ATIS STANDARD

ATIS-1000028.2008(R2013)

IP Device (SIP UA) to Network Interface Standard

AMERICAN NATIONAL STANDARD FOR TELECOMMUNICATIONS

AMERICAN NATIONAL STANDARD

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

> NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-1000028.2008(R2013), *IP Device (SIP UA) to Network Interface Standard*

Is an American National Standard developed by the **Signaling, Architecture, and Control (SAC)** Subcommittee under the **ATIS Packet Technologies and Systems Committee (PTSC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

(R2013)
ATIS-1000028.2008

American National Standard for Telecommunications for

IP Device (SIP UA) to Network Interface Standard

Alliance for Telecommunications Industry Solutions

Approved July 3, 2008

American National Standards Institute, Inc.

Abstract

This User to Network Interface (UNI) standard supports SIP based interconnection for VoIP between a carrier (SCF) and the user (EUF). The SIP UNI interface specified in this document is applicable to individual SIP phones as well as to SIP PBXs.

Foreword

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the Standard.

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, PTSC, which was responsible for its development, had the following roster:

J. Zebarth, PTSC Chair (Nortel)

J. McEachern, Technical Editor (Nortel)

C. Underkoffler, ATIS Chief Editor

The Signalling, Architecture, and Control (SAC) Subcommittee was responsible for the development of this document.

Table of Contents

Table of Figures

Table of Tables

American National Standard for Telecommunications –

IP Device (SIP UA) to Network Interface Standard

1 Scope

The specification of the SIP UNI in this document is based on a standard SIP User Agent (UA) connected to a Service Provider Network composed of standard SIP components (SIP proxies, etc.). Depending on the service scenario, the SIP UA can interact directly with an Application Server, or with another SIP UA via a SIP Application Server. The SIP UA implements standard SIP session control mechanisms for initiating sessions, and for responding to invites from another SIP UA or Application Server. Services are implemented in the SIP UA, in the Application Server (with the SIP UA interacting with the Application Server through standard SIP mechanisms) or in a combination of the SIP UA and Application Server.

This specification applies to a SIP UA associated with an individual SIP device as well as to a SIP UA associated with a SIP PBX. From the perspective of this specification, a SIP UA connects to a service provider network either directly, or via a SIP PBX .

2 References

The following standards contain provisions which, through reference in this text, constitute provisions of this American National Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this American National Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

2.1 Normative References

2.1.1 IETF[1]

[RFC 1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, IETF, April 1992.

[RFC 2205] R. Braden, R., Zhang, L., Berson, A., Herzog, S., and Jamin, S., “Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification”, RFC 2205, IETF, September 1997.

[RFC 2246] Dierks, T. and Allen, C., "The TLS Protocol Version 1.0", RFC 2246, IETF, January 1999.

[RFC 4566] Handley, Jacobson, Perkins, "SDP: Session Description Protocol", RFC 4566, IETF, July 2006.

[RFC 2401] Kent, S. and Atkinson, R., " Security Architecture for the Internet Protocol", RFC 2401, IETF, November 1998.

[1] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

[RFC 4733] Schulzrinne , H. and Petrack, S., “RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals”, RFC 4733, IETF, December 2006.

[RFC 3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP:Session Initiation Protocol", RFC 3261, IETF, June 2002.

[RFC 3262] J. Rosenberg, H. Schulzrinne, “Reliability of Provisional Responses in Session Initiation Protocol (SIP),” RFC 3262, June 2002.

[RFC 3263] Rosenberg, J. and Schulzrinne, H., "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, IETF, June 2002.

[RFC 3264] Rosenberg, J. and Schulzrinne, H., “An Offer/Answer Model with the Session Description Protocol (SDP)", RFC 3264, IETF, June 2002.

[RFC 3265] Roach, A., "Session Initiation Protocol (SIP)-Specific Event Notification", RFC 3265, IETF, June 2002.

[RFC 3311] J. Rosenberg, "The SIP UPDATE Method", RFC 3311, IETF, September, 2002.

[RFC 3312] Camarillo, G., Marshall, W. and Rosenberg, J., "Integration of Resource Management and Session Initiation Protocol (SIP)", RFC 3312, IETF, October, 2002.

[RFC 3323] J. Peterson, “A Privacy Mechanism for the Session Initiation Protocol (SIP)”, RFC 3323, IETF, November 2002.

[RFC 3324] M. Watson, “Short Term Requirements for Network Asserted Identity”, RFC 3324, IETF, November 2002.

[RFC 3325] C. Jennings, J. Peterson, and M. Watson, “Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks”, RFC 3325, IETF, November 2002.

[RFC 3326] Schulzrinne, H., Oran, D., Camarillo, G., "The Reason Header Field for the Session Initiation Protocol (SIP)", RFC 3326, IETF, December 2002.

[RFC 3428] Campbell, B., Rosenberg, J., Schulzrinne, H., Huitema, C. and Gurle, D., “Session Initiation Protocol (SIP) Extension for Instant Messaging”, RFC 3428, IETF, December 2002.

[RFC 3489] Rosenberg, J., Weinberger, J., Huitema, C. and Mahy, R., “STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)”, RFC 3489, IETF, March 2003.

[RFC 3550] Schulzrinne, H., Casner, S., Frederick, R. and Jacobson, V. "RTP: A Transport Protocol for Real-Time Applications", RFC 3550, IETF, July 2003

[RFC 3551] Schulzrinne, H. and Casner, S., "RTP Profile for Audio and Video Conferences with Minimal Control", RFC 3551, IETF, July 2003.

[RFC 3515] Sparks, R., “The Session Initiation Protocol (SIP) Refer Method”, RFC 3515, IETF, April 2003.

[RFC 3581] Rosenberg, J., Schulzrinne, H., "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Handling", RFC 3581, IETF, August 2003.

[RFC 3711] Baugher,M., McGrew, D., Naslund, M., Carrara, E. and Norrman, K.., "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, IETF, March 2004.

[RFC 3725] Rosenberg, J., Peterson, J., Schulzrinne, H., Camarillo, G., "Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)", RFC 3725, IETF, April 2004.

[RFC 3824] Peterson, J., Liu, H., Yu, J. and Campbell, B. “Using E.164 numbers with the Session Initiation Protocol (SIP)”, RFC 3824, IETF, June 2004.

[RFC 3842] Mahy, R., “A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)”, RFC 3842, IETF, August 2004.

[RFC 3856] Rosenberg, J, “A Presence Event Package for the Session Initiation Protocol (SIP)”, RFC 3856, IETF, August 2004.

