
Only numbers	Received numeric string
Starting with +81, and the part after + is composed of only numbers	Numeric string that omits +81 and starts with 0
Starting with +, the part after + is all composed of numbers, and the part next to + is not 81	Numeric string that omits + and starts with 010
NOTE – When used as display-name, it may be enclosed with a pair of double quotation marks.	

B.3.2.2 In the case that calling-party identity, cause of no ID, etc. are not notified

A `Privacy` header and a `P-Asserted-Identity` header are not set, and a character string which indicates cause of no ID is not set in *display-name* in a `From` header.

B.4 Destination notification

A network may populate a `P-Called-Party-ID` header [RFC 3455] in requests outside existing dialogues to a called terminal, and may set a URI which indicates a network-asserted user identity of the destination.

In the case that multiple network-asserted user identities are allocated, a terminal uses a `P-Called-Party-ID` header in order to identity towards which network-asserted user identity a call is directed. In the case that the `P-Called-Party-ID` header is not set, it should be recognized that the call is directed to the default network-asserted user identity.

B.5 URI format in the case that a national number is used

This clause describes a URI format for the case using a national number as network-asserted user identity and `Request-URI`. Other URI formats may be used (Table I.20, Item 1).

A SIP-URI or a TEL-URI is used for network-asserted user identity. Either one or multiple SIP-URIs are allocated as network-asserted user identity for each user. A SIP-URI or a TEL-URI is used for `Request-URI`.

A subaddress described in clause B.6 may be set.

B.5.1 user part and local-number-digits part

In a SIP-URI, a numeric string of national number is described in *user* part, and in a TEL-URI, a numeric string of national number is described in *local-number-digits* part. Note that letters equivalent to *visual-separator* are not to be used in either *user* part or *local-number-digits* part.

In the case of `Request-URI`, a numeric string that a user dialled is set as it is in the *user* part or in the *local-number-digits* part. In the case of network-asserted user identity, all digits of a telephone number starting with a national prefix (i.e., "0") are set.

B.5.2 hostport part and descriptor part of context

The *hostport* part of a SIP-URI and the *descriptor* part of TEL-URI *context* are to be set as domain name or host name (including IP address) that a network specifies (Table I.20, Item 2).

B.6 Subaddress

A network may provide services that are equivalent to services realized by the transfer of subaddress information that can be provided in the ISUP network through the interconnection interface as defined in [TTC JJ-90.10] (Table I.9, Items 1 and

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

B.6.1 Subaddress information

B.6.1.1 Contents of subaddress information

The subaddress is a numeric string of 19 digits or less using numbers 0 to 9. The details are based on [RFC 4715] and [TTC TS-1008].

B.6.1.2 Formats of subaddress information

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

Annex C

Registration

(This annex forms an integral part of this Recommendation.)

C.1 Overview

This annex describes the procedures of terminal registration.

C.2 Obtaining the network address

A network provides a terminal with a means of notifying a SCF IP address and port number. The network provides DHCP/DHCPv6, presetting, and other procedures that depend on the access line (Table I.24, Item 2).

The terminal transmits SIP messages to the obtained IP address and port number.

C.3 Registration

A terminal registers by sending to a network a `REGISTER` request in which a `Contact address` that it wants to register is set. A network may determine the setting conditions of the *q* parameter to the `Contact address` (Table I.24, Item 6).

The network may specify the `expires` parameter of a `Contact address` or the value set to an `Expires` header in the `REGISTER` request as a network option (Table I.24, Item 4).

C.3.1 path extension function and Service-Route header

A network may provide a pre-existing route using path extension function and *Service-Route* header (Table I.7, Item 7; Table I.23, Item 1).

In the case that a network provides a pre-existing route, a terminal lists path extension function in `Supported` header as described in [RFC 3327] and sends a `REGISTER` request. In the case that registration succeeds, a network sets a `Service-Route` header [RFC 3608] in a `200 OK` response, and notifies the SIP-URI on or after the second hop of the pre-existing route.

C.3.2 pre-existing route

In the case that a pre-existing route is provided using procedures described in clause C.3.1, a terminal set the pre-existing route in `Route` header when sending requests outside existing dialogues except for `REGISTER`. The first hop of the `Route` header shall contain a SIP-URI of the obtained SCF address provided in clause C.2 with loose-routing specifier (i.e., ";lr"). The second and further hops of the `Route` header shall contain the given pre-existing route according to procedures as described in clause C.3.1. For a `REGISTER` request, pre-existing route is not provided.

C.3.3 Difference of address format retained by network

There may be a difference between a `Contact address` registered by a network and a `Contact address` set in a `REGISTER` request by a terminal. A terminal must be aware of it when verifying the `Contact address` URI.

– A URI parameter unrecognized by a network may not be retained.

– A `Contact address` may be retained in the format specifying no port number in a network, even if the default SIP port number (5060) is specified in the hostport part. The opposite could also be true that a `Contact address` may be retained in the format with the default port number (5060) in a network, even when the port number is not specified.

C.4 Refresh

In the case of receiving a `200 (OK)` response from a network indicating completion of registration or refresh, a terminal records the `Contact address` requested by the `REGISTER` request, and the retention period (Z s) returned by the `expires` parameter or in the `Expires` header field in the response.

Refresh interval (T s) MUST be set so that it does not exceed the retention period (Z s) and it does not cause frequent `REGISTER` request submissions. For example, setting the interval to a certain percentage of the retention period (Z s) is a good idea. The interval must be shorter than the value of the retention period (Z s) minus Timer F (=32 s) specified in [RFC 3261] period in order to avoid expiration during resending the `REGISTER` request for refreshing. The refresh interval may be specified as a network option (Table I.24, Item 5).

C.5 Deletion

Considering that a terminal may experience a sudden power cut off or an unexpected sequence during the shutdown process, the terminal should delete all `Contact addresses` that it registers after startup and before starting to register. A complete deletion should be performed by sending a `REGISTER` request which specifies * in `Contact address` and 0 in `Expires` header, in the event that the deletion of certain location information previously registered in some way cannot be guaranteed.

C.5.1 Considerations on terminal halt and IP address modification

A terminal should delete or update the `Contact address` registered in a network at times of rebooting, IP address modification, or application termination (in the case of softphone), etc.

C.6 Registration event

A network may provide a registration event (*reg* event) which notifies a terminal of its change of state from registered to unregistered as defined in [RFC 3680] (Table I.24, Item 8).

In the case that a terminal desires to receive a notification of its change of registration state after registration is completed, it can be notified by using a registration event package function.

C.6.1 Subscription to registration event

In the case that a terminal desires to receive a notification of its change of state from registered to unregistered, it sets the registration event in a `SUBSCRIBE` request and requests to the network a subscription to the change notification of registration state (i.e., *reg* event). In the case that a network provides a change notification of registration state, it accepts the subscription, sets the information of registration state in a `NOTIFY` request, and notifies a terminal in accordance with the procedure defined in [RFC 3265].

C.6.2 Notification of registration event

In the case that a terminal registration state is changed to unregistered, a network sets the unregistered state information in a `NOTIFY` request and notifies the terminal that subscribes to the registration event.

Annex D

SIP capabilities exchange

(This annex forms an integral part of this Recommendation.)

D.1 Overview

This annex describes procedures for capabilities exchange with SIP messages.

D.2 Available methods

This standard requires that methods of `INVITE`, `ACK`, `BYE`, and `CANCEL` are available in any `INVITE` sessions. However, the availability of other methods the network allows terminals to send is dynamically determined through a procedure of capabilities exchange. This clause and its subclauses describes the procedure.

D.2.1 UPDATE

A terminal asserts its capabilities to receive an `UPDATE` request by listing `UPDATE` in `Allow` header of initial `INVITE` request and `18x/2xx` responses to the `INVITE` request.

The terminal is allowed to send the `UPDATE` request in the case that the `Allow` header is set in the initial `INVITE` request or the `18x/2xx` response recently received, and `UPDATE` is listed in the header. In an early dialogue, a `PRACK` transaction must be completed before sending the `UPDATE` request.

D.2.2 PRACK

In the case that a `Require` header is set in a `1xx` response (excluding `100 (Trying)`) received, and `100rel` is listed in the header, the terminal sends a `PRACK` to this response.

D.3 Extension function

This clause describes the procedure for capabilities exchange to judge whether to be able to use extension function.

D.3.1 Session timer function (timer)

A terminal sets `timer` in a `Supported` header when sending an `INVITE` request and an `UPDATE` request, and by doing so asserts to a network that it supports the function (A `Require` header must not be set to assert the `timer` in the `INVITE` request and the `UPDATE` request).

D.3.2 Provisional response reliability function (100rel)

A terminal asserts its support of this function by listing `100rel` in a `Supported` header when sending an `INVITE` request (A `Require` header must not be set to assert the `100rel` in the `INVITE` request).

In the case that the terminal receives a `1xx` response (excluding `100 (Trying)`) to the `INVITE` request sent and the response contains `100rel` in the `Require` header, the terminal enables the `100rel` extension function only for this response, and sends a `PRACK` request.

Annex E

SDP and media handling

(This annex forms an integral part of this Recommendation.)

E.1 Overview

This annex supplements [RFC 4566] and [RFC 3264], and describes the procedure of media establishment and media change using SDP.

E.2 Judging a media change request

E.2.1 Receiving SDP

In the case that a terminal receives a re-`INVITE` or an `UPDATE` request including SDP, the terminal determines the request means a media change only when the `sess-version` value in `o=` line of the SDP is different from that of the SDP received as either offer or answer in the previous media establishment/change.

In the case that the terminal cannot perform the requested media change, it returns a `488 (Not Acceptable Here)` response, but it will not terminate the existing session. Whether the existing session would be terminated or not is left to the judgment of the terminal which requested a media change.

E.2.2 Sending SDP

In the case that an offer is made which lists multiple codecs (offer using RTP as media and listing several payload types in the *fmt* part of `m=` line), only part of the codecs are selected in the answer. In the case that this terminal sends afterwards a re-`INVITE` or `UPDATE` request which does not request a media change such as session refresh, it does not change the `sess-version` value in `o=` line as specified in section 7.4 of [RFC 4028], nor change the content of SDP excluding `sess-version` as specified in section 8 of [RFC 3264] accordingly. In the case that a session refresh is performed using an `UPDATE` request, it is recommended not to use SDP, in accordance with section 7.4 of [RFC 4028].

E.3 Payload type

In the case that the media is RTP and a payload type number is statically assigned to the codec in [RFC 3551], the assigned number is used in the `fmt` part of `m=` line. For example, in the case of ITU-T G.711 μ-law, 0 is used in the `fmt` part.

In the case that a dynamic payload type number is specified due to the specifications of the codec, and the codec is selected as answer, the specified number in the offer is set to `m=` line of answer.

Note that a network may specify the maximum number of codecs that can be set in the `fmt` part of `m=` line (Table I.21, Item 3).

E.4 Fallback procedure

E.4.1 IP version incompatibility

A terminal should return a `488 (Not Acceptable Here)` response which includes a `Warning` header whose `warn-code` is `300 (Incompatible network protocol)` or `301 (Incompatible network address formats)` when it received an initial `INVITE` and determined that the requested IPv6 communication is not possible.

A terminal may receive a `488 (Not Acceptable Here)` response which includes a `Warning` header whose `warn-code` is `300 (Incompatible network protocol)` or `301 (Incompatible network address formats)` to the initial `INVITE` request it sent. In the case of receiving the above response to the session initiation with IPv6, the terminal interprets that communication using IPv6 is not possible and may try fallback with IPv4. However, further session initiation is not conducted even if it receives a `488` response to its fallback call.

E.4.2 Media type incompatibility

If no acceptable media type is set in the received SDP, a terminal returns a `488 (Not Acceptable Here)` response. The terminal sets `304 (Media type not available)` as `warn-code` in a `Warning` header of the `488` response.

Annex F

Congestion prevention and control

(This annex forms an integral part of this Recommendation.)

F.1 Overview

This annex describes behaviours that a network and a terminal should follow in order to prevent or control congestion.

F.2 Considerations on congestion control at time of registration

When a network requires terminal registration (REGISTER) at the UNI, all the users in this network are bound to send REGISTER requests regularly, which generates a load on the network to constantly process a multitude of messages. Therefore, considerations are necessary on the terminal behaviour so that it will not generate unnecessary loads on the network at time of registration.

F.2.1 Actions on receiving an error response

After sending a REGISTER request, a terminal may receive an error response that includes a Retry-After header (a 4xx-6xx response: in [RFC 3261], 404 (Not Found) response, 413 (Request Entity Too Large) response, 480 (Temporarily Unavailable) response, 486 (Busy Here) response, 500 (Server Internal Error) response, 503 (Service Unavailable) response, 600 (Busy Everywhere) response, and a 603 (Decline) response). In such a situation, the network may have some kind of problems such as congestion. Therefore, to avoid any further congestion, terminal registration is retried after the time interval specified in the Retry-After header (Note that an error response may be received again even when resending the REGISTER request after the specified time).

In the case that an error response is received without a Retry-After header, terminal registration is retried after an appropriate period of time (except on receiving a 401 (Unauthorized) response) for the same reason.

F.2.2 Actions on receiving no response

A terminal may not be able to receive a response to a REGISTER request sent due to the retransmission timeout of SIP messages. An error may also occur in a layer below the SIP application layer (e.g., ICMP error notification). In such a situation, the terminal retries registration after an appropriate period of time (Table I.24, Item 7).

F.2.3 Considerations on registering multiple Contact addresses

Considerations should be given so that a terminal does not send a series of REGISTER requests in a short time in order to prevent unnecessary loads on a network triggered by the terminal registration behaviour, in such cases where one terminal manages multiple AoRs, it needs to register multiple Contact addresses in the network, and consequently it sends multiple REGISTER requests, etc.

F.2.4 User name or password error

In the case that a terminal receives a 401 (Unauthorized) response from a network after sending a REGISTER request containing an Authorization header, it should refrain from retrying registration using the same user name and password (excluding the case in which the value of the stale parameter in the WWW-Authenticate header is *TRUE*) so as to avoid the submission of unnecessary REGISTER requests.

F.2.5 Re-registration at the occurrence of temporary faults

If a terminal detects that it cannot send or receive SIP messages for some reason but it returns later to a state in which it can, it should immediately updates registration or re-registration regardless of the change of its `Contact address` or registration retention period.

However, to avoid network congestion due to simultaneous registration behaviours caused by simultaneous terminal recoveries following a wide-area failure in the access network, and to avoid unnecessary repetition of terminal registration behaviours due to intermittent temporary faults, the submission of `REGISTER` requests following fault recovery is made only at statistically uniform time intervals within an appropriate period of time. The network may specify a period of interval to resend the `REGISTER` request in the case that the network gives no reply (Table I.24, Item 7).

F.3 Considerations on congestion control when originating a call

The congestion may worsen if terminals attempts to make more calls (sending of requests outside existing dialogues except for `REGISTER`) to a network which already experiences congestion and call loss. Therefore, this clause describes a series of procedures so that in the case of congestion, the network notifies the terminal of the congestion state, the terminal notifies the user of the information notified by the network, and by doing so, the network notifies the user of the congestion state and attempts to control and prevent the user from redialling.

This clause and its subclauses also describe call retrial conditions so that congestion is not caused by a terminal's unlimited call retrials on receiving an error response when the call is made.

F.3.1 Congestion notification

This clause and its subclauses describe the error response format of congestion notification from the network, and required actions for terminals on receiving the notification.

F.3.1.1 Notification to a terminal from a network

In the case that a network cannot provide service to any request from a terminal due to congestion, etc., a `503 (Service Unavailable)` response is sent including a `Reason` header (`protocol` is *ITU-T Q.850* and `protocol-cause` is *42*: switching equipment congestion) to a request from the terminal, which means that the network cannot provide service. The network never sends to the terminal the response including the `Reason` header (`protocol` is *ITU-T Q.850* and `protocol-cause` is 42) due to a cause other than congestion.

Notification of additional information indicated in clause F.3.2.1 may be performed along with congestion notification described in this clause.

F.3.1.2 Notification from a terminal to a user

In the case that a terminal receives a `503 (Service Unavailable)` response in which a `Reason` [RFC 3326] header (`protocol` is *ITU-T Q.850* and `protocol-cause` is 42: switching equipment congestion) is set, it recognizes that a network cannot provide service to any request due to congestion, etc., and then performs visible indication to notify a user of the situation, or audible sound generation, such as a guidance to notify congestion or a signal tone to indicate congestion built into the terminal. Subsequent automatic behaviour, such as automatic call retrial, must not be performed.

In the case that additional information notification indicated in clause F.3.2.1 is performed at the same time, display of additional information indicated in clause F.3.2.1 is prioritized.

F.3.2 Additional information notification

This clause and its subclauses describe a procedure to notify a terminal of additional information from a network using a `Warning` header.

F.3.2.1 Notification from a network to a terminal

In the case that a network desires to provide additional information to a user when an error occurs, etc., it can notify a terminal of the information by including a `Warning` header in a response message sent back to the terminal, setting `399 (Miscellaneous warning)` as *warn-code*, and listing given text information in *warn-text*. The network must not send to the terminal the response in which the `Warning` header is set with *warn-code* `399`, excluding the case that the information intended to be notified to the user is included.

F.3.2.2 Notification from a terminal to a user

In the case that a terminal receives a response in which a `Warning` header is set with *warn-code* `399`, it should notify a user of this text information. In the case that the terminal can visibly indicate the text information, it should provide the user by actively indicating the information. In the case that the terminal can generate audible sounds, the implementation of the information e.g., giving an audio announcement of the information should be considered.

F.3.3 User name or password error

In the case that a terminal receives a `407 (Proxy Authentication Required)` response including a `Proxy-Authenticate` header from a network after sending a request, it should refrain from resending a request using the same user name and password, excluding the case in which the value of the *stale* parameter in the `Proxy-Authenticate` header is *TRUE*, or in which a `WWW-Authenticate` header or `Proxy-Authenticate` header exists that has the `realm` parameter set and has never been received.

Annex G

Bandwidth control

(This annex forms an integral part of this Recommendation.)

G.1 Overview

This annex describes a signalling procedure and its relationship with a transport layer protocol in the case that SIP/SDP is used as signalling procedure and the token bucket model specified in [ITU-T Y.1221] is used as policing function for the bandwidth control function which is characteristic of NGN.

This annex is written as if bandwidth control is performed utilizing the resource and admission control functions (RACF) described in [TTC TR-1014]; however realizing it through a different implementation is allowed provided that no difference in external behaviour is visible. Note that even in that case, it is required that the bandwidth control function conforming to this annex is provided, and the bandwidth requested by this function is reserved inside the network.

G.2 Bandwidth control mechanism in NGN

An NGN enables multiple services with different conditions (traffic characteristics, quality requirement conditions) in the same network. The NGN performs end-to-end (for UNI-UNI/UNI-NNI interconnections) quality control in order to realize this. This mechanism is absent in a best-effort network where communication quality is not guaranteed.

End-to-end quality control is composed of two functions stated below.

One of the functions is the RACF described in [TTC TR-1014]. In the NGN architecture, judgment of whether a bandwidth requested by a call connection procedure (SIP/SDP) is available for the terminal/network relationship is provided per media/quality class. In the case it is available, the NGN guarantees communication quality by allocating the bandwidth to the session and performing priority transfer processing according to the quality class. In the case it is unavailable, the NGN rejects the session admission because it is unable to allocate to the session a bandwidth for guaranteeing communication quality.

The other function is the policing function (traffic flow rate monitoring function) per media. This is a function to monitor whether there is an inflow of traffic exceeding a bandwidth allocated by the RACF. When the traffic exceeding the allocated bandwidth flows in, it not only hinders guaranteeing communication quality to the session, but also affects bandwidth allocated to other sessions. In order to avoid a situation of this kind, an NGN strictly monitors the inflow of traffic by the policing function per media, and releases the IP packets when it detects that the inflow of traffic is exceeding the allocated bandwidth. Therefore, a terminal needs to send the traffic so that the allocated bandwidth is protected to ensure communication quality necessary for the session.

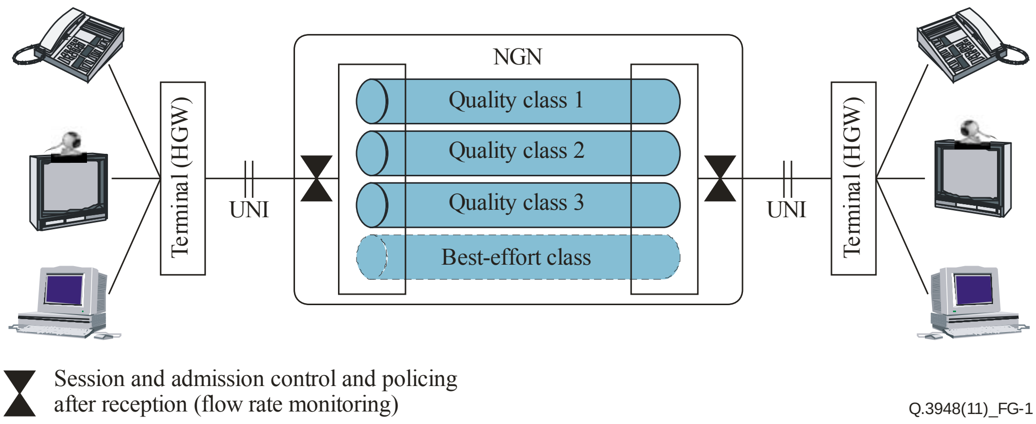

Figure G.1 – The image of end-to-end quality control in NGN

G.2.1 Resource and Admission Control Functions

In the NGN, judgment of whether a bandwidth requested by call control signals (SIP/SDP) is available between a terminal and a network is provided per media/quality class. This is called the Resource and Admission Control Function. (See section 4.1.2.1 in [TTC TR-1014].)

The image of the Resource and Admission Control Function is shown in Figure G.2. In the NGN, every time a bandwidth for a new session is requested, it is compared with an unused bandwidth per requested quality class, and when there is a bandwidth space available, it guarantees communication quality by admitting the session, allocating the bandwidth, and by performing priority transfer processing as per quality class. When there is no bandwidth, it means that the communication quality requested is not guaranteed, and therefore the admission of the session is rejected. As a matter of course, for the same volume of unused bandwidth, the smaller a requested bandwidth is, the more likely it becomes to be admitted. Also, for the same volume of network bandwidth, the smaller a requested bandwidth is, the more sessions which can be admitted there will be.

Whether each medium acts within the range of bandwidth allocated by the Resource and Admission Control Functions is monitored by the policing function as stated in the next clause G.2.2.

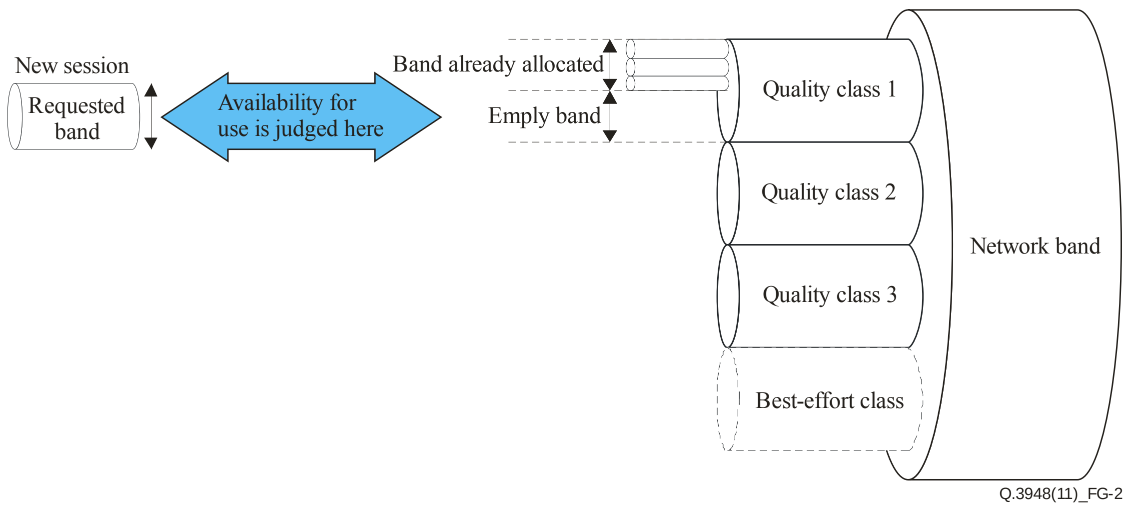

Figure G.2 – The image of session and admission control function

G.2.2 Policing function

The policing function (traffic flow rate monitoring function) is a function to monitor a traffic flow rate. It is a function that a network monitors whether traffic flows into the network following a bandwidth allocated to each medium by the Resource and Admission Control Functions as stated in clause G.2.1.

G.2.2.1 Behaviour of policer

As a specific policing function, a network monitors the inflow of traffic by the token bucket policer (see Appendix I and Appendix IV of [ITU-T Y.1221]).

Figure G.3 shows the behaviour overview of the token bucket policer.

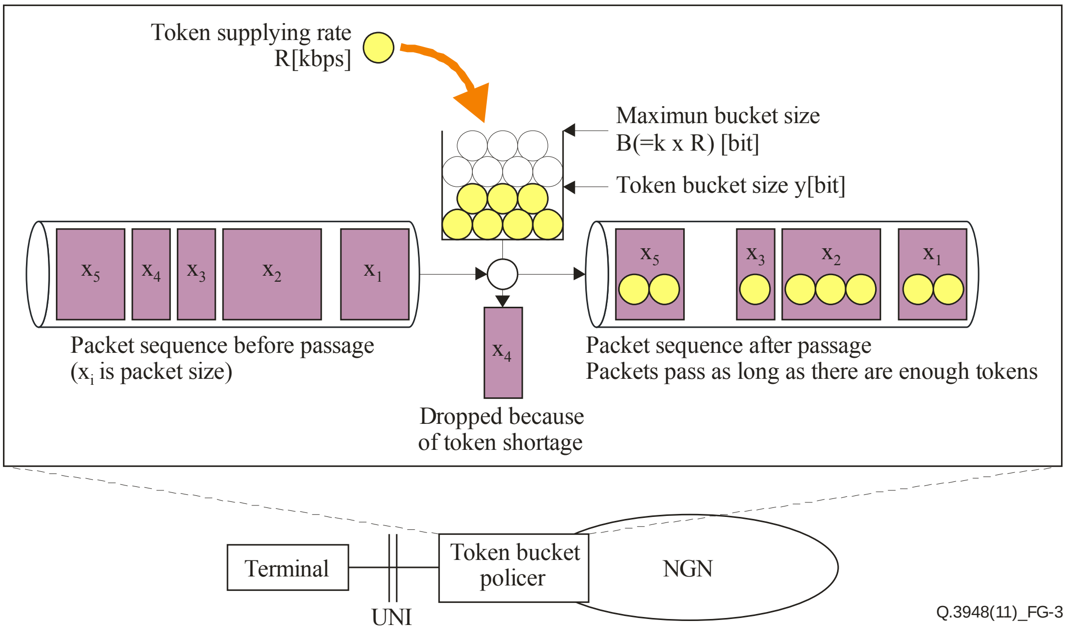

Figure G.3 – Behaviour overview of the token bucket policer

Token supplying rate (R[kbps]) is a rate equal to the bandwidth allocated to the media. For the specific contents of the token supplying rate (R), see clause G.2.2.2.

Maximum bucket size (B[bit]) is a value generally determined in proportion to the token supplying rate, and its proportionality coefficient (k[msec]) is a fixed value for each transfer quality class. This proportionality coefficient (k) is called rate coefficient.

Token bucket size (y[bit]) keeps getting supplied at a speed equal to the token supplying rate (R) until it reaches the maximum bucket size (B).

In the token bucket policer, an arrived packet size (x[bit]) is compared to a token bucket size (y) at that time.

In the case that x is equal to or less than y, the inflow packet is judged to be a conform packet, and is allowed to pass the policer. In this case, the token bucket size is consumed for the amount of x.

In the case that x is more than y, the inflow packet is judged to be a non-conform packet, and is dropped (not allowed to pass the policer). In this case, the token bucket size is not consumed.

Figure G.4 shows the time series for packet arrival and an example of token bucket size change.

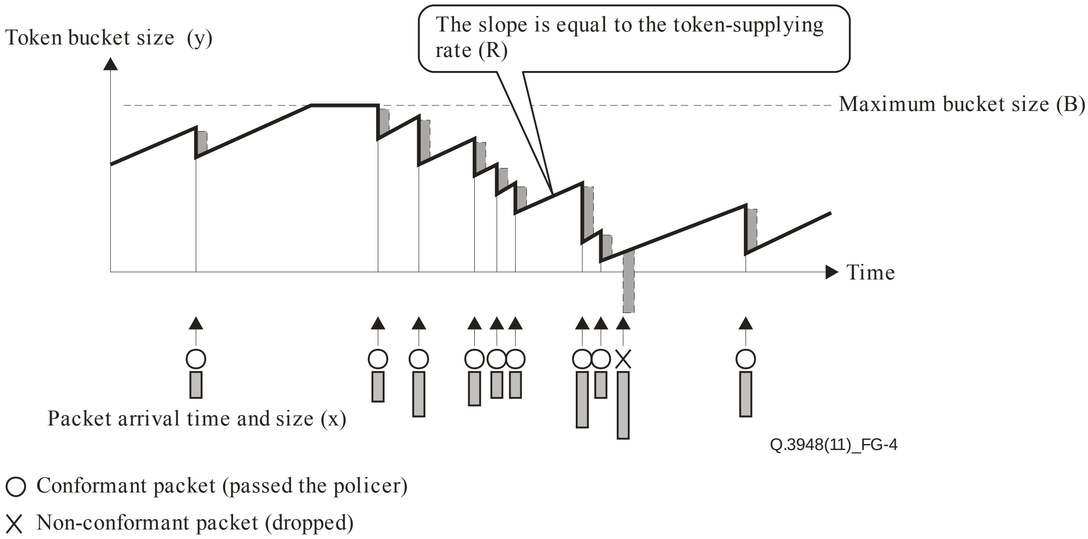

Figure G.4 – Time series for packet arrival and example of token bucket size change (image)

Note that the maximum bucket size and rate coefficient are determined by networks. These values may differ depending on quality classes shown in clause G.4 (Table I.13, Items 1 and 2).

G.2.2.2 Token supplying rate

Token supplying rate (R) is a value specified in a `b=` line of SDP, according to Appendix IV in [ITU-T Y.1221].

Note that in audio communication, a network may specify a specific token supplying rate to codecs and apply it instead of declaration from a terminal using a `b=` line (Table I.13, Item 3).

G.3 SIP/SDP specifications

Indicated here are specifications on SIP/SDP at the UNI regarding the NGN bandwidth control function shown in the previous clause.

G.3.1 Specifying RTP bandwidth

For the media using RTP, a token supplying rate is set in a `b=AS` line of this media.

Indicated in clauses G.3.1.1 and G.3.1.2 are points that need special caution for values of a `b=AS` line.

G.3.1.1 Considerations on overhead in lower layers

Take note of overhead, such as in headers of lower layers indicated in section 5.8 of [RFC 4566].

Bandwidth specified in a `b=AS` line include those of layer 4 and layer 3 described in section 6.2 of [RFC 3550]. Specifically speaking, those bandwidth specified in a `b=AS` line include the RTP header, UDP header and IP header, but do not include overhead of layer 2 protocol, such as the frame header of Ethernet.

G.3.1.2 Considerations on burstiness

In a traditional best-effort network, bandwidth has often been described by the average rate of a long period (e.g., by the unit of second). On the other hand, in an NGN, bandwidth is managed by the average rate of a short period (e.g., by the unit of dozens of milliseconds) determined by the token bucket policer. In designing an NGN terminal, caution is needed on the discrepancy between this long-term average rate and short-term average rate specified by a `b=AS` line.

A characteristic to send a large quantity of traffic continuously in a short time is called burstiness. Caution is needed that in the long-term average rate, packets may be dropped by the token bucket policer if the burstiness of sending traffic is high, even in the case that the traffic is of equal to or less than the rate specified in a `b=AS` line of SDP.

Cautionary notes are given below in the case of video communication whose burstiness tends to be particularly high.

– In video, encoding is performed by the unit of frame, and burstiness is high in the case of sending one frame of encoded data at one time. It is recommended to conduct shaping in sending RTP packets and send them out as constant traffic.

– In moving picture codecs, the inter-frame compression technology is generally used, and the data size of frames that performs only intra-frame compressing tends to be larger than that of frames that performs inter-frame compressing, which constitutes a factor to generate burstiness. It is recommended that traffic be smoothed by either adjusting the allocation of a bit rate to each frame and averaging it in performing encoding, or shaping in sending RTP packets.

G.3.2 RTCP bandwidth

The value to be specified in a `b=AS` line is RTP bandwidth, and does not include RTCP bandwidth.

For specifying RTCP bandwidth, a `b=RR` line and a `b=RS` line may be used as defined in [RFC 3556] (Table I.13, Item 4).

In the case that a `b=RR` line and a `b=RS` line are used, they are used as the value of token rate for RTCP.

In the case that a `b=RR` line and a `b=RS` line are not used, it is recommended to set the RTCP bandwidth at 5 percent of RTP bandwidth, as described in section 6.2 of [RFC 3550] (Table I.13, Item 5).

G.4 Quality class

In an NGN, multiple services with different conditions are provided in the same network, as described in clause G.2.

For example, in the case that http communication using Web browsers, etc. and IP telephone communication with 0AJ numbers are provided in the same network, quality of service (QoS) provided in each service differs in general.

This annex describes about the transfer quality of IP packets. In particular, IP packet transfer delay (IPTD), IP packet delay variation (IPDV) and IP packet loss ratio (IPLR), which are defined in [ITU-T Y.1540], are described. The other service-specific factors for the QoS are not discussed in this annex. The transfer quality of IP packets defined by this combination of IPTD, IPDV, and IPLR are referred to as "quality class". Note that providing quality class is determined by a network (Table I.13, Item 6).

G.4.1 Multiple quality classes and DiffServ

In NGN, service oriented quality class is made possible by allocating network resources per quality class, and a quality class per service. For instance, in the example of clause G.4, for http communication by web browsers, a quality class as best-effort communication which does not guarantee IPTD, IPDV, and IPLR is allocated. Likewise, for IP telephone communication with a 0AJ numbers, a quality class which guarantees IPTD, IPDV, and IPLR is allocated.

To meet the conditions defined for each quality class, the quality class of IP packets used in each communication needs to be identified in the NGN access network and core network, and the IP packets are handled appropriately to each quality class. Therefore, transfer is prioritized using the

DSCP value of IP packets, utilizing DiffServ, which is specified in [RFC 2474] and [RFC 2475], based on [ITU-T Y.1221] Appendix III. The network specifies DSCP value of DiffServ to be applied to the UNI (Table I.13, Item 7).

G.4.2 Setting of DSCP value

Priority control of IP packets is needed for the whole areas of UNI-UNI and UNI-NNI communication, in order to provide an NGN end-to-end quality class. Therefore, DSCP values are set to IP packets by a terminal and a network as follows.

– In order to appropriately perform priority control for the UNI zone, a terminal sets DSCP values when sending IP packets to a network

– In order to appropriately perform priority control inside a network, the network may change or normalize DSCP values when bringing inside the network IP packets received from a terminal.

Annex H

Constraints on string length and value range of SIP messages

(This annex forms an integral part of this Recommendation.)

H.1 Overview

This annex clarifies the maximum length of character string (hereinafter referred to as "string length") and value range of integer fields (hereinafter referred to as "value range") regarding SIP and SDP.

