SIP Telephony Device Requirements and Configuration

Status of This Memo

Copyright Notice

Abstract

   This document describes the requirements for SIP telephony devices,
   based on the deployment experience of large numbers of SIP phones and
   PC clients using different implementations in various networks. The
   objectives of the requirements are a well-defined set of
   interoperability and multi-vendor-supported core features, so as to
   enable similar ease of purchase, installation, and operation as found
   for PCs, PDAs, analog feature phones or mobile phones.

   We present a glossary of the most common settings and some of the
   more widely used values for some settings.

Table of Contents

1. Introduction

   This document has the objective of focusing the Internet
   communications community on requirements for telephony devices using
   SIP.

   We base this information from developing and using a large number of
   SIP telephony devices in carrier and private IP networks and on the
   Internet. This deployment has shown the need for generic
   requirements for SIP telephony devices and also the need for some
   specifics that can be used in SIP interoperability testing.

   SIP telephony devices, also referred to as SIP User Agents (UAs), can
   be any type of IP networked computing user device enabled for SIP-
   based IP telephony. SIP telephony user devices can be SIP phones,
   adaptors for analog phones and for fax machines, conference
   speakerphones, software packages (soft clients) running on PCs,
   laptops, wireless connected PDAs, 'Wi-Fi' SIP mobile phones, as well
   as other mobile and cordless phones that support SIP signaling for
   real-time communications. SIP-PSTN gateways are not the object of
   this memo, since they are network elements and not end user devices.

   SIP telephony devices can also be instant messaging (IM) applications
   that have a telephony option.

   SIP devices MAY support various other media besides voice, such as
   text, video, games, and other Internet applications; however, the
   non-voice requirements are not specified in this document, except
   when providing enhanced telephony features.

   SIP telephony devices are highly complex IP endpoints that speak many
   Internet protocols, have audio and visual interfaces, and require
   functionality targeted at several constituencies: (1) end users, (2)
   service providers and network administrators, (3) manufacturers, and
   (4) system integrators.

   The objectives of the requirements are a well-defined set of
   interoperability and multi-vendor-supported core features, so as to
   enable similar ease of purchase, installation, and operation as found
   for standard PCs, analog feature phones, or mobile phones. Given the
   cost of some feature-rich display phones may approach the cost of PCs
   and PDAs, similar or even better ease of use as compared to personal
   computers and networked PDAs is expected by both end users and
   network administrators.

   While some of the recommendations of this document go beyond what is
   currently mandated for SIP implementations within the IETF, this is
   believed necessary to support the specified operational objectives.

However, it is also important to keep in mind that the SIP
specifications are constantly evolving; thus, these recommendations
need to be considered in the context of that change and evolution.
Due to the evolution of IETF documents in the standards process, and
the informational nature of this memo, the references are all
informative.

1.1. Conventions used in this document

This document is informational and therefore the key words "MUST",
"SHOULD", "SHOULD NOT", and "MAY", in this document are not to be
interpreted as described in RFC 2119 [1], but rather indicate the
nature of the suggested requirement.

2. Generic Requirements

We present here a minimal set of requirements that MUST be met by all
SIP [2] telephony devices, except where SHOULD or MAY is specified.

2.1. SIP Telephony Devices

This memo applies mainly to desktop phones and other special purpose
SIP telephony hardware. Some of the requirements in this section are
not applicable to PC/laptop or PDA software phones (soft phones) and
mobile phones.

    Req-1: SIP telephony devices MUST be able to acquire IP network
           settings by automatic configuration using Dynamic Host
           Configuration Protocol (DHCP) [3].

    Req-2: SIP telephony devices MUST be able to acquire IP network
           settings by manual entry of settings from the device.

    Req-3: SIP telephony devices SHOULD support IPv6. Some newer
           wireless networks may mandate support for IPv6 and in such
           networks SIP telephony devices MUST support IPv6.

    Req-4: SIP telephony devices MUST support the Simple Network Time
           Protocol [4].

    Req-5: Desktop SIP phones and other special purpose SIP telephony
           devices MUST be able to upgrade their firmware to support
           additional features and the functionality.

    Req-6: Users SHOULD be able to upgrade the devices with no special
           applications or equipment; or a service provider SHOULD be
           able to push the upgrade down to the devices remotely.

2.2. DNS and ENUM Support

   Req-7: SIP telephony devices MUST support RFC 3263 [5] for locating a
          SIP server and selecting a transport protocol.

   Req-8: SIP telephony devices MUST incorporate DNS resolvers that are
          configurable with at least two entries for DNS servers for
          redundancy. To provide efficient DNS resolution, SIP
          telephony devices SHOULD query responsive DNS servers and skip
          DNS servers that have been non-responsive to recent queries.

   Req-9: To provide efficient DNS resolution and to limit post-dial
          delay, SIP telephony devices MUST cache DNS responses based on
          the DNS time-to-live.

   Req-10: For DNS efficiency, SIP telephony devices SHOULD use the
           additional information section of the DNS response instead of
           generating additional DNS queries.

   Req-11: SIP telephony devices MAY support ENUM [6] in case the end
           users prefer to have control over the ENUM lookup. Note: The
           ENUM resolver can also be placed in the outgoing SIP proxy to
           simplify the operation of the SIP telephony device. The
           Extension Mechanisms for DNS (EDNSO) in RFC 2671 SHOULD also
           be supported.

2.3. SIP Device Resident Telephony Features

   Req-12: SIP telephony devices MUST support RFC 3261 [2].

   Req-13: SIP telephony devices SHOULD support the SIP Privacy header
           by populating headers with values that reflect the privacy
           requirements and preferences as described in "User Agent
           Behavior", Section 4 of RFC 3323 [7].

   Req-14: SIP telephony devices MUST be able to place an existing call
           on hold, and initiate or receive another call, as specified
           in RFC 3264 [8] and SHOULD NOT omit the sendrecv attribute.

   Req-15: SIP telephony devices MUST provide a call waiting indicator.
           When participating in a call, the user MUST be alerted
           audibly and/or visually of another incoming call. The user
           MUST be able to enable/disable the call waiting indicator.

   Req-16: SIP telephony devices MUST support SIP message waiting [9]
           and the integration with message store platforms.

   Req-17: SIP telephony devices MAY support a local dial plan. If a
           dial plan is supported, it MUST be able to match the user
           input to one of multiple pattern strings and transform the
           input to a URI, including an arbitrary scheme and URI
           parameters.

