SPEERMINT Working Group
Internet-Draft
Intended status: Informational
Expires: August 28, 2008

J-F. Mule
CableLabs

February 25, 2008

SPEERMINT Requirements for SIP-based VoIP Interconnection
draft-ietf-speermint-requirements-04.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/1id-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 August 28, 2008.

Copyright Notice

Abstract

A number of use cases have been described for session peering of voice, presence, instant messaging and other types of multimedia traffic. This memo captures some of the requirements identified by these use case scenarios. It is intended to become an informational document linking the use cases to potential protocol solutions.

Table of Contents

1. Introduction

Peering at the session level represents an agreement between parties to allow the exchange of multimedia traffic. It is assumed that these sessions use the Session Initiation Protocol (SIP) protocol to enable peering between two or more actors. These actors are called SIP Service Providers (SSPs) and they are typically represented by users, user groups such as enterprises, real-time collaboration service communities, or other service providers offering voice or multimedia services.

Common terminology for SIP session peering is defined ([I-D.ietf-speermint-terminology]) and a reference architecture is described in [I-D.ietf-speermint-architecture]. A number of use cases have been exposed by users of SIP services and various other actors describing how layer-5 peering has been or could be deployed based on the reference architecture ([I-D.ietf-speermint-voip-consolidated-usecases] and [I-D.ietf-speermint-consolidated-presence-im-usecases]).

Peering at the session layer can be achieved on a bilateral basis (direct peering established directly between two SSPs), or on an indirect basis via an intermediary (indirect peering via a third-party SSP that has a trust relationship with the SSPs) - see the terminology document for more details.

This document first describes general requirements that have been derived from the working group discussions. The use cases are then analyzed in the spirit of extracting relevant protocol requirements that must be met to accomplish the use cases. These requirements are intended to be independent of the type of media exchanged such as Voice over IP (VoIP), video telephony, and instant messaging. In the case where some requirements are media-specific, we define them in a separate section.

It is not the goal of this document to mandate any particular use of IETF protocols by SIP Service Providers in order to establish session peering. Instead, the document highlights what requirements should be met and what protocols may be used to define the solution space.

Finally, we conclude with a list of parameters for the definition of a session peering policy, provided in an informative appendix. It should be considered as an example of the information SIP Service Providers may have to discuss or agree on to exchange SIP traffic.

2. Terminology

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 [RFC2119].

This document also reuses the SIP terminology defined in [I-D.ietf-speermint-terminology]. It is assumed that the reader is familiar with the Session Description Protocol (SDP) [RFC4566] and the Session Initiation Protocol (SIP) [RFC3261].

3. General Requirements

The following sub-sections contain general requirements applicable to multiple use cases for multimedia session peering.

3.1. Scope

The primary focus of this document is on the requirements applicable to the boundaries of Layer 5 SIP networks: SIP entities and Signaling path Border Elements (SBEs); any requirements touching SIP UA or end-devices are considered out of scope.

SSPs desiring to establish session peering relationships have to reach an agreement on numerous aspects.

This document highlights only certain aspects of a session peering agreement, mostly the requirements relevant to protocols, including the declaration, advertisement and management of ingress and egress for session signaling and media, information related to the Session Establishment Data (SED), and the security mechanisms a peer may use to accept and secure session exchanges.

Numerous other aspects of session peering arrangement are critical to reach a successful agreement but they are considered out of scope of the SPEERMINT working group. They include aspects such as SIP protocol support (e.g. SIP extensions and field conventions), media (e.g., type of media traffic to be exchanged, compatible media codecs and media transport protocols, mechanisms to ensure differentiated quality of service for media), SIP layer-3 IP connectivity between the Signaling Path and Data Path Border Elements, traffic capacity control (e.g. maximum number of SIP sessions at each ingress point, maximum number of concurrent IM or VoIP sessions), and accounting.

The informative Appendix A lists parameters that SPPs may consider when discussing the technical aspects of SIP session peering. The purpose of this list which has evolved through the working group use case discussions is to capture the parameters that are considered outside the scope of the protocol requirements.

3.2. Session Peering Points

For session peering to be scalable and operationally manageable, maximum flexibility should be given for how signaling path and media path border elements are declared, dynamically advertised and updated.