H.2 String length and value range

Indicated here are conditions that a terminal must receive and appropriately process messages from a network (terminal's receiving conditions). The terminal may be equipped with receiving capabilities higher than those described in this annex. Conditions of messages that are allowed to send from the terminal to the network are the same as those of receiving capabilities, but the network may set different conditions. The network may also add conditions to ones in this clause or make them more detailed (Table I.21, Items 1 and 2).

Note that the string length and value range unlisted in this annex conform to each document referred to in this standard.

H.2.1 SIP

Table H.1 shows the constraints on string length and value range for SIP along with recommended conditions. In the explanation of each item, field names of the ABNF grammar as indicated in section 25.1 of [RFC 3261] are used for clarification.

Table H.1 – String length and value range for SIP

Item		String length and value range	Remarks
General	String length per line of SIP message (*Request-Line*, *Status-Line*, *message-header*)	Equal to or less than 255 bytes including the end of line (CR+LF)	
Dialogue and route management	The number of *Via* hops (the number of `via-parm` parameters)	Equal to or less than 10 hops	
	String length of the *Via* branch (`via-branch`)	Equal to or less than 128 bytes, including z9hG4bK	
	String length of the `To/From` tag (*token* in `tag-param`)	Equal to or less than 128 bytes	
	String length of *Call-ID* (`callid`)	Equal to or less than 128 bytes	
	The number of URIs that constitute the Route Set	Equal to or less than 10 hops	
	String length per URI (`rec-route`) for *Record-Route*	Equal to or less than 128 bytes	
	String length of *Contact address* (`contact-param`)	Equal to or less than 128 bytes	

Table H.1 – String length and value range for SIP

Item		String length and value range	Remarks
Originating and Terminating URIs	String length for the originating URI (`Request-URI`)	Equal to or less than 128 bytes	
	String length per URI of the `P-Preferred-Identity` and `P-Asserted-Identity`	Equal to or less than 128 bytes	
Terminal registration	SIP-URI to which a `REGISTER` is sent (`Request-URI` of a `REGISTER` request)	Equal to or less than 32 bytes	
	String length of `realm` at time of HTTP Digest authentication	Equal to or less than 64 bytes	
	String length of `user name` at time of HTTP Digest authentication	Equal to or less than 32 bytes	
	String length of password at time of HTTP Digest authentication	Equal to or less than 32 bytes	

H.2.2 SDP

Table H.2 shows the constraints on string length and value range for SDP along with recommended conditions. In the explanation of each item, field names of the ABNF grammar indicated in section 9 of [RFC 4566] are used for clarification.

Table H.2 – Character string length and set value conditions for SDP

Item		String length and value range	Remarks
General	String length per line of SDP	Equal to or less than 255 bytes including the end of a line (CR+LF)	
	Length of SDP (`session-description`)	Equal to or less than 1000 bytes (when using UDP)	
o=	String length of `username` in `o=` line	Equal to or less than 64 bytes	
	Value range of `sess-id` in `o=` line	63-bit nonnegative integer (0 to 2^{63}–1)	Section 5 in [RFC 3264]
	Value range of `sess-version` in `o=` line	63-bit nonnegative integer (0 to 2^{63}–1)	
s=	String length of `text` in `s=` line	Equal to or less than 64 bytes	

Annex J

Audio terminal behaviour

(This annex forms an integral part of this Recommendation.)

J.1 Overview

This annex describes the behaviours specific to a telephone terminal or TV telephone terminal, etc. featured out of NGN terminals.

J.2 Codec

Support for ITU-T G.711 μ-law (64kbit/s) as defined in [ITU-T G.711] is mandatory. It is recommended that the packet loss concealment (PLC) function as defined in Appendix I of [ITU-T G.711] be provided.

J.2.1 Packetization period

In the case that ITU-T G.711 μ-law is included in SDP negotiation, a terminal must support 20 ms as the packetization period for ITU-T G.711 μ-law.

In the case that an `a=ptime` line is set in ITU-T G.711 μ-law for SDP offer, it is recommended to set 20 ms as packetization period. A network may specify setting conditions for the `a=ptime` line and values to be set as packetization period (Table I.15, Items 1 and 2).

In the case that an `a=ptime` line is set in ITU-T G.711 μ-law for SDP answer, the packetization period set in the `a=ptime` line in the offer is specified. In the case that the `a=ptime` line is not set in the offer, 20 ms is set for SDP answer. The network may specify the setting conditions for the `a=ptime` line (Table I.15, Item 1).

J.3 Behaviour at time of disconnection

At the time of user operation to disconnecting a call, a variety of unexpected states can be considered in SIP message sequences. For example, resending of `CANCEL` requests with no response, receiving no final response to initial `INVITE` request, resending of `BYE` requests with no `200 (OK)` response, and so on. In any cases, it must be possible for the terminal to send or receive a new initial `INVITE` request accompanying the outgoing or incoming of a new call in parallel with such states.

J.3.1 Sending a CANCEL/BYE request

After a terminal sends a `CANCEL` request to perform call cancellation caused by a user operation (at the time of an on-hook behaviour, application termination, etc.) and so forth, the terminal must be possible to create the next `INVITE` transaction and send out a new initial `INVITE` request when a new call request has been issued by the user – even if the terminal could not receive `2xx` response to the `CANCEL` request, or the terminal could not receive final response to the Initial `INVITE` request after `2xx` response of `CANCEL` request received. If a new call is issued during cancellation of the previous call, the terminal shall maintain both of them.

When the terminal detects the call disconnection of the user resource while the call is in progress, and has not received a `BYE` request, it sends a `BYE` request that releases the dialogue and performs releasing the dialogue/media/user resource. Regardless of the `BYE` transaction state (such as a BYE-request-resend state or error-response-receive state), it shall be possible to send or receive an initial `INVITE` request for a new outgoing or incoming call.

J.3.2 Receiving a CANCEL/BYE request (before final response)

In the case that a terminal receives a CANCEL request or a BYE request while still in the state that it has not sent the final response to an initial INVITE request, it performs stops/releases processing of the user resources after sending the response to the request and initial INVITE request. In this case, if a 487 (Request Terminated) response is in the process of being resent due to the non-receipt of an ACK request, the terminal must still be able to perform, in parallel, the sending or receiving of an initial INVITE request due to a new outgoing or incoming call.

In the case of receiving a BYE request while a call is in progress, the terminal sends a response to the BYE request, and sends the user resource a Busy Tone or performs an equivalent behaviour.

J.3.3 Receiving a CANCEL request (after final response)

Up to the time that an ACK request is received after a called terminal sends a 2xx response in reply to an initial INVITE request, a CANCEL request may be received to that INVITE transaction or dialogue. In this case, the called terminal should use the receipt of the CANCEL request as a trigger to send a Busy Tone (or to perform an equivalent behaviour) for the called user resource so as to notify it that a disconnect has occurred on the caller.

On receiving the CANCEL request after sending the 200 (OK) response as described above, the called terminal may enter into a state in which 200 (OK) responses are being resent due to the non-receipt of an ACK request or in which a BYE request has not yet been received after receiving the ACK request. In this state, the terminal must still be able to perform, in parallel, the sending or receiving of an initial INVITE request due to a new outgoing or incoming call.

J.3.4 Receiving a 3xx response

In the case that a terminal receives a 3xx response to the initial INVITE request, and does not send an initial INVITE request to the destination specified in a Contact header included in the response, it stops calling on receiving the 3xx response, runs a busy tone etc. to the user and notifies that a call cannot be made.

J.3.5 Receiving a 4xx to 6xx response

In the case that a terminal receives a 4xx to 6xx response to the initial INVITE request, and does not perform retransmission for authentication or fallback (restarting a call based on changed media conditions of SDP, etc.), it stops calling on receiving the 4xx to 6xx response and indicates a busy tone, etc. to the user, notifying her or him that a call cannot be made.

In particular, in the case that the terminal receives a 503 response in the format indicated in clause F.3.1.1 and clause F.3.2.1 it notifies it to the user for congestion control, based on clause F.3.1.2 and clause F.3.2.2.

J.3.6 Sending a 4xx to 6xx response

In the case of sending a 4xx to 6xx response to the initial INVITE request, a terminal must be able to process the sending or receiving of an initial INVITE request, in parallel, when the user resource is able to process the sending or receiving of a new call in the state that it is still waiting for an ACK request.

J.4 Ringing tone generation and dialogue management

J.4.1 Sending a 18x response

In the case that a precondition extension function is not used, a terminal must not send a 1xx (excluding 100 (Trying)) response until the user calling state can be ascertained (e.g., up until an extension-designation receive-completion signal is received from the user (such as a PBX) assuming that the user resource is a two-wire analogue interface and that a dial-in sequence is used, or up until a receive-completion signal is received from an information-receiving terminal in the case of a "Number-Display" sequence), and must send it as soon as the user calling state can be ascertained.

A network specifies whether to allow or disallow setting SDP to the sending of the 1xx response by the terminal (Table I.22, Item 1).

J.4.2 Receiving a 18x response

J.4.2.1 Ringing tone generation

In the case that a 180 (Ringing) response without SDP is received before receiving any *1xx* (excluding 100 (Trying)) response with SDP, a terminal must generate a ringing tone using its own sound source from that point. Then, within the same dialogue, the ringing tone must continue to be generated as long as any subsequently received 1xx response does not include SDP (in other words, the ringing tone must not be restarted). However, if SDP is included in a 1xx response, a media path must be connected as described in clause J.4.2.2 and a sound must be generated from the network.

J.4.2.2 Early media generation

In the case of receiving a 1xx response with SDP set, a terminal must be able to establish early media by connecting a path. The received media must continue to be generated, with or without SDP in any subsequently received 1xx response for the same dialogue (i.e., reprocessing of that media must not take place).

J.4.2.2.1 Media modification by an UPDATE request

In the case that media modification specified in an offer from the network by an UPDATE request is acceptable to the terminal, the terminal must return a 200 (OK) response including an appropriate answer and modify the media. In the case that the specified media modification cannot be performed, it must return a 488 (Not Acceptable Here) response. Note that disconnection processing of the existing session is not performed from the terminal after returning the 488 (Not Acceptable Here) response.

A network specifies whether to allow or disallow sending the UPDATE in the early dialogue by the terminal (Table I.23, Item 1).

J.4.2.2.2 Management of multiple dialogues and media

Because a terminal may receive multiple 1xx (excluding 100 (Trying)) responses whose To-tags are different from each other, the terminal must be able to establish multiple dialogues for one initial INVITE request. In addition to any existing dialogue (or dialogues), a terminal must create a new dialogue when it receive a response with a new To-tag.

The terminal must also be able to accommodate multiple dialogues using different media.

Table J.1 summarizes the mandatory or recommended implementation of calling terminal taking the above requirements into account.

Table J.1 – Management of multiple dialogues and media (calling SIP terminal)

	Existing dialogue	New dialogue	Processing
1	Early dialogue	Early dialogue	On receiving a new response, the terminal may select a dialogue used to its user interface under a certain policy. The policy takes into account the presence of SDP, the content of SDP, etc. If using `100rel`, however, a `2xx` response may be received without an SDP answer, in which case it is recommended that all media information be saved or send `BYE` requests to disconnect the early dialogues explicitly. If there are no information for making a decision, the newer dialogue is selected (taking into account call forwarding no reply, etc.).

J.4.3 Receiving a 2xx response

In the case that an SDP answer was received by a `1xx` response belonging to the same dialogue as a `2xx` response before the terminal received the `2xx` response, the content of the SDP included in the `2xx` response is expected to be the same as the previously established media and is therefore ignored. If an SDP answer was not received before receiving the `2xx` response, the session is established according to the SDP answer included in the `2xx` response.

J.4.3.1 Management of multiple dialogues and media

Because a terminal may receive multiple `2xx` responses whose `To`-tags are different from each other, the terminal must be able to establish multiple dialogues for one initial `INVITE` request. In addition to any existing dialogue (or dialogues), a terminal must create a new dialogue when it receives a response with a new `To`-tags.

The terminal must also be able to accommodate multiple dialogues using different media.

Table J.2 summarizes the mandatory or recommended implementation of calling terminal taking the above requirements into account.

Table J.2 – Management of multiple dialogues and media (calling SIP terminal)

	Existing dialogue	New dialogue	Processing
1	Early dialogue	Confirmed dialogue	Changes the media according to the content of the confirmed dialogue. The remaining early dialogue is either explicitly disconnected by sending a `BYE` request or its content is abandoned after 64 × T1.
2	Confirmed dialogue	Confirmed dialogue	On receiving a new response, the terminal may select a dialogue under a certain policy. The policy takes into account SDP content, etc. When the terminal select a dialogue, the other dialogue should be explicitly released by sending a `BYE` request (no return of `ACK` requests will result in more retransmissions of `2xx` responses).

J.5 Media change

J.5.1 IP address and port number

When receiving a media-change request involving the changing of IP addresses or port numbers (or both), the terminal must be equipped with the capability of making those changes.

Appendix I

Option items

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

I.1 Introduction

The following tables show the option items of [ITU-T Q.3402]. The objective of these tables is to enhance interoperability between NGN and SIP terminals through UNI. NGN carriers are allowed to select each "UNI condition" option item, and terminals are allowed to select each "Terminal selection" option item as far as the choice is allowed by "UNI condition" selected by the NGN carrier to which the terminal is willing to connect.

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

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

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

I.2 Option item extraction policy

Option items are extracted from a following viewpoint:

The option items are extracted to improve interoperability of SIP terminals connected to the network through the UNI, and classified into different categories for ease of reference.

I.3 Option item table format

Table I.1 shows and explains the format of the option item table presented here.

Table I.1 – Format example

<table>
<tr><th>Item</th><th>Name of option</th><th colspan="2">UNI condition</th><th>Terminal selection</th><th>Relevant items
(reference clauses, etc.)</th><th>Special notes</th><th>Remarks</th></tr>
<tr><td rowspan="3">1</td><td rowspan="3">IPv4</td><td rowspan="3">Provides IPv4 connection</td><td>Terminal is required to be equipped with IPv4 connection function</td><td>May connect with IPv4</td><td rowspan="3">Clause 13</td><td rowspan="3"></td><td rowspan="3"></td></tr>
<tr><td rowspan="2">Terminal may be equipped with IPv4 connection function</td><td>May connect with IPv4</td></tr>
<tr><td>Not connect with IPv4</td></tr>
</table>

Table I.1 – Format example

Name of option:	shows option items.
UNI condition:	shows patterns that a network can select as UNI conditions.
Terminal selection:	shows patterns that a terminal can select compared to network selection.
Relevant items:	shows for each option item, relevant clauses of [ITU-T Q.3402].
Special notes:	shows option items that should be determined in addition to "UNI condition" and "Terminal selection" columns. Special notes for "UNI condition" and "Terminal selection" are shown within the brackets of [ ] and << >>, respectively.

I.4 Option item table

Option item tables are shown in Tables I.2 to I.25. Items that shall be supported in the main body and annexes are not explicitly shown in the tables.

Table I.2 – SIP methods

Item	Name of option	UNI condition	Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
1	`REGISTER` [Terminal sends]	Terminal is required to register by `REGISTER`	–	Clause 10.2.1.10 Clause 10.2.3	[In case of using `REGISTER`, `Contact address` types and the number of them are listed here.]	
		Terminal is required not to register by `REGISTER`	–			
2	`MESSAGE` (outside existing dialogues) [Terminal sends]	Allow	May send	Clause 10.1 Table 10-2/ [RFC 3428] Clause 10.2.3	<<In the case that terminal sends, `Content-Type` and message body format are listed here.>>	
			Not send			
		Disallow	Not send			
3	`MESSAGE` (outside existing dialogues) [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 10-2/ [RFC 3428] Clause 10.2.3	<<In the case that terminal is equipped with receiving function, `Content-Type` and message body format are listed here.>>	
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
4	`MESSAGE` (inside existing dialogues) [Terminal sends]	Allow	May send	Clause 10.1 Table 10-2/ [RFC 3428] Clause 10.2.3	<<In the case that terminal sends, `Content-Type` and message body format are listed here.>>	
			Not send			
		Disallow	Not send			

Table I.2 – SIP methods

Item	Name of option	UNI condition	Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
5	`MESSAGE` (inside existing dialogues) [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 10-2/ [RFC 3428] Clause 10.2.3	<<In the case that terminal is equipped with receiving function, `Content-Type` and message body format are listed here.>>	
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
6	`REFER` (outside existing dialogues) [Terminal sends]	Allow	May send	Clause 10.1 Table 10-2/ [RFC 3515] Clause 10.2.3		
			Not send			
		Disallow	Not send			
7	`REFER` (outside existing dialogues) [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 10-2/ [RFC 3515] Clause 10.2.3		
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
8	`REFER` (inside existing dialogues) [Terminal sends]	Allow	May send	Clause 10.1 Table 10-2/ [RFC 3515] Clause 10.2.3		
			Not send			
		Disallow	Not send			

Table I.2 – SIP methods

Item	Name of option	UNI condition	Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
9	REFER (inside existing dialogues) [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 10-2/ [RFC 3515] Clause 10.2.3		
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
10	SUBSCRIBE (outside INVITE dialogues) [Terminal sends]	Allow	May send	Clause 10.1 Table 10-2/ [RFC 3265] Clause 10.2.3	<<In the case that terminal sends, the event names are listed here.>>	
			Not send			
		Disallow	Not send			
11	SUBSCRIBE (outside INVITE dialogues) [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 10-2/ [RFC 3265] Clause 10.2.3	<<In the case that terminal is equipped with receiving function, the event names are listed here.>>	
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
12	SUBSCRIBE (inside INVITE dialogues) [Terminal sends]	Allow	May send	Clause 10.1 Table 10-2/ [RFC 3265] Clause 10.2.3	<<In the case that terminal sends, the event names are listed here.>>	
			Not send			
		Disallow	Not send			

Table I.2 – SIP methods

Item	Name of option	UNI condition	Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
13	`SUBSCRIBE` (inside `INVITE` dialogues) [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 10-2/[RFC 3265] Clause 10.2.3	<<In the case that terminal is equipped with receiving function, the event names are listed here.>>	
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
14	`NOTIFY` [Terminal sends]	Allow	May send	Clause 10.1 Table 10-2/[RFC 3265] Clause 10.2.3	<<In the case that terminal sends, the event names are listed here.>>	
			Not send			
		Disallow	Not send			
15	`NOTIFY` [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 10-2/[RFC 3265] Clause 10.2.3	<<In the case that terminal is equipped with receiving function, the event names are listed here.>>	
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
16	`PUBLISH` (outside `INVITE` dialogues) [Terminal sends]	Allow	May send	Clause 10.1 Table 10-2/[RFC 3903] Clause 10.2.3	<<In the case that terminal sends, the event names are listed here.>>	
			Not send			
		Disallow	Not send			

Table I.2 – SIP methods

Item	Name of option	UNI condition	Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
17	PUBLISH (outside INVITE dialogues) [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 10-2/ [RFC 3903] Clause 10.2.3	<<In the case that terminal is equipped with receiving function, the event names are listed here.>>	
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
18	PUBLISH (inside INVITE dialogues) [Terminal sends]	Allow	May send	Clause 10.1 Table 10-2/ [RFC 3903] Clause 10.2.3	<<In the case that terminal sends, the event names are listed here.>>	
			Not send			
		Disallow	Not send			
19	PUBLISH (inside INVITE dialogues) [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 10-2/ [RFC 3903] Clause 10.2.3	<<In the case that terminal is equipped with receiving function, the event names are listed here.>>	
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
20	Other methods [Terminal sends]	Allow	May send	Clause 10.2.3	[In the case that network allows the use, the method name are listed here.] <<In the case that terminal sends, the method names are listed here.>>	
			Not send			
		Disallow	Not send			

Table I.2 – SIP methods

Item	Name of option	UNI condition	Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
21	Other methods [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.2.3	[In the case that network requests that terminal is equipped with receiving function, the method names are listed here.] <<In the case that terminal is equipped with receiving function, the method names are listed here.>>	
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			

Table I.3 – IP version and IP extension function

Item	Name of option	UNI condition		Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
1	IPv4	Provide IPv4 connection	Terminal is required to be equipped with IPv4 connection function	May connect with IPv4	Clause 13		
			Terminal may be equipped with IPv4 connection function	May connect with IPv4			
				Not connect with IPv4			
2	IPv6	Provide IPv6 connection	Terminal is required to be equipped with IPv6 connection function	May connect with IPv6	Clause 13		
			Terminal is not required to be equipped with IPv6 connection function	May connect with IPv6			
				Not connect with IPv6			
		Not provide IPv6 connection	Terminal does not connect with IPv6	–			
3	IP versions of call control signals and media	Allow only the same IP version		Use the same IP version	Clause 13		
		Allow the same or different IP version		Use the same IP version			
				Use the same or different IP version			

Table I.3 – IP version and IP extension function

Item	Name of option	UNI condition		Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
4	Use of IPsec for call control signals	Provide IPsec connection	Terminal is required to be equipped with IPsec connection function, and always use IPsec.	–	Clause 13	[In the case that IPsec connection is provided, conditions are listed here.]	
			Terminal is not required to be equipped with IPsec connection function.	May connect with IPsec			
				Not connect with IPsec			
		Not provide IPsec connection	Terminal does not connect with IPsec.	–			

Table I.4 – Layer 4 protocol for call control signals

Item	Name of option	UNI condition		Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
1	UDP	Provide UDP connection	Terminal is required to be equipped with UDP connection function.	May connect with UDP	Clause 12	[In the case that a port number other than the default number (5060) is used for sending or receiving, describe the port number here.]	
			Terminal is not required to be equipped with UDP connection function.	May connect with UDP			
				Not connect with UDP			
		Not provide UDP connection	Terminal does not connect with UDP.	–			

Table I.4 – Layer 4 protocol for call control signals

Item	Name of option	UNI condition		Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
2	TCP (no TLS)	Provide TCP connection	Terminal is required to be equipped with TCP connection function.	May connect with TCP	Clause 12	[In the case that a port number other than the default number (5060) is to be listened, describe the port number here.]	
			Terminal is not required to be equipped with TCP connection function.	May connect with TCP			
				Not connect with TCP			
		Not provide TCP connection	Terminal does not connect with TCP.	–			
3	TCP (with TLS)	Provide TLS connection (Note)	Terminal is required to be equipped with TLS connection function.	May connect with TLS	Clause 12	[In the case that a port number other than the default number (5061) is used for listen, describe the port number here.]	
			Terminal is not required to be equipped with TLS connection function.	May connect with TLS			
				Not connect with TLS			
		Not provide TLS connection	Terminal does not connect with TLS.	–			
NOTE – In the case that authentication is performed when using TLS connection, HTTP Digest authentication must be selected as the authentication procedure in Table I.11, Items 1 and 2.							

Table I.5 – SigComp

<table>
<tr><th>Item</th><th>Name of option</th><th colspan="2">UNI condition</th><th>Terminal selection</th><th>Relevant items
(reference clauses, etc.)</th><th>Special notes</th><th>Remarks</th></tr>
<tr><td rowspan="4">1</td><td rowspan="4">Use of SigComp</td><td>Use in all sessions</td><td>Terminal is required to be equipped with this function, and performs sending and receiving using this function in all messages.</td><td>–</td><td rowspan="4">Clause 10.1
Table 10-2/ [RFC 3320]
Table 10-2/ [RFC 3485]
Table 10-2/ [RFC 3486]
Table 10-2/ [RFC 5049]</td><td rowspan="4"></td><td rowspan="4"></td></tr>
<tr><td rowspan="2">Use in each session as necessary</td><td rowspan="2">Terminal has receiving function of signals using this function.</td><td>May send signals using this function</td></tr>
<tr><td>Not send signals using this function</td></tr>
<tr><td>Not use</td><td>Terminal does not send signals using this function, and if received, ignore them.</td><td>–</td></tr>
</table>

Table I.6 – Hosted NAT

<table>
<tr><th>Item</th><th>Name of option</th><th>UNI condition</th><th>Terminal selection</th><th>Relevant items
(reference clauses, etc.)</th><th>Special notes</th><th>Remarks</th></tr>
<tr><td rowspan="3">1</td><td rowspan="3">Allowing Hosted NAT in the lower part of the UNI (inside the user's residence)</td><td rowspan="2">Allow</td><td>Use Hosted NAT</td><td rowspan="3">Clause 10.1
Table 10-2/ [RFC 3581]</td><td rowspan="3"></td><td rowspan="3"></td></tr>
<tr><td>Not use Hosted NAT</td></tr>
<tr><td>Disallow</td><td>Not use Hosted NAT</td></tr>
</table>

Table I.7 – SIP option tags

<table>
<tr><th>Item</th><th>Name of option</th><th colspan="2">UNI condition</th><th>Terminal selection</th><th>Relevant items
(reference clauses, etc.)</th><th>Special notes</th><th>Remarks</th></tr>
<tr><td rowspan="3">1</td><td rowspan="3">Session timer function (`timer`)</td><td>Use in all sessions</td><td>Terminal is required to be equipped[a)] with this function, accepts if required[b)], assert[c)], and requires[d)] if asserted.</td><td>–</td><td rowspan="3">Clause 10.2.1.20.32</td><td rowspan="3">[In the case of specifying a session timeout period, describe the `delta-seconds` values here.]</td><td rowspan="3"></td></tr>
<tr><td rowspan="2">Use in each session as necessary</td><td rowspan="2">Terminal is required to be equipped with this function, and accepts if required.</td><td>Assert, and require if asserted</td></tr>
<tr><td>May not assert, or may not require.</td></tr>
<tr><td rowspan="5">2</td><td rowspan="5">Provisional response reliability function (`100rel`)</td><td>Use in all sessions</td><td>Terminal is required to be equipped with this function, accepts if required, assert, and required if asserted.</td><td>–</td><td rowspan="5">Clause 10.1
Table 10-2/ [RFC 3262]
Clause 10.2.1.20.32</td><td rowspan="5"></td><td rowspan="5"></td></tr>
<tr><td rowspan="4">Use in each session as necessary</td><td rowspan="2">Terminal is required to be equipped with this function, and accepts if required.</td><td>Assert, and require if asserted</td></tr>
<tr><td>May assert and may require</td></tr>
<tr><td rowspan="2">Terminal is not required to be equipped with this function.</td><td>Assert, and require if asserted</td></tr>
<tr><td>May assert and may require</td></tr>
</table>

Table I.7 – SIP option tags

Item	Name of option	UNI condition		Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
3	Dialogue replacement function (`replaces`)	Use in each session as necessary	Terminal is required to be equipped with this function, and accepts if required.	May assert and may require	Clause 10.1 Table 10-2/[RFC 3891]		
				Not assert and not require			
			Terminal is not required to be equipped with this function.	May assert and may require			
				Not assert and not require			
		Not use	Terminal does not assert and require this function, and rejects[e)] if required.	–			
4	Conference session participation function (`join`)	Use in each session as necessary	Terminal is required to be equipped with this function, and accepts if required.	May assert and may require	Clause 10.1 Table 10-2/[RFC 3911]		
				Not assert and not require			
			Terminal is not required to be equipped with this function.	May assert and not require			
				Not assert and not require			
		Not use	Terminal does not assert and require this function, and rejects if required.	–			

Table I.7 – SIP option tags

<table>
<tr><th>Item</th><th>Name of option</th><th colspan="2">UNI condition</th><th>Terminal selection</th><th>Relevant items
(reference clauses, etc.)</th><th>Special notes</th><th>Remarks</th></tr>
<tr><td rowspan="5">5</td><td rowspan="5">Bandwidth reservation function before establishment (`precondition`)</td><td rowspan="4">Use in each session as necessary</td><td rowspan="2">Terminal is required to be equipped with this function, and accepts if required.</td><td>May assert and may require</td><td rowspan="5">Clause 10.1
Table 10-2/ [RFC 3312]
Table 10-2/ [RFC 4032]</td><td rowspan="5"></td><td rowspan="5"></td></tr>
<tr><td>Not assert and not require</td></tr>
<tr><td rowspan="2">Terminal is not required to be equipped with this function.</td><td>May assert and may require</td></tr>
<tr><td>Not assert and not require</td></tr>
<tr><td>Not use</td><td>Terminal does not assert and require this function, and rejects if required.</td><td>–</td></tr>
<tr><td rowspan="5">6</td><td rowspan="5">Terminal capabilities notification function (`pref`)</td><td rowspan="4">Use in each session as necessary</td><td rowspan="2">Terminal is required to be equipped with this function, and accepts if required.</td><td>May assert and may require</td><td rowspan="5">Clause 10.1
Table 10-2/ [RFC 3840]
Table 10-2/ [RFC 3841]</td><td rowspan="5"></td><td rowspan="5"></td></tr>
<tr><td>Not assert and not require</td></tr>
<tr><td rowspan="2">Terminal is not required to be equipped with this function.</td><td>May assert and not require</td></tr>
<tr><td>Not assert and not require</td></tr>
<tr><td>Not use</td><td>Terminal does not assert and require this function, and rejects if required.</td><td>–</td></tr>
<tr><td rowspan="2">7</td><td rowspan="2">*REGISTER* route recording function (`path`)</td><td>Use</td><td>Terminal is required to be equipped with this function, and always asserts in registration.</td><td>–</td><td rowspan="2">Clause 10.1
Table 10-2/ [RFC 3327]</td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td>Not use</td><td>Terminal does not assert this function.</td><td>–</td></tr>
</table>

Table I.7 – SIP option tags

<table>
<tr><th>Item</th><th>Name of option</th><th colspan="2">UNI condition</th><th>Terminal selection</th><th>Relevant items (reference clauses, etc.)</th><th>Special notes</th><th>Remarks</th></tr>
<tr><td rowspan="2">8</td><td rowspan="2">Security capabilities exchange function (<code>sec-agree</code>)</td><td>Use</td><td>Terminal is required to be equipped with this function, and always requires it.</td><td>–</td><td rowspan="2">Clause 10.1
Table 10-2/ [RFC 3329]</td><td rowspan="2">[In the case of use, the security capabilities are listed here.]
<<In the case of use, the security capabilities with which terminal is equipped are listed here. >></td><td rowspan="2"></td></tr>
<tr><td>Not use</td><td>Terminal does not require this function.</td><td>–</td></tr>
<tr><td rowspan="3">9</td><td rowspan="3">Other SIP option tags</td><td rowspan="2">Use in each session as necessary</td><td>Terminal is required to be equipped with the functions of other option tags the network specifies.</td><td>–</td><td rowspan="3">Clause 10.2.1.20.32</td><td rowspan="3">[In the case of use, describe the names of SIP option tags and use conditions.]</td><td rowspan="3"></td></tr>
<tr><td>Terminal is not required to be equipped with functions of other option tags.</td><td>–</td></tr>
<tr><td>Not use</td><td>Terminal does not assert or require other functions, and rejects if required.</td><td>–</td></tr>
<tr><td colspan="8">a) "Equipped" with the function means that the function is implemented in the terminal (not necessarily meaning to perform the function).
b) "Accept" means to perform this function in the case it is specified in the <code>Require</code> header.
c) "Assert" means to indicate in the <code>Supported</code> header to notify the peer or the network of information that the function is equipped.
d) "Require" means to indicate in the <code>Require</code> header to require for the peer or the network to perform the function.
e) "Reject " means to return a <code>420</code> response and not accept the requirement if the function is required in the <code>Require</code> header of a request.</td></tr>
</table>

Table I.8 – timer

Item	Name of option	UNI condition		Terminal Selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
1	Session refresh by UPDATE method	Use	Terminal is required to be equipped with this function, and uses the function if it can.	–	Clause 10.1 Table 10-2/ [RFC 4028]		
		Not use	Terminal does not refresh a session by UPDATE	–			

Table I.9 – Subaddress

Item	Name of option	UNI condition		Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
1	Originating subaddress	Provides originating subaddress function	Terminal is required to be equipped with originating subaddress receiving function at time of terminating a call.	May use originating subaddress at time of originating a call	Clause B.6		
				Not use originating subaddress at time of originating a call			
		Not provide originating subaddress function	Terminal does not use originating subaddress and, if received, ignores it.	–			

Table I.9 – Subaddress

Item	Name of option	UNI condition		Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
2	Terminating subaddress	Provide terminating subaddress function	Terminal is required to be equipped with terminating subaddress receiving function at time of terminating a call	May use terminating subaddress at time of originating a call	Clause B.6		
				Not use terminating subaddress at time of originating a call			
		Not provide terminating subaddress function	Terminal does not use terminating subaddress and, if received, ignores it.	–			

Table I.10 – MIME Multipart

Item	Name of option	UNI condition	Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
1	Use of MIME Multipart in `INVITE` requests [Terminal sends]	Allow	May send	Clause 10.1 Table 10-2/ [RFC 2046]	<<In the case that terminal sends, the contents of Multipart are listed here.>>	
			Not send			
		Disallow	Not send			
2	Use of MIME Multipart in `INVITE` requests [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 10-2/ [RFC 2046]	[The contents of Multi- part are listed here that terminal is required to be equipped with receiving function.] <<The contents of Multipart are listed here that terminal is equipped with receiving function.>>	
		Terminal are not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
3	Use of MIME Multipart in a `MESSAGE` request [Terminal sends]	Allow	May send	Clause 10.1 Table 10-2/ [RFC 2046]	<<In the case that terminal sends, the contents of Multipart are listed here.>>	
			Not send			
		Disallow	Not send			

Table I.10 – MIME Multipart

<table>
<tr><th>Item</th><th>Name of option</th><th>UNI condition</th><th>Terminal selection</th><th>Relevant items
(reference clauses, etc.)</th><th>Special notes</th><th>Remarks</th></tr>
<tr><td rowspan="4">4</td><td rowspan="4">Use of MIME Multipart in a MESSAGE request
[Terminal receives]</td><td>Terminal is required to be equipped with receiving function.</td><td>–</td><td rowspan="4">Clause 10.1
Table 10-2/ [RFC 2046]</td><td rowspan="4">[The content of Multipart are listed here that terminal is required to be equipped with receiving function.]
<<The contents of Multipart are listed here that terminal is equipped with receiving function.>></td><td rowspan="4"></td></tr>
<tr><td rowspan="2">Terminal is not required to be equipped with receiving function.</td><td>Equipped with receiving function</td></tr>
<tr><td>On receiving a request, return an appropriate error response.</td></tr>
<tr><td>In the case that terminal receives, return an appropriate error response.</td><td>–</td></tr>
</table>

Table I.11 – Authentication

<table>
<tr><th>Item</th><th>Name of option</th><th colspan="2">UNI condition</th><th>Terminal selection</th><th>Relevant items
(reference clauses, etc.)</th><th>Special notes</th><th>Remarks</th></tr>
<tr><td rowspan="3">1</td><td rowspan="3">Authentication
(REGISTER)</td><td>Perform HTTP Digest authentication</td><td>Terminal is required to be equipped with HTTP Digest authentication function.</td><td>–</td><td rowspan="3">Clause 10.1
Table 10-2/ [RFC 2617]
Table 10-2/ [RFC 3310]
Table 10-2/ [RFC 3329]</td><td rowspan="3"></td><td rowspan="3"></td></tr>
<tr><td>Perform AKA authentication (Note)</td><td>Terminal is required to be equipped with AKA authentication function.</td><td>–</td></tr>
<tr><td>Not perform (perform access-line based authentication)</td><td>–</td><td>–</td></tr>
</table>

Table I.11 – Authentication

Item	Name of option	UNI condition		Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
2	Authentication (Requests outside existing dialogues except for `REIGSTER`)	Perform HTTP Digest authentication	Terminal is required to be equipped with HTTP Digest authentication function.	–	Clause 10.1 Table 10-2/ [RFC 2617] Table 10-2/ [RFC 3310] Table 10-2/ [RFC 3329]		
		Perform AKA authentication (Note)	Terminal is required to be equipped with AKA authentication function.	–			
		Not perform (perform access-line based authentication	–	–			
NOTE – In the case of performing AKA authentication, IPsec connection needs to be provided in Table I.3, Item 4.							

