Speermint Working Group   R. Penno
Internet Draft   Juniper Networks
Intended status: Informational   D. Malas
Expires: September 2008   CableLabs
                                                       S. Khan
                                                       Comcast
                                                     A. Uzelac
                                               Global Crossing
                                                     M. Hammer
                                                 Cisco Systems
                                                   May 2, 2008

SPEERMINT Peering Architecture
draft-ietf-speermint-architecture-06

Status of this Memo

Copyright Notice

Abstract

   This document defines the SPEERMINT peering architecture, its
   functional components and peering interface functions. It also

describes the steps taken to establish a session between two peering
domains in the context of the functions defined.

Conventions used in this document

The key words "must", "must NOT", "REQUIRED", "SHALL", "SHALL NOT",
"should", "should NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in RFC-2119[1]

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
   INTerconnect (SPEERMINT). In this process, we define the peering
   reference architecture (reference, for short), it's 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 [13] and
   Terminology [12] 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 [12], so the reader should be familiar with all the terms
   defined there.

2. **Network Context**

   Figure 1 shows an example network context. Two SSPs can form a Layer
   5 peering over either the public Internet or private Layer3
   networks. In addition, two or more providers may form a SIP (Layer
   5) federation [13] on either the public Internet or private Layer 3
   networks. This document does not make any assumption whether the SIP
   providers directly peer to each other or through Layer 3 transit
   network as per use case of [16].

   Note that Figure 1 allows for the following potential SPEERMINT
   peering scenarios:

