Speermint Working Group
Internet Draft
Intended status: Informational
Expires: January 2008

R. Penno
Juniper Networks
D. Malas
Level 3
S. Khan
Comcast
A. Uzelac
Global Crossing
August 10, 2007

SPEERMINT Peering Architecture
draft-ietf-speermint-architecture-04

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 real-time communications (Voice and Multimedia) IP Service provider network.

This architecture allows the interconnection of two service providers in layer 5 peering as defined in the SPEERMINT Requirements [13] and Terminology [12] documents for the purpose SIP-based voice and multimedia traffic.

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].

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 [17] 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:

- 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.

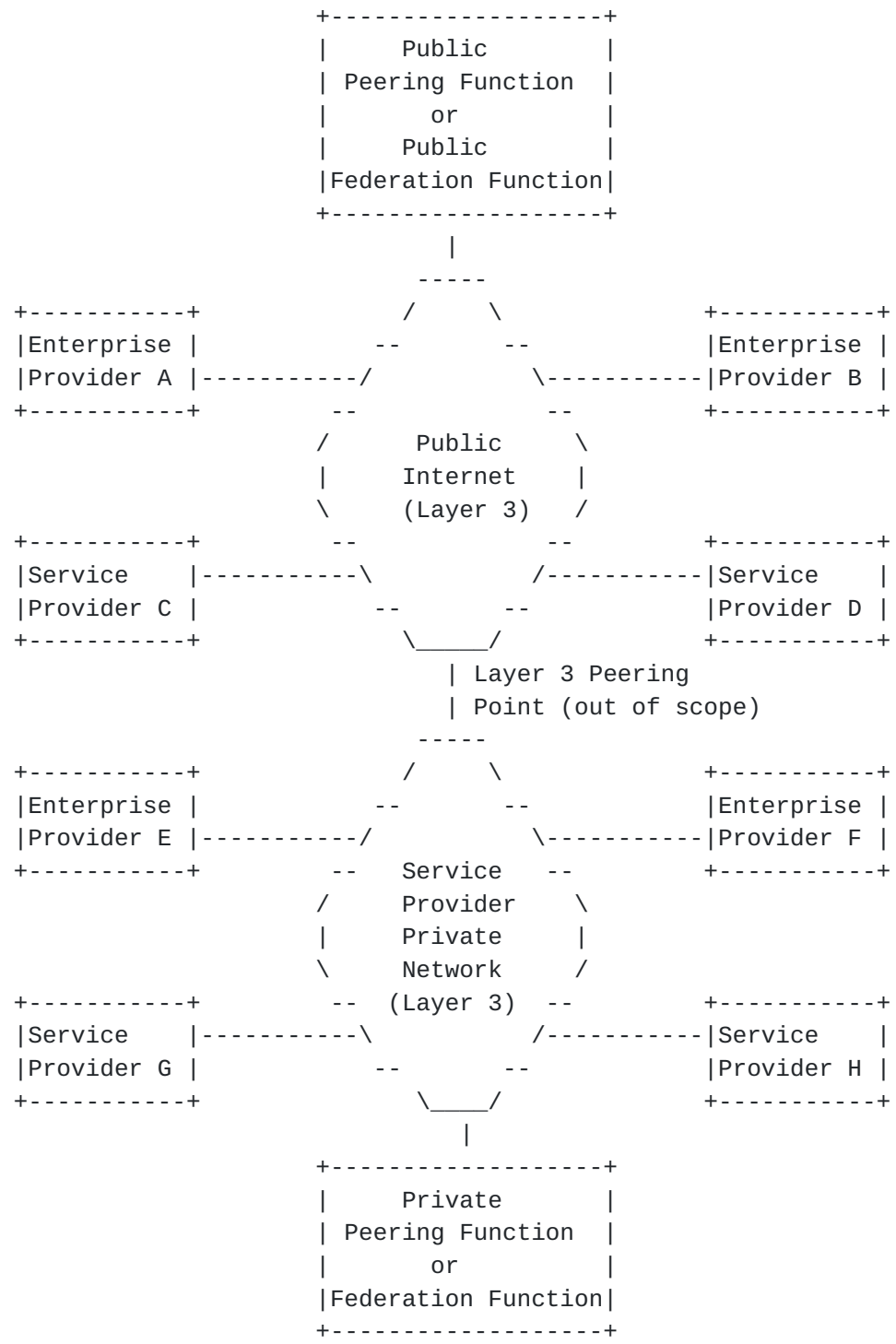

Figure 1: SPEERMINT Network Context

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:

1. The analysis of a target address.
    a. If the target address represents an intra-VSP resource, we go directly to step 4.
2. the discovery of the receiving peering point address,
3. the enforcement of authentication and other policy,
4. the discovery of end user address,
5. the routing of SIP messages,
6. the session establishment,
7. the transfer of media,
8. and the session termination.

4. Reference SPEERMINT Architecture

Figure 2 depicts the SPEERMINT architecture and logical functions that form the peering between two SIP service providers.

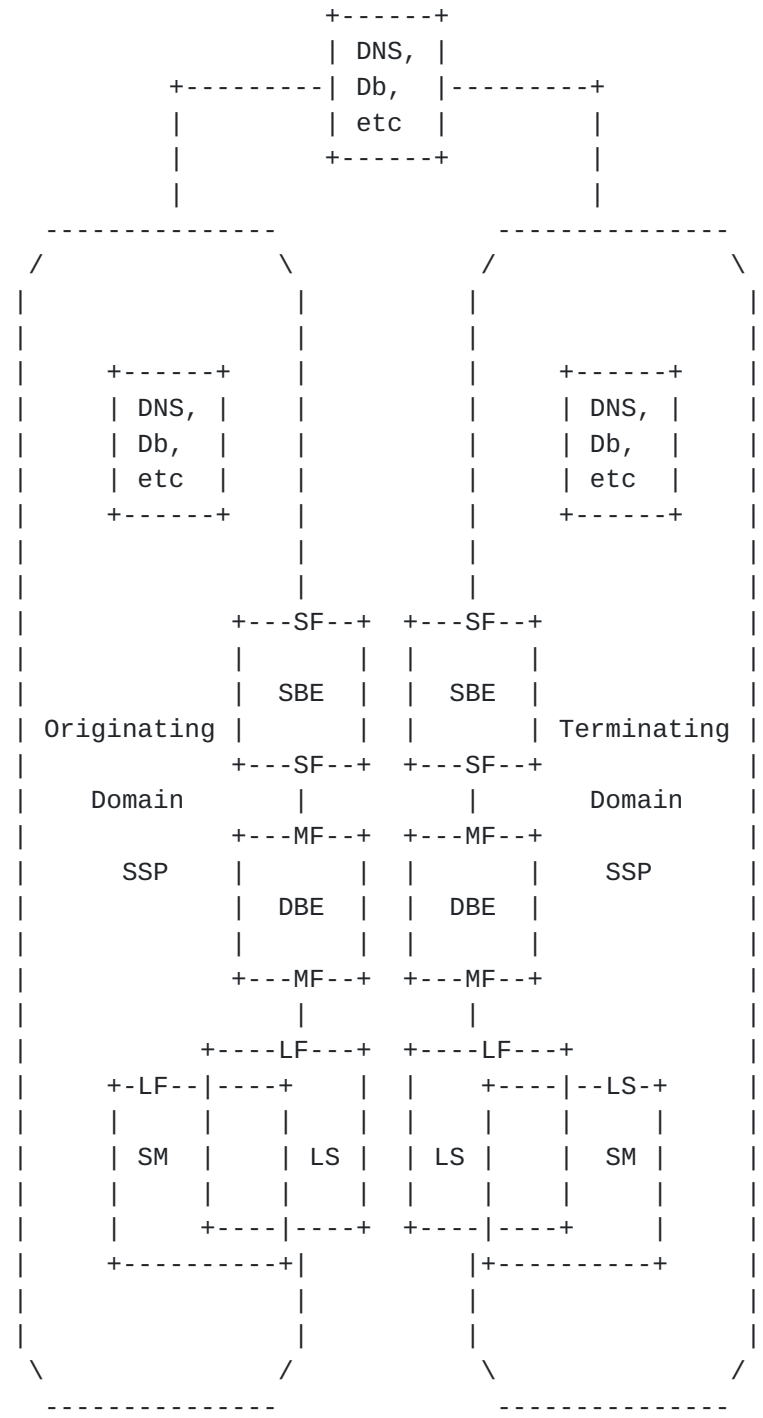

Figure 2: Reference SPEERMINT Architecture

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

- Location Function (LF): Purpose is to develop Session Establishment Data (SED) by discovering the Signaling Function (SF) and the end user's reachable host (IP address and port). The location function is distributed across the Location Server (LS) and Session Manager (SM).

- 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). The signaling function is located within the Signaling Path Border Element (SBE)

- Media Function (MF): Purpose is to perform media related function such as media transcoding and media security implementation between two SIP providers. The media function is located within the Data Path Border Element (DBE).

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 [14].

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

Purpose is to develop Session Establishment Data (SED) [12] by discovering the Signaling Function (SF), 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 [8]. 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.

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 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 5.1.5.

If an im: or pres: URI is chosen for 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.

5.1.3. Carrier ENUM lookup

Next the initiating peer checks for a carrier-of-record in a carrier ENUM domain according to the procedures described in [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 5.1.5, 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 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 [6] 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 a public external peer, entities compliant to this document MUST only select a TLS-protected transport for communication from the initiating peer to the receiving peer. Note that this is a single-hop requirement. Either peer MAY insist on using a sips: URI which asserts that each hop is TLS-protected, but this document does not require protection over each hop.

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.

5.2.3. Subscribe Notify

Policy function may also be optionally implemented by dynamic subscribe, notify, and exchange of policy information and feature information among providers [22].

5.3. 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 [10]

