

P2P SIP Working Group
Internet Draft

H. Sinnreich/Adobe, editor
A. Johnston/Avaya
E. Shim/Locus
K. Singh/Adobe

Intended status: Informational
March 2, 2007

Expires: September 2007

Simple SIP Usage Scenario for Applications in the Endpoints
<draft-sinnreich-sip-tools-01.txt>

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>

This Internet-Draft will expire on September 2, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This memo discusses the usage scenario of SIP where all the applications reside in the endpoints. This is an alternative to the current usage of SIP where the services reside in the network.

The use of SIP where the applications reside in the endpoints is applicable to P2P SIP networks and also to client-server networks.

Such an approach reduces the number of required SIP related standards (as by spring 2007) from roughly 100 to about 11.

Successful IP communications must also include the relevant standards for NAT traversal, some of which are not directly related to SIP and also several standards for security. These standards are included in the simple usage scenario for SIP as well.

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [1].

Table of Contents

1. Introduction.....	3
2. Motivation.....	5
2.1. Using SIP for network based applications is not optimal...	5
2.2. Cost, scalability and reliability of applications.....	8
2.3. The endpoint application imperative for SIP deployments...	8
3. Methodology to Deploy Endpoint SIP Applications.....	10
3.1. Updating the use of SIP and SDP.....	11
3.2. Re-using other SIP standards.....	11
4. Presence and Instant Messaging.....	12
4.1. Presence.....	12
4.2. Instant Messaging.....	12
5. NAT and Firewall Traversal.....	12
6. Security Considerations.....	13
6.1. Security for SIP Signaling.....	13
6.2. Media Security.....	13
6.3. Authenticated Identity for SIP.....	13
7. IANA Considerations.....	14
8. Conclusions.....	14
9. Acknowledgments.....	14
10. References.....	14
10.1. Normative References.....	14
10.2. Informative References.....	15
Author's Addresses.....	17
Intellectual Property Statement.....	17
Disclaimer of Validity.....	18

1. Introduction

SIP standardization was started in the IETF in 1996 in the expectation to have a simple and flexible protocol for establishing multimedia communications. The flexibility of SIP has been a mixed blessing however: SIP has been fully embraced as the standard for IP communications, while at the same time all stakeholders in the communications industry have built equipment and launched services using SIP. As a result, in the over ten years that have passed, the SIP family of related protocols has grown into approximately 100 RFCs with thousands of pages of specifications [12] and an ever increasing number of Internet Drafts, many of them about to increase even more the large number of existing RFCs on SIP. The ITU-T and other organizations have added to this complexity by layering more and more services on top of SIP. Competitive pressure makes the steady increase in the number of new applications inevitable. This raises the question of how scalable can such a multi-service standard be and where does it make sense to draw a line?

It is of interest to note that other VoIP and IM protocols that are using servers in the network have comparable large numbers of specifications, similar to SIP, even when no attempt is made to emulate the PSTN and ISDN networks.

The meaning in this memo of network based services is any SIP call control feature that goes beyond the remote endpoint discovery and the setting up of a multimedia session. Services such as voice mail, conferencing or call transfer can be implemented either in a feature server or as an application in the endpoints. We will use this meaning to explore the cause of the complexity of SIP.

The common root of SIP's complexity is

- (a) the overuse of the client server model and the resulting migration of endpoint applications, such as voice, presence, IM, video and their various derivatives into
- (b) 'network based services' trying to emulate the Intelligent Network of the telephone system, especially reincarnations of ISDN type of services.

By contrast, simple client-server (CS) systems and peer-to-peer (P2P) SIP systems may not need to support any of the network based services, except the rendezvous function for which SIP was initially designed. Also, by the nature of P2P systems, their architectural difference from client server (CS) systems, P2P SIP systems may need

approaches different from those taken in the context of CS SIP to realize various functions.

The emergence of P2P SIP raises the question as to what parts of SIP must be used to (1) preserve the core SIP properties, (2) preserve basic interoperability with server based SIP systems and (3) preserve the advantages of SIP for use in P2P communication systems.

The objective of this memo is to clarify what parts of SIP are essential to meet these objectives. We will refer for brevity to these essential parts of SIP as 'simple SIP'. In a nutshell, simple SIP uses only message routing required for session initiation and leaves all the complexity of the applications to be handled in the endpoints. Simple SIP is thus an alternative usage scenario to the use and proliferation of feature servers and other elements in the network.

