SPEERMING Working Group A. Uzelac, Ed.
Internet-Draft Global Crossing
Intended status: Informational Y. Lee, Ed.
Expires: November 30, 2008 Comcast Cable
May 29, 2008

VoIP SIP Peering Use Cases
draft-ietf-speermint-voip-consolidated-usecases-08

Status of this Memo

Abstract

This document depicts many common VoIP use case for 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. This document captures them to provide a reference.

Table of Contents

1. Introduction

This document attempts to capture VoIP use cases for Session Initiation Protocol (SIP) [RFC3261] based peering. These use cases will assist in identifying requirements and future works for VoIP Peering using SIP.

Only use cases related to VoIP are considered in this document. Other real-time SIP communications use cases, like Instant Messaging (IM) and presence are out of scope for this document. In describing use cases, the intent is descriptive, not prescriptive.

There are existing documents [I-D.lee-speermint-use-case-cable], [I-D.lendl-speermint-federations], [I-D.mahy-speermint-direct-peering], [I-D.schwartz-speermint-use-cases-federations], and [I-D.uzelac-speermint-use-cases] that have captured use case scenarios. This draft draws from those documents. The use cases contained in this document attempts to be as comprehensive as possible, but should not be considered the exclusive set of use cases.

2. Terminology

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].

3. Reference Architecture

The diagram below provides the reader with a context for the VoIP use cases in this draft.

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

General Overview

Figure 1

PLEASE NOTE: In Figure 1 - the elements defined are optional in many use cases.

4. Contexts of Use Cases

Use cases are sorted into two general groups: Static and On-demand Peering [I-D.ietf-speermint-terminology]. Each group can be further sub-divided to Direct Peering and Indirect Peering [I-D.ietf-speermint-terminology]. Though 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 member when peering.

These can include:

- Peer Discovery - Peer discovery via a Look-Up Function (LUF) to determine the administrative domain of the target.

- Location Determination - A location determination process serves to create the Session Establishment Data (SED). Examples: Public User-ENUM, public Infrastructure ENUM, private ENUM tree, SIP Redirect, DUNDi.

- Next Hop Determination - A next hop determination based on the SED is then completed. If Location Routing Function (LRF) query did not return an URI of the form sip:user@IP-address, then the originating SSP has to translate the domain part of the URI to an IP-address (plus perhaps fall-backs) in order to contact the next hop. Examples: [RFC3263] in the public DNS. [RFC3263] in a federation private DNS. [RFC3263] in the public DNS with split-DNS, P2P SIP, modified [RFC3263] in the public DNS (e.g. a federation-specific prefix to the domain name).

- Call setup - SSPs that are interconnecting to one another may also define specifics on what SIP features 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 L3 network), which TLS client certificate [RFC4366] to use, and other authentication schemes.

- Call reception - This step serves to ensure that the type of relationship (static or on-demand, indirect or direct) is understood and acceptable. For instance, the receiving side border elements need to determine whether the INVITE it just received really came from a member of the federation, possibly via an access control list entry. This is the flip side of step four. Example: verify TLS certificate [RFC4366] check incoming interface/VLAN,check source IP address against a configured list of valid ones.

5. User 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 Speermint.

5.1. Static Peering Use Cases

Static Peering [I-D.ietf-speermint-terminology] 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 remote proxy IP address and QoS parameters, can be defined upfront and known by each SSP prior to peering.

5.1.1. 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 is direct between the connected SSPs. The peers may exchange interconnection parameters such as DSCP policies, subscriber SIP-URI and proxy location prior to establishing the interconnection. Typically, they only accept 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 +============+=====(12)====+=============+ 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:+19172223333@example.com;user=phone SIP/2.0
Via: SIP/2.0/TCP client.example.com:5060
  ;branch=z9hG4bK74bf9
Max-Forwards: 10
From: Alice <sip:+14083332222@example.com;user=phone>
  ;tag=12345
To: Bob <sip+19172223333@example.com;user=phone>
Call-ID: abcde@client.example.com
CSeq: 1 INVITE
Contact: <sip:+14083332222@client.example.com;user=phone
  ;transport=tcp>
```

2. Note that UAC only knows UAS's TN but not UAS's domain. It appends its own domain to generate the SIP-URI in R-URI and To header. O-Proxy checks the R-URI's domain and discovers that the UAS's domain is internal but the TN is unknown to O-Proxy. So, O-Proxy queries 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 3.3.3.3.2.2.2.7.1.9.1.example.com
NAPTR 10 100 "u" "E2U+SIP"
 "!^.*!sip:\1@t-sbe.example.net!"
```