Indeed, in any session peering environment, there is a need for a SIP Service Provider to declare or dynamically advertise the SIP entities

that will face the peer's network. The media or data path border elements are typically signaled dynamically in the session description.

The use cases defined ([I-D.ietf-speermint-voip-consolidated-usecases]) catalog the various session peering points between SIP Service Providers; they include Signaling Path Border Elements (SBEs) and SIP proxies (or any SIP entity at the boundary of the Layer 5 network).

- Requirement #1:
  Protocol mechanisms must exist for a SIP Service Provider (SSP) to communicate the ingress Signaling Path Border Elements of its service domain.

  Notes on solution space:
  The SBEs may be advertised to session peers using static mechanisms or they may be dynamically advertised. There seems to be general agreement that [RFC3263] provides a solution for dynamically advertising ingress SBEs in most cases of Direct or Indirect peering. However, this DNS-based solution may be limited in cases where the DNS response varies based on who sends the query (peer-dependent SBEs, see below).

- Requirement #2:
  Protocol mechanisms should exist for a SIP Service Provider (SSP) to communicate the egress SBEs of its service domain.

  Notes on motivations for this requirement:
  For the purposes of capacity planning, traffic engineering and call admission control, a SIP Service Provider may be asked where it will generate SIP calls from. Note that this may not be applicable to all types of session peering (voice may be a particular case where this is needed -- at least based on current practices).

If the SSP also provides media streams to its users as shown in the use cases for "Originating" and "Terminating" SSPs, a mechanism should exist to allow SSPs to advertise their media border elements responsible for egress and ingress data path border elements (DBEs), if applicable. While some SPPs may have open policies and accept media traffic from anywhere outside their network to anywhere inside their network, some SSPs may want to optimize media delivery and identify media paths between peers prior to traffic being sent (layer 5 to layer 3 QoS mapping).

- Requirement #3:
  Protocol mechanisms should be available to allow a SIP Service

Provider to communicate its DBEs to its peers.

Notes: Some SSPs engaged in SIP interconnects do exchange this type of DBE information today in a static manner. Some SSPs do not.

Some SSPs may have some restrictions on the type of media traffic their SIP entities acting as SBEs are capable of establishing. In order to avoid a failed attempt to establish a session, a mechanism may be provided to allow SSPs to indicate if some restrictions exist on the type of media traffic: ingress and egress SBE points may be peer-dependent, and/or media-dependent.

- Requirement #4:
  The mechanisms recommended for the declaration or advertisement of SBE and DBE entities must allow for peer and media variability.

  Notes on solution space:
  For advertising peer-dependent SBEs (peer variability), the solution space based on [RFC3263] is under specified and there are no know best current practices. Is DNS the right place for putting data that varies based on who asks?
  For advertising media-dependent SBEs, solutions exist as long as URIs are protocol-dependent URIs. A protocol-dependent URI like a SIP URI can be mapped to more than one types of media. It should be noted that some URIs like the IM URI are abstract ([RFC3428]) and need to be translated to protocol dependent URIs. It is also not possible to know what media is supported by the SIP SBE before initiating a query by using mechanisms like [RFC3263].

The following example provides some additional motivations for the above requirement on advertising media-dependent SBEs to peers.
In large multi-service SIP networks, an SSP chooses to have several SBEs for receiving incoming SIP session requests (ingress SBEs), and several SBEs for outgoing SIP session requests (egress SBEs). In order to facilitate the operations, feature management, and maintenance of its SBEs, the SSP opts for having distinct SBEs for voice, real-time collaboration, etc. Some SBEs are therefore dedicated to exchanging certain types of media traffic due to specific SIP extensions required for certain media types (e.g. SIMPLE, the SIP MESSAGE Method for Instant Messaging [RFC3428] or the Message Sessions Relay Protocol (MSRP)). Note that this example is applicable to some enterprise networks where IP voice traffic hits different SIP gateways and voice servers (e.g. IP-PBX) than Instant Messaging and real-time collaboration servers (e.g. real-time collaboration and IM server supporting SIMPLE and XMPP).