      o   Enterprise to Enterprise across the public Internet

      o   Enterprise to SSP across the public Internet

   o SSP to SSP across the public Internet

   o Enterprise to enterprise across a private Layer 3 network

   o Enterprise to SSP across a private Layer 3 network

   o SSP to SSP across a private Layer 3 network

   The members of a federation may jointly use a set of functions such
   as location function, signaling function, media function, ENUM
   database or SIP Registrar, SIP proxies, and/or functions that
   synthesize various SIP and non-SIP based applications. Similarly,
   two SSPs may jointly use a set of functions. The functions can be
   either public or private.

```
                         +------------------+
                         |                  |
                         |     Public       |
                         |      SIP         |
                         |    Peering       |
                         |                  |
                         +------------------+
                                 |
                               -----
    +-----------+             /     \             +-----------+
    |Enterprise |           --       --           |Enterprise |
    |Provider A |----------/           \----------|Provider B |
    +-----------+        --               --      +-----------+
                        /     Public        \
                        |    Internet       |
                        \    (Layer 3)      /
    +-----------+        --               --      +-----------+
    |  SSP C    |----------\           /----------|   SSP D    |
    |           |           --       --           |            |
    +-----------+            \_____/              +-----------+
                             | Layer 3 Peering
                             | Point (out of scope)
                               -----
    +-----------+             /     \             +-----------+
    |Enterprise |           --       --           |Enterprise |
    |Provider E |----------/           \----------|Provider F |
    +-----------+        --   Private    --       +-----------+
                        /     Network      \
                        |     (Layer 3)     |
                        \                   /
    +-----------+        --               --      +-----------+
    |  SSP G    |----------\           /----------|   SSP H    |
    |           |           --       --           |            |
    +-----------+            \____/               +-----------+
                               |
                         +------------------+
                         |                  |
                         |    Private       |
                         |      SIP         |
                         |    Peering       |
                         |                  |
                         +------------------+
```
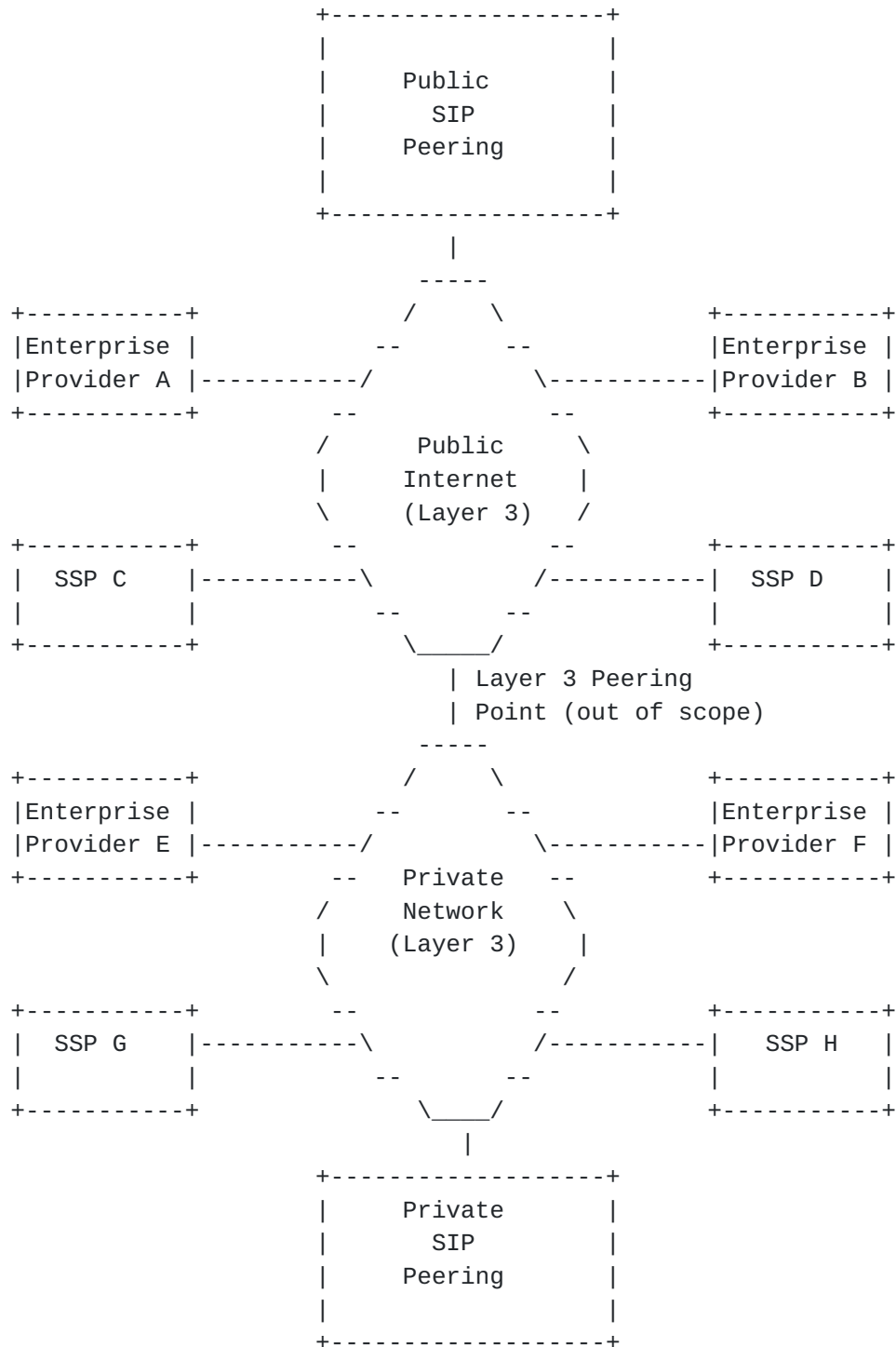
                   Figure 1: SPEERMINT Network Context

[3](#). Procedures

This document assumes that in order for call to be establish from a
UAC end user in the initiating peer's network to a UAS in the
receiving peer's network the following steps are taken:

1. The analysis of the target address.

   . If the target address represents an intra-SSP resource, the
     behavior is out-of-scope with respect to this draft.

2. the determination of the target SSP,

3. the determination of the SF next-hop in the target SSP,

4. the enforcement of authentication and potentially other
   policies,

5. the determination of the UAS,

6. the session establishment,

7. the transfer of media which could include voice, video, text
   and others,

8. and the session termination.

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

In the case the target SSP is different from the terminating SSP it
would repeat steps 1-4. This is reflected in Figure 2 that shows the
target SSP with its own peering functions.