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

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

```
INVITE sip:+19172223333@t-sbe.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=192.0.2.1
Max-Forwards: 9
Route: <sip:o-sbe1.example.com;lr>
Record-Route: <sip:o-proxy.example.com;lr>
From: Alice <sip:+14083332222@example.com;user=phone>
  ;tag=12345
To: Bob <sip+19172223333@example.com;user=phone>
Call-ID: abcde@client.example.com
CSeq: 1 INVITE
Contact: <sip:+14083332222@client.example.com;user=phone
  ;transport=tcp>
```

4. O-SBE receives the requests and pops the top entry of the Route header which contains "o-sbe1.exapmle.com". O-SBE examines the R-URI and does a LRF for "t-sbe.example.net". In this example, the LRF is a DNS lookup of the domain name. O-SBE receives a NAPTR response form LRF. The response looks similar to this:

```
;;        order perf flags service   regxp replacement
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 for transport protocol, so it sends a DNS query for the SRV record for "_sip._tcp.t-sbe.example.net".

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

6. O-SBE sends a DNS query for "t-sbe1.example.net" to get the A-Record:

```
;; DNS ANSWER
t-sbe1.example.net   A   192.0.2.10
t-sbe1.example.net   A   192.0.2.11
```

7. O-SBE sends the INVITE to T-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 B2BUA , it will terminate the call and generate a new back-to-back INVITE request. If O-SBC 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:+19172223333@t-sbe1.example.net;user=phone SIP/2.0
Via: SIP/2.0/TCP o-sbe1.example.com:5060
  ;branch= z9hG4bK2d4zzz;
Max-Forwards: 10
From: Alice <sip:+14083332222@example.com;user=phone>
  ;tag=54321
To: Bob <sip:+19172223333@t-sbe1.example.net;user=phone>
Call-ID: abcde-osbe1@o-sbe1.example.com
CSeq: 1 INVITE
Contact: <sip:+14083332222@o-sbe1.example.com;user=phone
  ;transport=tcp>
```

Note that O-SEB may re-write the R-URI with the target domain in the SIP-URI. Some proxy implementation will only accept the request if the R-URI contains its own domain.

8. T-SBE determines called party home proxy and directs call to called party. T-SBE may use ENUM or other internal mechanism to locate the home proxy. If T-SSP uses ENUM, this internal ENUM entry is different from the external ENUM entry populated for O-SSP. For internal use, it should return the home proxy of UAS. For external use, it should return T-SBE.

```
$ORIGIN 3.3.3.3.2.2.2.7.1.9.1.example.net
NATPTR 10 100 "u" "E2U+SIP"
  "!^.*!sip:+19172223333@t-proxy.example.net!"
```

9. T-SBE receives the NAPTR record and query DNS for the "t-proxy.example.net". The DNS returns an A-Record:

```
;; DNS ANSWER
t-proxy.example.net   A   192.0.2.20
```

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

```
INVITE sip:+19172223333@t-proxy.example.net;user=phone SIP/2.0
Via: SIP/2.0/TCP t-sbe1.example.net:5060
  ;branch= z9hG4bK28uyyy;
Max-Forwards: 10
From: Alice <sip:+14083332222@example.com;user=phone>
  ;tag=54321
To: Bob <sip:+19172223333@t-proxy.example.net;user=phone>
Call-ID: abcde-tsbe1@t-sbe1.example.com
CSeq: 1 INVITE
Contact: <sip:+14083332222@t-sbe1.example.net;user=phone
  ;transport=tcp>
```

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

```
INVITE sip:+19172223333@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=192.0.2.20
Max-Forwards: 9
Record-Route: <sip:t-proxy.example.net:5060;lr>,
  <sip:t-sbe1.example.net:5060;lr>
From: Alice <sip:+14083332222@example.com;user=phone>
  ;tag=54321
To: Bob <sip:+19172223333@t-proxy.example.net;user=phone>
Call-ID: abcde-tsbe1@t-sbe1.example.com
CSeq: 1 INVITE
Contact: <sip:+14083332222@t-sbe1.example.net;user=phone
  ;transport=tcp>
```

