SPEERMINT Working Group A. Uzelac, Ed.
Internet-Draft Global Crossing
Intended status: Informational Y. Lee, Ed.
Expires: April 19, 2012 Comcast
October 17, 2011

VoIP SIP Peering Use Cases
draft-ietf-speermint-voip-consolidated-usecases-19

Abstract

This document depicts many common Voice over IP (VoIP) use cases for Session Initiation Protocol (SIP) Peering. These use cases are categorized into static and on-demand, and then further sub-categorized into direct and indirect. These use cases are not an exhaustive set, but rather the most common use cases deployed today.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

This document describes important Voice over IP (VoIP) use cases Session Initiation Protocol (SIP) [RFC3261] based peering. These use cases are determined by the SPEERMINT working group and will assist in identifying requirements and other issues to be considered for future resolution by the working group.

Only use cases related to VoIP are considered in this document. Other real-time SIP communications use cases, like Instant Messaging (IM), Video Chat, and Presence are out of scope for this document.

The use cases contained in this document are described as comprehensive as possible, but should not be considered the exclusive set of use cases.

2. Terminology

This document uses terms defined in [RFC5486]. Please refer to it for definitions.

3. Reference Architecture

The diagram below provides the reader with a context for the VoIP use cases in this document. Terms such as SIP Service Provider (SSP), Look-Up Function (LUF), Location Routing Function (LRF), Signaling Path Border Element (SBE) and Data Path Border Element (DBE) are defined in [RFC5486].

Originating SSP (O-SSP) is the SSP originating a SIP request. Terminating SSP (T-SSP) is the SSP terminating the SIP request originating from O-SSP. Assisting LUF and LRF Provider offers LUF and LRF services to O-SSP. Indirect SSP (I-SSP) is the SSP providing indirect peering service(s) to O-SSP to connect to T-SSP.

```
    +--------------------+------------------------+--------------------+
    |  Originating SSP   |  Assisting LUF and LRF |  Terminating SSP   |
    |     Domain         |    Provider Domain     |      Domain        |
    |                    |                        |                    |
    |  +------+  +------+ |    +-------+ +-------+ |  +------+  +------+ |
    |  |O-LUF|  |O-LRF| |    |A-LUF | | A-LRF|  |  |T-LUF|  |T-LRF| |
    |  +------+  +------+ |    +-------+ +-------+ |  +------+  +------+ |
    |                    |                        |                    |
    | +--------+ +------+ +------------------------+  +------+ +--------+ |
    | |O-Proxy| |O-SBE| |  Indirect SSP Domain   |  |T-SBE| |T-Proxy| |
    | +--------+ +------+ |                        |  +------+ +--------+ |
    |                    |    +------+  +------+   |                    |
    |    +---+  +------+ |    |O-SBE|  |O-DBE|   |  +------+  +---+    |
    |    |UAC|  |O-DBE| |    +------+  +------+   |  |T-DBE|  |UAS|    |
    |    +---+  +------+ |                        |  +------+  +---+    |
    |                    |                        |                    |
    +--------------------+------------------------+--------------------+
```

General Overview

Figure 1

Note that some elements included in Figure 1 are optional.

4. Contexts of Use Cases

Use cases are sorted into two general groups: Static and On-demand Peering [RFC5486]. Each group can be further sub-divided into Direct Peering and Indirect Peering [RFC5486]. Although there may be some overlap among the use cases in these categories, there are different requirements between the scenarios. Each use case must specify a basic set of required operations to be performed by each SSP when peering.

These can include:

- Peer Discovery - Peer discovery via a Look-Up Function (LUF) to determine the Session Establishment Data (SED) [RFC5486] of the request. In VoIP use cases, a request normally contains a phone number. The O-SSP will input the phone number to the LUF and the LUF will normally return a SIP AOR [RFC3261] which contains a domain name.

- Next Hop Routing Determination - Resolving the SED information is necessary to route the request to the T-SSP. The LRF is used for this determination. After obtaining the SED, the O-SSP may use the standard procedure defined in [RFC3263] to discover the next

hop address.

o Call setup - SSPs that are interconnecting to one another may also define specifics on what peering policies need to be used when contacting the next hop in order to a) reach the next hop at all and b) to prove that the sender is a legitimate peering partner.

Examples: hard-code transport (TCP/UDP/TLS), non-standard port number, specific source IP address (e.g. in a private Layer-3 network), which TLS client certificate [RFC5246] to use, and other authentication schemes.

o Call reception - This step serves to ensure that the type of relationship (static or on-demand, indirect or direct) is understood and acceptable. For example, the receiving SBE needs to determine whether the INVITE it received really came from a trusted member.

5. Use Cases

Please note there are intra-domain message flows within the use cases to serve as supporting background information. Only inter-domain communications are germane to this document.

