SPEERMINT Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: January 10, 2008

J-F. Mule
CableLabs

July 9, 2007

SPEERMINT Requirements for SIP-based VoIP Interconnection
draft-ietf-speermint-requirements-02.txt

Status of this Memo

Copyright Notice

Abstract

This memo defines Best Current Practices for session peering between SIP Service Providers for voice or other types of multimedia traffic exchanges. In its current state, this document describes high-level guidelines and general requirements for session peering for multimedia interconnect . It also defines a minimum set of requirements applicable to session peering for voice over IP, presence and instant messaging interconnects. It is intended to become best current practices based on the use cases discussed in the SPEERMINT working group.

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 describes guidelines and requirements that are intended to become Best Current Practices for session peering (direct, indirect or assisted). 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. The document also defines a minimum set of specific requirements for VoIP, presence and instant messaging interconnects.
It is not the goal of this document to mandate any particular use of any IETF protocols to establish session peering. However, when protocol mechanisms are used, the document aims at providing guidelines or best current practices on how they should be implemented, configured or configurable in order to facilitate session peering.

Finally, a list of parameters for the definition of a session peering policy is provided in an informative appendix. It should be considered as an example of the information a SIP Service Provider may require in order to connect to another using SIP.

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].

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. General Requirements

The following sections define general guidelines and requirements applicable to session peering for multimedia sessions.

3.1. Scope

SSPs desiring to establish session peering relationships have to reach an agreement on numerous aspects.
This document only addresses best current practice for certain aspects of a session peering agreement, 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), the security requirements each peer may enforce on its network to accept and secure session exchanges, and, the format and necessary details to determine the minimum set of parameters required to achieve SIP and SDP interoperability.
Several other aspects of session peering 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 should consider when discussing the technical aspects of SIP session peering.

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 and media entities that will face the peer's network.

An SSP SHOULD declare the signaling border elements responsible for egress and ingress points so called Signaling Path Border Elements (SBEs). If the SSP also provides media streams to its users, an SSP SHOULD declare the media border elements responsible for egress and ingress points so called Signaling Path Data Elements (SDEs); if such

an SSP relies on STUN servers ([RFC3489]) and STUN Relay extensions to permit the traversal of NAT devices, the SSP SHOULD declare those STUN servers as part of its SDEs. It is RECOMMENDED that SSPs use DNS and provide one or more domain names to be used with [RFC3263] to locate SBEs.
An SPP SHOULD also indicate if some restrictions exist on the type of media traffic the SIP entities acting as SBEs are capable of establishing. Ingress and egress SBE points MAY be peer-dependent, and/or media-dependent. An SSP SHOULD be able to accomodate multiple, media-dependent ingress points from a peer's network. The mechanisms recommended for the declaration and advertisement of SBE and SDE entities MUST allow for peer and media variability.

Motivations:
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)).

An SSP SHOULD communicate how authentication of the peer's SBEs will occur (see the security requirements for more details). The use of access control lists based on fixed IP addresses or fixed IP sub-nets of the SBEs is NOT RECOMMENDED as it does not scale: it not only involves an error-prone manual process to configure access control lists but it also prevents peers from dynamically making IP network addressing changes to their SBE egress points without advertising those changes "manually".

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 outgoing SBEs need to complete the session establishment, some information must be shared between SSPs on special requirements or conventions required for a successful session establishment. The following paragraphs capture the recommended best practices for 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]).
The use of DNS domain names and hostnames is RECOMMENDED in SIP URIs and they MUST 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, an SSP SHOULD NOT need to be aware of which individual user identities are valid within a peer's domain.

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.

Motivations:
When SSP support voice, telephone numbers commonly appear in the username portion of a SIP URI. 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]. The recommendations defined in [RFC3824] SHOULD be followed by implementers when using E.164 numbers with SIP. Furthermore, it is commonly assumed that all SIP URIs with the same domain-part 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.

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.

The use of DNS domain names and hostnames is RECOMMENDED in SIP URIs and they MUST be resolvable on the public Internet. The DNS procedures specified in [RFC3263] SHOULD be followed to resolve a SIP URI into a reachable host (IP address and port), and transport protocol. Note that RFC 3263 relies on DNS SRV [RFC2782] and NAPTR Resource Records [RFC2915].

Motivations:
This requirement is important as unsuccessful call attempts are highly undesirable since they can introduce high delays due to timeouts and can act as an unintended denial of service attack (e.g., by repeated TLS handshakes). There should be a high probability of successful call completion for policy-conforming peers.

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 are left here but have been re-written without requirements verbs for the most part.

- Session peering should be 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]...

- 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-framework].

- 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 maximizing SIP-based interconnections between SSPs. It should be considered as the minimal set of requirements to be implemented to perform SIP interconnects for presence, IM, or VoIP.

4.1. Protocol Specifications

A detailed list of SIP and SDP RFCs the session peers' SBEs must conform to must 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.

In the cases of indirect or assisted peering, it is also important that an adequate level of SIP message transparency is available. In particular, the intermediary SBE MUST NOT modify or remove information in the SIP or SDP parameters beyond what is required for the purpose of call routing. In particular, intermediary SBE SHOULD

NOT:

- Remove SIP header lines, SIP header fields and SIP message bodies that are intended for the destination SBE, or the called SIP UA irrespective of whether or not those header lines or parameters are understood by the intermediary SBE;

- Modify header fields and bodies in a way that may break any integrity protection.

4.3. Media-related Requirements

SSPs engaged in session peering SHOULD support of compatible codecs. 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. SSPs SHOULD discuss mechanisms employed for IPv4-IPv6 translation of media, 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:

- 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.

- 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.

- 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.

- 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.

- 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.

- 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 TLS/SIP 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, 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. 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.

7. References

7.1. Normative References

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

7.2. 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-05 (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-framework]
Hilt, V., "A Framework for Session Initiation Protocol (SIP) Session Policies", draft-ietf-sipping-session-policy-framework-01 (work in progress), June 2006.

[I-D.ietf-speermint-architecture]
Penno et al., R., "SPEERMINT Peering Architecture", April 2007.

[I-D.ietf-speermint-terminology]
Meyer, R. and D. Malas, "SPEERMINT Terminology", July 2007.

[I-D.ietf-speermint-voip-consolidated-usecases]
Uzelac et al., A., "VoIP SIP Peering Use Cases", June 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 must 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.

- 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].

- Presence and Instant Messaging: TBD

- 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.

- 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].

- Security:
  A 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, ...).

- IP Network Connectivity (assumed, requirements out of scope of this document)
- 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
- SIP
  - SIP RFCs, methods and error responses
  - headers and header values
  - possibly, list of SIP RFCs supported by groups (e.g. by call feature)
- Accounting
- 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.
- 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

Full Copyright Statement

Intellectual Property

Acknowledgment

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