12. RTP is established between UAC and UAS.

5.1.1.1. Administrative characteristics

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

5.1.1.2. Options and Nuances

In Figure 2. O-SSP and T-SSP peer via SBEs. Normally, the operator will deploy the SBE in the edge of its administrative domain. The signalling traffic will pass between two networks through the SBEs. The operator has many reasons to deploy a SBE. For example, either

proxy and UA may use [RFC1918] addresses that 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 L5 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 a SBE, 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 administrative domain or both administrative domains can decide to deploy SBE. To the peer network, most important is to identify the next-hop address. Whether next-hop is a proxy or SBE, the peer network will not see any difference.

5.1.2. Static Direct Peering Use Case - Assisted LUF and LRF

This use case shares many properties with the static direct use case. There must exist a pre-association between the O-SSP and T-SSP. The difference is O-SSP will use the Assisted LUF/LRF Provider for LUF and LRF. This LUF/LRF provider stores the SED pre-populated by T-SSP. One important motivation to use the Assisted LUR/LRF provider is that T-SSP only needs to populate its SED once to the provider. Any O-SSP who wants to query T-SSP's SED can use this LUF/LRF provider. Current practice has shown that it is impractical for T-SSP to populate its SED to every O-SSP who likes to reach the T-SSP's subscribers. This is especially true in Enterprise environments.

```
                            +-----------------+
                            |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 +======|0-DBE+=======(12)======+T-DBE+=======+ UAS | |
       | +-----+      +-----+                 +-----+       +-----+ |
       +--------------------+                 +---------------------+
             example.com                            example.net
```

Static Direct Peering with Assisted LUF and LRF

Figure 3

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

Note that the media passes through O-DBE and T-DBE in the Figure 3. This is optional. A DBE may be needed for transcoding or other traffic policy for media.

5.1.2.1. Administrative Characteristics

The Assisted LUF/LRF provider provides the LUF and LRF services for the O-SSP. As such , LUF/LRF providers, O-SSP and T-SSP form a trusted administrative domain. To reach T-SSP, O-SSP must still require pre-arranged assignments for the peer relationship with T-SSP. L5 policy is maintained in the O-SSP and T-SSP domains, and LUF/LRF provider may not aware any L5 policy between O-SSP and T-SSP.

An Assisted LUF/LRF provider can serve multiple administrative

domains. the Assisted LUF/LRF provider must not share SED from one administrative domain to another administrative domain without appropriate permission granted.

5.1.2.2. Options and Nuances

The Assisted LRF/LRF provider can use multiple methods to provide SED to O-SSP. Most commonly used are ENUM query and SIP Redirect. O-SSP should negotiate with the Assisted LUF/LRF provider which query method it will use prior to sending query to the provider.

T-SSP needs to populate its users' SED to LUF/LRF provider. Currently, this procedure is non-standardized and labor intensive. IETF is working on this problem and trying to standardize this procedure for ENUM. [I-D.newton-peppermint-problem-statement], [I-D.lewis-peppermint-enum-reg-if], and [I-D.schwartz-peppermint-problem-statement] list the problem statements and requirements.

5.1.3. Static Indirect Peering Use Case - Assisted LUF and LRF

The difference between Static Direct Use Case and Static Indirect Use Case lies with the Layer-5 relationship O-SSP and T-SSP maintain. 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, O-SSP and T-SSP want to form peer relationship. For some reason, O-SSP and T-SSP don't have direct L5 connectivity. The reasons may vary, for example business demands and/or domain policy controls. Due to this indirect relationship the signalling will traverse from O-SSP to one or multiple I-SSP(s) to reach T-SSP.

In Enterprise environments, O-SSP normally forms peer relationship with an I-SSP or two I-SSP for redundancy. To reach T-SSP, O-SSP will forward the request to I-SSP and rely on I-SSP to route the request to T-SSP. This setup alleviates the requirements to establish direct peer relationship to every T-SSP. Thus, reduces the administration cost to manage a large number of peer relationships.

To further reduce the administration cost, O-SSP in this use case use an Assisted LUF/LRF provider to manage LUF/LRF.