Table I.12 – Redirection

Item	Name of option	UNI condition	Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
1	Use of redirection by `3xx` response [Terminal sends]	Provide redirection function	May send	Clause 10.2.1.8.3	[In the case that redirection is allowed, methods and response codes are listed here.]	
			Not send			
		Not provide redirection function	Not send			
2	Use of redirection by `3xx` response [Terminal receives]	Terminal is required to perform redirection at time of receiving `3xx` response.	–	Clause 10.2.1.8.3	[In the case that redirection is allowed, methods and response codes are listed here.]	
		Terminal is required not to perform redirection at time of receiving `3xx` response	–			

Table I.13 – Bandwidth control

<table>
<tr><th>Item</th><th>Name of option</th><th colspan="2">UNI condition</th><th>Terminal selection</th><th>Relevant items (reference clauses, etc.)</th><th>Special notes</th><th>Remarks</th></tr>
<tr><td rowspan="3">1</td><td rowspan="3">Maximum bucket size</td><td colspan="2">Fixed value, and not determined by token rate
(see Example 1 in ITU-T Y.1221 Appendix IV)</td><td>–</td><td rowspan="3">Clause G.2.2.1</td><td rowspan="3">[Values considered to be necessary in each model are listed here.]</td><td rowspan="3"></td></tr>
<tr><td colspan="2">Proportional to token rate
(see Example 2 in ITU-T Y.1221 Appendix IV)</td><td>–</td></tr>
<tr><td colspan="2">Proportional to token rate, but minimum and maximum values are determined
(see Example 3 in ITU-T Y.1221 Appendix IV)</td><td>–</td></tr>
<tr><td rowspan="2">2</td><td rowspan="2">Rate coefficient</td><td colspan="2">Rate coefficient is specified per quality class.</td><td>–</td><td rowspan="2">Clause G.2.2.1</td><td rowspan="2">[Values of rate coefficients are listed here.]</td><td rowspan="2"></td></tr>
<tr><td colspan="2">Single rate coefficient is specified.</td><td>–</td></tr>
<tr><td rowspan="2">3</td><td rowspan="2">Token rate corresponding to codec</td><td colspan="2">Use</td><td>–</td><td rowspan="2">Clause G.2.2.2</td><td rowspan="2">[In the case of use, show conditions per codec.]</td><td rowspan="2"></td></tr>
<tr><td colspan="2">Not use</td><td>–</td></tr>
<tr><td rowspan="4">4</td><td rowspan="4">Specifying RTCP bandwidth using b=RR / b=RS</td><td rowspan="3">Use</td><td rowspan="2">Terminal is equipped with receiving function of b=RR / b=RS.</td><td>Use</td><td rowspan="4">Clause G.3.2</td><td rowspan="4"></td><td rowspan="4"></td></tr>
<tr><td>Not use</td></tr>
<tr><td>Terminal may ignore b=RR / b=RS at time of receiving messages.</td><td>Not use</td></tr>
<tr><td>Not use</td><td>Terminal ignores b=RR / b=RS at time of receiving messages.</td><td>Not use</td></tr>
<tr><td rowspan="2">5</td><td rowspan="2">RTCP bandwidth at time of unspecified b=RR / b=RS</td><td colspan="2">Set to be 5% of RTP bandwidth</td><td>–</td><td rowspan="2">Clause 10.1
Table 10-2/ [RFC 3556]
Clause G.3.2</td><td rowspan="2">[In the case of using bandwidth other than 5%, show methods to determine the bandwidth.]</td><td rowspan="2"></td></tr>
<tr><td colspan="2">Use a value except for 5%</td><td>–</td></tr>
</table>

Table I.13 – Bandwidth control

Item	Name of option	UNI condition	Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
6	Quality class	Provide multiple quality classes	–	Clause G.4	[In the case of specifying quality class, quality class for each factor is listed.] <<Terminal lists quality class to use.>>	
		Provide single quality class	–			
7	DSCP value per quality class	Specify	–	Clause G.4.1	[In the case of specifying the DSCP value, it is listed here.]	
		Not specify	–			

Table I.14 – Media

Item	Name of option	UNI condition	Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
1	Video (m=*video*)	Allow	May use	Clause 10.3.1 / Table 10-8		
			Not use			
		Disallow	Not use			
2	Data communication (m=*application*, m=*data*, etc.)	Allow	May use	Clause 10.3.1 / Table 10-8	[Determine the *media* type (*m=* line of SDP) to allow.] <<In the case that terminal uses, *media* type is listed here.>>	
			Not use			
		Disallow	Not use			
3	Media TCP connection	Allow	May offer	Clause 10.3.1 / Table 10-8	[Determine the *media* type (*m=* line of SDP) and the *proto* part that allow TCP.] <<In the case that terminal uses, the *media* type and the *proto* part are listed here.>>	
			Not offer			
		Disallow	Not offer			

Table I.15 – Conditions when using ITU-T G.711 μ-law

Item	Name of option	UNI condition	Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
1	Settings for `a=ptime` line in the case of using ITU-T G.711 μ-law	Mandatory	Set	Annex J.2.1		
		Not mandatory	Set			
			Not set			
2	Packetization period in the case of offering ITU-T G.711 μ-law	Allow only 20 ms	–	Annex J.2.1	[In the case of allowing values other than 20 ms, the allowed packetization period is listed here.]	
		Allow values other than 20 ms	–			

Table I.16 – Codecs to be included in codec list/ protocols for data communication

Item	Name of option	UNI condition	Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
1	Voice band codec other than ITU-T G.711 μ-law	Allow voice band codecs other than ITU-T G.711 μ-law	Use voice band codec other than ITU-T G.711 μ-law	Clause 8.1	[In the case of allowing codecs other than ITU-T G.711 μ-law, they are listed.] <<In the case that terminal uses codecs other than ITU-T G.711 μ-law, they are listed here.>>	
			Not use voice band codec other than ITU-T G.711 μ-law			
		Disallow voice band codec other than ITU-T G.711 μ-law	Not use voice band codec other than ITU-T G.711 μ-law			
2	Video codec	Allow	Use	Clause 8.1	[In the case video codecs are allowed, codec names are listed.] <<In the case that terminal uses video codecs, codec names are listed here.>>	
			Not use			
		Disallow	Not use			
3	Data communication	Allow	Use	Clause 8.1	[In the case of allowing data communication, protocol names are listed here.] <<In the case that terminal uses data communication, protocol names are listed here.>>	
			Not use			
		Disallow	Not use			

Table I.17 – Media-related SIP headers

<table>
<tr><th>Item</th><th>Name of option</th><th colspan="2">UNI condition</th><th>Terminal selection</th><th>Relevant items (reference clauses, etc.)</th><th>Special notes</th><th>Remarks</th></tr>
<tr><td rowspan="4">1</td><td rowspan="4"><code>P-Media-Authorization</code> header</td><td rowspan="3">Use</td><td>Terminal is required to be equipped with capabilities to receive messages.</td><td>Not send</td><td rowspan="4">Clause 10.1
Table 10-2/ [RFC 3313]</td><td rowspan="4"></td><td rowspan="4"></td></tr>
<tr><td rowspan="2">Terminal is not required to be equipped with capabilities to receive messages.</td><td>Not send, and on receiving messages, behave according to the header content</td></tr>
<tr><td>Not send, and on receiving messages, ignore it.</td></tr>
<tr><td>Not use</td><td>Terminal does not send, and on receiving messages, ignores it.</td><td>–</td></tr>
</table>

Table I.18 – Media grouping

<table>
<tr><th>Item</th><th>Name of option</th><th colspan="2">UNI condition</th><th>Terminal selection</th><th>Relevant items (reference clauses, etc.)</th><th>Special notes</th><th>Remarks</th></tr>
<tr><td rowspan="5">1</td><td rowspan="5">Media grouping (<code>a=group</code> line, <code>a=mid</code> line)</td><td rowspan="4">Use</td><td rowspan="2">Terminal is required to be equipped with capabilities to receive messages.</td><td>May send</td><td rowspan="5">Clause 10.1
Table 10-2/ [RFC 3388]
Table 10-2/ [RFC 3524]</td><td rowspan="5">[In the case of use, available semantics is listed here.]
<<In the case that terminal uses, semantics to be used is listed here.>></td><td rowspan="5"></td></tr>
<tr><td>Not send</td></tr>
<tr><td rowspan="2">Terminal is not required to be equipped with capabilities to receive messages.</td><td>May send</td></tr>
<tr><td>Not send</td></tr>
<tr><td>Not use</td><td>On receiving messages, terminal ignores it.</td><td>Not send</td></tr>
</table>

Table I.19 – Feedback control using RTCP

Item	Name of option	UNI condition		Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
1	RTCP packets for feedback control using RTCP (RTPFB, PSFB)	Allow	–	May use	Clause 11.1	<<In the case that terminal uses, feedback format is listed here.>>	
				Not use			
		Disallow	On receiving messages, terminal ignores it.	Not use			
2	Use of SDP description for feedback control using RTCP (RTP/AVPF)	Allow	–	May use	Clause 11.1	<<In the case that terminal uses, feedback format is listed here.>>	
				Not use			
		Disallow	In the case that terminal receives, return an appropriate error response.	Not use			

Table I.20 – URI format

Item	Name of option	UNI condition	Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
1	`Request-URI` format when using numbers other than national numbers (requests outside existing dialogues except for `REGISTER`)	Allow	May use	Clause 9 Clause B.5	[In the case it is allowed, URI format is listed.] <<URI format to be used is listed here.>>	
			Not use			
		Disallow	Not use			
2	The *hostport* part of a SIP-URI and the *descriptor* part of *context* in a TEL-URI when using national numbers	Specifies domain	–	Clause 9 Clause B.5.2	[Shows domain name or IP address.]	
		Specifies IP address	–			

Table I.21 – SIP/SDP character string length and set value range

Item	Name of option	UNI condition	Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
1	Conditions on SIP string length and value range unspecified in h.	Set	–	Clause H.2.1	[In the case of setting, show specific conditions on sending/receiving messages.]	
		Not set	–			
2	Conditions on SDP string length and value range unspecified in h.	Set	–	Clause H.2.2	[In the case of setting, show specific conditions on sending/receiving messages.]	
		Not set	–			
3	Number of payload types that can be set in the *fmt* part of `m=` line	Network specifies the maximum value.	–	Clause E.3	[In the case of specifying the maximum value, the value is described here.]	
		Network does not specify the maximum value.	–		<<In the case that terminal offers, the maximum payload value to be described in the *fmt* part is described here.>>	

Table I.22 – Media negotiation

Item	Name of option	UNI condition	Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
1	SDP settings to a `1xx` response [Terminal sends]	Allow	May set	Clause G.3.1		
			Not send			
		Disallow	Not send			
2	SDP offer by a `PRACK` request [Terminal sends]	Allow	May set	Clause 10.2.1.7.4.1		
			Not set			
		Disallow	Not set			

Table I.22 – Media negotiation

Item	Name of option	UNI condition	Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
3	SDP offer by a `PRACK` request [Terminal receives]	Terminal is required to be equipped with capabilities to receive messages	–	Clause 10.2.1.7.4.1		
		Terminal is not required to be equipped with capabilities to receive messages.	Equipped with capabilities to receive messages			
			Not equipped with capabilities to receive messages			
4	Optional SDP lines [Terminal sends]	Use	–	Clause 10.3.1 Table 10-8	[SDP lines to be used are listed here.] <<SDP lines to be sent are listed here.>>	
		Not use	–			
5	Optional SDP lines [Terminal receives]	Use	–	Clause 10.3.1 Table 10-8	[SDP lines to be used to are listed here.] <<SDP lines to support receiving are listed here.>>	
		Not use	–			

Table I.23 – Media modification

Item	Name of option	UNI condition	Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
1	Media modification in early dialogue [Terminal sends]	Allow	May send	Clause 10.1 Table 10-2/ [RFC 3311]		
			Not send			
		Disallow	Not send			
2	Media modification in early dialogue [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 10-2/ [RFC 3311]		
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving messages, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			

Table I.23 – Media modification

Item	Name of option	UNI condition	Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
3	Media modification by re-`INVITE` after dialogue establishment [Terminal sends]	Allow	May send	Clause 10.2.1.14		
			Not send			
		Disallow	Not send			
4	Media modification by re-`INVITE` after dialogue establishment [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.2.1.14		
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving messages, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
5	Media modification by `UPDATE` after dialogue establishment [Terminal sends]	Allow	May send	Clause 10.2.1.14		
			Not send			
		Disallow	Not send			
6	Media modification by `UPDATE` after dialogue establishment [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.2.1.14		
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving messages, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			

Table I.24 – Registration

Item	Name of option	UNI condition		Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
1	Providing pre-existing route at time of registration (`Service-Route` header) (Note)	Provide	Terminal uses provided pre-existing route.	–	Clause C.3.1		
		Not provide	Terminal does not set pre-existing route.	–			
2	Obtaining SCF address	Provide IP address/port number of SCF by DHCP/DHCPv6.		–	Clause C.2	[Procedures are listed here in the case of procedures other than DHCP and presettings.]	
		Preset IP address/port number of SCF in the terminal		–			
		Provide IP address/port number by methods other than the above		–			
3	Notifying network-asserted user identity at time of `REGISTER`	May notify		In the case of receiving notification, use the received SIP-URI.	Clause B.2.1	[In the case of notifying, conditions are listed here.]	
		Not notify		–			
4	The *expires* parameter value in the `Contact` header or the value in the `Expires` header at time of registration	Network specifies a fixed value		Set specified value	Clause C.3	[In the case of specifying the set value, the value is listed here.]	
		Network does not specify a fixed value		Set any value			
				Not set			
5	The *expires* parameter value in the `Contact` header or the value in the `Expires` header at time of refresh	Network specifies		Set specified value	Clause C.4	[In the case of specifying calculation formula or fixed value, it is listed here.]	
		Network does not specify		Set any value			
				Not set			
6	Setting the *q* parameter to the `Contact address`	Allow		Set	Clause C.3	[In the case it is allowed by the network, the setting conditions are listed here.]	
				Not set			
		Disallow		Not set			

Table I.24 – Registration

Item	Name of option	UNI condition	Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
7	Interval to send a `REGISTER` request at time of no reply by the network	Network specifies	Send specified value	Clause F.2.5	[In the case of being specified by the network, the interval is listed here.] <<In the case of not being specified by the network, the interval of sending from the terminal is listed here.>>	
		Network does not specify	Send according to terminal implementation			
8	Registration state notification (*reg* event) function of the terminal	Provide	May subscribe to registration notification	Clause C.6		
			Not subscribe to registration notification			
		Not provide	Not subscribe to registration notification			

NOTE – In order to use this procedure, the terminal capabilities notification function (path) in Table I.7, Item 7 must be used.

Table I.25 – Sending and receiving RTP packets

Item	Name of option	UNI condition	Terminal selection	Relevant items (reference clauses, etc.)	Special notes	Remarks
1	RTP sending behaviour of the terminal when receiving a `1xx` response to an `INVITE` request	Start sending	–	Clause 7.1		
		May start sending	Send			
			Not send			
		Not start sending	–			
2	Handling of media packets before performing final SDP negotiation to an initial `INVITE`	May start sending to terminal	–	Clause 7.1		
		Not start sending to terminal	–			

Appendix II

Response code usage

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

II.1 Introduction

The acronym NGN is used in various forms of communication, such as message and data communication, in addition to speech communication. In traditional speech communication, when connection fails to be established, the audio guidance is simply run to the user. However, in message and data communication, etc., notification based on SIP response codes must be delivered to the user, instead of the audio guidance. Also, in the case of the softphone and other highly functional terminals with display capabilities, although the terminal may be intended for speech communication, it is considered desirable to display the cause of error on the display according to response codes.

For the terminal to appropriately display the cause of error based on SIP response codes, the information represented by the response codes must match between the network and the terminal. However, the definitions of response codes indicated in [RFC 3261] do not represent actual incidents that have occurred in the real world of NGN communication. Therefore, there is the risk of generating discrepancies between the specific incidents and the response codes and, as a result, not displaying properly to the user.

For this reason, this appendix shows specific examples of response code usage to help interpret the meaning of response codes. Note that usage of response codes that is not shown in this appendix may be allowed by the network.

II.2 4xx response

II.2.1 403 Forbidden

In the case that connection is attempted to a resource which forbids access from a subscriber or a terminal, e.g., when a destination specified by the terminal is not allowed to the subscriber, a network returns a `403 (Forbidden)` response.

In the case that a terminal rejects a call on judging the calling-party's identity, it returns a `403 (Forbidden)` response. If the `403 (Forbidden)` response is received, it should be interpreted that the call was rejected by the network or the terminal on the terminating side ("Connection is rejected").

II.2.2 404 Not Found

In the case that a specified subscriber does not exist, no route towards the subscriber is available, or the `Request-URI` is inappropriate, e.g., when a destination numeric string is too long, a network may return a `404 (Not Found)` response instead of providing audio guidance.

In the case that a terminal which accepts a call with a subaddress specified by the network does not exist, it returns a `404 (Not Found)` response. If the `404 (Not Found)` response is received, it should be interpreted that the destination was inappropriate ("Unallocated number or no destination").

II.2.3 410 Gone

In the case that the specified destination by a subscriber has been changed to a URI different from the original, but that no redirection instruction is given to the terminal, the network may return a `410 (Gone)` response, instead of playing an audio guidance, to notify the relocation. In other cases, the `410 (Gone)` response should not be returned.

The terminal should not send unnecessary `410` responses in order to avoid confusion with the relocation. If the `410 (Gone)` response is received, it should be interpreted that the URI has been changed ("Relocated") due to the relocation of the destination, etc.

II.2.4 433 Anonymity Disallowed

A network which provides a service to reject an anonymous call may return a `433 (Anonymity Disallowed)` response, specified in [RFC 5079], instead of providing an audio guidance, when rejecting with the service.

In the case of rejecting the call because the calling-party's identity is anonymous, a terminal returns a `433 (Anonymity Disallowed)` response. If the `433 (Anonymity Disallowed)` response is received, it should be interpreted that the call was rejected on the grounds of undisclosed identity ("Rejection for anonymous calls").

II.2.5 480 Temporarily Unavailable

In the case that a specified subscriber exists but that communication is impossible because a terminal is disconnected, etc., (for instance, when the terminal is unregistered or the registration is expired, etc.), a network may return a `480 (Temporarily Unavailable)` response instead of providing an audio guidance.

In the case that a terminal receives the `480 (Temporarily Unavailable)` response, it should be interpreted that the terminal on the terminating side is temporarily unable to receive the call because the terminal is disconnected ("Terminal is unavailable "), etc.

II.2.6 486 Busy Here

In the case that a call connection that is to be made will exceed the number of sessions allowed for a calling subscriber or called subscriber, the network returns a `486 (Busy Here)` response.

In the case that a called terminal is already engaged in communication and cannot receive a call, it returns a `486 (Busy Here)` response. If the `486 (Busy Here)` response is received, it should be interpreted that the number of sessions of the network or the called terminal necessary for the call connection is insufficient ("Busy"). It should be noted that the `486 (Busy Here)` response may be returned to requests such as `MESSAGE`, `SUBSCRIBE`, and `REGISTER`, in addition to an `INVITE` request.

II.2.7 487 Request Terminated

In the case of terminating an unestablished call while still calling, a network may return a `487 (Request Terminated)` response, regardless of whether it receives a `CANCEL` request from a terminal. This is applied when the time taken to try establishing the call exceeds a certain amount of time, or a guidance is terminated, etc.

In the case that the terminal receives the `487 (Request Terminated)` response, it should be interpreted that the events described above have occurred.

II.2.8 488 Not Acceptable Here

In the case that the contents of SDP set in an `INVITE` or `UPDATE` request sent from a terminal are unacceptable (i.e., communication using media type, codec, bandwidth, IP version, etc., set in the SDP is impossible), a network returns a `488 (Not Acceptable Here)` response. In other cases, the `488 (Not Acceptable Here)` should not be returned.

In the case that the contents of SDP set in the `INVITE` or `UPDATE` request sent from the terminal are unacceptable, the terminal returns the `488 (Not Acceptable Here)` response. In other cases, the `488 (Not Acceptable Here)` should not be returned. In the case that the `488 (Not Acceptable Here)` is received, it should be interpreted that the network or the terminal on the terminating side did not accept the SDP.

II.3 5xx response

II.3.1 503 Service Unavailable

In the case that a network cannot provide service to a terminal due to such states as congestion or failure, it returns a `503 (Service Unavailable)` response as described in Annex F.

The terminal should not send unnecessary `503 (Service Unavailable)` responses in order to avoid confusion with the network congestion or failure. In the case that the `503 (Service Unavailable)` is received, it behaves as described in Annex F.

Appendix III

Mapping SDP description to QoS classes

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

III.1 Overview

This appendix shows a way of mapping QoS classes corresponding to SDP media description contents in order to determine QoS classes specified in Annex G. The mapping of QoS classes at the UNI are not limited to examples shown in this appendix.

III.2 Concept

In the case that a network provides multiple QoS classes, it is necessary to select a QoS class that is appropriate to the nature of media. This appendix introduces an implicit rule of selecting a QoS class as described below. As a rule, correspondence to QoS class is determined by the media description in SDP, which describes the nature of the media.

The nature of media regarding IP packet transfer quality is composed of media type and direction.

Media types fall into the following communication types: audio (`m=audio`), video (`m=video`), and data (`m=application`, etc.), and it is indicated in the *proto* of `m=` line in SDP.

For audio, it is desirable to maintain a low level of transfer delay, variation, and loss ratio (to provide the quality required by the regulation for 0AJ). Even for video, the delay, variation and loss ratio at the same level as audio could be considered desirable, taking the lip-sync with audio into account. On the other hand, in general it is not required to keep the level of delay or variation as low for data communication as for audio or video. For the loss ratio, the packet loss could often be recovered by retransmission in the case of data communication. In this way, taking the media type into account, it is considered appropriate to assign a higher priority of QoS class to audio and video media, and to assign a lower priority of QoS class to data media.

Media direction falls into the following communication types: bidirectional (`a=sendrecv`) or unidirectional (`a=recvonly` / `a=sendonly`), and it is indicated in direction attributes in SDP.

In bidirectional communication (e.g., audio telephone or television telephone), a delay in the network is directly felt by the user as round-trip time to return a response to the information received from a party on the other side of the communication. On the other hand, in unidirectional communication (e.g., streaming), the delay in the network is not so obvious because it takes only sending to, or receiving from, the party on the other side. Therefore, it is considered to be appropriate to assign higher priority of QoS class to unidirectional communication and to assign a lower priority of QoS class to bidirectional communication.

III.3 Example of correspondence

This clause shows examples of QoS class corresponding to each media from SDP media description contents based on media type and direction.

III.3.1 SDP

The media type of audio (`m=audio`) and video (`m=video`) is given high priority and the media type of data (`m=application`) is given low priority. For audio and video media which is highly prioritized, higher priority is given when the media direction attribute is bidirectional (`a=sendrecv`), and lower priority is given when the media direction attribute is unidirectional (`a=recvonly` / `a=sendonly`).

One of the three types of QoS classes is selected from the SDP description according to the above way of mapping (Table III.1)

Table III.1 – Example of QoS class corresponding to SDP description

QoS class	SDP description of media		Service example
	Type	Direction attribute	
Highest priority class	Audio (m=audio) Video (m=video)	Bidirectional (a=sendrecv)	Audio telephone, television telephone
High priority class	Audio (m=audio) Video (m=video)	Unidirectional (a=recvonly / a=sendonly)	Video streaming
Priority class	Data (m=application)	Bidirectional or Unidirectional (a=sendrecv / a=recvonly / a=sendonly)	Data communication, remote control of device

Note that for communication that does not require quality, the best-effort class is assumed to be set as a QoS class, lower than the "priority class" shown in Table III.1, where resource admission control using SIP/SDP is not performed.

Appendix IV

Security considerations

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

IV.1 Overview

This appendix shows examples of solutions expected to be effective in meeting requirements indicated in clause 14 of [ITU-T Q.3402] regarding security over the UNI.

IV.2 Requirements for the UNI

The following items should be considered from the security standpoint in the UNI.

1) Prevention of tampering

   SIP messages transferred over the UNI shall not be tampered with by a third party.

2) Prevention of spoofing

   SIP messages that a terminal receives shall be forwarded safely from the SIP trust domain without the occurrence of any spoofing.

3) Hiding of user information

   Information which specifies that a user shall not be unnecessarily notified to the opposing terminal.

IV.3 Solution examples

IV.3.1 Filtering through source IP address

The process of filtering incoming packets through the source IP address is expected to be effective for the prevention of spoofing. Following are examples of the filtering process:

– Packet filtering is performed by some means at the UNI to ensure that a SIP message packet, which is sent to a terminal and has a source IP address corresponding to a network boundary (group), is indeed a packet from a network boundary (group). This prevents spoofing with respect to the source IP address.

– The terminal judges that a received SIP message is sent from a valid SIP trust domain only when its source IP address is the same as a previously acquired address of a network boundary (group). Only on validation does the terminal accept the connection.

IV.3.2 Limiting use of the port

The process to limit use of the port is expected to be effective for the prevention of spoofing. Following are examples of procedures to limit use of the port:

– The port number that a terminal uses to send or receive SIP messages is limited to specific ports.

– Packet filtering is performed by some means at the UNI to ensure that a packet, which is received by the terminal and has a destination port number corresponding to the specific port set in the previous item, is indeed a packet from a network boundary (group). This prevents specified ports from being used by other parties.

Note that in such cases, the specified ports can no longer be used for other purposes.

IV.3.3 Randomization of a Contact header (on terminal registration)

If a network structure allows a terminal to receive a SIP messages directly from outside of the SIP trusted domain, the terminal is recommended to set a random string, which cannot be guessed easily by a third party, in the *user* part of the `Contact address` specified at the time of terminal registration. The reasons for this recommendation are stated below.

– When receiving requests from outside existing dialogues, a terminal judges the validity of the received requests by comparing the `Request-URI` and registered `Contact address`. If the values are easy-to-guess (e.g., user name or telephone number), there is a high risk of suffering from a prank call (e.g., "spit") caused by invalid requests outside existing dialogues not transmitted through the SIP trust domain.

– In the case that a network has a structure that configures IP addresses of terminals dynamically (e.g., DHCP or PPPoE) and the IP address is changed every time a terminal acquires it, the network retains the `Contact address` in the event of an unexpected failure (e.g., power blackout) at the terminal. In this situation, and when the IP address has been assigned to another terminal, a request may end up being sent to a terminal different from the one that experiences the unexpected failure and to which the request was originally intended to be sent. However, a malfunctioning behaviour can be prevented on the surface by checking if the *user* part is the same when the terminal receives the requests outside existing dialogues.

IV.3.4 Randomization of a Contact header (on initiating sessions)

If a network structure allows a terminal to receive SIP messages directly from outside of the SIP trusted domain, it is desirable that the terminal generates a unique string, which cannot be guessed easily by a third party, and uses it for the *user* part of the `Contact address` in requests outside existing dialogues. It is also desirable that the *user* part is different from that of a `Contact address` in a `REGISTER` request at the time of registration. Note that the string is not modified in subsequent transactions in the same dialogue.

IV.3.5 Considerations on transparent transfer of SIP messages

The SIP/SDP information set by a terminal may not be filtered or rewritten in a network, and may be notified transparently to the UNI or NNI on the terminating side. Therefore, strings involved with user identity should not be set in SIP headers not indicated in Annex B or SDP constituent elements.

Appendix V

Discovery procedure of the SCF

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

V.1 Overview

This appendix shows an example of procedures for obtaining the SCF address used in the terminal registration specified in clause C.3. Note that procedures to obtain the SCF address are not limited to the example shown in this appendix.

V.2 DHCP/DHCPv6

In the case that a network provides IPv4 connectivity, it provides procedures using DHCP, as defined in [RFC 2131], to IPv4 terminals. In the case of using DHCP, the IPv4 address and the port number of the SCF is provided by the terminal requesting the option 120 specified in [RFC 3361]. In the case that a domain list is returned to the option 120 request, the IPv4 address and the port number need to be resolved using DNS, following further the specifications of [RFC 3263].

In the case that the network provides IPv6 connectivity, it provides procedures using DHCPv6 specified in [RFC 3315] to IPv6 terminals. In the case of using DHCPv6, the IPv6 address and the port number of the SCF is provided by the terminal requesting the option 22 specified in [RFC 3319] or the option 21 specified in [RFC 3319]. In the case that the domain list is returned to the option 21, the IPv6 address and the port number need to be resolved using DNS, following further the specifications of [RFC 3263].

V.3 Terminal preconfiguration

The terminals are preconfigured with the IP address and the port number of the SCF.

Annex VI

Signalling rule of SIP messages and headers

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

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

VI.1 Dynamic view and static view

VI.1.1 Static view

Static view refers to the form which can be seen in Annex A of [3GPP TS 24.229], where "sending" and "receiving" SIP entities' functional implementation is expressed as M (Mandatory), O (Optional), etc., in regard to the application conditions of each header.

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

VI.1.2 Dynamic view

Dynamic view refers to the header application condition table which can be seen in [RFC 3261], where it indicates M (Mandatory), O (Optional), etc., depending on whether the headers appear and exist as information items for signalling over an interface between SIP entities, instead of using application categorization such as "sending" and "receiving" sides, as in static view.

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

VI.1.3 Adoption of dynamic view for this appendix

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

VI.1.4 Definition of notation codes in the tables in this annex

The definition of the notation codes described in the columns of "RFC status" and "Status in this standard" for each table is identical to that of [RFC 3261].

Table VI.1 – Definition of notation codes

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

VI.2 ACK

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

VI.2.1 Supported headers in the ACK request

Table VI.2 – Supported headers in the ACK request

Message type: Request
Method: ACK

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
`Accept-Contact`	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
`Allow-Events`	[RFC 3265]	o	o	o	c2 (Table I.2, Items 10 to 15)	c2 (Table I.2, Items 10 to 15)	
`Authorization`	[RFC 3261]	o	–	–	c3	c3	
`Call-ID`	[RFC 3261]	m	m	m			
`Contact`	[RFC 3261]	o	o	o			
`Content-Disposition`	[RFC 3261]	o	–	–	c4	c4	
`Content-Encoding`	[RFC 3261]	o	–	–	c4	c4	
`Content-Language`	[RFC 3261]	o	–	–	c4	c4	
`Content-Length`	[RFC 3261]	t	t	t			
`Content-Type`	[RFC 3261]	*	–	–	c4	c4	
`CSeq`	[RFC 3261]	m	m	m			
`Date`	[RFC 3261]	o	o	o			(Note)
`From`	[RFC 3261]	m	m	m			
`Max-Forwards`	[RFC 3261]	m	m	m			
`MIME-Version`	[RFC 3261]	o	–	–	c4	c4	
`P-Media-Authorization`	[RFC 3313]	o	–	–	c5	c6	
`Privacy`	[RFC 3323]	o	–	–	c7	c7	

Table VI.2 – Supported headers in the ACK request

Message type: Request
Method: ACK

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Proxy-Authorization	[RFC 3261]	o	o	–	c8 (when Table I.11, Item 2 is stated "Perform HTTP Digest authentication" for UNI condition.)	c9	
			–	–	c8 (when Table I.11, Item 2 is stated other than "Perform HTTP Digest authentication" for UNI condition.)	c9	
Reason	[RFC 3326	o	o	o			(Note)
Record-Route	[RFC 3261]	o	o	o			(Note)
Reject-Contact	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
Request-Disposition	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
Route	[RFC 3261]	c	c	–		c10	
Timestamp	[RFC 3261]	o	o	o			(Note)
To	[RFC 3261]	m	m	m			
User-Agent	[RFC 3261]	o	o	o			(Note)
Via	[RFC 3261]	m	m	m			
Message body	[RFC 3261]	o	–	–	c4	c4	

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available over the UNI, the header information is handled as valid information (Table I.7, Item 6).

c2: In the case that SUBSCRIBE/NOTIFY is available over the UNI, the header information is handled as valid information (Table I.2, Items 10 to 15).

c3: The Authorization header is used only when REGISTER requests from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Table A.1 in clause A.3.

c4: The message body is not to be used because SDP negotiation by ACK is not performed, according to 10.2.1.13 of Table A.1 in clause A.3.

c5: Not to be used in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c6: Notification of the authentication token using the P-Media-Authorization header is not performed because SDP negotiation by *ACK* is not performed, according to 10.2.1.13 of Table A.1 in clause A.3.

c7: The Privacy header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.4 of Table A.1 in clause A.3.

c8: To be used in the case of performing HTTP Digest authentication to requests outside existing dialogues except for REGISTER (Table I.11, Item 2).

c9: The Proxy-Authorization header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.28 in the main body.

Table VI.2 – Supported headers in the ACK request

Message type: Request
Method: ACK

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
c10: The `Route` header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body. NOTE – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies the header in the SIP message to send is dependent on the policy of the NGN carrier.							

VI.2.2 Supported headers in the ACK response

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

VI.3 BYE

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

VI.3.1 Supported headers in the BYE request

Table VI.3 – Supported headers in the BYE request

Message type: Request
Method: BYE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
`Accept`	[RFC 3261]	o	o	o			
`Accept-Contact`	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
`Accept-Encoding`	[RFC 3261]	o	o	o			
`Accept-Language`	[RFC 3261]	o	o	o			
`Allow`	[RFC 3261]	o	o	o			
`Allow-Events`	[RFC 3265]	o	o	o	c2 (Table I.2, Items 10 to 15)	c2 (Table I.2, Items 10 to 15)	

Table VI.3 – Supported headers in the BYE request

Message type: Request
Method: BYE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Authorization	[RFC 3261]	o	–	–	c3	c3	
Call-ID	[RFC 3261]	m	m	m			
Content-Disposition	[RFC 3261]	o	o	o			(Note)
Content-Encoding	[RFC 3261]	o	o	o			(Note)
Content-Language	[RFC 3261]	o	o	o			(Note)
Content-Length	[RFC 3261]	t	t	t			
Content-Type	[RFC 3261]	*	*	*			(Note)
CSeq	[RFC 3261]	m	m	m			
Date	[RFC 3261]	o	o	o			(Note)
From	[RFC 3261]	m	m	m			
Max-Forwards	[RFC 3261]	m	m	m			
MIME-Version	[RFC 3261]	o	o	o			(Note)
P-Access-Network-Info	[RFC 3455]	o	o	–		c4	(Note)
P-Asserted-Identity	[RFC 3325]	o	–	–	c5	c5	
P-Charging-Function-Addresses	[RFC 3455]	o	–	–	c6	c6	
P-Charging-Vector	[RFC 3455]	o	–	–	c6	c6	
P-Preferred-Identity	[RFC 3325]	o	–	–	c7	c7	
Privacy	[RFC 3323]	o	–	–	c8	c8	
Proxy-Authorization	[RFC 3261]	o	o	–	c9 (when Table I.11, Item 2 is stated "Perform HTTP Digest authentication" for UNI condition.)	c10	
			–	–	c9 (when Table I.11, Item 2 is stated other than "Perform HTTP Digest authentication" for UNI	c10	

Table VI.3 – Supported headers in the BYE request

Message type: Request
Method: BYE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
					condition.)		
Proxy-Require	[RFC 3261]	o	o	–		c11	
Reason	[RFC 3326]	o	o	o			(Note)
Record-Route	[RFC 3261]	o	o	o			(Note)
Referred-By	[RFC 3892]	o	o	o	c12 (Table I.2, Items 6 to 9)	c12 (Table I.2, Items 6 to 9)	(Note)
Reject-Contact	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
Request-Disposition	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
Require	[RFC 3261]	c	c	c			
Route	[RFC 3261]	c	c	–		c13	
Security-Client	[RFC 3329]	o	o	–	c14 (Table I.11, Items 1 and 2, Table I.4, Item 3)	c15	
Security-Verify	[RFC 3329]	o	o	–	c14 (Table I.11, Items 1 and 2, Table I.4, Item 3)	c15	
Supported	[RFC 3261]	o	o	o			(Note)
Timestamp	[RFC 3261]	o	o	o			(Note)
To	[RFC 3261]	m	m	m			
User-Agent	[RFC 3261]	o	o	o			(Note)
Via	[RFC 3261]	m	m	m			
Message body	[RFC 3261]	o	o	o			(Note)

c1: In the case that the terminal capabilities notification function, Caller Preferences (pref tag), is available over the UNI, the header information is handled as valid information (Table I.7, Item 6).
c2: In the case that SUBSCRIBE/NOTIFY is available over the UNI, the header information is handled as valid information (Table I.2, Items 10 to 15).
c3: The Authorization header is used only when REGISTER requests from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Table A.1 in clause A.3.
c4: The P-Access-Network-Info header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.
c5: The P-Asserted-Identity header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.2 of Table A.1 in clause A.3.
c6: The P-Charging-Vector and P-Charging-Function-Addresses headers are not to be used, according to 10.1 of Table A.1 in clause A.3.