5.1. Static Peering Use Cases

Static Peering [RFC5486] describes the use case when two SSPs form a peering relationship with some form of association established prior to the exchange of traffic. Pre-association is a prerequisite to static peering. Static peering is used in cases when two peers want a consistent and tightly controlled approach to peering. In this scenario, a number of variables, such as an identification method (remote proxy IP address) and Quality of Service (QoS) parameters, can be defined upfront and known by each SSP prior to peering.

5.2. Static Direct Peering Use Case

This is the simplest form of a peering use case. Two SSPs negotiate and agree to establish a SIP peering relationship. The peer connection is statically configured and the peer SSPs are directly connected. The peers may exchange interconnection parameters such as DSCP [RFC2474] policies, the maximum number of requests per second, and proxy location prior to establishing the interconnection. Typically, the T-SSP only accepts traffic originating directly from the trusted peer.

```
+--------------------+             +---------------------+
|        O-SSP       |             |        T-SSP        |
|       +-----+      |             |       +-----+       |
|       |O-LUF|      |             |       |T-LUF|       |
|       |O-LRF|      |             |      /|T-LRF|       |
|      /+-----+\     |             |     / +-----+       |
|    (2)     (4,5,6) |             |    /                |
|    /           \   |             |   /(8,9)            |
|+-------+     +-----+             +-----+      +-------+|
||O-Proxy|-(3)-|O-SBE+-----(7)-----+T-SBE|-(10)-|T-Proxy||
|+-------+     +-----+             +-----+      +-------+|
|    |               |             |                |    |
|   (1)              |             |               (11)  |
|    |               |             |                |    |
| +-----+      +-----+             +-----+       +-----+ |
| | UAC +======|O-DBE+=====(12)====+T-DBE|=======+ UAS | |
| +-----+      +-----+             +-----+       +-----+ |
+--------------------+             +---------------------+
     example.com                         example.net
```

Static Direct Peering Use Case

Figure 2

The following is a high-level depiction of the use case:

1. UAC initiates a call via SIP INVITE to O-Proxy. O-Proxy is the home proxy for UAC.

```
INVITE sip:+19175550100@example.com;user=phone SIP/2.0
Via: SIP/2.0/TCP client.example.com:5060
  ;branch=z9hG4bK74bf9
Max-Forwards: 10
From: Alice <sip:+14085550101@example.com;user=phone>
  ;tag=12345
To: Bob <sip:+19175550100@example.com;user=phone>
Call-ID: abcde
CSeq: 1 INVITE
<allOneLine>
Contact: <sip:+19175550100@client.example.com;user=phone;
transport=tcp>
</allOneLine>
```

Note that UAC inserted its Fully Qualified Domain Name (FQDN) in the VIA and CONTACT headers. This example assumes that UAC has its own FQDN.

2. UAC knows UAS's TN, but does not know UAS's domain. It appends its own domain to generate the SIP URI in Request-URI and TO header. O-Proxy checks the Request-URI and discovers that the Request-URI contains user parameter "user=phone". This parameter signifies that the Request-URI is a phone number. So O-Proxy will extract the TN from the Request-URI and query LUF for SED information from a routing database. In this example, the LUF is an ENUM [RFC3761] database. The ENUM entry looks similar to this:

```
$ORIGIN 0.0.1.0.5.5.5.7.1.9.1.e164.arpa.
IN NAPTR (
  10
  100
  "u"
  "E2U+SIP"
  "!^.*$!sip:+19175550100@example.net!"
  . )
```

This SED data can be provisioned by O-SSP or populated by the T-SSP.

3. O-Proxy examines the SED and discovers the domain is external. Given the O-Proxy's internal routing policy, O-Proxy decides to use O-SBE to reach T-SBE. O-Proxy routes the INVITE request to O-SBE and adds a Route header which contains O-SBE.

```
INVITE sip:+19175550100@example.net;user=phone SIP/2.0
Via: SIP/2.0/TCP o-proxy.example.com:5060
  ;branch=z9hG4bKye8ad
Via: SIP/2.0/TCP client.example.com:5060
  ;branch=z9hG4bK74bf9;received=192.0.1.1
Max-Forwards: 9
Route: <sip:o-sbe1.example.com;lr>
Record-Route: <sip:o-proxy.example.com;lr>
From: Alice <sip:+14085550101@example.com;user=phone>
  ;tag=12345
To: Bob <sip:+19175550100@example.com;user=phone>
Call-ID: abcde
CSeq: 1 INVITE
<allOneLine>
Contact: <sip:+19175550100@client.example.com;user=phone;
transport=tcp>
</allOneLine>
```

4. O-SBE receives the requests and pops the top entry of the Route header which contains "o-sbe1.example.com". O-SBE examines the Request-URI and does a LRF for "example.net". In this example,

the LRF is a NAPTR DNS query [RFC3403] of the domain name. O-SBE receives a NAPTR response from LRF. The response looks similar to this:

```
IN NAPTR (
  50
  50
  "S"
  "SIP+D2T"
  ""
  _sip._tcp.t-sbe.example.net. )

IN NAPTR (
  90
  50
  "S"
  "SIP+D2U"
  ""
  _sip._udp.t-sbe.example.net. )
```