This memo is not trying to redefine SIP in any sense since it is based on RFC 3261 and a small number of follow-up RFCs that tighten the concepts found in RFC 3261, that is define SIP simply as a rendezvous service to discover endpoints and establish a multimedia session between them.

The so called 'network based services' using feature servers are not part of RFC 3261 and we also draw here the line for simple SIP. Once a session has been established between endpoints, it is up to the applications in the endpoints how to provide the best multimedia service to the users. SIP call control documents [13], [14] and the endpoint controlled call control (EPCC) [15] provide ample evidence that all possible and desirable services can be provided by the endpoints, without any support from feature servers in the network.

Also, it is important to note that simple SIP is not a profile of SIP, but an alternative usage scenario to 'network services'. It involves no modifications or subtractions to the MUSTs in RFC 3261. It represents an attempt to reign in the seemingly endless set of SIP extensions which add 'network services' to the native SIP rendezvous and session initiation functions.

Though simple SIP is targeted primarily for P2P SIP, simple SIP is also useful for basic CS SIP systems that use the peer-to-peer SIP call control. Peer-to-peer SIP call control is not to be confused with P2P SIP, since it makes no assumption of the existence of a P2P overlay network.

In conclusion, simple SIP is limited to the original intent of SIP; establishing sessions between endpoints and leaving the applications in the endpoints. Establishing a session also includes the negotiation of the session parameters.

The proposed simple SIP benefits users, endpoint manufacturers, application developers and service providers alike, since it fully enables innovations in the endpoints and decouples the network functions of service providers from the endpoints. Simple SIP reduces the cost and complexity for enterprise networks and for service providers alike and these benefits can be passed along to users. Device manufacturers have already proven in commercial products that a P2P PBX for example can be implemented such that all the PBX functions reside in the end devices - the desktop phones, PCs and mobile devices.

In the following section we drill into more detail on the problems that are avoided by using simple SIP.

2. Motivation

2.1. Using SIP for network based applications is not optimal

There is a clear distinction between the SIP servers defined in RFC 3261 and feature servers used for network based applications. The SIP server functions in RFC3261 are the registrar, the proxy and redirect and they are used only for routing SIP messages between endpoints, not for the support of applications in the network. This is the key to simple SIP.

By contrast, feature servers are dedicated to provide network based applications, such as voice mail, call control server (PBX or local telephone switch), IP Centrex emulation, interactive voice response, presence service, etc.

RFC 3261 does not mention any feature servers. Applications in the network are in contradiction with the e2e principle of the Internet.

As we will see in the following, contradicting the end-to-end principle of the Internet for applications creates non-trivial technical problems. Adding new network based applications may require massive re-engineering every time and thus complicates or blocks the introduction of innovation.

The difficulties resulting from telephony style network based applications are not specific to SIP and RTP. They are also encountered by any other signaling protocols attempting to support

network based applications. A similar analysis for H.323 and XMPP is however beyond the scope of this memo, even though it is worthwhile to notice that neither H.323 nor XMPP have been used for multimedia network services to the extent of SIP.

The placement of applications in the network will unavoidably lead to SIP network designs that are optimized for one business model or another. In fact, the SIP routing for these networks is actually not designed to enable new services but to make it easy to deny service to those who have not paid for specific service provider applications. This leads to technically indefensible architectures in which, for example, a SIP request between two UAs routes through multiple B2BUAs. Another example is the mandatory use of an outgoing SIP proxy when a mobile user is in a visited network. The sole rationale for the visited proxy is to apply roaming charges, since on the Internet endpoint mobility is a native property. The routing of messages within such SIP networks will therefore reflect the respective business model.

Searching for a standard for SIP routing to accommodate different and often competing business models for network based applications is futile. Large SIP networks have such complex routing rules that multi-vendor interoperability is a significant engineering effort or may be just not practical. An example at hand is forking within the network, instead of forking to multiple endpoints only. The special case of forking to several PSTN gateways [16] is best dealt with at the edge between the IP and the PSTN networks and must not burden the SIP routing elsewhere.

Another example is the SIP implementation in IMS where the current business model and the resulting architecture will not support many services without additional extensions and conventions in SIP.