   Example: If a local dial plan is supported, it SHOULD be configurable
   to generate any of the following URIs when "5551234" is dialed:

   tel:+12125551234
   sip:+12125551234@example.net;user=phone
   sips:+12125551234@example.net;user=phone
   sip:5551234@example.net
   sips:5551234@example.net
   tel:5551234;phone-context=nyc1.example.net
   sip:5551234;phone-
   context=nyc1.example.net@example.net;user=phone
   sips:5551234;phone-
   context=nyc1.example.net@example.net;user=phone
   sip:5551234;phone-
   context=nyc1.example.net@example.net;user=dialstring
   sips:5551234;phone-
   context=nyc1.example.net@example.net;user=dialstring
   tel:5551234;phone-context=+1212
   sip:5551234;phone-context=+1212@example.net;user=phone
   sips:5551234;phone-context=+1212@example.net;user=phone
   sip:5551234;phone-context=+1212@example.net;user=dialstring
   sips:5551234;phone-context=+1212@example.net;user=dialstring

   If a local dial plan is not supported, the device SHOULD be
   configurable to generate any of the following URIs when "5551234" is
   dialed:

   sip:5551234@example.net
   sips:5551234@example.net
   sip:5551234;phone-
   context=nyc1.example.net@example.net;user=dialstring
   sips:5551234;phone-
   context=nyc1.example.net@example.net;user=dialstring
   sip:5551234;phone-context=+1212@example.net;user=dialstring
   sips:5551234;phone-context=+1212@example.net;user=dialstring"

   Req-18: SIP telephony devices MUST support URIs for telephone numbers
           as per RFC 3966 [10]. This includes the reception as well as
           the sending of requests. The reception may be denied
           according to the configurable security policy of the device.
           It is a reasonable behavior to send a request to a
           preconfigured outbound proxy.

   Req-19: SIP telephony devices MUST support REFER and NOTIFY for call
           transfer [11], [12]. SIP telephony devices MUST support
           escaped Replaces-Header (RFC 3891) and SHOULD support other
           escaped headers in the Refer-To header.

   Req-20: SIP telephony devices MUST support the unattended call
           transfer flows as defined in [12].

   Req-21: SIP telephony devices MUST support the attended call transfer
           as defined in [12].

   Req-22: SIP telephony devices MAY support device-based 3-way calling
           by mixing the audio streams and displaying the interactive
           text of at least 2 separate calls.

   Req-23: SIP telephony devices MUST be able to send dual-tone multi-
           frequency (DTMF) named telephone events as specified by RFC
           2833 [13].

   Req-24: Payload type negotiation MUST comply with RFC 3264 [8] and
           with the registered MIME types for RTP payload formats in RFC
           3555 [14].

   Req-25: The dynamic payload type MUST remain constant throughout the
           session. For example, if an endpoint decides to renegotiate
           codecs or put the call on hold, the payload type for the re-
           invite MUST be the same as the initial payload type. SIP
           devices MAY support Flow Identification as defined in RFC
           3388 [15].

   Req-26: When acting as a User Agent Client (UAC), SIP telephony
           devices SHOULD support the gateway model of RFC 3960 [16].
           When acting as a User Agent Server (UAS), SIP telephony
           devices SHOULD NOT send early media.

   Req-27: SIP telephony devices MUST be able to handle multiple early
           dialogs in the context of request forking. When a confirmed
           dialog has been established, it is an acceptable behavior to
           send a BYE request in response to additional 2xx responses
           that establish additional confirmed dialogs.

   Req-28: SIP devices with a suitable display SHOULD support the call-
           info header and depending on the display capabilities MAY,
           for example, display an icon or the image of the caller.

   Req-29: To provide additional information about call failures, SIP
           telephony devices with a suitable display MUST render the
           "Reason Phrase" of the SIP message or map the "Status Code"
           to custom or default messages. This presumes the language
           for the reason phrase is the same as the negotiated language.
           The devices MAY use an internal "Status Code" table if there
           was a problem with the language negotiation.

   Req-30: SIP telephony devices MAY support music on hold, both in
           receive mode and locally generated. See also "SIP Service
           Examples" for a call flow with music on hold [17].

   Req-31: SIP telephony devices MAY ring after a call has been on hold
           for a predetermined period of time, typically 3 minutes.

2.4. Support for SIP Services

   Req-32: SIP telephony devices MUST support the SIP Basic Call Flow
           Examples as per RFC 3665 [17].

   Req-33: SIP telephony devices MUST support the SIP-PSTN Service
           Examples as per RFC 3666 [18].

   Req-34: SIP telephony devices MUST support the Third Party Call
           Control model [19], in the sense that they may be the
           controlled device.

   Req-35: SIP telephony devices SHOULD support SIP call control and
           multi-party usage [20].

   Req-36: SIP telephony devices SHOULD support conferencing services
           for voice [21], [22] and interactive text [23] and if
           equipped with an adequate display MAY also support instant
           messaging (IM) and presence [24], [25].

   Req-37: SIP telephony devices SHOULD support the indication of the
           User Agent capabilities and MUST support the caller
           capabilities and preferences as per RFC 3840 [26].

   Req-38: SIP telephony devices MAY support service mobility: Devices
           MAY allow roaming users to input their identity so as to have
           access to their services and preferences from the home SIP
           server. Examples of user data to be available for roaming
           users are: user service ID, dialing plan, personal directory,
           and caller preferences.

2.5. Basic Telephony and Presence Information Support

   The large color displays in some newer models make such SIP phones
   and applications attractive for a rich communication environment.
   This document is focused, however, only on telephony-specific
   features enabled by SIP Presence and SIP Events.

   SIP telephony devices can also support presence status, such as the
   traditional Do Not Disturb, new event state-based information, such
   as being in another call or being in a conference, typing a message,
   emoticons, etc. Some SIP telephony User Agents can support, for
   example, a voice session and several IM sessions with different
   parties.

   Req-39: SIP telephony devices SHOULD support Presence information
           [24] and SHOULD support the Rich Presence Information Data
           Format [27] for the new IP communication services enabled by
           Presence.

   Req-40: Users MUST be able to set the state of the SIP telephony
           device to "Do Not Disturb", and this MAY be manifested as a
           Presence state across the network if the UA can support
           Presence information.

   Req-41: SIP telephony devices with "Do Not Disturb" enabled MUST
           respond to new sessions with "486 Busy Here".

2.6. Emergency and Resource Priority Support

   Req-42: Emergency calling: For emergency numbers (e.g., 911, SOS
           URL), SIP telephony devices SHOULD support the work of the
           ECRIT WG [28].

   Req-43: Priority header: SIP devices SHOULD support the setting by
           the user of the Priority header specified in RFC 3261 for
           such applications as emergency calls or for selective call
           acceptance.

   Req-44: Resource Priority header: SIP telephony devices that are used
           in environments that support emergency preparedness MUST also
           support the sending and receiving of the Resource-Priority
           header as specified in [29]. The Resource Priority header
           influences the behavior for message routing in SIP proxies
           and PSTN telephony gateways and is different from the SIP
           Priority header specified in RFC 3261. Users of SIP
           telephony devices may want to be interrupted in their lower-
           priority communications activities if such an emergency
           communication request arrives.

Note: As of this writing, we recommend that implementers follow the
work of the Working Group on Emergency Context Resolution with
Internet Technologies (ecrit) in the IETF. The complete solution is
for further study at this time. There is also work on the
requirements for location conveyance in the SIPPING WG, see [30].

2.7. Multi-Line Requirements

A SIP telephony device can have multiple lines: One SIP telephony
device can be registered simultaneously with different SIP registrars
from different service providers, using different names and
credentials for each line. The different sets of names and
credentials are also called 'SIP accounts'. The "line" terminology
has been borrowed from multi-line PSTN/PBX phones, except that for
SIP telephony devices there can be different SIP registrars/proxies
for each line, each of which may belong to a different service
provider, whereas this would be an exceptional case for the PSTN and
certainly not the case for PBX phones. Multi-line SIP telephony
devices resemble more closely e-mail clients that can support several
e-mail accounts.

