SPEERMINT Working Group
Internet-Draft
Intended status: Informational
Expires: May 22, 2008

J-F. Mule
CableLabs
November 19, 2007

SPEERMINT Requirements for SIP-based VoIP Interconnection
draft-ietf-speermint-requirements-03.txt

Status of this Memo

Copyright Notice

Abstract

A number of use cases have been identified for session peering of voice and other types of multimedia traffic. This memo captures some of the requirements that enable these use case scenarios. In its current version, this document describes both general and use case specific requirements for session peering for multimedia interconnect. It is intended to become an informational document linking the use cases with potential protocol solutions.

Table of Contents

1. Introduction

Peering at the session level represents an agreement between parties to allow the exchange of traffic according to a policy. It is assumed that these sessions use the Session Initiation Protocol (SIP) protocol to enable peering between two or more actors. The actors of SIP session peering are called SIP Service Providers (SSPs) and they are typically represented by users, user groups such as enterprises or 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]. As the traffic exchanged using SIP as the session establishment protocol increases between parties, a number of use cases have been exposed by users of SIP services and various other actors for how session level peering has been or could be deployed based on the reference architecture ([I-D.ietf-speermint-voip-consolidated-usecases]).

Peering at the session layer can be achieved on a bilateral basis (direct peering with SIP sessions 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), or on a multilateral basis (assisted peering using a federation model between SSPs) - see the terminology document for more details.

This document first describes general guidelines that have been derived from the working group discussions in the context of session peering (direct, indirect or assisted). 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 also independent of the type of media exchanged by the parties and should be applicable to any type of multimedia session peering 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 any IETF protocols on SIP Service Providers 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 connect to one another.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [RFC2119].

3. General Requirements

The following sections illustrates general requirements applicable to multiple session peering use cases for multimedia sessions. This memo makes use of the following terms and acronyms defined in [I-D.ietf-speermint-terminology]: SIP Service Provider (SSP), Signaling Path Border Element (SBE), Data Path Border Element (DBE), Session Establishment Data (SED), Layer 3 and Layer 5 peering, session peering, federation, etc. It is assumed that the reader is familiar with the Session Description Protocol (SDP) [RFC4566] and the Session Initiation Protocol (SIP) [RFC3261].

3.1. Scope

SSPs desiring to establish session peering relationships have to reach an agreement on numerous aspects.
This document only addresses 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 and conventions 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 and not addressed in this document. They include aspects such as 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), 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 primary focus of this document is on the requirements applicable to the boundaries of Layer 5 SIP networks: SIP UA or end-device requirements are also considered out of scope.

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 by SSPs, 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 path border elements are typically signaled dynamically in the session messaging; some SSPs may want to statically or dynamically announce these media paths to do proper capacity planning, QoS mapping with lower layers, etc.

The use cases defined ([I-D.ietf-speermint-voip-consolidated-usecases]) catalog the various session peering points between SIP Service Providers; they include the Session Managers (SM) or Signaling Path Border Elements (SBEs).

> Requirement #1: protocol mechanisms must exist for SSPs to communicate the egress and ingress points of its service domain. The session peering points may be advertized to session peers using static mechanisms or they may be dynamically advertized.

> Notes on solution space: there seems to be general agreement that [RFC3263] provides a solution for dynamic advertisements in most cases of Direct, Indirect and Assistent peering use cases. There continues to be discussion on how to best use this to advertize peer-dependent SBEs (see below).

If the SSP also provides media streams to its users as shown in the use cases for the SSPs in the "Originating" and "Terminating" Domains, a mechanism should exist to allow SSPs to advertize their media border elements responsible for egress and ingress points so called Signaling Path Data Elements (SDEs). While some SPPs may have open policies and accept media traffic from anywhere to anywhere inside their network, some SSPs may want to optimize media delivery and identifying media paths between peers prior to traffic being sent.

> Requirement #2: protocol mechanisms must exist for SSPs to communicate the egress and ingress media points or SDEs of its service domain.

> Notes on solution space: SSPs engaged in SIP interconnects do exchange this information today in a static manner.

Some SPP may impose some restrictions on the type of media traffic the 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 #3: the mechanisms recommended for the declaration and advertisement of SBE and SDE entities must allow for peer and media variability.