[4](#). Reference SPEERMINT Architecture

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

```
                            +------+
                            | DNS, |
                +---------->| Db,  |<---------+
                |           | etc  |          |
                |           +------+          |
                |                             |
          ------|--------            -------|-------
         /      v         \          /      v        \
        |     +--LUF-+     |        |     +--LUF-+     |
        |     |      |     |        |     |      |     |
        |     |      |     |        |     |      |     |
        |     |      |     |        |     |      |     |
        |     +------+     |        |     +------+     |
        |                  |        |                  |
        |     +--LRF-+     |        |     +--LRF-+     |
        |     |      |     |        |     |      |     |
        |     |      |     |        |     |      |     |
        |     |      |     |        |     |      |     |
        |     +------+     |        |     +------+     |
        |                  |        |                  |
        |                  |        |                  |
        |         +---SF--+   +---SF--+                |
        |         |       |   |       |                |
        |         |  SBE  |   |  SBE  |                |
        | Originating |       |   |       | Target     |
        |         +---SF--+   +---SF--+                |
        |  SSP    |               |        SSP         |
        |         +---MF--+   +---MF--+                |
        |         |       |   |       |                |
        |         |  DBE  |   |  DBE  |                |
        |         |       |   |       |                |
        |         +---MF--+   +---MF--+                |
         \            /           \               /
          ---------------        ---------------
```
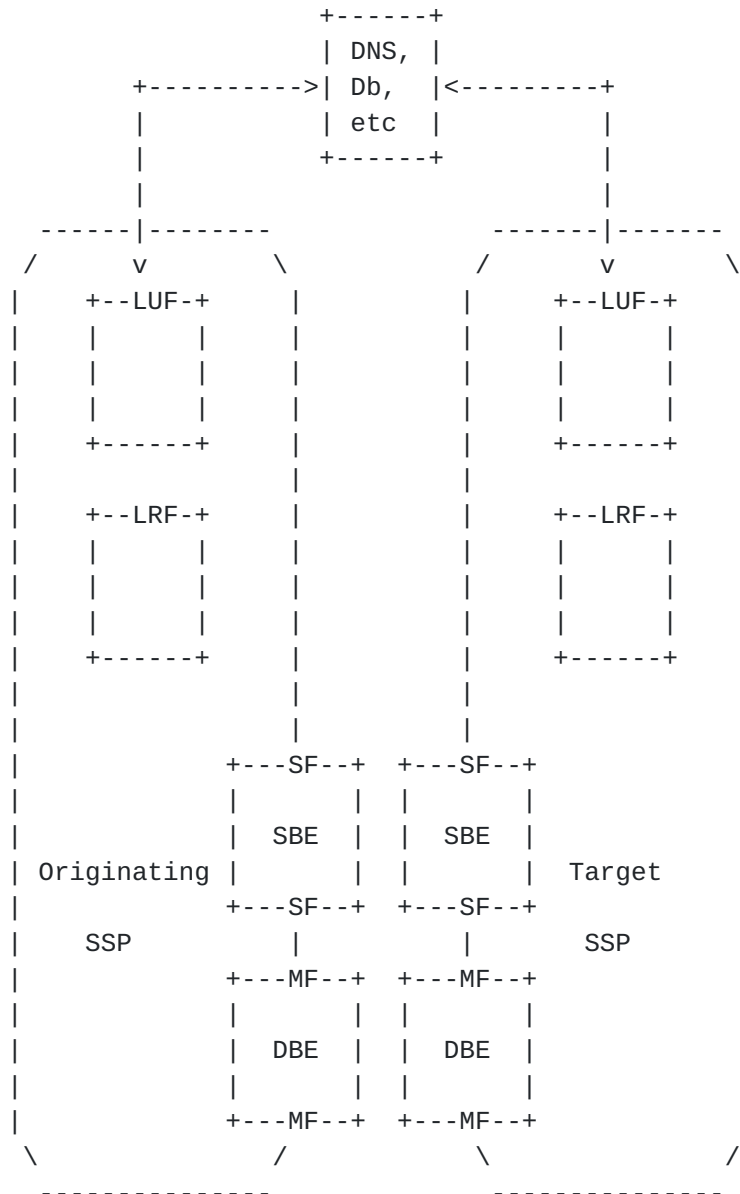
                  Figure 2: Reference SPEERMINT Architecture

   The procedures presented in section 3 are implemented by a set of
   peering functions:

   The Look-Up Function (LUF) provides a mechanism for determining for
   a given request the target domain to which the request should be
   routed.

