SPEERMINT	D. Malas, Ed.	
Internet-Draft	CableLabs	
Intended status: Informational	J. Livingood, Ed.	
Expires: May 12, 2011	Comcast	
	November 8, 2010	

TOC

SPEERMINT Peering Architecture
draft-ietf-speermint-architecture-16

Abstract

This document defines a peering architecture for the Session Initiation Protocol (SIP) [RFC3261], it's functional components and interfaces. It also describes the components and the steps necessary to establish a session between two SIP Service Provider (SSP) peering domains.

Status of this Memo

Copyright Notice

Table of Contents

---

1. Introduction

TOC

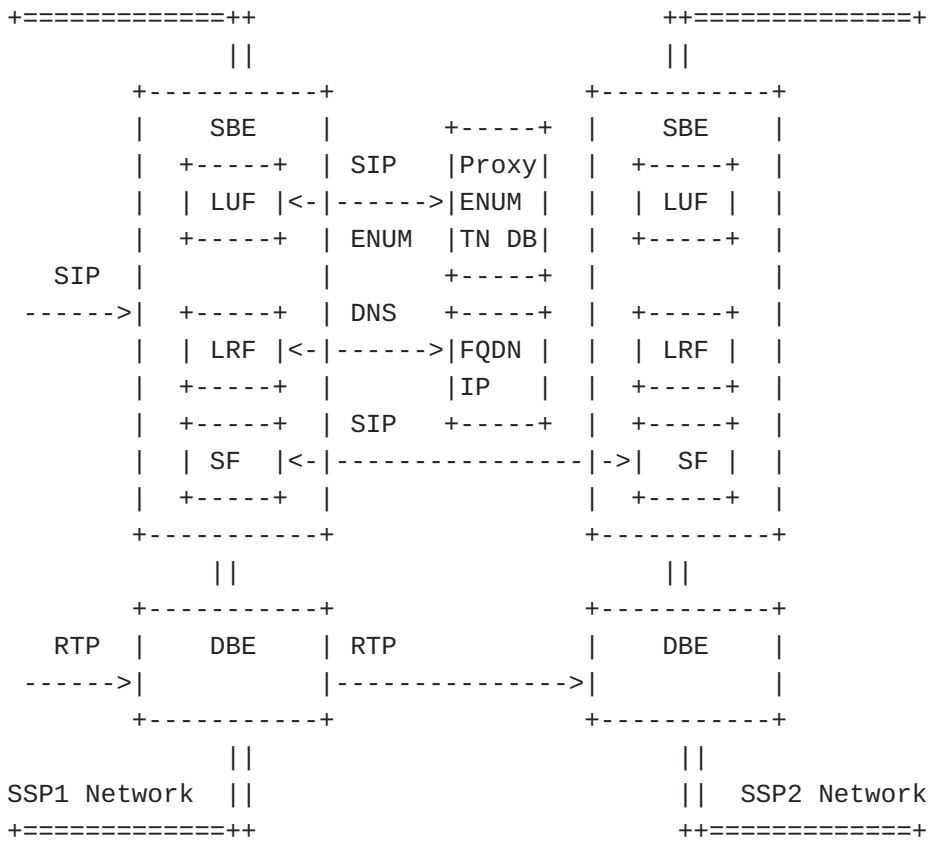
This document defines a reference peering architecture for the Session Initiation Protocol (SIP)[RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, “SIP: Session Initiation Protocol,” June 2002.), it's functional components and interfaces, in the context of session peering for multimedia interconnects. In this process, we define the peering reference architecture, its functional components, and peering interface functions from the perspective of a SIP Service providers [RFC5486] (Malas, D. and D. Meyer, “Session Peering for Multimedia Interconnect (SPEERMINT) Terminology,” March 2009.) network. Thus, it also describes the components and the steps necessary to establish a session between two SIP Service Provider (SSP) peering domains.
This architecture enables the interconnection of two SSPs in layer 5 peering, as defined in the SIP-based session peering requirements [I-D.ietf-speermint-requirements] (Mule, J., “Requirements for SIP-based Session Peering,” October 2010.).
Layer 3 peering is outside the scope of this document. Hence, the figures in this document do not show routers so that the focus is on layer 5 protocol aspects.
This document uses terminology defined in the Session Peering for Multimedia Interconnect (SPEERMINT) Terminology document [RFC5486] (Malas, D. and D. Meyer, “Session Peering for Multimedia Interconnect (SPEERMINT) Terminology,” March 2009.).

