Network Working Group R.Penno (Editor)
Internet Draft Juniper Networks
Expires: February 2007 August 8, 2006

# SPEERMINT Peering Architecture
# draft-ietf-speermint-architecture-00

## Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of 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 November 2006.

## Abstract

This document defines a SPEERMINT peering reference architecture, its functional components and peering interface functions.

## 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 [RFC2119]

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 a peering reference architecture, its functional components, and peering interface functions from the perspective of a real-time communications (Voice and Multimedia) IP Service provider network.

This reference architecture allows the interconnection of two service providers in layer 5 peering as defined in the SPEERMINT Requirements [2] and Terminology [1] documents for the purpose SIP-based voice and multimedia traffic.

IP Layer peering is outside the scope of SPEERMINT at this time; thus, we do not include them in the SPEEMINT Peering Architecture. Note that IP Routers are not shown in the subsequent figures so that the focus is on Layer 5 protocol aspects.

This document uses terminology defined in the SPEERMINT Terminology document [1].

## 2. Network Context

Figure 1 shows an example network context. Two SIP providers can form a Layer 5 peer over either the public Internet or private Layer 3 networks. In addition, two or more providers may form a SIP (Layer 5) federation [1][9] 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 [7].

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

- Enterprise to Enterprise across the public Internet
- Enterprise to Service Provider across the public Internet
- Service Provider to Service Provider across the public Internet
- Enterprise to enterprise across a private Layer 3 network
- Enterprise to Service Provider across a private Layer 3 network
- Service Provider to Service Provider across a private Layer 3 network

The members of a federation may jointly use a set of functions such as location peering function, application function, subscriber database function, SIP proxies, and/or functions that synthesize various SIP and non-SIP based applications. Similarly, two providers may jointly use a set of peering functions. The federation functions or the peering functions can be either public or private.

```
                          +------------------+
                          |     Public       |
                          | Peering Function |
                          |       or         |
                          |     Public       |
                          |Federation Function|
                          +------------------+
                                   |
                                 -----
     +-----------+              /     \              +-----------+
     |Enterprise |            --       --            |Enterprise |
     |Provider A |-----------/           \-----------|Provider B |
     +-----------+         --             --         +-----------+
                          /      Public     \
                          |     Internet    |
                          \     (Layer 3)   /
     +-----------+         --             --         +-----------+
     |Service    |-----------\           /-----------|Service    |
     |Provider C |            --       --            |Provider D |
     +-----------+              \_____/              +-----------+
                                   | Layer 3 Peering
                                   | Point (out of scope)
                                 -----
     +-----------+              /     \              +-----------+
     |Enterprise |            --       --            |Enterprise |
     |Provider E |-----------/           \-----------|Provider F |
     +-----------+         --   Service   --         +-----------+
                          /     Provider    \
                          |     Private     |
                          \     Network     /
     +-----------+         --  (Layer 3)  --         +-----------+
     |Service    |-----------\           /-----------|Service    |
     |Provider G |            --       --            |Provider H |
     +-----------+               \____/              +-----------+
                                    |
                           +------------------+
                           |     Private      |
                           | Peering Function |
                           |       or         |
                           |Federation Function|
                           +------------------+
```

Figure 1: SPEERMINT Network Context

## 3. Procedures

This document assumes that a call from an end user in the initiating peer goes through the following steps to establish a call to an end user in the receiving peer:

. the analysis of a target address,

. the discovery of the receiving peering point address,

. the enforcement of authentication and other policy,

. the discovery of end user address,

. the routing of SIP messages,

. the session establishment,

. the transfer of media,

. and the session termination.

## 4. Reference SPEERMINT Architecture

Figure 2 depicts the SPEERMINT reference architecture and logical functions that form the peering between two SIP service providers I and R, where I is the Initiating peer and R is the Receiving peer.

```
                +----+
                | LF |
     -------    +----+     -------
    /       \    |  |     /       \
   |        LF---+  +---LF         |
   |         |           |         |
   |        PF-----------PF        |
   |         |           |         |
   |   SIP  SF-----------SF  SIP   |
   | Service |           | Service |
   |Provider MF---------MF Provider|
   |    I    |           |    R    |
   |         |           |         |
   |         |           |         |
    \       /             \       /
     -------               -------
```

Figure 2: Reference SPEERMINT Architecture

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

- o Location Function (LF): Purpose is to develop call routing data (CRD) by discovering the Signaling Function (SF), Policy Function (PF), and end user's reachable host (IP address and port).