5. Given the lower order for TCP in the NAPTR response, O-SBE decides to use TCP as the transport protocol, so it sends a SRV DNS query for the SRV record [RFC2782] for "_sip._tcp.t-sbe.example.net." to O-LRF.

```
;;     priority  weight   port  target
IN SRV 0         2        5060  t-sbe1.example.net.
IN SRV 0         1        5060  t-sbe2.example.net.
```

6. Given the higher weight for "t-sbe1.example.net", O-SBE sends an A record DNS query for "t-sbe1.example.net." to get the A record:

```
;; DNS ANSWER
t-sbe1.example.net.   IN A   192.0.2.100
t-sbe1.example.net.   IN A   192.0.2.101
```

7. O-SBE sends the INVITE to T-SBE. O-SBE is the egress point to the O-SSP domain, so it should ensure subsequent mid-dialog requests traverse via itself. If O-SBE chooses to act as a Back-to-Back User Agent (B2BUA) [RFC3261], it will generate a new INVITE request in next step. If O-SBE chooses to act as a proxy, it should record-route to stay in the call path. In this example, O-SBE is a B2BUA.

```
INVITE sip:+19175550100@example.net;user=phone SIP/2.0
Via: SIP/2.0/TCP o-sbe1.example.com:5060
  ;branch= z9hG4bK2d4zzz
Max-Forwards: 8
From: Alice <sip:+14085550101@example.com;user=phone>
  ;tag=54321
To: Bob <sip:+19175550100@example.net;user=phone>
Call-ID: abcde-osbe1
CSeq: 1 INVITE
<allOneLine>
Contact: <sip:+19175550100@o-sbe1.example.com;user=phone;
transport=tcp>
</allOneLine>
```

Note that O-SBE may re-write the Request-URI with the target domain in the SIP URI. Some proxy implementations will only accept the request if the Request-URI contains their own domains.

8. T-SBE determines the called party home proxy and directs the call to the called party. T-SBE may use ENUM lookup or other internal mechanism to locate the home proxy. If T-SSP uses ENUM ookup, this internal ENUM entry is different from the external ENUM entry populated for O-SSP. In this example, the internal ENUM query returns the UAS's home proxy.

```
$ORIGIN 0.0.1.0.5.5.5.7.1.9.1.e164.arpa.
IN NAPTR (
  10
  100
  "u"
  "E2U+SIP"
  "!^.*$!sip:+19175550100@t-proxy.example.net!"
  . )
```

9. T-SBE receives the NAPTR record and following the requirements in [RFC3263] queries DNS for the SRV records indicated by the NAPTR result. Not finding any, the T-SBE then queries DNS for the A record of domain "t-proxy.example.net.".

```
;; DNS ANSWER
t-proxy.example.net.   IN A   192.0.2.2
```

10. T-SBE is a B2BUA, so it generates a new INVITE and sends it to UAS's home proxy:

```
INVITE sip:bob@t-proxy.example.net;user=phone SIP/2.0
Via: SIP/2.0/TCP t-sbe1.example.net:5060
  ;branch= z9hG4bK28uyyy
Max-Forwards: 7
From: Alice <sip:+14085550101@example.com;user=phone>
  ;tag=54321
To: Bob <sip:+19175550100@t-proxy.example.net;user=phone>
Call-ID: abcde-tsbe1
CSeq: 1 INVITE
<allOneLine>
Contact: <sip:+19175550100@t-sbe1.example.net;user=phone;
transport=tcp>
</allOneLine>
```

11. Finally, UAS's home proxy forwards the INVITE request to the UAS.

```
INVITE sip:+19175550100@server.example.net;user=phone SIP/2.0
Via: SIP/2.0/TCP t-proxy.example.net:5060
  ;branch= z9hG4bK28u111
Via: SIP/2.0/TCP t-sbe1.example.net:5060
  ;branch= z9hG4bK28uyyy; received=192.2.0.100
Max-Forwards: 6
Record-Route: <sip:t-proxy.example.net:5060;lr>,
  <sip:t-sbe1.example.net:5060;lr>
From: Alice <sip:+14085550101@example.com;user=phone>
  ;tag=54321
To: Bob <sip:+19175550100@t-proxy.example.net;user=phone>
Call-ID: abcde-tsbe1
CSeq: 1 INVITE
<allOneLine>
Contact: <sip:+19175550100@t-sbe1.example.net;user=phone;
transport=tcp>
</allOneLine>
```

12. RTP is established between the UAC and UAS. Note that the media shown in Figure 2 passes through O-DBE and T-DBE, but the use of DBE is optional.

