INTERNATIONAL TELECOMMUNICATION UNION

**TELECOMMUNICATION STANDARDIZATION SECTOR**

STUDY PERIOD 2005-2008

**STUDY GROUP 11**

# TD 185 Rev.1 (PLEN/11)

**English only**

**Original: English**

**Question(s):** 3/11 Seoul, 16 - 23 January 2008

**TEMPORARY DOCUMENT**

**Source:** Co-Editors

**Title:** Draft Recommendation Q.3402 (for consent)

**Abstract**

This document contains the draft Recommendation Q.3402 for consent to AAP at this SG11 meeting (January 2008).

| | | |
|---|---|---|
| **Contact:** | Martin Dolly<br>AT&T<br>United States of America | Tel: +1 732 420 4174<br>Fax:<br>Email: mdolly<at>att.com |
| **Contact:** | Jerry Ezrol<br>AT&T<br>United States of America | Tel: +1 703-691-6848<br>Fax:<br>Email: ezrol<at>att.com |
| **Contact:** | Takumi Ohba<br>NTT Corporation<br>Japan | Tel: +81 422 59 7748<br>Fax: +81 422 60 7429<br>Email: ohba.takumi<at>lab.ntt.co.jp |
| **Contact:** | Mitsuko Koga<br>NTT Corporation<br>Japan | Tel: +81 422 36 7565<br>Fax: +81 422 37 7966<br>Email: mitsuko.koga<at>ntt-at.co.jp |

**ITU-T draft Recommendation Q.3402**

# NGN UNI Signalling Profile (Protocol Set 1)

**Summary**

This Recommendation defines the NGN user-to-network interface (UNI) signalling profile for use between users and networks of protocol set 1 for voice, video, and data services.

**Keywords**

NGN, SIP, SDP, Signalling, Profile

## 1. Scope

This Recommendation specifies a service-level profile, i.e. SIP/SDP interface description between a user and a network, and a transport-level profile, e.g. RTP.

For protocol set 1 of the NGN UNI profile, this Recommendation covers multimedia (voice, video, and data) which include VoIP, multimedia telephony, DTMF, T.38 fax, and multimedia ring back and ringing tones and announcements.

This Recommendation covers all terminal types, e.g. SIP Residential Gateway, SIP Phone, and SIP IP PBX. Therefore, the following UNI interfaces are specified:

- SIP Residential Gateway - to - Service Provider, where PSTN/ISDN terminals or IP phones can be connected to Residential Gateway.
- SIP Phone - to - Service Provider, where the SIP phone can be either a soft phone or a hard phone implemented by IMS based SIP specifications.
- SIP IP PBX - to - Service Provider, where the IP PBX can be either a proxy or B2BUA.

## 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.

### 2.1. ITU and ISO/IEC references

[Y.2012] ITU-T Recommendation Y.2012 (2006), Functional requirements and architecture of the NGN

[T.38] ITU-T Recommendation T.38 (2007), Procedures for real-time Group 3 facsimile communication over IP networks

[T.140] ITU-T Recommendation T.140 (1998), "Protocol for multimedia application text conversation"

[G.711] ITU-T Recommendation G.711 (1988), "Pulse code modulation (PCM) of voice frequencies",

[G.722] ITU-T Recommendation G.722 (1988), "7 kHz audio-coding within 64 kbit/s"

[G.722.1] ITU-T Recommendation G.722.1 (2005), "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss"

[G.722.2] ITU-T Recommendation G.722.2 (2003), "Wideband coding of speech at around 16 kbit/s using Adaptive Multi-Rate Wideband (AMR-WB)"

[G.726] ITU-T Recommendation G.726 (1990), "40, 32, 24, 16 kbit/s Adaptive Differential Pulse Code Modulation (ADPCM)"

[G.729] ITU-T Recommendation G.729 (1996), "Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)"

[G.729A] ITU-T Recommendation G.729 Annex A (1996), "Reduced complexity 8 kbit/s CS-ACELP speech codec"

[G.729.1] ITU-T Recommendation G.729.1 (2006), "G.729 based Embedded Variable bit-rate coder: An 8-32 kbit/s scalable wideband coder bitstream interoperable with G.729"

[H.263] ITU-T Recommendation H.263 (2005), Video coding for low bit rate communication

[H.264] ITU-T Recommendation H.264 (2005), Advanced video coding for generic audiovisual services

[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

## 2.2. IETF references

### 2.2.1. Service-level signalling specifications

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

[RFC 2327] IETF RFC 2327 (1998), SDP: Session Description Protocol

[RFC 2617] IETF RFC 2617 (1999), HTTP Authentication: Basic and Digest Access Authentication

[RFC 2976] IETF RFC 2976 (2000), The SIP INFO Method

[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 3263] IETF RFC 3263 (2002), Session Initiation Protocol (SIP): Locating SIP Servers

[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 3420] IETF RFC 3420 (2002), Internet Media Type message/sipfrag

[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 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 3725] IETF RFC 3725 (2004), Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)

[RFC 3824] IETF RFC 3824 (2004), Using E.164 numbers with the Session Initiation Protocol (SIP)

[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 3842] IETF RFC 3842 (2004), A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)

[RFC 3853] IETF RFC 3853 (2004), S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)

[RFC 3856] IETF RFC 3856 (2004), A Presence Event Package for the Session Initiation Protocol (SIP)

[RFC 3857] IETF RFC 3857 (2004), A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP)

[RFC 3858] IETF RFC 3858 (2004), An Extensible Markup Language (XML) Based Format for Watcher Information

[RFC 3859] IETF RFC 3859 (2004), Common Profile for Presence (CPP)

[RFC 3860] IETF RFC 3860 (2004), Common Profile for Instant Messaging (CPIM)

[RFC 3861] IETF RFC 3861 (2004), Address Resolution for Instant Messaging and Presence

[RFC 3862] IETF RFC 3862 (2004), Common Presence and Instant Messaging (CPIM): Message Format

[RFC 3863] IETF RFC 3863 (2004), Presence Information Data Format (PIDF)

[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 3960] IETF RFC 3960 (2004), Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)

[RFC 3966] IETF RFC 3966 (2004), The tel URI for Telephone Numbers

[RFC 3994] IETF RFC 3994 (2005), Indication of Message Composition for Instant Messaging

[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 4168] IETF RFC 4168 (2005), The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)

[RFC 4235] IETF RFC 4235 (2005), An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)

[RFC 4244] IETF RFC 4244 (2005), An Extension to the Session Initiation Protocol (SIP) for Request History Information

[RFC 4320] IETF RFC 4320 (2006), Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction

[RFC 4412] IETF RFC 4412 (2006), Communications Resource Priority for the Session Initiation Protocol (SIP)

[RFC 4458] IETF RFC 4458 (2006), Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)

[RFC 4480] IETF RFC 4480 (2006), RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)

[RFC 4483] IETF RFC 4483 (2006), A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages

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

[RFC 4575] IETF RFC 4575 (2006), A Session Initiation Protocol (SIP) Event Package for Conference State

[RFC 4579] IETF RFC 4579 (2006), Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents

[RFC 4583] IETF RFC 4583 (2006), Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams

[RFC 4662] IETF RFC 4662 (2006), A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists

[RFC 4715] IETF RFC 4715 (2006), The Integrated Services Digital Network (ISDN) Subaddress Encoding Type for tel URI

[RFC 4730] IETF RFC 4730 (2006), A Session Initiation Protocol (SIP) Event Package for Key Press Stimulus (KPML)

[RFC 5031] IETF RFC 5031 (2008), A Uniform Resource Name (URN) for Emergency and Other Well-Known Services

[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)

### 2.2.2. Transport-level specifications

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

[RFC 3047] IETF RFC 3047 (2001), RTP Payload Format for ITU-T Recommendation G.722.1

[RFC 3267] IETF RFC 3267 (2002), Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs

[RFC 3389] IETF RFC 3389 (2002), Real-time Transport Protocol (RTP) Payload for Comfort Noise (CN)

[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 3558] IETF RFC 3558 (2003), RTP Payload Format for Enhanced Variable Rate Codecs (EVRC) and Selectable Mode Vocoders (SMV)

[RFC 3611] IETF RFC 3611 (2003), RTP Control Protocol Extended Reports (RTCP XR)

[RFC 3711] IETF RFC 3711 (2004), The Secure Real-time Transport Protocol (SRTP)

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

[RFC 4103] IETF RFC 4103 (2005), RTP Payload for Text Conversation

[RFC 4348] IETF RFC 4348 (2006), Real-Time Transport Protocol (RTP) Payload Format for the Variable-Rate Multimode Wideband (VMR-WB) Audio Codec

[RFC 4629] IETF RFC 4629 (2007), RTP Payload Format for ITU-T Rec. H.263 Video

[RFC 4733] IETF RFC 4733 (2006), RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals

[RFC 4749] IETF RFC 4749 (2006), RTP Payload Format for the G.729.1 Audio Codec

## 2.3. ETSI references

[EN 301 703] ETSI EN 301 703 V7.0.2 (1999-12), Digital cellular telecommunications system (Phase 2+); Adaptive Multi-Rate (AMR); Speech processing functions; General description (GSM 06.71 version 7.0.2 Release 1998)

### 2.4. Other references

[TIA-127] TIA-127-A, Enhanced Variable Rate Codec (EVRC) Speech Option 3 for Wideband Spread Spectrum Digital Systems (May 2004)

[TIA-1016] TIA-1016-A, Source-Controlled Variable-Rate Multimode Wideband Speech Codec (VMR-WB), Service Options 62 and 63 for Spread Spectrum Systems (January 2006)

## 3. Definitions

For SIP- and SDP-specific terminology, reference shall be made to [RFC 3261], [RFC3264], [RFC 2327], and [RFC 4566]. For NGN-specific terminology, reference shall be made to [Y.2012]. Definitions for additional terminology used in this Recommendation are as follows:

**3.1. recommended-codec list**: A recommended-codec list contains the codecs that should be shown by the network to the user in SIP/SDP messages exchanged over the UNI.

Note: The purpose of the recommended-codec list is just to show the codecs that a network recommends for use in the UNI, and the recommended-codec list does not recommend terminals to implement all the codecs shown in the list.

**3.2. EUF**: The end-user functions (EUF) includes end-user equipment both the legacy terminals and NGN terminals, and it also includes customer networks. End-user equipment may be either mobile or fixed. The end-user interfaces via which the EUF is connected to NGN are supported by both physical and functional (control) interfaces.

**3.3. SCF**: The service control functions (SCF) establish, monitor, support, and release multimedia sessions and manage the user's service interactions.

**3.4. SIP B2BUA**: A back-to-back user agent (B2BUA) is a concatenation of a SIP user agent client (UAC) and user agent server (UAS).
Note: The IETF defines the B2BUA in [RFC 3261] as “a logical entity that receives a request and processes it as a user agent server (UAS). In order to determine how the request should be answered, it acts as a user agent client (UAC) and generates requests. Unlike a proxy server, it maintains dialog state and shall participate in all requests sent on the dialogs it has established. Since it is a concatenation of a UAC and UAS, no explicit definitions are needed for its behavior.” (UAC and UAS behaviours are defined in [RFC 3261].) A B2BUA reformulates a message before sending it as a new request.

## 4. Abbreviations

This Recommendation uses the following abbreviations:

| | |
|---|---|
| 3GPP | 3rd-Generation Partnership Project |
| AKA | Authentification and Key Agreement |
| AMR | Adaptive Multirate (codec) |
| AMR NB | AMR Narrowband |
| AMR WB | AMR Wideband |
| B2BUA | Back-to-Back User Agent |

| | |
|---|---|
| CSC-FE | Call Session Control Functional Entity |
| CSMA/CD | Carrier Sense Multiple Access with Collision Detection |
| DTMF | Dual-Tone Multifrequency |
| EUF | End-User Functions |
| EVRC | Enhanced Variable Rate Codec |
| FQDN | Fully Qualified Domain Name |
| GRUU | Globally Routable User Agent URIs |
| HTTP | Hypertext Transfer Protocol |
| IBC-FE | Interconnection Border gateway Control Functional Entity |
| ICMP | Internet Control Message Protocol |
| IETF | Internet Engineering Task Force |
| IP PBX | IP Private Branch eXchange |
| ISDN | Integrated Services Digital Network |
| ISO/IEC | International Standardization Organization/International Electrotechnical Commission |
| ISUP | ISDN User Part |
| ITU-T | International Telecommunication Union-Telecommunication |
| IVR | Interactive Voice Response |
| KPML | Key Press Stimulus |
| MIME | Multi-purpose Internet Mail Extensions |
| MPEG | Moving Picture Experts Group |
| NAT | Network Address Translation |
| NGN | Next Generation Network |
| NGN-TE | NGN Terminal Equipment |
| PSTN | Public Switched Telephone Network |
| QoS | Quality of Service |
| RFC | Request For Comments |
| RGW | Residential Gateway |
| RTCP | RTP Control Protocol |
| RTCP XR | RTCP eXtended Reports |
| RTP | Real-Time Transport Protocol |
| SCF | Service Control Functions |
| SCTP | Stream Control Transmission Protocol |
| SDP | Session Description Protocol |
| SIP | Session Initiation Protocol |

| | |
|---|---|
| SIPS | Session Initiation Protocol Secure |
| SMV | Selectable Mode Vocoders |
| SRTP | Secure Real-time Transport Protocol |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| UA | User Agent |
| UAC | User Agent Client |
| UAS | User Agent Server |
| UDP | User Datagram Protocol |
| UNI | User-to-Network Interface |
| URI | Universal Resource Identifier |
| VMR-WB | Variable-Rate Multi-Mode Wideband |
| VoIP | Voice over IP |

## 5. Reference Model

The UNI interface defined in [Y.2012] is the scope covered by this Recommendation in the NGN architecture.