[RFC 3857] Rosenberg, J. “Watcher Information Event Template-Package for the Session Initiation Protocol (SIP)”, RFC 3857, IETF, August 2004.

[RFC 3858] Rosenberg, J. “An Extensible Markup Language (XML) Based Format for Watcher Information”, RFC 3858, IETF, August 2004.

[RFC 3859] Peterson, J. “Common Profile for Presence (CPP)”, RFC 3859, IETF, August 2004.

[RFC 3860] Peterson, J. “Common Profile for Instant Messaging (CPIM)”, RFC 3860, IETF, August 2004.

[RFC 3861] Peterson, J. “Address Resolution for Instant Messaging and Presence”, RFC 3861, IETF, August 2004.

[RFC 3862] Klyne, G. and Atkins, D. “Common Presence and Instant Messaging (CPIM): Message Format”, RFC 3862, IETF, August 2004.

[RFC 3863] Sugano, H., Fujimoto, S., Klyne, G., Bateman, A., Carr, W. and Peterson, J. “Presence Information Data Format (PIDF)”, RFC 3863, IETF, August 2004.

[RFC 3891] Mahy, R., Biggs, B., Dean, R. “The Session Initiation Protocol (SIP) "Replaces" Header”, RFC 3891, IETF, September 2004.

[RFC 3892] Sparks, R. “The Session Initiation Protocol (SIP) Referred-By Mechanism”, RFC 3892, IETF, September 2004.

[RFC 3903] Niemi, A., “Session Initiation Protocol (SIP) Extension for Event State Publication”, RFC 3903, IETF, October 2004.

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

[RFC 3960] Camarillo, G. and Schulzrinne, H., “Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)”, RFC 3960, IETF, December 2004.

[RFC 3966] Schulzrinne, H. “The tel URI for Telephone Numbers”, RFC 3966, IETF, December 2004.

[RFC 3994] Schulzrinne, H. “Indication of Message Composition for Instant Messaging”, RFC 3994, IETF, January 2005.

[RFC 4028] Donovan, S. and Rosenberg, J., “Session Timers in the Session Initiation Protocol (SIP)”, RFC 4028, IETF, April 2005.

[RFC 4032] Camarillo, G. and Kyzivat, P., “Update to the Session Initiation Protocol (SIP) Preconditions Framework”, RFC 4032, IETF, March 2005.

[RFC 4040] Kreuter, R. “RTP Payload Format for a 64 kbit/s Transparent Call”, RFC 4040, IETF, April, 2005.

[RFC 4244] M. Barnes, “An Extension to the Session Initiation Protocol (SIP) for Request History Information”, RFC 4244, IETF, November 2005.

[RFC 4412] Schulzrinne, H. and Polk, J., “Communications Resource Priority for the Session Initiation Protocol (SIP)”, RFC 4412, IETF, February 2006.

[RFC 4504] Sinnreich, H., Lass, S. and Stredicke, C., "SIP Telephony Device Requirements and Configuration", RFC 4504, IETF, May 2006.

[RFC 4568] Andreasen, Baugher, Wing, "Session Description Protocol (SDP) Security Descriptions for Media Streams", RFC 4568, IETF, July 2006.

[draft-ietf-mmusic-ice-19] Rosenberg, J., “Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Multimedia Session Establishment Protocols”, draft-ietf-mmusic-ice-15, IETF, September 2007.

[RFC 4458] Jennings, C., Audet, F., and Elwell, J., “Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)” RFC 4458, IETF, April 2006.

[RFC 4480] Schulzrinne, H, Gurbani, V., Kyzivat, P. and Rosenberg, J. “RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)”, RFC 4480, IETF, July 2006.

[RFC 4629] Ott, J., Bormann, C., Sullivan, G., Wenger, S., Even, R. “RTP Payload Format for ITU-T Rec. H.263 Video”, RFC 4629, IETF, January 2007.

[RFC 4662] Roach, A.B., Campbell, B. and Rosenberg, J. “A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists”, RFC 4662, IETF, August 2006.

[draft-ietf-simple-partial-pidf-format-10] Lonnfors, M., Leppanen, E., Khartabil, H., and Urpalainen, J. “Presence Information Data format (PIDF) Extension for Partial Presence”, draft-ietf-partial-pidf-format-08, IETF, November 2006.

[RFC 4579] Johnston, A. and Levin, O., “Session Initiation Protocol Call Control - Conferencing for User Agents”, RFC 4579, IETF, August 2006.

[RFC 4575] Rosenberg, J., Schulzrinne, H. and Levin, O., “A Session Initiation Protocol (SIP) Event Package for Conference State”, RFC 4575, IETF, August 2006.

[RFC 4730] Burger, E. and Dolly, M., "A Session Initiation Protocol (SIP) Event Package for Key Press Stimulus (KPML)", RFC 4730, IETF, November 2006.

[RFC 4961] Wing , D., “Symmetric RTP / RTP Control Protocol (RTCP)”, RFC 4961, IETF, July 2007.

2.1.2 ITU-T[2]

[G.711] ITU-T G.711 Pulse Code Modulation (PCM) of Voice Frequencies, November 1988.

T.38 Procedures for real-time Group 3 facsimile communication over IP networks, April 2007.

2.2 Informative References

2.2.1 ITU[2] and ISO/IEC[3]

[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)"

[2] This document is available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

[3] This document is available from the International Organization for Standardization. < http://www.iso.ch/iso/en/prods-services/ISOstore/store.html >

[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

2.2.2 IETF[1]

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

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

2.2.3 ETSI[4]

[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)

2.2.4 Other[5]

[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

3.1 Definitions

In this document, the label "*must*" indicates that it *must* be conformant to all mandatory provisions of the corresponding specification. However, it should be noted that being "conformant to all mandatory provisions" means that it is mandatory to be able to respond to all required messages/headers, but it may not be mandatory in all circumstances to be able to send certain messages/headers. In addition, the label "*must*" means that the functionality must be implemented, although it is recognized that carriers, enterprise networks and devices may choose to not activate the functionality in some or all circumstances. The label "*must*^{1}" indicates that all mandatory provisions of the corresponding specification *must* be implemented, but configuration or negotiation determines whether the feature is used.

The label *"shall"* indicates a mandatory requirement of this American National Standard.

The label "*should*" indicates that it *should* be conformant to the corresponding specification. The label "*should*^{2}" is used in the case of draft specifications for which the requirement is likely to become a "*must*" in a future version of this profile, after the draft specification has been promoted to an RFC. However, because draft specifications are subject to change, it is not feasible to make such specifications a "*must*" for the purposes of this version of the profile. Similarly, the label "*should* ^{1,2}" indicates the requirement may become a "*must*^{1}" in a future version of this profile. The word *may* denotes a optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

The words "see text" indicates that a description of the conformance criteria follows in this text. "N/A" indicates the corresponding specification is not required.