5.4. The Signaling Function (SF) of an Initiating Provider

5.4.1. Setup TLS connection

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 MUST verify the server certificate which SHOULD be rooted in a well-known certificate authority. The initiating provider MUST be prepared to provide a TLS client certificate upon request during the TLS handshake. The client certificate MUST contain a DNS or URI choice type in the subjectAltName 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.

5.4.2. 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.

5.4.3. Co-Location

In this scenario the signaling functions 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 domains would be sent as clear text.

5.4.4. Send the SIP request

Once a TLS connection between the peers is established, the initiating peer sends the request. When sending some requests, the initiating peer MUST verify and assert the senders identity using the SIP Identity mechanism.

The domain name in the URI of the From: header MUST be a domain which was present in the certificate presented when establishing the TLS connection for this request, even if the user part has an anonymous value. If the From header contains the user URI parameter with the value of "phone", the user part of the From header URI MUST be a complete and valid tel: URI [9] telephone-subscriber production, and SHOULD be a global-number. For example, the following are all acceptable, the first three are encouraged:

```
From: "John Doe" <john.doe@example.net>
From: "+12125551212" <+12125551212@example.net;user=phone>
From: "Anonymous" <anonymous@example.net>
From: <4092;phone-context=+12125554000@example.net;user=phone>
From: "5551212" <5551212@example.net>
```

The following are not acceptable:

```
From: "2125551212" <2125551212@example.net;user=phone>
From: "Anonymous" <anonymous@anonymous.invalid>
```

In addition, for new dialog-forming requests and non-dialog-forming requests, the request MUST contain a valid Identity and Identity-Info header as described in [12]. The Identity-Info header must present a domain name which is represented in the certificate presented 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.

The initiating peer MAY include any SIP option-tags in Supported, Require, or Proxy-Require headers according to procedures in standards-track SIP extensions. Note however that the initiating peer MUST be prepared to fallback to baseline SIP functionality as defined by the mandatory-to-implement features of RFC 3261, RFC 3263, and RFC 3264 [7], except that peers implementing this specification MUST implement SIP over TLS using the sip: URI scheme, the SIP Identity header, and RFC 4320 [10] non-INVITE transaction fixes.

5.5. The Signaling Function (SF) of an Initiating Provider

5.5.1. Verify TLS connection

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 MUST request and verify the client certificate during the TLS handshake.