5.2.1. Administrative characteristics

The static direct peering use case is typically implemented in a scenario where there is a strong degree of trust between the two administrative domains. Both administrative domains typically sign a peering agreement which state clearly the policies and terms.

5.2.2. Options and Nuances

In Figure 2 O-SSP and T-SSP peer via SBEs. Normally, the operator will deploy the SBE at the edge of its administrative domain. The signaling traffic will pass between two networks through the SBEs. The operator has many reasons to deploy a SBE. For example, the O-SSP may use [RFC1918] addresses for their UA and proxies. These addresses are not routable in the target network. The SBE can perform a NAT function. Also, the SBE eases the operation cost for deploying or removing Layer-5 network elements. Consider the deployment architecture where multiple proxies connect to a single SBE. An operator can add or remove a proxy without coordinating with the peer operator. The peer operator "sees" only the SBE. As long as the SBE is maintained in the path, the peer operator does not need to be notified.

When an operator deploys SBEs, the operator is required to advertise the SBE to the peer LRF so that the peer operator can locate the SBE and route the traffic to the SBE accordingly.

SBE deployment is a decision within an administrative domain. Either one or both administrative domains can decide to deploy SBE(s). To the peer network, most important is to identify the next-hop address. This decision does not affect the network's ability to identify the next-hop address.

5.3. Static Direct Peering Use Case - Assisting LUF and LRF

This use case shares many properties with the Static Direct Peering Use Case. There must exist a pre-association between the O-SSP and T-SSP. The difference is O-SSP will use the Assisting LUF/LRF Provider for LUF and LRF. The LUF/LRF Provider stores the SED to reach T-SSP and provides it to O-SSP when O-SSP requests it.

```
                            +-----------------+
                            |LUF/LRF Provider |
                            |                 |
                            |     +-------+   |
                            |   +-+ A-LUF |   |
                            |  /  | A-LRF |   |
       +--------------------+ /  ++-------+   +---------------------+
       |       O-SSP        |/  /             |         T-SSP       |
       |       +------------/(4,5,6)          |        +-----+      |
       |      /             | /               |        |T-LUF|      |
       |    (2)           +-+/                |      +-|T-LRF|      |
       |    /            /  |                 |     /  +-----+      |
       |   /            /   |                 |    /(8,9)           |
       |+-------+     +-----+                 +-----+      +-------+|
       ||O-Proxy|-(3)-|O-SBE+-------(7)-------+T-SBE|-(10)-|T-Proxy||
       |+-------+     +-----+                 +-----+      +-------+|
       |    |               |                 |                |    |
       |   (1)              |                 |              (11)   |
       |    |               |                 |                |    |
       | +-----+      +-----+                 +-----+       +-----+ |
       | | UAC +======|O-DBE+=======(12)======+T-DBE+=======+ UAS | |
       | +-----+      +-----+                 +-----+       +-----+ |
       +--------------------+                 +---------------------+
             example.com                            example.net
```

Static Direct Peering with Assisting LUF and LRF

Figure 3

The call flow looks almost identical to Static Direct Peering Use Case except Step 2,4,5 and 6 involve the LUF/LRF Provider instead of happening in O-SSP domain.

Similar to Static Direct Peering Use case, O-DBE and T-DBE in Figure 3 are optional.

5.3.1. Administrative Characteristics

The LUF/LRF Provider provides the LUF and LRF services for the O-SSP. Taken together LUF/LRF Provider, O-SSP, and T-SSP form a trusted administrative domain. To reach T-SSP, O-SSP must still require pre-arranged agreements for the peer relationship with T-SSP. The Layer-5 policy is maintained in the O-SSP and T-SSP domains, and the LUF/LRF Provider may not be aware of any Layer-5 policy between the O-SSP and T-SSP.

A LUF/LRF Provider can serve multiple administrative domains. The

LUF/LRF Provider typically does not share SED from one administrative domain to another administrative domain without appropriate permission.

5.3.2. Options and Nuances

The LUF/LRF Provider can use multiple methods to provide SED to O-SSP. The most commonly used are an ENUM lookup and a SIP Redirect. The O-SSP should negotiate with the LUF/LRF Provider which query method it will use prior to sending request to LUF/LRF Provider.

The LUF/LRF Providers must be populated with the T-SSP's AORs and SED. Currently, this procedure is non-standardized and labor intensive. A more detailed description of this problem has been documented in the work in progress [I-D.ietf-drinks-usecases-requirements].

5.4. Static Indirect Peering Use Case - Assisting LUF and LRF

The difference between a Static Direct Use Case and a Static Indirect Use Case lies within the Layer-5 relationship maintained by O-SSP and T-SSP. In the Indirect use case, the O-SSP and T-SSP do not have direct Layer-5 connectivity. They require one or multiple Indirect Domains to assist routing the SIP messages and possibly the associated media.