The showcase of the futility of embedding business models into SIP routing arises when emulating PSTN and ISDN services. For example supporting early media throughout a SIP network is still a topic of much debate. Since early media is required for compatibility with the PSTN, it is best handled at the IP network edge with the PSTN and need not burden the whole SIP network. The reliance on the legacy telephone numbering system has also led to the overuse of ENUM and dependency on legacy phone number data bases for SIP networks. Instead of keeping ENUM at the edge of SIP networks with the PSTN, ENUM has often become a central design item and has now its own life with business models of its own, designed to monetize the value of existing telephone number databases or to enable closed routing between confederated VoIP providers. Using telephone numbers as handles for SIP call routing negates most of the values found in IP

networks where the URI and URL is the native, much more powerful addressing mode found on the web, e-mail, presence and IM, etc.

Many VoIP SIP network designs include intermediaries known as B2BUA that may actually break applications in the endpoints that they don't understand. The use of some B2BUA called Session Border Controllers (SBC) raises fundamental architectural issues that are detailed in [17] and the misuse of B2BUA is still attempted to be minimized or avoided. For example if the communicating user agents can do screen sharing but the intermediate B2BUA can't negotiate that, then the user agents are deprived of this function. See also the generic arguments for preserving the e2e transparency on the Internet [18].

The result of placing features in servers in the network has so far made SIP routing a manual art that requires great expertise and costly engineering, since a SIP routing protocol that can be executed in software similar to IP routing could not be defined.

Multi-vendor interoperability in SIP networks is not feasible without detailed custom engineering. The custom engineering effort increases faster than the number of new applications introduced in the network due to the mesh of interdependency of SIP routing and the characteristics of the feature servers.

The combined message flows required for SIP signaling between all feature servers, TLS and SRTP key exchanges and message flows, new complex SDP negotiation, NAT traversal, QoS, AAA functions and policy servers is literally overwhelming. The number of messages can reach 100 and more, to support all the feature servers. The total number of servers and other network elements, such as B2BUA is also in the 10-100 range.

Such complexity forces service providers into complete vertical bundles from single vendors who control this complexity by choosing their own shortcuts.

Security may be another victim of placing services in the network. The lack of a straightforward standard for SIP routing and the large number of network elements make security audits very difficult. The last defense for network based services is obscuring the network details to the outside using a fronting proxy. This may however provide no protection against network compromise from an insider. The possibility of compromising the network from the inside increases with more application servers in the network.

A lot of trust is also required in all intermediaries and a multi-hop SIP signaling path, especially when more than one service provider is

involved. In other words, multi-hop SIP signaling may not be secure, and there are discussions on how much trust to put on secure SIP (SIPS). If the last hop is to a PSTN gateway and on the other side of the PSTN may be other gateways to unknown IP networks, SIPS obviously loses its meaning. This item is mentioned here as a caution to avoid PSTN gateways as much as possible, not only for their limitation to narrowband 3.1 kHz audio, loss of IM and video, the inevitable charging for the voice call, but also for security reasons.

2.2. Cost, scalability and reliability of applications

Large scale VoIP systems have experienced load problems and there are proposals on how to deal with large loads on SIP servers that support mostly voice. Presence servers in large networks experience both a tremendous message load and require very large storage capacity, especially in interconnected networks, see for example the numbers reported in [19]. By contrast, distributing the presence processing in the endpoints, no presence servers are required at all.

Deployment experience shows that client-server based system scalability comes at a cost that grows faster than the number of new users. This places a practical upper limit on scalability for client-server based VoIP systems.

Reliable and robust server-based VoIP infrastructure requires geographically distributed backup servers. These further add to the cost of server based applications.

For inter-domain traffic the proxy server function is inevitable, though it can be better distributed in p2p systems as we will discuss below.

Note the technical difficulties of server based communication applications have nothing to do with the cost of deploying server hardware, which is low indeed. The operational costs of deploying and maintaining feature servers are discussed separately in the following section.