In the use cases provided as part of direct and indirect scenarios,

an SSP deals with multiple SIP entities and multiple SBEs in its own domain. There is often a many-to-many relationship between SIP Proxies and Signaling path Border Elements.
It should be possible for an SSP to define which egress SBE a SIP entity must use based on a given peer destination. For example, in the case of an indirect peering scenario (section 5.1.5 of [I-D.ietf-speermint-voip-consolidated-usecases], Figure 5), it should be possible for the O-Proxy to choose the appropriate O-SBE based on the information the O-Proxy receives from the Lookup Function (LUF) or Location Routing Function (LRF) - message response labeled (3).
Note that this example also applies to the case of Direct Peering when a service provider has multiple service areas and each service area involves multiple SIP Proxies and a few SBEs.

o Requirement #5:
The mechanisms recommended for the lookup and location routing service must be capable or returning both a target URI destination and a SIP Route.

Notes: solutions exist if the protocol used between the Proxy and the LUF/LRF is SIP; if ENUM is used, the author of this document does not know of any solution today.

It is desirable for an SSP to be able to communicate how authentication of a peer's SBEs will occur (see the security requirements for more details).

o Requirement #6:
The mechanisms recommended for locating a peer's SBE must be able to convey how a peer should initiate secure session establishment.

Notes : certain mechanisms exist; for example, the required protocol use of SIP over TLS may be discovered via [RFC3263].

3.3. Session Establishment Data

The Session Establishment Data (SED) is defined in [I-D.ietf-speermint-terminology] as the data used to route a call to the next hop associated with the called domain's ingress point. The following paragraphs capture some general requirements on the SED data.

3.3.1. User Identities and SIP URIs

User identities used between peers can be represented in many different formats. Session Establishment Data should rely on URIs (Uniform Resource Identifiers, [RFC3986]) and SIP URIs should be preferred over tel URIs ([RFC3966]) for session peering of VoIP

traffic.
The use of DNS domain names and hostnames is recommended in SIP URIs and they should be resolvable on the public Internet. It is recommended that the host part of SIP URIs contain a fully-qualified domain name instead of a numeric IPv4 or IPv6 address. As for the user part of the SIP URIs, the mechanisms for session peering should not require an SSP to be aware of which individual user identities are valid within its peer's domain.

o Requirement #7:
The protocols used for session peering must accommodate the use of different types of URIs. URIs with the same domain-part should share the same set of peering policies, thus the domain of the SIP URI may be used as the primary key to any information regarding the reachability of that SIP URI.

o Requirement #8:
The mechanisms for session peering should not require an SSP to be aware of which individual user identities are valid within its peer's domain.

o Notes on the solution space for #7 and #8:
This is generally well supported by IETF protocols. When telephone numbers are in tel URIs, SIP requests cannot be routed in accordance with the traditional DNS resolution procedures standardized for SIP as indicated in [RFC3824]. This means that the solutions built for session peering must not solely use PSTN identifiers such as Service Provider IDs (SPIDs) or Trunk Group IDs (they should not be precluded but solutions should not be limited to these).
Motivations:
Although SED data may be based on E.164-based SIP URIs for voice interconnects, a generic peering methodology should not rely on such E.164 numbers.

3.3.2. URI Reachability

Based on a well-known URI type (for e.g. sip, pres, or im URIs), it must be possible to determine whether the SSP domain servicing the URI allows for session peering, and if it does, it should be possible to locate and retrieve the domain's policy and SBE entities.
For example, an originating service provider must be able to determine whether a SIP URI is open for direct interconnection without requiring an SBE to initiate a SIP request. Furthermore, since each call setup implies the execution of any proposed algorithm, the establishment of a SIP session via peering should incur minimal overhead and delay, and employ caching wherever possible to avoid extra protocol round trips.

o Requirement #9:
The mechanisms for session peering must allow an SBE to locate its peer SBE given a URI type and the target SSP domain name.

3.4. Other Considerations

The considerations listed below were gathered early on in the SPEERMINT working group as part of discussions to define the scope of the working group. They have not been updated in this revision of the draft.

o It is assumed that session peering is independent of lower layers. The mechanisms used to establish session peering should accommodate diverse supporting lower layers. It should not matter whether lower layers rely on the public Internet or are implemented by private L3 connectivity, using firewalls or L2/L3 Virtual Private Networks (VPNs), IPSec tunnels or Transport Layer Security (TLS) connections [RFC3546]...