Note that the Assisted 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)=|0-DBE+=====+I-DBE+======+T-DBE+=======+ UAS | |
       | +-----+      +-----+     +-----+      +-----+       +-----+ |
       +-------------------------------------------------------------+
            example.com          example.org         example.net
```

Indirect Peering via LUR/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:+19172223333@example.com;user=phone SIP/2.0
Via: SIP/2.0/TCP client.example.com:5060
  ;branch=z9hG4bK74bf9
Max-Forwards: 10
From: Alice <sip:+14083332222@example.com;user=phone>
  ;tag=12345
To: Bob <sip+19172223333@example.com;user=phone>
Call-ID: abcde@client.example.com
CSeq: 1 INVITE
Contact: <sip:+14083332222@client.example.com;user=phone
  ;transport=tcp>
```

2. UAC only knows UAS's TN but not UAS's domain. It appends its domain to generate the SIP-URI in R-URI and To header. O-Proxy checks the R-URI's domain and discovers that the UAS's domain is internal but the TN is unknown to O-Proxy. So, O-Proxy queries 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 3.3.3.3.2.2.2.7.1.9.1.example.com
  NATPTR 10 100 "u" "E2U+SIP"
   "!^.* !sip:\\1@i-sbe.example.org!"
```

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

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

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

```
 INVITE sip:+19172223333@i-sbe.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=192.0.2.1
 Max-Forwards: 9
 Route: <sip:o-sbe1.example.com;lr>
 Record-Route: <sip:o-proxy.example.com;lr>
 From: Alice <sip:+14083332222@example.com;user=phone>
   ;tag=12345
 To: Bob <sip+19172223333@example.net;user=phone>
 Call-ID: abcde@client.example.com
 CSeq: 1 INVITE
 Contact: <sip:+14083332222@client.example.com;user=phone
   ;transport=tcp>
```

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 R-URI and does a LRF for "i-sbe.example.org". In this example, the LRF is a DNS lookup of the domain. O-SBE receives a response similar to this:

```
;;       order perf flags service    regxp replacement
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 DNS query for the SRV record for "_sip._tcp.i-sbe.example.org".

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

6. O-SBE sends a DNS query for "i-sbe1.example.org" to get the A-Record:

```
;; DNS ANSWER
i-sbe1.example.org   A   192.0.2.10
i-sbe1.example.org   A   192.0.2.11
```

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 B2BUA, it will terminate the call and generate a new back-to-back INVITE request. If O-SBC 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:+19172223333@i-sbe1.example.org;user=phone SIP/2.0
Via: SIP/2.0/TCP o-sbe1.example.com:5060
  ;branch= z9hG4bK2d4zzz;
Max-Forwards: 10
From: Alice <sip:+14083332222@example.com;user=phone>
  ;tag=54321
To: Bob <sip:+19172223333@example.net;user=phone>
Call-ID: abcde-osbe1@o-sbe1.example.com
CSeq: 1 INVITE
Contact: <sip:+14083332222@o-sbe1.example.com;user=phone
  ;transport=tcp>
```

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:+19172223333@t-sbe1.example.net;user=phone SIP/2.0
Via: SIP/2.0/TCP i-sbe1.example.com:5060
  ;branch= z9hG4bK2d4777;
Max-Forwards: 10
From: Alice <sip:+14083332222@example.com;user=phone>
  ;tag=54321
To: Bob <sip:+19172223333@example.net;user=phone>
Call-ID: abcde-isbe1@i-sbe1.example.org
CSeq: 1 INVITE
Contact: <sip:+14083332222@i-sbe1.example.org;user=phone
  ;transport=tcp>
```

Note that 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 called party home proxy and directs call to called party. T-SBE may use ENUM or other internal mechanism to locate the home proxy. If T-SSP uses ENUM, this internal ENUM entry is different from the external ENUM entry populated for O-SSP. For internal use, it should return the home proxy of UAS. For external use, it should return T-SBE.

```
$ORIGIN 3.3.3.3.2.2.2.7.1.9.1.example.net
NATPTR 10 100 "u" "E2U+SIP"
  "!^.* !sip:+19172223333@t-proxy.example.net!"
```

10. T-SBE receives the NAPTR record and query DNS for the "t-proxy.example.net". The DNS returns an A-Record:

```
;; DNS ANSWER
t-proxy.example.net   A   192.0.2.20
```