   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 Session Establishment Data (SED) required
to route the request to that domain.

Signaling Function (SF): Purpose is to perform SIP call routing, to
optionally perform termination and re-initiation of call, to
optionally implement security and policies on SIP messages, and to
assist in discovery/exchange of parameters to be used by the Media
Function (MF).

Media Function (MF): Purpose is to perform media related function
such as media transcoding and media security implementation between
two SIP providers.

The intention of defining these functions is to provide a framework
for design segmentation and allow each one to evolve independently.

5. 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 chapter is taken from [14] 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 (SED)
[12].

5.1.1.1. Target address analysis

When the initiating SSP receives a request to communicate, it
analyzes the target URI to determine whether the call needs to be
terminated internally or externally to its network. The analysis
method is internal to the SSP; thus, outside the scope of SPEERMINT.
Note that the SSP is free to consult any manner of private data
sources to make this determination.

If the target address does not represent a resource inside the
initiating SSP's administrative domain or federation of domains, the
initiating SSP 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 initiating peer follows the procedures in [8]. If the
highest priority supported URI scheme is sip: or sips:, the
initiating peer 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 initiating peer skips to SIP DNS resolution in
Section 5.1.2.2.

If the target address corresponds to a specific E.164 address, the
peer 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 peer has an
E.164 address, it can use ENUM.

5.1.1.2. User ENUM Lookup

If an external E.164 address is the target, the initiating peer
consults the public "User ENUM" rooted at e164.arpa, according to
the procedures described in RFC 3761. The peer must query for the
"E2U+sip" enumservice as described in RFC 3764 [11], but MAY check
for other enumservices. The initiating peer MAY consult a cache or
alternate representation of the ENUM data rather than actual DNS
queries. Also, the peer may skip actual DNS queries if the
initiating peer is sure that the target address country code is not
represented in e164.arpa. If a sip: or sips: URI is chosen the peer
skips to Section 5.1.6.

If an im: or pres: URI is retrieved based on an "E2U+im" [10] or
"E2U+pres" [9] enumserver, the peer follows the procedures for
resolving these URIs to URIs for specific protocols such a SIP or
XMPP as described in the previous section.

5.1.1.3. Infrastructure ENUM lookup

Next the initiating peer checks for a carrier-of-record in a carrier
ENUM domain according to the procedures described in [12]. As in
the previous step, the peer may consult a cache or alternate
representation of the ENUM data in lieu of actual DNS queries. The
peer first checks for records for the "E2U+sip" enumservice, then
for the "E2U+pstn" enumservice as defined in [21]. If a terminal
record is found with a sip: or sips: URI, the peer skips to Section
5.1.2.2. , otherwise the peer continues processing according to the
next section.

[5.1.2](#). Location Routing Function (LRF)

   The LRF of an Initiating SSP analyzes target address 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.

[5.1.2.1](#). Routing Table

   If there is no user ENUM records and the initiating peer cannot
   discover the carrier-of-record or if the initiating peer cannot
   reach the carrier-of-record via SIP peering, the initiating peer
   still needs to deliver the call to the PSTN or reject it. Note that
   the initiating peer may still forward the call to another SSP for
   PSTN gateway termination by prior arrangement using the routing
   table.

   If so, the initiating peer may rewrite 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.

   Alternatively to Request-URI re-writing, the initiating peer may
   populate the Route header with the address of the gateway resource
   in the target SSP's domain and forward the request on to that SSP
   using the procedures described in the remainder of these steps, but
   applied to the Route header.

[5.1.2.2](#). SIP DNS Resolution

   Once a sip: or sips: in an external domain is selected as the
   target, the initiating peer may apply local policy to decide whether
   forwarding requests to the target domain is acceptable. If so, the
   initiating peer uses the procedures in [RFC 3263](#) [[4](#)] [Section 4](#) to
   determine how to contact the receiving peer. 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.
   Note that these are queries of records in the global DNS.