Note: Each SIP account can usually support different Addresses of
Record (AORs) with a different list of contact addresses (CAs), as
may be convenient, for example, when having different SIP accounts
for business and personal use. However, some of the CAs in different
SIP accounts may point to the same devices.

Req-45: Multi-line SIP telephony devices MUST support a unique
        authentication username, authentication password, registrar,
        and identity to be provisioned for each line. The
        authentication username MAY be identical with the user name
        of the AOR and the domain name MAY be identical with the host
        name of the registrar.

Req-46: Multi-line SIP telephony devices MUST be able to support the
        state of the client to Do Not Disturb on a per line basis.

Req-47: Multi-line SIP telephony devices MUST support multi-line call
        waiting indicators. Devices MUST allow the call waiting
        indicator to be set on a per line basis.

Req-48: Multi-line SIP telephony devices MUST be able to support a
        few different ring tones for different lines. We specify
        here "a few", since provisioning different tones for all
        lines may be difficult for phones with many lines.

2.8. User Mobility

   The following requirements allow users with a set of credentials to
   use any SIP telephony device that can support personal credentials
   from several users, distinct from the identity of the device.

   Req-49: User-mobility-enabled SIP telephony devices MUST store static
           credentials associated with the device in non-volatile
           memory. This static profile is used during the power up
           sequence.

   Req-50: User-mobility-enabled SIP telephony devices SHOULD allow a
           user to walk up to a device and input their personal
           credentials. All user features and settings stored in home
           SIP proxy and the associated policy server SHOULD be
           available to the user.

   Req-51: User-mobility-enabled SIP telephony devices registered as
           fixed desktop with network administrator MUST use the local
           static location data associated with the device for emergency
           calls.

2.9. Interactive Text Support

   SIP telephony devices supporting instant messaging based on SIMPLE
   [24] support text conversation based on blocks of text. However,
   continuous interactive text conversation may be sometimes preferred
   as a parallel to voice, due to its interactive and more streaming-
   like nature, and thus is more appropriate for real-time conversation.
   It also allows for text captioning of voice in noisy environments and
   for those who cannot hear well or cannot hear at all.

   Finally, continuous character-by-character text is preferred by
   emergency and public safety programs (e.g., 112 and 911) because of
   its immediacy, efficiency, lack of crossed messages problem, better
   ability to interact with a confused person, and the additional
   information that can be observed from watching the message as it is
   composed.

   Req-52: SIP telephony devices such as SIP display phones and IP-
           analog adapters SHOULD support the accessibility requirements
           for deaf, hard-of-hearing and speech-impaired individuals as
           per RFC 3351 [31] and also for interactive text conversation
           [23], [32].

Req-53: SIP telephony devices SHOULD provide a way to input text and
        to display text through any reasonable method. Built-in user
        interfaces, standard wired or wireless interfaces, and/or
        support for text through a web interface are all considered
        reasonable mechanisms.

Req-54: SIP telephony devices SHOULD provide an external standard
        wired or wireless link to connect external input (keyboard,
        mouse) and display devices.

Req-55: SIP telephony devices that include a display, or have a
        facility for connecting an external display, MUST include
        protocol support as described in RFC 4103 [23] for real-time
        interactive text.

Req-56: There may be value in having RFC 4103 support in a terminal
        also without a visual display. A synthetic voice output for
        the text conversation may be of value for all who can hear,
        and thereby provides the opportunity to have a text
        conversation with other users.

Req-57: SIP telephony devices MAY provide analog adaptor
        functionality through an RJ-11 FXS port to support FXS
        devices. If an RJ-11 (FXS) port is provided, then it MAY
        support a gateway function from all text-telephone protocols
        according to ITU-T Recommendation V.18 to RFC 4103 text
        conversation (in fact, this is encouraged in the near term
        during the transition to widespread use of SIP telephony
        devices). If this gateway function is not included or fails,
        the device MUST pass through all text-telephone protocols
        according to ITU-T Recommendation V.18, November 2000, in a
        transparent fashion.

Req-58: SIP telephony devices MAY provide a 2.5 mm audio port, in
        portable SIP devices, such as PDAs and various wireless SIP
        phones.

2.10. Other Related Protocols

Req-59: SIP telephony devices MUST support the Real-Time Protocol and
        the Real-Time Control Protocol, RFC 3550 [33]. SIP devices
        SHOULD use RTCP Extended Reports for logging and reporting on
        network support for voice quality, RFC 3611 [34] and MAY also
        support the RTCP summary report delivery [35].

2.11. SIP Device Security Requirements

   Req-60: SIP telephony devices MUST support digest authentication as
           per RFC 3261. In addition, SIP telephony devices MUST
           support Transport Layer Security (TLS) for secure transport
           [36] for scenarios where the SIP registrar is located outside
           the secure, private IP network in which the SIP UA may
           reside. Note: TLS need not be used in every call, though.

   Req-61: SIP telephony devices MUST be able to password protect
           configuration information and administrative functions.

   Req-62: SIP telephony devices MUST NOT display the password to the
           user or administrator after it has been entered.

   Req-63: SIP clients MUST be able to disable remote access, i.e.,
           block incoming Simple Network Management Protocol (SNMP)
           (where this is supported), HTTP, and other services not
           necessary for basic operation.

   Req-64: SIP telephony devices MUST support the option to reject an
           incoming INVITE where the user-portion of the SIP request URI
           is blank or does not match a provisioned contact. This
           provides protection against war-dialer attacks, unwanted
           telemarketing, and spam. The setting to reject MUST be
           configurable.

   Req-65: When TLS is not used, SIP telephony devices MUST be able to
           reject an incoming INVITE when the message does not come from
           the proxy or proxies where the client is registered. This
           prevents callers from bypassing terminating call features on
           the proxy. For DNS SRV specified proxy addresses, the client
           must accept an INVITE from all of the resolved proxy IP
           addresses.

2.12. Quality of Service

   Req-66: SIP devices MUST support the IPv4 Differentiated Services
           Code Point (DSCP) field for RTP streams as per RFC 2597 [37].
           The DSCP setting MUST be configurable to conform with the
           local network policy.

   Req-67: If not specifically provisioned, SIP telephony devices SHOULD
           mark RTP packets with the recommended DSCP for expedited
           forwarding (codepoint 101110) and mark SIP packets with DSCP
           AF31 (codepoint 011010).

   Req-68: SIP telephony devices MAY support Resource Reservation
           Protocol (RSVP) [38].

2.13. Media Requirements

   Req-69: To simplify the interoperability issues, SIP telephony
           devices MUST use the first matching codec listed by the
           receiver if the requested codec is available in the called
           device. See the offer/answer model in RFC 3261.

   Req-70: To reduce overall bandwidth, SIP telephony devices MAY
           support active voice detection and comfort noise generation.

2.14. Voice Codecs

   Internet telephony devices face the problem of supporting multiple
   codecs due to various historic reasons, on how telecom industry
   players have approached codec implementations and the serious
   intellectual property and licensing problems associated with most
   codec types. For example, RFC 3551 [39] lists 17 registered MIME
   subtypes for audio codecs.