2.3. The endpoint application imperative for SIP deployments

The above deployment problems of network based applications lead to the conclusion that P2P SIP systems are unavoidable for the following expected advantages and characteristics of P2P SIP systems:

- o Peer routing and discovery protocols in overlay networks are quite mature and sophisticated to meet the requirements of the SIP registration and location service.
- o The applications can reside in the endpoints. There can be specialized applications that reside in dedicated endpoints, such as proxies to connect to the DNS world and from there to various outside systems. Small scale conferencing can also be hosted in endpoints. Large scale conferencing is better accomplished using application layer multicast. Other types of dedicated endpoints can also perform specialized telephony functions such as the auto-attendant, the receptionist workstation and contact center agent workstation. The main P2P SIP network is however not burdened with any such application functionality.
- o The overlay network is completely transparent to applications. Current work on P2P SIP networks recommends flexibility in the choice of the P2P overlay, thus further decoupling the P2P network design from the application design.
- o All peer nodes have identical peer protocol software.
- o None of the peer nodes require individual user data provisioning from service provider IT systems.
- o The fulfillment process to add/remove users can be completely separated from all network elements and be delegated to user enrollment servers that are generic to any other Internet type of businesses. They need only provide users with cryptographic keys to execute the fulfillment process for new customers. This is probably the simplest order fulfillment process known today and is the very opposite to the complex fulfillment processes used in telecoms VoIP, where feature servers must be made aware of individual customer data.
- o P2P SIP systems do not require any manual engineering for operation, no matter if and how many new users or new applications are added.
- o P2P SIP nodes may use URIs but do not require DNS. ENUM is also not required. Only peer nodes that have off-net connectivity and act as

proxies require DNS support. As mentioned, the use of ENUM can be delegated to edge networks that provide PSTN gateway service and ENUM does not need to burden simple SIP.

- o P2P SIP inherits also the generic benefits of p2p systems, such as:
 - o The overlay network is self organizing and requires no manual configuration,
 - o The system is fully decentralized and therefore more robust,
 - o P2P systems are fully scalable and get better the bigger the system grows,
 - o The cost of deploying server farms; computing, bandwidth, real estate and electricity is moved to the endpoints were the incremental cost of P2P is arguably not perceived due to the power of personal computing and broadband connectivity.

With this motivation in mind we will explore in the following which SIP and the related standards are required and applicable for P2P SIP and basic CS SIP systems.

3. Methodology to Deploy Endpoint SIP Applications

The method to deploy endpoint SIP applications has several parts:

a. Preserve the basic SIP definitions as per RFC 3261 [2]. SIP can work with or without servers. The trapezoid model in RFC 3261 is only an example and a usage scenario how to connect two SIP CS systems.

In the trapezoid model no attempt is made to provide any specific applications in the network, since the proxies only act as application level message routers. We do not propose any changes to RFC 3261, to eliminate any methods or headers, error messages, etc., since this would carry among other risks the danger of losing backward interoperability and lack of flexibility.

b. Analyze the main SIP related specifications as highlighted in [20] and eliminate all network based applications residing in feature servers and various other network elements.

c. Adopt the NAT traversal techniques developed for SIP.

d. Adopt the protocol security techniques developed for SIP and RTP, to the extent that they are not dependent on central control and they are not focused on providing network based telephony style services.

As specified in [21], SIP is not meant to be used as a strict Public Switched Telephone Network (PSTN) signaling replacement.

3.1. Updating the use of SIP and SDP

We do not intend to re-write RFC 3261 for simple SIP, but to take into account later work in SIP. Examples are:

- o Add items that have been developed in recent work on SIP, such as the use of "rport" in the Via header and how to use the connection data "c=" in the SDP body behind a NAT. This information is now used differently as per RFC 3489bis defining the STUN protocol.
- o Add the offer/answer model with SDP as per RFC 3264 [3].
- o Add Locating SIP Servers [4].
- o Make TLS mandatory and leave S/MIME optional since it has not found as wide acceptance. Note that not making S/MIME mandatory does not preclude end-to-end privacy of messages in P2P SIP. End-to-end privacy is still possible in the SIP level single hop P2P architecture.
- o Simplify early media by specifying that User Agents accept but do not generate early media. Early media functionality is best delegated to IP-PSTN VoIP gateway networks.

Most of the User Agent behavior described in RFC 3261 can be re-used in endpoint based applications, while the proxy behavior should be limited to the most basic interoperability between P2P SIP nodes and CS SIP systems.

One key difference between RFC 3261 and P2P SIP systems is the replacement of the location database at the back side of SIP proxy and registrar servers with the P2P DHT layer as proposed in [22].