In this use case, the O-SSP and T-SSP want to form a peer relationship. For some reason, the O-SSP and T-SSP do not have direct Layer-5 connectivity. The reasons may vary, for example business demands and/or domain policy controls. Due to this indirect relationship the signaling will traverse from O-SSP through one or multiple I-SSP(s) to reach T-SSP.

In addition, O-SSP is using a LUF/LRF Provider. This LUF/LRF Provider stores the T-SSP's SED pre-populated by T-SSP. One important motivation to use the LUF/LRF Provider is that T-SSP only needs to populate its SED once to the provider. Using LUF/LRF Provider allows the T-SSP to populate its SED once, while any O-SSP T-SSP's SED can use this LUF/LRF Provider. Current practice has shown that it is rather difficult for the T-SSP to populate its SED to every O-SSP who must reach the T-SSP's subscribers. This is especially true in the Enterprise environment.

Note that the LUF/LRF Provider and I-SSP can be the same provider or different providers.

```
                            +------------------+
                            | LUF/LRF Provider |
                            |       I-SSP      |
                            |      +-------+   |
                            |   ---+ A-LUF |   |
                            |  /   | A-LRF |   |
       +--------------------+ /    +-------+   +---------------------+
       |       O-SSP        |/     /           |         T-SSP       |
       |      +-------------/     /            |        +-----+      |
       |     /              |(4,5,6)           |        |T-LUF|      |
       |    /               |   /              |   +----+T-LRF|      |
       |  (2)             + +---               |  /     +-----+      |
       |  /              /  |                  | /(9,10)             |
       |+-------+     +-----+     +-----+      +-----+      +-------+|
       ||O-Proxy|-(3)-|O-SBE+-(7)-+I-SBE+-(8)--+T-SBE+-(11)-|T-Proxy||
       |+-------+     +-----+     +-----+      +-----+      +-------+|
       |    |               |                  |                |    |
       |   (1)              |                  |               (12)  |
       |    |               |                  |                |    |
       | +-----+      +-----+     +-----+      +-----+       +-----+ |
       | | UAC +=(13)=|O-DBE+=====+I-DBE+======+T-DBE+=======+ UAS | |
       | +-----+      +-----+     +-----+      +-----+       +-----+ |
       +-------------------------------------------------------------+
            example.com          example.org         example.net
```

Indirect Peering via LUF/LRF Provider and I-SSP (SIP and media)

Figure 4

The following is a high-level depiction of the use case:

1. UAC initiates a call via SIP INVITE to O-Proxy. O-Proxy is the home proxy for UAC.

```
INVITE sip:+19175550100@example.com;user=phone SIP/2.0
Via: SIP/2.0/TCP client.example.com:5060
  ;branch=z9hG4bK74bf9
Max-Forwards: 10
From: Alice <sip:+14085550101@example.com;user=phone>
  ;tag=12345
To: Bob <sip:+19175550100@example.com;user=phone>
Call-ID: abcde
CSeq: 1 INVITE
<allOneLine>
Contact: <sip:+19175550100@client.example.com;user=phone;
transport=tcp>
</allOneLine>
```

2. UAC knows UAS's TN, but does not know UAS's domain. It appends its own domain to generate the SIP URI in Request-URI and TO header. O-Proxy checks the Request-URI and discovers that the Request-URI contains user parameter "user=phone". This parameter indicates that the Request-URI is a phone number. So O-Proxy will extract the TN from the Request-URI and query LUF for SED information from a routing database. In this example, the LUF is an ENUM database. The ENUM entry looks similar to this:

```
$ORIGIN 0.0.1.0.5.5.5.7.1.9.1.e164.arpa.
IN NAPTR (
  10
  100
  "u"
  "E2U+SIP"
  "!^.*$!sip:+19175550100@example.org!"
  . )
```

   Note that the response shows the next-hop is the SBE in I-SSP.

   Alternatively, O-SSP may have a pre-association with I-SSP. As such, O-SSP will forward all requests which contains an external domain in the Request-URI or unknown TN to I-SSP. The O-SSP will rely on the I-SSP to determine the T-SSP and route the request correctly. In this configuration, the O-SSP can skip Steps 2,4,5 and 6 and forward the request directly to the I-SBE. This configuration is commonly used in the Enterprise environment.