The following definitions are applicable to the SIP UNI framework as defined in this document:

Device: A device is the instrument through which an end user is connecting to the Carrier network and contains a User Agent and a user interface. A device is a specific instance of the more generic EUF.

[4] This document is available from the European Telecommunications Standards Institute (ETSI).
< http://www.etsi.org/getastandard/home.htm >

[5] This document is available from the Telecommunications Industry Association (TIA).
< http://www.tiaonline.org/standards/overview.cfm >

User Agent: A User Agent (UA) is a SIP construct that represents the device in a SIP-based network. It has an IP network connection on one side and a user interface connection on the other side.

User interface: the user interface is the means by which a user of the DEVICE interacts with the User Agent in order to initiate and receive voice communication, and is presented through something like a telephone or PC.

Carrier network: A Carrier network is a SIP-based VoIP network that contains one or more elements, at least one of which is an application server (AS), which is responsible for applying service logic to call requests or media streams.

Application Server: An Application Server (AS) is an entity in the Carrier network that is responsible for applying service logic to call requests or media streams. Application servers implement services, in combination with service logic in the User Agent.

EUF: The end-user functions (EUF) includes end-user equipment, both the legacy terminals and NGN terminals, and 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. A SIP EUF contains a User Agent.

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

(SIP) Proxy, Proxy Server: A Proxy or Proxy Server is an intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, which means its job is to ensure that a request is sent to another entity "closer" to the targeted user. Proxies are also useful for enforcing policy (for example, making sure a user is allowed to make a call). A proxy interprets, and, if necessary, rewrites specific parts of a request message before forwarding it.

(SIP) B2B UA: 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.

SIP PBX: A Private Branch eXchange is a telephone exchange that serves a particular business or office, as opposed to one a common carrier or telephone company operates for many businesses or for the general public. A SIP PBX has a SIP interface to the Carrier network. The SIP PBX may implement a SIP Proxy or a B2BUA. The SIP PBX, in the context of this specification, appears to the network as if it is a device or EUF, even though the User Agent may be in the PBX, or in the physical device connected to the PBX.

User Network Interface: The User-Network Interface (UNI) is the interface between the User Agent (UA) and the network.

Services: The collection of behaviors to be applied to communications requests on behalf of the end user.

4 ABBREVIATIONS

4.1 Abbreviations

ABNF	Augmented BNF

AMR	Adaptive Multirate (codec)
AMR NB	AMR Narrowband
AMR WB	AMR Wideband
ANSI	American National Standards Institute
B2BUA	Back-to-Back User Agent
BNF	Backus-Naur Form
CPE	Customer Premises Equipment
CSC-FE	Call Session Control Functional Entity
DNS	Domain Name Service
DTMF	Dual Tone Multi Frequency
EUF	End-User Functions
EVRC	Enhanced Variable Rate Codec
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transport Protocol
IBC-FE	Interconnection Border gateway Control Functional Entity
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISO/IEC	International Standardization Organization/International Electrotechnical Commission
ITU-T	International Telecommunications Union – Telecommunication
IVR	Interactive Voice Response
KPML	Key Press Markup Language
MIME	Multipurpose Internet Mail Extensions
MPEG	Moving Picture Experts Group
MWI	Message Waiting Indication
NAT	Network Address Translation
NGN	Next Generation Network
NGN-TE	NGN Terminal Equipment
PBX	Private Branch eXchange
PCM	Pulse Code Modulation
PoC	Push to talk over Cellular
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RFC	Request for Comments
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
SCF	Service Control Functions
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
UI	User-Interface
UNI	User-Network Interface
URI	Uniform Resource Identifier
VMR-WB	Variable-Rate Multi-Mode Wideband
VoIP	Voice over IP
VPN	Virtual Private Network
WPA	Wi-Fi Protected Access
XML	Extensible Markup Language

5 REFERENCE MODEL

The *User-Network Interface* (UNI) is the interface between the User Agent (UA) and the network. The network is viewed here as more or less a single entity, although in fact different signaling will interact with different network elements.

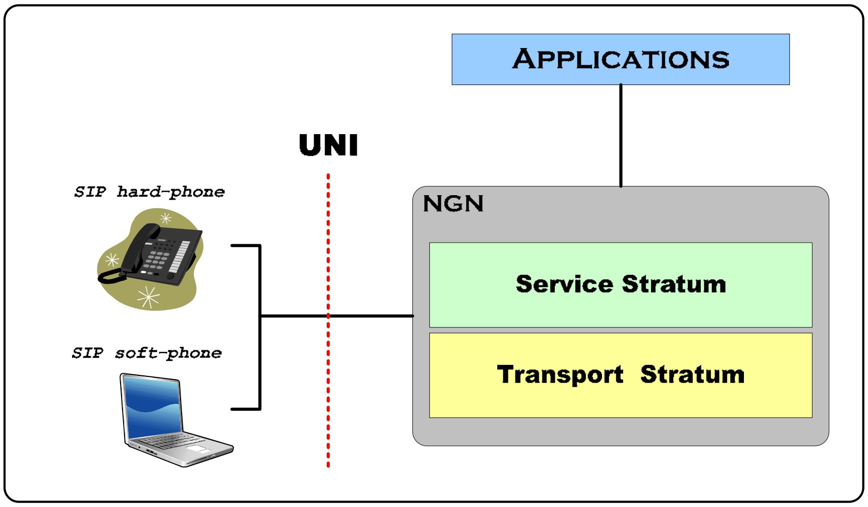

Figure 1.a: User-Network Interface Model for SIP phone connected directly to Carrier Network

The UNI for SIP phones connected to the SIP network covers both residential and enterprise applications where the customer wants to take full advantage of the future SIP multi-media capabilities. This specification applies equally to SIP "Hard Phones" and "Soft Phones". The services are implemented in the SIP UA, in the Application Server, or in a combination of the two, depending on the specific service.