Table VI.3 – Supported headers in the BYE request

Message type: Request
Method: BYE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
c7: The P-Preferred-Identity header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.3 of Table A.1 in clause A.3.							
c8: The Privacy header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.4 of Table A.1 in clause A.3.							
c9: To be used in the case of performing HTTP Digest authentication to requests outside existing dialogues except for REGISTER (Table I.11, Item 2).							
c10: The Proxy-Authorization header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.28 in the main body.							
c11: The Proxy-Require header is not to be used in the direction from the SCF to the EUF, according to 10.2.1.20.29 of Table A.1 in clause A.3.							
c12: The Referred-By header may be used as a result of using REFER (Table I.2, Items 6 to 9). In the case that REFER is available over the UNI, the header information may be handled as valid information. It does not guarantee that the Referred-By header is used as a result of using REFER.							
c13: The Route header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body.							
c14: To be handled as valid in the case that AKA authentication is used or TLS connection of call control signals is used (Table I.11, Items 1 and 2, Table I.4, Item 3).							
c15: The Security-Client and Security-Verify headers are not applicable to requests in the direction from the SCF to the EUF, according to 10.1 of Table A.1 in clause A.3.							
NOTE – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies the header in the SIP message to send is dependent on the policy of the NGN carrier.							

VI.3.2 Supported headers in the BYE response

Table VI.4 – Supported headers in the BYE response

Message type: Response
Method: BYE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Accept	415	[RFC 3261]	c	c	c			
Accept-Encoding	415	[RFC 3261]	c	c	c			
Accept-Language	415	[RFC 3261]	c	c	c			
Allow	2xx	[RFC 3261]	o	o	o			

Table VI.4 – Supported headers in the BYE response

Message type: Response
Method: BYE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Allow	405	[RFC 3261]	m	m	m			
Allow	others	[RFC 3261]	o	o	o			
Allow-Events	2xx	[RFC 3265]	o	o	o	c1 (Table I.2, Items 10 to 15)	c1 (I.2, Items 10 to 15)	
Authentication-Info	2xx	[RFC 3261]	o	–	–	c2	c2	
Call-ID		[RFC 3261]	m	m	m			
Contact	3xx	[RFC 3261]	o	-	-	c3	c3	
Contact	485	[RFC 3261]	o	o	o			
Content-Disposition		[RFC 3261]	o	o	o			(Note)
Content-Encoding		[RFC 3261]	o	o	o			(Note)
Content-Language		[RFC 3261]	o	o	o			(Note)
Content-Length		[RFC 3261]	t	t	t			
Content-Type		[RFC 3261]	*	*	*			(Note)
CSeq		[RFC 3261]	m	m	m			
Date		[RFC 3261]	o	o	o			(Note)
Error-Info	300-699	[RFC 3261]	o	o	o			(Note)
From		[RFC 3261]	m	m	m			
MIME-Version		[RFC 3261]	o	o	o			(Note)
P-Access-Network-Info		[RFC 3455]	o	o	–		c4	(Note)
P-Asserted-Identity		[RFC 3325]	o	–	–	c5	c5	
P-Charging-Function-Addresses		[RFC 3455]	o	–	–	c6	c6	

Table VI.4 – Supported headers in the BYE response

Message type: Response
Method: BYE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
P-Charging-Vector		[RFC 3455]	o	–	–	c6	c6	
P-Preferred-Identity		[RFC 3325]	o	–	–	c7	c7	
Privacy		[RFC 3323]	o	–	–	c8	c8	
Proxy-Authenticate	401	[RFC 3261]	o	–	–	c9	c10	
Proxy-Authenticate	407	[RFC 3261]	m	–	m	c9		
Reason		[RFC 3326]	o	o	o			(Note)
Record-Route	18x 2xx	[RFC 3261]	o	o	o			(Note)
Require		[RFC 3261]	c	c	c			(Note)
Retry-After	404 413 480 486	[RFC 3261]	o	o	o			(Note)
Retry-After	500 503	[RFC 3261]	o	o	o			(Note)
Retry-After	600 603	[RFC 3261]	o	o	o			(Note)
Security-Server	421 494	[RFC 3329]	o	–	o	c11	c12 (Table I.11, Items 1 and 2, Table I.4, Item 3)	
Server		[RFC 3261]	o	o	o			(Note)
Supported	2xx	[RFC 3261]	o	o	o			(Note)
Timestamp		[RFC 3261]	o	o	o			(Note)
To		[RFC 3261]	m	m	m			
Unsupported	420	[RFC 3261]	m	m	m			

Table VI.4 – Supported headers in the BYE response

Message type: Response
Method: BYE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
User-Agent		[RFC 3261]	o	o	o			(Note)
Via		[RFC 3261]	m	m	m			
Warning		[RFC 3261]	o	o	o			(Note)
WWW-Authenticate	401	[RFC 3261]	m	–	–	c13	c13	
WWW-Authenticate	407	[RFC 3261]	o	–	–	c13	c13	
Message body		[RFC 3261]	o	o	o			(Note)

c1: In the case that SUBSCRIBE/NOTIFY is available over the UNI, the header information is handled as valid information (Table I.2, Items 10 to 15).

c2: Update of authentication information by the Authentication-Info header is not performed because the Authorization header is not to be used in the corresponding request.

c3: Redirection using 3xx responses is not to be used, according to 10.2.1.8.3 of Table A.1 in clause A.3.

c4: The P-Access-Network-Info header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c5: The P-Asserted-Identity header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.2 of Table A.1 in clause A.3.

c6: The P-Access-Network-Info, P-Charging-Vector, and P-Charging-Function-Addresses headers are not to be used, according to 10.1 of Table A.1 in clause A.3.

c7: The P-Preferred-Identity header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.3 of Table A.1 in clause A.3.

c8: The Privacy header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.4 of Table A.1 in clause A.3.

c9: The Proxy-Authenticate header is not to be used in the direction from the EUF to the SCF, according to clause 10.2.1.20.27 in the main body. In other words, 401/407 responses themselves are not to be used.

c10: The Proxy-Authenticate header is not to be used in 401 responses, according to 10.2.1.20.27 of Table A.1 in clause A.3. In other words, 401 response itself is not to be used.

c11: The Security-Server header is not applicable to responses from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c12: To be used in the case that AKA authentication is used or TLS connection of call control signals is used (Table I.11, Items 1 and 2, Appendix I, Table I.4, Item 3).

c13: The WWW-Authenticate header is applicable only to the REGISTER request authentication, according to 10.2.1.20.44 of Table A.1 in clause A.3. In other words, 401/407 responses themselves are not to be used.

NOTE – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

VI.4 CANCEL

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

VI.4.1 Supported headers in the CANCEL request

Table VI.5 – Supported headers in the CANCEL request

Message type: Request
Method: CANCEL

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
`Accept-Contact`	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
`Authorization`	[RFC 3261]	o	–	–	c2	c2	
`Call-ID`	[RFC 3261]	m	m	m			
`Content-Length`	[RFC 3261]	t	t	t			
`CSeq`	[RFC 3261]	m	m	m			
`Date`	[RFC 3261]	o	o	o			(Note)
`From`	[RFC 3261]	m	m	m			
`Max-Forwards`	[RFC 3261]	m	m	m			
`Privacy`	[RFC 3323]	o	–	–	c3	c3	
`Reason`	[RFC 3326]	o	o	o			(Note)
`Record-Route`	[RFC 3261]	o	o	o			(Note)
`Reject-Contact`	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
`Request-Disposition`	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
`Route`	[RFC 3261]	c	c	–		c4	
`Supported`	[RFC 3261]	o	o	o			(Note)
`Timestamp`	[RFC 3261]	o	o	o			(Note)
`To`	[RFC 3261]	m	m	m			
`User-Agent`	[RFC 3261]	o	o	o			(Note)
`Via`	[RFC 3261]	m	m	m			

Table VI.5 – Supported headers in the CANCEL request

Message type: Request
Method: CANCEL

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available over the UNI, the header information is handled as valid information (Table I.7, Item 6). c2: The `Authorization` header is used only when `REGISTER` requests from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Table A.1 in clause A.3. c3: The `Privacy` header is applicable only to requests outside existing dialogues except for `REGISTER`, according to 10.2.2.2.4 of Table A.1 in clause A.3. c4: The `Route` header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body. NOTE – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.							

VI.4.2 Supported headers in the CANCEL response

Table VI.6 – Supported headers in the CANCEL response

Message type: Response
Method: CANCEL

Header	Application	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
`Call-ID`		[RFC 3261]	m	m	m			
`Content-Length`		[RFC 3261]	t	t	t			
`CSeq`		[RFC 3261]	m	m	m			
`Date`		[RFC 3261]	o	o	o			(Note)
`Error-Info`	300-699	[RFC 3261]	o	o	o			(Note)
`From`		[RFC 3261]	m	m	m			
`Privacy`		[RFC 3323]	o	–	–	c1	c1	

Table VI.6 – Supported headers in the CANCEL response

Message type: Response
Method: CANCEL

Header	Application	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
`Proxy-Authenticate`	401	[RFC 3261]	o	–	–	c2	c2	
`Reason`		[RFC 3326]	o	o	o			(Note)
`Record-Route`	18x 2xx	[RFC 3261]	o	o	o			(Note)
`Retry-After`	404 413 480 486	[RFC 3261]	o	o	o			(Note)
`Retry-After`	500 503	[RFC 3261]	o	o	o			(Note)
`Retry-After`	600 603	[RFC 3261]	o	o	o			(Note)
`Server`		[RFC 3261]	o	o	o			(Note)
`Supported`	2xx	[RFC 3261]	o	o	o			(Note)
`Timestamp`		[RFC 3261]	o	o	o			(Note)
`To`		[RFC 3261]	m	m	m			
`User-Agent`		[RFC 3261]	o	o	o			(Note)
`Via`		[RFC 3261]	m	m	m			
`Warning`		[RFC 3261]	o	o	o			(Note)

c1: The `Privacy` header is applicable only to requests outside existing dialogues except for `REGISTER`, according to 10.2.2.2.4 of Table A.1 in clause A.3.

c2: The `Proxy-Authenticate` header is not to be used in the direction from the EUF to the SCF, nor be used in `401` responses in the direction from the SCF to the EUF, according to 10.2.1.20.27 of Table A.1 in clause A.3. In other words, `401` response itself is not to be used.

NOTE – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

VI.5 INVITE

This message is used for call initiation.

VI.5.1 Supported headers in the INVITE request

Table VI.7 – Supported headers in the INVITE request

Message type: Request
Method: INVITE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF SCF Send	
Accept	[RFC 3261]	o	o	o			
Accept-Contact	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
Accept-Encoding	[RFC 3261]	o	o	o			
Accept-Language	[RFC 3261]	o	o	o			
Alert-Info	[RFC 3261]	o	o	o			(Note 1)
Allow	[RFC 3261]	o	m* / o	m* / o	c2	c2	
Allow-Events	[RFC 3265]	o	o	o	c3 (Table I.2, Items 10 to 15)	c3 (Table I.2, Items 10 to 15)	
Authorization	[RFC 3261]	o	–	–	c4	c4	
Call-ID	[RFC 3261]	m	m	m			
Call-Info	[RFC 3261]	o	o	o			(Note 1)
Contact	[RFC 3261]	m	m	m			
Content-Disposition	[RFC 3261]	o	o	o			
Content-Encoding	[RFC 3261]	o	o	o			
Content-Language	[RFC 3261]	o	o	o			
Content-Length	[RFC 3261]	t	t	t			
Content-Type	[RFC 3261]	*	*	*			
CSeq	[RFC 3261]	m	m	m			
Date	[RFC 3261]	o	o	o			(Note 1)
Expires	[RFC 3261]	o	o	o			(Note 1)
From	[RFC 3261]	m	m	m			

Table VI.7 – Supported headers in the INVITE request

Message type: Request
Method: INVITE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF SCF Send	
In-Reply-To	[RFC 3261]	o	o	o			(Note 1)
Join	[RFC 3911]	o	o	o	c5 (when Table I.7, Item 4 states that UNI condition are "Used in each session as necessary".)	c5 (when Table I.7, Item 4 states that UNI condition are "Used in each session as necessary".)	
			–	–	c5 (when Table I.7, Item 4 is stated "Not use" for UNI condition.)	c5 (when Table I.7, Item 4 is stated "Not use" for UNI condition.)	
Max-Forwards	[RFC 3261]	m	m	m			
MIME-Version	[RFC 3261]	o	o	o	c6	c6	
Min-SE	[RFC 4028]	o	o	o	c7	c7	
Organization	[RFC 3261]	o	o	o			(Note 1)
P-Access-Network-Info	[RFC 3455]	o	o	–		c8	(Note 1)
P-Asserted-Identity	[RFC 3325]	o	–	o / –	c9	c9	
P-Called-Party-ID	[RFC 3455]	o	–	o / –	c10	c10	
P-Charging-Function-Addresses	[RFC 3455]	o	–	–	c11	c11	
P-Charging-Vector	[RFC 3455]	o	–	–	c11	c11	
P-Media-Authorization	[RFC 3313]	o	–	o	c12	c13 (when Table I.17, Item 1 is stated "Use" for UNI condition.)	
			–	–	c12	c13 (when able I.17, Item 1 is stated "Not use" for UNI condition.)	
P-Preferred-Identity	[RFC 3325]	o	o / –	–	c14	c14	
P-Visited-Network-ID	[RFC 3455]	o	–	–	c11	c11	

Table VI.7 – Supported headers in the INVITE request

Message type: Request
Method: INVITE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF SCF Send	
`Priority`	[RFC 3261]	o	o	o			(Note 1)
`Privacy`	[RFC 3323]	o	o / –	o / –	c15	c15	
`Proxy-Authorization`	[RFC 3261]	o	o	–	c16 (when Table I.11, Item 2 is stated "Perform HTTP Digest authentication" for UNI condition.)	c17	
			–	–	c16 (when Table I.11, Item 2 is stated other than "Perform HTTP Digest authentication" for UNI condition.)	c17	
`Proxy-Require`	[RFC 3261]	o	o	–		c18	
`Reason`	[RFC 3326]	o	– / o	– / o	(Note 2)	(Note 2)	(Note 1)
`Record-Route`	[RFC 3261]	o	o	o			
`Referred-By`	[RFC 3892]	o	o	o	c19 (Table I.2, Items 6 to 9)	c19 (Table I.2, Items 6 to 9)	
`Reject-Contact`	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
`Replaces`	[RFC 3891]	o	o	o	c20 (when Table I.7, Item 3 states that UNI condition are "Used in each session as necessary".)	c20 (when Table I.7, Item 3 states that UNI condition are "Used in each session as necessary".)	
			–	–	c21 (when Table I.7, Item 3 is stated "Not use" for UNI condition.)	c21 (when Table I.7, Item 3 is stated "Not use" for UNI condition.)	
`Reply-To`	[RFC 3261]	o	o	o			(Note 1)
`Request-Disposition`	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
`Require`	[RFC 3261]	c	c	c	c22	c22	

Table VI.7 – Supported headers in the INVITE request

Message type: Request
Method: INVITE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF SCF Send	
Route	[RFC 3261]	c	m / c	–	c23 (when Table I.24, Item 1 is stated "Use" for UNI condition.)	c24	
			– / c	–	c23 (when Table I.24, Item 1 is stated "Not use" for UNI condition.)	c24	
Security-Client	[RFC 3329]	o	o	–	c24 (Table I.11, Items 1 and 2, Table I.4, Item 3)	c25	
Security-Verify	[RFC 3329]	o	o	–	c24 (Table I.11, Items 1 and 2, Table I.4, Item 3)	c25	
Session-Expires	[RFC 4028]	o	m	m	c7 (when Table I.7, Item 1 states that UNI condition are "Used in all sessions".)	c7 (when Table I.7, Item 1 states that UNI condition are "Used in all sessions".)	
			o	o	c7 (when Table I.7, Item 1 states that UNI condition are "Used in each session as necessary".)	c7 (when Table I.7, Item 1 states that UNI condition are "Used in each session as necessary".)	
Subject	[RFC 3261]	o	o	o			(Note 1)
Supported	[RFC 3261]	m*	m*	m*	c21	c21	
Timestamp	[RFC 3261]	o	o	o			(Note 1)
To	[RFC 3261]	m	m	m			
User-Agent	[RFC 3261]	o	o	o			(Note 1)
Via	[RFC 3261]	m	m	m			
Message body	[RFC 3261]	o	m	m	c26	c26	
c1: In the case that the terminal capabilities notification function, Caller Preferences (`pref tag`), is available over the UNI, the header information is handled as valid information (Table I.7, Item 6).							

Table VI.7 – Supported headers in the INVITE request

Message type: Request
Method: INVITE

<table>
<tr><th rowspan="2">Header</th><th rowspan="2">Reference</th><th rowspan="2">RFC status</th><th colspan="2">Status in this standard</th><th colspan="2">Application conditions</th><th rowspan="2">Remarks</th></tr>
<tr><th>EUF Send</th><th>SCF Send</th><th>EUF Send</th><th>SCF
SCF Send</th></tr>
<tr><td colspan="8">c2: The setting of Allow header is necessary for initial INVITE, according to clause 10.2.1.20.5. (Note that the initial INVITE without the setting is not handled as error when received.)
c3: In the case that SUBSCRIBE/NOTIFY is available over the UNI, the header information is handled as valid information (Table I.2, Items 10 to 15).
c4: The Authorization header is used only when REGISTER requests from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Table A.1 in clause A.3.
c5: In the case that the conference session participation function (join) is available over the UNI, the header can be used (Table I.7, Item 4).
c6: In the case that MIME Multipart is used in a message body, the header information is handled as valid information (Table I.10, Items 1 and 2).
c7: The header must be used as specified in clause 10.2.2.2.1 and 10.2.2.2.7 in the main body. In the case that Session-Timer is used, at least the setting of value to the Session-Expires header (delta-seconds) is necessary.
c8: The P-Access-Network-Info header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.
c9: The P-Asserted-Identity header can be set in requests outside existing dialogues (not to be used inside existing dialogues) only in the direction of messages from the SCF to the EUF except for REGISTER, and transmits the calling-party's information, according to 10.2.2.2.2 of Table A.1 in clause A.3 and Annex B. (It can be set to initial-INVITE, but not to be set to re-INVITE.)
c10: The P-Called-Party-ID header can be set in requests outside existing dialogues (not to be used inside existing dialogues) only in the direction of messages from the SCF to the EUF except for REGISTER, and performs the notification of the called-party, according to Annex B. (It can be set to initial-INVITE, but not to be set to re-INVITE.)
c11: The P-Charging-Vector, P-Charging-Function-Addresses, and P-Visited-Network-ID headers are not to be used, according to 10.1 of Table A.1 in clause A.3.
c12: Not to be used in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.
c13: In the case that a message body is set and the notification of an authorization token is performed by the P-Media-Authorization header, the header information is handled as valid information (Table I.17, Item 1).
c14: The P-Preferred-Identity header can be set in requests outside existing dialogues (not to be used inside existing dialogues) only in the direction of messages from the EUF to the SCF except for REGISTER, and transmits the calling-party's information that the EUF requests of notification, according to 10.2.2.2.3 of Table A.1 in clause A.3 and Annex B. (It can be set to initial-INVITE, but not to be set to re-INVITE.)
c15: The Privacy header can be set in requests outside existing dialogues (not to be used inside existing dialogues) except for REGISTER, and transmits the presentation/restriction information of the calling-party's information, according to 10.2.2.2.4 of Table A.1 in clause A.3. (It can be set to initial-INVITE, but not to be set to re-INVITE.)
c16: To be used in the case of performing HTTP Digest authentication to requests outside existing dialogues except for REGISTER (Table I.11, Item 2).
c17: The Proxy-Authorization header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.28 in the main body.
c18: The Proxy-Require header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.29 in the main body.
c19: The Referred-By header may be used as a result of using REFER (Table I.2, Items 6 to 9). In the case that REFER is available over the UNI, the header information may be handled as valid information. It does not guarantee that the Referred-By header is used as a result of using REFER.
c20: In the case that the dialogue replacement function (replaces) is available over the UNI, the header information can be used (Table I.7, Item 3).
c21: "timer" needs to be set to the Require header and the Supported header in terms of the context, according to clause 10.2.1.20.32 and clause 10.2.1.20.37 in the main body. ("timer"</td></tr>
</table>

Table VI.7 – Supported headers in the INVITE request

Message type: Request
Method: INVITE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF SCF Send	
should be contextually set to the Supported header of initial INVITE and re-INVITE.) c22: In the case that the pre-existing route function is used over the UNI, the setting of the Route header in an initial INVITE is necessary (Table I.24, Item 1). c23: The Route header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body. c24: To be handled as valid in the case that AKA authentication is used or TLS connection of call control signals is used (Table I.11, Items 1 and 2, Table I.4, Item 3). c25: The Security-Client and Security-Verify headers are not applicable to a request in the direction from the SCF to the EUF, according to 10.1 Table A.1 in clause A.3. c26: SDP offer is described in the body part of an INVITE request, according to 10.2.1.13 and 10.2.1.14 of Table A.1 in clause A.3. NOTE 1 – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier. NOTE 2 – The Reason header is specified in [RFC 3326], and it is applicable to all the requests inside existing dialogues, CANCEL, and all responses, according to the specification. Therefore, it can be used in re-INVITE, but cannot be used in initial INVITE.							

VI.5.2 Supported headers in the INVITE response

Table VI.8 – Supported headers in the INVITE response

Message type: Response
Method: INVITE

Header	Application	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Accept	2xx	[RFC 3261]	o	o	o			
Accept	415	[RFC 3261]	c	c	c			
Accept-Encoding	2xx	[RFC 3261]	o	o	o			
Accept-Encoding	415	[RFC 3261]	c	c	c			
Accept-Language	2xx	[RFC 3261]	o	o	o			
Accept-Language	415	[RFC 3261]	c	c	c			

Table VI.8 – Supported headers in the INVITE response

Message type: Response
Method: INVITE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Alert-Info	180	[RFC 3261]	o	o	o			(Note 1)
Allow	2xx	[RFC 3261]	m*	m*	m*			
Allow	405	[RFC 3261]	m	m	m			
Allow	others	[RFC 3261]	o	o	o			
Allow-Events	2xx	[RFC 3265]	o	o	o	c1 (Table I.2, Items 10 to 15)	c1 (Table I.2, Items 10 to 15)	
Authentication-Info	2xx	[RFC 3261]	o	–	–	c2	c2	
Call-ID		[RFC 3261]	m	m	m			
Call-Info		[RFC 3261]	o	o	o			(Note 1)
Contact	1xx	[RFC 3261]	o	o	o	c3	c3	
Contact	2xx	[RFC 3261]	m	m	m			
Contact	3xx	[RFC 3261]	o	o	o			(Note 2)
Contact	485	[RFC 3261]	o	o	o			
Content-Disposition		[RFC 3261]	o	o	o			
Content-Encoding		[RFC 3261]	o	o	o			
Content-Language		[RFC 3261]	o	o	o			
Content-Length		[RFC 3261]	t	t	t			
Content-Type		[RFC 3261]	*	*	*			
CSeq		[RFC 3261]	m	m	m			
Date		[RFC 3261]	o	o	o			(Note 1)
Error-Info	300-699	[RFC 3261]	o	o	o			(Note 1)
Expires		[RFC 3261]	o	o	o			(Note 1)
From		[RFC 3261]	m	m	m			
MIME-Version		[RFC 3261]	o	o	o	c4	c4	

Table VI.8 – Supported headers in the INVITE response

Message type: Response
Method: INVITE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Min-SE	422	[RFC 4028]	m	m	m	c5 (Table I.7, Item 1)	c5 (Table I.7, Item 1)	
Organization		[RFC 3261]	o	o	o			(Note 1)
P-Access-Network-Info		[RFC 3455]	o	o	–		c6	(Note 1)
P-Asserted-Identity		[RFC 3325]	o	–	–	c7	c7	
P-Charging-Function-Addresses		[RFC 3455]	o	–	–	c8	c8	
P-Charging-Vector		[RFC 3455]	o	–	–	c8	c8	
P-Media-Authorization	101-199	[RFC 3313]	o	–	o	c9	c10 (when Table I.17, Item 1 is stated "Use" for UNI condition.)	
				–	–	c9	c10 (when Table I.17, Item 1 is stated "Not use" for UNI condition.)	
P-Media-Authorization	2xx	[RFC 3313]	o	–	o	c9		
P-Preferred-Identity		[RFC 3325]	o	–	–	c11	c11	
Privacy		[RFC 3323]	o	–	–	c12	c12	
Proxy-Authenticate	401	[RFC 3261]	o	–	–	c13	c14	
Proxy-Authenticate	407	[RFC 3261]	m	–	m	c13		
Reason		[RFC 3326]	o	o	o			(Note 1)
Record-Route	18x 2xx	[RFC 3261]	o	o	o	c3	c3	
Reply-To		[RFC 3261]	o	o	o			(Note 1)
Require		[RFC 3261]	c	c	c	c3, c5	c3, c5	
Retry-After	404 413	[RFC 3261]	o	o	o			(Note 1)

Table VI.8 – Supported headers in the INVITE response

Message type: Response
Method: INVITE

Header	Application	Reference	RFC status	Status in this standard: EUF Send	Status in this standard: SCF Send	Application conditions: EUF Send	Application conditions: SCF Send	Remarks
	480 486							
Retry-After	500 503	[RFC 3261]	o	o	o			(Note 1)
Retry-After	600 603	[RFC 3261]	o	o	o			(Note 1)
RSeq	1xx	[RFC 3262]	o	o	o	c3	c3	
Security-Server	421 494	[RFC 3329]	o	–	o	c15	c16 (Table I.11, Items 1 and 2, Table I.4, Item 3)	
Server		[RFC 3261]	o	o	o			(Note 1)
Session-Expires	2xx	[RFC 4028]	o	m	m	c5 (when Table I.7, Item 1 states that UNI conditions are "Used in all sessions".)	c5 (when Table I.7, Item 1 states that UNI conditions are "Used in all sessions".)	
				o	o	c5 (when Table I.7, Item 1 states that UNI conditions are "Used in each session as necessary".)	c5 (when Table I.7, Item 1 states that UNI conditions are "Used in each session as necessary".)	
Supported	2xx	[RFC 3261]	m*	m*	m*			
Timestamp		[RFC 3261]	o	o	o			(Note 1)
To		[RFC 3261]	m	m	m			
Unsupported	420	[RFC 3261]	m	m	m			
User-Agent		[RFC 3261]	o	o	o			(Note 1)
Via		[RFC 3261]	m	m	m			
Warning	488	[RFC 3261]	o	o	o	c17	c17	
Warning	others	[RFC 3261]	o	o	o			(Note 1)
WWW-Authenticate	401	[RFC 3261]	m	–	–	c18	c18	

Table VI.8 – Supported headers in the INVITE response

Message type: Response
Method: INVITE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
WWW-Authenticate	407	[RFC 3261]	o	–	–	c18	c18	
Message body		[RFC 3261]	o	o	o			

c1: In the case that SUBSCRIBE/NOTIFY is available over the UNI, the header information is handled as valid information (Table I.2, Items 10 to 15).

c2: Update of authentication information by the Authentication-Info header is not performed because the Authorization header is not to be used in the corresponding request.

c3: In the case of providing a reliable provisional response, the setting of "100rel" to the Require header and the setting of the RSeq header are necessary, according to clause 10.2.2.2.6 in the main body. The setting of the Contact header is necessary to receive a subsequent PRACK request. In the case that the Record-Route header is set to the 2xx response to an INVITE request, the Record-Route header of the same content should be set to the reliable provisional response as well.

c4: In the case that MIME Multipart is used in a message body, the header information is handled as valid information (Table I.10, Items 1 and 2).

c5: The header must be used as specified in clause 10.2.1.20.32, 10.2.2.1 and 10.2.2.2.7 in the main body. In the case that Session-Timer is used, at least the setting of value to the Session-Expires header (delta-seconds) is necessary. In the case that the refresher is "uac", the setting of "timer" to the Require header is necessary (Table I.7, Item 1).

c6: The P-Access-Network-Info header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c7: The P-Asserted-Identity header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.2 of Table A.1 in clause A.3.

c8: The P-Charging-Vector and P-Charging-Function-Addresses headers are not to be used, according to 10.1 of Table A.1 in clause A.3.

c9: Not to be used in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c10: In the case that a message body is set and the notification of an authorization token is performed by the P-Media-Authorization header, the header information is handled as valid information (Table I.17, Item 1).

c11: The P-Preferred-Identity header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.3 of Table A.1 in clause A.3.

c12: The Privacy header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.4 of Table A.1 in clause A.3.

c13: The Proxy-Authenticate header is not to be used in the direction from the EUF to the SCF, according to clause 10.2.1.20.27 in the main body. In other words, 401/407 responses themselves are not to be used.

c14: The Proxy-Authenticate header is not to be used in 401 responses, according to 10.2.1.20.27 of Table A.1 in clause A.3.

c15: The Security-Server header is not applicable to the response from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c16: To be used in the case that AKA authentication is used or TLS connection of call control signals is used (Table I.11, Items 1 and 2; Table I.4, Item 3).

c17: Incompatibility of IP version or media type can be notified by setting the Warning header in the 488 (Not Acceptable Here) response and using the set values in Annex e, according to 13 of Table A.1 in clause A.3 and Annex e.

c18: The WWW-Authenticate header is applicable only to the REGISTER request authentication, according to 10.2.1.20.44 of Table A.1 in clause A.3. In other words, 401/407 responses themselves are not to be used.

Table VI.8 – Supported headers in the INVITE response

Message type: Response
Method: INVITE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
NOTE 1 – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier. NOTE 2 – In the case that the redirection function of the `3xx` response is available over the UNI, the header information is handled as valid information, according to clause 10.2.1.8.3 in the main body (Table I.12, Items 1 and 2).								

VI.6 MESSAGE

This message is used for stateless short message services. `MESSAGE` can be used outside existing dialogues.

VI.6.1 Supported headers in the MESSAGE request

Table VI.9 – Supported headers in the `MESSAGE` request

Message type: Request
Method: MESSAGE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF sends	SCF sends	
`Accept-Contact`	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
`Allow`	[RFC 3261]	o	o	o			
`Authorization`	[RFC 3261]	o	–	–	c2	c2	
`Call-ID`	[RFC 3261]	m	m	m			
`Call-Info`	[RFC 3261]	o	o	o			(Note 1)
`Content-Disposition`	[RFC 3261]	o	o	o			
`Content-Encoding`	[RFC 3261]	o	o	o			
`Content-Language`	[RFC 3261]	o	o	o			
`Content-Length`	[RFC 3261]	t	t	t			

Table VI.9 – Supported headers in the MESSAGE request

Message type: Request
Method: MESSAGE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF sends	SCF sends	
Content-Type	[RFC 3261]	*	*	*			
CSeq	[RFC 3261]	m	m	m			
Date	[RFC 3261]	o	o	o			(Note 1)
Expires	[RFC 3261]	o	o	o			(Note 1)
From	[RFC 3261]	m	m	m			
In-Reply-To	[RFC 3261]	o	o	o			(Note 1)
Max-Forwards	[RFC 3261]	m	m	m			
MIME-Version	[RFC 3261]		o	o	c3	c3	
Organization	[RFC 3261]	o	o	o			(Note 1)
P-Access-Network-Info	[RFC 3455]	o	o	–		c4	(Note 1)
P-Asserted-Identity	[RFC 3325]		–	o / –	c5	c5	
P-Called-Party-ID	[RFC 3455]	o	–	o / –	c6	c6	
P-Charging-Function-Addresses	[RFC 3455]	o	–	–	c7	c7	
P-Charging-Vector	[RFC 3455]	o	–	–	c7	c7	
P-Preferred-Identity	[RFC 3325]		o / –	–	c8	c8	
P-Visited-Network-ID	[RFC 3455]	o	–	–	c7	c7	
Priority	[RFC 3261]	o	o	o			(Note 1)
Privacy	[RFC 3323]	o	o / –	o / –	c9	c9	
Proxy-Authorization	[RFC 3261]	o	o	–	c10 (when Table I.11, Item 2 is stated "Perform HTTP Digest authentication" for UNI condition.)	c11	
			–	–	c10 (when Table I.11, Item 2 is stated other than "Perform HTTP Digest authentication" for UNI condition.)	c11	

Table VI.9 – Supported headers in the MESSAGE request

Message type: Request
Method: MESSAGE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF sends	SCF sends	
Proxy-Require	[RFC 3261]	o	o	–		c12	
Reason	[RFC 3326]	o	– / o	- / o	(Note 2)	(Note 2)	(Note 1)
Referred-By	[RFC 3892]		o	o	c13 (Table I.2, Items 6 to 9)	c13 (Table I.2, Items 6 to 9)	(Note 1)
Reject-Contact	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
Reply-To	[RFC 3261]	o	o	o			(Note 1)
Request-Disposition	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
Require	[RFC 3261]	c	c	c			
Route	[RFC 3261]	c	m / c	–	c14 (when Table I.24, Item 1 is stated "Use" for UNI condition.)	c15	
			– / c	–	c14 (when Table I.24, Item 1 is stated "Not use" for UNI condition.)	c15	
Security-Client	[RFC 3329]	o	o	–	c16 (Table I.11, Items 1 and 2, Table I.4, Item 3)	c17	
Security-Verify	[RFC 3329]	o	o	–	c16 (Table I.11, Items 1 and 2, Table I.4, Item 3)	c17	
Subject	[RFC 3261]	o	o	o			(Note 1)
Timestamp	[RFC 3261]	o	o	o			(Note 1)
To	[RFC 3261]	m	m	m			
User-Agent	[RFC 3261]	o	o	o			(Note 1)
Via	[RFC 3261]	m	m	m			
Message body	[RFC 3261]		o	o			

c1: In the case that the terminal capabilities notification function, Caller Preferences (pref tag), is available over the UNI, the header information is handled as valid information (Table I.7, Item 6).
c2: The Authorization header is used only when a REGISTER request from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Table A.1 in clause A.3.
c3: In the case that MIME Multipart is used in a message body, the header information is handled as valid information (Table I.10, Items 3 and 4).
c4: The P-Access-Network-Info header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.
c5: The P-Asserted-Identity header can be set in requests outside existing dialogues (not to be used inside existing dialogues) only in the direction of messages from the SCF to the EUF

Table VI.9 – Supported headers in the MESSAGE request

Message type: Request
Method: MESSAGE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF sends	SCF sends	

except for REGISTER, and transmits the calling-party's information, according to 10.2.2.2.2 of Table A.1 in clause A.3 and Annex B. (It can be set to MESSAGE requests outside existing dialogues, but not to be set to MESSAGE requests inside existing dialogues.)

c6: The P-Called-Party-ID header can be set in requests outside existing dialogues (not to be used inside existing dialogues) only in the direction of messages from the SCF to the EUF except for REGISTER, and performs the notification of the called-party, according to Annex B. (It can be set to MESSAGE requests outside existing dialogues, but not to be set to MESSAGE requests inside existing dialogues.)

c7: The P-Charging-Vector, P-Charging-Function-Addresses, and P-Visited-Network-ID headers are not to be used, according to 10.1 of Table A.1 in clause A.3.

c8: The P-Preferred-Identity header can be set in requests outside existing dialogues (not to be used inside existing dialogues) only in the direction of messages from the EUF to the SCF except for REGISTER, and transmits the calling-party's information that the EUF requests of notification, according to 10.2.2.2.3 of Table A.1 in clause A.3 and Annex B. (It can be set to initial-INVITE, but not to be set to re-INVITE.)

c9: The Privacy header can be set in requests outside existing dialogues (not to be used inside existing dialogues) except for REGISTER, and transmits the presentation/restriction information of the calling-party's information, according to 10.2.2.2.4 of Table A.1 in clause A.3. (It can be set to MESSAGE requests outside existing dialogues, but not to be set to MESSAGE requests inside existing dialogues.)

c10: To be used in the case of performing HTTP Digest authentication to requests outside existing dialogues except for REGISTER (Table I.11, Item 2).

c11: The Proxy-Authorization header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.28 in the main body.

c12: The Proxy-Require header is not to be used in the direction from the SCF to the EUF, according to 10.2.1.20.29 of Table A.1 in clause A.3.

c13: The Referred-By header may be used as a result of using REFER (Table I.2, Items 6 to 9). In the case that REFER is available over the UNI, the header information may be handled as valid information. It does not guarantee that the Referred-By header is used as a result of using REFER.

c14: In the case that the pre-existing route function is used over the UNI, the setting of the Route header in a MESSAGE requests outside existing dialogues is necessary (Table I.24, Item 1).

c15: The Route header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body.

c16: To be handled as valid in the case that AKA authentication is used or TLS connection of call control signals is used (Table I.11, Items 1 and 2, Table I.4, Item 3).

c17: The Security-Client and Security-Verify headers are not applicable to a request in the direction from the SCF to the EUF, according to 10.1 of Table A.1 in clause A.3.