   Ideally, the more codecs can be supported in a SIP telephony device,
   the better, since it enhances the chances of success during the codec
   negotiation at call setup and avoids media intermediaries used for
   codec mediation.

   Implementers interested in a short list MAY, however, support a
   minimal number of codecs used in wireline Voice over IP (VoIP), and
   also codecs found in mobile networks for which the SIP UA is
   targeted. An ordered short list of preferences may look as follows:

   Req-71: SIP telephony devices SHOULD support Audio/Video Transport
           (AVT) payload type 0 (G.711 uLaw) as in [40] and its Annexes
           1 and 2.

   Req-72: SIP telephony devices SHOULD support the Internet Low Bit
           Rate codec (iLBC) [41], [42].

   Req-73: Mobile SIP telephony devices MAY support codecs found in
           various wireless mobile networks. This can avoid codec
           conversion in network-based intermediaries.

   Req-74: SIP telephony devices MAY support a small set of special
           purpose codecs, such as G.723.1, where low bandwidth usage is
           needed (for dial-up Internet access), Speex [43], or G.722
           for high-quality audio conferences.

   Req-75: SIP telephony devices MAY support G.729 and its annexes.
           Note: The G.729 codec is included here for backward
           compatibility only, since the iLBC and the G.723.1 codecs are
           preferable in bandwidth-constrained environments.

           Note: The authors believe the Internet Low Bit Rate codec
           (iLBC) should be the default codec for Internet telephony.

           A summary count reveals up to 25 and more voice codec types
           currently in use. The authors believe there is also a need
           for a single multi-rate Internet codec, such as Speex or
           similar that can effectively be substituted for all of the
           multiple legacy G.7xx codec types, such as G.711, G.729,
           G.723.1, G.722, etc., for various data rates, thus avoiding
           the complexity and cost to implementers and service providers
           alike who are burdened by supporting so many codec types,
           besides the licensing costs.

2.15. Telephony Sound Requirements

   Req-76: SIP telephony devices SHOULD comply with the handset receive
           comfort noise requirements outlined in the ANSI standards
           [44], [45].

   Req-77: SIP telephony devices SHOULD comply with the stability or
           minimum loss defined in ITU-T G.177.

   Req-78: SIP telephony devices MAY support a full-duplex speakerphone
           function with echo and side tone cancellation. The design of
           high-quality side tone cancellation for desktop IP phones,
           laptop computers, and PDAs is outside the scope of this memo.

   Req-79: SIP telephony device MAY support different ring tones based
           on the caller identity.

2.16. International Requirements

   Req-80: SIP telephony devices SHOULD indicate the preferred language
           [46] using User Agent capabilities [26].

   Req-81: SIP telephony devices intended to be used in various language
           settings MUST support other languages for menus, help, and
           labels.

2.17. Support for Related Applications

   The following requirements apply to functions placed in the SIP
   telephony device.

   Req-82: SIP telephony devices that have a large display and support
           presence SHOULD display a buddy list [24].

   Req-83: SIP telephony devices MAY support Lightweight Directory
           Access Protocol (LDAP) for client-based directory lookup.

   Req-84: SIP telephony devices MAY support a phone setup where a URL
           is automatically dialed when the phone goes off-hook.

2.18. Web-Based Feature Management

   Req-85: SIP telephony devices SHOULD support an internal web server
           to allow users the option to manually configure the phone and
           to set up personal phone applications such as the address
           book, speed-dial, ring tones, and, last but not least, the
           call handling options for the various lines and aliases, in a
           user-friendly fashion. Web pages to manage the SIP telephony
           device SHOULD be supported by the individual device, or MAY
           be supported in managed networks from centralized web servers
           linked from a URI.

           Managing SIP telephony devices SHOULD NOT require special
           client software on the PC or require a dedicated management
           console. SIP telephony devices SHOULD support https
           transport for this purpose.

           In addition to the Web Based Feature Management requirement,
           the device MAY have an SNMP interface for monitoring and
           management purposes.

2.19. Firewall and NAT Traversal

   The following requirements allow SIP clients to properly function
   behind various firewall architectures.

   Req-86: SIP telephony devices SHOULD be able to operate behind a
           static Network Address Translation/Port Address Translation
           (NAPT) device. This implies the SIP telephony device SHOULD
           be able to 1) populate SIP messages with the public, external
           address of the NAPT device; 2) use symmetric UDP or TCP for
           signaling; and 3) use symmetric RTP [47].

      Req-87: SIP telephony devices SHOULD support the Simple Traversal of
              UDP through NATs (STUN) protocol [48] for determining the
              NAPT public external address. A classification of scenarios
              and NATs where STUN is effective is reported in [49].
              Detailed call flows for interactive connectivity
              establishment (ICE) [50] are given in [51].

              Note: Developers are strongly advised to follow the document
              on best current practices for NAT traversal for SIP [51].

      Req-88: SIP telephony devices MAY support UPnP (http://www.upnp.org/)
              for local NAPT traversal. Note that UPnP does not help if
              there is NAPT in the network of the service provider.

      Req-89: SIP telephony devices MUST be able to limit the ports used
              for RTP to a provisioned range.

2.20. Device Interfaces

      Req-90: SIP telephony devices MUST support two types of addressing
              capabilities, to enable end users to "dial" either phone
              numbers or URIs.

      Req-91: SIP telephony devices MUST have a telephony-like dial-pad and
              MAY have telephony-style buttons such as mute, redial,
              transfer, conference, hold, etc. The traditional telephony
              dial-pad interface MAY appear as an option in large-screen
              telephony devices using other interface models, such as
              Push-To-Talk in mobile phones and the Presence and IM
              graphical user interface (GUI) found in PCs, PDAs, mobile
              phones, and cordless phones.

      Req-92: SIP telephony devices MUST have a convenient way for entering
              SIP URIs and phone numbers. This includes all alphanumeric
              characters allowed in legal SIP URIs. Possible approaches
              include using a web page, display and keyboard entry, type-
              ahead, or graffiti for PDAs.

      Req-93: SIP telephony devices should allow phone number entry in
              human-friendly fashion, with the usual separators and
              brackets between digits and digit groups.

3. Glossary and Usage for the Configuration Settings

   SIP telephony devices are quite complex, and their configuration is
   made more difficult by the widely diverse use of technical terms for
   the settings. We present here a glossary of the most common settings
   and some of the more widely used values for some settings.

   Settings are the information on a SIP UA that it needs so as to be a
   functional SIP endpoint. The settings defined in this document are
   not intended to be a complete listing of all possible settings. It
   MUST be possible to add vendor-specific settings.

   The list of available settings includes settings that MUST, SHOULD,
   or MAY be used by all devices (when present) and that make up the
   common denominator that is used and understood by all devices.
   However, the list is open to vendor-specific extensions that support
   additional settings, which enable a rich and valuable set of
   features.

   Settings MAY be read-only on the device. This avoids the
   misconfiguration of important settings by inexperienced users
   generating service cost for operators. The settings provisioning
   process SHOULD indicate which settings can be changed by the end user
   and which settings should be protected.