---

2. Reference Architecture

TOC

The following figure depicts the architecture and logical functions that form peering between two SSPs.



Reference Architecture

Figure 1

For further details on the elements and functions described in this figure, please refer to [RFC5486] (Malas, D. and D. Meyer, “Session Peering for Multimedia Interconnect (SPEERMINT) Terminology,” March 2009.).

---

3. Procedures of Inter-Domain SSP Session Establishment

TOC

This document assumes that in order for a session to be established from a UA in the originating (or indirect) SSP's network to an UA in the Target SSP's network the following steps are taken:

1. Determine the target or indirect SSP via the LUF. (Note: If the target address represents an intra-SSP resource, the behavior is out-of-scope with respect to this draft.)

2. Determine the address of the SF of the target SSP via the LRF.

3. Establish the session

4. Exchange the media, which could include voice, video, text, etc.

5. End the session (BYE)

The originating or indirect SSP would likely perform steps 1-4, and the target SSP would likely perform steps 4-5.
In the case the target SSP changes, then steps 1-4 would be repeated.
This is reflected in Figure 1 that shows the target SSP with its own peering functions.

---

4. Relationships Between Functions/Elements

TOC

*An SBE can contain a SF function.

*An SF can perform LUF and LRF functions.

*As an additional consideration, a Session Border Controller, can contain an SF, SBE and DBE, and may perform the LUF and LRF functions.

*The following functions can communicate as follows, depending upon various real-world implementations:

-SF can communicate with LUF, LRF, SBE and SF

-LUF can communicator with SF and SBE

-LRF can communicate with SF and SBE

---

5. Recommended SSP Procedures

TOC

This section describes the functions in more detail and provides some recommendations on the role they would play in a SIP call in a Layer 5 peering scenario.
Some of the information in the section is taken from [I-D.ietf-speermint-requirements] (Mule, J., “Requirements for SIP-based Session Peering,” October 2010.) and is put here for continuity purposes.

5.1. Originating or Indirect SSP Procedures

TOC

This section describes the procedures of the originating or indirect SSP.

5.1.1. The Look-Up Function (LUF)

TOC

The purpose of the LUF is to determine the SF of the target domain of a given request and optionally to develop Session Establishment Data. It is important to note that the LUF may utilize the public e164.arpa ENUM root, as well as one or more private roots. When private roots are used specialized routing rules may be implemented, and these rules may vary depending upon whether an originating or indirect SSP is querying the LUF.

5.1.1.1. Target Address Analysis

TOC

When the originating (or indirect) SSP receives a request to communicate, it analyzes the target URI to determine whether the call needs to be routed internal or external to its network. The analysis method is internal to the SSP; thus, outside the scope of SPEERMINT.
If the target address does not represent a resource inside the originating (or indirect) SSP's administrative domain or federation of domains, then the originating (or indirect) SSP performs a Lookup Function (LUF) to determine a target address, and then is resolves the call routing data by using the Location routing Function (LRF).
For example, if the request to communicate is for an im: or pres: URI type [RFC3861] (Peterson, J., “Address Resolution for Instant Messaging and Presence,” August 2004.) [RFC3953] (Peterson, J., “Telephone Number Mapping (ENUM) Service Registration for Presence Services,” January 2005.), the originating (or indirect) SSP follows the procedures in [RFC3861] (Peterson, J., “Address Resolution for Instant Messaging and Presence,” August 2004.). If the highest priority supported URI scheme is sip: or sips: the originating (or indirect) SSP skips to SIP DNS resolution in Section 5.1.3. Likewise, if the target address is already a sip: or sips: URI in an external domain, the originating (or indirect) SSP skips to SIP DNS resolution in Section 5.1.2.1 (DNS Resolution). This may be the case, to use one example, with "sips:bob@biloxi.example.com".
If the target address corresponds to a specific E.164 address, the SSP may need to perform some form of number plan mapping according to local policy. For example, in the United States, a dial string beginning "011

44" could be converted to "+44", or in the United Kingdom "00 1" could be converted to "+1". Once the SSP has an E.164 address, it can use ENUM.