NOTE 1 – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

NOTE 2 – The Reason header is specified in [RFC 3326], and it is applicable to all the requests inside existing dialogues, CANCEL, and all responses, according to the specification. Therefore, it can be used in MESSAGE requests inside existing dialogues, but cannot be used in MESSAGE requests outside existing dialogues.

VI.6.2 Supported headers in the MESSAGE response

Table VI.10 – Supported headers in the MESSAGE response

Message type: Response
Method: MESSAGE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Accept	415	[RFC 3261]	m*	m*	m*			
Accept-Encoding	415	[RFC 3261]	m*	m*	m*			
Accept-Language	415	[RFC 3261]	m*	m*	m*			
Allow	2xx	[RFC 3261]	o	o	o			
Allow	405	[RFC 3261]	m	m	m			
Allow	others	[RFC 3261]	o	o	o			
Authentication-Info	2xx	[RFC 3261]	o	–	–	c1	c1	
Call-ID		[RFC 3261]	m	m	m			
Call-Info		[RFC 3261]	o	o	o			(Note 1)
Contact	3xx	[RFC 3261]	o	o	o			(Note 2)
Contact	485	[RFC 3261]	o	o	o			
Content-Disposition		[RFC 3261]	o	o	o			(Note 1)
Content-Encoding		[RFC 3261]	o	o	o			(Note 1)
Content-Language		[RFC 3261]	o	o	o			(Note 1)
Content-Length		[RFC 3261]	t	t	t			
Content-Type		[RFC 3261]	*	*	*			(Note 1)
CSeq		[RFC 3261]	m	m	m			
Date		[RFC 3261]	o	o	o			(Note 1)
Error-Info	300-699	[RFC 3261]	o	o	o			(Note 1)
Expires		[RFC 3261]	o	o	o			(Note 1)
From		[RFC 3261]	m	m	m			

Table VI.10 – Supported headers in the MESSAGE response

Message type: Response
Method: MESSAGE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
MIME-Version	4xx- 6xx	[RFC 3261]		o	o	c2	c2	(Note 1)
Organization		[RFC 3261]	o	o	o			(Note 1)
P-Access-Network-Info		[RFC 3455]	o	o	–		c3	(Note 1)
P-Charging-Function-Addresses		[RFC 3455]	o	–	–	c4	c4	
P-Charging-Vector		[RFC 3455]	o	–	–	c4	c4	
Privacy		[RFC 3323]	o	–	–	c5	c5	
Proxy-Authenticate	401	[RFC 3261]	o	–	–	c6	c7	
Proxy-Authenticate	407	[RFC 3261]	m	–	m	c6		
Reason		[RFC 3326]	o	o	o			(Note 1)
Reply-To		[RFC 3261]	o	o	o			(Note 1)
Require		[RFC 3261]	c	c	c			(Note 1)
Retry-After	404 413 480 486	[RFC 3261]	o	o	o			(Note 1)
Retry-After	500 503	[RFC 3261]	o	o	o			(Note 1)
Retry-After	600 603	[RFC 3261]	o	o	o			(Note 1)
Security-Server	421 494	[RFC 3329]	o	–	o	c8	c9 (Table I.11, Items 1 and 2, Table I.4, Item 3)	
Server		[RFC 3261]	o	o	o			(Note 1)
Timestamp		[RFC 3261]	o	o	o			(Note 1)

Table VI.10 – Supported headers in the MESSAGE response

Message type: Response
Method: MESSAGE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
To		[RFC 3261]	m	m	m			
Unsupported	420	[RFC 3261]	o	m	m	(Note 3)	(Note 3)	
User-Agent		[RFC 3261]	o	o	o			(Note 1)
Via		[RFC 3261]	m	m	m			
Warning		[RFC 3261]	o	o	o			(Note 1)
WWW-Authenticate	401	[RFC 3261]	m	–	–	c10	c10	
WWW-Authenticate	407	[RFC 3261]	o	–	–	c10	c10	
Message body	2xx-3xx	[RFC 3261]	–	–	–			
Message body	4xx-6xx	[RFC 3261]	o	o	o			(Note 1)

c1: Update of authentication information by the Authentication-Info header is not performed because the Authorization header is not to be used in the corresponding request.

c2: In the case that MIME Multipart is used in a message body, the header information is handled as valid information (Table I.10, Items 3 and 4).

c3: The P-Access-Network-Info header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c4: The P-Charging-Vector and P-Charging-Function-Addresses headers are not to be used, according to 10.1 of Table A.1 in clause A.3.

c5: The Privacy header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.4 of Table A.1 in clause A.3.

c6: The Proxy-Authenticate header is not to be used in the direction from the EUF to the SCF, according to clause 10.2.1.20.27 in the main body. In other words, 401/407 responses themselves are not to be used.

c7: The Proxy-Authenticate header is not to be used in 401 responses, according to 10.2.1.20.27 of Table A.1 in clause A.3.

c8: The Security-Server header is not applicable to the response from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c9: To be used in the case that AKA authentication is used or TLS connection of call control signals is used (Table I.11, Items 1 and 2, Table I.4, Item 3).

c10: The WWW-Authenticate header is applicable only to the REGISTER request authentication, according to 10.2.1.20.44 of Table A.1 in clause A.3. In other words, 401/407 responses themselves are not to be used.

NOTE 1 – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

Table VI.10 – Supported headers in the MESSAGE response

Message type: Response
Method: MESSAGE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
NOTE 2 – In the case that the redirection function of the `3xx` response is available over the UNI, the header information is handled as valid information, according to clause 10.2.1.8.3 in the main body (Table I.12, Items 1 and 2). NOTE 3 – Although specified as "o" in [RFC 3903], the Unsupported header is set to be "m" based on [RFC 3261].								

VI.7 NOTIFY

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

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

VI.7.1 Supported headers in the NOTIFY request

Table VI.11 – Supported headers in the NOTIFY request

Message type: Request
Method: NOTIFY

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
`Accept`	[RFC 3261]	o	o	o			
`Accept-Contact`	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
`Accept-Encoding`	[RFC 3261]	o	o	o			
`Accept-Language`	[RFC 3261]	o	o	o			
`Allow`	[RFC 3261]	o	o	o			
`Allow-Events`	[RFC 3265	o	o	o			
`Authorization`	[RFC 3261]	o	–	–	c2	c2	

Table VI.11 – Supported headers in the NOTIFY request

Message type: Request
Method: NOTIFY

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
`Call-ID`	[RFC 3261]	m	m	m			
`Call-Info`	[RFC 3261]		–	–	(Note 2)	(Note 2)	
`Contact`	[RFC 3261]	m	m	m			
`Content-Disposition`	[RFC 3261]	o	o	o			
`Content-Encoding`	[RFC 3261]	o	o	o			
`Content-Language`	[RFC 3261]	o	o	o			
`Content-Length`	[RFC 3261]	t	t	t			
`Content-Type`	[RFC 3261]	*	*	*			
`CSeq`	[RFC 3261]	m	m	m			
`Date`	[RFC 3261]	o	o	o			(Note 1)
`Event`	[RFC 3265]	m	m	m			
`From`	[RFC 3261]	m	m	m			
`Max-Forwards`	[RFC 3261]	m	m	m			
`MIME-Version`	[RFC 3261]	o	o	o			
`P-Access-Network-Info`	[RFC 3455]	o	o	–		c3	(Note 1)
`P-Asserted-Identity`	[RFC 3325]	o	–	–	c4	c4	
`P-Charging-Function-Addresses`	[RFC 3455]	o	–	–	c5	c5	
`P-Charging-Vector`	[RFC 3455]	o	–	–	c5	c5	
`P-Preferred-Identity`	[RFC 3325]	o	–	–	c6	c6	
`Privacy`	[RFC 3323]	o	–	–	c7	c7	

Table VI.11 – Supported headers in the NOTIFY request

Message type: Request
Method: NOTIFY

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Proxy-Authorization	[RFC 3261]	o	o	–	c8 (when Table I.11, Item 2 is stated "Perform HTTP Digest authentication".)	c9	
			–	–	c8 (when Table I.11, Item 2 is stated other than "Perform HTTP Digest authentication".)	c9	
Proxy-Require	[RFC 3261]	o	o	–		c10	
Reason	[RFC 3326]	o	o	o			(Note 1)
Record-Route	[RFC 3261]	o	o	o			(Note 1)
Reject-Contact	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
Request-Disposition	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
Require	[RFC 3261]	o	o	o			
Route	[RFC 3261]	c	c	–		c11	
Security-Client	[RFC 3329]	o	o	–	c12 (Table I.11, Items 1 and 2, Table I.4, Item 3)	c13	
Security-Verify	[RFC 3329]	o	o	–	c12 (Table I.11, Items 1 and 2, Table I.4, Item 3)	c13	
Subscription-State	[RFC 3265]	m	m	m			
Supported	[RFC 3261]	o	o	o			
Timestamp	[RFC 3261]	o	o	o			(Note 1)
To	[RFC 3261]	m	m	m			
User-Agent	[RFC 3261]	o	o	o			(Note 1)
Via	[RFC 3261]	m	m	m			
Warning	[RFC 3261]	o	o	o			(Note 1)
Message body	[RFC 3261]		o	o	(Note 3)	(Note 3)	

Table VI.11 – Supported headers in the NOTIFY request

Message type: Request
Method: NOTIFY

<table>
<tr><th rowspan="2">Header</th><th rowspan="2">Reference</th><th rowspan="2">RFC status</th><th colspan="2">Status in this standard</th><th colspan="2">Application conditions</th><th rowspan="2">Remarks</th></tr>
<tr><th>EUF Send</th><th>SCF Send</th><th>EUF Send</th><th>SCF Send</th></tr>
<tr><td colspan="8">c1: In the case that the terminal capabilities notification function, Caller Preferences (pref tag), is available over the UNI, the header information is handled as valid information (Table I.7, Item 6).
c2: The Authorization header is used only when a REGISTER request from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Table A.1 in clause A.3.
c3: The P-Access-Network-Info header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.
c4: The P-Asserted-Identity header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.2 of Table A.1 in clause A.3.
c5: The P-Charging-Vector and P-Charging-Function-Addresses headers are not to be used, according to 10.1 of Table A.1 in Table A.1.
c6: The P-Preferred-Identity header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.3 of Table A.1 in clause A.3.
c7: The Privacy header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.4 of Table A.1 in clause A.3. (NOTIFY is used within a subscription (equivalent to a dialogue). Therefore, the header is not applicable.)
c8: To be used in the case of performing HTTP Digest authentication to requests outside existing dialogues except for REGISTER (Table I.11, Item 2).
c9: The Proxy-Authorization header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.28 in the main body.
c10: The Proxy-Require header is not to be used in the direction from the SCF to the EUF, according to 10.2.1.20.29 of Table A.1 in clause A.3.
c11: The Route header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body.
c12: To be handled as valid in the case that AKA authentication is used or TLS connection of call control signals is used (Table I.11, Items 1 and 2, Table I.4, Item 3).
c13: The Security-Client and Security-Verify headers are not applicable to a request in the direction from the SCF to the EUF, according to 10.1 of Table A.1 in clause A.3.
NOTE 1 – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.
NOTE 2 – The Call-Info header shows additional information about the sender of the messages. There is no description of the application of the header into NOTIFY in RFCs and other documents. Therefore, it is difficult to define its reaction when using the header in NOTIFY. Furthermore, security risks of Call-Info are noted in [RFC 3261]. An ill-prepared use of the header should be avoided.
NOTE 3 – It is used when additional information is present. Formatting and other features depend on Content-Type.</td></tr>
</table>

VI.7.1 Supported headers in the NOTIFY response

Table VI.12 – Supported headers in the NOTIFY response

Message type: Response
Method: NOTIFY

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Accept	415		o	o	o			
Accept-Encoding	415	[RFC 3261]	o	o	o			
Accept-Language	415	[RFC 3261]	o	o	o			
Allow	2xx	[RFC 3261]	o	o	o			
Allow	405	[RFC 3261]	m	m	m			
Allow	others	[RFC 3261]	o	o	o			
Allow-Events	2xx	[RFC 3265]	o	o	o			
Allow-Events	489	[RFC 3265]	m	m	m			
Authentication-Info	2xx	[RFC 3261]	o	–	–	c1	c1	
Call-ID		[RFC 3261]	m	m	m			
Call-Info		[RFC 3261]		–	–	(Note 2)	(Note 2)	
Contact	1xx	[RFC 3261]	o	o	o			
Contact	2xx	[RFC 3261]	o	o	o			
Contact	3xx	[RFC 3261]	m	–	–	c2	c2	
Contact	485	[RFC 3261]	o	o	o			
Content-Disposition		[RFC 3261]	o	o	o			(Note 1)
Content-Encoding		[RFC 3261]	o	o	o			(Note 1)
Content-Language		[RFC 3261]	o	o	o			(Note 1)
Content-Length		[RFC 3261]	t	t	t			
Content-Type		[RFC 3261]	*	*	*			(Note 1)
CSeq		[RFC 3261]	m	m	m			
Date		[RFC 3261]	o	o	o			(Note 1)

Table VI.12 – Supported headers in the NOTIFY response

Message type: Response
Method: NOTIFY

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Error-Info	300-699	[RFC 3261]	o	o	o			(Note 1)
From		[RFC 3261]	m	m	m			
MIME-Version		[RFC 3261]	o	o	o			(Note 1)
P-Access-Network-Info		[RFC 3455]	o	o	–		c3	(Note 1)
P-Asserted-Identity		[RFC 3325]	o	–	–	c4	c4	
P-Charging-Function-Addresses		[RFC 3455]	o	–	–	c5	c5	
P-Charging-Vector		[RFC 3455]	o	–	–	c5	c5	
P-Preferred-Identity		[RFC 3325]	o	–	–	c6	c6	
Privacy		[RFC 3323]	o	–	–	c7	c7	
Proxy-Authenticate	407	[RFC 3261]	m	–	m	c8		
Reason		[RFC 3326]	o	o	o			(Note 1)
Record-Route	2xx 401 484	[RFC 3261]	o	o	o			(Note 1)
Require		[RFC 3261]	o	o	o			
Retry-After	404 413 480 486	[RFC 3261]	o	o	o			(Note 1)
Retry-After	500 503	[RFC 3261]	o	o	o			(Note 1)
Retry-After	600 603	[RFC 3261]	o	o	o			(Note 1)
RSeq	1xx	[RFC 3261]	o	–	–	(Note 3)	(Note 3)	

Table VI.12 – Supported headers in the NOTIFY response

Message type: Response
Method: NOTIFY

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Security-Server	421 494	[RFC 3329]	o	–	–	c9	c10 (Table I.11, Items 1 and 2, Table I.4, Item 3)	
Server		[RFC 3261]	o	o	o			(Note 1)
Supported	2xx	[RFC 3261]	o	o	o			
Timestamp		[RFC 3261]	o	o	o			(Note 1)
To		[RFC 3261]	m	m	m			
Unsupported	420	[RFC 3261]	o	m	m	(Note 4)	(Note 4)	
User-Agent		[RFC 3261]	o	o	o			(Note 1)
Via		[RFC 3261]	m	m	m			
Warning		[RFC 3261]	o	o	o			(Note 1)
WWW-Authenticate	401	[RFC 3261]	m	–	–	c11	c11	
Message body		[RFC 3261]		o	o	(Note 5)	(Note 5)	(Note 1)

c1: Update of authentication information by the Authentication-Info header is not performed because the Authorization header is not to be used in the corresponding request.

c2: Redirection using 3xx responses is not to be used, according to 10.2.1.8.3 of Table A.1 in clause A.3.

c3: The P-Access-Network-Info header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c4: The P-Asserted-Identity header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.2 of Table A.1 in clause A.3.

c5: The P-Charging-Vector and P-Charging-Function-Addresses headers are not to be used, according to 10.1 of Table A.1 in clause A.3.

c6: The P-Preferred-Identity header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.3 of Table A.1 in clause A.3.

c7: The Privacy header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.4 of Table A.1 in clause A.3.

c8: The Proxy-Authenticate header is not to be used in the direction from the EUF to the SCF, according to clause 10.2.1.20.27 in the main body. In other words, the 407 response itself is not to be used.

c9: The Security-Server header is not applicable to the response from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c10: To be used in the case that AKA authentication is used or TLS connection of call control signals is used (Table I.11, Items 1 and 2, Table I.4, Item 3).

c11: The WWW-Authenticate header is applicable only for the REGISTER request authentication, according to 10.2.1.20.44 of Table A.1 in clause A.3. In other words, 401 response itself is not to be used.

Table VI.12 – Supported headers in the NOTIFY response

Message type: Response
Method: NOTIFY

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
NOTE 1 – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier. NOTE 2 – The `Call-Info` header shows additional information about the sender of the messages. There is no description of the application of the header into `NOTIFY` in RFCs and other documents. Therefore, it is difficult to define its reaction when using the header in `NOTIFY`. Furthermore, security risks of `Call-Info` are noted in [RFC 3261]. An ill-prepared use of the header should be avoided. NOTE 3 – The `100rel` option (`PRACK`) is not to be used in NOTIFY. NOTE 4 – Although specified as "o" in [RFC 3265], the `Unsupported` header is set to be "m" based on [RFC 3261]. NOTE 5– It is used when notification information is present. Formatting and other features depend on Content-Type.								

VI.8 PRACK

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

VI.8.1 Supported headers in the PRACK request

Table VI.13 – Supported headers in the PRACK request

Message type: Request
Method: PRACK

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
`Accept`	[RFC 3261]	o	o	O			
`Accept-Contact`	[RFC 3841]	o	o	O	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
`Accept-Encoding`	[RFC 3261]	o	o	O			
`Accept-Language`	[RFC 3261]	o	o	O			

Table VI.13 – Supported headers in the PRACK request

Message type: Request
Method: PRACK

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Allow	[RFC 3261]	o	o	o			
Allow-Events	[RFC 3265]	o	o	o	c2 (Table I.2, Items 10 to 15)	c2 (Table I.2, Items 10 to 15)	
Authorization	[RFC 3261]	o	–	–	c3	c3	
Call-ID	[RFC 3261]	m	m	m			
Content-Disposition	[RFC 3261]	o	o	o			
Content-Encoding	[RFC 3261]	o	o	o			
Content-Language	[RFC 3261]	o	o	o			
Content-Length	[RFC 3261]	t	t	t			
Content-Type	[RFC 3261]	*	*	*			
CSeq	[RFC 3261]	m	m	m			
Date	[RFC 3261]	o	o	o			(Note)
From	[RFC 3261]	m	m	m			
Max-Forwards	[RFC 3261]	m	m	m			
MIME-Version	[RFC 3261]	o	o	o			
P-Access-Network-Info	[RFC 3455]	o	o	–		c4	(Note)
P-Charging-Function-Addresses	[RFC 3455]	o	–	–	c5	c5	
P-Charging-Vector	[RFC 3455]	o	–	–	c5	c5	
P-Media-Authorization	[RFC 3313]	o	–	o	c6	c7	
Privacy	[RFC 3323]	o	–	–	c8	c8	

Table VI.13 – Supported headers in the PRACK request

Message type: Request
Method: PRACK

<table>
<tr><th rowspan="2">Header</th><th rowspan="2">Reference</th><th rowspan="2">RFC status</th><th colspan="2">Status in this standard</th><th colspan="2">Application conditions</th><th rowspan="2">Remarks</th></tr>
<tr><th>EUF Send</th><th>SCF Send</th><th>EUF Send</th><th>SCF Send</th></tr>
<tr><td rowspan="2">Proxy-Authorization</td><td rowspan="2">[RFC 3261]</td><td rowspan="2">o</td><td>o</td><td>–</td><td>c9 (when Table I.11, Item 2 is stated "Perform HTTP Digest authentication".)</td><td>c10</td><td></td></tr>
<tr><td>–</td><td>–</td><td>c9 (when Table I.11, Item 2 is stated other than "Perform HTTP Digest authentication".)</td><td>c10</td><td></td></tr>
<tr><td>Proxy-Require</td><td>[RFC 3261]</td><td>o</td><td>o</td><td>–</td><td></td><td>c11</td><td></td></tr>
<tr><td>RAck</td><td>[RFC 3262]</td><td>m</td><td>m</td><td>m</td><td></td><td></td><td></td></tr>
<tr><td>Reason</td><td>[RFC 3326]</td><td>o</td><td>o</td><td>o</td><td></td><td></td><td>(Note)</td></tr>
<tr><td>Record-Route</td><td>[RFC 3261]</td><td>o</td><td>o</td><td>o</td><td></td><td></td><td>(Note)</td></tr>
<tr><td>Reject-Contact</td><td>[RFC 3841]</td><td>o</td><td>o</td><td>o</td><td>c1 (Table I.7, Item 6)</td><td>c1 (Table I.7, Item 6)</td><td></td></tr>
<tr><td>Request-Disposition</td><td>[RFC 3841]</td><td>o</td><td>o</td><td>o</td><td>c1 (Table I.7, Item 6)</td><td>c1 (Table I.7, Item 6)</td><td></td></tr>
<tr><td>Require</td><td>[RFC 3261]</td><td>c</td><td>c</td><td>c</td><td></td><td></td><td></td></tr>
<tr><td>Route</td><td>[RFC 3261]</td><td>c</td><td>c</td><td>–</td><td></td><td>c12</td><td></td></tr>
<tr><td>Supported</td><td>[RFC 3261]</td><td>o</td><td>o</td><td>o</td><td></td><td></td><td>(Note)</td></tr>
<tr><td>Timestamp</td><td>[RFC 3261]</td><td>o</td><td>o</td><td>o</td><td></td><td></td><td>(Note)</td></tr>
<tr><td>To</td><td>[RFC 3261]</td><td>m</td><td>m</td><td>m</td><td></td><td></td><td></td></tr>
<tr><td>User-Agent</td><td>[RFC 3261]</td><td>o</td><td>o</td><td>o</td><td></td><td></td><td>(Note)</td></tr>
<tr><td>Via</td><td>[RFC 3261]</td><td>m</td><td>m</td><td>m</td><td></td><td></td><td></td></tr>
<tr><td>Message body</td><td>[RF]C 3261]</td><td></td><td>o</td><td>o</td><td>c13 (Table I.22, Items 2 to 3)</td><td>c13 (Table I.22, Items 2 to 3)</td><td></td></tr>
<tr><td colspan="8">c1: In the case that the terminal capabilities notification function, Caller Preferences (pref tag), is available over the UNI, the header information is handled as valid information (Table I.7, Item 6).
c2: In the case that SUBSCRIBE/NOTIFY is available over the UNI, the header information is handled as valid information (Table I.2, Items 10 to 15).
c3: The Authorization header is used only when a REGISTER request from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Table A.1 in clause A.3.
c4: The P-Access-Network-Info header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.
c5: The P-Charging-Vector and P-Charging-Function-Addresses headers are not to be used, according to 10.1 of Table A.1 in clause A.3.</td></tr>
</table>

Table VI.13 – Supported headers in the PRACK request

Message type: Request
Method: PRACK

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
c6: Not to be used in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3. c7: In the case that SDP offer is performed by `PRACK`, the header information is handled as valid information (Table I.22, Item 3). c8: The Privacy header is applicable only to requests outside existing dialogues except for `REGISTER`, according to 10.2.2.2.4 of Table A.1 in clause A.3. c9: To be used in the case of performing HTTP Digest authentication to requests outside existing dialogues except for `REGISTER` (Table I.11, Item 2). c10: The `Proxy-Authorization` header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.28 in the main body. c11: The `Proxy-Require` header is not to be used in the direction from the SCF to the EUF, according to 10.2.1.20.29 of Table A.1 in clause A.3. c12: The `Route` header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body. c13: The message body part of `PRACK` should be supported, according to clause 10.2.1.7.4.1 in the main body. In the case that the SDP setting of the body part is available over the UNI, the message body information is handled as valid information (Table I.22, Items 2 to 3). NOTE – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.							

VI.8.2 Supported headers in the PRACK response

Table VI.14 – Supported headers in the PRACK response

Message type: Response
Method: PRACK

Header	Application	Reference	RFC status	Status in this standard		Application conditions		Remarks
				SCF Send	EUF Send	EUF Send	SCF Send	
`Accept`	415	[RFC 3261]	c	c	c			
`Accept-Encoding`	415	[RFC 3261]	c	c	c			
`Accept-Language`	415	[RFC 3261]	c	c	c			
`Allow`	2xx	[RFC 3261]	o	o	o			

Table VI.14 – Supported headers in the PRACK response

Message type: Response
Method: PRACK

Header	Application	Reference	RFC status	Status in this standard		Application conditions		Remarks
				SCF Send	EUF Send	EUF Send	SCF Send	
Allow	405	[RFC 3261]	m	m	m			
Allow	others	[RFC 3261]	o	o	o			
Allow-Events	2xx	[RFC 3265]	o	o	o	c1 (Table I.2, Items 10 to 15)	c1 (Table I.2, Items 10 to 15)	
Authentication-Info	2xx	[RFC 3261]	o	–	–	c2	c2	
Call-ID		[RFC 3261]	m	m	m			
Contact	3xx	[RFC 3261]	o	–	–	c3	c3	
Contact	485	[RFC 3261]	o	o	o			
Content-Disposition		[RFC 3261]	o	o	o			
Content-Encoding		[RFC 3261]	o	o	o			
Content-Language		[RFC 3261]	o	o	o			
Content-Length		[RFC 3261]	t	t	t			
Content-Type		[RFC 3261]	*	*	*			
CSeq		[RFC 3261]	m	m	m			
Date		[RFC 3261]	o	o	o			(Note)
Error-Info	300-699	[RFC 3261]	o	o	o			(Note)
From		[RFC 3261]	m	m	m			
MIME-Version		[RFC 3261]	o	o	o			
P-Access-Network-Info		[RFC 3455]	o	o	–		c4	(Note)
P-Charging-Function-Addresses		[RFC 3455]	o	–	–	c5	c5	
P-Charging-Vector		[RFC 3455]	o	–	–	c5	c5	
P-Media-Authorization	2xx	[RFC 3313]	o	–	o	c6	c7	

Table VI.14 – Supported headers in the PRACK response

Message type: Response
Method: PRACK

Header	Application	Reference	RFC status	Status in this standard		Application conditions		Remarks
				SCF Send	EUF Send	EUF Send	SCF Send	
Privacy		[RFC 3323]	o	–	–	c8	c8	
Proxy-Authenticate	401	[RFC 3261]	o	–	–	c9	c10	
Proxy-Authenticate	407	[RFC 3261]	m	–	m	c9		
Reason		[RFC 3326]	o	o	o			(Note)
Record-Route	18x 2xx	[RFC 3261]	o	o	o			(Note)
Require		[RFC 3261]	c	c	c			
Retry-After	404 413 480 486	[RFC 3261]	o	o	o			(Note)
Retry-After	500 503	[RFC 3261]	o	o	o			(Note)
Retry-After	600 603	[RFC 3261]	o	o	o			(Note)
Server		[RFC 3261]	o	o	o			(Note)
Supported	2xx	[RFC 3261]	o	o	o			(Note)
Timestamp		[RFC 3261]	o	o	o			(Note)
To		[RFC 3261]	m	m	m			
Unsupported	420	[RFC 3261]	m	m	m			
User-Agent		[RFC 3261]	o	o	o			(Note)
Via		[RFC 3261]	m	m	m			
Warning		[RFC 3261]	o	o	o			(Note)
WWW-Authenticate	401	[RFC 3261]	m	–	–	c11	c11	

Table VI.14 – Supported headers in the PRACK response

Message type: Response
Method: PRACK

Header	Application	Reference	RFC status	Status in this standard		Application conditions		Remarks
				SCF Send	EUF Send	EUF Send	SCF Send	
Message body		[RFC 3261]		o	o	c12	c12	
c1: In the case that SUBSCRIBE/NOTIFY is available over the UNI, the header information is handled as valid information (Table I.2, Items 10 to 15). c2: Update of authentication information by the Authentication-Info header is not performed because the Authorization header is not to be used in the corresponding request. c3: Redirection using 3xx responses is not to be used, according to 10.2.1.8.3 of Table A.1 in clause A.3. c4: The P-Access-Network-Info header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3. c5: The P-Charging-Vector and P-Charging-Function-Addresses headers are not to be used, according to 10.1 of Table A.1 in clause A.3. c6: Not to be used in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3. c7: In the case that SDP offer is performed by PRACK, the header information is handled as valid information (Table I.22, Item 3). c8: The Privacy header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.4 of Table A.1 in clause A.3. c9: The Proxy-Authenticate header is not to be used in the direction from the EUF to the SCF, according to clause 10.2.1.20.27 in the main body. In other words, 401/407 responses themselves are not to be used. c10: The Proxy-Authenticate header is not to be used in 401 responses, according to 10.2.1.20.27 of Table A.1 in clause A.3. c11: The WWW-Authenticate header is applicable only for the REGISTER request authentication, according to 10.2.1.20.44 of Table A.1 in clause A.3. In other words, 401 response itself is not to be used. c12: The message body part of PRACK should be supported, according to clause 10.2.1.7.4.1 in the main body. In the case that the SDP setting of the body part is available over the UNI, the message body information is handled as valid information (Table I.22, Items 2 to 3). NOTE – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.								

VI.9 PUBLISH

This message is used in the case of newly issuing or updating the subscribed information, such as presence information.

VI.9.1 Supported headers in the PUBLISH request

Table VI.15 – Supported headers in the PUBLISH request

Message type: Request
Method: PUBLISH

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Accept	[RFC 3261]	o	o	o			
Accept-Contact	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
Accept-Encoding	[RFC 3261]	o	o	o			
Accept-Language	[RFC 3261]	o	o	o			
Allow	[RFC 3261]	o	o	o			
Allow-Events	[RFC 3265]	o	o	o	c2 (Table I.2, Items 10 to 15)	c2 (Table I.2, Items 10 to 15)	
Authorization	[RFC 3261]	o	–	–	c3	c3	
Call-ID	[RFC 3261]	m	m	m			
Call-Info	[RFC 3261]	o	o	o			(Note 1)
Content-Disposition	[RFC 3261]	o	o	o			
Content-Encoding	[RFC 3261]	o	o	o			
Content-Language	[RFC 3261]	o	o	o			
Content-Length	[RFC 3261]	t	t	t			
Content-Type	[RFC 3261]	*	*	*			
CSeq	[RFC 3261]	m	m	m			
Date	[RFC 3261]	o	o	o			(Note 1)
Event	[RFC 3265]	m	m	m			
Expires	[RFC 3261]	o	o	o			
From	[RFC 3261]	m	m	m			
Max-Forwards	[RFC 3261]	m	m	m			
MIME-Version	[RFC 3261]	o	o	o			
Organization	[RFC 3261]	o	o	o			(Note 1)
P-Access-Network-Info	[RFC 3455]		o	–		c4	(Note 1)

Table VI.15 – Supported headers in the PUBLISH request

Message type: Request
Method: PUBLISH

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
P-Asserted-Identity	[RFC 3325]		–	o / –	c5	c5	
P-Called-Party-ID	[RFC 3455]		–	o / –	c6	c6	
P-Charging-Function-Addresses	[RFC 3455]		–	–	c7	c7	
P-Charging-Vector	[RFC 3455]		-	–	c7	c7	
P-Preferred-Identity	[RFC 3325]		o / –	–	c8	c8	
P-Visited-Network-ID	[RFC 3455]		–	–	c7	c7	
Priority	[RFC 3261]	o	o	o			(Note 1)
Privacy	[RFC 3323]		o / –	o / –	c9	c9	
Proxy-Authorization	[RFC 3261]	o	o	–	c10 (when Table I.11, Item 2 is stated "Perform HTTP Digest authentication".)	c11	
			–	–	c10 (when Table I.11, Item 2 is stated other than "Perform HTTP Digest authentication".)	c11	
Proxy-Require	[RFC 3261]	o	o	–		c12	
Reason	[RFC 3326]	o	– / o	– / o	(Note 2)	(Note 2)	(Note 1)
Referred-By	[RFC 3892]		o	o	c13 (Table I.2, Items 6 to 9)	c13 (Table I.2, Items 6 to 9)	(Note 1)
Reject-Contact	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
Request-Disposition	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
Require	[RFC 3261]	o	o	o			
Route	[RFC 3261]	c	m / c	–	c14 (when Table I.24, Item 1 is stated "Use" for UNI condition.)	c15	
			– / c	–	c14 (when Table I.24, Item 1 is stated "Not use" for UNI condition.)	c15	

Table VI.15 – Supported headers in the PUBLISH request

Message type: Request
Method: PUBLISH

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Security-Client	[RFC 3329]		o	–	c16 (Table I.11, Items 1 and 2, Table I.4, Item 3)	c17	
Security-Verify	[RFC 3329]		o	–	c16 (Table I.11, Items 1 and 2, Table I.4, Item 3)	c17	
SIP-If-Match	[RFC 3261]	o	o	o			
Subject	[RFC 3261]	o	o	o			(Note 1)
Timestamp	[RFC 3261]	o	o	o			(Note 1)
To	[RFC 3261]	m	m	m			
User-Agent	[RFC 3261]	o	o	o			(Note 1)
Via	[RFC 3261]	m	m	m			
Message body	[RFC 3261]		o	o			

c1: In the case that the terminal capabilities notification function, Caller Preferences (pref tag), is available over the UNI, the header information is handled as valid information (Table I.7, Item 6).

c2: In the case that SUBSCRIBE/NOTIFY is available over the UNI, the header information is handled as valid information (Table I.2, Items 10 to 15).

c3: The Authorization header is used only when a REGISTER request from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Table A.1 in clause A.3.

c4: The P-Access-Network-Info header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c5: The P-Asserted-Identity header can be set in requests outside existing dialogues (not to be used inside existing dialogues) only in the direction of messages from the SCF to the EUF except for REGISTER, and transmits the calling-party's information, according to 10.2.2.2.2 of Table A.1 in clause A.3 and Annex B. (It can be set to PUBLISH requests outside INVITE dialogues, but not to be set to PUBLISH requests inside INVITE dialogues.)

c6: The P-Called-Party-ID header can be set in requests outside existing dialogues (not to be used inside existing dialogues) only in the direction of messages from the SCF to the EUF except for REGISTER, and performs the notification of the called-party, according to Annex B. (It can be set to PUBLISH requests outside INVITE dialogues, but not to be set to PUBLISH requests inside INVITE dialogues.)

c7: The P-Charging-Vector, P-Charging-Function-Addresses, and P-Visited-Network-ID headers are not to be used, according to 10.1 of Table A.1 in clause A.3.

c8: The P-Preferred-Identity header can be set in requests outside existing dialogues (not to be used inside existing dialogues) only in the direction of messages from the EUF to the SCF except for REGISTER, and transmits the calling-party's information that the EUF requests of notification, according to 10.2.2.2.3 of Table A.1 in clause A.3 and Annex B. (It can be set to PUBLISH requests outside INVITE dialogues, but not to be set to PUBLISH requests inside INVITE dialogues.)

c9: The Privacy header can be set in requests outside existing dialogues (not to be used inside existing dialogues) except for REGISTER, and transmits the presentation/restriction information of the calling-party's information, according to 10.2.2.2.4 of Table A.1 in clause A.3. (It can be set to PUBLISH requests outside INVITE dialogues, but not to be set to PUBLISH requests inside INVITE dialogues.)