   In order to achieve wide adoption of any settings format, it is
   important that it should not be excessive in size for modest devices
   to use it. Any format SHOULD be structured enough to allow flexible
   extensions to it by vendors. Settings may belong to the device or to
   a SIP service provider and the Address of Record (AOR) registered
   there. When the device acts in the context of an AOR, it will first
   try to look up a setting in the AOR context. If the setting cannot
   be found in that context, the device will try to find the setting in
   the device context. If that also fails, the device MAY use a default
   value for the setting.

   The examples shown here are just of informational nature. Other
   documents may specify the syntax and semantics for the respective
   settings.

3.1. Device ID

   A device setting MAY include some unique identifier for the device it
   represents. This MAY be an arbitrary device name chosen by the user,
   the MAC address, some manufacturer serial number, or some other
   unique piece of data. The Device ID SHOULD also indicate the ID
   type.
   Example: DeviceId="000413100A10;type=MAC"

3.2. Signaling Port

   The port that will be used for a specific transport protocol for SIP
   MAY be indicated with the SIP ports setting. If this setting is
   omitted, the device MAY choose any port within a range as specified
   in 3.3. For UDP, the port may also be used for sending requests so
   that NAT devices will be able to route the responses back to the UA.
   Example: SIPPort="5060;transport=UDP"

3.3. RTP Port Range

   A range of port numbers MUST be used by a device for the consecutive
   pairs of ports that MUST be used to receive audio and control
   information (RTP and RTCP) for each concurrent connection. Sometimes
   this is required to support firewall traversal, and it helps network
   operators to identify voice packets.
   Example: RTPPorts="50000-51000"

3.4. Quality of Service

   The Quality of Service (QoS) settings for outbound packets SHOULD be
   configurable for network packets associated with call signaling (SIP)
   and media transport (RTP/RTCP). These settings help network
   operators in identifying voice packets in their network and allow
   them to transport them with the required QoS. The settings are
   independently configurable for the different transport layers and
   signaling, media, or administration. The QoS settings SHOULD also
   include the QoS mechanism.

   For both categories of network traffic, the device SHOULD permit
   configuration of the type of service settings for both layer 3 (IP
   DiffServ) and layer 2 (for example, IEEE 802.1D/Q) of the network
   protocol stack.
   Example: RTPQoS="0xA0;type=DiffSrv,5;type=802.1DQ;vlan=324"

3.5. Default Call Handling

   All of the call handling settings defined below can be defined here
   as default behaviors.

3.5.1. Outbound Proxy

   The outbound proxy for a device MAY be set. The setting MAY require
   that all signaling packets MUST be sent to the outbound proxy or that
   only in the case when no route has been received the outbound proxy
   MUST be used. This ensures that application layer gateways are in

the signaling path. The second requirement allows the optimization
of the routing by the outbound proxy.
Example: OutboundProxy="sip:nat.proxy.com"

3.5.2. Default Outbound Proxy

The default outbound proxy SHOULD be a global setting (not related to
a specific line).
Example: DefaultProxy="sip:123@proxy.com"

3.5.3. SIP Session Timer

The re-invite timer allows User Agents to detect broken sessions
caused by network failures. A value indicating the number of seconds
for the next re-invite SHOULD be used if provided.
Example: SessionTimer="600;unit=seconds"

3.6. Telephone Dialing Functions

As most telephone users are used to dialing digits to indicate the
address of the destination, there is a need for specifying the rule
by which digits are transformed into a URI (usually SIP URI or TEL
URI).

3.6.1. Phone Number Representations

SIP phones need to understand entries in the phone book of the most
common separators used between dialed digits, such as spaces, angle
and round brackets, dashes, and dots.
Example: A phonebook entry of "+49(30)398.33-401" should be
translated into "+493039833401".

3.6.2. Digit Maps and/or the Dial/OK Key

A SIP UA needs to translate user input before it can generate a valid
request. Digit maps are settings that describe the parameters of
this process. If present, digit maps define patterns that when
matched define the following:

1) A rule by which the endpoint can judge that the user has completed
   dialing, and
2) A rule to construct a URI from the dialed digits, and optionally
3) An outbound proxy to be used in routing the SIP INVITE.

A critical timer MAY be provided that determines how long the device
SHOULD wait before dialing if a dial plan contains a T (Timer)
character. It MAY also provide a timer for the maximum elapsed time
that SHOULD pass before dialing if the digits entered by the user

   match no dial plan. If the UA has a Dial or OK key, pressing this
   key will override the timer setting.

   SIP telephony devices SHOULD have a Dial/OK key. After sending a
   request, the UA SHOULD be prepared to receive a 484 Address
   Incomplete response. In this case, the UA should accept more user
   input and try again to dial the number.

   An example digit map could use regular expressions like in DNS NAPTR
   (RFC 2915) to translate user input into a SIP URL. Additional
   replacement patterns like "d" could insert the domain name of the
   used AOR. Additional parameters could be inserted in the flags
   portion of the substitution expression. A list of those patterns
   would make up the dial plan:

   |^([0-9]*)#$|sip:\1@\d;user=phone|outbound=proxy.com
   |^([a-zA-Z0-9&=+\$,;?\-_.!~*'()%]+@.+)|sip:\1|
   |^([a-zA-Z0-9&=+\$,;?\-_.!~*'()%]+)$|sip:\1@\d|
   |^(.*)$|sip:\1@\d|timeout=5

3.6.3. Default Digit Map

   The SIP telephony device SHOULD support the configuration of a
   default digit map. If the SIP telephony device does not support
   digit maps, it SHOULD at least support a default digit map rule to
   construct a URI from digits. If the endpoint does support digit
   maps, this rule applies if none of the digit maps match.

   For example, when a user enters "12345", the UA might send the
   request to "sip:12345@proxy.com;user=phone" after the user presses
   the OK key.

3.7. SIP Timer Settings

   The parameters for SIP (like timer T1) and other related settings MAY
   be indicated. An example of usage would be the reduction of the DNS
   SRV failover time.
   Example: SIPTimer="t1=100;unit=ms"

   Note: The timer settings can be included in the digit map.

3.8. Audio Codecs

   In some cases, operators want to control which codecs may be used in
   their network. The desired subset of codecs supported by the device
   SHOULD be configurable along with the order of preference. Service
   providers SHOULD have the possibility of plugging in their own codecs

of choice. The codec settings MAY include the packet length and
other parameters like silence suppression or comfort noise
generation.

The set of available codecs will be used in the codec negotiation
according to RFC 3264.
Example: Codecs="speex/8000;ptime=20;cng=on,gsm;ptime=30"

The settings MUST include hints about privacy for audio using Secure
Realtime Transport Protocol (SRTP) that either mandate or encourage
the usage of secure RTP.
Example: SRTP="mandatory"

3.9. DTMF Method

Keyboard interaction can be indicated with in-band tones or
preferably with out-of-band RTP packets (RFC 2833 [13]). The method
for sending these events SHOULD be configurable with the order of
precedence. Settings MAY include additional parameters like the
content-type that should be used.
Example: DTMFMethod="INFO;type=application/dtmf, RFC2833".

3.10. Local and Regional Parameters

Certain settings are dependent upon the regional location for the
daylight saving time rules and for the time zone.