3. Given the O-Proxy's internal routing policy, O-Proxy decides to use O-SBE to reach I-SBE. O-Proxy routes the INVITE request to O-SBE and adds a Route header which contains the O-SBE.

```
INVITE sip:+19175550100@example.org;user=phone SIP/2.0
Via: SIP/2.0/TCP o-proxy.example.com:5060
  ;branch=z9hG4bKye8ad
Via: SIP/2.0/TCP client.example.com:5060
  ;branch=z9hG4bK74bf9;received=192.0.1.1
Max-Forwards: 9
Route: <sip:o-sbe1.example.com;lr>
Record-Route: <sip:o-proxy.example.com;lr>
From: Alice <sip:+14085550101@example.com;user=phone>
  ;tag=12345
To: Bob <sip:+19175550100@example.net;user=phone>
Call-ID: abcde
CSeq: 1 INVITE
<allOneLine>
Contact: <sip:+19175550100@client.example.com;user=phone;
transport=tcp>
</allOneLine>
```

4. O-SBE receives the requests and pops the top entry of the Route header which contains "sip:o-sbe1.example.com". O-SBE examines the Request-URI and does a LRF for "example.org". In this example, the LRF is a NAPTR DNS query of the domain. O-SBE receives a response similar to this:

```
IN NAPTR (
  50
  50
  "S"
  "SIP+D2T"
  ""
  _sip._tcp.i-sbe.example.org. )

IN NAPTR (
  90
  50
  "S"
  "SIP+D2U"
  ""
  _sip._udp.i-sbe.example.org. )
```

5. Given the lower order for TCP in the NAPTR response, O-SBE decides to use TCP for transport protocol, so it sends a SRV DNS query for the SRV record for "_sip._tcp.i-sbe.example.org." to O-LRF.

```
;;     priority  weight   port  target
IN SRV 0         2        5060  i-sbe1.example.org.
IN SRV 0         1        5060  i-sbe2.example.org.
```

6. Given the higher weight for "i-sbe1.example.org", O-SBE sends a DNS query for A record of "i-sbe1.example.org." to get the A record:

```
;; DNS ANSWER
i-sbe1.example.org.   IN A   192.0.2.200
i-sbe1.example.org.   IN A   192.0.2.201
```

7. O-SBE sends the INVITE to I-SBE. O-SBE is the entry point to the O-SSP domain, so it should ensure subsequent mid-dialog requests traverse via itself. If O-SBE chooses to act as a B2BUA, it will generate a new back-to-back INVITE request in next step. If O-SBE chooses to act as proxy, it should record-route to stay in the call path. In this example, O-SBE is a B2BUA.

```
INVITE sip:+19175550100@example.org;user=phone SIP/2.0
Via: SIP/2.0/TCP o-sbe1.example.com:5060
  ;branch= z9hG4bK2d4zzz
Max-Forwards: 8
Route:  <sip:i-sbe1.example.org;lr>
From: Alice <sip:+14085550101@example.com;user=phone>
  ;tag=54321
To: Bob <sip:+19175550100@example.net;user=phone>
Call-ID: abcde-osbe1
CSeq: 1 INVITE
<allOneLine>
Contact: <sip:+19175550100@o-sbe1.example.com;user=phone;
transport=tcp>
</allOneLine>
```

8. I-SBE receives the request and queries its internal routing database on the TN. It determines the target belongs to T-SSP. Since I-SBE is a B2BUA, I-SBE generates a new INVITE request to T-SSP.

```
INVITE sip:+19175550100@.example.net;user=phone SIP/2.0
Via: SIP/2.0/TCP i-sbe1.example.org:5060
  ;branch= z9hG4bK2d4777
Max-Forwards: 7
Route: <sip:t-sbe1.example.net;lr>
From: Alice <sip:+14085550101@example.com;user=phone>
  ;tag=54321
To: Bob <sip:+19175550100@example.net;user=phone>
Call-ID: abcde-isbe1
CSeq: 1 INVITE
<allOneLine>
Contact: <sip:+19175550100@i-sbe1.example.org;user=phone;
transport=tcp>
</allOneLine>
```

Note that if I-SSP wants the media to traverse through the I-DBE, I-SBE must modify the SDP in the Offer to point to its DBE.

9. T-SBE determines the called party home proxy and directs the call to the called party. T-SBE may use ENUM lookup or other internal mechanism to locate the home proxy. If T-SSP uses ENUM lookup, this internal ENUM entry is different from the external ENUM entry populated for O-SSP. This internal ENUM entry will contain the information to identify the next-hop to reach the called party. In this example, the internal ENUM query returns the UAS's home proxy.

```
$ORIGIN 0.0.1.0.5.5.5.7.1.9.1.e164.arpa.
IN NAPTR (
  10
  100
  "u"
  "E2U+SIP"
  "!^.*$!sip:+19175550100@t-proxy.example.net!"
  . )
```

Note that this step is optional. If T-SBE has other ways to locate the UAS home proxy, T-SBE can skip this step and send the request to the UAS's home proxy. We show this step to illustrate one of the many possible ways to locate UAS's home proxy.