Table VI.15 – Supported headers in the PUBLISH request

Message type: Request
Method: PUBLISH

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
c10: To be used in the case of performing HTTP Digest authentication to requests outside existing dialogues except for REGISTER (Table I.11, Item 2). c11: The Proxy-Authorization header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.28 in the main body. c12: The Proxy-Require header is not to be used in the direction from the SCF to the EUF, according to 10.2.1.20.29 of Table A.1 in clause A.3. c13: The Referred-By header may be used as a result of using REFER (Table I.2, Items 6 to 9). In the case that REFER is available over the UNI, the header information may be handled as valid information. It does not guarantee that the Referred-By header is used as a result of using REFER. c14: In the case that the pre-existing route function is used over the UNI, the setting of the Route header in PUBLISH requests outside INVITE dialogues is necessary (Table I.24, Item 1). c15: The Route header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body. c16: To be handled as valid in the case that AKA authentication is used or TLS connection of call control signals is used (Table I.11, Items 1 and 2, Table I.4, Item 3). c17: The Security-Client and Security-Verify headers are not applicable to a request in the direction from the SCF to the EUF, according to 10.1 of Table A.1 in clause A.3. NOTE 1 – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier. NOTE 2 – The Reason header is specified in [RFC 3326], and it is applicable to all the requests inside existing dialogues, CANCEL, and all responses, according to the specification. Therefore, it can be used in PUBLISH requests inside INVITE dialogues, but cannot be used in PUBLISH requests outside INVITE dialogues.							

VI.9.2 Supported headers in the PUBLISH response

Table VI.16 – Supported headers in the PUBLISH response

Message type: Response
Method: PUBLISH

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Accept	415	[RFC 3261]	m*	m*	m*			
Accept-Encoding	415	[RFC 3261]	m*	m*	m*			
Accept-Language	415	[RFC 3261]	m*	m*	m*			

Table VI.16 – Supported headers in the PUBLISH response

Message type: Response
Method: PUBLISH

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Allow	405	[RFC 3261]	M	m	m			
Allow	others	[RFC 3261]	O	o	o			
Allow-Events	489	[RFC 3261]	M	m	m			
Authentication-Info	2xx	[RFC 3261]	O	–	–	c1	c1	
Call-ID		[RFC 3261]	m	m	m			
Call-Info		[RFC 3261]	o	o	o			(Note 1)
Contact	3xx	[RFC 3261]	o	o	o			(Note 2)
Contact	485	[RFC 3261]	o	o	o			
Content-Disposition		[RFC 3261]	o	o	o			(Note 1)
Content-Encoding		[RFC 3261]	o	o	o			(Note 1)
Content-Language		[RFC 3261]	o	o	o			(Note 1)
Content-Length		[RFC 3261]	t	t	t			
Content-Type		[RFC 3261]	*	*	*			(Note 1)
CSeq		[RFC 3261]	m	m	m			
Date		[RFC 3261]	o	o	o			(Note 1)
Error-Info	300-699	[RFC 3261]	o	o	o			(Note 1)
Expires	2xx	[RFC 3261]	m	m	m			
Expires	others	[RFC 3261]	o	o	o			
From		[RFC 3261]	m	m	m			
Min-Expires	423	[RFC 3261]	m	m	m			
MIME-Version		[RFC 3261]	o	o	o			(Note 1)
Organization		[RFC 3261]	o	o	o			(Note 1)
P-Access-Network-Info		[RFC 3455]		o	–		c2	(Note 1)

Table VI.16 – Supported headers in the PUBLISH response

Message type: Response
Method: PUBLISH

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
P-Charging-Function-Addresses		[RFC 3455]		–	–	c3	c3	
P-Charging-Vector		[RFC 3455]		–	–	c3	c3	
Privacy		[RFC 3323]		–	–	c4	c4	
Proxy-Authenticate	401	[RFC 3261]	o	–	–	c5	c6	
Proxy-Authenticate	407	[RFC 3261]	m	–	m	c5		
Reason		[RFC 3326]	o	o	o			(Note 1)
Require		[RFC 3261]	o	o	o			
Retry-After	404 413 480 486	[RFC 3261]	o	o	o			(Note 1)
Retry-After	500 503	[RFC 3261]	o	o	o			(Note 1)
Retry-After	600 603	[RFC 3261]	o	o	o			(Note 1)
Security-Server	421 494	[RFC 3329]		–	o	c7	c8 (Table I.11, Items 1 and 2, Table I.4, Item 3)	
Server		[RFC 3261]	o	o	o			(Note 1)
SIP-ETag	2xx	[RFC 3261]	m	m	m			
Supported	2xx	[RFC 3261]	o	o	o			
Timestamp		[RFC 3261]	o	o	o			(Note 1)
To		[RFC 3261]	m	m	m			
Unsupported	420	[RFC 3261]	o	m	m	(Note 3)		
User-Agent		[RFC 3261]	o	o	o			(Note 1)

Table VI.16 – Supported headers in the PUBLISH response

Message type: Response
Method: PUBLISH

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Via		[RFC 3261]	m	m	m			
Warning		[RFC 3261]	o	o	o			(Note 1)
WWW-Authenticate	401	[RFC 3261]	m	–	–	c9	c9	
WWW-Authenticate	407	[RFC 3261]	o	–	–	c9	c9	
Message body		[RFC 3261]		o	o			(Note 1)

c1: Update of authentication information by the Authentication-Info header is not performed because the Authorization header is not to be used in the corresponding request.
c2: The P-Access-Network-Info header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.
c3: The P-Charging-Vector and P-Charging-Function-Addresses headers are not to be used, according to 10.1 of Table A.1 in clause A.3.
c4: The Privacy header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.4 of Table A.1 in clause A.3.
c5: The Proxy-Authenticate header is not to be used in the direction from the EUF to the SCF, according to clause 10.2.1.20.27 in the main body. In other words, 401/407 responses themselves are not to be used.
c6: The Proxy-Authenticate header is not to be used in 401 responses, according to 10.2.1.20.27 of Table A.1 in clause A.3.
c7: The Security-Server header is not applicable to the response from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.
c8: To be used in the case that AKA authentication is used or TLS connection of call control signals is used (Table I.11, Items 1 and 2, Table I.4, Item 3).
c9: The WWW-Authenticate header is applicable only to the REGISTER request authentication, according to 10.2.1.20.44 of Table A.1 in clause A.3. In other words, 401/407 responses themselves are not to be used.
NOTE 1 – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.
NOTE 2 – In the case that the redirection function of the 3xx response is available over the UNI, the header information is handled as valid information, according to clause 10.2.1.8.3 in the main body (Table I.12, Items 1 and 2).
NOTE 3 – Although specified as "o" in [RFC 3903], the Unsupported header is set to be "m" based on [RFC 3261].

VI.10 REFER

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

VI.10.1 Supported headers in the REFER request

Table VI.17 – Supported headers in the REFER request

Message type: Request
Method: REFER

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Accept	[RFC 3261]	o	o	o			
Accept-Contact	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
Accept-Encoding	[RFC 3261]	o	o	o			
Accept-Language	[RFC 3261]	o	o	o			
Allow	[RFC 3261]	o	o	o			
Allow-Events	[RFC 3265]		o	o	(Note 2)	(Note 2)	
Authorization	[RFC 3261]	o	–	–	c2	c2	
Call-ID	[RFC 3261]	m	m	m			
Contact	[RFC 3261]	m	m	m			
Content-Disposition	[RFC 3261]	o	o	o			
Content-Encoding	[RFC 3261]	o	o	o			
Content-Language	[RFC 3261]	o	o	o			
Content-Length	[RFC 3261]	o	t	t	(Note 3)		
Content-Type	[RFC 3261]	*	*	*			
CSeq	[RFC 3261]	m	m	m			
Date	[RFC 3261]	o	o	o			(Note 1)
Expires	[RFC 3261]	o	o	o			(Note 1)
From	[RFC 3261]	m	m	m			
Max-Forwards	[RFC 3261]	m	m	m			
MIME-Version	[RFC 3261]	o	o	o			
Organization	[RFC 3261]	o	o	o			(Note 1)
P-Access-Network-Info	[RFC 3455]	o	o	–		c3	(Note 1)

Table VI.17 – Supported headers in the REFER request

Message type: Request
Method: REFER

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
P-Asserted-Identity	[RFC 3325]	o	–	o / –	c4	c4	
P-Called-Party-ID	[RFC 3455]	o	–	o / –	c5	c5	
P-Charging-Function-Addresses	[RFC 3455]	o	–	–	c6	c6	
P-Charging-Vector	[RFC 3455]	o	–	–	c6	c6	
P-Preferred-Identity	[RFC 3325]	o	o / –	–	c7	c7	
P-Visited-Network-ID	[RFC 3455]	o	–	–	c6	c6	
Privacy	[RFC 3323]	o	o / –	o / –	c8	c8	
Proxy-Authorization	[RFC 3261]	o	o	–	c9 (when Table I.11, Item 2 is stated "Perform HTTP Digest authentication".)	c10	
			–	–	c9 (when Table I.11, Item 2 is stated other than "Perform HTTP Digest authentication".)	c10	
Proxy-Require	[RFC 3261]	o	o	–		c11	
Reason	[RFC 3326]	o	– / o	– / o	(Note 4)	(Note 4)	(Note 1)
Record-Route	[RFC 3261]	o	o	o			
Refer-To	[RFC 3515]	m	m	m			
Referred-By	[RFC 3892]		o	o	c12 (Table I.2, Items 6 to 9)	c12 (Table I.2, Items 6 to 9)	
Reject-Contact	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
Request-Disposition	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
Require	[RFC 3261]	c	c	c			
Route	[RFC 3261]	c	m / c	–	c13 (when Table I.24, Item 1 is stated "Use" for UNI condition.)	c14	

Table VI.17 – Supported headers in the REFER request

Message type: Request
Method: REFER

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
			– / c	–	c13 (when Table I.24, Item 1 is stated "Not use" for UNI condition.)	c14	
`Security-Client`	[RFC 3329]		o	–	c15 (Table I.11, Items 1 and 2, Table I.4, Item 3)	c16	
`Security-Verify`	[RFC 3329]		o	–	c15 (Table I.11, Items 1 and 2, Table I.4, Item 3)	c16	
`Supported`	[RFC 3261]	o	o	o			
`Timestamp`	[RFC 3261]	o	o	o			(Note 1)
`To`	[RFC 3261]	m	m	m			
`User-Agent`	[RFC 3261]	o	o	o			(Note 1)
`Via`	[RFC 3261]	m	m	m			
`Message body`	[RFC 3261]		o	o	(Note 5)	(Note 5)	

c1: In the case that the terminal capabilities notification function, Caller Preferences (pref tag), is available over the UNI, the header information is handled as valid information (Table I.7, Item 6).

c2: The `Authorization` header is used only when a `REGISTER` request from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Table A.1 in clause A.3.

c3: The `P-Access-Network-Info` header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c4: The `P-Asserted-Identity` header can be set in requests outside existing dialogues (not to be used inside existing dialogues) only in the direction of messages from the SCF to the EUF except for `REGISTER`, and transmits the calling-party's information, according to 10.2.2.2.2 of Table A.1 in clause A.3 and Annex B. (It can be set to REFER outside existing dialogues, but not to be set to `REFER` inside existing dialogues.)

c5: The `P-Called-Party-ID` header can be set in requests outside existing dialogues (not to be used inside existing dialogues) only in the direction of messages from the SCF to the EUF except for `REGISTER`, and performs the notification of the called-party, according to Annex B. (It can be set to `REFER` outside existing dialogues, but not to be set to `REFER` inside existing dialogues.)

c6: The `P-Charging-Vector`, `P-Charging-Function-Addresses`, and `P-Visited-Network-ID` headers are not to be used, according to 10.1 of Table A.1 in clause A.3.

c7: The `P-Preferred-Identity` header can be set in requests outside existing dialogues (not to be used inside existing dialogues) only in the direction of messages from the EUF to the SCF except for `REGISTER`, and transmits the calling-party's information that the EUF requests of notification, according to 10.2.2.2.3 of Table A.1 in clause A.3 and Annex B. (It can be set to `REFER` outside existing dialogues, but not to be set to `REFER` inside existing dialogues.)

Table VI.17 – Supported headers in the REFER request

Message type: Request

Method: REFER

<table>
<tr><th rowspan="2">Header</th><th rowspan="2">Reference</th><th rowspan="2">RFC status</th><th colspan="2">Status in this standard</th><th colspan="2">Application conditions</th><th rowspan="2">Remarks</th></tr>
<tr><th>EUF Send</th><th>SCF Send</th><th>EUF Send</th><th>SCF Send</th></tr>
<tr><td colspan="8">c8: The Privacy header can be set in requests outside existing dialogues (not to be used inside existing dialogues) except for REGISTER, and transmits the presentation/restriction information of the calling-party's information, according to 10.2.2.2.4 of Table A.1 in clause A.3. (It can be set to REFER requests outside existing dialogues, but not to be set to REFER requests inside existing dialogues.)
c9: To be used in the case of performing HTTP Digest authentication to requests outside existing dialogues except for REGISTER (Table I.11, Item 2).
c10: The Proxy-Authorization header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.28 in the main body.
c11: The Proxy-Require header is not to be used in the direction from the SCF to the EUF, according to 10.2.1.20.29 of Table A.1 in clause A.3.
c12: The Referred-By header may be used as a result of using REFER (Table I.2, Items 6 to 9). In the case that REFER is available over the UNI, the header information may be handled as valid information. It does not guarantee that the Referred-By header is used as a result of using REFER.
c13: In the case that the pre-existing route function is used over the UNI, the setting of the Route header in REFER requests outside existing dialogues is necessary (Table I.24, Item 1).
c14: The Route header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body.
c15: To be handled as valid in the case that AKA authentication is used or TLS connection of call control signals is used (Table I.11, Items 1 and 2, Table I.4, Item 3).
c16: The Security-Client and Security-Verify headers are not applicable to a request in the direction from the SCF to the EUF, according to 10.1 of Table A.1 in clause A.3.
NOTE 1 – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.
NOTE 2 – UA sending REFER is considered to support "refer" event option and there may be a possibility of related information being set. Therefore, although there are no RFC specifications, it is indicated as optional.
NOTE 3 – Although specified as "o" in [RFC 3515], the Content-Length header is set to be "t" based on [RFC 3261].
NOTE 4 – The Reason header is specified in [RFC 3326], and it is applicable to all the requests inside existing dialogues, CANCEL, and all responses, according to the specification. Therefore, it can be used in REFER inside existing dialogues, but cannot be used in REFER outside existing dialogues.
NOTE 5 – It is used when notification information is present. Formatting and other features depend on Content-Type.</td></tr>
</table>

VI.10.2 Supported headers in the REFER response

Table VI.18 – Supported headers in the REFER response

Message type: Response
Method: REFER

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Accept	415	[RFC 3261]	c	c	c			
Accept-Encoding	415	[RFC 3261]	c	c	c			
Accept-Language	415	[RFC 3261]	c	c	c			
Allow	2xx	[RFC 3261]	o	o	o			
Allow	405	[RFC 3261]	m	m	m			
Allow	others	[RFC 3261]	o	o	o			
Allow-Events		[RFC 3265]		o	o	(Note 2)	(Note 2)	
Authentication-Info	2xx	[RFC 3261]	o	–	–	c1	c1	
Call-ID		[RFC 3261]	m	m	m			
Contact	2xx	[RFC 3261]	m	m	m			
Contact	3xx-6xx	[RFC 3261]	o	o	o			(Note 3)
Content-Disposition		[RFC 3261]	o	o	o			
Content-Encoding		[RFC 3261]	o	o	o			
Content-Language		[RFC 3261]	o	o	o			
Content-Length		[RFC 3261]	o	t	t	(Note 4)	(Note 4)	
Content-Type		[RFC 3261]	*	*	*			
CSeq		[RFC 3261]	m	m	m			
Date		[RFC 3261]	o	o	o			(Note 1)
Error-Info	3xx-6xx	[RFC 3261]	o	o	o			(Note 1)
Expires		[RFC 3261]	o	o	o			
From		[RFC 3261]	m	m	m			

Table VI.18 – Supported headers in the REFER response

Message type: Response
Method: REFER

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
MIME-Version		[RFC 3261]	o	o	o			
Organization		[RFC 3261]	o	o	o			(Note 1)
P-Access-Network-Info		[RFC 3455]	o	o	–		c2	(Note 1)
P-Asserted-Identity		[RFC 3325]	o	–	–	c3	c3	
P-Charging-Function-Addresses		[RFC 3455]	o	–	–	c4	c4	
P-Charging-Vector		[RFC 3455]	o	–	–	c4	c4	
P-Preferred-Identity		[RFC 3325]	o	–	–	c5	c5	
Privacy		[RFC 3323]	o	–	–	c6	c6	
Proxy-Authenticate	401	[RFC 3261]	o	–	–	c7	c8	
Proxy-Authenticate	407	[RFC 3261]	m	–	m	c7		
Reason		[RFC 3326]	o	o	o			(Note 1)
Record-Route	18x 2xx	[RFC 3261]	o	o	o			
Require		[RFC 3261]	c	c	c			
Retry-After	404 413 480 486	[RFC 3261]	o	o	o			(Note 1)
Retry-After	500 503	[RFC 3261]	o	o	o			(Note 1)
Retry-After	600 603	[RFC 3261]	o	o	o			(Note 1)
Security-Server	421 494	[RFC 3329]		–	o	c9	c10 (Table I.11, Items 1 and 2, Table I.4, Item 3)	

Table VI.18 – Supported headers in the REFER response

Message type: Response
Method: REFER

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
`Server`		[RFC 3261]	o	o	o			(Note 1)
`Supported`	2xx	[RFC 3261]	o	o	o			
`Timestamp`		[RFC 3261]	o	o	o			(Note 1)
`To`		[RFC 3261]	m	m	m			
`Unsupported`	420	[RFC 3261]	o	m	m	(Note 5)	(Note 5)	
`User-Agent`		[RFC 3261]	o	o	o			(Note 1)
`Via`		[RFC 3261]	m	m	m			
`Warning`		[RFC 3261]	o	o	o			(Note 1)
`WWW-Authenticate`	401	[RFC 3261]	m	–	–	c11	c11	
`WWW-Authenticate`	407	[RFC 3261]	o	–	–	c11	c11	
`Message body`		[RFC 3261]		o	o	(Note 6)	(Note 6)	

c1: Update of authentication information by the `Authentication-Info` header is not performed because the `Authorization` header is not to be used in the corresponding request.

c2: The `P-Access-Network-Info` header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c3: The `P-Asserted-Identity` header is applicable only to requests outside existing dialogues except for `REGISTER`, according to 10.2.2.2.2 of Table A.1 in clause A.3.

c4: The `P-Charging-Vector` and `P-Charging-Function-Addresses` headers are not to be used, according to 10.1 of Table A.1 in clause A.3.

c5: The `P-Preferred-Identity` header is applicable only to requests outside existing dialogues except for `REGISTER`, according to 10.2.2.2.3 of Table A.1 in clause A.3.

c6: The `Privacy` header is applicable only to requests outside existing dialogues except for `REGISTER`, according to 10.2.2.2.4 of Table A.1 in clause A.3.

c7: The `Proxy-Authenticate` header is not to be used in the direction from the EUF to the SCF, according to clause 10.2.1.20.27 in the main body. In other words, `401/407` responses themselves are not to be used.

c8: The `Proxy-Authenticate` header is not to be used in 401 responses, according to 10.2.1.20.27 of Table A.1 in clause A.3.

c9: The `Security-Server` header is not applicable to the response from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c10: To be used in the case that AKA authentication is used or TLS connection of call control signals is used (Table I.11, Items 1 and 2, Table I.4, Item 3).

c11: The `WWW-Authenticate` header is applicable only to the `REGISTER` request authentication, according to 10.2.1.20.44 of Table A.1 in clause A.3. In other words, `401/407` responses themselves are not to be used.

NOTE 1 – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

Table VI.18 – Supported headers in the REFER response

Message type: Response
Method: REFER

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
NOTE 2 – UA receiving REFER is considered to support "refer" event options and there may be a possibility of the information being set. Therefore, although there are no RFC specifications, it is indicated as optional. NOTE 3 – In the case that the redirection function of the 3xx response is available over the UNI, the header information is handled as valid information, according to clause 10.2.1.8.3 in the main body (Table I.12, Items 1 and 2). NOTE 4 – Although specified as "o" in [RFC 3515], the Content-Length header is set to be "t" based on [RFC 3261]. NOTE 5 – Although specified as "o" in [RFC 3515], the Unsupported header is set to be "m" based on [RFC 3261]. NOTE 6 – It is used when notification information is present. Formatting and other features depend on Content-Type.								

VI.11 REGISTER

This message is used for terminal registration, deletion, or registration update.

VI.11.1 Supported headers in the REGISTER request

Table VI.19 – Supported headers in the REGISTER request

Message type: Request
Method: REGISTER

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Accept	[RFC 3261]	o	o				
Accept-Encoding	[RFC 3261]	o	o				
Accept-Language	[RFC 3261]	o	o				
Allow	[RFC 3261]	o	o				
Allow-Events	[RFC 3265]	o	o		c1		

Table VI.19 – Supported headers in the REGISTER request

Message type: Request
Method: REGISTER

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Authorization	[RFC 3261]	o	o		c2 (when Table I.11, Item 1 is stated other than "Not perform" for UNI condition.)		
			–		c2 (when Table I.11, Item 1 is stated "Not perform" for UNI condition.)		
Call-ID	[RFC 3261]	m	m				
Call-Info	[RFC 3261]	o	o				(Note)
Contact	[RFC 3261]	o	o				
Content-Disposition	[RFC 3261]	o	o				(Note)
Content-Encoding	[RFC 3261]	o	o				(Note)
Content-Language	[RFC 3261]	o	o				(Note)
Content-Length	[RFC 3261]	t	t				
Content-Type	[RFC 3261]	*	*				(Note)
CSeq	[RFC 3261]	m	m				
Date	[RFC 3261]	o	o				(Note)
Expires	[RFC 3261]	o	o				
From	[RFC 3261]	m	m				
Max-Forwards	[RFC 3261]	m	m				
MIME-Version	[RFC 3261]	o	o				(Note)
Organization	[RFC 3261]	o	o				(Note)
P-Access-Network-Info	[RFC 3455]	o	o				(Note)
P-Charging-Function-Addresses	[RFC 3455]	o	–		c3		
P-Charging-Vector	[RFC 3455]	o	–		c3		

Table VI.19 – Supported headers in the REGISTER request

Message type: Request
Method: REGISTER

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
P-Visited-Network-ID	[RFC 3455]	o	–		c3		
Path	[RFC 3327]	o	–		c4		
Privacy	[RFC 3323]	o	–		c5		
Proxy-Authorization	[RFC 3261]	o	–		c6		
Proxy-Require	[RFC 3261]	o	o				
Referred-By	[RFC 3892]	o	o		c7 (Table I.2, Items 6 to 9)		(Note)
Request-Disposition	[RFC 3841]	o	o		c8 (Table I.7, Item 6)		
Require	[RFC 3261]	c	c				
Route	[RFC 3261]	c	–		c9		
Security-Client	[RFC 3329]	o	o		c10 (Table I.11, Items 1 and 2, Table I.4, Item 3)		
Security-Verify	[RFC 3329]	o	o		c11 (Table I.11, Items 1 and 2, Table I.4, Item 3)		
Supported	[RFC 3261]	o	o		c12		
Timestamp	[RFC 3261]	o	o				(Note)
To	[RFC 3261]	m	m				
User-Agent	[RFC 3261]	o	o				(Note)
Via	[RFC 3261]	m	m				
Message body	[RFC 3261]	o	o				(Note)

c1: In the case that the terminal capabilities notification function, Caller Preferences (pref tag), is available over the UNI, the header information is handled as valid information (Table I.7, Item 6).
c2: To be used in the case that the HTTP Digest authentication or AKA authentication is performed to REGISTER requests (Table I.11, Item 1).
c3: The P-Charging-Vector, P-Charging-Function-Addresses, and P-Visited-Network-ID headers are not to be used, according to 10.1 of Table A.1 in clause A.3.
c4: The Path header is not applicable to a request in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.
c5: The Privacy header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.4 of Table A.1 in clause A.3.

Table VI.19 – Supported headers in the REGISTER request

Message type: Request
Method: REGISTER

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
c6: The `Proxy-Authorization` header is not applicable to `REGISTER` requests, according to 10.2.1.20.28 of Table A.1 in clause A.3. c7: The `Referred-By` header may be used as a result of using `REFER` (Table I.2, Items 6 to 9). In the case that `REFER` is available over the UNI, the header information may be handled as valid information. It does not guarantee that the `Referred-By` header is used as a result of using `REFER`. c8: In the case that the terminal capabilities notification function, Caller Preferences (pref tag), is available over the UNI, the header information is handled as valid information (Table I.7, Item 6). c9: The pre-existing route is not to be provided to `REGISTER` requests, according to 10.2.1.20.34 of Table A.1 in clause A.3 and clause C.3.2. c10: The `Security-Client` and `Security-Verify` headers are to be handled as valid in the case that AKA authentication is used or TLS connection of call control signals is used, according to 10.1 of Table A.1 in clause A.3 (Table I.11, Items 1 and 2, Table I.4, Item 3). c11: In the case that the `REGISTER` route record function (path) is used, "path" needs to be listed (Table I.24, Item 1). NOTE – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.							

VI.11.2 Supported headers in the REGISTER response

Table VI.20 – Supported headers in the REGISTER response

Message type: Response
Method: REGISTER

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF sends	EUF sends	SCF sends	
`Accept`	2xx	[RFC 3261]	o		o			
`Accept`	415	[RFC 3261]	c		c			
`Accept-Encoding`	2xx	[RFC 3261]	o		o			
`Accept-Encoding`	415	[RFC 3261]	c		c			
`Accept-Language`	2xx	[RFC 3261]	o		o			

Table VI.20 – Supported headers in the REGISTER response

Message type: Response
Method: REGISTER

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF sends	EUF sends	SCF sends	
`Accept-Language`	415	[RFC 3261]	c		c			
`Allow`	2xx	[RFC 3261]	o		o			
`Allow`	405	[RFC 3261]	m		m			
`Allow`	others	[RFC 3261]	o		o			
`Allow-Events`	2xx	[RFC 3265]	o		o		c1 (Table I.2, Items 10 to 15)	
`Authentication-Info`	2xx	[RFC 3261]	o		o			
`Call-ID`		[RFC 3261]	m		m			
`Call-Info`		[RFC 3261]	o		o			
`Contact`	2xx	[RFC 3261]	o		o			
`Contact`	3xx	[RFC 3261]	o		–		c2	
`Contact`	485	[RFC 3261]	o		o			
`Content-Disposition`		[RFC 3261]	o		o			
`Content-Encoding`		[RFC 3261]	o		o			
`Content-Language`		[RFC 3261]	o		o			
`Content-Length`		[RFC 3261]	t		t			
`Content-Type`		[RFC 3261]	*		*			
`CSeq`		[RFC 3261]	m		m			
`Date`		[RFC 3261]	o		o			
`Error-Info`	300-699	[RFC 3261]	o		o			
`Expires`		[RFC 3261]	o		o			
`From`		[RFC 3261]	m		m			
`Min-Expires`	423	[RFC 3261]	m		m			

Table VI.20 – Supported headers in the REGISTER response

Message type: Response
Method: REGISTER

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF sends	EUF sends	SCF sends	
MIME-Version		[RFC 3261]	o		o			
Organization		[RFC 3261]	o		o			
P-Access-Network-Info		[RFC 3455]	o		–		c3	
P-Associated-URI	2xx	[RFC 3455]	o		o		c4 (when Table I.24, Item 3 is stated "May notify" for UNI condition.)	
					–		c4 (when Table I.24, Item 3 is stated "Not notify" for UNI condition.)	
P-Charging-Function-Addresses		[RFC 3455]	o		–		c5	
P-Charging-Vector		[RFC 3455]	o		–		c5	
Path	2xx	[RFC 3327]	o		o			
Privacy		[RFC 3323]	o		–		c6	
Proxy-Authenticate	401	[RFC 3261]	o		–		c7	
Proxy-Authenticate	407	[RFC 3261]	m		–		c7	
Reason		[RFC 3326]	o		o			
Require		[RFC 3261]	c		c			
Retry-After	404 413 480 486	[RFC 3261]	o		o			
Retry-After	500 503	[RFC 3261]	o		o			
Retry-After	600 603	[RFC 3261]	o		o			

Table VI.20 – Supported headers in the REGISTER response

Message type: Response
Method: REGISTER

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF sends	EUF sends	SCF sends	
Security-Server	421 494	[RFC 3329]	o		o		c8 (Table I.11, Items 1 and 2, Table I.4, Item 3)	
Service-Route	2xx	[RFC 3608]	o		o		c9 (when Table I.24, Item 1 is stated "Provide" for UNI condition.)	
					–		c9 (when Table I.24, Item 1 is stated "Not provide" for UNI condition.)	
Server		[RFC 3261]	o		o			
Supported	2xx	[RFC 3261]	o		o			
Timestamp		[RFC 3261]	o		o			
To		[RFC 3261]	m		m			
Unsupported	420	[RFC 3261]	m		m			
User-Agent		[RFC 3261]	o		o			
Via		[RFC 3261]	m		m			
Warning		[RFC 3261]	o		o			
WWW-Authenticate	401	[RFC 3261]	m		m			
WWW-Authenticate	407	[RFC 3261]	o		o			
Message body		[RFC 3261]	o		o			

c1: In the case that SUBSCRIBE/NOTIFY is available over the UNI, the header information is handled as valid information (Table I.2, Items 10 to 15).
c2: Redirection using 3xx responses is not to be used, according to 10.2.1.8.3 of Table A.1 in clause A.3.
c3: The P-Access-Network-Info header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.
c4: To be used in the case that the notification of network-asserted user identity using the P-Associated-URI header is performed (Table I.24, Item 3).
c5: The P-Charging-Vector and P-Charging-Function-Addresses headers are not to be used, according to 10.1 of Table A.1 in clause A.3.
c6: The Privacy header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.4 of Table A.1 in clause A.3.

Table VI.20 – Supported headers in the REGISTER response

Message type: Response
Method: REGISTER

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF sends	EUF sends	SCF sends	
c7: The `Proxy-Authenticate` header is not to be used in a `REGISTER` request, according to 10.2.1.20.27 of Table A.1 in clause A.3.								
c8: The `Security-Server` header applicable in the case that AKA authentication is used or TLS connection of call control signals is used, according to 10.1 of Table A.1 in clause A.3 (Table I.11, Items 1 and 2, Table I.4, Item 3).								
c9: In the case that the pre-existing route function is used over the UNI, the setting is necessary (Table I.24, Item 1).								