Time Zone and UTC Offset: A time zone MAY be specified for the user.
Where one is specified; it SHOULD use the schema used by the Olson
Time One database [52].

Examples of the database naming scheme are Asia/Dubai or America/Los
Angeles where the first part of the name is the continent or ocean
and the second part is normally the largest city in that time zone.
Optional parameters like the UTC offset may provide additional
information for UAs that are not able to map the time zone
information to a internal database.
Example: TimeZone="Asia/Dubai;offset=7200"

3.11. Time Server

A time server SHOULD be used. DHCP is the preferred way to provide
this setting. Optional parameters may indicate the protocol that
SHOULD be used for determining the time. If present, the DHCP time
server setting has higher precedence than the time server setting.
Example: TimeServer="12.34.5.2;protocol=NTP"

3.12. Language

   Setting the correct language is important for simple installation
   around the globe.

   A language setting SHOULD be specified for the whole device. Where
   it is specified, it MUST use the codes defined in RFC 3066 to provide
   some predictability.
   Example: Language="de"

   It is recommended to set the language as writable, so that the user
   MAY change this. This setting SHOULD NOT be AOR related.

   A SIP UA MUST be able to parse and accept requests containing
   international characters encoded as UTF-8 even if it cannot display
   those characters in the user interface.

3.13. Inbound Authentication

   SIP allows a device to limit incoming signaling to those made by a
   predefined set of authorized users from a list and/or with valid
   passwords. Note that the inbound proxy from most service providers
   may also support the screening of incoming calls, but in some cases
   users may want to have control in the SIP telephony device for the
   screening.

   A device SHOULD support the setting as to whether authentication (on
   the device) is required and what type of authentication is required.
   Example: InboundAuthentication="digest;pattern=*"

   If inbound authentication is enabled, then a list of allowed users
   and credentials to call this device MAY be used by the device. The
   credentials MAY contain the same data as the credentials for an AOR
   (i.e., URL, user, password digest, and domain). This applies to SIP
   control signaling as well as call initiation.

3.14. Voice Message Settings

   Various voice message settings require the use of URIs for the
   service context as specified in RFC 3087 [53].

   The message waiting indicator (MWI) address setting controls where
   the client SHOULD SUBSCRIBE to a voice message server and what MWI
   summaries MAY be displayed [9].
   Example: MWISubscribe="sip:mailbox01@media.proxy.com"

User Agents SHOULD accept MWI information carried by SIP MESSAGE
without prior subscription. This way the setup of voice message
settings can be avoided.

3.15. Phonebook and Call History

The UA SHOULD have a phonebook and keep a history of recent calls.
The phonebook SHOULD save the information in permanent memory that
keeps the information even after restarting the device or save the
information in an external database that permanently stores the
information.

3.16. User-Related Settings and Mobility

A device MAY specify the user that is currently registered on the
device. This SHOULD be an address-of-record URL specified in an AOR
definition.

The purpose of specifying which user is currently assigned to this
device is to provide the device with the identity of the user whose
settings are defined in the user section. This is primarily
interesting with regards to user roaming. Devices MAY allow users to
sign on to them and then request that their particular settings be
retrieved. Likewise, a user MAY stop using a device and want to
disable their AOR while not present. For the device to understand
what to do, it MUST have some way of identifying users and knowing
which user is currently using it. By separating the user and device
properties, it becomes clear what the user wishes to enable or to
disable. Providing an identifier in the configuration for the user
gives an explicit handle for the user. For this to work, the device
MUST have some way of identifying users and knowing which user is
currently assigned to it.

One possible scenario for roaming is an agent who has definitions for
several AORs (e.g., one or more personal AORs and one for each
executive for whom the administrator takes calls) that they are
registered for. If the agent goes to the copy room, they would sign
on to a device in that room and their user settings including their
AOR would roam with them.

The alternative to this is to require the agent to individually
configure each of the AORs (this would be particularly irksome using
standard telephone button entry).

The management of user profiles, aggregation of user or device AOR,
and profile information from multiple management sources are
configuration server concerns that are out of the scope of this
document. However, the ability to uniquely identify the device and

   user within the configuration data enables easier server-based as
   well as local (i.e., on the device) configuration management of the
   configuration data.

3.17. AOR-Related Settings

   SIP telephony devices MUST use the AOR-related settings, as specified
   here.

   There are many properties which MAY be associated with or SHOULD be
   applied to the AOR or signaling addressed to or from the AOR. AORs
   MAY be defined for a device or a user of the device. At least one
   AOR MUST be defined in the settings; this MAY pertain to either the
   device itself or the user.
   Example: AOR="sip:12345@proxy.com"

   It MUST be possible to specify at least one set of domain, user name,
   and authentication credentials for each AOR. The user name and
   authentication credentials are used for authentication challenges.

3.18. Maximum Connections

   A setting defining the maximum number of simultaneous connections
   that a device can support MUST be used by the device. The endpoint
   might have some maximum limit, most likely determined by the media
   handling capability. The number of simultaneous connections may be
   also limited by the access bandwidth, such as of DSL, cable, and
   wireless users. Other optional settings MAY include the enabling or
   disabling of call waiting indication.

   A SIP telephony device MAY support at least two connections for
   three-way conference calls that are locally hosted.
   Example: MaximumConnections="2;cwi=false;bw=128".

   See the recent work on connection reuse [54] and the guidelines for
   connection-oriented transport for SIP [55].

3.19. Automatic Configuration and Upgrade

   Automatic SIP telephony device configuration SHOULD use the processes
   and requirements described in [56]. The user name or the realm in
   the domain name SHOULD be used by the configuration server to
   automatically configure the device for individual- or group-specific
   settings, without any configuration by the user. Image and service
   data upgrades SHOULD also not require any settings by the user.

3.20. Security Configurations

   The device configuration usually contains sensitive information that
   MUST be protected. Examples include authentication information,
   private address books, and call history entries. Because of this, it
   is RECOMMENDED to use an encrypted transport mechanism for
   configuration data. Where devices use HTTP, this could be TLS.

   For devices which use FTP or TFTP for content delivery this can be
   achieved using symmetric key encryption.

   Access to retrieving configuration information is also an important
   issue. A configuration server SHOULD challenge a subscriber before
   sending configuration information.

   The configuration server SHOULD NOT include passwords through the
   automatic configuration process. Users SHOULD enter the passwords
   locally.

4. Security Considerations

4.1. Threats and Problem Statement

   While Section 2.11 states the minimal security requirements and
   NAT/firewall traversal that have to be met respectively by SIP
   telephony devices, developers and network managers have to be aware
   of the larger context of security for IP telephony, especially for
   those scenarios where security may reside in other parts of SIP-
   enabled networks.

   Users of SIP telephony devices are exposed to many threats [57] that
   include but are not limited to fake identity of callers,
   telemarketing, spam in IM, hijacking of calls, eavesdropping, and
   learning of private information such as the personal phone directory,
   user accounts and passwords, and the personal calling history.
   Various denial of service (DoS) attacks are possible, such as hanging
   up on other people's conversations or contributing to DoS attacks of
   others.