Notes on solution space: for advertising peer-dependent SBEs (peer variability), the solution space based on is under specified and there are no know best current practices. For advertising media-dependent SBEs, solutions exist as long as URIs are protocol-dependent URIs, and a protocol-dependent URI like a SIP URI can be mapped to one type of media. First, some URIs like the IM URI are abstract ([RFC3428]) and need to be translated to protocol dependent URIs. Second, by using mechamisms available today, it is not possible to know what media is supported by the SIP SBE before initiating a query.

Motivations for the media variability:
While there could be one single Signaling Path Border Element (SBE) in some SSP networks that communicates with all SIP peer networks, an SSP may choose to have one or more SBEs for receiving incoming SIP session requests (ingress signaling points), and one or more SBEs for outgoing SIP session requests (egress signaling points). Ingress and egress signaling points may be distinct SIP entities and could be media-dependent. Some providers deploy SIP entities specialized for voice, real-time collaboration, etc. For example, within an SSP network, some SBEs may be dedicated for 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)).

In the use cases provided as part of direct and indirect scenarios, an SSP may deal with multiple Session Managers and multiple SBEs in its own domain. There is often a many-to-many relationship between Session Managers and Signaling path Border Elements. It should be possible for an SSP to define which egress SBE a Session Manager must use based on a given peer destination. For example, in the case of an indirect peering scenario via Transit PSP (Figure 3 of [I-D.ietf-speermint-voip-consolidated-usecases]), it should be possible for the O-SM to choose the appropriate O-SBE based on the information the O-SM receives in the 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 Session Managers and a few SBEs. This is also implied in the Direct Use Case (section 3.1 of [I-D.ietf-speermint-voip-consolidated-usecases]), by the use of the route terminology in step 3 "Routing database entity replies with route to called party" (route in the sense of both target URI and SIP Route or next hop SIP or SBE entity as defined in [RFC3261]).

Requirement #4: the mechanisms recommended for the location service must be capable or returning both a target URI destination and a SIP Route.

Notes on solution space: solutions exist if the protocol used between the SM and the LS 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 the peer's SBEs will occur (see the security requirements for more details).

Requirement #5: the mechanisms recommended for locating a peer's SBE must be able to convey how a peer should initiate secure session establishment.

Notes on the solution space: certain mechanisms exist, for e.g. the required use of SIP over TLS may be discovered via RFC 3263.

3.3. Session Establishment Data (SED)

The Session Establishment Data (SED) is defined as the data used to route a call or SIP session to the called domain's ingress point ([I-D.ietf-speermint-terminology]). Given that SED is the set of parameters that the Session Managers and outgoing SBEs need to complete the session establishment, some information is shared between SSPs. 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, RFC 3986 [RFC3986]) and SIP URIs should be preferred over tel URIs (RFC 3966 [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.

Requirement #6: the protocols used for session peering must accomodate 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.

Requirement #7: the mechanisms for session peering should not require a peer to be aware of which individual user identities are valid within its peer's domain.

Notes on the solution space for #6 and #7: generally well understood in IETF. 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 RFC 3824 [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 (these 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. As described in [I-D.draft-elwell-speermint-enterprise-usecases], in some use cases for enterprise to enterprise peering (even if a transit SSP is involved), it should be possible to use user identity URIs that do not map to E.164 numbers, e.g. for presence, instant messaging and even for voice.

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.

Requirement #8: the mechanisms for session peering must allow an SBE to locate its peer SBE given a SSP hostname or domain name.

Notes on the solution space: generally well understood in IETF. Open questions exist in how dynamic should the mechanism be to be able to retrieve the domain's policy for secure signaling between SBEs, peer-dependent/media-dependent policies.

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.

- 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

imcompatible policy parameters will cause the session to fail (this was originally referred to as "no blocked calls").

4. Signaling and Media Guidelines for Session Peering

This section provides some guidelines for SIP-based interconnections. This section should be partially or entirely removed from the next revision of this document given the intent of this memo.

4.1. Protocol Specifications

While it is generally agreed that this is out of the scope of speermint, a detailed list of SIP and SDP RFCs the session peers' SBEs must conform to should be provided by SSPs. It is not recommended to rely on Internet-Drafts for commercial SIP interconnects, but if applicable, a list of supported or required IETF Internet-Drafts should be provided. Such specifications should include protocol implementation compliance statements, indicate the minimal extensions that must be supported, and the full details on what options and protocol features must be supported, must not be supported or may be supported. This specification should include a high-level description of the services that are expected to be supported by the peering relationship and it may include sample message flows.