VI.12 SUBSCRIBE

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

VI.12.1 Supported headers in the SUBSCRIBE request

Table VI.21 – Supported headers in the SUBSCRIBE request

Message type: Request
Method: SUBSCRIBE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
`Accept`	[RFC 3261]	O	o	o			
`Accept-Contact`	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
`Accept-Encoding`	[RFC 3261]	o	o	o			
`Accept-Language`	[RFC 3261]	o	o	o			
`Allow`	[RFC 3261]	o	o	o			
`Allow-Events`	[RFC 3265	o	o	o			
`Authorization`	[RFC 3261]	o	–	–	c2	c2	

Table VI.21 – Supported headers in the SUBSCRIBE request

Message type: Request
Method: SUBSCRIBE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Call-ID	[RFC 3261]	m	m	m			
Contact	[RFC 3261]	m	m	m			
Content-Disposition	[RFC 3261]	o	o	o			
Content-Encoding	[RFC 3261]	o	o	o			
Content-Language	[RFC 3261]	o	o	o			
Content-Length	[RFC 3261]	t	t	t			
Content-Type	[RFC 3261]	*	*	*			
CSeq	[RFC 3261]	m	m	m			
Date	[RFC 3261]	o	o	o			(Note 1)
Event	[RFC 3265]	m	m	m			
Expires	[RFC 3261]	o	o	o			
From	[RFC 3261]	m	m	m			
Max-Forwards	[RFC 3261]	m	m	m			
MIME-Version	[RFC 3261]	o	o	o			
Organization	[RFC 3261]	o	o	o			(Note 1)
P-Access-Network-Info	[RFC 3455]	o	o	–		c3	(Note 1)
P-Asserted-Identity	[RFC 3325]	o	–	o / –	c4	c4	
P-Called-Party-ID	[RFC 3455]	o	–	o / –	c5	c5	
P-Charging-Function-Addresses	[RFC 3455]	o	–	–	c6	c6	
P-Charging-Vector	[RFC 3455]	o	–	–	c6	c6	
P-Preferred-Identity	[RFC 3325]	o	o / -	–	c7	c7	
P-Visited-Network-ID	[RFC 3455]	o	–	–	c6	c6	
Priority	[RFC 3261]	o	o	o			(Note 1)

Table VI.21 – Supported headers in the SUBSCRIBE request

Message type: Request
Method: SUBSCRIBE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Privacy	[RFC 3323]	o	o / -	o / -	c8	c8	
Proxy-Authorization	[RFC 3261]	o	o	–	c9 (when Table I.11, Item 2 is stated "Perform HTTP Digest authentication".)	c10	
			–	–	c9 (when Table I.11, Item 2 is stated other than "Perform HTTP Digest authentication".)	c10	
Proxy-Require	[RFC 3261]	o	o	–		c11	
Reason	[RFC 3326]	o	– / o	– / o	(Note 2)	(Note 2)	(Note 1)
Record-Route	[RFC 3261]	o	o	o			
Referred-By	[RFC 3892]	o	o	o	c12 (Table I.2, Items 6 to 9)	c12 (Table I.2, Items 6 to 9)	
Reject-Contact	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
Request-Disposition	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
Require	[RFC 3261]	o	o	o			
Route	[RFC 3261]	c	m / c	–	c13 (when Table I.24, Item 1 is stated "Use" for UNI condition.)	c14	
			– / c	–	c13 (when Table I.24, Item 1 is stated "Not use" for UNI condition.)	c14	
Security-Client	[RFC 3329]	o	o	–	c15 (Table I.11, Items 1 and 2, Table I.4, Item 3)	c16	
Security-Verify	[RFC 3329]	o	o	–	c15 (Table I.11, Items 1 and 2, Table I.4, Item 3)	c16	
Supported	[RFC 3261]	o	o	o			
Timestamp	[RFC 3261]	o	o	o			(Note 1)

Table VI.21 – Supported headers in the SUBSCRIBE request

Message type: Request
Method: SUBSCRIBE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
To	[RFC 3261]	m	m	m			
User-Agent	[RFC 3261]	o	o	o			(Note 1)
Via	[RFC 3261]	m	m	m			
Message body	[RFC 3261]		o	o	(Note 3)	(Note 3)	

c1: In the case that the terminal capabilities notification function, Caller Preferences (pref tag), is available over the UNI, the header information is handled as valid information (Table I.7, Item 6).

c2: The Authorization header is used only when a REGISTER request from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Table A.1 in clause A.3.

c3: The P-Access-Network-Info header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c4: The P-Asserted-Identity header can be set in requests outside existing dialogues (not to be used inside existing dialogues) only in the direction of messages from the SCF to the EUF except for REGISTER, and transmits the calling-party's information, according to 10.2.2.2.2 of Table A.1 in clause A.3 and Annex B. (It can be set to initial-SUBSCRIBE, but not to be set to re-SUBSCRIBE.)

c5: The P-Called-Party-ID header can be set in requests outside existing dialogues (not to be used inside existing dialogues) only in the direction of messages from the SCF to the EUF except for REGISTER, and performs the notification of the called-party, according to Annex B. (It can be set to initial-SUBSCRIBE outside INVITE dialogues, but not to be set to SUBSCRIBE requests inside INVITE dialogues or re-SUBSCRIBE inside existing subscriptions.)

c6: The P-Charging-Vector, P-Charging-Function-Addresses, and P-Visited-Network-ID headers are not to be used, according to 10.1 of Table A.1 in clause A.3.

c7: The P-Preferred-Identity header can be set in requests outside existing dialogues (not to be used inside existing dialogues) only in the direction of messages from the EUF to the SCF except for REGISTER, and transmits the calling-party's information that the EUF requests of notification, according to 10.2.2.2.3 of Table A.1 in clause A.3 and Annex B. (It can be set to initial SUBSCRIBE, but not to be set to re-SUBSCRIBE.)

c8: The Privacy header can be set in requests outside existing dialogues (not to be used inside existing dialogues) except for REGISTER, and transmits the presentation/restriction information of the calling-party's information, according to 10.2.2.2.4 of Table A.1 in clause A.3. (It can be set to initial SUBSCRIBE outside INVITE dialogues, but not to be set to SUBSCRIBE requests inside INVITE dialogues or re-SUBSCRIBE inside existing subscriptions.)

c9: To be used in the case of performing HTTP Digest authentication to requests outside existing dialogues except for REGISTER (Table I.11, Item 2).

c10: The Proxy-Authorization header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.28 in the main body.

c11: The Proxy-Require header is not to be used in the direction from the SCF to the EUF, according to 10.2.1.20.29 of Table A.1 in clause A.3.

c12: The Referred-By header may be used as a result of using REFER (Table I.2, Items 6 to 9). In the case that REFER is available over the UNI, the header information may be handled as valid information. It does not guarantee that the Referred-By header is used as a result of using REFER.

c13: In the case that the pre-existing route function is used over the UNI, the setting of the Route header in an initial SUBSCRIBE outside INVITE dialogues is necessary (Table I.24, Item 1).

c14: The Route header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body.

c15: To be handled as valid in the case that AKA authentication is used or TLS connection of call control signals is used (Table I.11, Items 1 and 2, Table I.4, Item 3).

Table VI.21 – Supported headers in the SUBSCRIBE request

Message type: Request
Method: SUBSCRIBE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
c16: The `Security-Client` and `Security-Verify` headers are not applicable to a request in the direction from the SCF to the EUF, according to 10.1 of Table A.1 in clause A.3.							
NOTE 1 – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.							
NOTE 2 – The `Reason` header is specified in [RFC 3326], and it is applicable to all the requests inside existing dialogues, `CANCEL`, and all responses, according to the specification. Therefore, it can be used in a SUBSCRIBE requests inside INVITE dialogues or re-`SUBSCRIBE` inside existing subscriptions, but cannot be used in initial `SUBSCRIBE` outside `INVITE` dialogues.							
NOTE 3 – It is used when notification information is present. Formatting and other features depend on Content-Type.							

VI.12.2 Supported headers in the SUBSCRIBE response

Table VI.22 – Supported headers in the SUBSCRIBE response

Message type: Response
Method: SUBSCRIBE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF sends	SCF sends	
`Accept`	415	[RFC 3261]	o	o	o			
`Accept-Encoding`	415	[RFC 3261]	o	o	o			
`Accept-Language`	415	[RFC 3261]	o	o	o			
`Allow`	2xx	[RFC 3261]	o	o	o			
`Allow`	405	[RFC 3261]	m	m	m			
`Allow`	others	[RFC 3261]	o	o	o			
`Allow-Events`	489	[RFC 3265]	m	m	m			
`Authentication-Info`	2xx	[RFC 3261]	o	–	–	c1	c1	
`Call-ID`		[RFC 3261]	m	m	m			

Table VI.22 – Supported headers in the SUBSCRIBE response

Message type: Response
Method: SUBSCRIBE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF sends	SCF sends	
Call-Info		[RFC 3261]		–	–	(Note 2)	(Note 2)	
Contact	1xx	[RFC 3261]	o	o	o			
Contact	2xx	[RFC 3261]	m	m	m			
Contact	3xx	[RFC 3261]	m	m	m			(Note 3)
Contact	485	[RFC 3261]	o	o	o			
Content-Disposition		[RFC 3261]	o	o	o			
Content-Encoding		[RFC 3261]	o	o	o			
Content-Language		[RFC 3261]	o	o	o			
Content-Length		[RFC 3261]	t	t	t			
Content-Type		[RFC 3261]	*	*	*			
CSeq		[RFC 3261]	m	m	m			
Date		[RFC 3261]	o	o	o			(Note 1)
Error-Info	300-699	[RFC 3261]	o	o	o			(Note 1)
Expires	2xx	[RFC 3261]	m	m	m			
From		[RFC 3261]	m	m	m			
Min-Expires	423	[RFC 3261]	m	m	m			
MIME-Version		[RFC 3261]	o	o	o			
Organization		[RFC 3261]	o	o	o			(Note 1)
P-Access-Network-Info		[RFC 3455]	o	o	–		c3	(Note 1)
P-Asserted-Identity		[RFC 3325]	o	–	–	c4	c4	
P-Charging-Function-Addresses		[RFC 3455]	o	–	–	c5	c5	
P-Charging-Vector		[RFC 3455]	o	–	–	c5	c5	
P-Preferred-Identity		[RFC 3325]	o	–	–	c6	c6	

Table VI.22 – Supported headers in the SUBSCRIBE response

Message type: Response
Method: SUBSCRIBE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF sends	SCF sends	
Privacy		[RFC 3323]	o	–	–	c2	c2	
Proxy-Authenticate	407	[RFC 3261]	m	–	m	c7		
Reason		[RFC 3326]	o	o	o			(Note 1)
Record-Route	2xx 401 484	[RFC 3261]	o	o	o			
Require		[RFC 3261]	o	o	o			
Retry-After	404 413 480 486	[RFC 3261]	o	o	o			(Note 1)
Retry-After	500 503	[RFC 3261]	o	o	o			(Note 1)
Retry-After	600 603	[RFC 3261]	o	o	o			(Note 1)
RSeq	1xx	[RFC 3262]	o	–	–	(Note 4)	(Note 4)	
Security-Server	421 494	[RFC 3329]	o	–	–	c8	c9 (Table I.11, Items 1 and 2, Table I.4, Item 3)	
Server		[RFC 3261]	o	o	o			(Note 1)
Supported	2xx	[RFC 3261]	o	o	o			
Timestamp		[RFC 3261]	o	o	o			(Note 1)
To		[RFC 3261]	m	m	m			
Unsupported	420	[RFC 3261]	o	m	m	(Note 5)	(Note 5)	
User-Agent		[RFC 3261]	o	o	o			(Note 1)
Via		[RFC 3261]	m	m	m			

Table VI.22 – Supported headers in the SUBSCRIBE response

Message type: Response
Method: SUBSCRIBE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF sends	SCF sends	
Warning		[RFC 3261]	o	o	o			(Note 1)
WWW-Authenticate	401	[RFC 3261]	m	–	–	c10	c10	
Message body		[RFC 3261]		o	o	(Note 6)	(Note 6)	

c1: Update of authentication information by the Authentication-Info header is not performed because the Authorization header is not to be used in the corresponding request.

c2: The Privacy header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.4 of Table A.1 in clause A.3.

c3: The P-Access-Network-Info header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c4: The P-Asserted-Identity header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.2 of Table A.1 in clause A.3.

c5: The P-Charging-Vector and P-Charging-Function-Addresses headers are not to be used, according to 10.1 of Table A.1 in clause A.3.

c6: The P-Preferred-Identity header is applicable only to requests outside existing dialogues except for REGISTER, according to 10.2.2.2.3 of Table A.1 in clause A.3.

c7: The Proxy-Authenticate header is not to be used in the direction from the EUF to the SCF, according to clause 10.2.1.20.27 in the main body. In other words, 407 response itself is not to be used.

c8: The Security-Server header is not applicable to the response from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c9: To be used in the case that AKA authentication is used or TLS connection of call control signals is used (Table I.11, Items 1 and 2, Table I.4, Item 3).

c10: The WWW-Authenticate header is applicable only for the REGISTER request authentication, according to 10.2.1.20.44 of Table A.1 in clause A.3. In other words, 401 response itself is not to be used.

NOTE 1 – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

NOTE 2 – Call-Info shows additional information about the sender of the messages. There is no description of the application of the header into SUBSCRIBE in RFCs and other documents. Therefore, it is difficult to define its reaction in the case of using the header in SUBSCRIBE. Furthermore, security risks of Call-Info are noted in [RFC 3261]. An ill-prepared use of the header should be avoided.

NOTE 3 – In the case that the redirection function of the 3xx response is available over the UNI, the header information is handled as valid information, according to clause 10.2.1.8.3 in the main body (Table I.12, Items 1 and 2).

NOTE 4 – The 100rel option (PRACK) is not to be used in SUBSCRIBE.

NOTE 5 – Although specified as "o" in [RFC 3265], the Unsupported header is set to be "m" based on [RFC 3261].

NOTE 6 – It is used when notification information is present. Formatting and other features depend on Content-Type.

VI.13 UPDATE

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

VI.13.1 Supported headers in the UPDATE request

Table VI.23 – Supported headers in the UPDATE request

Message type: Request
Method: UPDATE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Accept	[RFC 3261]	o	o	o			
Accept-Contact	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
Accept-Encoding	[RFC 3261]	o	o	o			
Accept-Language	[RFC 3261]	o	o	o			
Allow	[RFC 3261]	o	o	o			
Authorization	[RFC 3261]	o	–	–	c2	c2	
Call-ID	[RFC 3261]	m	m	m			
Call-Info	[RFC 3261]	o	o	o			(Note)
Contact	[RFC 3261]	m	m	m			
Content-Disposition	[RFC 3261]	o	o	o			
Content-Encoding	[RFC 3261]	o	o	o			
Content-Language	[RFC 3261]	o	o	o			
Content-Length	[RFC 3261]	t	t	t			
Content-Type	[RFC 3261]	*	*	*			
CSeq	[RFC 3261]	m	m	m			
Date	[RFC 3261]	o	o	o			(Note)
From	[RFC 3261]	m	m	m			
Max-Forwards	[RFC 3261]	m	m	m			
MIME-Version	[RFC 3261]	o	o	o			
Min-SE	[RFC 4028]	o	o	o	c3	c3	

Table VI.23 – Supported headers in the UPDATE request

Message type: Request
Method: UPDATE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Organization	[RFC 3261]	o	o	o			(Note)
P-Access-Network-Info	[RFC 3455]	o	o	–		c4	(Note)
P-Charging-Function-Addresses	[RFC 3455]	o	–	–	c5	c5	
P-Charging-Vector	[RFC 3455]	o	–	–	c5	c5	
P-Media-Authorization	[RFC 3313]	o	–	o	c6	c7	
Privacy	[RFC 3323]	o	–	–	c8	c8	
Proxy-Authorization	[RFC 3261]	o	o	–	c9 (when Table I.11, Item 2 is stated "Perform HTTP Digest authentication".)	c10	
			–	–	c9 (when Table I.11, Item 2 is stated other than "Perform HTTP Digest authentication".)	c10	
Proxy-Require	[RFC 3261]	o	o	–		c11	
Reason	[RFC 3326]	o	o	o			(Note)
Record-Route	[RFC 3261]	o	o	o			(Note)
Reject-Contact	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
Request-Disposition	[RFC 3841]	o	o	o	c1 (Table I.7, Item 6)	c1 (Table I.7, Item 6)	
Require	[RFC 3261]	c	c	c	c12	c12	
Route	[RFC 3261]	c	c	–		c13	
Security-Client	[RFC 3329]	o	o	–	c14 (Table I.11, Items 1 and 2, Table I.4, Item 3)	c15	
Security-Verify	[RFC 3329]	o	o	–	c14 (Table I.11, Items 1 and 2, Table I.4, Item 3)	c15	

Table VI.23 – Supported headers in the UPDATE request

Message type: Request
Method: UPDATE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Session-Expires	[RFC 4028]	o	m	m	c3 (when Table I.7, Item 1 states that UNI condition are "Used in all sessions".)	c3 (when Table I.7, Item 1 states that UNI conditions are "Used in all sessions".)	
			o	o	c3 (when Table I.7, Item 1 states that UNI condition are "Used in each session as necessary".)	c3 (when Table I.7, Item 1 states that UNI conditions are "Used in each session as necessary".)	
Supported	[RFC 3261]	o	o	o	c12	c12	
Timestamp	[RFC 3261]	o	o	o			(Note)
To	[RFC 3261]	m	m	m			
User-Agent	[RFC 3261]	o	o	o			(Note)
Via	[RFC 3261]	m	m	m			
Message body	[RFC 3261]	o	o	o			

c1: In the case that the terminal capabilities notification function, Caller Preferences (pref tag), is available over the UNI, the header information is handled as valid information (Table I.7, Item 6).

c2: The `Authorization` header is used only when a `REGISTER` request from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Table A.1 in clause A.3.

c3: The header must be used as specified in clause 10.2.2.2.1 and 10.2.2.2.7 in the main body. In the case that Session-Timer is used, at least the setting of value to the `Session-Expires` header (delta-seconds) is necessary.

c4: The `P-Access-Network-Info` header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c5: The `P-Charging-Vector` and `P-Charging-Function-Addresses` headers are not to be used, according to 10.1 of Table A.1 in clause A.3.

c6: Not to be used in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c7: In the case that SDP offer is performed by `UPDATE`, the header information is handled as valid information (Table I.23, Item 6).

c8: The `Privacy` header is applicable only to requests outside existing dialogues except for `REGISTER`, according to 10.2.2.2.4 of Table A.1 in clause A.3.

c9: To be used in the case of performing HTTP Digest authentication to requests outside existing dialogues except for REGISTER (Table I.11, Item 2).

c10: The `Proxy-Authorization` header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.28 in the main body.

c11: The `Proxy-Require` header is not to be used in the direction from the SCF to the EUF, according to 10.2.1.20.29 of Table A.1 in clause A.3.

c12: "timer" needs to be set to the `Require` header and the `Supported` header in terms of the context, according to clause 10.2.1.20.32 and clause 10.2.1.20.37 in the main body. ("timer" should be contextually set to the `Supported` header in an `UPDATE` request.)

Table VI.23 – Supported headers in the UPDATE request

Message type: Request
Method: UPDATE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
c13: The `Route` header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body.							
c14: To be handled as valid in the case that AKA authentication is used or TLS connection of call control signals is used (Table I.11, Items 1 and 2, Table I.4, Item 3).							
c15: The `Security-Client` and `Security-Verify` headers are not applicable to a request in the direction from the SCF to the EUF, according to 10.1 of Table A.1 in clause A.3.							
NOTE – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.							

VI.13.2 Supported headers in the UPDATE response

Table VI.24 – Supported headers in the UPDATE response

Message type: Response
Method: UPDATE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
`Accept`	2xx	[RFC 3261]	o	o	o			
`Accept`	415	[RFC 3261]	c	c	c			
`Accept-Encoding`	2xx	[RFC 3261]	o	o	o			
`Accept-Encoding`	415	[RFC 3261]	c	c	c			
`Accept-Language`	2xx	[RFC 3261]	o	o	o			
`Accept-Language`	415	[RFC 3261]	c	c	c			
`Allow`	2xx	[RFC 3261]	o	o	o			
`Allow`	405	[RFC 3261]	m	m	m			
`Allow`	others	[RFC 3261]	o	o	o			
`Authentication-Info`	2xx	[RFC 3261]	o	–	–	c1	c1	

Table VI.24 – Supported headers in the UPDATE response

Message type: Response
Method: UPDATE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Call-ID		[RFC 3261]	m	m	m			
Call-Info		[RFC 3261]	o	o	o			(Note)
Contact	1xx	[RFC 3261]	o	o	o			
Contact	2xx	[RFC 3261]	m	m	m			
Contact	3xx	[RFC 3261]	o	–	–	c2	c2	
Contact	485	[RFC 3261]	o	o	o			
Content-Disposition		[RFC 3261]	o	o	o			
Content-Encoding		[RFC 3261]	o	o	o			
Content-Language		[RFC 3261]	o	o	o			
Content-Length		[RFC 3261]	t	t	t			
Content-Type		[RFC 3261]	*	*	*			
CSeq		[RFC 3261]	m	m	m			
Date		[RFC 3261]	o	o	o			(Note)
Error-Info	300-699	[RFC 3261]	o	o	o			(Note)
From		[RFC 3261]	m	m	m			
MIME-Version		[RFC 3261]	o	o	o			
Min-SE	422	[RFC 4028]	m	m	m	c3 (Table I.7, Item 1)	c3 (Table I.7, Item 1)	
Organization		[RFC 3261]	o	o	o			(Note)
P-Access-Network-Info		[RFC 3455]	o	o	–		c4	(Note)
P-Charging-Function-Addresses		[RFC 3455]	o	–	–	c5	c5	
P-Charging-Vector		[RFC 3455]	o	–	–	c5	c5	
P-Media-Authorization	2xx	[RFC 3313]	o	–	o	c6	c7	
Privacy		[RFC 3323]	o	–	–	c8	c8	

Table VI.24 – Supported headers in the UPDATE response

Message type: Response
Method: UPDATE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Proxy-Authenticate	401	[RFC 3261]	o	–	–	c9	c10	
Proxy-Authenticate	407	[RFC 3261]	m	–	m	c9		
Reason		[RFC 3326]	o	o	o			(Note)
Record-Route	18x 2xx	[RFC 3261]	o	o	o			(Note)
Require		[RFC 3261]	c	c	c	c3	c3	
Retry-After	404 413 480 486	[RFC 3261]	o	o	o			(Note)
Retry-After	500 503	[RFC 3261]	o	o	o			(Note)
Retry-After	600 603	[RFC 3261]	o	o	o			(Note)
Security-Server	421 494	[RFC 3329]	o	–	o	c11	c12 (Table I.11, Items 1 and 2, Table I.4, Item 3)	
Server		[RFC 3261]	o	o	o			(Note)
Session-Expires	2xx	[RFC 4028]	o	m	m	c3 (when Table I.7, Item 1 states that UNI condition are "Used in all sessions".)	c3 (when Table I.7, Item 1 states that UNI condition are "Used in all sessions".)	
				o	o	c3 (when Table I.7, Item 1 states that UNI condition are "Used in each session as necessary".)	c3 (when Table I.7, Item 1 states that UNI condition are "Used in each session as necessary".)	
Supported	2xx	[RFC 3261]	o	o	o			
Timestamp		[RFC 3261]	o	o	o			(Note)
To		[RFC 3261]	m	m	m			

Table VI.24 – Supported headers in the UPDATE response

Message type: Response
Method: UPDATE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
`Unsupported`	420	[RFC 3261]	m	m	m			
`User-Agent`		[RFC 3261]	o	o	o			(Note)
`Via`		[RFC 3261]	m	m	m			
`Warning`		[RFC 3261]	o	o	o			(Note)
`WWW-Authenticate`	401	[RFC 3261]	m	–	–	c13	c13	
`WWW-Authenticate`	407	[RFC 3261]	o	–	–	c13	c13	
`Message body`		[RFC 3261]		o	o			

c1: Update of authentication information by the `Authentication-Info` header is not performed because the `Authorization` header is not to be used in the corresponding request.

c2: Redirection using `3xx` responses is not to be used, according to 10.2.1.8.3 of Table A.1 in clause A.3.

c3: The header must be used as specified in clause 10.2.1.20.32, 10.2.2.1 and 10.2.2.2.7 in the main body. In the case that Session-Timer is used, at least the setting of value to the `Session-Expires` header (delta-seconds) is necessary. In the case that the refresher is "uac", the setting of "timer" to the `Require` header is necessary (Table I.7, Item 1).

c4: The `P-Access-Network-Info` header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c5: The `P-Charging-Vector` and `P-Charging-Function-Addresses` headers are not to be used, according to 10.1 of Table A.1 in clause A.3.

c6: Not to be used in the direction from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c7: In the case that SDP offer is performed by `UPDATE`, the header information is handled as valid information (Table I.23, Item 6).

c8: The `Privacy` header is applicable only to requests outside existing dialogues except for `REGISTER`, according to 10.2.2.2.4 of Table A.1 in clause A.3.

c9: The `Proxy-Authenticate` header is not to be used in the direction from the EUF to the SCF, according to clause 10.2.1.20.27 in the main body. In other words, `401/407` responses themselves are not to be used.

c10: The `Proxy-Authenticate` header is not to be used in `401` responses, according to 10.2.1.20.27 of Table A.1 in clause A.3.

c11: The `Security-Server` header is not applicable to the response from the EUF to the SCF, according to 10.1 of Table A.1 in clause A.3.

c12: To be used in the case that AKA authentication is used or TLS connection of call control signals is used (Table I.11, Items 1 and 2, Table I.4, Item 3)

c13: The `WWW-Authenticate` header is applicable only to the `REGISTER` request authentication, according to 10.2.1.20.44 of Table A.1 in clause A.3. In other words, `401/407` responses themselves are not to be used.

NOTE – Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

Appendix VII

Message examples

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

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

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

Table VII.1 – List of sequence examples

No.	Sequence Name	Corresponding clauses and figures
1	Terminal registration (access-line based authentication)	Clause VII.1.1
2	Terminal registration (HTTP Digest authentication)	Clause VII.1.2
3	Deletion of terminal registration (access-line based authentication)	Clause VII.1.3
4	Call origination to disconnection (IPv4, Use of `timer` and `100rel`, ITU-T G.711 μ-law)	Clause VII.1.4
5	Call origination to disconnection (IPv4, Use of `timer` and `100rel`, ITU-T G.711 μ-law, HTTP Digest authentication)	Clause VII.1.5
6	Call termination to disconnection (IPv4, Use of `timer` and `100rel`, ITU-T G.711 μ-law)	Clause VII.1.6
7	Call cancellation	Clause VII.1.7
8	Busy on the terminating side	Clause VII.1.8
9	Hearing the guidance	Clause VII.1.9
10	Connection after hearing the guidance (using `UPDATE`)	Clause VII.1.10
11	Sending `MESSAGE` (IPv6)	Clause VII.1.11
12	Receiving `MESSAGE` (IPv6)	Clause VII.1.12
13	Subscription to registration event	Clause VII.1.13
14	Notification of registration event (on deletion of terminal registration)	Clause VII.1.14

VII.1 Sequence examples

VII.1.1 Terminal registration (access line-based authentication)

This clause shows an example message flow in the case that a network requires a `REGISTER` from a terminal, and access-line based terminal authentication is performed. An IPv4 address and an IPv6 address are used as `Contact address`, and `REGISTER` is performed by IPv4 UDP. The network notifies the pre-existing route by a `Service-Route` header and the available network-asserted user identity by a `P-Associated-URI` header.

In the example of terminal registration such as the one shown below, a SIP-URI composed of a telephone number is used as the URI to be specified in the `From` header and the `To` header at the time of terminal registration, like the example of the caller number shown in clause VII.1.4, etc. Note that there may be a case of using a SIP-URI which is not composed of the telephone number, according to the NGN carrier policy.

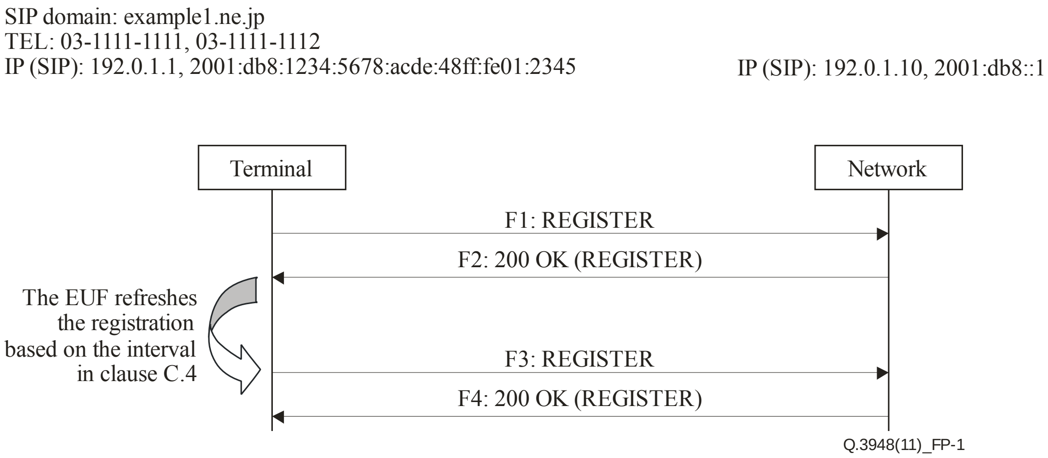

Figure VII.1 – Terminal registration (access-line based authentication)

F1: REGISTER

```
REGISTER sip:example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111111
Max-Forwards: 70
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111111
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 REGISTER
Contact: <sip:qwertyui@192.0.1.1>,<sip:asdfghjk@[2001:db8:1234:5678:acde:48ff:fe01:2345]>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE
Expires: 3600
Supported: path
Content-Length: 0
```

F2: 200 OK (REGISTER)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111111
Path: <sip:192.0.1.10;lr>
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101010
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111111
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 REGISTER
Contact:  <sip:qwertyui@192.0.1.1>;expires=3600,<sip:asdfghjk@[2001:db8:1234:5678:48ff:fe01:2345
]>;expires=3600
Supported: path
Service-Route: <sip:s-cscf.example1.ne.jp;lr>
P-Associated-URI: <sip:0311111111@example1.ne.jp>,<sip:0311111112@example1.ne.jp>
Content-Length: 0
```

F3: REGISTER

```
REGISTER sip:example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Max-Forwards: 70
To: <sip:0311111111@example1.ne.jp>
```

```
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Contact: <sip:qwertyui@192.0.1.1>,<sip:asdfghjk@[2001:db8:1234:5678:acde:48ff:fe01:2345]>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE
Expires: 3600
Supported: path
Content-Length: 0
```

F4: 200 OK (REGISTER)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Path: <sip:192.0.1.10;lr>
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101011
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Contact:  <sip:qwertyui@192.0.1.1>;expires=3600,<sip:asdfghjk@[2001:db8:1234:5678:48ff:fe01:2345
]>;expires=3600
Supported: path
Service-Route: <sip:s-cscf.example1.ne.jp;lr>
P-Associated-URI: <sip:0311111111@example1.ne.jp>,<sip:0311111112@example1.ne.jp>
Content-Length: 0
```

VII.1.2 Terminal registration (HTTP Digest authentication)

This clause shows an example message flow when the network performs terminal authentication using HTTP Digest authentication, which is different from the sequence in clause VII.1.1.

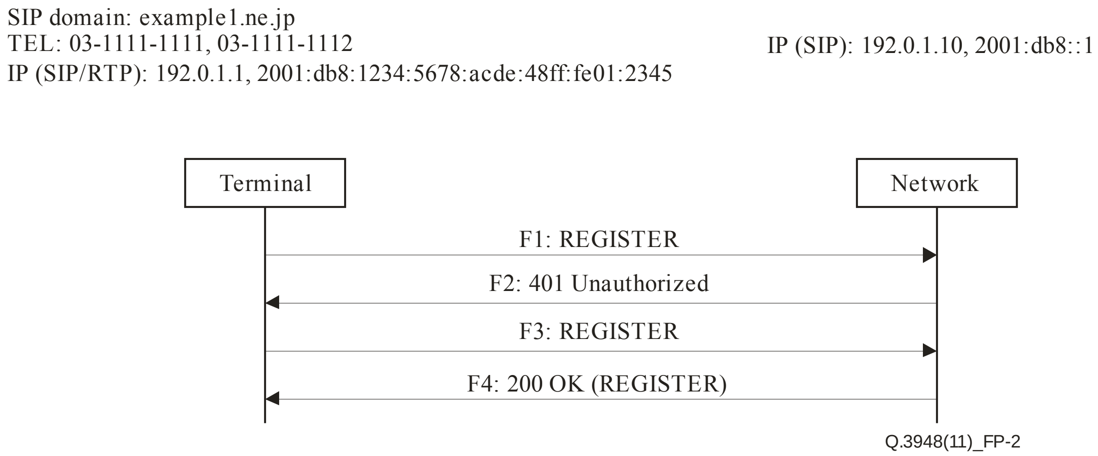

Figure VII.2 – Terminal registration (HTTP Digest authentication)

F1: REGISTER

```
REGISTER sip:example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111111
Max-Forwards: 70
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111111
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 REGISTER
Contact: <sip:qwertyui@192.0.1.1>,<sip:asdfghjk@[2001:db8:1234:5678:acde:48ff:fe01:2345]>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE
Expires: 3600
Supported: path
Content-Length: 0
```

F2: 401 Unauthorized

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111111
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101010
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111111
Call-ID: qwertyuiop11111111@192.0.1.1
CSeq: 1 REGISTER
Supported: path
WWW-Authenticate: Digest realm="example1.ne.jp",nonce="M5vIfYzRWDkD3E-iFxCJBfk8c68JXm5s",algori
thm=MD5
Content-Length: 0
```

F3: REGISTER

```
REGISTER sip:example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Max-Forwards: 70
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abce-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Contact: <sip:qwertyui@192.0.1.1>,<sip:asdfghjk@[2001:db8:1234:5678:acde:48ff:fe01:2345]>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE
Expires: 3600
Supported: path
Authorization: Digest realm="example1.ne.jp",nonce="M5vIfYzRWDkD3E-iFxCJBfk8c68JXm5s",uri="sip:
example1.ne.jp",username="0311111111",response="70849961c8f5513ca19cbfc44c147c35",algorithm=MD5
Content-Length: 0
```

F4: 200 OK (REGISTER)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Path: <sip:192.0.1.10;lr>
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxv-10101011
From: <sip:0311111111@example1.ne.jp>;tag=1234abce-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Contact:  <sip:qwertyui@192.0.1.1>;expires=3600,<sip:asdfghjk@[2001:db8:1234:5678:48ff:fe01:2345
]>;expires=3600
Supported: path
Service-Route: <sip:s-cscf.example1.ne.jp;lr>
P-Associated-URI: <sip:0311111111@example1.ne.jp>,<sip:0311111112@example1.ne.jp>
Content-Length: 0
```

VII.1.3 Deletion of terminal registration (access-line based authentication)

This clause shows an example message flow when terminal registration is deleted under the same condition of option item selection as in clause VII.1.1, assuming that the old registration of the terminal remains in the network when the power of the terminal turns on.

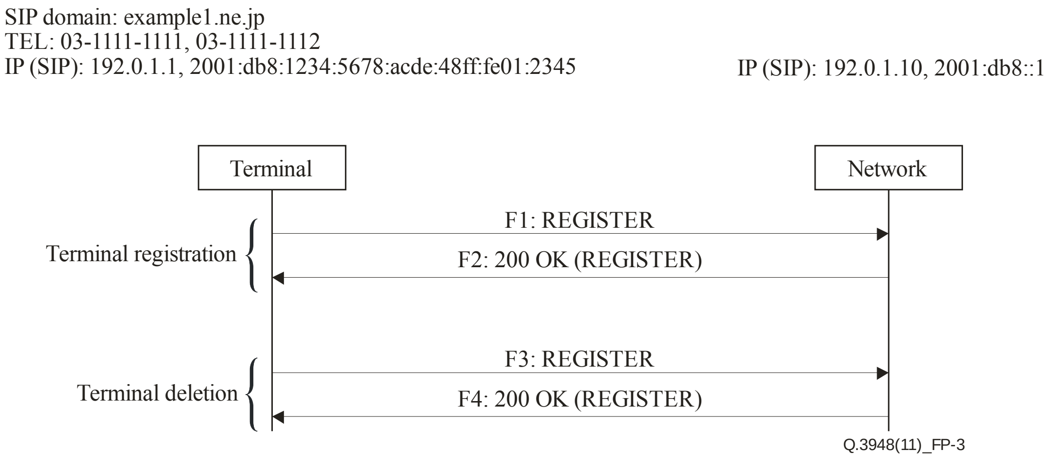

Figure VII.3 – Deletion of terminal registration (access-line based authentication)

F1 to F2 are omitted because they are the same as those of clause VII.1.1.