10. T-SBE receives the NAPTR record and following the requirements in [RFC3263] queries DNS for the SRV records indicated by the NAPTR result. Not finding any, the T-SBE then queries DNS for the A record of domain "t-proxy.example.net.".

```
;; DNS ANSWER
t-proxy.example.net.   IN A   192.0.2.2
```

11. T-SBE sends the INVITE to UAS's home proxy:

```
INVITE sip:+19175550100@t-proxy.example.net;user=phone SIP/2.0
Via: SIP/2.0/TCP t-sbe1.example.net:5060
  ;branch= z9hG4bK28uyyy
Max-Forwards: 6
Record-Route: <sip:t-sbe1.example.net:5060;lr>
From: Alice <sip:+14085550101@example.com;user=phone>
  ;tag=54321
To: Bob <sip:+19175550100@example.net;user=phone>
Call-ID: abcde-tsbe1
CSeq: 1 INVITE
<allOneLine>
Contact: <sip:+19175550100@t-sbe1.example.com;user=phone;
transport=tcp>
</allOneLine>
```

12. Finally, UAS's home proxy forwards the INVITE request to UAS.

```
INVITE sip:+19175550100@server.example.net;user=phone SIP/2.0
Via: SIP/2.0/TCP t-proxy.example.net:5060
  ;branch= z9hG4bK28u111
Via: SIP/2.0/TCP t-sbe1.example.net:5060
  ;branch= z9hG4bK28uyyy; received=192.2.0.100
Max-Forwards: 5
Record-Route: <sip:t-proxy.example.net:5060;lr>,
  <sip:t-sbe1.example.net:5060;lr>
From: Alice <sip:+14085550101@example.com;user=phone>
  ;tag=54321
To: Bob <sip:+19175550100@example.net;user=phone>
Call-ID: abcde-tsbe1
CSeq: 1 INVITE
<allOneLine>
Contact: <sip:+19175550100@t-sbe1.example.com;user=phone;
transport=tcp>
</allOneLine>
```

13. In Figure 4, RTP is established between UAC and UAS via O-DBE, I-DBE and T-DBE. The use of DBE is optional.

5.4.1. Administrative characteristics

This use case looks very similar to the Static Direct Peering with Assisting LUF and LRF. The major difference is the O-SSP and T-SSP do not have direct Layer-5 connectivity. Instead, O-SSP connects to

T-SSP indirectly via I-SSP.

Typically, a LUF/LRF Provider serves multiple O-SSPs. Two O-SSPs may use different I-SSP to reach the same T-SSP. For example, O-SSP1 may use I-SSP1 to reach T-SSP, but O-SSP2 may use I-SSP2 to reach T-SSP. Given the O-SSP and T-SSP pair as input, the LUF/LRF Provider will return the SED of I-SSP that is trusted by O-SSP to forward the request to T-SSP.

In this use case. there are two levels of trust relationship. First trust relationship is between the O-SSP and LUF/LRF Provider. The O-SSP trusts the LUF/LRF to provide the T-SSP's SED. Second trust relationship is between O-SSP and I-SSP. The O-SSP trusts the I-SSP to provide Layer-5 connectivity to assist the O-SSP to reach T-SSP. The O-SSP and I-SSP have a pre-arranged agreement for policy. Note that Figure 4 shows a single provider to provide both LUF/LRF and I-SSP, but O-SSP can choose two different providers.

5.4.2. Options and Nuances

Similar to the Static Direct Peering Use Case, the O-SSP and T-SSP may deploy SBE and DBE for NAT traversal, security, transcoding, etc. I-SSP can also deploy SBE and DBE for similar reasons. (as depicted in Figure 4)

5.5. Static Indirect Peering Use Case

This use case shares many properties with the Static Indirect Use Case with Assisting LUF and LRF. The difference is that the O-SSP uses its internal LUF/LRF to control the routing database. By controlling the database, O-SSP can apply different routing rules and policies to different T-SSPs. For example, O-SSP can use I-SSP1 and Policy-1 to reach T-SSP1, and use I-SSP2 and Policy-2 to reach T-SSP2. Note that there could be multiple I-SSPs and multiple SIP routes to reach the same T-SSP; the selection process is out of scope of this document.

```
      +--------------------+-------------------+---------------------+
      |       O-SSP        |       I-SSP       |         T-SSP       |
      |      +-----+       |                   |        +-----+      |
      |     -+O-LUF|       |                   |        |T-LUF|      |
      |    / |O-LRF+\      |                   |   +----+T-LRF|      |
      |   /  +-----+ \     |                   |  /     +-----+      |
      |  /(2)         \(4,5,6)                 | /(9,10)             |
      |+--------+    +-----+      +-----+      +-----+     +--------+|
      ||O-Proxy|-(3)-|O-SBE+--(7)-+I-SBE+-(8)--+T-SBE+-(11)-|T-Proxy||
      |+--------+    +-----+      +-----+      +-----+     +--------+|
      |    |               |                   |                |    |
      |   (1)              |                   |               (12)  |
      |    |               |                   |                |    |
      | +-----+      +-----+      +-----+      +-----+       +-----+ |
      | | UAC +=(13)=+O-DBE+======+I-DBE+======+T-DBE+=======+ UAS | |
      | +-----+      +-----+      +-----+      +-----+       +-----+ |
      +--------------------------------------------------------------+
           example.com          example.org          example.net
```

Indirect Peering via I-SSP (SIP and media)

Figure 5

5.5.1. Administrative characteristics

The Static Indirect Peering Use Case is implemented in cases where no direct interconnection exists between the originating and terminating domains due to either business or physical constraints.