3.2. Re-using other SIP standards

A summary review of the other over roughly 100 SIP related standards reveals that they are mostly dedicated to telephony style of "services in the network" and therefore are out of scope for simple SIP. The only exception is RFC 3840 for indicating user agent capabilities [5], such as for various media types and SIP events.

4. Presence and Instant Messaging

4.1. Presence

Subscriptions and notifications for presence based on SIP have been defined in [6] and the data format for presence information has been defined in [7].

Rich presence information can be conveyed about the location, activity and other data about a user. Presence can also be used to integrate applications and communications in the endpoints. Such extended applications for presence are however beyond the scope of this memo.

4.2. Instant Messaging

Instant messaging for SIP is based on the simple extension "MESSAGE" defined in [8].

Interesting activity information can be conveyed in various ways, such as the indication of "is typing" [9].

5. NAT and Firewall Traversal

While NAT traversal is not strictly speaking a SIP signaling property, we believe that any IP communication and application is useless without complete NAT traversal capabilities. The essential documents for a complete solution for NAT traversal for SIP based communications are referenced here.

- A. Requirements for NAT to "behave" [23] for UDP packets.
- B. NAT Traversal for SIP
 - 1. Updating the Via header information with "rport" for symmetric response routing [10].
 - 2. Connection reuse [24] for "SIP Outbound".
- C. NAT Traversal for RTP/RTCP Media
 - 1. Symmetric RTP [11]
 - 2. Simple Traversal Under NAT (STUN) [25]
 - 3. Media relay function for STUN servers [26]

4. Interactive Connectivity Establishment (ICE) [27].

An excellent summary of all the above in the form of deployment examples is given in the document on NAT scenarios [28].

6. Security Considerations

Security for SIP communications touches on both signaling and media. Existing security standards for CS SIP are described here. In P2P SIP systems, besides the security for signaling and media, the additional security for the P2P layer must also be provided. There are however no security standards as yet for P2P SIP.

6.1. Security for SIP Signaling

SIP secure authentication between the UA and the server is based on the digest authentication schema as specified in RFC 3261. SIP transport security for confidentiality is based on Transport Level Security (TLS) that is also specified in RFC 3261.

End-to-end SIP security through intermediaries based on S/MIME has not found wide application at present, but it MAY be implemented in Lightweight SIP. Instead, P2P TLS connections SHOULD be used to achieve end-to-end security.

6.2. Media Security

End-to-end media security without any dependency on intermediaries, such as SIP proxies and certificate authorities will be provided using SRTP as per RFC 3711.

Key management for SRTP is currently an active area of discussion and standardization in the IETF.

The authors favor key management approaches that have no reliance on centralized certificate authorities and PKI infrastructures. For VoIP, the recommended protocol is ZRTP protocol [29]. ZRTP is based on users authenticating themselves to each other by voice, before activating media encryption for the rest of the conversation and for all following communications.

6.3. Authenticated Identity for SIP

In scenarios where the identity and authentication is required, the SIP identity header will be used as described in [30]. In P2P systems, the user enrollment server can be the source for the authentication service.

7. IANA Considerations

There are no IANA considerations associated with this memo.

8. Conclusions

We have shown in this document how the number of SIP related standards for presence, IM and multimedia communications can be reduced by (1) using SIP without network based applications and (2) without emulating the telephone network. This approach for SIP reduces the number of SIP related standards, currently from roughly 100 to about 11. Successful IP communications must however include a number of standards for NAT traversal, some of which are not directly related to SIP. The standards for NAT traversal are however referenced here, since SIP based communications must traverse NAT.

9. Acknowledgments

We would like to thank Wilhelm Wimmreuter for the detailed review of the initial draft and to Arjun Roychaudhury for the comments regarding the need for a definition of network based services.

This document was prepared using 2-Word-v2.0.template.dot.

10. References

10.1. Normative References

- [1] RFC 2119: "Key words for use in RFCs to Indicate Requirement Levels" by S. Bradner. IETF, March 1997.
- [2] RFC 3261: "SIP: Session Initiation Protocol" by J. Rosenberg et al. IETF June 2002.
- [3] RFC 3264: "An Offer/Answer Model with Session Description Protocol (SDP)" by J. Rosenberg and H. Schulzrinne. June 2002.
- [4] RFC 3263 "Locating SIP Servers" by J. Rosenberg and H. Schulzrinne. IETF, June 2002.
- [5] RFC 3840: "Indicating User Agent Capabilities in SIP" by J. Rosenberg, et al. IETF, August 2004.
- [6] RFC 3856: "A Presence Event Package for SIP" by J. Rosenberg. IETF, August 2004.