o Session Peering Policies and Extensibility:
Mechanisms developed for session peering should be flexible and extensible to cover existing and future session peering models. It is also recommended that SSP policies be published via local configuration choices in a distributed system like DNS rather than in a centralized system like a 'peering registry'.
In the context of session peering, a policy is defined as the set of parameters and other information needed by an SPP to connect to another. Some of the session policy parameters may be statically exchanged and set throughout the lifetime of the peering relationship. Others parameters may be discovered and updated dynamically using by some explicit protocol mechanisms. These dynamic parameters may also relate to an SSP's session-dependent or session independent policies as defined in [I-D.ietf-sipping-session-policy].

o Administrative and Technical Policies:
Various types of policy information may need to be discovered or exchanged in order to establish session peering. At a minimum, a policy should specify information related to session establishment data in order to avoid session establishment failures. A policy may also include information related to QoS, billing and accounting, layer-3 related interconnect requirements which are out of the scope of this document, see examples in Section Appendix A.

Motivations:
The reasons for declining or accepting incoming calls from a prospective peering partner can be both administrative

(contractual, legal, commercial, or business decisions) and technical (certain QoS parameters, TLS keys, domain keys, ...). The objectives are to provide a baseline framework to define, publish and optionally retrieve policy information so that a session establishment does not need to be attempted to know that incompatible policy parameters will cause the session to fail (this was originally referred to as "no blocked calls").

4. Considerations and Requirements for Session Peering of Presence and Instant Messaging

This section describes requirements for presence and instant messaging session peering. Several use cases for presence and instant messaging peering are described in [I-D.ietf-speermint-consolidated-presence-im-usecases], a document authored by A. Houri, E. Aoki and S. Parameswar. Credits for this section must go to A. Houri, E. Aoki and S. Parameswar.

The following requirements for presence and instant messaging session peering are derived from [I-D.ietf-speermint-consolidated-presence-im-usecases] and [I-D.houri-speermint-presence-im-requirements]:

- Requirement #10:
  The mechanisms recommended for the exchange of presence information between SSPs MUST allow a user of one SSP's presence community to subscribe presentities served by another SSP via its local community, including subscriptions to a single presentity, a personal, public or ad-hoc group list of presentities.

  Notes: see section 2.2 of [I-D.ietf-speermint-consolidated-presence-im-usecases].

- Requirement #11:
  The mechanisms recommended for Instant Messaging message exchanges between SSPs MUST allow a user of one SSP's community to communicate with users of the other SSP community via their local community using various methods. Such methods include sending a one-time IM message, initiating a SIP session for transporting sessions of messages, participating in n-way chats using chat rooms with users from the peer SSPs, sending a file or sharing a document.

  Notes: see section 2.6 of [I-D.ietf-speermint-consolidated-presence-im-usecases].

- Requirement #12: Privacy Sharing
  In order to enable sending less notifications between communities, there should be a mechanism that will enable sharing privacy information of users between the communities. This will enable sending a single notification per presentity that will be sent to the appropriate watchers on the other community according to the presentity's privacy information.
  The privacy sharing mechanism must be done in a way that will enable getting the consent of the user whose privacy will be sent to the other community prior to sending the privacy information.

if user consent is not give, it should not be possible to this optimization. In addition to getting the consent of users regarding privacy sharing, the privacy data must be sent only via secure channels between communities.

Notes: see section 2.3 of [I-D.ietf-speermint-consolidated-presence-im-usecases].

- Requirement #13: Multiple Recipients
  It should be possible to send a presence document with a list of watchers on the other community that should receive the presence document notification. This will enable sending less presence document notifications between the communities while avoiding the need to share privacy information of presentities from one community to the other.

- Requirement #14: Mappings
  Early deployments of SIP based presence and IM gateways are done in front of legacy proprietary systems that use different names for different properties that exist in PIDF. For example "Do Not Disturb" may be translated to "Busy" in another system. In order to make sure that the meaning of the status is preserved, there is a need that either each system will translate its internal statuses to standard PIDF based statuses of a translation table of proprietary statuses to standard based PIDF statuses will be provided from one system to the other.

5. Security Requirements

Session peering does bring a new environment in which security requirements should be analyzed but the fundamental mechanisms for securing SIP and media exchanges remain applicable (see Section 26.2 of [RFC3261]. The issues are less in the mechanisms that do exist and can be used to mitigate threats than they are in getting two SSPs to agree on which ones to use.