- o Policy Function (PF): Purpose is to perform authentication and to exchange policy parameters to be used by the SF.

- o Signaling Function (SF): Purpose is to perform routing of SIP messages, 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).

- o 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 separately.

## 5. Peer Function Examples

This section describes the peering functions in more detail and provides some examples 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 [4].

### 5.1. The Location Function (LF) of an Initiating Provider

Purpose is to develop call routing data (CRD) [1] by discovering the Signaling Function (SF), Policy Function (PF), and end user's reachable host (IP address and host). The LF of an Initiating provider analyzes target address and discovers the next hop signaling function (SF) in a peering relationship using DNS, SIP Redirect Server, or a functional equivalent database.

#### 5.1.1. Target address analysis

When the initiating provider receives a request to communicate, the initiating provider analyzes the target state data to determine whether the call needs to be terminated internal or external to its network. The analysis method is internal to the provider's policy; thus, outside the scope of SPEERMINT. Note that the peer 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 peer's administrative domain or federation of domains, the initiating provider resolves the call routing data by using the Location Function (LF). Examples of the LF are the functions of ENUM, Routing Table, SIP DNS, and SIP Redirect Server.

If the request to communicate is for an im: or pres: URI type, the initiating peer follows the procedures in [RFC3861].  If the highest priority supported URI scheme is sip: or sips:, the initiating peer skips to SIP DNS resolution in Section 5.1.5. 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 5.1.5.5.1.5.

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.

#### 5.1.2. 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 3674 [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 5.1.5.

If an im: or pres: URI is chosen for based on an "E2U+im" [10] or "E2U+pres" [RFC3953] 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.

### 5.1.3. Carrier ENUM lookup

Next the initiating peer checks for a carrier-of-record in a carrier ENUM domain according to the procedures described in [11]. 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 [12]. If a terminal record is found with a sip: or sips: URI, the peer skips to Section 5.1.5, otherwise the peer continues processing according to the next section.

### 5.1.4. 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 the call. Note that the initiating peer MAY still sends the call to another provider for PSTN gateway termination by prior arrangement using a routing table. If so, the initiating peer rewrites the Request-URI to address the gateway resource in the target provider's domain and MAY forward the request on to that provider using the procedures described in the remainder of these steps.

### 5.1.5. SIP DNS Resolution

Once a sip: or sips: in an external domain is selected as the target, the initiating peer uses the procedures described in [RFC3263] Section 4. 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.

#### 5.1.6. SIP Redirect Server

A SIP Redirect Server may help in resolving current address of a mobile target address.

### 5.2. The Location Function (LF) of a Receiving Provider

#### 5.2.1. Publish ENUM records

The receiving peer SHOULD participate by publishing "E2U+sip" and "E2U+pstn" records with sip: or sips: URIs wherever a public carrier ENUM root is available. This assumes that the receiving peer wants to peer by default. Even when the receiving peer does not want to accept traffic from specific initiating peers, it MAY still reject requests on a case-by-case basis.

#### 5.2.2. Publish SIP DNS records

To receive peer requests, the receiving peer MUST insure that it publishes appropriate NAPTR, SRV, and address (A and/or AAAA) records in the global DNS that resolve an appropriate transport, port, and address to a relevant SIP server.

### 5.3. Policy Function (PF)

Policy function is optional. The purpose of policy function is to perform authentication and to exchange peering policy capabilities to be used by the signaling function.