O-SSP <---> I-SSP = Relationship O-I

In the O-I relationship, typical policies, features or functions that deem this relationship necessary are number portability, Ubiquity of termination options, security certificate management and masquerading of originating VoIP network gear.

T-SSP <---> I-SSP = Relationship T-I

In the T-I relationship, typical policies, features or functions observed consist of codec "scrubbing", anonymizing, and transcoding. I-SSP must record-route and stay in the signaling path. T-SSP will not accept message sent directly from O-SSP.

5.5.2. Options and Nuances

In Figure 5, we show I-DBE. Using I-DBE is optional. For example, the I-DBE can be used is when the O-SSP and T-SSP do not have a

common codec. To involve I-DBE, I-SSP should know the list of codecs supported by O-SSP and T-SSP. When I-SBE receives the INVITE request, it will make a decision to invoke the I-DBE. An I-DBE may also be used if O-SSP uses SRTP [RFC3711] for media and T-SSP does not support SRTP.

5.6. On-demand Peering Use Case

On-demand Peering [RFC5486] describes how two SSPs form the peering relationship without a pre-arranged agreement.

The basis of this use case is built on the fact that there is no pre-established relationship between the O-SSP and T-SSP. The O-SSP and T-SSP does not share any information prior to the dialog initiation request. When the O-Proxy invokes the LUF and LRF on the Request-URI, the terminating user information must be publicly available. When the O-Proxy routes the request to the T-Proxy, the T-Proxy must accept the request without any pre-arranged agreement with O-SSP.

The On-demand Peering Use Case is uncommon in production. In this memo, we capture only the high-level descriptions. Further analysis is expected when this use case becomes more popular.

5.6.1. Administrative characteristics

The On-demand Direct Peering Use Case is typically implemented in a scenario where the T-SSP allows any O-SSP to reach its serving subscribers. T-SSP administrative domain does not require any pre-arranged agreement to accept the call. The T-SSP makes its subscribers information publicly available. This model mimics the Internet email model. Sender does not need an pre-arranged agreement to send email to the receiver.

5.6.2. Options and Nuances

Similar to the Static Direct Peering Use Case, the O-SSP and T-SSP can decide to deploy SBE. Since T-SSP is open to the public, T-SSP is considered to be in higher security risk than static model because there is no trusted relationship between O-SSP and T-SSP. T-SSP should protect itself from any attack launched by untrusted O-SSP.

6. Acknowledgments

Michael Haberler, Mike Mammer, Otmar Lendl, Rohan Mahy, David Schwartz, Eli Katz and Jeremy Barkan are the authors of the early individual drafts. Their use cases are captured in this document. Besides, Jason Livingood, Daryl Malas, David Meyer, Hadriel Kaplan,

John Elwell, Reinaldo Penno, Sohel Khan, James McEachern, Jon Peterson, Alexander Mayrhofer, and Jean-Francois Mule made many valuable comments to this document. The editors would also like to extend a special thank to Spencer Dawkins for his detailed review of this document.

7. Security Considerations

Session interconnect for VoIP, as described in this document, has a wide variety of security issues that should be considered. For example, if the O-SSP and T-SSP peer through public Internet, O-SSP must protect the signaling channel and accept messages only from authorized T-SSP. This document does not analyze the threats in details. [I-D.ietf-speermint-voipthreats] discusses the different security threats and countermeasures related to VoIP peering.

8. IANA Considerations

Note to RFC Editor: please delete this section before publication.

9. References

9.1. Normative References

[I-D.ietf-speermint-voipthreats]
Niccolini, S., Chen, E., Seedorf, J., and H. Scholz, "SPEERMINT Security Threats and Suggested Countermeasures", draft-ietf-speermint-voipthreats-01 (work in progress), July 2009.

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

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

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

June 2002.

[RFC3403] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database", RFC 3403, October 2002.

[RFC3761] Faltstrom, P. and M. Mealling, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", RFC 3761, April 2004.

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

9.2. Informative References

[I-D.ietf-drinks-usecases-requirements] Channabasappa, S., "DRINKS Use cases and Protocol Requirements", draft-ietf-drinks-usecases-requirements-00 (work in progress), May 2009.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998.

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, March 2004.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

Authors' Addresses

Adam Uzelac (editor)
Global Crossing
U.S.A.

Email: adam.uzelac@globalcrossing.com
URI: http://www.globalcrossing.com

Yiu L.Lee (editor)
Comcast Cable
U.S.A.

Email: yiu_lee@cable.comcast.com
URI: http://www.comcast.com