This section first provides a broad picture of the various mechanisms used today in the context of SIP session peering. We then describe security considerations for the three types of information flows described in the use cases: the data queried from the Lookup or Location Routing Functions, data exchanged in the SIP signaling between SSPs (directly and indirectly), and media.

5.1. Security in SIP networks in the context of session peering

In today's SIP deployments, various approaches exist to secure exchanges between SIP Service Providers. Lookup, signaling and media security are the three primary topics for consideration in most deployments.
A number of transport, network and session-level mechanisms are used for SIP by some categories of SSPs. TLS is used in the enterprise networks for applications such as VoIP and secure Instant Messaging and session-level security is used end-to-end for some instant messaging systems or in service provider networks for Instant Messaging and presence applications. At the network-level, IPsec and L2/L3 VPNs are widely used in some SSP networks where there is a desire to secure all signaling and media traffic at or below the IP layer.
Media level security between providers is not widely used today for media transported using the Real-Time Protocol (RTP), even though it is in use in few deployments where the privacy of voice and other RTP media is critical.

A security threat analysis provides guidance for session peering ([I-D.draft-niccolini-speermint-voipthreats]). More discussions based on this threat analysis and use cases continue to be required in the working group to define what hop-by-hop or end-to-end security requirements are necessary in the context of session peering.

5.2. Security Requirements for the Lookup and Location Routing Data

The Look-Up Function (LUF) and Location Routing Function (LRF) are defined in [I-D.ietf-speermint-terminology]. They provide a mechanism for determining for a given request the target domain to which the request should be routed, and SED required to route the

request to that domain.

Requirement #15:
The protocols used for the LUF and LRF must allow the look-up and SED data to be exchanged securely (authentication and encryption services should be provided).

Notes on the solution space: ENUM, SIP and proprietary protocols are typically used today for accessing these functions.

5.3. Hop-by-hop Security for SIP Signaling and TLS Considerations

Given the direct and indirect peering uses cases referenced in the previous sections of this document, hop-by-hop security between two SSPs using Transport Layer Security (TLS) is desirable.

The Transport Layer Security (TLS) is a standard way to secure signaling between SIP entities. TLS can be used in direct peering to mutually authenticate SSPs and provide message confidentiality and integrity protection. The remaining paragraphs explore how TLS could be deployed and used between 2 SSPs to secure SIP exchanges. The intent is to capture what two SSPs should discuss and agree on in order to establish TLS connections for SIP session peering.

1. One or more Certificate Authorities (CAs) should be agreed between SSPs for securing session peering exchanges. Alternatively, self-signed certificates may also be used.

   Motivations:
   An SSP should have control over which root CAs it trusts for SIP communications. This may imply creating a certificate trust list and including the peer's CA for each authorized domain. In the case of a federation, this requirement allows for the initiating side to verify that the server certificate chains up to a trusted root CA. This also means that SIP servers should allow the configuration of a certificate trust list in order to allow an SSP to control which peer's CAs are trusted for TLS connections. Note that these considerations seem to be around two themes: one is trusting a root, the other is trusting intermediate CAs.
   There are various use cases of direct peering where there is no pre-established trust relationship that can rely on self-signed certificates.

2. Peers should indicate whether their domain policies require proxy servers to inspect and verify the identity provided in SIP requests as defined in [RFC4474]. Federations supporting [RFC4474] and CA(s) must specify the CA(s) permitted to issue certificates of the authentication service.

3. SIP entities and SBEs involved in the secure session establishment over TLS must have valid X.509 certificates and must be able to receive a TLS connection on a well-known port as defined in [RFC3261].

4. The following SIP and TLS protocol parameters should be agreed upon as part of session peering policies: the version of TLS supported by SIP entities and SBEs (TLSv1, TLSv1.1), the SIP TLS port (default 5061), the server-side session timeout (default 300 seconds), the list of supported or recommended ciphersuites, the list of trusted root CAs if applicable or whether self-signed certs are acceptable.

5. SIP entities and SBEs involved in the session establishment over TLS must verify and validate the client certificates. See section 9 and 9.3 of [I-D.ietf-sip-certs].

6. A session peering policy should include details on SIP session establishment over TLS if TLS is supported.

5.4. End-to-End Media Security

Media security is critical to guarantee end-to-end confidentiality of the communication between the end-users' devices, independently of how many direct or indirect peers are along the signaling path.

o Requirement #16:
It is recommended that the establishment of media security be provided along the media path and not over the signaling path given the indirect peering use cases.