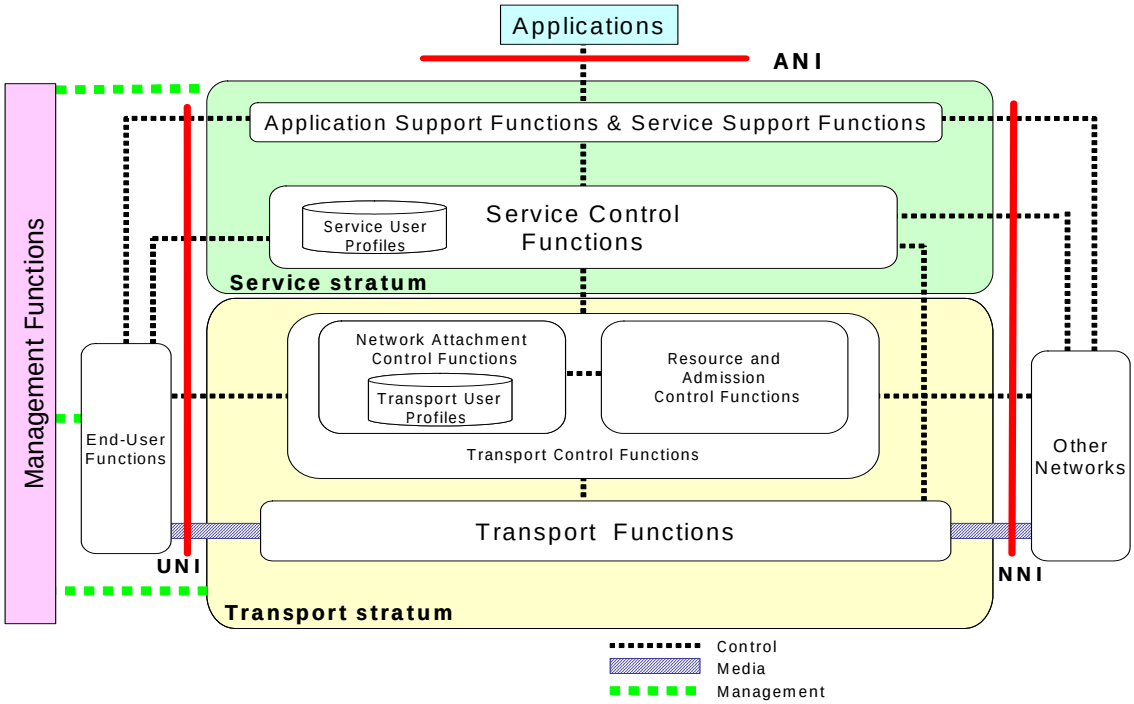


Figure 1: UNI interface covered by this Recommendation within NGN architecture

Figures 2, 3, and 4 illustrate the possible scenarios of terminal types within the EUF.

Figure 2 shows the scenario for PSTN/ISDN terminals and IP phones connected to a service provider via a SIP Residential Gateway.

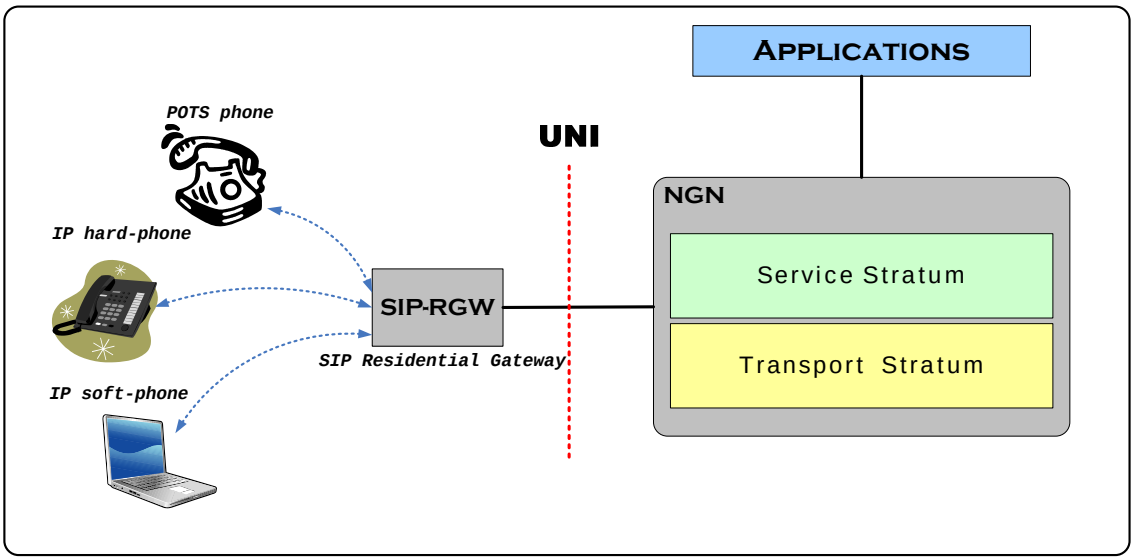


Figure 2: Scenario for SIP Residential Gateway

Figure 3 shows the scenario for IMS-based SIP phones connected directly to a service provider.

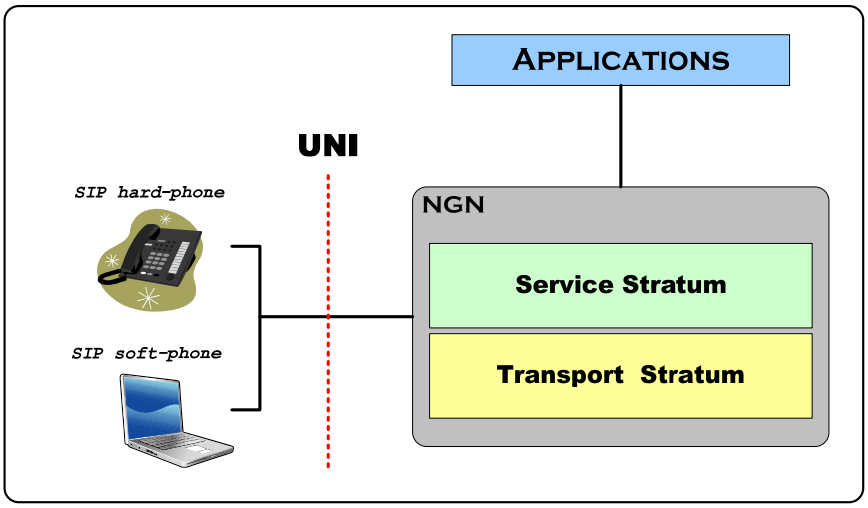


Figure 3: Scenario for IMS-based SIP phone

Figure 4 shows the scenario for SIP phones connected to a service provider via a SIP IP PBX.

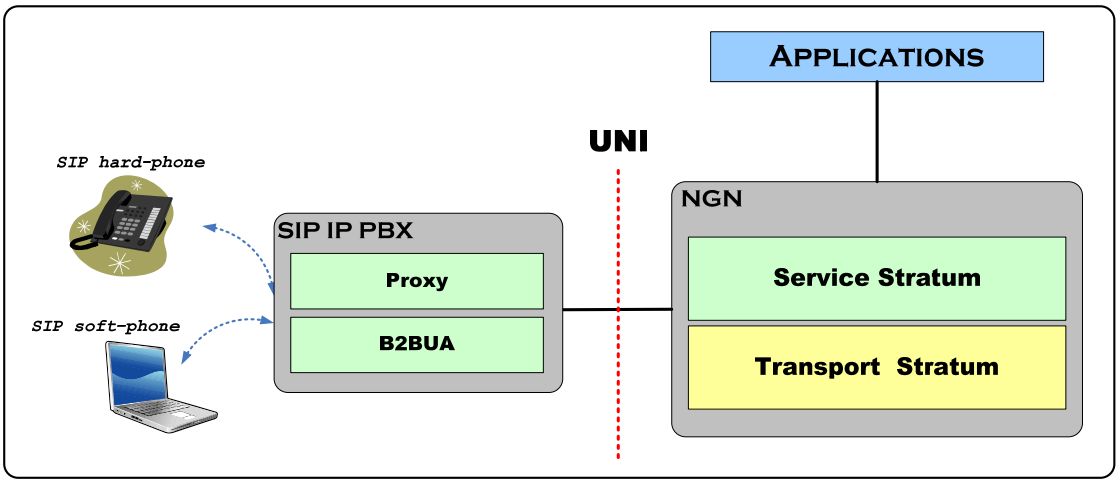


Figure 4: Scenario for SIP IP PBX

## 6. Assumptions

This Recommendation is based on the following set of assumptions:

1. SIP/SDP is used for session control.
2. RTP or SRTP is used for voice and video transport; other transport protocols may be used for data applications.

## 7. Media Availability in a SIP Session

### 7.1 Consideration related to media packets

The following apply to any media session established across the UNI using SIP:

a) Originating-side EUF

- shall send media packets from the originating party in the direction toward the network upon and after receiving a final SDP answer within a SIP 2xx response to the INVITE for normal dialog.
- may send media packets from the originating party in the direction toward the network as early as the first SDP answer has occurred, which is in a SIP 1xx response to the INVITE, when early dialog has been set up. A network, as a policy, may choose not to pass media packets from the originating party until the final SDP offer/answer has been made to avoid theft-of-service in cases where usage-sensitive billing is employed.
- shall be prepared to receive media packets from the terminating party via the network after sending the INVITE with an SDP offer.

b) Terminating-side EUF

- shall send media packets from the terminating party in the direction toward the network upon and after sending a SIP 2xx response to the INVITE with SDP.
- shall be prepared to receive media packets from the originating party via the network after sending a SIP 2xx response to the INVITE.

c) As per [RFC 3261], once a SIP dialog has ended, the flow of media packets shall be halted.

d) The absence of media packets across the UNI over any time interval in either direction shall not be taken by either a EUF or the network as a sufficient reason to clear the SIP session. When the

status of media flows is active according to the SDP negotiation, the absence of packets across the UNI for a given duration may constitute a reason to clear the SIP session.

Note: The absence of packets across the UNI for a given duration can be a reason to clear the SIP session only when it is sure that is because of the failure.

### 7.2 Addition or deletion of any media stream

Any media session established across the UNI using SIP starts either with one kind of media type (e.g. voice) or with different kind of media types for multiple media streams (e.g. voice and video) by exchanging SDP offer/answer between the originating and terminating parties. Adding different type of media streams or removing any other kind of media streams is possible during the communication.

## 8. Codec

### 8.1. Codec list

It is the responsibility of entities at the rim of the NGN (e.g. NGN-TE) and network equipment originating and terminating the NGN IP media flows to negotiate and select a common codec for each “end-to-end” media session. Therefore, the NGN shall allow end-to-end negotiation within the recommended-codec list from the network and may allow it outside the list based on its network policy.

Note 1: In case a common codec cannot be negotiated, this Recommendation does not provide procedures for the UNI.

Note 2: In the interest of promoting interoperability, limiting the number of transcodings on network connections, and possibly improving network resource management, it is desirable that the NGN recommends the recommended-codec list to users. SIP/SDP messages exchanged over the UNI indicate a request to use one or more of the codecs in this recommended-codec list.

The way of handling messages with codecs that are not in the recommended-codec list or with no codec in the list depends on the network policy, i.e. some networks may allow the use of codecs that are not in the recommended-codec list, while others may reject such messages.

Recommendation on a recommended-codec list does not put any direct requirement on the codecs that have to be implemented in the network for transcoding purposes, nor does it mean that terminals shall support all the codecs in the list. Hence, conformance of a SIP/SDP offer to the list does not ensure successful codec negotiation.

Note 3: When the codecs to be supported across a UNI is restricted, due to network policy, a recommendation, as in note 2, is desirable. When such a recommendation cannot be provided, the recommended-codec list shall contain G.711 A/mu law [G.711].