   When communicating with another SSP, entities compliant to this
   document should select a TLS-protected transport for communication
   from the initiating peer to the receiving peer if available. Note
   that this is a single-hop requirement.

5.1.2.3. SIP Redirect Server

A SIP Redirect Server may help in resolving the current address of
the next-hop SF in the target domain.

5.1.3. The Signaling Function (SF)

The purpose of signaling function is to perform routing of SIP
messages, to optionally perform termination and re-initiation of a
call, to 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 are performed by the
signaling path border element (SBE).

Optionally, a SF may perform additional functions such as Session
Admission Control, SIP Denial of Service protection, SIP Topology
Hiding, SIP header normalization, and SIP security, privacy and
encryption.

The SF 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 [10]

5.1.3.1. Establishing a Trusted Relationship

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

5.1.3.1.1. TLS connection

Once a transport, port, and address are found, the initiating SSP
will open or find a reusable TLS connection to the peer. The
procedures to authenticate the SSP's target domain is specified in
[24]

5.1.3.1.2. 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.

5.1.3.1.3. 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 would be sent as clear text.

5.1.3.2. Sending the SIP request

Once a trust relationship between the peers is established, the initiating peer sends the request.

5.1.3.2.1. TLS

If the trust relationship was established through TLS, the initiating peer can optionally verify and assert the sender's identity using the SIP Identity mechanism.

In addition, new requests should contain a valid Identity and Identity-Info header as described in [12]. The Identity-Info header must present a domain name that is represented in the certificate provided when establishing the TLS connection over which the request is sent. The initiating peer should include an Identity header on in-dialog requests as well if the From header field value matches an identity the initiating peer is willing to assert.

5.2. Terminating SSP Procedures

5.2.1. The Location Function (LF)

5.2.1.1. Publish ENUM records

The receiving peer should publish "E2U+SIP" and "E2U+pstn" records with sip: or sips: URIs wherever a public carrier ENUM root is available. In the event that a public root is not available, a publishing to a common ENUM registry with the originating peer will suffice.

This assumes that the receiving peer wants to peer by default. When the receiving peer does not want to accept traffic from specific initiating peers, it may still reject requests on a call-by-call basis.

5.2.1.2. Publish SIP DNS records

To receive peer requests, the receiving peer must ensure that it
publishes appropriate NAPTR, SRV, and address (A and/or AAAA)
records in the LF relevant to the originating peer's SF.

5.2.1.3. Subscribe Notify

A policy notification function may also be optionally implemented by
dynamic subscribe, notify, and exchange of policy information and
feature information among SSPs [21].

5.2.2. Signaling Function (SF)

5.2.2.1. TLS

When the receiving peer 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 terminating SF 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.

5.2.2.2. Receive SIP requests

Once a trust relationship is established, the receiving peer is
prepared to receive incoming SIP requests. For new requests (dialog
forming or not) the receiving peer 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 peer can verify that it
corresponds to the top-most Route header field value.

The receiving peer may reject incoming requests due to local policy.
When a request is rejected because the initiating peer is not
authorized to peer, the receiving peer should respond with a 403
response with the reason phrase "Unsupported Peer".

5.3. Target SSP Procedures

5.3.1. Signaling Function (SF)

5.3.1.1. TLS

When the receiving peer 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].

If the requests should contain a valid Identity and Identity-Info
header as described in [12] the target SF 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.

5.3.1.2. Receive SIP requests

The procedures of the SF of the target SSP are the same as the ones
described in section 5.2.2.2 with the addition that it might
establish a connection to another target SSP, and in this case use
the procedures recommended to an originating SSP (section 5.1).

5.4. Media Function (MF)

The purpose of the MF 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.

5.5. Policy Considerations

In the context of the SPEERMINT working group when two SSPs peer,
there MAY be a desire to exchange peering policy information
dynamically. There are specifications in progress in the SIPPING
working group to define policy exchange between an UA and a domain
[23] and providing profile data to SIP user agents [24] These
considerations borrow from both.