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

```
INVITE sip:+19172223333@t-proxy.example.net;user=phone SIP/2.0
Via: SIP/2.0/TCP t-sbe1.example.net:5060
  ;branch= z9hG4bK28uyyy;
Max-Forwards: 10
Record-Route: <sip:t-sbe1.example.net:5060;lr>
From: Alice <sip:+14083332222@example.com;user=phone>
  ;tag=54321
To: Bob <sip:+19172223333@example.net;user=phone>
Call-ID: abcde-tsbe1@t-sbe1.example.net
CSeq: 1 INVITE
Contact: <sip:+14083332222@t-sbe1.example.net;user=phone
  ;transport=tcp>
```

12. Finally, UAS's home proxy forwards the INVITE request to UAS.
13. RTP is established between UAC and UAS.

5.1.3.1. Administrative characteristics

This use case looks very similar to Static Direct Peering with Assisted LUF and LRF. The major difference is O-SSP and T-SSP do not have direct L5 connectivity. Instead, O-SSP connects to T-SSP indirectly via I-SSP.

O-SSP uses this use case when it uses different I-SSP to reach different T-SSP. Typically, LUF/LRF provider serves multiple O-SSP. Two O-SSP 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. In other words, given the O-SSP and T-SSP pair as input, LUF/LRF provider will return the SED of I-SSP that is trusted by O-SSP to forward the request to T-SSP.

There are two levels of trust relationship. First trust relationship between O-SSP and LUF/LRF provider. LUF/LRF provider provides LUF and LRF for O-SSP. Once O-SSP queries the SED, LUF/LRF provider is out of the picture. Second trust relationship is between O-SSP and I-SSP. I-SSP provides L5 connectivity to assist O-SSP to reach T-SSP. O-SSP and I-SSP have a pre-association for policy before peering happened. Although Figure 4 shows a single provider to provide both LUR/LRF and I-SSP, O-SSP can choose two different providers.

5.1.3.2. Options and Nuances

Similar to the Static Direct Peering Use Case, 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 5)

5.1.4. Static Indirect Peering Use Case

This use case O-SSP uses its internal LUF/LRF. One of the reasons of using internal LUF/LRF is 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. The challenge for O-SSP is to decide which I-SSP should be used to reach T-SSP. O-SSP could manually enter I-SSP information in the routing database. However, when O-SSP peers to multiple I-SSP, O-SSP may have multiple routes to reach the same T-SSP. If we further consider that an I-SSP may use another I-SSP to reach T-SSP, the permutation can grow exponentially. This is similar to the IP

routing problem eventually solved by BGP [RFC4271]. TRIP [RFC3219] is a candidate to solve this problem. However, market has yet to deploy TRIP in large scale.

```
+--------------------+-------------------+---------------------+
|       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)=+0-DBE+======+I-DBE+======+T-DBE+=======+ UAS | |
| +-----+      +-----+      +-----+      +-----+       +-----+ |
+--------------------------------------------------------------+
     example.com          example.org          example.net
```

Indirect Peering via I-SSP (SIP and media)

Figure 5

5.1.4.1. Administrative characteristics

The Static Indirect Use Case is implemented in cases where no direct interconnection exists between 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 signalling path. T-SSP will not accept message directly sent from O-SSP.

5.1.4.2. Options and Nuances

In Figure 4, we show I-DBE. This will be used when O-SSP and T-SSP do not have a common code. To involve I-DBE, I-SSP should know the list of codec supported by O-SSP and T-SSP. When I-SBE receives the INVITE, it will make a decision to invoke the I-DBE. Another scenario an I-DBE will be used is if O-SSP uses SRTP [RFC3711] for media and T-SSP does not support SRTP, I-DBE can be used.

6. On-demand Peering Use Cases

On-demand Peering [I-D.ietf-speermint-terminology] describes two SSPs form the peering relationship without a pre-arranged agreement.

6.1. On-demand Direct Peering Use Case

The basis of this use case is built on the fact that there is NOT a pre-established relationship between the O-SSP and the T-SSP. The O-SSP and T-SSP did not share any information prior to the dialog initiation request. When the O-Proxy invokes the LUF and LRF on the R-URI, the terminating user information must be publicly available. Besides, when the O-Proxy routes the request to the T-Proxy, the T-Proxy must accept the request without any pre-association with O-SSP.