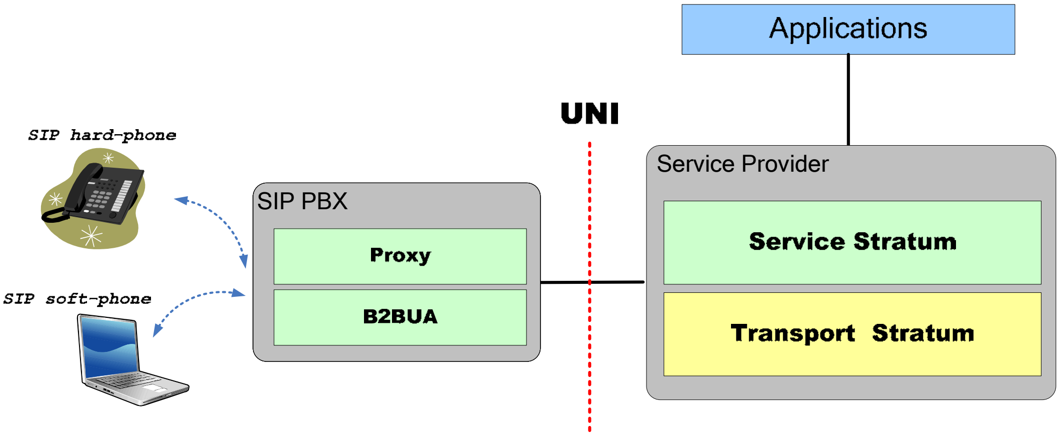

Figure 1.b: User-Network Interface Model for SIP PBX to Service Provider

The SIP PBX to Service provider scenario is aimed at the enterprise market. The UNI allows for the SIP PBX to be managed by either the enterprise, or the Service Provider. The UNI does not restrict the types of terminals, and can include both SIP "Hard Phones" and "Soft Phones". In the case of SIP Phones, the SIP PBX can act as either a proxy or a B2B UA.

This specification assumes that the PBX will register users individually, however it is recognized that there may be value in supporting the capability for a SIP PBX to bulk register users. This later case, referred to as "aggregate end points", is for further study.

6 ASSUMPTIONS

This collection of baseline protocols is designed to enable implementation of basic function phones as well as rich feature phones. This informative section is intended to provide some background for the collection of normative specifications defined in the sections that follow.

The specification in this document applies to the implementation of the components on either side of the SIP UNI. The specification does not in general apply to the use of these components, which is a local matter for the carrier. For example, this document specifies that TLS *shall* be supported. This means that equipment must include the functionality necessary to initiate calls using TLS. However, the carrier may choose not to use it for a given call, or even to disable this capability in a given deployment. This specification is intended to maximize interoperability, not to restrict a carriers business decisions.

Using TLS over TCP is the preferred transport for SIP messages, however it is recognized that many SIP devices use UDP, so UDP is also a requirement of the Network Edge. In addition, devices *shall* support SRTP for media encryption, although some configurations may not use SRTP for some calls. Other encryption is also possible but not required, such as IPSec as a VPN-tunneling mechanism to the service provider. IPSec is of particular interest for several reasons including: its common use over numerous interconnections, such as WiFi which may or may not also have additional security mechanisms such as WPA; and its use in the PacketCable Security Specification, **http://www.packetcable.com/downloads/specs/PKT-SP-SEC1.5-I01-050128.pdf**, January 2005.

Symmetric RTP and outbound proxy support is part of the Baseline Profile so that signaling and media can traverse typical consumer firewalls and NATs using “network hosted NAT traversal”, with minimum impact on the device implementation. By adjusting the SIP Registration timeout to keep a NAT pinhole open, (for example, through correction of IP addresses and port numbers in SIP messages and SDPs) symmetric UDP allows the media to flow through typical firewalls and NATs, and can be directed to the appropriate target. There are deployment topologies in which symmetric RTP is not required.

The outbound proxy for a device *may* be set. The setting *may* require that all signaling packets *shall* be sent to the outbound proxy or that only in the case when no route has received the outbound proxy *shall* be used. This ensures that NAT application layer gateways are always in the signaling path. The second requirement allows the optimization of the routing by the outbound proxy. Example: OutboundProxy="sip:nat.proxy.com" The default outbound proxy *should* be a global setting (not related to a specific line. Example: DefaultProxy="sip:123@proxy.com".

6.1 Each user identity is assigned to only one user-domain

Each device user-identity is assigned to only one SIP Registrar and no more than one Presence Server. This Profile doesn’t include the ability for user to share the same identity with different service providers or enterprises.

6.2 Presence Publication and Presence-Watcher Package

“Presence Publication” is required so that all devices can support the protocols and indicate to other devices that the user is available/busy/etc. The optional “Presence-Watcher” package enables some types of devices to show a contact/buddy list of who else is currently available.

The reasoning for this requirement is that some devices will have a user-interface (UI) to show contact/buddy lists, and others won’t. But even those that have no such UI, need to support the publication protocol so they show up on devices that do. The support of presence capability between an Enterprise network and a Carrier network is a matter of policy.

6.3 Use Cases

The intent of this document is that the collection of underlying protocols defined here is sufficient to support the following use cases in an interoperable manner. Some of these use cases require implementation in the device or network that is beyond the scope of this document, but the underlying protocols are intended to be sufficient to support it:

Voice

- Call Waiting
- Caller ID & Caller ID Block/Unblock
- Caller Name Presentation
- Conferencing (3-way)
- DID (Direct Inward Dialing)
- DOD (Direct Outward)
- Personalized call handling for VIPs, family members & others (Need to define)
- Locate-me
- Billing/Account Codes
- Bridged Line Appearances
- Call Forwarding
- Call Groups
- Call Hold
- Call Logs
- Call Park
- Call Pick-up
- Simultaneous Ring
- Mid-Call Move
- Voicemail (UM and MWI)
- Outlook Integration
- Audio Conferencing
- Bridged Line Appearances

Instant Messaging

- Presence status control (online, away, busy)
- Do not disturb setting, disabling notifications
- Server-side or "roaming" contact list
- Offline status
- Contact search outside contact list

Other

- PoC-to-Voice IM Inter-working
- Audio/video and IM text encryption

7 MEDIA AVAILABILITY IN A SIP SESSION

This section is normative.

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) 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 duration is a matter for local policy.) However, when the status of the media flows is not active according to the SDP negotiations, the absence of media packets across the UNI over any time interval in either direction shall not be taken by either a UA or the network as a sufficient reason to clear the SIP session.

Note: When it is certain that a failure affecting the SIP session has occurred, the SIP session can be cleared whether the status of the media flows is active or inactive.

Note: Requirements for SDP are also discussed in Section 10.1 and 10.3 of this document. The Media Description table in Section 10.1 specifies the basic requirement for support of RFC 4566: SDP, while Section 10.3 defines an SDP profile for use in UA and network.

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

This section is normative.

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 NGN policy.

Note 1: In case a common codec cannot be negotiated, this Standard 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. 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: 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.