4.2. Minimum set of SIP-SDP-related requirements

The main objective of SIP interconnects being the establishment of successful SIP calls between peer SSPs, this section provides some guidelines for the minimum set of SIP specifications that should be supported by SBEs.

The Core SIP Specifications as defined in [RFC3261] and [I-D.ietf-sip-hitchhikers-guide] MUST be supported by Signaling Path Border Elements (SBEs) and any other SIP implementations involved in session peering. The specifications contained in the Core SIP group provide the fundamental and basic mechanisms required to enable SIP interconnects. The Hitchkiker's guide include specific sections for voice, instant message and presence.

Furthermore, SBE implementers must follow the recommendations contained in RFC 3261 regarding the use of the Supported and Require headers. Signaling Path Border Elements should include the supported SIP extensions in the Supported header and the use of the Require header must be configurable on a per SSP target domain basis in order to match a network peer's policy and to maximize interoperability.

4.3. Media-related Requirements

Compatible codecs must be support by SSPs engaged in session peering. An SSP domain policy should specify media-related parameters that

their user's SIP entities support or that the SSP authorizes in its domain's policy. Direct media exchange between the SSPs' user devices is preferred and media transcoding should be avoided by proposing commonly agreed codecs. Mechanisms employed for IPv4-IPv6 translation of media should also be agreed upon, as well as solutions used for NAT traversal such as ICE [I-D.ietf-ice] and STUN ([RFC3489]).

Motivations: The media capabilities of an SSP's network are either a property of the SIP end-devices, SIP applications, or, a combination of the property of end-devices and Data Path Border Elements that may provide media transcoding.

The choice of one or more common media codecs for SIP sessions between SSPs is outside the scope of SPEERMINT. A list of media-related policy parameters are provided in the informative Appendix A.

For media related security guidance, please refer to Section Section 4.5.

4.4. Requirements for Presence and Instant Messaging

This section lists some presence and Instant Messaging requirements defined in [I-D.presence-im-requirements] and authored by A. Houri, E. Aoki and S. Parameswar. Credits must go to A. Houri, E. Aoki and S. Parameswar.

It was requested to integrate [I-D.presence-im-requirements] into this draft since some of the requirements are generic and non specific to any application type. In particular, requirements numbered PRES-IM-REQ-001, PRES-IM-REQ-002, PRES-IM-REQ-010, PRES-IM-REQ-011, PRES-IM-REQ-015 and PRES-IM_REQ-017 are covered by guidelines provided in other parts of this document.

The numbering of the requirements is as defined in the above mentioned ID. It is expected that as more discussions occur and consensus is achieved in the working group, those requirements will be renumbered or re-written in the mindset of a BCP document. The following list describes requirements for presence and instant messaging session peering:

- o From (PRES-IM-REQ-003, PRES-IM-REQ-004 and PRES-IM-REQ-005): 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 public or private (personal) list of presentities.

o From (PRES-IM-REQ-006, PRES-IM-REQ-007, PRES-IM-REQ-008 and PRES-IM-REQ-009): The mechanisms recommended for Instant Messaging message exchanges between SSPs MUST allow a user of SSP's community to communicate with users of the other SSP community via their local community using various methods, including 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, or sending a file.

o PRES-IM-REQ-012: 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.

o PRES-IM-REQ-013: Privacy Sharing Security - 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.

o PRES-IM-REQ-014: 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.

o PRES-IM-REQ-016: Mappings - A lot of the early deployments of SIP based presence and IM gateways are deployed 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.

4.5. Security Requirements

4.5.1. Security in today's VoIP networks

In today's SIP deployments, various approaches exist to secure exchanges between SIP Service Providers. Signaling and media security are the two primary topics for consideration in most deployments. A number of transport-layer and network-layer mechanisms are widely used for SIP by some categories of SSPs: TLS in the enterprise networks for applications such as VoIP and secure Instant Messaging or in service provider networks for Instant Messaging and presence applications, IPsec and L2/L3 VPNs 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 is not widely used today between providers 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 VoIP session peering ([I-D.draft-niccolini-speermint-voipthreats]). More discussions based on this threat analysis and use cases is required in the working group to define best current practices that this document, or a separate memo should recommend for both signaling and media security.