The policy capabilities should be specified through well defined XML schemas. These policies define the capabilities of each peer and its devices used for peering. For example, the following capabilities could be exchanged through the policy function:

- Adjacency (Next hop network attributes)
  - If there are many adjacent proxies to use, the choice could be based on:
    - Location of the proxy
    - Maximum number of calls per second (CPS)
    - Maximum number of established calls
    - Maximum allowed bandwidth (KBS)

o  Path Discovery (Domains that are NOT adjacent)

  o What are the paths to the destination domain that can:

   . Guarantee quality

   . Participate in Guarantee's for Trust

   . Are these paths available?

o  Adjacency and Path Congestion detection/avoidance

  o  Inflow Traffic Restriction (not call-by-call)

   o For maintenance actions

   o For congestion management

  o  How can a carrier prevent upstream networks from submitting calls for certain destinations in overload

The Policy function can be implemented by method such as described in [6] as subscribe-notify.

The authentication policy function can be implemented by TLS (as described in (5.3.1), IPSec or any other method that meet the security needs to a specific deployment.

Editor's Note: This section will be updated based on the progress on the SPEERMINT policy document.

### 5.3.1. TLS

Once a transport, port, and address are found, the initiating peer will open or find a reusable TLS connection to the peer.  The initiating provider should verify the server certificate which should be rooted in a well-known certificate authority.  The initiating provider should be prepared to provide a TLS client certificate upon request during the TLS handshake.  The client certificate should contain a DNS or URI choice type in the subject AltName which corresponds to the domain asserted in the host production of the From header URI.  The certificate should be valid and rooted in a well-known certificate authority. Note that the client certificate MAY contain a list of entries in the subjectAltName, only one of which has to match the domain in the From header URI.

When the receiving peer receives a TLS client hello, it responds with its certificate. The receiving peer certificate SHOULD be valid and rooted in a well-known certificate authority. The receiving peer should request and verify the client certificate during the TLS handshake.

#### 5.3.2. IPSec

Editor's Note: will be described later.

#### 5.3.3. Subscribe Notify

Policy function may also be optionally implemented by dynamic subscribe, notify, and exchange of policy information and feature information among providers.

### 5.4. 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 routing of SIP messages are performed by SIP proxies. The optional termination and re-initiation of calls are performed by B2BUA.

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 signaling function 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 network layer to pass Layer 3 related policies [GATE]

Signaling Function supports the following RFCs as per SPEERMINT Requirement document [2]:

- o SF MUST support the core SIP RFCs defined in SIP Hitchhikers Guide [5].

- o SF MUST support SDP related RFCs: the Session

Description Protocol (SDP) [RFC2327], and the Offer/Answer mechanism with SDP [RFC3264].

- SF SHOULD support: Reliability of Provisional Responses in SIP - PRACK [RFC3262], the SIP UPDATE method (for e.g. for codec changes during a session) [RFC3311], the Reason header field [RFC3326].

### 5.5. Media Function (MF)

Examples of the media function is to transform voice payload from one coding (e.g., G.711) to another (e.g., EvRC), media relaying, media security, privacy, and encryption.

Editor's Note: This section will be further updated.

## 6. Call Control and Media Control Deployment Options

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

Composed or Decomposed:  Addresses the question whether the media paths must flow through the same physical and geographic nodes as the call signaling,

Centralized or Distributed:  Addresses the question whether the logical and physical peering points are in one geographical location or distributed to multiple physical locations on the service provider 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. Composed Peering

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

In a decomposed model, SF and MF are implemented in separate peering logical elements. Signaling functions are implemented in a proxy and media functions 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 peering proxies. Generally, a vertical protocol associates the relationship between a SF and a MF. This architecture reduces the potential of single point failure. This architecture, 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. 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.

## 8. IANA Considerations

There are no IANA considerations at this time.

## 9. Conclusions

The proposed peering reference architecture decomposes the peering interface into a set of well defined functions.  Such an arrangement allows each function to the specified and evolved separately.

## 10. 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 [4] with permission from the author R. Mahy. The other important contributor is Otmar Lendl.

Author's Addresses

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

Sohel Khan, Ph.D.
Technology Strategist
Sprint
6220 Sprint Parkway
Overland Park, KS 66251
U.S.A
Email: Sohel.Q.Khan@sprint.com

Daryl Malas
Level 3 Communications LLC
1025 Eldorado Blvd.
Broomfield, CO 80021
USA
EMail: daryl.malas@level3.com

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

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

## 11. References

### 11.1. Normative References

[RFC2119]  Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2327] Handley, M. and V. Jacobson, "SDP: Session Description Protocol", RFC 2327, April 1998.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[RFC2915] Mealling, M. and R. Daniel, "The Naming Authority Pointer (NAPTR) DNS Resource Record", RFC 2915, September 2000.