5.1.1.2. ENUM Lookup

TOC

If an external E.164 address is the target, the originating (or indirect) SSP consults the public "User ENUM" rooted at e164.arpa, according to the procedures described in [RFC3761] (Faltstrom, P. and M. Mealling, “The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM),” April 2004.). The SSP must query for the "E2U+sip" enumservice as described in [RFC3764] (Peterson, J., “enumservice registration for Session Initiation Protocol (SIP) Addresses-of-Record,” April 2004.), but may check for other enumservices. The originating (or indirect) SSP may consult a cache or alternate representation of the ENUM data rather than actual DNS queries. Also, the SSP may skip actual DNS queries if the originating (or indirect) SSP is sure that the target address country code is not represented in e164.arpa.
If an im: or pres: URI is chosen for based on an "E2U+im" [RFC3861] (Peterson, J., “Address Resolution for Instant Messaging and Presence,” August 2004.) or "E2U+pres" [RFC3953] (Peterson, J., “Telephone Number Mapping (ENUM) Service Registration for Presence Services,” January 2005.) enumserver, the SSP follows the procedures for resolving these URIs to URIs for specific protocols such a SIP or XMPP as described in the previous section.
The NAPTR response to the ENUM lookup may be a SIP AoR (such as "sips:bob@example.com") or SIP URI (such as "sips:bob@sbe1.biloxi.example.com"). In the case of when a SIP URI is returned, the originating (or indirect) SSP has sufficient routing information to locate the target SSP. In the case of when a SIP AoR is returned, the SF then uses the LRF to determine the URI for more explicitly locating the target SSP.

5.1.2. Location Routing Function (LRF)

TOC

The LRF of an originating (or indirect) SSP analyzes target address and target domain identified by the LUF, and discovers the next hop signaling function (SF) in a peering relationship. The resource to determine the SF of the target domain might be provided by a third-party as in the assisted-peering case. The following sections define mechanisms which may be used by the LRF. These are not in any particular order and, importantly, not all of them may be used.

5.1.2.1. DNS Resolution

TOC

The originating (or indirect) SSP uses the procedures in Section 4 of [RFC3263] (Rosenberg, J. and H. Schulzrinne, “Session Initiation Protocol (SIP): Locating SIP Servers,” June 2002.) to determine how to contact the receiving SSP. To summarize the [RFC3263] (Rosenberg, J. and H. Schulzrinne, “Session Initiation Protocol (SIP): Locating SIP Servers,” June 2002.) procedure: unless these are explicitly encoded in the target URI, a transport is chosen using NAPTR records, a port is chosen using SRV records, and an address is chosen using A or AAAA records.
When communicating with another SSP, entities compliant to this document should select a TLS-protected transport for communication from the originating (or indirect) SSP to the receiving SSP if available, as described further in Section 5.2.1 (TLS).

5.1.2.2. Routing Table

TOC

If there are no End User ENUM records and the originating (or indirect) SSP cannot discover the carrier-of-record or if the originating (or indirect) SSP cannot reach the carrier-of-record via SIP peering, the originating (or indirect) SSP may deliver the call to the PSTN or reject it. Note that the originating (or indirect) SSP may forward the call to another SSP for PSTN gateway termination by prior arrangement using the routing table.
If so, the originating (or indirect) SSP rewrites the Request-URI to address the gateway resource in the target SSP's domain and may forward the request on to that SSP using the procedures described in the remainder of these steps.

5.1.2.3. LRF to LRF Routing

TOC

Communications between the LRF of two interconnecting SSPs may use DNS or statically provisioned IP Addresses for reachability. Other inputs to determine the path may be code-based routing, method-based routing, Time of day, least cost and/or source-based routing.

TOC

5.1.3. The Signaling Path Border Element (SBE)

The purpose of signaling function is to perform routing of SIP messages as well as optionally implement security and policies on SIP messages, and to assist in discovery/exchange of parameters to be used by the Media Function (MF). The signaling function performs the routing of SIP messages. The SBE may be a B2BUA or it may act as a SIP proxy. Optionally, a SF may perform additional functions such as Session Admission Control, SIP Denial of Service protection, SIP Topology Hiding, SIP header normalization, SIP security, privacy, and encryption. The SF of a SBE can also process SDP payloads for media information such as media type, bandwidth, and type of codec; then, communicate this information to the media function.

5.1.3.1. Establishing a Trusted Relationship

TOC

Depending on the security needs and trust relationships between SSPs, different security mechanism can be used to establish SIP calls. These are discussed in the following subsections.