Notes on the solution space:
Media carried over the Real-Time Protocol (RTP) can be secured using secure RTP or sRTP ([RFC3711]). A framework for establishing sRTP security using Datagram TLS [RFC4347] is described in [I-D.ietf-sip-dtls-srtp-framework]: it allows for end-to-end media security establishment using extensions to DTLS ([I-D.ietf-avt-dtls-srtp]). This DTLS-SRTP framework meets the above requirement.

Note that media can also be carried in numerous protocols other than RTP such as SIP (SIP MESSAGE method), MSRP, XMPP, etc. In these cases, the above requirement is also met given the security features of these protocols.

6. Acknowledgments

This document is a work-in-progress and it is based on the input and contributions made by a large number of people in the SPEERMINT working group, including: Edwin Aoki, Scott Brim, John Elwell, Mike Hammer, Avshalom Houri, Richard Shocky, Henry Sinnreich, Richard Stastny, Patrik Faltstrom, Otmar Lendl, Daryl Malas, Dave Meyer, Sriram Parameswar, Jon Peterson, Jason Livingood, Bob Natale, Benny Rodrig, Brian Rosen, Eric Rosenfeld, Adam Uzelac and Dan Wing. Specials thanks go to Rohan Mahy, Brian Rosen, John Elwell for their initial drafts describing guidelines or best current practices in various environments, and to Avshalom Houri, Edwin Aoki and Sriram Parameswar for authoring the presence and instant messaging requirements.

7. IANA Considerations

None.

8. Security Considerations

Securing session peering communications involves numerous protocol exchanges, first and foremost, the securing of SIP signaling and media sessions. The security considerations contained in [RFC3261], and [RFC4474] are applicable to the SIP protocol exchanges. A number of security considerations are also described in Section Section 5.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

9.2. Informative References

[I-D.draft-malas-performance-metrics]
Malas, D., "SIP End-to-End Performance Metrics", December 2007.

[I-D.draft-niccolini-speermint-voipthreats]
Niccolini, S., Chen, E., and J. Seedorf, "VoIP Security Threats relevant to SPEERMINT", draft-niccolini-speermint-voipthreats-03.txt (work in progress), February 2008.

[I-D.houri-speermint-presence-im-requirements]
Houri, A., Aoki, E., and S. Parameswar, "Presence and IM Requirements", May 2007.

[I-D.ietf-avt-dtls-srtp]
McGrew, D. and E. Rescorla, "DTLS Extensions to Establish Keys for SRTP", draft-ietf-avt-dtls-srtp-01.txt (work in progress), November 2007.

[I-D.ietf-sip-certs]
Jennings, C., Peterson, J., and J. Fischl, "Certificate Management Service for The Session Initiation Protocol (SIP)", draft-ietf-sip-certs-05.txt (work in progress), January 2008.

[I-D.ietf-sip-dtls-srtp-framework]
Fischl, J., Tschofenig, H., and E. Rescorla, "DTLS-SRTP Framework", draft-ietf-sip-dtls-srtp-framework-01 (work in progress), February 2008.

[I-D.ietf-sip-hitchhikers-guide]
Rosenberg, J., "A Hitchhikers Guide to the Session Initiation Protocol (SIP)", July 2007.

[I-D.ietf-sipping-session-policy]
Hilt, V. and G. Camarillo, "A Session Initiation Protocol (SIP) Event Package for Session-Specific Session Policies", draft-ietf-sipping-policy-package-04.txt (work in progress), August 2007.

[I-D.ietf-speermint-architecture]
Penno et al., R., "SPEERMINT Peering Architecture", draft-ietf-speermint-architecture-04.txt (work in progress), August 2007.

[I-D.ietf-speermint-consolidated-presence-im-usecases]
Houri, A., Aoki, E., and S. Parameswar, "Presence & Instant Messaging Peering Use Cases", draft-ietf-speermint-consolidated-presence-im-usecases-04 (work in progress), February 2008.

[I-D.ietf-speermint-terminology]
Meyer, R. and D. Malas, "SPEERMINT Terminology", draft-ietf-speermint-terminology-16.txt (work in progress), February 2008.