Note 4: For voice communication, the recommended-codec list shall contain G.711 A or mu law. While any other codec may be used within the recommended-codec list, based on the network policy, it is recommended that the list contain AMR NB [EN 301 703], EVRC [TIA-127], G.729 [G.729], G.729A [G.729A], G.722.1 [G.722.1], G.726 [G.726], and MPEG-4 Audio [ISO/IEC 14496-3]. To enable the provision of voice service with a superior quality, it is highly

recommended that the list contain a wide-band codec such as AMR-WB [G.722.2], VMR-WB [TIA-1016], G.722 [G.722], G.729.1 [G.729.1]. To support hard of hearing, it is recommended that T.140 [T.140] is supported as a codec in the codec list. Where the interconnect is to be an existing PSTN/ISDN, it is recommended that T.140 [T.140] is adapted to be carried over G.711 A/mu law [G.711]. For video communication, the recommended-codec list is recommended to contain H.263 [H.263], H.264 [H.264], and MPEG-4 Visual [ISO/IEC 14496-2]. For data communication, the network is recommended to show its preferred data applications to the user.

Note 5: For individual sessions, a call signalling element, such as a CSC-FE, an application server or an IBC-FE, that has visibility of the end-to-end codec negotiation may determine the need and may initiate transcoding between the endpoints.

Note 6: Although transcoding should be avoided wherever possible, the network may support transcoding to increase the chance of session establishment (e.g. in configurations where the codecs supported by the endpoints belong to the recommended-list but no common codec can be found). However, a recommendation on a recommended-codec list does not imply that the network should support transcoding between one of the codecs in the list and any other codec nor between any combination of the codecs in the list.

### 8.2. Packetization size

When a packetization size is not selected by codec negotiation between terminals and/or network elements or not recommended by the network policy, a speech packetization sampling size of 10 ms should be used for G.711 coded speech; this is recommended as an optimum value balancing end-to-end delay with network utilisation. It is recognised that there may be network constraints that require that a higher value is recommended by the network policy; in such cases, a value of 20 ms is recommended. It is also recognized that there should be the network policy on an upper limit of packetization size that should not be exceeded, e.g. 60 ms.

Note: Where a packetization size is selected by codec negotiation between terminals and/or network elements this Recommendation places no requirements on the value to be selected.

## 9. Routing and Addressing

Table 1 describes URI formats that shall be supported on the UNI.

Other formats may be supported.

Table 1 URI formats

| | |
|---|---|
| SIP URI | sip:userinfo@hostport;uri-parameters (Note 1) |
| | Description: “userinfo”, “hostport” and “uri-parameters” are set based on section 25 of RFC3261. “userinfo” includes global E.164 number or local number |
| | Reference: [RFC 3261] [RFC 3966] |
| tel URI | tel:telephone-subscriber |
| | Description: telephone-subscriber is global E.164 number or local number |

| | |
|---|---|
| | Reference: [RFC 3966] |
| Note 1 | “hostport” includes either a domain name or IP address.<br>“hostport” may also include a port number. |

In the REGISTER method, the SIP URI in Request-URI shall not include “userinfo” including “@”, as specified in [RFC3261].

## 10. Service Level Signalling Profile

### 10.1. RFCs to be supported

Table 2: Notations of M/O/C in UNI

| Code | Code name | Meaning |
|---|---|---|
| M | Mandatory | The UNI shall comply with the listed RFC. For further information on the handling of element in the mandatory RFC's, see the relevant section below. |
| O | Optional | The UNI may comply with the listed RFC. |
| C | Conditional | The UNI shall comply with the listed RFC conditionally based on the context. For the context on the handling of element in the mandatory RFC's, see the relevant section below. |

**Table 3 RFCs to be Supported in UNI**

| Category | RFC | Title | EUF | SCF |
|---|---|---|---|---|
| Identity and Privacy | RFC 3323 | "A Privacy Mechanism for the Session Initiation Protocol (SIP)" | M (Note 1) | M |
| | RFC 3324 | Short Term Requirements for Network Asserted Identity | M (Note 1) | M |
| | RFC 3325 | "Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks" | M (Note 1) | M |
| URI | RFC 3966 | "The tel URI for Telephone Numbers" | M (Note 2) | M (Note 2) |
| | RFC 4715 | The Integrated Services Digital Network (ISDN) Subaddress Encoding Type for tel URI | O | O |
| | RFC 3824 | Using E.164 numbers with the Session Initiation Protocol (SIP) | C1 | C1 |
| | RFC 4458 | ”Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)” | C2 | C2 |
| | RFC 5031 | A Uniform Resource Name (URN) for Emergency and Other Well-Known Services | O | O |

| | | | | |
|---|---|---|---|---|
| SIP & Extension | RFC 3261 | "SIP: Session Initiation Protocol" | M | M |
| | RFC 3262 | "Reliability of provisional responses in Session Initiation Protocol (SIP)" | C3 | M |
| | RFC 3263 | “Session Initiation Protocol (SIP): Locating SIP Servers" | C4 | C4 |
| | RFC 3264 | "An Offer/Answer Model with Session Description Protocol (SDP)" | M | M |
| | RFC 3265 | "Session Initiation Protocol (SIP) Specific Event Notification" | C5 | C5 |
| | RFC 3310 | "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)" | C6 | C6 |
| | RFC 3311 | "The Session Initiation Protocol (SIP) UPDATE method" | M (Note 3) | M (Note 3) |
| | RFC 3312 | "Integration of resource management and Session Initiation Protocol (SIP)" | O | O |
| | RFC 3326 | "The Reason Header Field for the Session Initiation Protocol (SIP)" | O | O |
| | RFC 3327 | "Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts" | O | O |
| | RFC 3313 | "Private Session Initiation Protocol (SIP) Extensions for Media Authorization" | O | O |
| | RFC 3320 | "Signaling Compression (SigComp)" | O | O |
| | RFC 3515 | "The Session Initiation Protocol (SIP) REFER method" | C7 | C7 |
| | RFC 3581 | "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing" | C8 | C8 |
| | RFC 3891 | "The Session Initiation Protocol (SIP) "Replaces" Header" | C7 | C7 |
| | RFC 3892 | "The Session Initiation Protocol (SIP) Referred-By Mechanism" | C7 | C7 |
| | RFC 4244 | "An Extension to the Session Initiation Protocol for Request History Information" | C9 (Note 4) | C9 (Note 4) |
| | RFC 3959 | The Early Session Disposition Type for the Session Initiation Protocol (SIP) | O | O |
| | RFC 3960 | Early Media and Ringback Tone Generation in the Session Initiation Protocol | C10 | C10 |
| | RFC 3842 | "A Message Summary and Message Waiting Indication Event Package for the Session | C11 | C11 |

| | | | | |
|---|---|---|---|---|
| | | Initiation Protocol (SIP)" | | |
| | RFC 4028 | "Session Timers in the Session Initiation Protocol (SIP)" | M | M |
| | RFC 3725 | “Best Current Practices for Third Party Call Control (3pcc)in the Session Initiation Protocol (SIP)” | O | O |
| | RFC 4730 | “A Session Initiation Protocol (SIP) Event Package for Key Press Stimulus (KPML)” | O | O |
| | RFC 2617 | "HTTP Authentication: Basic and Digest Access Authentication" | O (Note 5) | O (Note 5) |
| | RFC 2976 | "The SIP INFO method" | O | O |
| | RFC 3911 | "The Session Initiation Protocol (SIP) "Join" Header" | O | O |
| | RFC 3840 | "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)" | O | O |
| | RFC 3841 | "Caller Preferences for the Session Initiation Protocol (SIP)" | O | O |
| | RFC 3608 | "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration" | O | O |
| | RFC 3680 | "A Session Initiation Protocol (SIP) Event Package for Registrations" | O | O |
| | RFC 3329 | "Security Mechanism Agreement for the Session Initiation Protocol (SIP)" | O | O |
| | RFC 3455 | "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)" | O | O |
| | RFC 3485 | "The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) static dictionary for Signaling Compression (SigComp)" | O | O |
| | RFC 3486 | "Compressing the Session Initiation Protocol (SIP)" | O | O |
| | RFC 3853 | S/MIME AES Requirement for SIP | O | O |
| | RFC 4320 | Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) non-INVITE Transaction | O (Note 6) | O (Note 6) |
| | RFC 4412 | Communications Resource Priority for the Session Initiation Protocol (SIP) | O | O |
| | RFC 4483 | A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages | O | O |

| | | | | |
|---|---|---|---|---|
| | RFC 4032 | "Update to the Session Initiation Protocol (SIP) Preconditions Framework" | O | O |
| | RFC 4235 | An INVITE Initiated Dialog Event Package for the Session Initiation Protocol (SIP) | O | O |
| | RFC 4168 | The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP) | O | O |
| | RFC 5079 | "Rejecting Anonymous Requests in the Session Initiation Protocol (SIP)" | O | O |
| | RFC 5049 | "Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP)" | O | O |
| Media Description | RFC 2046 | Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types | O | O |
| | RFC 3388 | "Grouping of Media Lines in Session Description Protocol" | O | O |
| | RFC 3420 | "Internet Media Type message/sipfrag" | O | O |
| | RFC 3524 | Mapping of Media Streams to Resource Reservation Flows | O | O |
| | RFC 3556 | "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth" | O | O |
| | RFC 4145 | TCP-Based Media Transport in the Session Description Protocol (SDP) | O | O |
| | RFC 4566 | "SDP: Session Description Protocol" | M (Note 7) | M (Note 7) |
| | RFC 4583 | Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams | O | O |
| Conference | RFC 4575 | "A Session Initiation Protocol (SIP) Event Package for Conference State" | C12 | C12 |
| | RFC 4579 | Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents | C13 | C13 |
| Instance Messaging | RFC 3428 | "Session Initiation Protocol (SIP) Extension for Instant Messaging" | C14 | C14 |
| | RFC 3860 | Common Profile for Instant Messaging (CPIM) | O | O |
| | RFC 3861 | "Address Resolution for Instant Messaging and Presence" | O | O |
| | RFC 3862 | Common Presence and Instant Messaging (CPIM): Message Format | O | O |

| | | | | |
|---|---|---|---|---|
| | RFC 3994 | Indication of Message Composition for Instant Messaging | O | O |
| Presence | RFC 3903 | "An Event State Publication Extension to the Session Initiation Protocol (SIP)" | C15 | C15 |
| | RFC 3856 | "A Presence Event Package for the Session Initiation Protocol (SIP)" | C15 | C15 |
| | RFC 3857 | "A Watcher Information Event Template Package for the Session Initiation Protocol (SIP)" | O | O |
| | RFC 3858 | An Extensible Markup Language (XML) Based Format for Watcher Information | O | O |
| | RFC 3859 | Common Profile for Presence (CPP) | O | O |
| | RFC 3863 | “Presence Information Data Format” | O | O |
| | RFC 4480 | RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF) | O | O |
| | RFC 4662 | "A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists" | O | O |

C1: [RFC 3824] is conditional mandatory when used for mandatory guidance for formatting SIP URI with ENUM.

C2: [RFC 4458] is conditional mandatory when retargeting is required.

C3: [RFC 3262] is conditional mandatory when reliability of provisional response is required.

C4: [RFC 3263] may not be required in well-managed networks with provisioned devices or if the outbound proxy’s address is received during the network attachment, but it is conditional mandatory for other cases.

C5: [RFC 3265] is conditional mandatory when event notification, such as message wait indication, is required.

C6: [RFC 3310] is conditional mandatory for mobile user equipment. However, it is optional for fixed-line terminal.

C7: [RFC 3515], [RFC 3891], and [RFC 3892] are conditional mandatory when referring requests is required.

C8: [RFC 3581] is conditional mandatory when it is used for NAT traversal.

C9: [RFC 4244] is conditional mandatory when call diversion is required and call diversion related information is transferred over the UNI.

C10: Section 3 of [RFC 3960] is conditional mandatory when used for mandatory guidance for providing and receiving announcements except when P-early media header is supported.

C11: [RFC 3842] is conditional mandatory when message indication, such as indication of the number of voice mails, is required.

C12: [RFC 4575] is conditional mandatory when conferencing is required.

C13: [RFC 4579] is conditional mandatory for conferencing to add clarity on how to support normative RFCs for conferencing.

C14: [RFC 3428] is conditional mandatory when instant messaging is required.

C15: [RFC 3903] and [RFC 3856] are conditional mandatory when presence is required.

Note 1: Supporting these [RFC 3323], [RFC 3324], and [RFC 3325] for enterprise networks is optional.

Note 2: Even if only SIP URI is supported, [RFC 3966] is mandatory for the [E.164]-based userinfo field in SIP URI.