Note 4: 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 5: For voice communication, the recommended-codec list *shall* contain G.711 A and 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. 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 preferable data applications to the user.

Note 6: 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.

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 20 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 also recognized that there should be a 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 Standard places no requirements on the value to be selected.

9 ROUTING AND ADDRESSING

This section is normative.

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 (Note1)
	Description: "userinfo", "hostport" and "uri-parameters" are set based on section 25 of RFC3261. "userinfo" includes global E.164 number or local number
	References: RFC 3261, RFC 3966
tel URI	tel:telephone-subscriber
	Description: telephone-subscriber is global E.164 number or local number
	References: RFC 3261, RFC 3966
Note 1	"hostport" includes either a domain name or IP address. "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 SIGNALING PROFILE

10.1 RFCs to be Supported

This section is normative.

Mandatory Baseline for all Devices and Networks

This section defines the protocols and the features that a Device's interface (EUF) to the Network *shall* adhere to in order to be conformant. This section also defines the protocols and the features that a Network's interface (SCF) to the Device *shall* adhere to in order to be conformant.

The table below describes the requirements for support of various RFCs. However, it is important to understand the information in the subsequent sections of this document, as well as in the RFCs themselves. RFCs have many requirements that may not be mandatory in all circumstances. For example, in many cases, it is mandatory to be able to respond to a message, but it may not be mandatory to be able to send it.

Table 2 - Mandatory Baseline for all Devices and Networks

	EUF (End User Function)	SCF (Session Control Function)	Justifying Use Case
Identity and Privacy			
RFC 3323: Privacy Mechanism for SIP	*Should* (see text)	*Shall* (see text)	Enables feature similar to caller-ID blocking. Users are empowered to hide their identity and related personal information when they issue requests, but intermediaries and designated recipients of requests are entitled to reject requests whose originator cannot be identified.
RFC 3324: Short Term Requirements for Network Asserted Identity	*Should* (see text)	*Shall* (see text)	Requirements for RFC 3325
RFC 3325: Private Extensions to SIP for Asserted Identity within Trusted Networks	*Should* (see text)	*Shall* (see text)	Enables feature similar to caller-ID, within a trusted domain.
URI			
RFC 3824 Using E.164 numbers with SIP	see text	see text	
RFC 3966: The tel URI for Telephone Numbers			
RFC 4458: Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)	see text	see text	

RFC 3323, 3324, and 3325: It is optional to support these RFCs for enterprise networks.

RFC 3824: E.164 numbers, RFC 3966: tel URI for Telephone Numbers

Devices and Networks *shall* be capable of accepting calls using RFC 3824 format (SIP URI) and *shall* be capable of accepting calls using RFC 3966 format (tel URI). Devices and Networks *shall* be capable of initiating calls using one or both of these formats: RFC 3824 or RFC 3966.

RFC 4458: This RFC *shall* be used when retargeting is required.

SIP & Extension			
RFC 3261: SIP	see Section 10.2	see Section 10.2	Fundamental signaling Protocol
RFC 3262: Reliability of Provisional Responses in SIP	see text	see text	
RFC 3263: Locating SIP Servers	*Shall*see text	*Shall*see text	Fundamental DNS procedures used to connect SIP clients and proxies
RFC 3311: The UPDATE Method	see text	see text	
RFC 3264: Offer/Answer	*Shall*	*Shall*	Fundamental SDP offer/answer model to negotiate common capabilities
RFC 3265: Subscribe/Notify	*Shall*	*Shall*	Event notification used by message-waiting (RFC 3842) and presence (RFC 3856)
RFC 3515: Refer Method	*Shall*	*Shall*	Enables call-transfer and other features
RFC 3326: The Reason Header Field for SIP	see text	*Shall*	Standard should define specific values
RFC 4244: Extension to SIP for Request History Information[6]	see text	*Shall* see text	Example: diversion to voicemail may vary for busy / timeout
RFC 4412: Communications Resource Priority for the Session Initiation Protocol (SIP)	See text	*Shall*	
RFC 3581: Extension to SIP for Symmetric Response Routing	*Shall*	*Shall*	Used for traversing NATs
RFC 3725: Best Current Practices for Third Party Call Control in SIP	*Should*	*Should*	e.g. routing from a media server to caller
RFC 3891: SIP "Replaces" Header	*Should*	*Shall*	
RFC 3892: SIP Referred-By Mechanism	see text	see text	

[6] RFC 4244 is the standardized mechanism to provide the functionality that was initially proposed in draft-levy-sip-diversion-08. This draft has now expired and is unlikely to ever become an RFC. However, networks and devices *Should* support this draft for backward compatibility with deployed devices. Draft-levy-sip-diversion-08 can be found at http://tools.ietf.org/id/draft-levy-sip-diversion-08.txt and at http://www.softarmor.com/wgdb/docs/draft-levy-sip-diversion-08.txt

Section 3 of RFC 3960: Early Media and Ringing Tone Generation **SECTION 3 ONLY is MANDATORY**	*Shall*See Text	*Shall*See Text	Early media required to facilitate interoperability with the PSTN, and to invoke an IVR. Examples generated by the callee include ringing tone and announcements (e.g., queuing status). Examples generated by the caller include voice commands or dual tone.
RFC 3842: Message Waiting Indication Event Package	*Shall*see text	*Shall*see text	Enables message-waiting feature
RFC 4730: SIP Event Package for KPML	*Should*	*Should*	
RFC 4028: Session Timers in SIP	*Shall*	*Shall*	Minimum requirement is to support the empty UPDATE keep-alive

RFC 3262: Reliability of provisional responses in SIP

Devices and Networks *shall* support reliability of provisional responses for UDP transport.

Devices and Networks *may* support reliability of provisional responses for TCP transport.

Devices and Network *should* maintain TCP transport connections for the duration of the SIP dialog to avoid loss of provisional responses.

RFC 3263: Locating SIP Servers

RFC 3263 may not be required in enterprise networks, nor in the carrier network that supports these enterprise connections.

RFC3263 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.

RFC 3311: SIP Update Method

Devices and Networks *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 the 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 the new offer, a re-INVITE *should* be used.

RFC 3326: The Reason Header Field for SIP

This is only applicable for enterprise networks and the carrier networks supporting enterprise networks, but in any case, it is optional to implement this RFC in the EUF.

RFC 4244: Extension to SIP for Request History Information

Devices MAY and Networks *shall* support RFC 4244. A Device *may* include history-info whenever it is retargeting, including a reason parameter. The security and privacy requirements in the RFC *shall* be met.