Following the terminology introduced in [12], this package uses the
terms Peering Session-Independent and Session-Specific policies in
the following context.

o Peering Session-Independent policies include Diffserv Marking,
   Policing, Session Admission Control, and domain reachabilities,
   amongst others. The time period between Peering Session-
   Independent policy changes is much greater than the time it
   takes to establish a call.

o Peering Session-Specific polices includes supported
   connection/call rate, total number of connections/calls
   available, current utilization, amongst others. Peering
   Session-specific policies can change within the time it takes
   to establish a call.

Likewise, but orthogonal to session dependency, an SSP may have
policies that may be peer-dependent or peer-independent. That is,
the session-dependent and session-independent policies may by
further sub-divided and modified by additional controls that depend
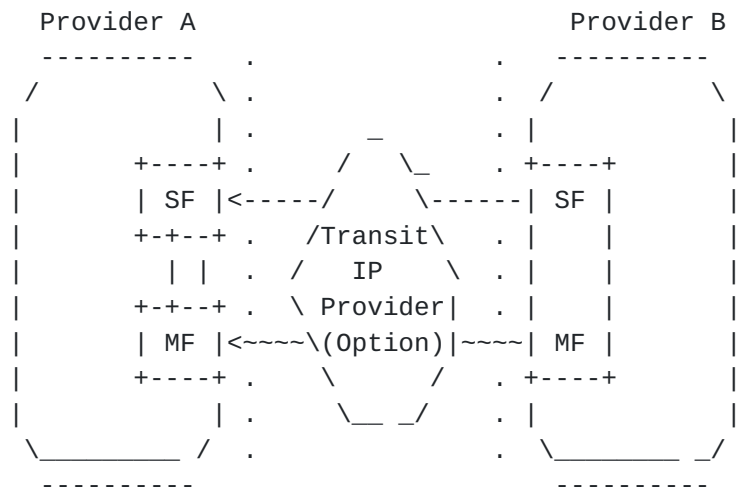on which peer SSP or federation with which communications is being
established.

[6]. Call Control and Media Control Deployment Options

The peering functions can be deployed along the following two
dimensions depending upon how the signaling and the media functions
along with IP layer are implemented:

Composed or Decomposed: Addresses the question whether the media
must flow through the same physical and geographic elements as SIP
dialogs and sessions.

Centralized or Distributed: Addresses the question whether the
logical and physical interconnections are in one geographical
location or distributed to multiple physical locations on the SSP's
network.

In a composed model, SF and MF functions are implemented in one
peering logical element.

```
              Provider A                          Provider B
               ----------    .              .   ----------
              /          \ .              . /          \
             |          | .       _      . |            |
             |     +----+ .      /   \_    . +----+      |
             |     | SF |<-----/      \------| SF |      |
             |     +-+--+ .   /Transit\   . |    |      |
             |       | | .   /   IP    \  . |    |      |
             |     +-+--+ .   \ Provider|  . |    |      |
             |     | MF |<~~~~\(Option)|~~~~| MF |      |
             |     +----+ .    \      /   . +----+      |
             |         | .      \__ _/    . |            |
              _____ / .              .  _____ _/
               ----------                    ----------
```