Note 3: EUF and SCF shall support all mandatory provisions of [RFC 3311]. To update parameters before the initial INVITE is completed, UPDATE shall be used. To update parameters after the initial INVITE is completed, a re-INVITE or an UPDATE shall be used. The use of UPDATE is contingent upon the user indicating its support in the Allow header field.

If the intent is to restrict the user at the other end from accepting or rejecting a new offer, an UPDATE should be used.

If the intent is to allow for the user at the other end to be given a chance to accept or reject a new offer, a re-INVITE should be used.

If the other end does not support UPDATE, a re-INVITE shall be used.

Note 4: draft-levy-sip diversion is supported in some legacy SIP implementation instead of [RFC 4244].

Note 5: BASIC authentication scheme shall not be used.

Note 6: It is recommended that this [RFC 4320] is implemented to handle non INVITE transactions.

Note 7: If any specifications specified only in [RFC 2327] are used, e.g. m=data, [RFC 2327] shall be supported.

## 10.2. SIP Profiles

### 10.2.1. SIP profile based on RFC 3261

This sub-clause defines a SIP profile for the EUF and the SCF at the UNI interface. This sub-clause is structured to mirror IETF RFC 3261 and its section numbering. The sub-clauses are numbered such that the fourth digit (i.e. x of 10.2.1.x) tracks the section numbers of RFC 3261, and sub-clause titles track the section titles of RFC 3261.

This sub-clause defines the set of enhancements of and restrictions on a standard SIP implementation based on RFC 3261.

Unless otherwise stated in this Recommendation, the EUF and the SCF shall act in accordance with RFC 3261.

#### 10.2.1.1. Introduction

RFC 3261 section 1 is informational.

#### 10.2.1.2. Overview of SIP Functionality

RFC 3261 section 2 is informational.

#### 10.2.1.3. Terminology

RFC 3261 section 3 is informational.

#### 10.2.1.4. Overview of Operation

RFC 3261 section 4 is informational.

#### 10.2.1.5. Structure of the Protocol

The structure of the protocol can be found in RFC 3261 section 5, which is informational.

#### 10.2.1.6. Definitions

RFC 3261 section 6 defines the terms that have special significance for SIP. Additional definitions can be found in clause 3 of this Recommendation.

The reader should note that the term “client” in this sub-clause covers both UACs and proxies.

#### 10.2.1.7. SIP Messages

The EUF and the SCF shall set the SIP profile in accordance with RFC 3261 section 7 except as noted in this sub-clause.

##### 10.2.1.7.1. Requests

The EUF and the SCF shall set the SIP profile in accordance with RFC 3261 section 7.1 except as noted in this sub-clause.

The EUF and the SCF shall support the INVITE, ACK, CANCEL, and BYE methods. The SCF shall support UPDATE and PRACK, and the EUF shall support UPDATE but shall support PRACK in case reliability of provisional response is required. The EUF shall support sending the REGISTER method, and the SCF shall support receiving the REGISTER method. The OPTIONS method may be supported.

The Request-URI shall be a SIP URI, as defined in RFC 3261, or a tel URI, as defined in [RFC 3966]. The SIPS URI format may be supported.

The Request-URI in an initial INVITE for a basic telephone call[1] shall identify the called party using a tel URI or by using the telephone-subscriber syntax (i.e. the dialled phone number) in a SIP URI. When the Request-URI is a SIP URI, the host part of the Request-URI shall identify the SCF or the entity to which the message is addressed.

The Request-URI for other requests associated with a basic telephone call shall identify the targeted host using the IP address or FQDN, as given by the Contact header.

The host part of the Request-URI typically agrees with one of the host names of the receiving server. However, if the Request-URI of a received INVITE does not so agree, the server should proxy the request to another entity based on saved translation information or preprovisioned policy information.

Note: The Request-URI in a REGISTER shall not include “userinfo” including “@” as specified in RFC 3261.

##### 10.2.1.7.2. Responses

The EUF and the SCF shall set the SIP profile in accordance with RFC 3261 section 7.2.

##### 10.2.1.7.3. Header Fields

The EUF and the SCF shall set the SIP profile in accordance with RFC 3261 section 7.3.

##### 10.2.1.7.4. Bodies

The EUF and the SCF shall set the SIP profile in accordance with RFC 3261 section 7.4 except as noted in this sub-clause.

---

[1] This includes INVITEs generated as a result of forwarding.

#### 10.2.1.7.4.1. Message Body Types

The EUF and the SCF shall set the SIP profile in accordance with RFC 3261 section 7.4.1 except as noted in this sub-clause.

The EUF and the SCF shall set the SIP profile to support the message body type “application/sdp”; other message body types may be supported.

The message body type "application/sdp" shall be supported with the INVITE and UPDATE methods as well as any non-failure response to these methods. And it should be supported with the PRACK method as well as any non-failure response to the method in order to allow interworking with H.323 network and support of services operating third party call control.

The message body type "application/sdp" may be supported with failure responses, such as 488 (Not Acceptable Here), to the above methods.

#### 10.2.1.7.4.2. Message Body Length

The EUF and the SCF shall set the SIP profile in accordance with RFC 3261 section 7.4.2.

#### 10.2.1.7.5. Framing SIP Messages

The EUF and the SCF shall set the SIP profile in accordance with RFC 3261 section 7.5.

### 10.2.1.8. General User Agent Behaviour

This sub-clause and its sub-clauses apply only if the EUF acts as a UA, i.e. UAC or a UAS, and only if the SCF acts as a UA, i.e. B2BUA or redirect server.

The EUF and the SCF shall behave in accordance with RFC 3261 section 8 except as noted in this sub-clause.

Support for multiple simultaneous media streams for a single call is optional.

Note that the behaviour defined in this sub-clause applies only to requests and responses outside a dialog. The behaviour within a dialog is defined in 10.2.1.12.

#### 10.2.1.8.1. UAC Behaviour

The EUF and the SCF shall behave in accordance with RFC 3261 section 8.1 except as noted in this sub-clause.

#### 10.2.1.8.1.1. Generating the Request

The EUF and the SCF shall behave in accordance with RFC 3261 section 8.1.1 except as noted in this sub-clause.

Request-URI in the request contains the address of the called party. This will normally be a telephone number, but it may also be a general SIP URI. The From and To fields in the request might contain random strings that protect the privacy of the session originator.

Refer to sub-clause 10.2.1.20 for further details of various header field values to be used.

#### 10.2.1.8.1.2. Sending the Request

The EUF and the SCF shall behave in accordance with RFC 3261 section 8.1.2.

#### 10.2.1.8.1.3. Processing Responses

The EUF and the SCF shall behave in accordance with RFC 3261 section 8.1.3 except as noted in this sub-clause.

If SIP authorization is required, the EUF and the SCF shall support the SIP authorization procedures with 401 (Unauthorized) in accordance with RFC 3261 section 8.1.3.5.

Support for the SIP authorization procedures with 407 (Proxy Authentication Required) is optional. If the support is provided, it shall be as specified in RFC 3261 section 8.1.3.5.

Support for the SIP retry procedures, which is used when 420 (Bad Extension) is received, is optional. If the support is provided, it shall be as specified in RFC 3261 section 8.1.3.5.

#### 10.2.1.8.2. UAS Behaviour

The EUF and the SCF shall behave in accordance with RFC 3261 section 8.2.

#### 10.2.1.8.3. Redirect Servers

The EUF and the SCF shall behave in accordance with RFC 3261 section 8.3 except as noted in this sub-clause.

The SCF is not required to provide the redirect server function. However, it may provide the redirect server function and invoke redirections for a limited number of INVITE requests. The rationale for limiting the number of redirections is to control SIP signalling traffic across the UNI and processing complexity associated with redirections. The Max-Forwards header (see Sub-clause 10.2.1.20), which is mandatory in all SIP requests, serves to limit the number of hops a request can make on the way to its destination. If the redirection function is supported, then the SCF shall be in accordance with RFC 3261 section 8.3.

3xx response codes may be supported at the UNI, based on a network policy or a subscription option to support redirections that may take place in the network or in a downstream network receiving the INVITE message.

### 10.2.1.9. Cancelling a Request

In this sub-clause and in its sub-clauses, the handling that is specific to a Proxy applies only if the SCF acts as a SIP proxy, the handling that is specific to a UA applies only if the EUF acts as a UA, i.e. UAC or a UAS, and only if the SCF acts as a UA, i.e. B2BUA or redirect server, and the handling that is specific to a registrar applies only if the SCF acts as a registrar.

The EUF and the SCF shall behave in accordance with RFC 3261 section 9.

### 10.2.1.10. Registrations

In this sub-clause and in its sub-clauses, the handling that is specific to a Proxy applies only if the SCF acts as a SIP proxy, the handling that is specific to a UA applies only if the EUF acts as a UA, i.e. UAC or a UAS, and only if the SCF acts as a UA, i.e. B2BUA or redirect server, and the handling that is specific to a registrar applies only if the SCF acts as a registrar.

The EUF and the SCF shall behave in accordance with RFC 3261 section 10.

### 10.2.1.11. Querying for Capabilities

In this sub-clause and in its sub-clauses, the handling that is specific to a Proxy applies only if the SCF acts as a SIP proxy, the handling that is specific to a UA applies only if the EUF acts as a UA, i.e. UAC or a UAS, and if the SCF acts as a UA, i.e. B2BUA or redirect server, and the handling that is specific to a registrar applies only if the SCF acts as a registrar.

Support for querying for capabilities is optional. If the support is provided, it shall be as specified in RFC 3261 section 11.

### 10.2.1.12. Dialogs

This sub-clause and its sub-clauses apply only if the EUF acts as a UA, i.e. UAC or a UAS, and only if the SCF acts as a UA, i.e. B2BUA or redirect server.

The EUF and the SCF shall behave in accordance with RFC 3261 section 12 except as noted in this sub-clause.

#### 10.2.1.12.1. Creation of a Dialog

Support for SIPS URIs is optional. If the support is provided, it shall be as specified in RFC 3261 section 12.1.

#### 10.2.1.12.2. Requests within a Dialog

Support for SIPS URIs is optional. If the support is provided, it shall be as specified in RFC 3261 section 12.2.

#### 10.2.1.12.3. Termination of a Dialog

The EUF and the SCF shall behave in accordance with RFC 3261 section 12.3.

### 10.2.1.13. Initiating a Session

This sub-clause and its sub-clauses apply only if the EUF acts as a UA, i.e. UAC or a UAS, and only if the SCF acts as a UA, i.e. B2BUA or redirect server.

The EUF and the SCF shall behave in accordance with RFC 3261 section 13 except as noted in this sub-clause.

The EUF on the sending side should include a message body type “application/sdp” with the initial INVITE whenever possible.

The support of initial INVITE without SDP offer is recommended to allow interworking with H.323 network and support of services operating third party call control.

To support codec selection:

– When the initial INVITE includes an SDP offer, an SDP answer may be included either in the provisional reliable non-failure response to the INVITE (e.g. 183-Session-Progress sent reliably) or in the final non-failure response to the INVITE (i.e. 2xx), and, if not included in the provisional reliable non-failure response, shall be included in the final non-failure response. If the final non-failure response includes an SDP answer, the same value of SDP may be included in the provisional unreliable non-failure response to the INVITE.

– When the initial INVITE does not include an SDP offer, the initial SDP offer shall be included in the first provisional reliable non-failure response to the INVITE, that is in the first 18x response sent reliably (e.g. 180-Ringing sent reliably) if any, or in the final non-failure response to the INVITE (i.e. 2xx) if not. If the initial SDP offer is included in a reliable provisional response, the SDP answer shall be included in the PRACK message acknowledging this response. If the initial SDP offer is included in the final non-failure response to the INVITE (i.e. 2xx), the SDP answer shall be included in the ACK message acknowledging this response.

### 10.2.1.14. Modifying an Existing Session

This sub-clause and its sub-clauses apply only if the EUF acts as a UA, i.e. UAC or a UAS, and only if the SCF acts as a UA, i.e. B2BUA or redirect server.

The EUF and the SCF shall behave in accordance with RFC 3261 section 14 except as noted in this sub-clause.

When constructing an SDP answer to a new received SDP offer contained in a re-INVITE or UPDATE method, the SCF that controls the transfer plane and the EUF should not modify the listening IP address and port number negotiated during the initial SDP negotiation procedure for a given media stream.

### 10.2.1.15. Terminating a Session

This sub-clause and its sub-clauses apply only if the EUF acts as a UA, i.e. UAC or a UAS, and only if the SCF acts as a UA, i.e. B2BUA or redirect server.

The EUF and the SCF shall behave in accordance with RFC 3261 section 15.

#### 10.2.1.16. Proxy Behaviour

This sub-clause and its sub-clauses apply only if the SCF acts as a SIP proxy.