[7] RFC 3863 "Presence Information Data Format (PIDF)" by H. Sugano et al. IETF, August 2004.

[8] RFC 3428: "SIP Extension for Instant Messaging" by B. Campbell et al. IETF, December 2002.

[9] RFC 3994: "Indication of Message Composition for Instant Messaging" by H. Schulzrinne. IETF, January 2005.

[10] RFC 3581: "An Extension to SIP for Symmetric Response Routing" by J. Rosenberg and H. Schulzrinne. IETF, August 2003.

[11] RFC xxxx: "Symmetric RTP and RTCP Considered Helpful" by D. Wing, IETF, 2006.

10.2. Informative References

[12] "VoIP RFC Watch" by Nils Ohlmeier, <http://rfc3261.net/>.

[13] "A Call Control and Multi-party usage framework for SIP" by R. Mahy et al. <draft-ietf-sipping-cc-framework-06.txt>. IETF, March 2006.

[14] "Remote Call Control in the Session Initiation Protocol (SIP) using the REFER method and the session-oriented dialog package by R. Mahy and C. Jennings, IETF, October 2006, work in progress.

[15] "Guidelines for Implementing the Dialog Event Package in User Agents" by D. Worley, IETF, February 2007, work in progress.

[16] "A New Forking Mechanism for Session Initiation Protocol (SIP)" by D. Worley, IETF, February 2007, work in progress.

[17] "Requirements for SBC Deployments" by J. Hautakorpi et al. IETF, October 2006, work in progress.

[18] "Reflections on Internet Transparency" by B. Aboba and E. Davies. IAB, February 2007, work in progress.

[19] "Problem Statement for SIP/SIMPLE" by A. Hourri et al. IETF, October 2006, work in progress.

[20] "A Hitchhikers Guide to SIP" by J. Rosenberg. IETF, October 2006, work in progress.

[21] RFC 4485: "Guidelines for Authors of Extensions to SIP" by J. Rosenberg and H. Schulzrinne. IETF May 2006.

[22] "SIP, P2P and internet Communications" by A. Johnston and H. Sinnreich. Work in progress, Internet Draft, IETF, March 2006.

[23] RFC 4787: "NAT Behavioral Requirements for Unicast UDP" by F. Audet and C. Jennings. IETF, January 2007.

[24] "Managing Client Initiated Connections in SIP" by C. Jennings and R. Mahy, work in progress, < draft-ietf-sip- outbound>, IETF, June 2006.

[25] RFC 3489bis: "Simple Traversal Under NAT (STUN)" by J. Rosenberg et al. Work in progress, < draft-ietf-behave-rfc3489bis> , IETF, July 2006.

[26] "Obtaining Relay Addresses from Simple Traversal of UDP Through NAT (STUN)" by J. Rosenberg, <draft-ietf-behave-turn>, work in progress, IETF, February 2006.

[27] "Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offer/Answer Protocols" by J. Rosenberg. Work in progress, <draft-ietf-mmusic-ice>, IETF, August 2006.

[28] "Best Current Practices for NAT Traversal for SIP" by C. Boulton et al. Work in progress, < draft-ietf-sipping-nat-scenarios>, IETF, June 2006.

[29] "ZRTP: Extensions to RTP for Diffie-Hellman Key Agreement for SRTP" by P. Zimmermann et al. Work in progress, IETF, March 2006.

[30] "Enhancements for Authenticated Identity Management in SIP" by J. Peterson and C. Jennings, <draft-ietf-sip-identity>, work in progress, IETF, October 2005

Author's Addresses

Henry Sinnreich
Adobe Systems, Inc.
601 Townsend Street,
San Francisco, CA 94103, USA
Email: henrys@adobe.com

Alan B. Johnston
Avaya
Saint Louis, MO, USA
Email: alan@sipstation.com

Eunsoo Shim
Locus Telecommunications, Inc.
111 Sylvan Avenue
Englewood Cliffs, NJ 07632 USA
eunsoo@locus.net

Kundan Singh
Adobe Systems, Inc.
601 Townsend Street,
San Francisco, CA 94103, USA
Email: kundan@adobe.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary

rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.