SPEERMINT	D. Malas, Ed.
Internet-Draft	CableLabs
Intended status: Informational	J. Livingood, Ed.
Expires: August 22, 2011	Comcast
	February 18, 2011

Session PEERing for Multimedia INTerconnect Architecture
draft-ietf-speermint-architecture-19

Abstract

This document defines a peering architecture for the Session Initiation Protocol (SIP), its 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

This document defines a reference peering architecture for the Session Initiation Protocol (SIP)[RFC3261], 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 Provider's (SSP) [RFC5486] network. Thus, it also describes the components and the steps necessary to establish a session between two SSP peering domains.
An SSP may also be referred to as an Internet Telephony Service Provider (ITSP). While the terms ITSP and SSP are frequently used interchangeably, this document and other subsequent SIP peering-related documents should use the term SSP. SSP more accurately depicts the use of SIP as the underlying layer 5 signaling protocol.
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].
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].
Apart from normative references included herein, readers may also find [I-D.ietf-speermint-voip-consolidated-usecases] informative.

2. New Terminology

[RFC5486] is a key reference for the majority of the SPEERMINT-related terminology used in this document. However, some additional new terms are used here as follows in this section.

2.1. Session Border Controller (SBC)

A Session Border Controller (SBC) is referred to in Section 5. An SBC can contain a Signaling Function (SF), Signaling Path Border Element (SBE) and Data Path Border Element (DBE), and may perform the Look-Up Function (LUF) and Location Routing Function (LRF) functions, as described in Section 3. Whether the SBC performs one or more of these functions is generally speaking dependent upon how a SIP Service Provider (SSP) configures such a network element. In addition, requirements for an SBC can be found in [RFC5853].

2.2. Carrier-of-Record

A carrier-of-record, as used in Section 6.1.2.2, is defined in [RFC5067]. That document describes the term to refer to the entity having discretion over the domain and zone content and acting as the registrant for a telephone number, as represented in ENUM. This can be:

* the Service Provider to which the E.164 number was allocated for end user assignment, whether by the National Regulatory Authority (NRA) or the International Telecommunication Union (ITU), for instance, a code under "International Networks" (+882) or "Universal Personal Telecommunications (UPT)" (+878) or,

* if the number is ported, the service provider to which the number was ported, or

* where numbers are assigned directly to end users, the service provider that the end user number assignee has chosen to provide a Public Switched Telephone Network/Public Land Mobile Network (PSTN/ PLMN) point-of-interconnect for the number.

It is understood that the definition of carrier-of-record within a given jurisdiction is subject to modification by national authorities.

3. Reference Architecture

The following figure depicts the architecture and logical functions that form peering between two SSPs.
For further details on the elements and functions described in this figure, please refer to [RFC5486]. The following terms, which appear in Figure 1, which are documented in [RFC5486] are reproduced here for simplicity.