   Service providers are also exposed to many types of attacks that
   include but are not limited to theft of service by users with fake
   identities, DoS attacks, and the liabilities due to theft of private
   customer data and eavesdropping in which poorly secured SIP telephony
   devices or especially intermediaries such as stateful back-to-back
   user agents with media (B2BUA) may be implicated.

SIP security is a hard problem for several reasons:

   o Peers can communicate across domains without any pre-arranged
     trust relationship.
   o There may be many intermediaries in the signaling path.
   o Multiple endpoints can be involved in such telephony operations
     as forwarding, forking, transfer, or conferencing.
   o There are seemingly conflicting service requirements when
     supporting anonymity, legal intercept, call trace, and privacy.
   o Complications arise from the need to traverse NATs and
     firewalls.

There are a large number of deployment scenarios in enterprise
networks, using residential networks and employees using Virtual
Private Network (VPN) access to the corporate network when working
from home or while traveling. There are different security scenarios
for each. The security expectations are also very different, say,
within an enterprise network or when using a laptop in a public
wireless hotspot, and it is beyond the scope of this memo to describe
all possible scenarios in detail.

The authors believe that adequate security for SIP telephony devices
can be best implemented within protected networks, be they private IP
networks or service provider SIP-enabled networks where a large part
of the security threats listed here are dealt with in the protected
network. A more general security discussion that includes network-
based security features, such as network-based assertion of identity
[58] and privacy services [7], is outside the scope of this memo, but
must be well understood by developers, network managers, and service
providers.

In the following, some basic security considerations as specified in
RFC 3261 are discussed as they apply to SIP telephony devices.

4.2. SIP Telephony Device Security

   Transport Level Security
         SIP telephony devices that operate outside the perimeter of
         secure private IP networks (this includes telecommuters and
         roaming users) MUST use TLS to the outgoing SIP proxy for
         protection on the first hop. SIP telephony devices that use
         TLS must support SIPS in the SIP headers.

         Supporting large numbers of TLS channels to endpoints is quite
         a burden for service providers and may therefore constitute a
         premium service feature.

Digest Authentication
        SIP telephony devices MUST support digest authentication to
        register with the outgoing SIP registrar. This ensures proper
        identity credentials that can be conveyed by the network to the
        called party. It is assumed that the service provider
        operating the outgoing SIP registrar has an adequate trust
        relationship with its users and knows its customers well enough
        (identity, address, billing relationship, etc.). The
        exceptions are users of prepaid service. SIP telephony devices
        that accept prepaid calls MUST place "unknown" in the "From"
        header.

End User Certificates
        SIP telephony devices MAY store personal end user certificates
        that are part of some Public Key Infrastructure (PKI) [59]
        service for high-security identification to the outgoing SIP
        registrar as well as for end-to-end authentication. SIP
        telephony devices equipped for certificate-based authentication
        MUST also store a key ring of certificates from public
        certificate authorities (CAs).

        Note the recent work in the IETF on certificate services that
        do not require the telephony devices to store certificates
        [60].

End-to-End Security Using S/MIME
        S/MIME [61] MUST be supported by SIP telephony devices to sign
        and encrypt portions of the SIP message that are not strictly
        required for routing by intermediaries. S/MIME protects
        private information in the SIP bodies and in some SIP headers
        from intermediaries. The end user certificates required for
        S/MIME ensure the identity of the parties to each other. Note:
        S/MIME need not be used, though, in every call.

4.3. Privacy

  Media Encryption
        Secure RTP (SRTP) [62] MAY be used for the encryption of media
        such as audio, text, and video, after the keying information
        has been passed by SIP signaling. Instant messaging MAY be
        protected end-to-end using S/MIME.

4.4. Support for NAT and Firewall Traversal

  The various NAT and firewall traversal scenarios require support in
  telephony SIP devices. The best current practices for NAT traversal
  for SIP are reviewed in [51]. Most scenarios where there are no
  SIP-enabled network edge NAT/firewalls or gateways in the enterprise

can be managed if there is a STUN client in the SIP telephony device
and a STUN server on the Internet, maintained by a service provider.
In some exceptional cases (legacy symmetric NAT), an external media
relay must also be provided that can support the Traversal Using
Relay NAT (TURN) protocol exchange with SIP telephony devices. Media
relays such as TURN come at a high bandwidth cost to the service
provider, since the bandwidth for many active SIP telephony devices
must be supported. Media relays may also introduce longer paths with
additional delays for voice.

Due to these disadvantages of media relays, it is preferable to avoid
symmetric and non-deterministic NATs in the network, so that only
STUN can be used, where required. Reference [63] deals in more
detail how NAT has to 'behave'.

It is not always obvious to determine the specific NAT and firewall
scenario under which a SIP telephony device may operate.

For this reason, the support for Interactive Connectivity
Establishment (ICE) has been defined to be deployed in all devices
that required end-to-end connectivity for SIP signaling and RTP media
streams, as well as for streaming media using Real Time Streaming
Protocol (RTSP). ICE makes use of existing protocols, such as STUN
and TURN.

Call flows using SIP security mechanisms
      The high-level security aspects described here are best
      illustrated by inspecting the detailed call flows using SIP
      security, such as in [64].

Security enhancements, certificates, and identity management
      As of this writing, recent work in the IETF deals with the SIP
      Authenticated Identity Body (AIB) format [65], new S/MIME
      requirements, enhancements for the authenticated identity, and
      Certificate Management Services for SIP. We recommend
      developers and network managers to follow this work as it will
      develop into IETF standards.

5. Acknowledgements

   Paul Kyzivat and Francois Audet have made useful comments how to
   support to the dial plan requirements in Req-17. Mary Barnes has
   kindly made a very detailed review of version 04 that has contributed
   to significantly improving the document. Useful comments on version
   05 have also been made by Ted Hardie, David Kessens, Russ Housley,
   and Harald Alvestrand that are reflected in this version of the
   document.

6. Informative References

   [1]   Bradner, S., "Key words for use in RFCs to Indicate Requirement
         Levels", BCP 14, RFC 2119, March 1997.

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

   [3]   Lemon, T. and S. Cheshire, "Encoding Long Options in the Dynamic
         Host Configuration Protocol (DHCPv4)", RFC 3396, November 2002.

   [4]   Mills, D., "Simple Network Time Protocol (SNTP) Version 4 for
         IPv4, IPv6 and OSI", RFC 4330, January 2006.

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

   [6]   Peterson, J., "enumservice registration for Session Initiation
         Protocol (SIP) Addresses-of-Record", RFC 3764, April 2004.

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

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

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

   [10] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966,
         December 2004.

   [11] Sparks, R., "The Session Initiation Protocol (SIP) Refer
         Method", RFC 3515, April 2003.

   [12] Johnston, A., "SIP Service Examples", Work in Progress, March
         2006.

   [13] Schulzrinne, H. and S. Petrack, "RTP Payload for DTMF Digits,
         Telephony Tones and Telephony Signals", RFC 2833, May 2000.

   [14] Casner, S. and P. Hoschka, "MIME Type Registration of RTP
         Payload Formats", RFC 3555, July 2003.

   [15] Camarillo, G., Eriksson, G., Holler, J., and H. Schulzrinne,
        "Grouping of Media Lines in the Session Description Protocol
        (SDP)", RFC 3388, December 2002.