The SCF shall behave in accordance with RFC 3261 section 16 except as noted in this sub-clause.

Support for multiple simultaneous media streams for a single call is optional.

#### 10.2.1.17. Transactions

In this sub-clause and in its sub-clauses, the handling that is specific to a Proxy applies only if the SCF acts as a SIP proxy, the handling that is specific to a UA applies only if the EUF acts as a UA, i.e. UAC or a UAS, and only if the SCF acts as a UA, i.e. B2BUA or redirect server, and the handling that is specific to a registrar applies only if the SCF acts as a registrar.

The EUF and the SCF shall behave in accordance with RFC 3261 section 17 except as noted in this sub-clause.

The EUF and the SCF may return error code 486 (Busy Here) to an INVITE request for a user if a dialog already exists for that user and the new INVITE is not part of that dialog.

#### 10.2.1.18. Transport

The EUF and the SCF shall behave in accordance with RFC 3261 section 18. However, clause 12 of this Recommendation takes precedence over RFC 3261 section 18 in case of any conflicts.

#### 10.2.1.19. Common Message Components

The EUF and the SCF shall set the SIP profile in accordance with RFC 3261 section 19 except as noted in this sub-clause.

Support for the SIPS URI is optional. If the support is provided, it shall be as specified in RFC 3261 section 19.1.1.

#### 10.2.1.20. Header Fields

The EUF and the SCF shall set the SIP profile in accordance with RFC 3261 section 20 except as noted in this sub-clause.

Below, the SIP headers defined in RFC 3261 are listed, and the requirements for supporting them in the EUF and the SCF are identified.

##### 10.2.1.20.1. Accept

Support for the Accept header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.1.

##### 10.2.1.20.2. Accept-Encoding

Support for the Accept-Encoding header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.2 except as noted below.

The Accept-Encoding header may be used by the EUF and the SCF. The "identity" encoding value shall be supported; other encodings may be supported.

##### 10.2.1.20.3. Accept-Language

Support for the Accept-Language header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.3.

##### 10.2.1.20.4. Alert-Info

Support for the Alert-Info header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.4.

Note that there are security risks associated with acting on the Alert-Info header, as described in RFC 3261 section 20.4.

#### 10.2.1.20.5. Allow

The Allow header shall be supported as specified in RFC 3261 section 20.5 except as noted below.

The Allow header shall be present in the initial INVITE and the 2xx response to the initial INVITE.

The header value shall list all supported methods, e.g. INVITE, ACK, CANCEL, BYE, UPDATE, and PRACK.

However, the EUF and the SCF need to prepare to receive messages without the Allow header field. The EUF and the SCF should continue the call control even if the Allow header is not present in the initial INVITE and the 2xx response to the initial INVITE.

#### 10.2.1.20.6. Authentication-Info

Support for the Authentication-Info header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.6.

#### 10.2.1.20.7. Authorization

If SIP authorization is required, the EUF shall support sending the Authorization header and the SCF shall support receiving the Authorization header in accordance with RFC 3261 section 20.7. Support for both sending and receiving the Authorization header in the EUF and support for sending the Authorization header in the SCF is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.7.

#### 10.2.1.20.8. Call-ID

The Call-ID header shall be supported as specified in RFC 3261 section 20.8 except as noted below.

The Call-ID value shall be globally unique as described in RFC 3261 section 8.1.1.4, and it should use a suitably long random value (the value used as the 'tag' for the From header of the request might even be reused) instead of appending the IP address or hostname to the Call-ID as described in [RFC 3323] section 4.1 for protecting privacy. When privacy is requested by the session originator, the EUF of the session originator should use a privacy protected Call-ID.

#### 10.2.1.20.9. Call-Info

Support for the Call-Info header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.9.

Note that there are security risks associated with acting on the Call-Info header, as described in RFC 3261 section 20.9.

#### 10.2.1.20.10. Contact

The Contact header shall be supported as specified in RFC 3261 section 20.10 except as noted below.

The EUF and the SCF shall set the SIP profile to populate the Contact header in an INVITE request, a reliable provisional response and in a 2xx response to an INVITE request, with a SIP URI. Support for any other type of URI is optional.

When the user is requesting privacy, the Contact header should not contain any domain names; the IP address form should be used instead. It should be noted that, in systems with multiple network interfaces, use of the (single) IP address form can reduce the overall system reliability. If multiple interfaces exist and reliability is a concern, then refraining from use of the IP address form is considered to be a reasonable trade-off.

The EUF and the SCF shall set the SIP profile to populate the Contact header in a 3xx response to an INVITE request with a valid SIP URI or tel URI. If the new destination is a telephone number, it shall contain a SIP URI or tel URI with the number of the new destination, as described is sub-clause 10.2.1.7.1 of this Recommendation. Support for any other type of URI is optional.

#### 10.2.1.20.11. Content-Disposition

Support for the Content-Disposition header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.11 except as noted below.

The Content-Disposition header may be used by the EUF and the SCF. The value "session" shall be supported; other values may be supported.

If early media is provided by the application server model defined in RFC 3959, the Content-Disposition header shall include the “early-session” value as specified in RFC 3959.

Note that the default value for message body type "application/sdp" is "session", whereas the default value for all other message body types (e.g. "message/sipfrag") is "render". If the default value is not desired, then the Content-Disposition header shall be included.

#### 10.2.1.20.12. Content-Encoding

Support for the Content-Encoding header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.12 except as noted below.

The Content-Encoding header may be used by the EUF and the SCF. The "identity" encoding shall be supported; other encodings may be supported.

#### 10.2.1.20.13. Content-Language

Support for the Content-Language header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.13.

#### 10.2.1.20.14. Content-Length

The Content-Length header shall be supported as specified in RFC 3261 section 20.14.

#### 10.2.1.20.15. Content-Type

The Content-Type header shall be supported as specified in RFC 3261 section 20.15 except as noted below.

The value “application/sdp” shall be supported; other values may be supported.

If early media is provided by the application server model defined in RFC 3959, the content type “multipart/mixed” shall be supported as specified in RFC 2046 to specify different session types (e.g. normal session and early session). Each content type encloses its specification by using the “boundary” tag in this header.

#### 10.2.1.20.16. CSeq

The CSeq header shall be supported as specified in RFC 3261 section 20.16.

#### 10.2.1.20.17. Date

Support for the Date header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.17.

#### 10.2.1.20.18. Error-Info

Support for the Error-Info header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.18.

Note that there are security risks associated with acting on the Error-Info header as described in RFC 3261 section 20.18.

#### 10.2.1.20.19. Expires

Support for the Expires header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.19.

#### 10.2.1.20.20. From

The From header shall be supported as specified in RFC 3261 section 20.20 except as noted below.

In support of user privacy, the SCF restricts the allowable contents of the From header.

When the session originator requests privacy, the EUF should generate a From header according to the following rules:

- The display-name may be “Anonymous”.
- The addr-spec shall contain the identifier “anonymous” for userinfo.
- The addr-spec shall contain the non-identifying hostname “anonymous.invalid”.

#### 10.2.1.20.21. In-Reply-To

Support for the In-Reply-To header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.21.

#### 10.2.1.20.22. Max-Forwards

Support for receiving the Max-Forwards header in the EUF is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.22. The EUF shall support sending the Max-Forwards header in accordance with RFC 3261 section 20.22.

The SCF shall support the Max-Forwards header as specified in RFC 3261 section 20.22 except as noted below.

When a B2BUA within the SCF forwards a request, it shall use a Max-Forwards value equal to the incoming Max-Forwards value minus one.

#### 10.2.1.20.23. Min-Expires

The EUF shall support receiving the Min-Expires header and the SCF shall support sending the Min-Expires header in accordance with RFC 3261 section 20.23. Support for the Min-Expires header in the direction from the EUF to the SCF is not applicable.

#### 10.2.1.20.24. MIME-Version

Support for the MIME-Version header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.24 except as noted below.

The version "1.0" value shall be supported; other values may be supported.

#### 10.2.1.20.25. Organization

Support for the Organization header is optional. If the support is provided, it shall be as specified in RFC3261 section 20.25.

#### 10.2.1.20.26. Priority

Support for the Priority header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.26.

Note that there are security ramifications for entities that act on this header.

#### 10.2.1.20.27. Proxy-Authenticate

Support for receiving the Proxy-Authenticate header in the EUF and support for sending the Proxy-Authenticate header in the SCF is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.27. Support for the Proxy-Authenticate header in the direction from the EUF to the SCF is not applicable.

#### 10.2.1.20.28. Proxy-Authorization

Support for sending the Proxy-Authorization header in the EUF and support for receiving the Proxy-Authorization header in the SCF is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.28. Support for the Proxy-Authorization header in the direction from the SCF to the EUF is not applicable.

#### 10.2.1.20.29. Proxy-Require

The SCF shall support receiving the Proxy-Require header. Support for both sending and receiving the Proxy-Require header in the EUF and support for sending the Proxy-Require header in the SCF is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.29 except as noted below.

The option tag "privacy" shall be supported in accordance with [RFC 3323]; other option tags may be supported.

#### 10.2.1.20.30. Record-Route

The Record-Route header shall be supported as specified in RFC 3261 section 20.30.

#### 10.2.1.20.31. Reply-To

Support for the Reply-To header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.31.

#### 10.2.1.20.32. Require

The Require header shall be supported as specified in RFC 3261 section 20.32 except as noted below.

The option tag "timer" shall be supported by the EUF and the SCF in accordance with [RFC 4028]. The option tag "100rel" shall be supported by the EUF if reliability of provisional response is required and shall be supported by the SCF in accordance with [RFC 3262]. Other option tags may be supported.

If early media is provided by the application server model defined in RFC 3959 and UAC expects the UAS to support the process of the early media request, the Require header shall include the "early-session" value as specified in RFC 3959.

#### 10.2.1.20.33. Retry-After

Support for the Retry-After header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.33 except as noted below.

After submitting REGISTER request, an EUF may receive an error response with a Retry-After header. In such a situation, resending the request after the time interval specified in the Retry-After header is recommended.

#### 10.2.1.20.34. Route

The EUF shall support sending the Route header and the SCF shall support receiving the Route header in accordance with RFC 3261 section 20.34. Support for the Route header in the direction from the SCF to the EUF is not applicable.

#### 10.2.1.20.35. Server

Support for the Server header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.35.

#### 10.2.1.20.36. Subject

Support for the Subject header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.36.

#### 10.2.1.20.37. Supported

The Supported header shall be supported as specified in RFC 3261 section 20.37 except as noted below.

The option tag "timer" shall be supported in accordance with [RFC 4028]. The option tag "100rel" shall be supported by the EUF if reliability of provisional response is required and shall be supported by the SCF in accordance with [RFC 3262]. Other option tags may be supported.

If early media is provided by the application server model defined in RFC 3959, the Supported header shall include the "early-session" value as specified in RFC 3959.

#### 10.2.1.20.38. Timestamp

Support for the Timestamp header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.38 except as noted below.

The EUF and the SCF may send the Timestamp header in requests; if received, this header shall be processed as described in RFC 3261 section 20.38.

#### 10.2.1.20.39. To

The To header shall be supported as specified in RFC 3261 section 20.39 except as noted below.

In support of user privacy, the EUF and the SCF may restrict the allowable content of the To header. Typically, the To header indicates the dialled digits in a SIP URI or tel URI. This information is of end-to-end significance and might reveal information about the caller's location, e.g. enterprise, local, long-distance, or international.

When the call originator requests privacy, the EUF and the SCF may generate a To header according to the following rules:

- The display-name shall be absent.
- If a global telephone number is used, then the userinfo part of the addr-spec shall contain a full E.164 number, including the country code.
- The host part of the addr-spec shall contain the non-identifying hostname "anonymous.invalid".

If anonymity is not requested by the call originator and the user dialled a telephone number, then the To header should contain a SIP URI or tel URI with the dialled digits.

#### 10.2.1.20.40. Unsupported

The Unsupported header shall be supported as specified in RFC3261 section 20.40.

#### 10.2.1.20.41. User-Agent

Support for the User-Agent header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.41.

#### 10.2.1.20.42. Via

The Via header shall be supported as specified in RFC 3261 section 20.42.

#### 10.2.1.20.43. Warning

Support for the Warning header is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.43.

#### 10.2.1.20.44. WWW-Authenticate

If SIP authorization is required, the EUF shall support receiving the WWW-Authenticate header and the SCF shall support sending the WWW-Authenticate header in accordance with RFC 3261 section 20.44

Support for sending the WWW-Authenticate header in the EUF and support for receiving the WWW-Authenticate header in the SCF is optional. If the support is provided, it shall be as specified in RFC 3261 section 20.44.

### 10.2.1.21. Response Codes

The EUF and the SCF shall set the SIP profile in accordance with RFC 3261 section 21.