- Data Path Border Element (DBE): A data path border element (DBE) is located on the administrative border of a domain through which flows the media associated with an inter-domain session. It typically provides media-related functions such as deep packet inspection and modification, media relay, and firewall-traversal support. The DBE may be controlled by the SBE.
- E.164 Number Mapping (ENUM): See [RFC3761].
- Fully Qualified Domain Name (FQDN): See Section 5.1 of [RFC1035].
- Location Routing Function (LRF): The Location Routing Function (LRF) determines for the target domain of a given request the location of the SF in that domain, and optionally develops other SED required to route the request to that domain. An example of the LRF may be applied to either example in Section 4.3.3 of [RFC5486]. Once the ENUM response or SIP 302 redirect is received with the destination's SIP URI, the LRF must derive the destination peer's SF from the FQDN in the domain portion of the URI. In some cases, some entity (usually a 3rd party or federation) provides peering assistance to the originating SSP by providing this function. The assisting entity may provide information relating to direct (Section 4.2.1 of [RFC5486]) or indirect (Section 4.2.2 of [RFC5486]) peering as necessary.
- Look-Up Function (LUF): The Look-Up Function (LUF) determines for a given request the target domain to which the request should be routed. An example of an LUF is an ENUM [4] look-up or a SIP INVITE request to a SIP proxy providing redirect responses for peers. In some cases, some entity (usually a 3rd party or federation) provides peering assistance to the originating SSP by providing this function. The assisting entity may provide information relating to direct (Section 4.2.1 of [RFC5486]) or indirect (Section 4.2.2 of [RFC5486]) peering as necessary.
- Real-Time Transport Protocol (RTP): See [RFC3550].
- Session Initiation Protocol (SIP): See [RFC3261].
- Signaling Path Border Element (SBE): A signaling path border element (SBE) is located on the administrative border of a domain through which inter-domain session layer messages will flow. It typically provides signaling functions such as protocol inter-working (for example, H.323 to SIP), identity and topology hiding, and Session Admission Control for a domain.
- Signaling Function (SF): The Signaling Function (SF) performs routing of SIP requests for establishing and maintaining calls, and to assist in the discovery or exchange of parameters to be used by the Media Function (MF). The SF is a capability of SIP processing elements such as SIP proxies, SBEs, and user agents.
- SIP Service Provider (SSP): A SIP Service Provider (SSP) is an entity that provides session services utilizing SIP signaling to its customers. In the event that the SSP is also a function of the SP, it may also provide media streams to its customers. Such an SSP may additionally be peered with other SSPs. An SSP may also interconnect with the PSTN.

```
+=============++                          ++=============+
              ||                           ||
        +-----------+                 +-----------+
        |    SBE    |       +-----+   |    SBE    |
        |  +-----+  | SIP   |Proxy|   |  +-----+  |
        |  | LUF |<-|------>|ENUM |   |  | LUF |  |
        |  +-----+  | ENUM  |TN DB|   |  +-----+  |
   SIP  |           |       +-----+   |           |
 ------>|  +-----+  | DNS   +-----+   |  +-----+  |
        |  | LRF |<-|------>|FQDN |   |  | LRF |  |
        |  +-----+  |       |IP   |   |  +-----+  |
        |  +-----+  | SIP   +-----+   |  +-----+  |
        |  | SF  |<-|----------------|->|  SF |  |
        |  +-----+  |                 |  +-----+  |
        +-----------+                 +-----------+
             ||                            ||
        +-----------+                 +-----------+
   RTP  |    DBE    | RTP             |    DBE    |
 ------>|           |---------------->|           |
        +-----------+                 +-----------+
              ||                           ||
 SSP1 Network ||                           || SSP2 Network
+=============++                          ++=============+
```

Reference Architecture

4. Procedures of Inter-Domain SSP Session Establishment

This document assumes that in order for a session to be established from a User Agent (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 perform steps 1-4, the target SSP would perform steps 4, and either one can perform step 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.

5. Relationships Between Functions/Elements

Please also refer to Figure 1.

* An SBE can contain a Signaling Function (SF).

* An SF can perform a Look-Up Function (LUF) and Location Routing Function (LRF).

* As an additional consideration, a Session Border Controller, can contain an SF, SBE and DBE, and may act as both an LUF and LRF.

* The following functions may communicate as follows in an example SSP network, depending upon various real-world implementations:

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

  - LUF may communicate with SF and SBE

  - LRF may communicate with SF and SBE

6. Recommended SSP Procedures

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] and is included here for continuity purposes.
It is also important to refer to Section 3.2 of [I-D.ietf-speermint-voipthreats], particularly with respect to the use of IPSec and TLS.

6.1. Originating or Indirect SSP Procedures

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

6.1.1. The Look-Up Function (LUF)

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.

6.1.1.1. Target Address Analysis

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 it 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] [RFC3953], the originating (or indirect) SSP follows the procedures in [RFC3861]. 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 6.1.2.1. 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.

6.1.1.2. ENUM Lookup

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]. The SSP must query for the "E2U+sip" enumservice as described in [RFC3764], 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 based on an "E2U+im" [RFC3861] or "E2U+pres" [RFC3953] enumserver, the SSP follows the procedures for resolving these URIs to URIs for specific protocols such as 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.

6.1.2. Location Routing Function (LRF)

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 have to be used.

6.1.2.1. DNS Resolution

The originating (or indirect) SSP uses the procedures in Section 4 of [RFC3263] to determine how to contact the receiving SSP. To summarize the [RFC3263] 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 6.2.1.

6.1.2.2. Routing Table

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 local SIP proxy 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.

6.1.2.3. LRF to LRF Routing

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.

6.1.3. 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, an 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 an 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.

6.1.3.1. Establishing a Trusted Relationship

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

6.1.3.2. IPSec

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. However, such IPSec use should be the subject of a future document as additional specification is necessary to use IPSec properly and effectively.

6.1.3.3. Co-Location

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 could be sent as clear text (unencrypted). However, even in these semi-trusted co-location facilities, other security or access control mechanisms may be appropriate, such as IP access control lists or other mechanisms.

6.1.3.4. Sending the SIP Request

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

6.2. Target SSP Procedures

This section describes the Target SSP Procedures.

6.2.1. TLS

The section defines the usage of TLS between two SSPs [RFC5246] [RFC5746] [RFC5878]. 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].
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.
As noted above in Section 6.1.3.2, some deployments may utilize IPSec rather than TLS.