[I-D.ietf-speermint-voip-consolidated-usecases]
Uzelac et al., A., "VoIP SIP Peering Use Cases", draft-ietf-speermint-voip-consolidated-usecases-05.txt (work in progress), February 2008.

[RFC2198] Perkins, C., Kouvelas, I., Hodson, O., Hardman, V., Handley, M., Bolot, J., Vega-Garcia, A., and S. Fosse-Parisis, "RTP Payload for Redundant Audio Data", RFC 2198, September 1997.

[RFC3261] 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.

[RFC3263] Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

[RFC3428] Campbell, B., Rosenberg, J., Schulzrinne, H., Huitema, C., and D. Gurle, "Session Initiation Protocol (SIP) Extension for Instant Messaging", RFC 3428, December 2002.

[RFC3455] Garcia-Martin, M., Henrikson, E., and D. Mills, "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)", RFC 3455, January 2003.

[RFC3546] Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, "Transport Layer Security (TLS) Extensions", RFC 3546, June 2003.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003.

[RFC3603] Marshall, W. and F. Andreasen, "Private Session Initiation Protocol (SIP) Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture", RFC 3603, October 2003.

[RFC3611] Friedman, T., Caceres, R., and A. Clark, "RTP Control Protocol Extended Reports (RTCP XR)", RFC 3611, November 2003.

[RFC3702] Loughney, J. and G. Camarillo, "Authentication, Authorization, and Accounting Requirements for the Session Initiation Protocol (SIP)", RFC 3702, February 2004.

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, March 2004.

[RFC3824] Peterson, J., Liu, H., Yu, J., and B. Campbell, "Using E.164 numbers with the Session Initiation Protocol (SIP)", RFC 3824, June 2004.

[RFC3966] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, December 2004.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[RFC4347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, April 2006.

[RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, August 2006.

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.

Appendix A. Policy Parameters for Session Peering

This informative section lists various types of parameters that should be first considered by implementers when deciding what configuration parameters to expose to system admins or management stations, and second, by SSPs or federations of SSPs when discussing the technical aspects of a session peering policy.

Some aspects of session peering policies must be agreed to and manually implemented; they are static and are typically documented as part of a business contract, technical document or agreement between parties. For some parameters linked to protocol support and capabilities, standard ways of expressing those policy parameters may be defined among SSP and exchanged dynamically. For e.g., templates could be created in various document formats so that it could be possible to dynamically discover some of the domain policy. Such templates could be initiated by implementers (for each software/ hardware release, a list of supported RFCs, RFC parameters is provided in a standard format) and then adapted by each SSP based on its service description, server or device configurations and variable based on peer relationships.

A.1. Categories of Parameters and Justifications

The following list should be considered as an initial list of "discussion topics" to be addressed by peers when initiating a VoIP peering relationship.

o IP Network Connectivity:
Session peers should define how the IP network connectivity between their respective SBEs and DBEs. While this is out of scope of session peering, SSPs must agree on a common mechanism for IP transport of session signaling and media. This may be accomplish via private (e.g. IPVPN, IPsec, etc.) or public IP networks.

o Media-related Parameters:

* Media Codecs: list of supported media codecs for audio, real-time fax (version of T.38, if applicable), real-time text (RFC 4103), DTMF transport, voice band data communications (as applicable) along with the supported or recommended codec packetization rates, level of RTP paylod redundancy, audio volume levels, etc.

* Media Transport: level of support for RTP-RTCP [RFC3550], RTP Redundancy (RTP Payload for Redundant Audio Data - [RFC2198]) , T.38 transport over RTP, etc.

* Other: support of the VoIP metric block as defined in RTP Control Protocol Extended Reports [RFC3611] , etc.

o SIP:

* A session peering policy should include the list of supported and required SIP RFCs, supported and required SIP methods (including private p headers if applicable), error response codes, supported or recommended format of some header field values , etc.