5.1.3.2. IPSec

TOC

In certain deployments the use of IPSec between the signaling functions of the originating and terminating domains can be used as a security mechanism instead of TLS.

5.1.3.3. Co-Location

TOC

In this scenario the SFs are co-located in a physically secure location and/or are members of a segregated network. In this case messages between the originating and terminating SSPs would be sent as clear text.

5.1.3.4. Sending the SIP Request

TOC

Once a trust relationship between the peers is established, the originating (or indirect) SSP sends the request.

5.2. Target SSP Procedures

TOC

This section describes the Target SSP Procedures.

5.2.1. TLS

TOC

The section defines uses of TLS between two SSPs [RFC5246] (Dierks, T. and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2,” August 2008.) [RFC5746] (Rescorla, E., Ray, M., Dispensa, S., and N. Oskov, “Transport Layer Security (TLS) Renegotiation Indication Extension,” February 2010.) [RFC5878] (Brown, M. and R. Housley, “Transport Layer Security (TLS) Authorization Extensions,” May 2010.).
When the receiving SSP receives a TLS client hello, it responds with its certificate. The Target SSP certificate should be valid and rooted in a well-known certificate authority. The procedures to authenticate the SSP's originating domain are specified in [RFC5922] (Gurbani, V., Lawrence, S., and A. Jeffrey, “Domain Certificates in the Session Initiation Protocol (SIP),” June 2010.).
The SF of the Target SSP verifies that the Identity header is valid, corresponds to the message, corresponds to the Identity-Info header, and that the domain in the From header corresponds to one of the domains in the TLS client certificate.

5.2.2. Receive SIP Requests

TOC

Once a trust relationship is established, the Target SSP is prepared to receive incoming SIP requests. For new requests (dialog forming or not) the receiving SSP verifies if the target (request-URI) is a domain that for which it is responsible. For these requests, there should be no remaining Route header field values. For in-dialog requests, the receiving SSP can verify that it corresponds to the top-most Route header field value.
The receiving SSP may reject incoming requests due to local policy. When a request is rejected because the originating (or indirect) SSP is not authorized to peer, the receiving SSP should respond with a 403 response with the reason phrase "Unsupported Peer".

TOC

5.3. Data Path Border Element (DBE)

The purpose of the DBE [RFC5486] (Malas, D. and D. Meyer, "Session Peering for Multimedia Interconnect (SPEERMINT) Terminology," March 2009.) is to perform media related functions such as media transcoding and media security implementation between two SSPs. An example of this is to transform a voice payload from one codec (e.g., G.711) to another (e.g., EvRC). Additionally, the MF may perform media relaying, media security [RFC3711] (Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)," March 2004.), privacy, and encryption.

---

6. Address Space Considerations

TOC

Peering must occur in a common IP address space, which is defined by the federation, which may be entirely on the public Internet, or some private address space [RFC1918] (Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets," February 1996.). The origination or termination networks may or may not entirely be in the same address space. If they are not, then a network address translation (NAT) or similar may be needed before the signaling or media is presented correctly to the federation. The only requirement is that all associated entities across the peering interface are reachable.

---

7. Acknowledgments

TOC

The working group would like to thank John Elwell, Otmar Lendl, Rohan Mahy, Alexander Mayrhofer, Jim McEachern, Jean-Francois Mule, Jonathan Rosenberg, and Dan Wing for their valuable contributions to various versions of this document.

---

8. IANA Considerations

TOC

This memo includes no request to IANA.

TOC

9. Security Considerations

In all cases, cryptographic-based security should be maintained as an optional requirement between peering providers conditioned on the presence or absence of underlying physical security of SSP connections, e.g. within the same secure physical building.
In order to maintain a consistent approach, unique and specialized security requirements common for the majority of peering relationships, should be standardized within the IETF. These standardized methods may enable capabilities such as dynamic peering relationships across publicly maintained interconnections.
Additional security considerations have been documented separately in [I-D.ietf-speermint-voipthreats] (Seedorf, J., Niccolini, S., Chen, E., and H. Scholz, “Session Peering for Multimedia Interconnect (SPEERMINT) Security Threats and Suggested Countermeasures,” November 2010.).

