SPEERMINT
Internet-Draft
Intended status: Informational
Expires: September 10, 2010

A. Uzelac, Ed.
Global Crossing
R. Penno
Juniper Networks
M. Hammer
Cisco Systems
D. Malas
CableLabs
S. Khan
Comcast
H. Kaplan
Acme Packet
J. Livingood
Comcast
D. Schwartz
XConnect Global Networks
R. Shockey
Shockey Consulting
March 9, 2010

SPEERMINT Peering Architecture
draft-ietf-speermint-architecture-10

Abstract

This document defines a peering architecture for the Session Initation Protocol (SIP) [RFC3261], it's functional components and interfaces. It also describes the steps necessary to establish a session between two peering domains in the context of the functions defined.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the

provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on September 10, 2010.

Copyright Notice

Table of Contents

1. Introduction

The objective of this document is to define a reference peering architecture 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.

This architecture allows 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 focus on Layer 5 protocol functions and elements.

This document uses terminology defined in the Session Peering for Multimedia Interconnect Terminology document [RFC5486].

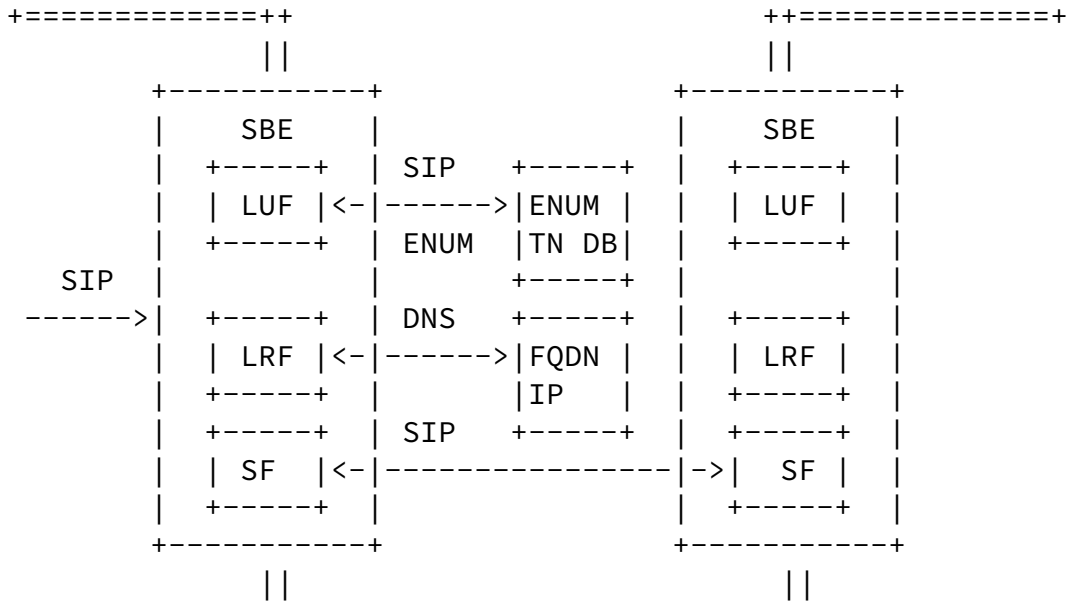
2. Reference Architecture

Figure 1 depicts the architecture and logical functions that form peering between two SSPs. The terms used in the diagram are expanded here for reference:

- SBE - Signaling Path Border Element is described in Section 5.1.3

- LUF - Look-up Function is described in Section 5.1.1
- LRF - Location Routing Function is described in Section 5.1.2
- SF - Signaling Function is defined in [RFC5486]
- SIP - Session Initiation Protocol is defined in [RFC3261]
- DBE - Data Path Border Element is described in Section 5.3
- DNS - Domain Name Service is described in Section 5.1.2.1
- ENUM - E.164 Number Mapping is described in Section 5.1.1.2
- FQDN - Fully Qualified Domain Name
- TN DB - Telephone Number Database

- IP - IPv4/v6 Address
- RTP - Real-time Transport Protocol is defined in [RFC3550]



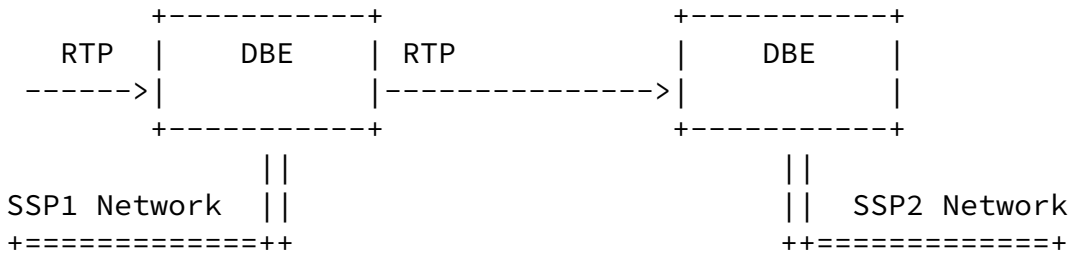


Figure 1

For further details on the elements and functions described in this figure, please refer to [RFC5486].

3. 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 SSP's network to a UA in the Target SSP's network the following steps are taken:

1. Determine the target SSP via the LUF. (Note: If the target address represents a resource within the originating SSP, 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

The originating SSP would likely perform steps 1-4, and the target SSP would likely perform steps 4-5.

If the target SSP is also an indirect peer, then steps 1-4 may be repeated. This is reflected in Figure 1 that shows the target SSP with its own peering functions.