Once the initiating peer has been authenticated, the receiving peer can authorize communication from this peer based on the domain name of the peer and the root of its certificate. This allows two authorization models to be used, together or separately. In the domain-based model, the receiving peer can allow communication from peers with some trusted administrative domains which use general-purpose certificate authorities, without explicitly permitting all domains with certificates rooted in the same authority. It also allows a certificate authority (CA) based model where every domain with a valid certificate rooted in some list of CAs is automatically authorized.

5.5.2. Receive SIP requests

Once a TLS connection is established, the receiving peer is prepared to receive incoming SIP requests. For new dialog-forming requests and out-of-dialog requests, the receiving peer verifies that the target (request-URI) is a domain which for which it is responsible. (For these requests, there should be no remaining Route header field

values.) Next the receiving 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.

For in-dialog requests, the receiving peer can verify that it corresponds to the top-most Route header field value. The peer also validates any Identity header if present.

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".

5.6. 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.

5.7. Policy Considerations

In the context of the SPEERMINT working group when two Layer 5 devices (e.g., SIP Proxies) peer, there is a need to exchange peering policy information. 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.

- Peering Session-Independent policies include Diffserv Marking, Policing, Session Admission Control, 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.

- 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.

These policies can be Peer dependent or independent, creating the following peering policy tree definition:

```
Peer Independent
   Session dependent
   Session independent
Peer Dependent
   Session dependent
   Session independent
```

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.

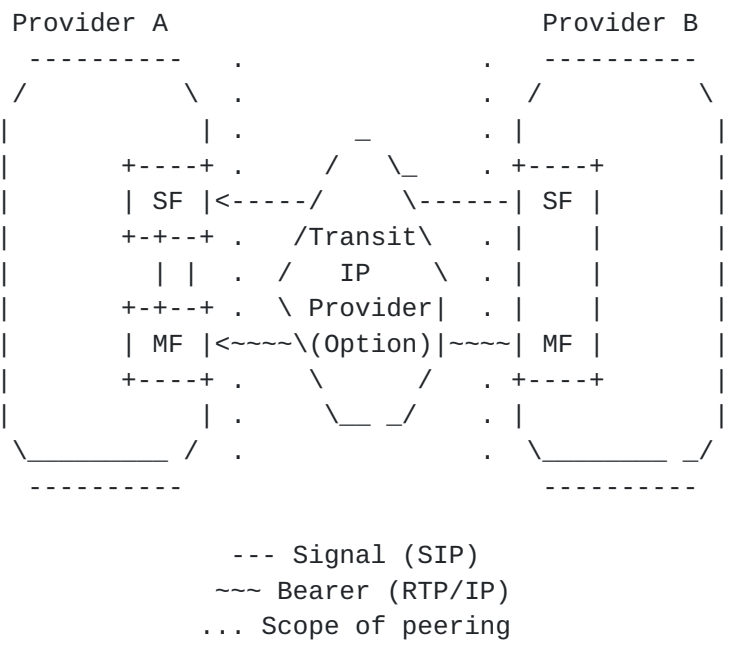

Figure 3: Decomposed v. Collapsed Peering

The advantage of a collapsed peering architecture is that one-element solves all peering issues. Disadvantage examples of this architecture are single point 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. Address space considerations

Peering must occur in a common 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 that same address space. If they are not, then a translation (NAT) may be needed before the signaling or media is presented to the federation. The only requirement is that all 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 significant portion of this draft is taken from [14] with permission from the author R. Mahy. The other important contributor is Otmar Lendl.

11. References

11.1. 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.

11.2. Informative References

[13] Meyer, D., "SPEERMINT Terminology", draft-ietf-speermint-terminology-08 (work in progress), Junly 2007.

[14] Mule, J-F., "SPEERMINT Requirements for SIP-based VoIP Interconnection", draft-ietf-speermint-requirements-02.txt, July 2007.

[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] Lee, Y., "Session Peering Use Case for Cable", draft-lee-speermint-use-case-cable-01.txt, June, 2006.

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

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

[20] 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.

[21] 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.

[22] 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.

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

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

Author's Addresses

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
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

Intellectual Property Statement

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

Copyright Statement

Acknowledgment

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