#### 10.2.1.22. Usage of HTTP Authentication

Support for HTTP Authentication is optional. If used, HTTP Authentication shall be as specified in RFC 3261 section 22.

#### 10.2.1.23. S/MIME

Support for S/MIME is optional. If used, S/MIME shall be as specified in RFC 3261 section 23.

#### 10.2.1.24. Examples

RFC 3261 section 24 is informational.

#### 10.2.1.25. Augmented BNF for the SIP Protocol

The EUF and the SCF shall set the SIP profile in accordance with RFC 3261 section 25.

### 10.2.2. SIP profile for extensions to RFC 3261

This sub-clause defines the extended methods, headers, and response codes that are defined in the mandatorily supported RFCs except for RFC 3261, as listed in section 10.1. If the support for the RFC is optional, then the support for the methods, headers, and response codes defined in those RFCs is accordingly optional, and this sub-clause does not describe those methods, headers, and response codes individually.

#### 10.2.2.1. Extended methods

The SCF shall support UPDATE and PRACK, and the EUF shall support UPDATE but shall support PRACK in case reliability of provisional response is required.

##### 10.2.2.1.1. UPDATE

The EUF and the SCF shall support the UPDATE method as specified in [RFC3311].

Before the initial INVITE is completed, UPDATE shall be used to update session parameters.

After initial INVITE is completed, re-INVITE or UPDATE may be used. It is recommended that the re-INVITE method is deployed for updating the session parameters. In particular, while communicating, addition of different media or removal of any media from earlier established media session should be performed by using re-INVITE instead of UPDATE with new media descriptions which contain modified SDP profiles according to the SDP offer/answer procedure.

##### 10.2.2.1.2. PRACK

The SCF shall support the PRACK method in accordance with [RFC 3262]. If reliability of provisional response is required, the EUF shall support the PRACK method as specified in [RFC 3262]. If the EUF on the sending side sends an initial request that contains ‘Require’ header with option tag “100rel” in order to guarantee reliability of provisional response, the EUF on the receiving side shall include “Require” header with “100rel” option tag into provisional response. If the SIP non-100 provisional response contains a “Require” header with option tag “100rel”, the EUF on the sending side shall send back a PRACK request in accordance with [RFC 3262]. If the EUF on the sending side sends an initial request that contains “Supported” header with option tag “100rel”, the EUF on the receiving side may send any non-100 provisional response to INVITE reliably. When non-100 provisional response contains “early-session” or “precondition” option tag in the “Require” header, it shall include the “100rel” tag in the Supported header field.

#### 10.2.2.2. Extended headers

##### 10.2.2.2.1. Min-SE

The Min-SE header field indicates the minimum value for the session interval in units of delta-seconds.

Support for sending the Min-SE header in the EUF is optional. If the support is provided, it shall be as specified in [RFC 4028]. The EUF shall support receiving the Min-SE header in accordance with [RFC 4028].

The SCF shall support the Min-SE header in accordance with [RFC 4028].

##### 10.2.2.2.2. P-Asserted-Identity

The P-Asserted-Identity header field is used among trusted SIP entities to carry the identity of the user sending a SIP message as it was verified by authentication.

The EUF shall support receiving the P-Asserted-Identity header and the SCF shall support sending the P-Asserted-Identity header in accordance with [RFC 3325]. Support for the P-Asserted-Identity header in the direction from the EUF to the SCF is not applicable.

##### 10.2.2.2.3. P-Preferred-Identity

The P-Preferred-Identity header field is used from a user agent to a trusted proxy to carry the identity the user sending the SIP message wishes to be used for P-Asserted-Header field value that the trusted element will insert.

Support for sending the P-Preferred-Identity header in the EUF is optional. If the support is provided, it shall be as specified in [RFC 3325]. The SCF shall support receiving the P-Preferred-Identity header in accordance with [RFC 3325]. Support for the P-Preferred-Identity header in the direction from the SCF to the EUF is not applicable.

##### 10.2.2.2.4. Privacy

The Privacy header allows a user agent to request a certain degree of privacy for a message.

The EUF shall support receiving the Privacy header and the SCF shall support both sending and receiving the Privacy header. Support for sending the Privacy header in the EUF is optional.

If the support is provided, it shall be as specified in [RFC 3323] except as noted below.

The application of the privacy option "id" shall be supported. Other privacy options may be supported based on a network policy or a subscription option.

##### 10.2.2.2.5. RAck

The RAck header is sent in a PRACK request to support reliability of provisional responses.

The RAck header shall be supported by the EUF if reliability of provisional response is required as specified in [RFC 3262] and shall be supported by the SCF in accordance with [RFC 3262].

##### 10.2.2.2.6. RSeq

The RSeq header is used in provisional responses in order to transmit them reliably.

The RSeq header shall be supported by the EUF if reliability of provisional response is required as specified in [RFC 3262] and shall be supported by the SCF in accordance with [RFC 3262].

##### 10.2.2.2.7. Session-Expires

The Session-Expires header field conveys the session interval for a SIP session.

The Session-Expires header shall be supported as specified in [RFC 4028].

#### 10.2.2.3. Extended response codes

##### 10.2.2.3.1. 422 (Session Interval Too Small)

Support for sending the 422 (Session Interval Too Small) in the EUF is optional. If the support is provided, it shall be as specified in [RFC 4028]. The EUF shall support receiving the 422 (Session Interval Too Small) in accordance with [RFC 4028].

The SCF shall support the 422 (Session Interval Too Small) in accordance with [RFC 4028].

### 10.2.3. Summary of SIP methods and headers

Support for the following SIP methods and headers is mandatory, optional, or Not Applicable as specified in Tables 4, 5, 6, and 7. Supporting sending or receiving given SIP methods or headers means that the methods or headers shall reliably across the UNI and does not mean that the header shall always be present in the relevant SIP messages over the UNI.

Note: For information about supporting the responses, see RFC 3261.

Table 4: RFC 3261 methods

| Method | EUF->SCF | | SCF->EUF | | Reference |
|---|---|---|---|---|---|
| | EUF Send | SCF Recv | SCF Send | EUF Recv | |
| ACK | M | M | M | M | See Sub-clause 10.2.1.7.1~~10.2.1.7.1~~10.2.1.7.1 |
| BYE | M | M | M | M | See Sub-clause 10.2.1.7.1~~10.2.1.7.1~~10.2.1.7.1 |
| CANCEL | M | M | M | M | See Sub-clause 10.2.1.7.1~~10.2.1.7.1~~10.2.1.7.1 |
| INVITE | M | M | M | M | See Sub-clause 10.2.1.7.1~~10.2.1.7.1~~10.2.1.7.1 |
| OPTIONS | O | O | O | O | See Sub-clause 10.2.1.7.1~~10.2.1.7.1~~10.2.1.7.1 |
| REGISTER | M | M | N/A | N/A | See Sub-clause 10.2.1.7.1~~10.2.1.7.1~~10.2.1.7.1 |

Table 5: Extended methods

| Method | EUF->SCF | | SCF->EUF | | Reference | RFC |
|---|---|---|---|---|---|---|
| | EUF Send | SCF Recv | SCF Send | EUF Recv | | |
| PRACK | C | M | M | C | See Sub-clause 10.2.1.7.1~~10.2.1.7.1~~10.2.1.7.1 | RFC 3262 |
| UPDATE | M | M | M | M | See Sub-clause 10.2.1.7.1~~10.2.1.7.1~~10.2.1.7.1 | RFC 3311 |

C: It's conditional mandatory when reliability of provisional response is required.

**Table 6: RFC3261 headers**

| Header | EUF->SCF | | SCF->EUF | | Reference |
|---|---|---|---|---|---|
| | EUF Send | SCF Recv | SCF Send | EUF Recv | |
| Accept | O | O | O | O | See Sub-clause 10.2.1.20.1 |
| Accept-Encoding | O | O | O | O | See Sub-clause 10.2.1.20.2 |
| Accept-Language | O | O | O | O | See Sub-clause 10.2.1.20.3 |
| Alert-Info | O | O | O | O | See Sub-clause 10.2.1.20.4 |
| Allow | M | M | M | M | See Sub-clause 10.2.1.20.5 |
| Authentication-Info | O | O | O | O | See Sub-clause 10.2.1.20.6 |
| Authorization | C | C | O | O | See Sub-clause 10.2.1.20.7 |
| Call-ID | M | M | M | M | See Sub-clause 10.2.1.20.8 |
| Call-Info | O | O | O | O | See Sub-clause 10.2.1.20.9 |
| Contact | M | M | M | M | See Sub-clause 10.2.1.20.10 |
| Content-Disposition | O | O | O | O | See Sub-clause 10.2.1.20.11 |
| Content-Encoding | O | O | O | O | See Sub-clause 10.2.1.20.12 |
| Content-Language | O | O | O | O | See Sub-clause 10.2.1.20.13 |
| Content-Length | M | M | M | M | See Sub-clause 10.2.1.20.14 |
| Content-Type | M | M | M | M | See Sub-clause 10.2.1.20.15 |
| CSeq | M | M | M | M | See Sub-clause 10.2.1.20.16 |
| Date | O | O | O | O | See Sub-clause 10.2.1.20.17 |
| Error-Info | O | O | O | O | See Sub-clause 10.2.1.20.18 |
| Expires | O | O | O | O | See Sub-clause 10.2.1.20.19 |
| From | M | M | M | M | See Sub-clause 10.2.1.20.20 |
| In-Reply-To | O | O | O | O | See Sub-clause 10.2.1.20.21 |
| Max-Forwards | M | M | M | O | See Sub-clause 10.2.1.20.22 |
| Min-Expires | N/A | N/A | M | M | See Sub-clause 10.2.1.20.23 |
| MIME-Version | O | O | O | O | See Sub-clause 10.2.1.20.24 |
| Organization | O | O | O | O | See Sub-clause 10.2.1.20.25 |
| Priority | O | O | O | O | See Sub-clause 10.2.1.20.26 |
| Proxy-Authenticate | N/A | N/A | O | O | See Sub-clause 10.2.1.20.27 |
| Proxy-Authorization | O | O | N/A | N/A | See Sub-clause 10.2.1.20.28 |
| Proxy-Require | O | M | O | O | See Sub-clause 10.2.1.20.29 |
| Record-Route | M | M | M | M | See Sub-clause 10.2.1.20.30 |
| Reply-To | O | O | O | O | See Sub-clause 10.2.1.20.31 |
| Require | M | M | M | M | See Sub-clause 10.2.1.20.32 |
| Retry-After | O | O | O | O | See Sub-clause 10.2.1.20.33 |
| Route | M | M | N/A | N/A | See Sub-clause 10.2.1.20.34 |
| Server | O | O | O | O | See Sub-clause 10.2.1.20.35 |
| Subject | O | O | O | O | See Sub-clause 10.2.1.20.36 |
| Supported | M | M | M | M | See Sub-clause 10.2.1.20.37 |
| Timestamp | O | O | O | O | See Sub-clause 10.2.1.20.38 |
| To | M | M | M | M | See Sub-clause 10.2.1.20.39 |
| Unsupported | M | M | M | M | See Sub-clause 10.2.1.20.40 |
| User-Agent | O | O | O | O | See Sub-clause 10.2.1.20.41 |
| Via | M | M | M | M | See Sub-clause 10.2.1.20.42 |
| Warning | O | O | O | O | See Sub-clause 10.2.1.20.43 |
| WWW-Authenticate | O | O | C | C | See Sub-clause 10.2.1.20.44 |

C: It’s conditional mandatory when SIP authorization is required.

**Table 7: Extended headers**

| Header | EUF->SCF | | SCF->EUF | | Reference | RFC |
|---|---|---|---|---|---|---|
| | EUF Send | SCF Recv | SCF Send | EUF Recv | | |
| Min-SE | O | M | M | M | See Sub-clause 10.2.2.2.1 | RFC 4028 |
| P-Asserted-Identity | N/A | N/A | M | M | See Sub-clause 10.2.2.2.2 | RFC 3325 |
| P-Preferred-Identity | O | M | N/A | N/A | See Sub-clause 10.2.2.2.3 | RFC 3325 |
| Privacy | O | M | M | M | See Sub-clause 10.2.2.2.4 | RFC 3323 |
| RAck | C | M | M | C | See Sub-clause 10.2.2.2.5 | RFC 3262 |
| RSeq | C | M | M | C | See Sub-clause 10.2.2.2.6 | RFC 3262 |
| Session-Expires | M | M | M | M | See Sub-clause 10.2.2.2.7 | RFC 4028 |

C: It's conditional mandatory when reliability of provisional response is required.