RFC 4412: Communications Resource Priority for the Session Initiation Protocol (SIP)

Devices *may* and enterprises *should* support RFC 4412. Networks (SCF) *shall* support RFC 4412

RFC 3892: SIP Referred-By Mechanism

RFC 3892 *shall* be supported by enterprise, and *may* be supported by other devices.

RFC 3960: Early Media and Ringing Tone Generation

Devices and networks *shall* support all Mandatory provisions of section 3 of RFC 3960. Other sections of RFC 3960 do not apply, and are not required.

RFC 3842: Message Waiting Indication Event Package

Devices and Networks *shall* support Message Waiting Indication Event Package RFC 3842. Devices *shall* have means of indicating to the user when there is a message waiting.

Media Description			
RFC 4566: SDP	*Shall*	*Shall*	Fundamental description format used by RFC 3264

Note: Requirements for SDP are also discussed in Section 7 and 10.3 of this standard. Section 7 provides detailed requirements for when the originating and terminating UA will begin sending and receiving media packets, while Section 10.3 defines an SDP profile for use in UA and network.

Conference			
RFC 4575: SIP Event Package for Conference State	*Shall*	*Shall*	
RFC 4579: SIP Call Control - Conferencing for User Agents	see text	see text	

Reservationless Network-based Conferencing

Explicit support for network-based conferencing is optional. All Devices and Networks that do explicitly support network-based conferencing, *shall* conform to this section.

RFC 4579: SIP Call Control - Conferencing for User Agents

Devices and Networks *shall* conform to all mandatory provisions of RFC 4579 with the following clarifications:

4. SIP Conferencing Primitives
   - 4.1 INVITE: Joining a Conference using the Conference URI - Dial In - *shall* be supported by any Focus
   - 4.2 INVITE: Adding a Participant by the Focus - *shall* be supported by any Focus
   - 4.3 INVITE: Manually Creating a Conference by Dialing into

a Conferencing Application - *may*be supported by a Focus

4.4 INVITE: Creating a Conference using Ad-Hoc SIP Methods - *should* be supported by Network

4.5 REFER: Requesting a Focus to Add a New Resource to a Conference (Dial-out to a new Participant) *should* be supported by any Focus

4.6 REFER: Requesting a User to Dial into a Conference Using a Conference URI - *shall* be supported by any client

4.7 REFER with REFER: Requesting a Focus to Refer a Participant to dial into the Conference - *may* only

4.8 Join Header Field: Dialing into a Conference Using a (3rd Party) Dialog Identifier - *should* be supported by any Focus

4.9 Replaces Header Field: Switching User Agents within a Conference - *may* be supported by any focus

4.10 Replaces Header Field: Transferring a Point-to-Point Session into a Conference - *should* be supported by any Focus

4.11 REFER with BYE: Requesting a Focus Remove a Participant from a Conference - *should* be supported by any Focus

4.12 Deleting a Conference - *shall* be supported by any Focus

4.13 Discovery of URI Properties using OPTIONS - *shall* be supported by any Focus

If 4.4 above is not supported by a carrier, the carrier *shall* support 4.3 for its foci instead.

Support for instant messaging is optional. All Devices that do support instant messaging, *shall* conform to the following section. All Networks *shall* conform where they logically terminate devices. Both Page mode (message) and MSRP mode *shall* be supported.

Instant Messaging		
	EUF	**SCF**
RFC 3428: SIP Extension for Instant Messaging	*Shall* See text	*Shall*
RFC 3857: Watcher Information Event Template-Package for SIP	*Should*	*Shall*
RFC 3858: XML Based Format for Watcher Information	*Should*	*Shall*
RFC 3859: Common Profile for Presence	*Should*	*Should*
RFC 3860: Common Profile for Instant Messaging	*Should*	*Should*
RFC 3861: Address Resolution for Instant Messaging and Presence	*Should*	*Should*
RFC 3862: Common Presence and Instant Messaging	*Shall*	*Shall*
RFC 3994: Indication of Message Composition for Instant Messaging	*Should*	*Should*
RFC 4480: Rich Presence Extensions to PIDF	*Should*	*Should*
RFC 4662: SIP Event Notification Extension for Resource Lists	*Should*	*Should*
draft-ietf-simple-partial-pidf-format-08	*Should*	*Should*

RFC 3428: SIP Extension for Instant Messaging

RFC3428 *shall* be implemented when instant messaging is required.

Presence			
RFC 3903: SIP Extension for Event State Publication	*Shall*see text	*Shall*	Indication of device status so that other devices may display in a contact/buddy list Only applicable for terminals that support Presence
RFC 3856: Presence Event Package	see text	see text	
RFC 3863: Presence Information Data Format	*Shall*	*Shall*	

RFC 3903: SIP Extension for Event State Publication

All devices *shall* support the publication of event state. The reasoning behind this is that some devices will have a user-interface to show contact/buddy lists, and others won't. But even those that have no such UI, need to support the publication protocol so they show up on devices that do.

Compliance to RFC 3903 is not applicable to enterprise based SIP PBXs.

RFC 3856: Presence Event Package

Devices and Networks *shall* support RFC 3856 (Devices and Networks *shall* respond to SUBSCRIBE with NOTIFY. Devices and Networks *may* send SUBSCRIBE messages.)

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 Standard, 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 Standard.

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. The EUF *shall* support UPDATE and PRACK. The EUF *shall*support sending the REGISTER method, and the SCF *shall*support receiving the REGISTER method. The OPTIONS method *should* be supported.

> Note: Though all devices must be able to support the REGISTER method, in specific Enterprise deployments these devices may not actually use the REGISTER method.

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[7] *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: As specified in RFC 3261, the Request-URI in a REGISTER *shall* NOT include "userinfo" including "@".

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

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.

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 to the EUF only if it acts as a UA, i.e. UAC or a UAS, and to the SCF only if it 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 authentication of requests from the EUF to the SCF is required, the EUF and the SCF *shall* support the SIP authentication procedures with 401 (Unauthorized) in accordance with RFC 3261 section 8.1.3.5. If SIP authentication of requests from the EUF to the SCF is not required, support of the SIP authentication procedures with 401 (Unauthorized) is optional. If the support is provided, it *shall* be as specified in RFC 3261 section 8.1.3.5.

Support for the SIP authentication 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 behavior *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.

It is recommended that the EUF on the sending side always include an SDP Offer with the initial INVITE when possible.
Sending an initial INVITE without SDP Offer (a.k.a., delayed Offer/Answer) *shall* only be used when it is not possible to include it, e.g., when interworking with an H.323 network using "slow-start" procedures, and for certain third party call control operations where the characteristics of the media are not yet known.