--- Signal (SIP)
~~~ Bearer (RTP/IP)
... Scope of peering

                   Figure 3: Decomposed v. Collapsed Peering

The advantage of a collapsed peering architecture is that one-
element solves all peering issues. Disadvantage examples of this
architecture are single point of failure, bottleneck, and complex
scalability.

In a decomposed model, SF and MF are implemented in separate peering
logical elements. SFs are implemented in a proxy and MFs are
implemented in another logical element. The scaling of signaling
versus scaling of media may differ between applications.
Decomposing allows each to follow a separate migration path.

This model allows the implementation of M:N model where one SF is
associated with multiple peering MF and one peering MF is associated
with multiple SFs. Generally, a vertical protocol associates the
relationship between a SF and a MF. This architecture reduces the
potential of a single point of failure. It allows separation of the
policy decision point and the policy enforcement point. An example
of disadvantages is the scaling complexity because of the M:N
relationship and latency due to the vertical control messages
between entities.

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. 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 function 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. 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 peer 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.

TODO: Address RFC-3552 BCP items.

9. IANA Considerations

There are no IANA considerations at this time.

10. Acknowledgments

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

A portion of this draft is taken from [14] with permission from the author R. Mahy. The other important contributor is Otmar Lendl.

References

10.1. Normative References

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

[2]   Mealling, M. and R. Daniel, "The Naming Authority Pointer
        (NAPTR) DNS Resource Record", RFC 2915, September 2000.

[3]   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.

[4]   Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol
        (SIP): Locating SIP Servers", RFC 3263, June 2002.

[5]   Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and
        T. Wright, "Transport Layer Security (TLS) Extensions", RFC
        4366, April 2006.

[6]   Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson,
        "RTP: A Transport Protocol for Real-Time Applications", STD
        64, RFC 3550, July 2003.

[7]   Peterson, J., Liu, H., Yu, J., and B. Campbell, "Using E.164
        numbers with the Session Initiation Protocol (SIP)", RFC 3824,
        June 2004.

[8]   Peterson, J., "Address Resolution for Instant Messaging and
        Presence",RFC 3861, August 2004.

[9]   Peterson, J., "Telephone Number Mapping (ENUM) Service
        Registration for Presence Services", RFC 3953, January 2005.

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

[11]   Peterson, J., "enumservice registration for Session Initiation
        Protocol (SIP) Addresses-of-Record", RFC 3764, April 2004.

[12]   Livingood, J. and R. Shockey, "IANA Registration for an
        Enumservice Containing PSTN Signaling Information", RFC 4769,
        November 2006.

10.2. **Informative References**

[13]   Malas, D., "SPEERMINT Terminology", draft-ietf-speermint-
       terminology-16 (work in progress), February 2008.

[14]   Mule, J-F., "SPEERMINT Requirements for SIP-based VoIP
       Interconnection", draft-ietf-speermint-requirements-04.txt,
       February 2008.

[15]   Mahy, R., "A Minimalist Approach to Direct Peering", draft-
       mahy-speermint-direct-peering-02.txt, July 2007.

[16]   Penno, R., et al., "SPEERMINT Routing Architecture Message
       Flows", draft-ietf-speermint-flows-02.txt", April 2007.

[17]   Houri, A., et al., "RTC Provisioning Requirements", draft-
       houri-speermint-rtc-provisioning-reqs-00.txt, June, 2006.

[18]   Habler, M., et al., "A Federation based VOIP Peering
       Architecture", draft-lendl-speermint-federations-03.txt,
       September 2006.

[19]   Mahy, R., "A Telephone Number Mapping (ENUM) Service
       Registration for Instant Messaging (IM) Services", draft-ietf-
       enum-im-service-03 (work in progress), March 2006.

[20]   Haberler, M. and R. Stastny, "Combined User and Carrier ENUM
       in the e164.arpa tree", draft-haberler-carrier-enum-03 (work
       in progress), March 2006.

[21]   Penno, R., Malas D., and Melampy, P., "A Session Initiation
       Protocol (SIP) Event package for Peering", draft-penno-
       sipping-peering-package-00 (work in progress), September 2006.

[22]   Hollander, D., Bray, T., and A. Layman, "Namespaces in XML",
       W3C REC REC-xml-names-19990114, January 1999.

[23]   Burger, E (Ed.), "A Mechanism for Content Indirection in
       Session Initiation Protocol (SIP) Messages", RFC 4483, May
       2006

[24]   Gurbani, V., Lawrence, S., and B. Laboratories, "Domain
       Certificates in the Session Initiation Protocol (SIP)", draft-
       ietf-sip-domain-certs-00 (work in progress), November 2007.

Author's Addresses

    Reinaldo Penno (Editor)
    Juniper Networks
    1194 N Mathilda Avenue
    Sunnyvale, CA
    USA
    Email: rpenno@juniper.net

    Mike Hammer
    Cisco Systems
    13615 Dulles Technology Drive
    Herndon, VA 20171
    USA
    Email: mhammer@cisco.com

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

    Daryl Malas
    CableLabs
    858 Coal Creek Circle
    Louisville, CO 80027
    Email: d.malas@cablelabs.com

    Adam Uzelac
    Global Crossing
    1120 Pittsford Victor Road
    PITTSFORD, NY 14534
    USA
    Email: adam.uzelac@globalcrossing.com