In the above Tables, M, O, C, and N/A have the following meanings:

Table 8: Notations of the Codes in Tables 4, 5, 6, and 7

| Code | Code name | EUF->SCF | | SCF->EUF | |
|---|---|---|---|---|---|
| | | EUF Send | SCF Recv | SCF Send | EUF Recv |
| M | Mandatory | The capability shall be supported.<br><br>The EUF shall be able to send if required. | The capability shall be supported.<br><br>Supporting receiving of a SIP message or header in the SCF at the UNI means that, if received from the UNI, this message or header shall be processed as expected. It does not imply that network elements inside the served network or user equipment connected to this network shall support this message or header.<br><br>Processing should not continue if required information is unavailable. (Suitable disconnection/release processing should be performed.)<br><br>However, when a default value has been decided upon, processing is performed using the default value. | The capability shall be supported.<br><br>Supporting sending of a SIP message or header in the SCF at the UNI means that this message or header shall be processed over the UNI if received from the served network. It does not imply that network elements inside the served network or user equipment connected to this network shall support this message or header. | The capability shall be supported.<br><br>Processing should not continue if required information is unavailable. (Suitable disconnection/release processing should be performed.)<br><br>However, when a default value has been decided upon, processing is performed using the default value. |

| Code | Code name | EUF->SCF | | SCF->EUF | |
|---|---|---|---|---|---|
| | | EUF Send | SCF Recv | SCF Send | EUF Recv |
| O | Optional | The capability may or may not be supported in the EUF at the UNI. It is an implementation choice. | The capability may or may not be supported in the SCF at the UNI. It is an implementation choice.<br><br>If possible, the processing expected by the EUF on the sending side should be performed.<br><br>When the processing expected by the EUF cannot be performed, the received content should be ignored and processing should continue. | The capability may or may not be supported in the SCF at the UNI. It is an implementation choice. | Same as for EUF on the sending side.<br><br>If possible, the processing expected by the SCF on the sending side should be performed.<br><br>When the processing expected by the SCF on the sending side cannot be performed, the received content should be ignored and processing should continue. |
| C <integer> | Conditional | The requirement for the capability (“M”, “O”) depends on the support of other optional or conditional items. <integer> is the identifier of the conditional expression. | Same as for EUF on the sending side. | Same as for EUF on the sending side. | Same as for EUF on the sending side. |
| N/A | Not Applicable | It is impossible to use the capability. No answer in the support column is required. | Same as for EUF on the sending side. | Same as for EUF on the sending side. | Same as for EUF on the sending side. |

## 10.3. SDP profile

### 10.3.1. SDP Usage

This sub-clause defines an SDP profile for use in the EUF and the SCF. It also defines the set of enhancements of and restrictions on a standard SDP implementation based on [RFC 2327] and [RFC 4566]. In Table 9, M, O, and C have the same meanings as in Table 8.

Table 9: SDP Usage

| Item | EUF->SCF | | SCF->EUF | |
|---|---|---|---|---|
| | EUF Send | SCF Recv | SCF Send | EUF Recv |
| **Session description** | | | | |
| v= (protocol version) | M | M | M | M |
| o= (owner/creator and session identifier) | M | M | M | M |
| s= (session name) | M | M | M | M |
| i= (session information) | O | M | O | M |
| u= (URI of description) | O | O | O | O |
| e= (email address) | O | O | O | O |
| p= (phone number) | O | O | O | O |
| c= (connection information) | C1 | M | C1 | M |
| b= (bandwidth information) | O | M | O | M |
| **Time description (one or more per description)** | | | | |
| t= (time the session is active) | M | M | M | M |
| r= (zero or more repeat times) | O | O | O | O |
| **Session level description (continue)** | | | | |
| z= (time zone adjustments) | O | O | O | O |
| k= (encryption key) | O | O | O | O |
| a= (zero or more session attribute lines) | O | M | O | M |
| **Media description (zero or more per description)** | | | | |
| m= (media name and transport address) | C2 | M | C2 | M |
| i= (media title) | O | O | O | O |
| c= (connection information) | C1, C2 | M | C1, C2 | M |
| b= (bandwidth information) | O | M | O | M |
| k= (encryption key) | O | O | O | O |
| a= (zero or more media attribute lines) (Note) | O | M | O | M |
| C1: At least one of the c lines in session and media descriptions shall be implemented.<br>C2: If media description is implemented, both m and c lines shall be implemented.<br>Note: In cases where video session is involved, video session description should be embedded into the 'fmtp' field in 'a' line of SDP as specified in [RFC 2429/4629], as well as in RFCs which define codec-specific format. Frame rate may be embedded into the 'framerate' field in 'a' line. In this case, the 'framerate' field value shall be the same as the embedded frame rate within the 'fmtp' field. | | | | |

Note: This Table 9 is described from an implementation point of view as described in Table 8, e.g. even if the c line in the media description is implemented it does not mean that every media description in specific SIP/SDP message includes c line. When the c line is included in the session description, the c line in the media description may not be included.

If a media session across the UNI utilizes video, the media type "video" shall be supported. The media description specified in Table 9 of this Recommendation (i.e. media codec, its attributes and values) is exchanged in a SIP/SDP message to set up a video connection.

### 10.3.2. Capabilities Negotiation

When sending an SDP answer, for each accepted media type (i.e. "m=" line), the EUF on the answering side should select only the first media format supported among the media formats proposed in the received SDP offer. That is different from the media format "telephone-event" because the "telephone-event" is included in the SDP answer if it is used.

## 11. Transport-level Profile

### 11.1. Specifications to be supported

In Table 10, M and O have the same meanings as defined in sub-clause 10.1 of this Recommendation.

Table 10: Supported transport-level specifications

| Specification | Title | EUF | SCF |
|---|---|---|---|
| RFC 3016 [RFC3016] | RTP Payload Format for MPEG-4 Audio/Visual Streams | O | O |
| RFC 3047 [RFC 3047] | RTP Payload Format for ITU-T Recommendation G.722.1 | O | O |
| RFC 3267 [RFC 3267] | Real-time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs | O | O |
| RFC 3389 [RFC 3389] | RTP Payload for Comfort Noise | O (Note 1) | O (Note 1) |
| RFC 3550 [RFC 3550] | RTP: A Transport Protocol for Real-Time Applications | M | M |
| RFC 3551 [RFC 3551] | RTP Profile for Audio and Video Conferences with Minimal Control | M | M |
| RFC 3558 [RFC 3558] | RTP Payload Format for Enhanced Variable Rate Codecs (EVRC) and Selectable Mode Vocoders (SMV) | O | O |
| RFC 3611 [RFC 3611] | RTP Control Protocol Extended Reports (RTCP XR) | O | O |
| RFC 3711 [RFC 3711] | The Secure Real-time Transport Protocol (SRTP) | O | O |
| RFC 3984 [RFC 3984] | RTP Payload Format for H.264 Video | O | O |
| RFC 4103 [RFC 4103] | RTP Payload for Text Conversation | O | O |
| RFC 4348 [RFC 4348] | Real-Time Transport Protocol (RTP) Payload Format for the Variable-Rate Multimode Wideband (VMR-WB) Audio Codec | O | O |
| RFC 4629 [RFC4629] | RTP Payload Format for ITU-T Rec. H.263 Video | O | O |
| RFC 4733 [RFC 4733] | RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals | M (Note 2) | M (Note 2) |
| RFC 4749 [RFC 4749] | RTP Payload Format for the G.729.1 Audio Codec | O | O |
| T.38 [T.38] | Procedures for real-time Group 3 facsimile communication over IP networks | O | O |

Note 1: For use with codecs such as G.711 [G.711] and G.726 [G.726] that do not themselves inherently support comfort noise.

Note 2: When G.711 [G.711] is used, [RFC 4733] is not mandatory.

The following list indicates a typical example of protocols that describe layers lower than those described in the protocols in Table 10. Other protocols may be supported for lower layers.

- IETF RFC768 (08/1980): User Datagram Protocol
- IETF RFC791 (09/1981): Internet Protocol
- IETF RFC792 (09/1981): Internet Control Message Protocol
- IETF RFC793 (09/1981): Transmission Control Protocol
- IETF RFC826 (11/1982): An Ethernet Address Resolution Protocol – or – Converting Network Protocol Address to 48bit Ethernet Address for Transmission on Ethernet Hardware
- IETF RFC2460 (12/1998): Internet Protocol, Version 6 (IPv6) Specification
- IETF RFC2461 (12/1998): Neighbor Discovery for IP Version 6 (IPv6)
- IETF RFC2463 (12/1998): Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- IEEE Std 802.3-2005 (12/2005): Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications - Media Access Control Parameters, Physical Layers and Management Parameters for subscriber access networks
- ISO/IEC 8877:1992 (12/1992): Information technology - Telecommunications and information exchange between systems - Interface connector and contact assignments for ISDN Basic Access Interface located at reference points S and T

### 11.2. DTMF Tone Handling

The SCF and the EUF including User Agent shall support a specific part of [RFC 4733] to transport DTMF events. When G.711 [G.711] is used, [RFC 4733] may not be mandatory.

There are specific requirements on equipment that operates with RTP audio on one side and non-RTP audio on the other. These shall be able to detect [RFC 4733] payloads from the RTP side and generate DTMF audio tones on the non-RTP side.

Conversely, they shall detect DTMF audio tones from the non-RTP side and generate [RFC 4733] payloads on the RTP side and should remove the DTMF tones from the in-band audio.

## 12. Call Control Signalling Transport

The UNI should use SIP transport over UDP as a default transport. SIP transport over TCP or SCTP may be used, e.g. for large messages. SIP transport over TLS may be used for security.

## 13. IP Protocol Version

The network shall support IPv4. In addition, the network may support IPv6.

The EUF shall support IPv4, and in addition, the EUF may support IPv6. However, if the EUF is not supposed to connect to a network that only supports IPv4, the EUF may only support IPv6.

## 14. Security Considerations

Signalling should be secure and media may be secure.

# Appendix I: Example Call Flows

Information flows described in this appendix are meant to provide some examples of media session establishment and session release between originating-side UA and terminating-side UA through UNI. Scenarios in this appendix are based on cases where UAs are connected across separate carriers, exchanging SIP messages in order to establish media sessions.

This appendix includes scenarios which represent basic conversational service examples of successful and unsuccessful call setup and call release between two UAs. Note that these scenarios do not illustrate call procedures between carrier networks which correspond to NNI.

## I.1. Successful scenario of SIP session establishment

This subsection provides information flows of successful basic service scenario between UA#1 and UA#2 where these UAs are connected to different carrier networks. Figure I.1 presents an example of service scenario in three parts: Initial Call Establishment, Re-Call Establishment with re-INVITE, and Call Release.

As shown in the part 1 of Figure I.1, UA#1 sends an INVITE message to UA#2 with the description of session parameters in SDP. Depending on media types (i.e. audio, video, etc) to be used during the session, specific media parameters and values should be negotiated between UAs. After exchanging ACK messages, the call will be established between UA#1 and UA#2.

The part 2 of Figure I.1 provides information flows of re-call establishment using re-INVITE after media session established between two UAs. In this example, the terminating-side UA (i.e. UA#2) sends an INVITE message with new session description in SDP to the originating-side UA (i.e. UA#1) in order to re-create a media session. These procedures allow to add new media types or remove any kind of media types from early established session as shown in the part 1.

Finally, UA#1 sends a BYE message to UA#2 to release the session at the point of terminating conversation as shown in the part 3 of Figure I.1. In this example, when UA#2 sends a 200 response message to UA#1, the session will be removed.