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.
- Although it is recommended that SDP should only be provided in provisional reliable responses, it is recognized that it may be transmitted in provisional responses that are not transmitted reliably. EUF and SCF SHOULD accept SDP in provisional responses that are not transmitted reliably.

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 Behavior

The SCF *shall* behave in accordance with RFC 3261 section 16.

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, except as noted in this clause. However, clause12 of this Standard takes precedence over RFC 3261 section 18 in case of any conflicts.

- Devices *shall* support TCP and SHOULD support TLS over TCP transport, and *may* support UDP transport for backward compatibility.
    - Using TLS over TCP is the preferred transport for SIP messages, however it is recognized that many SIP devices use UDP, so UDP is also a RECOMMENDED requirement of the Network Edge.

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 be prepared 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 authentication of requests from the EUF to the SCF is required, the EUF *shall* support sending the Authorization header and the SCF *shall* support receiving the Authorization header. If SIP authentication of requests from the EUF to the SCF is not required, support for sending the Authorization header in the EUF and for receiving the Authorization header in the SCF is optional. Support for sending the Authorization header in the SCF and for receiving the Authorization header in the EUF is optional. In all cases, 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.

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 Standard.

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 value *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 authentication of requests from the EUF to the SCF is required, the EUF *shall* support receiving the WWW-Authenticate header and the SCF *shall* support sending the WWW-Authenticate header.

If SIP authentication of requests from the EUF to the SCF is not required, support for receiving the WWW-Authenticate header in the EUF and for sending the WWW-Authenticate header in the SCF is optional. Support for receiving the WWW-Authenticate header in the SCF and for sending the WWW-

Authenticate header in the EUF is optional. In all cases, 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

If SIP authentication is required, HTTP Authentication *shall* be supported as specified in RFC 3261 section 22 although carriers may choose not to activate this. If SIP authentication is not required, support for HTTP Authentication is optional. If the support is provided, it *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. ABNF for the SIP Protocol

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

10.2.1.26. Security Considerations

Devices and Networks *shall* conform to all mandatory provisions of RFC 3261 Section 26, with the following exceptions/clarifications:

- Devices (i.e., TLS Client) *shall* support server-provided certificates (i.e., where TLS Client does not provide a certificate)
- Devices (i.e., TLS Client) *may* support Mutual TLS (i.e., when both TLS client and server provide certificates).
- Network Edge *shall* support TLS over TCP transport and *should* support Mutual TLS, and SHOULD support UDP transport for backward compatibility.
- For NAT traversal, TCP is RECOMMENDED, however, if UDP is used, it *shall* be symmetric RTP.
- Using TLS over TCP is the preferred transport for SIP messages, however it is recognized that many legacy SIP devices use UDP, so UDP is also a RECOMMENDED requirement of the Network Edge.

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, REFER, SUBSCRIBE, NOTIFY and PRACK, and the EUF *shall* support UPDATE, REFER, SUBSCRIBE, AND NOTIFY but *shall* support PRACK in the case that 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.

In the early dialog phase, UPDATE *shall* be used to update session parameters, if supported by the other end. If UPDATE is not supported by the other end, then it is not possible to update session parameters during the early dialog phase.

In the established dialog phase, re-INVITE or UPDATE may be used. It is recommended that the re-INVITE method is deployed for updating the session parameters if user input is desired (e.g., pop-up windows asking if it is ok to change codec, etc.). UPDATE should be used if the intent is that the process does not require user input (e.g., phone-number update).

10.2.2.1.2 REFER

The EUF and the SCF *shall* support the REFER method as specified in RFC3515.

10.2.2.1.3 SUBSCRIBE

The EUF and the SCF *shall* support the SUBSCRIBE method as specified in RFC3265.

10.2.2.1.4 NOTIFY

The EUF and the SCF *shall* support the NOTIFY method as specified in RFC3265.

10.2.2.1.5 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 RFC3262. 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 RFC3262. 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. **It is optional to support this RFC for enterprise networks.**

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. **It is optional to support this RFC for enterprise networks.**

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. **It is optional to support this RFC for enterprise networks.**

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.

10.2.2.2.8. Resource-Priority

The 'Resource-Priority' header field MAY be used by SIP user agents to influence the treatment of SIP requests, including the priority afforded to PSTN calls. The 'Resource-Priority' header field *shall* be supported by the SCF.

10.2.2.2.9. Accept-Resource-Priority

The 'Accept-Resource-Priority' response header field enumerates the resource values (r-values) a SIP user agent server is willing to process.

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 table 4, 5, 6, and 7. Table 8 provides authorization requirements for SIP Methods. Supporting sending or receiving a given SIP methods or headers means that the methods or headers *shall* reliably traverse 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 3 - RFC 3261 methods

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

Table 4 - Extended methods

Method	EUF->SCF		SCF->EUF		Reference	RFC
	EUF Send	SCF Recv	SCF Send	EUF Recv		
NOTIFY	M	M	M	M	See section 10.2.2.1.4	RFC 3265
PRACK	M	M	M	M	See section 10.2.2.1.5	RFC 3262
REFER	M	M	M	M	See section 10.2.2.1.2	RFC 3515
SUBSCRIBE	M	M	M	M	See section 10.2.2.1.3	RFC 3265
UPDATE	M	M	M	M	See section 10.2.2.1.1	RFC 3311

Table 5 - 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

Header	EUF->SCF		SCF->EUF		Reference
	EUF Send	SCF Recv	SCF Send	EUF Recv	
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 6 - Extended headers

Header	EUF->SCF		SCF->EUF		Reference	RFC
	EUF Send	SCF Recv	SCF Send	EUF Recv		
Accept-Resource-Priority	O	M	M	O		RFC 4412
Allow-Events	O	M	M	O		RFC 3265
Event	O	M	M	O		RFC 3265
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	M	M	M	M	See Sub-clause 10.2.2.2.5	RFC 3262
Refer-To	O	M	M	O		RFC 3515
Resource-Priority	O	M	M	O		RFC 4412
RSeq	M	M	M	M	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
Subscription-State	O	M	M	O		RFC 3265

Note: All of the headers in table 6 above are optional for enterprise PBX.

Table 7 - Authentication of SIP Requests

Method	EUF->SCF	SCF->EUF
ACK	N/A	N/A
BYE	C	O
CANCEL	N/A	N/A
INVITE	C	O
NOTIFY	C	O
OPTIONS	C	O
REFER	C	O
REGISTER	C	O
PRACK	C	O
SUBSCRIBE	C	O
UPDATE	C	O

C: Conditional mandatory when SIP authorization of requests from the EUF to the SCF is required, otherwise optional.

