Abstract

This document defines the SPEERMINT peering architecture, its functional components and peering interface functions. It also describes the steps taken
The objective of this document is to define a reference peering architecture in the context of Session PEERing for Multimedia INTerconnect (SPEERMINT). 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) network.
This architecture allows the interconnection of two SSPs in layer 5 peering as defined in the SPEERMINT Requirements [14] and Terminology [13] documents.

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 SPEERMINT Terminology document [13], so the reader should be familiar with all the terms defined there.

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 [RFC2119].
2. Reference SPEERMINT Architecture

Figure 2 depicts the SPEERMINT architecture and logical functions that form the peering between two SSPs.

Figure 1: Reference SPEERMINT Architecture

For further details on the elements and functions described in this figure, please refer to [RFC 5486].

3. Procedures of Inter-domain SSP Session Establishment

This document assumes that in order for a session to be established from a UA in the Originating SSP’s network to an UA in the Target SSP’s network the following steps are taken:

1. Determine the target SSP via the LUF.
a. 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, etc.

5. End the session (BYE)

The originating 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 2 that shows the target SSP with its own peering functions.

3.1. Relationships between functions/elements

- An SBE can contain a SF function.
- An SF can perform LUF and LRF functions.
- As an additional consideration, a Session Border Controller [SBC RFC], 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 communicate with SF and SBE
  - LRF can communicate with SF and SBE

4. 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 [14] and is put here for continuity purposes.

4.1. Originating SSP Procedures

4.1.1. 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.
4.1.1. Target Address Analysis

When the originating 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 SSP’s administrative domain or federation of domains, then the originating SSP performs a Lookup Function (LUF) to determine a target address, and then 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, the originating SSP follows the procedures in [8]. If the highest priority supported URI scheme is sip: or sips: the originating 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 SSP skips to SIP DNS resolution in Section 4.1.2.1.

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.

4.1.1.2. ENUM Lookup

If an external E.164 address is the target, the originating SSP consults the public "User ENUM" rooted at e164.arpa, according to the procedures described in RFC 3761. The SSP must query for the "E2U+sip" enumservice as described in RFC 3764 [11], 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 originating SSP is sure that the target address country code is not represented in e164.arpa. If a sip: or sips: URI is chosen the SSP skips to Section 5.1.6.

If an im: or pres: URI is chosen for based on an "E2U+im" [8] or "E2U+pres" [9] 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.

4.1.2. Location Routing Function (LRF)

The LRF of an Originating 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.

4.1.2.1. DNS Resolution

The originating SSP uses the procedures in RFC 3263 [4] Section 4 to determine how to contact the receiving SSP. To summarize the RFC 3263 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 SSP to the receiving SSP if available.

4.1.2.2. 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.

4.1.2.3. 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.

4.1.3. 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 optional termination and re-initiation of calls may be performed by the signaling path Session Border Element (SBE), or other signaling elements.
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. Signaling function may optionally communicate with the network to pass Layer 3 related policies.

4.1.3.1. 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.

4.1.3.1.1. 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.

4.1.3.1.2. 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.

4.1.3.2. Sending the SIP request

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

4.2. Target SSP Procedures

4.2.1. The Ingress Signaling Path Border Element (SBE)

4.2.1.1. TLS

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 [24].

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.

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

4.3. Data Path Border Element (DBE)

The purpose of the DBE [RFC 5486] 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, privacy, and encryption.

5. 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. 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.

6. 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.

7. IANA Considerations

There are no IANA considerations at this time.

8. Acknowledgments

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

A significant portion of this draft is taken from [14] with permission from the author R. Mahy. The other important contributor is Otmar Lendl. Special thanks to Jim McEachern for detailed comments and feedback.
9. References

9.1. Normative References


[10] ETSI TS 102 333: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Gate control protocol".


9.2. Informative References


Author’s Addresses

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

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

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

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

Daryl Malas
CableLabs
Louisville, CO - USA
Email: d.malas@cablelabs.com

Hadriel Kaplan
Acme Packet
Email: hkaplan@acmepacket.com

Jason Livingood
Comcast
Email: Jason_livingood@cable.comcast.com

David Schwartz
Kayote Systems
Email: david.schwartz@kayote.com

Rich Shockey
Unaffiliated
Email: Richard@shockey.us