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

   [17] Johnston, A., Donovan, S., Sparks, R., Cunningham, C., and K.
        Summers, "Session Initiation Protocol (SIP) Basic Call Flow
        Examples", BCP 75, RFC 3665, December 2003.

   [18] Johnston, A., Donovan, S., Sparks, R., Cunningham, C., and K.
        Summers, "Session Initiation Protocol (SIP) Public Switched
        Telephone Network (PSTN) Call Flows", BCP 76, RFC 3666, December
        2003.

   [19] Rosenberg, J., Peterson, J., Schulzrinne, H., and G. Camarillo,
        "Best Current Practices for Third Party Call Control (3pcc) in
        the Session Initiation Protocol (SIP)", BCP 85, RFC 3725, April
        2004.

   [20] Mahy, R., et al., "A Call Control and Multi-party usage
        framework for the Session Initiation Protocol (SIP)", Work in
        Progress, March 2006.

   [21] Johnston, A. and O. Levin, "Session Initiation Protocol Call
        Control - Conferencing for User Agents", Work in Progress,
        October 2005.

   [22] Even, R. and N. Ismail, "Conferencing Scenarios", Work in
        Progress, September 2005.

   [23] Hellstrom, G. and P. Jones, "RTP Payload for Text Conversation",
        RFC 4103, June 2005.

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

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

   [26] Rosenberg, J., Schulzrinne, H., and P. Kyzivat, "Indicating User
        Agent Capabilities in the Session Initiation Protocol (SIP)",
        RFC 3840, August 2004.

   [27] Schulzrinne, H., Gurbani, V., Kyzivat, P., and J. Rosenberg,
        "RPID: Rich Presence Extensions to the Presence Information Data
        Format (PIDF)", Work in Progress, September 2005.

   [28] See the Working Group on Emergency Context Resolution with
        Internet Technologies at
        http://www.ietf.org/html.charters/ecrit-charter.html

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

   [30] Polk, J. and B. Rosen, "Session Initiation Protocol Location
        Conveyance", Work in Progress, July 2005.

   [31] Charlton, N., Gasson, M., Gybels, G., Spanner, M., and A. van
        Wijk, "User Requirements for the Session Initiation Protocol
        (SIP) in Support of Deaf, Hard of Hearing and Speech-impaired
        Individuals", RFC 3351, August 2002.

   [32] van Wijk, A., "Framework of requirements for real-time text
        conversation using SIP", Work in Progress, September 2005.

   [33] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson,
        "RTP: A Transport Protocol for Real-Time Applications", STD 64,
        RFC 3550, July 2003.

   [34] Friedman, T., Caceres, R., and A. Clark, "RTP Control Protocol
        Extended Reports (RTCP XR)", RFC 3611, November 2003.

   [35] Pendleton, A., "SIP Package for Quality Reporting Event", Work
        in Progress, February 2006.

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

   [37] Heinanen, J., Baker, F., Weiss, W., and J. Wroclawski, "Assured
        Forwarding PHB Group", RFC 2597, June 1999.

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

   [39] Schulzrinne, H. and S. Casner, "RTP Profile for Audio and Video
        Conferences with Minimal Control", STD 65, RFC 3551, July 2003.

   [40] ITU-T Recommendation G.711, available online at
        http://www.itu.int.

   [41] Andersen, S., Duric, A., Astrom, H., Hagen, R., Kleijn, W., and
        J. Linden, "Internet Low Bit Rate Codec (iLBC)", RFC 3951,
        December 2004.

   [42] Duric, A. and S. Andersen, "Real-time Transport Protocol (RTP)
        Payload Format for internet Low Bit Rate Codec (iLBC) Speech",
        RFC 3952, December 2004.

   [43] Herlein, G., et al., "RTP Payload Format for the Speex Codec",
        Work in Progress, October 2005.

   [44] TIA/EIA-810-A, "Transmission Requirements for Narrowband Voice
        over IP and Voice over PCM Digital Wireline Telephones", July
        2000.

   [45] TIA-EIA-IS-811, "Terminal Equipment - Performance and
        Interoperability Requirements for Voice-over-IP (VoIP) Feature
        Telephones", July 2000.

   [46] Alvestrand, H., "Tags for the Identification of Languages", BCP
        47, RFC 3066, January 2001.

   [47] Wing, D., "Symmetric RTP and RTCP Considered Helpful", Work in
        Progress, October 2004.

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

   [49] Jennings, C., "NAT Classification Test Results", Work in
        Progress, July 2005.

   [50] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A
        Methodology for Network Address Translator (NAT) Traversal for
        Offer/Answer Protocols", Work in Progress, July 2005.

   [51] Boulton, C. and J. Rosenberg, "Best Current Practices for NAT
        Traversal for SIP", Work in Progress, October 2005.

   [52] P. Eggert, "Sources for time zone and daylight saving time
        data." Available at http://www.twinsun.com/tz/tz-link.htm.

   [53] Campbell, B. and R. Sparks, "Control of Service Context using
        SIP Request-URI", RFC 3087, April 2001.

   [54] Mahy, R., "Connection Reuse in the Session Initiation Protocol
        (SIP)", Work in Progress, February 2006.

[55] Jennings, C. and R. Mahy, "Managing Client Initiated Connections
     in the Session Initiation Protocol", Work in Progress, March
     2006.

[56] Petrie, D., "A Framework for SIP User Agent Profile Delivery",
     Work in Progress, July 2005.

[57] Jennings, C., "SIP Tutorial: SIP Security", presented at the VON
     Spring 2004 conference, March 29, 2004, Santa Clara, CA.

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

[59] Chokhani, S., Ford, W., Sabett, R., Merrill, C., and S. Wu,
     "Internet X.509 Public Key Infrastructure Certificate Policy and
     Certification Practices Framework", RFC 3647, November 2003.

[60] Jennings, C. and J. Peterson, "Certificate Management Service
     for The Session Initiation Protocol (SIP)", Work in Progress,
     March 2006.

[61] Ramsdell, B., "Secure/Multipurpose Internet Mail Extensions
     (S/MIME) Version 3.1 Message Specification", RFC 3851, July
     2004.

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

[63] Audet, F. and C. Jennings, "NAT Behavioral Requirements for
     Unicast UDP", Work in Progress, September 2005.

[64] Jennings, C., "Example call flows using SIP security
     mechanisms", Work in Progress, February 2006.

[65] Peterson, J., "Session Initiation Protocol (SIP) Authenticated
     Identity Body (AIB) Format", RFC 3893, September 2004.

Author's Addresses

   Henry Sinnreich
   Pulver.com
   115 Broadhollow Road
   Melville, NY 11747, USA

   EMail: henry@pulver.com
   Phone: +1-631-961-8950

   Steven Lass
   Verizon
   1201 East Arapaho Road
   Richardson, TX 75081, USA

   EMail: steven.lass@verizonbusiness.com
   Phone: +1-972-728-2363

   Christian Stredicke
   snom technology AG
   Gradestrasse, 46
   D-12347 Berlin, Germany

   EMail: cs@snom.de
   Phone: +49(30)39833-0