4.5.2. Signaling Security and TLS Considerations

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. SSPs should agree on one or more Certificate Authorities (CAs) to trust for securing session peering exchanges.
   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 a VSP/ASP 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.

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] must specify the CA(s) permitted to issue certificates of the authentication service.

3. SIP and SBE servers 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.

4. The following SIP and TLS protocol parameters should be agreed upon as part of session peering policies: the version of TLS supported by Signaling Border Elements (TLSv1, TLSv1.1), the SIP TLS port (default 5061), the server-side session timeout (default 300 seconds), the list of supported or recommended ciphersuites, and the list of trusted root CAs.

5. SIP and SBE servers involved in the session establishment over TLS must verify and validate the client certificates: the client certificate must contain a DNS or URI choice type in the subjectAltName which corresponds to the domain asserted in the host portion of the URI contained in the From header. It is also recommended that VSPs/ASPs convey the domain identity in the certificates using both a canonical name of the SIP server(s) and the SIP URI for the domain as described in section 4 of [I-D.gurbani-sip-domain-certs]. On the client side, it is also critical for the TLS client to authenticate the server as defined in [RFC3261] and in section 9 of [I-D.ietf-sip-certs].

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

4.5.3. Media Security

Media security for session peering is as important as signaling security, especially for SSPs that want to continue to meet commonly assumed privacy and confidentiality requirements outside their networks. Media can be secured using secure media transport protocols (e.g. secure RTP or sRTP). The issues of key management protocols for sRTP are being raised in IETF and this continues to be an area where requirements definition and protocol work is ongoing. More consensus is required outside SPEERMINT before best current practices can emerge. See media security requirements for SIP sessions ([I-D.ietf-wing-media-security-requirements]) and its references for more details. Some of these scenarios may be applicable to interdomain SSP session peering.

5. 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.

6. IANA Considerations

None.

7. 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 4.5.

8. References

8.1. Normative References

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

8.2. Informative References

[I-D.Malas-sip-performance]
Malas, D., "SIP End-to-End Performance Metrics", May 2007.

[I-D.draft-elwell-speermint-enterprise-usecases]
Elwell, J. and B. Rodrig, "Use cases for Enterprise Peering using the Session Initiation Protocol", draft-elwell-speermint-enterprise-usecases-00.txt (work in progress), February 2007.

[I-D.draft-niccolini-speermint-voipthreats]
Niccolini, S. and E. Chen, "VoIP Security Threats relevant to SPEERMINT", March 2007.

[I-D.gurbani-sip-domain-certs]
Gurbani, V., Jeffrey, A., and S. Lawrence, "Domain Certificates in the Session Initiation Protocol (SIP)", draft-gurbani-sip-domain-certs-06 (work in progress), June 2007.

[I-D.ietf-ice]
Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", June 2007.

[I-D.ietf-sip-certs]
Jennings, C., Peterson, J., and J. Fischl, "Certificate Management Service for The Session Initiation Protocol (SIP)", May 2007.

[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-03.txt (work in progress), April 2007.

[I-D.ietf-speermint-terminology]
Meyer, R. and D. Malas, "SPEERMINT Terminology", draft-ietf-speermint-terminology-13.txt (work in progress), November 2007.

[I-D.ietf-speermint-voip-consolidated-usecases]
Uzelac et al., A., "VoIP SIP Peering Use Cases", draft-ietf-speermint-voip-consolidated-usecases-03.txt (work in progress), July 2007.

[I-D.ietf-wing-media-security-requirements]
Wing, D., Fries, S., and H. Tschofenig, "Requirements for a Media Security Key Management Protocol", draft-wing-media-security-requirements (work in progress), June 2007.

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

[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.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[RFC2915] Mealling, M. and R. Daniel, "The Naming Authority Pointer (NAPTR) DNS Resource Record", RFC 2915, September 2000.

[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.

[RFC3489] 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.

[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.

[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.

[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.

- IP Network Connectivity:
  Session peers should define how the IP network connectivity between their respective SBEs and SDEs. 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.

- 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.Malas-sip-performance]; 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 4.5.

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 SDEs 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).