6.2.2. Receive SIP Requests

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".

6.3. Data Path Border Element (DBE)

The purpose of the DBE [RFC5486] 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], privacy, and encryption.

7. Address Space Considerations

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]. 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.

8. Acknowledgments

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.

9. IANA Considerations

This memo includes no request to IANA.

10. Security Considerations

The level (or types) of security mechanisms implemented between peering providers is in practice dependent upon on the underlying physical security of SSP connections. This means, as noted in Section 6.1.3.3, whether peering equipment is in a secure facility or not may bear on other types of security mechanisms which may be appropriate. Thus, if two SSPs peered across public Internet links, they are likely to use IPSec or TLS since the link between the two domains should be considered untrusted.
Many detailed and highly relevant security requirements for SPEERMINT have been documented in Section 5 of [I-D.ietf-speermint-requirements]. As a result, that document should be considered required reading. Additional and important security considerations have been documented separately in [I-D.ietf-speermint-voipthreats]. This document describes the many relevant security threats to SPEERMINT, as well the relevant countermeasures and security protections which are recommended to combat any potential threats or other risks. This includes a wide range of detailed threats in Section 2 of [I-D.ietf-speermint-voipthreats]. It also includes key requirements in Section 3.1 of [I-D.ietf-speermint-voipthreats], such as the requirement for the LUF and LRF to support mutual authentication for queries, among other requirements which are related to [I-D.ietf-speermint-requirements]. Section 3.2 of [I-D.ietf-speermint-voipthreats] explains how to meet these security requirements, and then Section 4 explores a wide range of suggested countermeasures.

11. Contributors

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

12. Change Log

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

*19: Additional change to the IPSec section at Jari Arkko's request.

*18: Made several changes based on feedback from Adrian Farrel, Bert Wijnen, Dan Romascanu, Avshalom Houri, Russ Housley, Sean Turner, Tim Polk, and Russ Mundy during IESG review.

*17: Misc. updates at the request of Gonzalo, the RAI AD, in order to clear his review and move to the IESG. This included adding terminology from RFC 5486 and expanding the document name.

*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.

13. References

13.1. Normative References

[I-D.ietf-speermint-requirements]	Mule, J, "Requirements for SIP-based Session Peering", Internet-Draft draft-ietf-speermint-requirements-11, March 2011.
[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", Internet-Draft draft-ietf-speermint-voipthreats-09, August 2011.
[RFC1035]	Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.
[RFC1918]	Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G. and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.
[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.
[RFC3550]	Schulzrinne, H., Casner, S., Frederick, R. and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003.
[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.
[RFC3764]	Peterson, J., "enumservice registration for Session Initiation Protocol (SIP) Addresses-of-Record", RFC 3764, April 2004.
[RFC3861]	Peterson, J., "Address Resolution for Instant Messaging and Presence", RFC 3861, August 2004.
[RFC3953]	Peterson, J., "Telephone Number Mapping (ENUM) Service Registration for Presence Services", RFC 3953, January 2005.
[RFC5067]	Lind, S. and P. Pfautz, "Infrastructure ENUM Requirements", RFC 5067, November 2007.
[RFC5486]	Malas, D. and D. Meyer, "Session Peering for Multimedia Interconnect (SPEERMINT) Terminology", RFC 5486, March 2009.
[RFC5853]	

	Hautakorpi, J., Camarillo, G., Penfield, R., Hawrylyshen, A. and M. Bhatia, "Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments", RFC 5853, April 2010.
[RFC5922]	Gurbani, V., Lawrence, S. and A. Jeffrey, "Domain Certificates in the Session Initiation Protocol (SIP)", RFC 5922, June 2010.
[RFC5246]	Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.
[RFC5746]	Rescorla, E., Ray, M., Dispensa, S. and N. Oskov, "Transport Layer Security (TLS) Renegotiation Indication Extension", RFC 5746, February 2010.
[RFC5878]	Brown, M. and R. Housley, "Transport Layer Security (TLS) Authorization Extensions", RFC 5878, May 2010.

13.2. Informative References

[I-D.ietf-speermint-voip-consolidated-usecases]	Uzelac, A and Y Lee, "VoIP SIP Peering Use Cases", Internet-Draft draft-ietf-speermint-voip-consolidated-usecases-19, October 2011.
[RFC3711]	Baugher, M., McGrew, D., Naslund, M., Carrara, E. and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, March 2004.

Authors' Addresses

Daryl Malas editor Malas CableLabs Louisville, CO US EMail: d.malas@cablelabs.com

Jason Livingood editor Livingood Comcast Philadelphia, PA US EMail: Jason_Livingood@cable.comcast.com