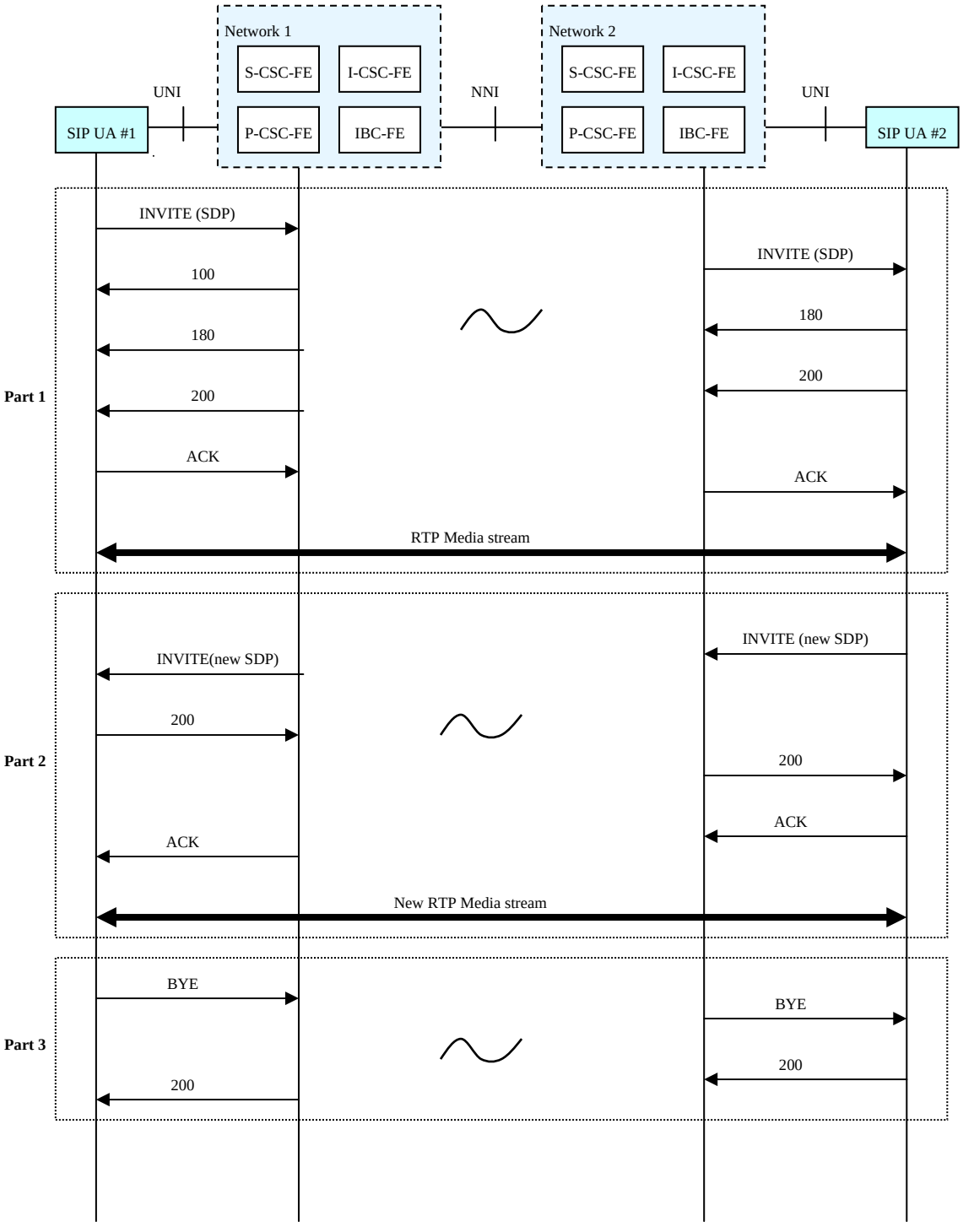


Figure I.1 Successful scenario of SIP session establishment

## I.2. Unsuccessful scenario of SIP session establishment

This subsection provides information flows of unsuccessful basic service scenario between UA#1 and UA#2 where these UAs are connected to different carrier networks.

Figure I.2 describes some specific unsuccessful service examples: Unsuccessful Busy and Unsuccessful No Response.

As shown in the part 1 of Figure I.2, the terminating-side UA (i.e. UA#1) is busy when it receives an INVITE message from the originating-side UA (i.e. UA#1). Therefore, it sends a 486 response message to UA#1 and consequently, media session is not established between them.

The part 2 of Figure I.2 shows information flows of call setup failure because UA#2 does not respond when it receives an INVITE message from UA#1. Note that the initial INVITE message will be re-transmitted to UA#2 six additional times. After this, UA#1 receives a 408 response message from the network.

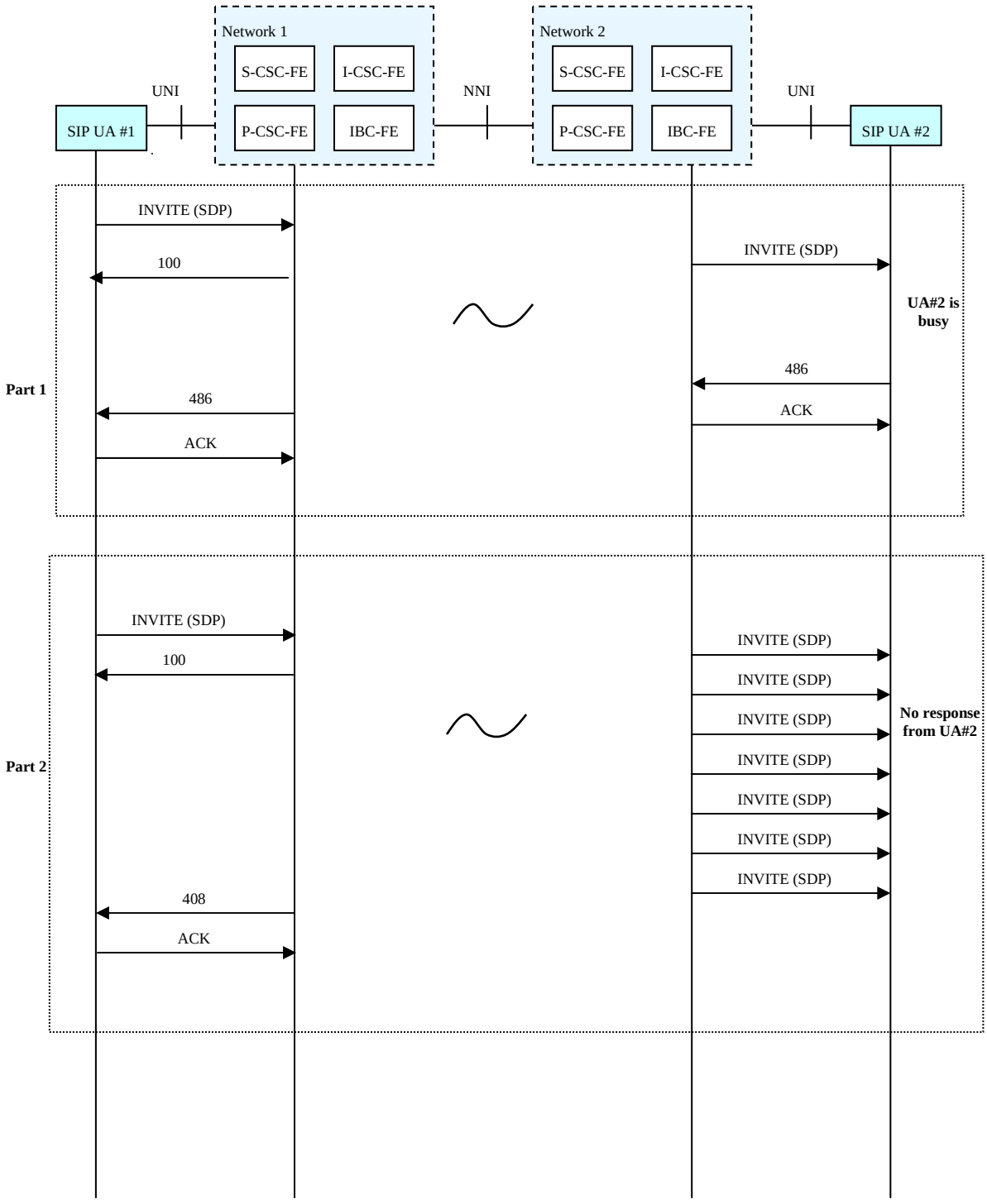


Figure I.2 Unsuccessful scenario of SIP session establishment

## I.3 Unsuccessful No Answer to Call Cancel

Figure I.3 shows an unsuccessful service example between SIP UA#1 and UA#2 where these UAs are connected to different carrier networks. UA#1 sends an INVITE message to set up a call with UA#2. UA#1 gives up on the call after it received a 180 response from UA#2. To cancel the call set up, UA#1 sends a CANCEL message however there is no response from UA#2. This case may occur when UA#2 was suddenly powered off or disconnected from the network.

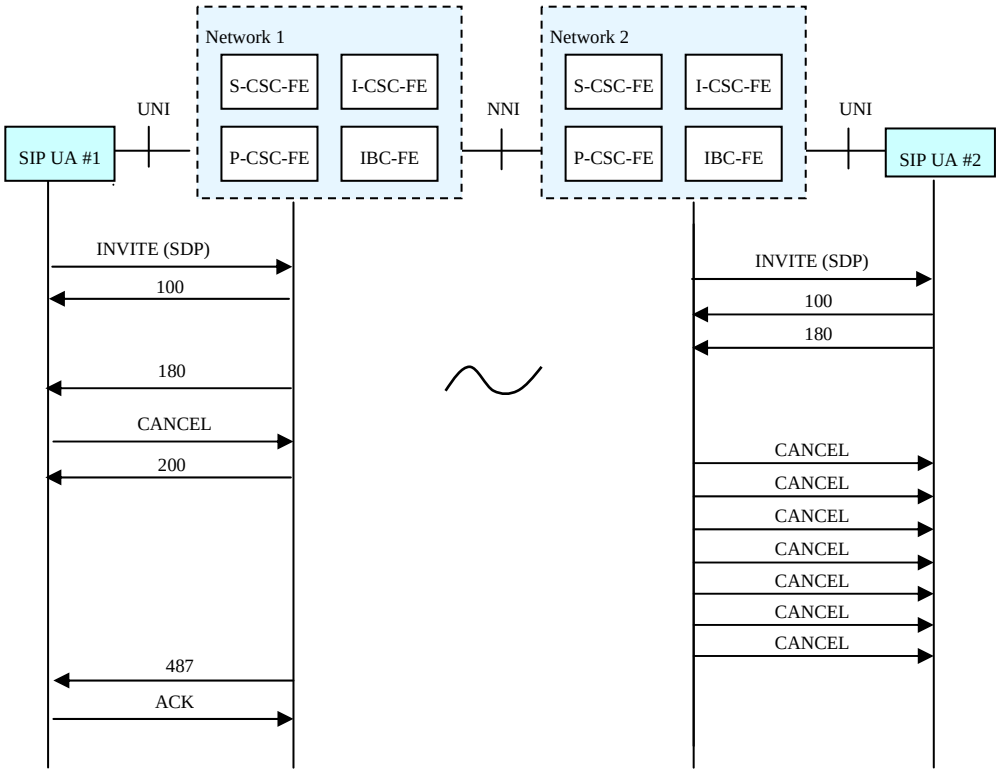


Figure I.3 Unsuccessful No Answer to Call Cancel

## I.4 Unsuccessful Call Setup

Figure I.4 shows an unsuccessful service example between SIP UA#1 and UA#2 where these UAs are connected to different carrier networks. UA#1 sends an INVITE message to set up a call with UA#2. The called party was successfully contacted however UA#2 rejected the call by sending a 4xx (Client-Error) response message. This case may occur when UA#2 identified the calling party and decided to no participate.

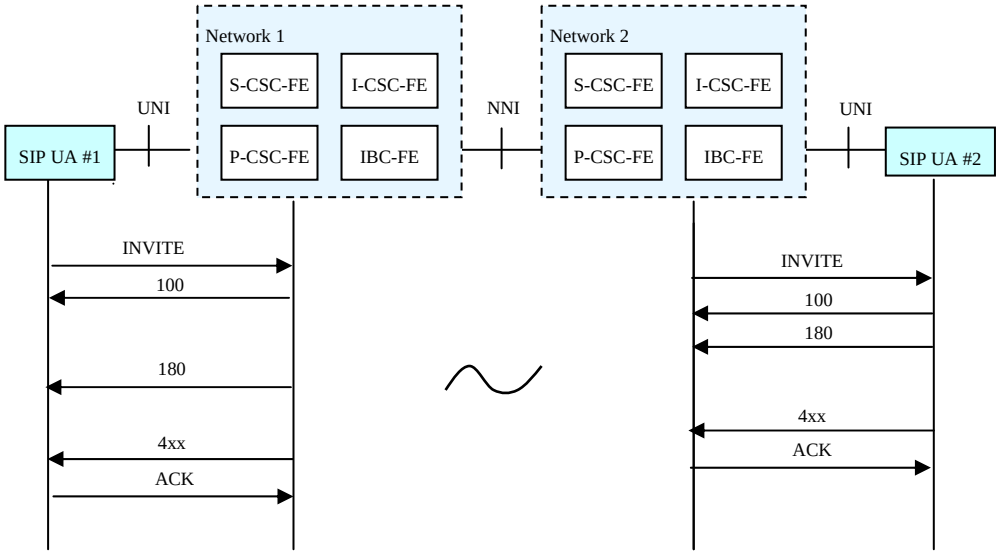


Figure I.4 Unsuccessful Call Setup

## Bibliography

– [b-ETSI ES 282 007] ETSI ES 282 007 (2006), Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture

– [b-ETSI TS 182 006] ETSI TS 182 006 (2006), Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Stage 2 description (3GPP TS 23.228 v7.2.0, modified)

– [b-ETSI ES 283 003] ETSI ES 283 003 (2007), Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 [3GPP TS 24.229 (Release 7), modified]

– [b-3GPP TS24.229] 3GPP TS24.229 (2007), 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3

_____