* It should also be possible to describe the list of supported SIP RFCs by various functional groupings. A group of SIP RFCs may represent how a call feature is implemented (call hold, transfer, conferencing, etc.), or it may indicate a functional grouping as in [I-D.ietf-sip-hitchhikers-guide].

o Presence and Instant Messaging: TBD

o Accounting:
Methods used for call or session accounting should be specified. An SSP may require a peer to track session usage. It is critical for peers to determine whether the support of any SIP extensions for accounting is a pre-requisite for SIP interoperability. In some cases, call accounting may feed data for billing purposes but not always: some operators may decide to use accounting as a 'bill and keep' model to track session usage and monitor usage against service level agreements.
[RFC3702] defines the terminology and basic requirements for accounting of SIP sessions. A few private SIP extensions have also been defined and used over the years to enable call accounting between SSP domains such as the P-Charging* headers in [RFC3455], the P-DCS-Billing-Info header in [RFC3603], etc.

o Performance Metrics:
Layer-5 performance metrics should be defined and shared between peers. The performance metrics apply directly to signaling or media; they may be used pro-actively to help avoid congestion, call quality issues or call signaling failures, and as part of monitoring techniques, they can be used to evaluate the performance of peering exchanges.
Examples of SIP performance metrics include the maximum number of SIP transactions per second on per domain basis, Session Completion Rate (SCR), Session Establishment Rate (SER), etc. Some SIP end-to-end performance metrics are defined in [I-D.draft-malas-performance-metrics]; a subset of these may be applicable to session peering and interconnects.
Some media-related metrics for monitoring VoIP calls have been

defined in the VoIP Metrics Report Block, in Section 4.7 of [RFC3611].

o Security:
An SSP should describe the security requirements that other peers must meet in order to terminate calls to its network. While such a list of security-related policy parameters often depends on the security models pre-agreed to by peers, it is expected that these parameters will be discoverable or signaled in the future to allow session peering outside SSP clubs. The list of security parameters may be long and composed of high-level requirements (e.g. authentication, privacy, secure transport) and low level protocol configuration elements like TLS parameters.
The following list is not intended to be complete, it provides a preliminary list in the form of examples:

* Call admission requirements: for some providers, sessions can only be admitted if certain criteria are met. For example, for some providers' networks, only incoming SIP sessions signaled over established IPSec tunnels or presented to the well-known TLS ports are admitted. Other call admission requirements may be related to some performance metrics as descrived above. Finally, it is possible that some requiremetns be imposed on lower layers, but these are considered out of scope of session peering.

* Call authorization requirements and validation: the presence of a caller or user identity may be required by an SSP. Indeed, some SSPs may further authorize an incoming session request by validating the caller's identity against white/black lists maintained by the service provider or users (traditional caller ID screening applications or IM white list).

* Privacy requirements: an SSP may demand that its SIP messages be securely transported by its peers for privacy reasons so that the calling/called party information be protected. Media sessions may also require privacy and some SSP policies may include requirements on the use of secure media transport protocols such as sRTP, along with some contraints on the minimum authentication/encryption options for use in sRTP.

* Network-layer security parameters: this covers how IPSec security associated may be established, the IPSec key exchange mechanisms to be used and any keying materials, the lifetime of timed Security Associated if applicable, etc.

* Transport-layer security parameters: this covers how TLS connections should be established as described in Section

Section 5.

A.2. Summary of Parameters for Consideration in Session Peering Policies

The following is a summary of the parameters mentioned in the previous section. They may be part of a session peering policy and appear with a level of requirement (mandatory, recommended, supported, ...).

- o IP Network Connectivity (assumed, requirements out of scope of this document)

- o Media session parameters:

  * Codecs for audio, video, real time text, instant messaging media sessions

  * Modes of communications for audio (voice, fax, DTMF), IM (page mode, MSRP)

  * Media transport and means to establish secure media sessions

  * List of ingress and egress DBEs where applicable, including STUN Relay servers if present

- o SIP

  * SIP RFCs, methods and error responses

  * headers and header values

  * possibly, list of SIP RFCs supported by groups (e.g. by call feature)

- o Accounting

- o Capacity Control and Performance Management: any limits on, or, means to measure and limit the maximum number of active calls to a peer or federation, maximum number of sessions and messages per specified unit time, maximum number of active users or subscribers per specified unit time, the aggregate media bandwidth per peer or for the federation, specified SIP signaling performance metrics to measure and report; media-level VoIP metrics if applicable.

- o Security: Call admission control, call authorization, network and transport layer security parameters, media security parameters

Author's Address

Jean-Francois Mule
CableLabs
858 Coal Creek Circle
Louisville, CO 80027
USA

Email: jf.mule@cablelabs.com

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).