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

Table 8 - Definitions for M, O, and N/A

Code	Code name	EUF->SCF		SCF->EUF	
		EUF Send	SCF Recv	SCF Send	EUF Recv
M	Mandatory	The capability *shall* be supported. The EUF *shall* be able to send if required.	The capability *shall* be supported. 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 MUST 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. Processing should not continue if required information is unavailable. (Suitable disconnection/release processing should be performed.) However, when a default value has been decided upon, processing is performed using the default value.	The capability *shall* be supported. Supporting sending of a SIP message or header in the SCF at the UNI means that this message or header MUST be processed, and the appropriate response sent 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. Processing should not continue if required information is unavailable. (Suitable disconnection/release processing should be performed.) However, when a default value has been decided upon, processing is performed using the default value.
O	Optional	The capability may 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. If possible, the processing expected by the EUF on the sending side should be performed. 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. If possible, the processing expected by the SCF on the sending side should be performed. When the processing expected by the SCF on the sending side cannot be performed, the received content should be ignored and processing should continue.
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

This section 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, and O have the same meanings as in table 8.

Note: SDP requirements are also discussed in sections 7 and 10.1. Section 7 provides detailed requirements for when the originating and terminating UA will begin sending and receiving media packets, while the Media Description table in Section 10.1 specifies the basic requirement for support of RFC 4566: SPD.

10.3.1 SDP Usage

Table 9 - SDP Usage

Item	UA->Network		Network->UA	
	UA Send	Network Recv	Network Send	UA 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)	O	M	O	M
C1: At least one of the c lines in session and media descriptions *shall* be implemented. C2: If media description is implemented, both m and c lines *shall* be implemented. 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: 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 the c line. When the c line is included in the session description, the c line in the media description may not be included.

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

This section is normative.

11.1 Specifications to be Supported

Table 10 - Transport Specifications

RTP			
RFC 3550: RTP	see text	see text	Fundamental media protocol
RFC 3551: RTP Profile	*Shall*	*Shall*	Fundamental audio media protocol
RFC 4733: RTP Payload for DTMF	see text	see text	Standard method for DTMF
RFC 3711: Secure RTP	*Shall*	*Shall*	Media encryption
RFC 4568: SDESCRIPTIONS	*Shall*	*Shall*	Key negotiation necessary for RFC 3711
RFC 4961: Symmetric RTP	*Shall*	*Shall*	

RFC 3550: RTP

Devices and Networks *shall* conform to all mandatory provisions of RFC 3550

SIP telephony devices *shall* be able to limit the ports used for RTP to a provisioned range.

RFC 4733: RTP Payload for DTMF

Devices and Networks *shall* support Table 3, Section 3.2 and Sections 2.2, 2.3, and 3.2 of RFC 4733*.* Devices and Networks *shall* not interpret in-band (in-the-clear) DTMF audio tones. This places specific requirements on PSTN gateways and terminal adapters, which both operate on RTP audio on one side and non-RTP audio on the other. PSTN gateways and terminal adapters *shall* detect RFC 4733 payloads from the RTP side and generate DTMF audio tones on the non-RTP side and, conversely, 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.

11.2 DTMF Tone Handling

The SCF and the EUF including User Agent *shall* support the specific part of RFC 4733 in order to transport DTMF events.

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.

11.3 Fax and Modem Support

The SCF *shall* support the Internet Fax Protocol (IFP), as specified in ITU-T T.38. The SCF *shall* also support inband fax and modem calls, which includes passing relevant fax and modem tones as described in RFC 4733. Fax and modem support by the EUF and by enterprise networks is optional.

12 CALL CONTROL SIGNALING TRANSPORT

This section is normative.

Table 11 - Call Control Signaling Transport Specifications

Transport			
QoS / Priority	see text	see text	
RFC 2401: (IPSec) Security Architecture for IP	*Should*	*Shall*See text	
RFC 2246: TLS Protocol Version 1.0	*Shall*	*Shall*See text	
RFC 1321: The MD5 Message-Digest Algorithm (see text for RFC 1312)	*Shall*	*Shall*	
Mutual TLS optional package in RFC 2246 (see text for RFC 2246)	*May*	*May*	

RFC 1321: The MD5 Message-Digest Algorithm

RFC 1321 is not generally applicable to enterprise based devices.

RFC 2401: (IPSec) Security Architecture for IP

RFC 2401 is optional for enterprise networks.

RFC 2246: TLS Protocol Version 1.0

For SIP messages transported over TCP, Devices and Networks *shall* conform to all mandatory provisions of RFC 2246. Although TLS must be implemented, it may not always be used.

13 IP PROTOCOL VERSION

This section is normative.

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 which only supports IPv4, the EUF may only support IPv6.

14 SIP UA CONFIGURATION

This section is normative.

Table 12 - SIP UA Configuration

SIP UA Configuration			
RFC 4504: SIP Device Requirements and Configuration	see text	see text	
Device bootstrapping mechanisms	see text	see text	

RFC 4504: SIP Device Requirements and Configuration

SIP telephony devices will generally be controlled in the Enterprise by the SIP PBX. Devices and Networks *shall* conform to all mandatory provisions of RFC 4504 with the following exceptions:

- Replace
  - Req-61: “SIP telephony devices *must* be able to password protect configuration information and administrative functions.”
- With:
  - Req-61: “SIP telephony devices *must* be able to protect (by password or other means) configuration information and administrative functions.”
- Req-71, Req-72, Req-73, Req-74 and Req-75 are not required for conformance to this Profile. (Section 4.1.20 addresses codec requirements for this Profile).
- The user-to-device interface is out-of-scope for this Profile, and therefore such requirements in RFC 4504 are not required for conformance to this Profile, including: Req-40, Req-55, Req-62 and Req-91.
- Also out-of-scope and not required for conformance to this Profile are Req-83 and Req-85.

Device bootstrapping mechanisms

This is for further study.

15 FIREWALLS, NAT TRAVERSAL CONSIDERATIONS

This section is normative.

Table 13 - Firewall/NAT Traversal

Firewall/NAT Traversal			
RFC 3489: STUN	*Shall*[1]	*Shall*[1]	
draft-ietf-mmusic-ice-15	*Should*	*Should*	

16 QOS CONSIDERATIONS

This section is normative.

QoS / Priority

Devices and Networks with Wi-Fi connections *shall* support WiFi Alliance WiFi Multimedia version 1.1.

Devices and Networks with Ethernet connections *should* support 802.1q [Virtual LAN tags].

17 SECURITY CONSIDERATIONS

This section is normative.

Signaling *should* be secure and media may be secure.