F3: REGISTER

```
REGISTER sip:example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Max-Forwards: 70
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Contact: *
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE
Expires: 0
Supported: path
Content-Length: 0
```

F4: 200 OK (REGISTER)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Path: <sip:192.0.1.10;lr>
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101011
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Supported: path
Service-Route: <sip:s-cscf.example1.ne.jp;lr>
P-Associated-URI: <sip:0311111111@example1.ne.jp>,<sip:0311111112@example1.ne.jp>
Content-Length: 0
```

VII.1.4 Call origination to disconnection (IPv4, Use of timer and 100rel, ITU-T G.711 μ-law)

This clause shows an example message flow of a call connection sequence on the originating side when `timer` and `100rel` are enabled on both the originating and the terminating sides. IPv4 is used for call control signals and media, UDP is used for call control, and ITU-T G.711 μ-law is used as audio media. Session refresh is performed by `UPDATE`, and disconnection (by the originating side) is finally performed by `BYE`.

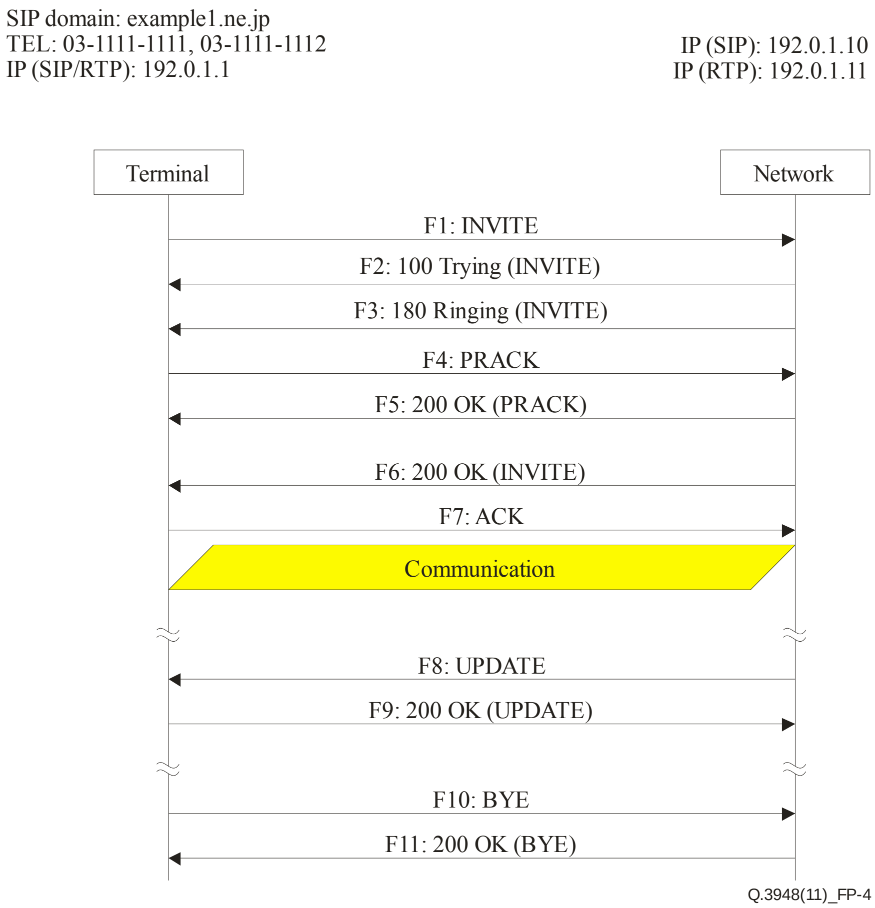

Figure VII.4 – Call origination to disconnection (IPv4, Use of `timer` and `100rel`, ITU-T G.711 μ-law) (access-line based authentication)

F1: INVITE

```
INVITE tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>,<sip:s-cscf.example1.ne.jp;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:zxcvbnm@192.0.1.1>
P-Preferred-Identity: <sip:0311111112@example1.ne.jp>
Privacy: none
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: 100rel,timer
Session-Expires: 300
Content-Type: application/sdp
Content-Length: 195

v=0
o=- 82664419472 82664419472 IN IP4 192.0.1.1
```

```
s=-
c=IN IP4 192.0.1.1
t=0 0
m=audio 10000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F2: 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Content-Length: 0
```

F3: 180 Ringing

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Record-Route: <sip:192.0.1.10;lr>
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: 100rel
RSeq: 1
Content-Length: 0
```

F4: PRACK

```
PRACK sip:mnbvcxz@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111122
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 2 PRACK
RAck: 1 1 PRACK
Content-Length: 0
```

F5: 200 OK (PRACK)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111122
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 2 PRACK
Content-Length: 0
```

F6: 200 OK (INVITE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Record-Route: <sip:192.0.1.10;lr>
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uas
Content-Type: application/sdp
Content-Length: 197

v=0
o=- 82917391739 82917391739 IN IP4 192.0.1.11
s=-
c=IN IP4 192.0.1.11
t=0 0
m=audio 20000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F7: ACK

```
ACK sip:mnbvcxz@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111123
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

F8: UPDATE

```
UPDATE sip:zxcvbnm@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-22222222
Max-Forwards: 64
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 100 UPDATE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: timer,100rel
Session-Expires: 300;refresher=uac
Content-Length: 0
```

F9: 200 OK (UPDATE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-22222222
To: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111121
From: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 100 UPDATE
Contact: <sip:zxcvbnm@192.0.1.1>
```

```
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uac
Content-Length: 0
```

F10: BYE

```
BYE sip:mnbvcxz@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK5678-11111124
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 3 BYE
Content-Length: 0
```

F11: 200 OK (BYE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK5678-11111124
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 3 BYE
Content-Length: 0
```

VII.1.5 Call origination to disconnection (IPv4, Use of timer and 100rel, ITU-T G.711 µ-law, HTTP Digest authentication)

This clause shows an example message flow when HTTP Digest authentication is performed to an `INVITE` request, which is different from the sequence in clause VII.1.4.

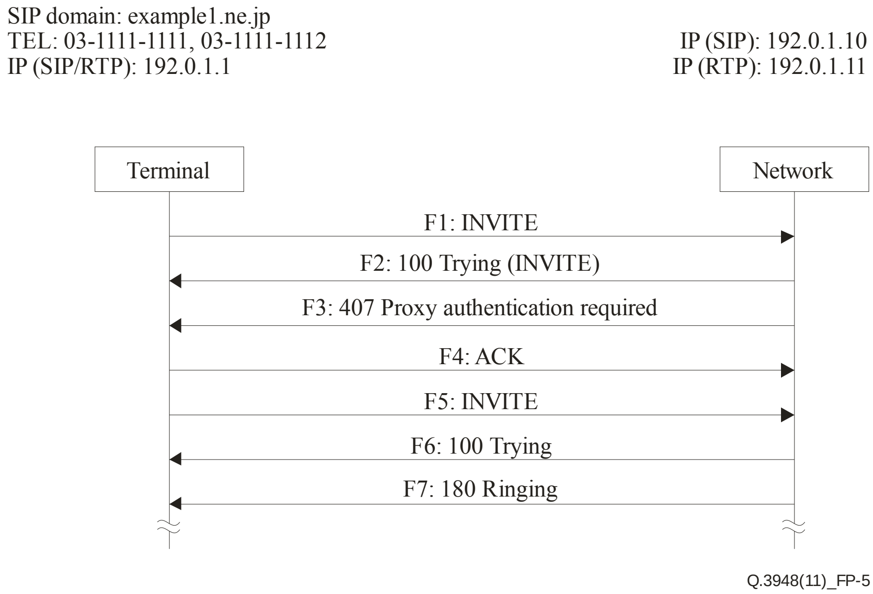

Figure VII.5 – Call origination to disconnection
(IPv4, Use of `timer` and `100rel`, ITU-T G.711 µ-law) (HTTP Digest authentication)

F1: INVITE

```
INVITE tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:zxcvbnm@192.0.1.1>
P-Preferred-Identity: <sip:0311111112@example1.ne.jp>
Privacy: none
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: 100rel,timer
Session-Expires: 300
Content-Type: application/sdp
Content-Length: 195

v=0
o=- 82664419472 82664419472 IN IP4 192.0.1.1
s=-
c=IN IP4 192.0.1.1
t=0 0
m=audio 10000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F2: 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Content-Length: 0
```

F3: 407 Proxy Authentication Required

```
SIP/2.0 407 Proxy Authentication Required
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Proxy-Authenticate:  Digest  realm="example1.ne.jp",nonce="rBqRaPCEcljUN-VQ9wS97fgQHOs9Ig4k",algo
rithm=MD5
Content-Length: 0
```

F4: ACK

```
ACK tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK2345678-11111121
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

F5: INVITE

```
INVITE tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111122
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111122
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 2 INVITE
Proxy-Authorization: Digest username="0311111111",realm="example1.ne.jp",nonce="rBqRaPCEcljUN-V
Q9wS97fgQHOs9Ig4k",uri="tel:0322222222;phone-context=example1.ne.jp",response="0cd3f053fe229503
6b73613dce5b2fa3",algorithm=MD5
Contact: <sip:xcvbnmz@192.0.1.1>
P-Preferred-Identity: <sip:0311111112@example1.ne.jp>
Privacy: none
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: 100rel,timer
Session-Expires: 300
Content-Type: application/sdp
Content-Length: 195

v=0
o=- 82664419518 82664419518 IN IP4 192.0.1.1
s=-
c=IN IP4 192.0.1.1
t=0 0
m=audio 10000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F6: 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111122
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111122
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 2 INVITE
Content-Length: 0
```

F7: 180 Ringing

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111122
Record-Route: <sip:192.0.1.10;lr>
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101021
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111122
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 2 INVITE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: 100rel
RSeq: 1
Content-Length: 0
```

VII.1.6 Call termination to disconnection (IPv4, Use of timer and 100rel, ITU-T G.711 μ-law)

This clause shows an example message flow on the terminating side under the same condition of option item selections as in clause VII.1.4. After receiving a call from the network, session refresh is performed by `UPDATE`, and disconnection (by the terminating side) is performed by `BYE`. The network notifies the calling-party's identity information by the `P-Asserted-Identity` header, and the called-party's information by the `P-Called-Party-ID` header to the called terminal.

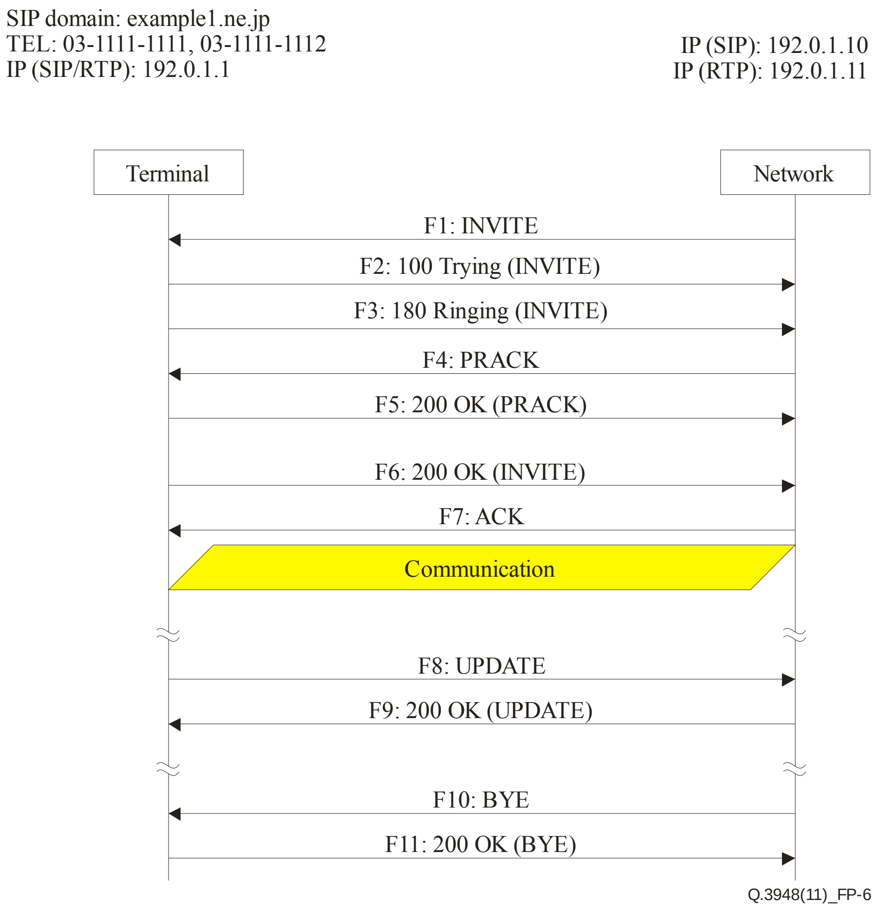

Figure VII.6 – Call termination to disconnection (IPv4, Use of timer and 100rel, ITU-T G.711 μ-law)

F1: INVITE

```
INVITE sip:qwertyui@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101020
Record-Route: <sip:192.0.1.10;lr>
Max-Forwards: 64
To: <sip:0311111112@example1.ne.jp>
From: <sip:03122222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101020@192.0.1.10
CSeq: 101 INVITE
Contact: <sip:lkjhgfds@192.0.1.10>
P-Asserted-Identity: "0322222223" <sip:0322222223@example1.ne.jp>,"0322222223" <tel:0322222223;
phone-context=example1.ne.jp>
Privacy: none
P-Called-Party-ID: <sip:0311111112@example1.ne.jp>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: 100rel,timer
Session-Expires: 300
Content-Type: application/sdp
Content-Length: 197
```

```
v=0
o=- 82664482616 82664482616 IN IP4 192.0.1.11
s=-
c=IN IP4 192.0.1.11
t=0 0
m=audio 40000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F2: 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101020
To: <sip:0311111112@example1.ne.jp>
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101020@192.0.1.10
CSeq: 101 INVITE
Content-Length: 0
```

F3: 180 Ringing

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101020
Record-Route: <sip:192.0.1.10;lr>
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 101 INVITE
Contact: <sip:asdfghjk@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: 100rel
RSeq: 1
Content-Length: 0
```

F4: PRACK

```
PRACK sip:asdfghjk@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101021
Max-Forwards: 64
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 102 PRACK
RAck: 1 1 PRACK
Content-Length: 0
```

F5: 200 OK (PRACK)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101021
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 102 PRACK
Content-Length: 0
```

F6: 200 OK (INVITE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101020
Record-Route: <sip:192.0.1.10;lr>
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101020@192.0.1.10
CSeq: 101 INVITE
Contact: <sip:asdfghjk@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uas
Content-Type: application/sdp
Content-Length: 195

v=0
o=- 82917391739 82917391739 IN IP4 192.0.1.1
s=-
c=IN IP4 192.0.1.1
t=0 0
m=audio 30000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F7: ACK

```
ACK sip:asdfghjk@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101022
Max-Forwards: 70
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 101 ACK
Content-Length: 0
```

F8: UPDATE

```
UPDATE sip:lkjhgfds@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111125
Max-Forwards: 70
To: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 201 UPDATE
Contact: <sip:asdfghjk@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: timer,100rel
Session-Expires: 300;refresher=uac
Content-Length: 0
```

F9: 200 OK (UPDATE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111125
To: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 201 UPDATE
Contact: <sip:lkjhgfds@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
```

```
Require: timer
Session-Expires: 300;refresher=uac
Content-Length: 0
```

F10: BYE

```
BYE sip:asdfghjk@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-11111124
Max-Forwards: 70
To: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-11111121
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 103 BYE
Content-Length: 0
```

F11: 200 OK (BYE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-11111124
To: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-11111121
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 103 BYE
Content-Length: 0
```

VII.1.7 Call cancellation (disconnection while ringing)

This clause shows an example message flow for call cancellation by the originating side under the same condition of option item selections as in clause VII.1.4.

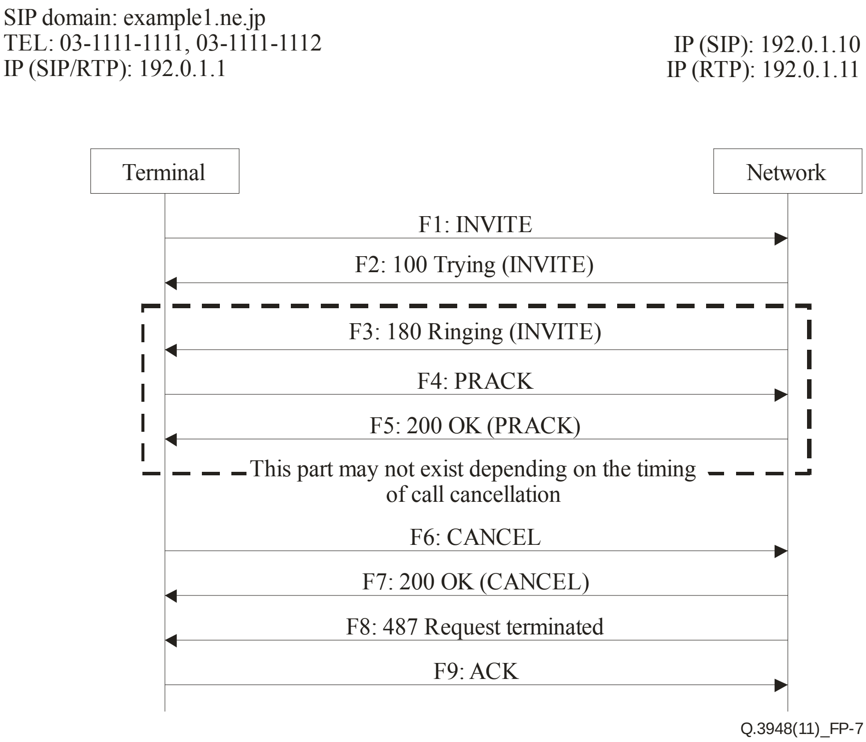

Figure VII.7 – Call cancellation (disconnection while ringing)

F1 to F5 are omitted because they are the same as those of clause VII.1.4.

F6: CANCEL

```
CANCEL tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>,<sip:s-cscf.example1.ne.jp;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 CANCEL
Content-Length: 0
```

F7: 200 OK (CANCEL)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 CANCEL
Content-Length: 0
```

F8: 487 Request Terminated

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 INVITE
Content-Length: 0
```

F9: ACK

```
ACK tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

VII.1.8 Busy on the terminating side

This clause shows an example message flow in the case that the destination is busy (short of empty sessions) under the same condition of option item selections as in clause VII.1.4.

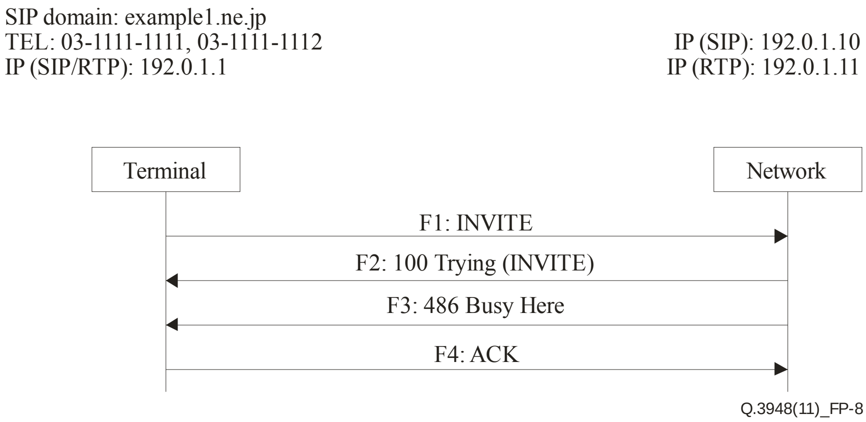

Figure VII.8 – Busy on the terminating side

F1 to F2 are omitted because they are the same as those of clause VII.1.4.

F3: 486 Busy Here

```
SIP/2.0 486 Busy Here
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 INVITE
Content-Length: 0
```

F4: ACK

```
ACK tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

VII.1.9 Hearing the guidance

This clause shows an example message flow in the case that the call is terminated after audio guidance is provided under the same condition of option item selections as in clause VII.1.4.

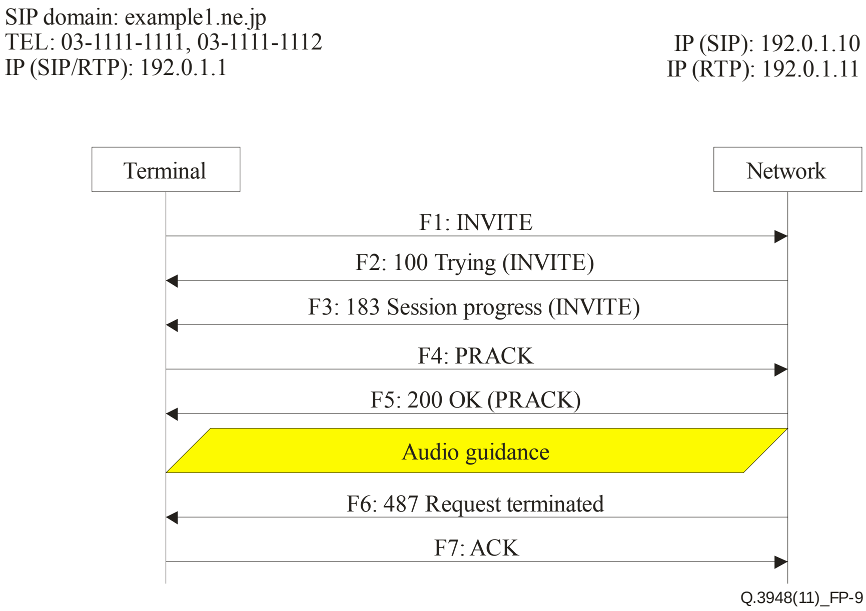

Figure VII.9 – Hearing the guidance

F1 to F2 are omitted because they are the same as those of clause VII.1.4.

F3: 183 Session Progress (INVITE)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Record-Route: <sip:192.0.1.10;lr>
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: 100rel
RSeq: 1
Content-Type: application/sdp
Content-Length: 197

v=0
o=- 82917391739 82917391739 IN IP4 192.0.1.11
s=-
c=IN IP4 192.0.1.11
t=0 0
m=audio 20000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F4 to F5 are omitted because they are the same as those of clause VII.1.4.

F6: 487 Request Terminated

```
SIP/2.0 487 Request Terminated
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
```

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

F7: ACK

```
ACK tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

VII.1.10 Connection after hearing the guidance (using UPDATE)

This clause shows an example message flow when a communication takes place by connecting to the final called-party after the guidance is provided from the network, in the same sequence as in clause VII.1.9. In switching from the guidance to the final called-party, an UPDATE request in the early dialogue is used.

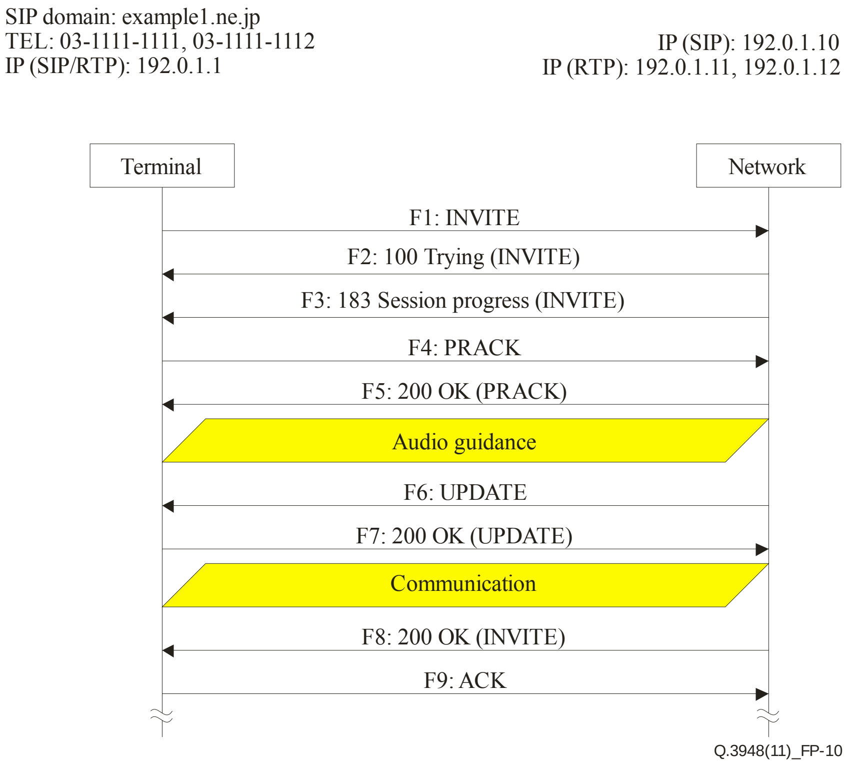

Figure VII.10 – Connection after hearing the guidance (using UPDATE)

F1 to F5 are omitted because they are the same as those of clause VII.1.9.

F6: UPDATE

```
UPDATE sip:zxcvbnm@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-22222222
Max-Forwards: 64
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: qwertyuiop111112@192.0.1.1
```

```
CSeq: 100 UPDATE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: timer,100rel
Content-Length: 197

v=0
o=- 82917391739 82917391740 IN IP4 192.0.1.11
s=-
c=IN IP4 192.0.1.12
t=0 0
m=audio 21000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F7: 200 OK (UPDATE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-22222222
To: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222222@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 100 UPDATE
Contact: <sip:zxcvbnm@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Content-Length: 195

v=0
o=- 82664419472 82664419472 IN IP4 192.0.1.1
s=-
c=IN IP4 192.0.1.1
t=0 0
m=audio 10000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F8: 200 OK (INVITE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Record-Route: <sip:192.0.1.10;lr>
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uas
Content-Length: 0
```

F9: ACK

```
ACK sip:mnbvcxz@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111123
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
```

```
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

VII.1.11 Sending MESSAGE (using IPv6)

This clause shows an example of message flow to send a short text message by using a `MESSAGE` request. SIP messages are sent and received by using IPv6 UDP.

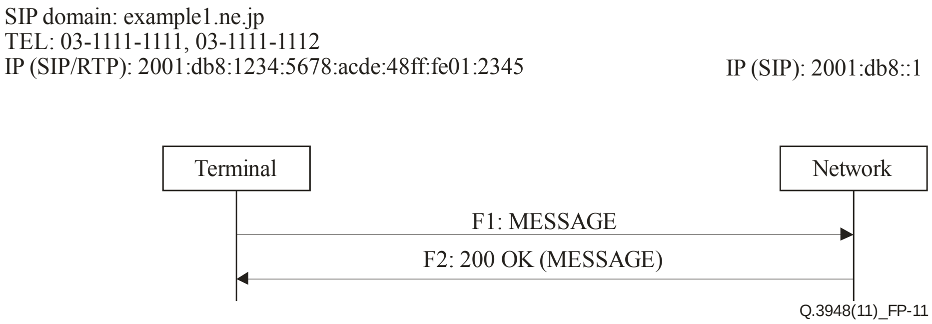

Figure VII.11 – Sending MESSAGE (using IPv6)

F1: MESSAGE

```
MESSAGE tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP [2001:db8:1234:5678:acde:48ff:fe01:2345]:5060;branch=z9hG4bK12345678-11111131
Route: <sip:[2001:db8::1];lr>,<sip:s-cscf.example1.ne.jp;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111131
Call-ID: qwertyuiop111113@[2001:db8:1234:5678:acde:48ff:fe01:2345]
CSeq: 1001 MESSAGE
P-Preferred-Identity: <sip:0311111112@example1.ne.jp>
Privacy: none
Content-Type: text/plain;charset=utf-8
Content-Length: 13

foo bar baz
```

F6: 200 OK (MESSAGE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [2001:db8:1234:5678:acde:48ff:fe01:2345]:5060;branch=z9hG4bK12345678-11111131
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101030
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111131
Call-ID: qwertyuiop111113@[2001:db8:1234:5678:acde:48ff:fe01:2345]
CSeq: 1001 MESSAGE
Content-Length: 0
```

VII.1.12 Receiving MESSAGE (using IPv6)

This clause shows an example of message flow to receive a short text message by using a `MESSAGE` request. SIP messages are sent and received by using IPv6 UDP.

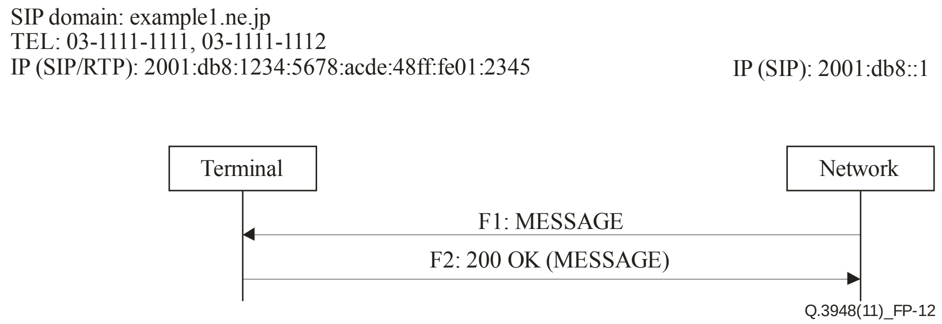

Figure VII.12 – Receiving MESSAGE (using IPv6)

F1: MESSAGE

```
MESSAGE sip:asdfghjk@[2001:db8:1234:5678:acde:48ff:fe01:2345] SIP/2.0
Via: SIP/2.0/UDP [2001:db8::1]:5060;branch=z9hG4bK87654321-10101030
Max-Forwards: 64
To: <sip:0311111112@example1.ne.jp>
From: <sip:03122222223@example1.ne.jp>;tag=9876zyxw-10101030
Call-ID: poiuytrewq101030@[2001:db8::1]
CSeq: 2001 MESSAGE
P-Asserted-Identity: "0322222223" <sip:0322222223@example1.ne.jp>,"0322222223" <tel:0322222223;
phone-context=example1.ne.jp>
Privacy: none
P-Called-Party-ID: <sip:0311111112@example1.ne.jp>
Content-Type: text/plain;charset=utf-8
Content-Length: 13

foo bar baz
```

F6: 200 OK (MESSAGE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [2001:db8::1]:5060;branch=z9hG4bK87654321-10101030
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111131
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101030
Call-ID: poiuytrewq101030@[2001:db8::1]
CSeq: 2001 MESSAGE
Content-Length: 0
```

VII.1.13 Subscription to registration event

This clause shows an example message flow in the case of subscribing (SUBSCRIBE) to the registration (reg) event described in clause C.6.

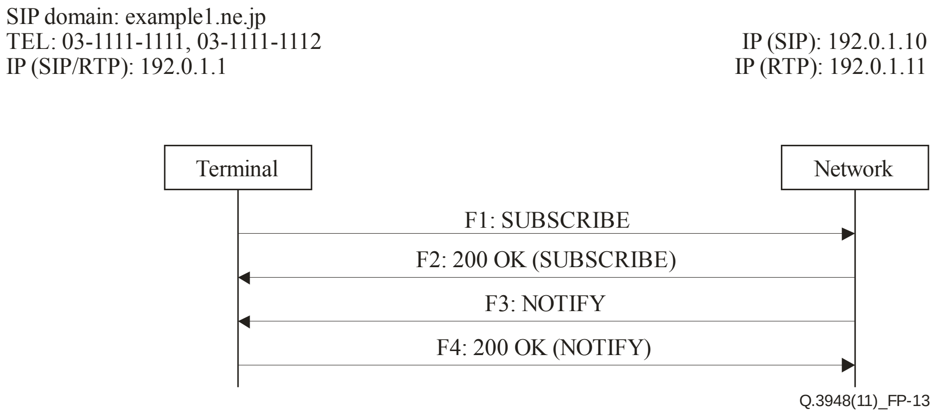

Figure VII.13 – Subscription to registration event

F1: SUBSCRIBE

```
SUBSCRIBE sip:0311111111@example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111141
Max-Forwards: 70
Route: <sip:192.0.1.10;lr>,<sip:s-cscf.example1.ne.jp>
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111141
Call-ID: qwertyuiop111114@192.0.1.1
CSeq: 1 SUBSCRIBE
Contact: <sip:wertyuio@192.0.1.1>
P-Preferred-Identity: <sip:0311111111@example1.ne.jp>
Privacy: none
Event: reg
Expires: 3600
Accept: application/reginfo+xml
Content-Length: 0
```

F2: 200 OK (SUBSCRIBE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060; branch=z9hG4bK12345678-11111141
Record-Route: <sip:192.0.1.10;lr>
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101040
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111141
Call-ID: qwertyuiop111114@192.0.1.1
CSeq: 1 SUBSCRIBE
Contact: <sip:oiuytrew@192.0.1.10>
Event: reg
Expires: 3600
Content-Length: 0
```

F3: NOTIFY

```
NOTIFY sip:wertyuio@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK12345678-10101040
Max-Forwards: 69
To: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111141
From: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101040
Call-ID: qwertyuiop111114@192.0.1.1
CSeq: 101 NOTIFY
Contact: <sip:oiuytrew@192.0.1.10>
Subscription-State: active;expires=3600
Event: reg
Expires: 3600
```

```
Content-Type: application/reginfo+xml
Content-Length: 741

<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
             version="1" state="full">
  <registration aor="sip:0311111111@example1.ne.jp" id="a7" state="active">
    <contact id="76" state="active" event="registered">
      <uri>sip:qwertyui@192.0.1.1</uri>
    </contact>
  </registration>
  <registration aor="sip:0311111112@example1.ne.jp" id="a8" state="active">
    <contact id="77" state="active" event="registered">
      <uri>sip:qwertyui@192.0.1.1</uri>
    </contact>
  </registration>
  <registration aor="tel:+81311111111" id="a9" state="active">
    <contact id="78" state="active" event="registered">
      <uri>sip:qwertyui@192.0.1.1</uri>
    </contact>
  </registration>
</reginfo>
```

F4: 200 OK (NOTIFY)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK12345678-10101040
To: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111141
From: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101040
Call-ID: qwertyuiop111114@192.0.1.1
CSeq: 101 NOTIFY
Content-Length: 0
```

VII.1.14 Notification of registration event (on deletion of terminal registration)

This clause shows an example message flow in the case that notification is given to the terminal by a NOTIFY request when the terminal registration is deleted by the network. Subscription to the registration event is as described in clause VII.1.13.

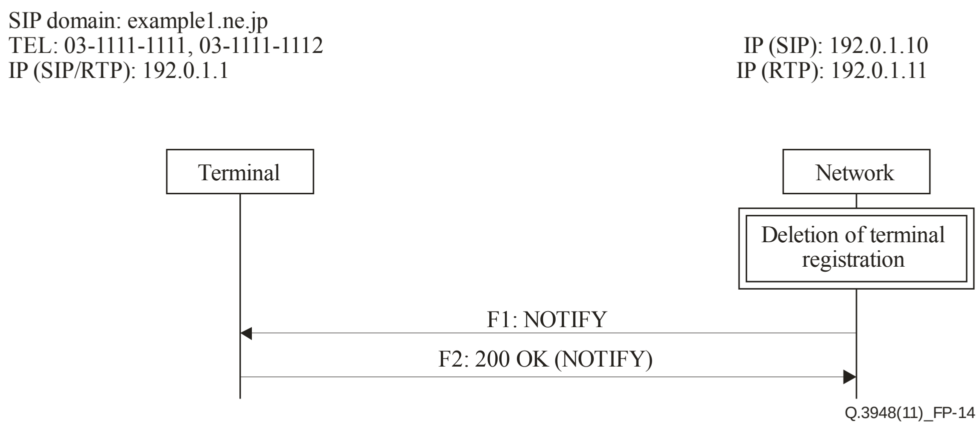

Figure VII.14 – Notification of registration event

F1: NOTIFY

```
NOTIFY sip:wertyuio@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK12345678-10101041
Max-Forwards: 69
To: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111141
```

```
From: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101040
Call-ID: qwertyuiop111114@192.0.1.1
CSeq: 101 NOTIFY
Contact: <sip:oiuytrew@192.0.1.10>
Subscription-State: terminated
Event: reg
Expires: 3600
Content-Type: application/reginfo+xml
Content-Length: 758

<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
             version="1" state="full">
  <registration aor="sip:0311111111@example1.ne.jp" id="a7" state="active">
    <contact id="76" state="terminated" event="deactivated">
      <uri>sip:qwertyui@192.0.1.1</uri>
    </contact>
  </registration>
  <registration aor="sip:0311111112@example1.ne.jp" id="a8" state="active">
    <contact id="77" state="terminated" event="deactivated ">
      <uri>sip:qwertyui@192.0.1.1</uri>
    </contact>
  </registration>
  <registration aor="tel:+81311111111" id="a9" state="active">
    <contact id="78" state="terminated" event="deactivated ">
      <uri>sip:qwertyui@192.0.1.1</uri>
    </contact>
  </registration>
</reginfo>
```

F2: 200 OK (NOTIFY)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK12345678-10101041
To: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111141
From: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101040
Call-ID: qwertyuiop111114@192.0.1.1
CSeq: 101 NOTIFY
Content-Length: 0
```

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	**Switching and signalling**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2012