4. Relationships between functions/elements

- An SBE can contain a SF function.
- An SF can perform LUF and LRF functions.
- As an additional consideration, in current Session Border Controller (SBC) implementations, an SBC 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 and another SF
  - LUF can communicate with SF
  - LRF can communicate with SF

5. Recommended SSP Procedures

This section describes the functions in more detail and provides some recommendations on the role they would play in an example SIP telephony call scenario.

Some of the information in the section is taken from [I-D.ietf-speermint-requirements] and is put here for continuity purposes.

5.1. Originating SSP Procedures

5.1.1. The Look-Up Function (LUF)

Purpose is to determine the SF of the target domain of a given request and optionally develop Session Establishment Data.

5.1.1.1. Target Address Analysis

When the originating SSP receives a SIP request, it analyzes the target URI to determine whether the call needs to be routed internal or external to its network.

If the target address does not represent a resource inside the originating SSP's administrative domain, then the originating SSP performs a Lookup (LUF) to determine the target domain, and then it resolves the call routing data by using Location Routing (LRF).

For example, if the request to communicate is for an im: or pres: URI type, the originating SSP follows the procedures in [RFC3861]. If the highest priority supported URI scheme is sip: or sips: the originating SSP skips to SIP DNS resolution. Likewise, if the target address is already a sip: or sips: URI in an external domain, the originating SSP skips to SIP DNS resolution in Section 5.1.2.1

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

If an external E.164 address is the target, the originating SSP consults a private or public ENUM server, 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 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 target domain is represented as an IPv4/v6 address.

If an im: or pres: URI is chosen for 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 a SIP or XMPP.

5.1.2. Location Routing Function (LRF)

The LRF of an Originating SSP analyzes the 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 indirect 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

The originating SSP uses the procedures in [RFC3263] to determine how to contact the target SSP. To summarize the RFC 3263 procedure: unless these are explicitly encoded in the target URI, a transport is chosen using Naming Authority Pointer (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 SSP to the target SSP if available.

5.1.2.2. Routing Table

If there are no End User ENUM records and the Originating SSP cannot discover the carrier-of-record or if the Originating SSP cannot reach the carrier-of-record via SIP peering, the Originating SSP may deliver the call to the PSTN or reject it. Note that the originating SSP may forward the call to another SSP for PSTN gateway termination by prior arrangement using the routing table.

If so, the originating 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

Communication 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.

5.1.3. Signaling Path Border Element (SBE)

The purpose of signaling path border element 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 optional termination and re-initiation of calls may be performed by the signaling path Session Border Element (SBE), or other signaling elements.

Optionally, the SF of a SBE 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. Signaling function may optionally communicate with the network to pass Layer 3 related policies.

5.1.4. Establishing a Trusted Relationship

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.

5.1.4.1. 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.

5.1.4.2. 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 would be sent as clear text.

5.1.4.3. Sending the SIP Request

Once a trust relationship between the peers is established, the originating SSP sends the request.

5.2. Target SSP Procedures

5.2.1. The Ingress SBE

5.2.1.1. TLS

When the target SSP receives a TLS client hello, it responds with its certificate. The Originating 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 [I-D.ietf-sip-domain-certs].

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.

5.2.1.2. 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 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 SSP is not authorized to peer, the receiving SSP should respond with a 403 response with the reason phrase "Unsupported Peer".

5.3. 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., Enhanced Variable Rate Codec (EvRC)). Additionally, the MF may perform media relaying, media security,

privacy, and encryption.

6. Acknowledgments

The working group thanks Sohel Khan for his initial architecture draft that helped to initiate work on this draft.

Other contributors include Rohan Mahy, Otmar Lendl, Jim McEachern and

John Elwell for detailed comments and feedback.

7. IANA Considerations

This memo includes no request to IANA.

8. 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.

9. Normative References

[I-D.ietf-sip-domain-certs]
Gurbani, V., Lawrence, S., and B. Laboratories, "Domain Certificates in the Session Initiation Protocol (SIP)", draft-ietf-sip-domain-certs-05 (work in progress), March 2010.

[I-D.ietf-speermint-requirements]
Mule, J., "SPEERMINT Requirements for SIP-based Session

Peering", draft-ietf-speermint-requirements-09 (work in progress), October 2009.

[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.

[RFC5486] Malas, D. and D. Meyer, "Session Peering for Multimedia Interconnect (SPEERMINT) Terminology", RFC 5486, March 2009.

Authors' Addresses

Adam Uzelac (editor)
Global Crossing
Rochester, NY

US

Email: adam.uzelac@globalcrossing.com

Reinadlo Penno
Juniper Networks
Sunnyvale, CA
US

Email: rpenno@juniper.net

Mike Hammer
Cisco Systems
Herndon, VA
US

Email: mhammer@cisco.com

Daryl Malas
CableLabs
Louisville, CO
US

Email: d.malas@cablelabs.com

Sohel Khan
Comcast
Philadelphia, PA
US

Email: sohel_khan@cable.comcast.com

Hadriel Kaplan
Acme Packet

Burlington, MA
US

Email: hkaplan@acmepacket.com

Jason Livingood
Comcast
Philadelphia, PA
US

Email: Jason_Livingood@cable.comcast.com

David Schwartz
XConnect Global Networks
Jerusalem
Israel

Email: dschwartz@xconnnect.net

Richard Shockey
Shockey Consulting
US

Email: Richard@shockey.us