[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.

[RFC3262] Rosenberg, J. and H. Schulzrinne, "Reliability of Provisional Responses in Session Initiation Protocol (SIP)", RFC 3262, June 2002.

[RFC3263] Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

[RFC3264] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, June 2002.

[RFC3311] Rosenberg, J., "The Session Initiation Protocol (SIP) UPDATE Method", RFC 3311, October 2002.

[RFC3326] Schulzrinne, H., Oran, D., and G. Camarillo, "The Reason Header Field for the Session Initiation Protocol (SIP)", RFC 3326, December 2002.

[RFC3546] Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, "Transport Layer Security (TLS) Extensions", RFC 3546, June 2003.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time

Applications", STD 64, RFC 3550, July 2003.

[RFC3611] Friedman, T., Caceres, R., and A. Clark, "RTP Control Protocol Extended Reports (RTCP XR)", RFC 3611, November 2003.

[RFC3764] Peterson, J., "enumservice registration for Session Initiation Protocol (SIP) Addresses-of-Record", RFC 3764, April 2004.

[RFC3824] Peterson, J., Liu, H., Yu, J., and B. Campbell, "Using E.164 numbers with the Session Initiation Protocol (SIP)", RFC 3824, June 2004.

[RFC3861] Peterson, J., ''Address Resolution for Instant Messaging and Presence'',RFC 3861, August 2004.

[RFC3951] Andersen, S., Duric, A., Astrom, H., Hagen, R., Kleijn, W., and J. Linden, "Internet Low Bit Rate Codec (iLBC)", RFC 3951, December 2004.

[RFC3952] Duric, A. and S. Andersen, "Real-time Transport Protocol (RTP) Payload Format for internet Low Bit Rate Codec (iLBC) Speech", RFC 3952, December 2004.

[RFC3953] Peterson, J., "Telephone Number Mapping (ENUM) Service Registration for Presence Services", RFC 3953, January 2005.

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

### 11.2. Informative References

[1] Meyer, D., "SPEERMINT Terminology", draft-ietf-speermint-terminology-01 (work in progress), May 2006.

[2] Mule, J-F., ''SPEERMINT Requirements for SIP-based VoIP Interconnection'', draft-ietf-speermint-requirements-00.txt, June 2006.

[3] Hilt, V., Camarillo, G., and J. Rosenberg, "A Framework for Session Initiation Protocol (SIP) Session Policies", draft-ietf-sipping-session-policy-framework-00 (work in progress)

[4] Mahy, R., ''A Minimalist Approach to Direct Peering'', draft-mahy-speermint-direct-peering-00.txt, June 19, 2006.

[5] Rosenberg, J., "A Hitchhikers Guide to the Session Initiation Protocol (SIP)", February 2006.

[6] Penno, R., et al., ''SPEERMINT Routing Architecture Message Flows'', draft-ietf-speermint-message-flows-00.txt'', August 2006.

[7] Lee, Y., ''Session Peering Use Case for Cable'', draft-lee-speermint-use-case-cable-00.txt, June, 2006.

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

[9] Habler, M., et al., ''A Federation based VOIP Peering Architecture'', draft-lendl-speermint-federations-01.txt, June 2006.

[10] Mahy, R., "A Telephone Number Mapping (ENUM) Service Registration for Instant Messaging (IM) Services", draft-ietf-enum-im-service-00 (work in progress), March 2006.

[11] Haberler, M. and R. Stastny, "Combined User and Carrier ENUM in the e164.arpa tree", draft-haberler-carrier-enum-02 (work in progress), March 2006.

[12] Livingood, J. and R. Shockey, "IANA Registration for an Enumservice Containing PSTN Signaling Information", draft-ietf-enum-pstn-04 (work in progress), May 2006.

## Intellectual Property Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.