---

10. Contributors

TOC

Mike Hammer
Cisco Systems
Herndon, VA - USA
Email: mhammer@cisco.com

Hadriel Kaplan
Acme Packet
Burlington, MA - USA
Email: hkaplan@acmepacket.com

Sohel Khan, Ph.D.
Comcast Cable
Philadelphia, PA - USA
Email: sohel_khan@cable.comcast.com

Reinaldo Penno
Juniper Networks
Sunnyvale, CA - USA
Email: rpenno@juniper.net

David Schwartz
XConnect Global Networks
Jerusalem - Israel
Email: dschwartz@xconnnect.net

Rich Shockey
Shockey Consulting
USA

Email: Richard@shockey.us

Adam Uzelac
Global Crossing
Rochester, NY - USA
Email: adam.uzelac@globalcrossing.com

---

11. Change Log

TOC

NOTE TO RFC EDITOR: PLEASE REMOVE THIS SECTION PRIOR TO PUBLICATION.

*16: Yes, one final outdated reference to fix.

*15: Doh! Uploaded the wrong doc to create -14. Trying again. :-)

*14: WGLC ended. Ran final nits check prior to sending proto to the AD and sending the doc to the IESG. Found a few very minor nits, such as capitalization and replacement of an obsoleted RFC, which were corrected per nits tool recommendation. The -14 now moves to the AD and the IESG.

*13: Closed out all remaining tickets, resolved all editorial notes.

*12: Closed out several open issues. Properly XML-ized all references. Updated contributors list.

*11: Quick update to refresh the I-D since it expired, and cleaned up some of the XML for references. A real revision is coming soon.

---

12. Open Issues

TOC

NOTE TO RFC EDITOR: PLEASE REMOVE THIS SECTION PRIOR TO PUBLICATION.

*NONE!

---

13. References

TOC

13.1. Normative References

TOC

[I-D.ietf-speermint-requirements]	Mule, J., "Requirements for SIP-based Session Peering," draft-ietf-speermint-requirements-10 (work in progress), October 2010 (TXT).
[I-D.ietf-speermint-voipthreats]	Seedorf, J., Niccolini, S., Chen, E., and H. Scholz, "Session Peering for Multimedia Interconnect (SPEERMINT) Security Threats and Suggested Countermeasures," draft-ietf-speermint-voipthreats-06 (work in progress), November 2010 (TXT).
[RFC1918]	Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets," BCP 5, RFC 1918, February 1996 (TXT).
[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 (TXT).
[RFC3263]	Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers," RFC 3263, June 2002 (TXT).
[RFC3761]	Faltstrom, P. and M. Mealling, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)," RFC 3761, April 2004 (TXT).
[RFC3764]	Peterson, J., "enumservice registration for Session Initiation Protocol (SIP) Addresses-of-Record," RFC 3764, April 2004 (TXT).
[RFC3861]	Peterson, J., "Address Resolution for Instant Messaging and Presence," RFC 3861, August 2004 (TXT).
[RFC3953]	Peterson, J., "Telephone Number Mapping (ENUM) Service Registration for Presence Services," RFC 3953, January 2005 (TXT).
[RFC5246]	Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246, August 2008 (TXT).
[RFC5486]	Malas, D. and D. Meyer, "Session Peering for Multimedia Interconnect (SPEERMINT) Terminology," RFC 5486, March 2009 (TXT).
[RFC5746]	Rescorla, E., Ray, M., Dispensa, S., and N. Oskov, "Transport Layer Security (TLS) Renegotiation Indication Extension," RFC 5746, February 2010 (TXT).
[RFC5878]	Brown, M. and R. Housley, "Transport Layer Security (TLS) Authorization Extensions," RFC 5878, May 2010 (TXT).

[RFC5922]	Gurbani, V., Lawrence, S., and A. Jeffrey, "Domain Certificates in the Session Initiation Protocol (SIP)," RFC 5922, June 2010 (TXT).

13.2. Informative References

TOC

[I-D.ietf-speermint-voip-consolidated-usecases]	Uzelac, A. and Y. Lee, "VoIP SIP Peering Use Cases," draft-ietf-speermint-voip-consolidated-usecases-18 (work in progress), April 2010 (TXT).
[RFC3711]	Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)," RFC 3711, March 2004 (TXT).

Authors' Addresses

TOC

	Daryl Malas (editor)
	CableLabs
	Louisville, CO
	US
Email:	d.malas@cablelabs.com
	Jason Livingood (editor)
	Comcast
	Philadelphia, PA
	US
Email:	Jason_Livingood@cable.comcast.com