6.1.1. 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. T-SSP makes its subscribers information available in public. This model mimics the Internet email model. Sender does not need an pre-arranged agreement to send email to the receiver.

6.1.2. Options and Nuances

Similar to Static Direct Peering Use Case, O-SSP and T-SSP can decide to deploy SBE. T-SSP is open to the public, T-SSP should prepare to suffer from the spam problem existing in email system. VoIP spam is considered more annoying than email spam to the subscribers. T-SSP should apply rules to filter spam calls.

7. Federations

This section discusses the federation concept, explains which

technical parameters make up the foundation of a federation and provides examples.

The concrete implementation details (e.g. "direct with one SBE" versus "direct with two SBEs") can involve all the use cases thus far described in the document.

7.1. Federation Examples

This section lists some examples of how federations can operate.

7.1.1. Trivial Federations

A private peering arrangement between two SSPs is a special case of a federation. These two SSP have agreed to exchange calls amongst themselves and they have set up whatever LUF/LRF/SBE plus Layer 3 infrastructure they need to route and complete the calls. This can be in a direct or indirect manner, but usually follows the direct call model.

It is thus not needed to treat bi-lateral peering as conceptually different to federation-based peering.

On the other extreme, the set of all SSPs implementing an open SIP service according to [RFC3261], [RFC3263], [RFC3761] also fulfills the definition of a federation. In that case, the technical rules are contained in these three RFCs, the LS is the public DNS. Whether some of these SSPs use SBCs as border elements is not relevant.

The administrative model of this federation is the "email model": There is no "member list", any SIP server operating on the Internet which implements call routing according to these RFCs is implicitly a member of that federation. No business relationship is needed between "members", thus no money is likely to change hands for terminating calls. There is no contractual protection against nuisance calls, SPIT or denial of service attacks.

7.1.2. Access List based Federations

If running an open SIP proxy is not desired, then a group of SSPs which want to allow calls from each other can collect the list of IP addresses of all their border elements.

This list is redistributed to all members which use it to configure firewalls in front of their ingress elements. Thus calls from other members of this federation are accepted while calls from other hosts on the Internet are blocked.

Whether SSPs deploy SBEs as border elements is not relevant. Call routing can still be done via standard RFC rules.

Whenever a new member joins this club every other SSP needs to adapt its filter rules.

7.1.3. Central SIP Proxy Federations

One way to simplify the management of these firewall rules is to route all SIP messages via a central proxy.

In that case, all federation members just need to open up their ingress elements to requests from that central server. A new SSP just triggers a change in the configuration of this box and not at all other SSPs.

While centralized solutions may entail typical hub-and-spoke architecture considerations, the added overall federation scalability with respect to the number of interconnects required, their associated policies and management make this approach quite popular today.

This is an example of Indirect Peering.

7.1.4. Architecture, scalability and business scalability

The network architecture which in the case centralized model would reflect a hub and spoke model - should be weighed against a distributed model. While such a centralized model presents well-known network and server scalability challenges, a distributed model requires higher interconnection complexity, reflected in provisioning and the need for the maintenance of such relationships.

8. Acknowledgments

This draft is a consolidation of many early individual drafts. Michael Haberler, Mike Mammer, Otmar Lendl, Rohan Mahy, David Schwartz, Eli Katz and Jeremy Barkan are the authors of the early individal drafts. 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 draft.

9. Security Considerations

This document introduces no new security considerations. However, it

is important to note that session interconnect, as described in this document, has a wide variety of security issues that should be considered in documents addressing both protocol and use case analyzes.

10. IANA Considerations

This document creates no new requirements on IANA namespaces [RFC5226].

11. References

11.1. Normative References

[I-D.lee-speermint-use-case-cable]
Lee, Y., "Session Peering Use Case for Cable", draft-lee-speermint-use-case-cable-01 (work in progress), September 2006.

[I-D.lendl-speermint-federations]
Lendl, O., "A Federation based VoIP Peering Architecture", draft-lendl-speermint-federations-03 (work in progress), September 2006.

[I-D.mahy-speermint-direct-peering]
Mahy, R., "A Minimalist Approach to Direct Peering", draft-mahy-speermint-direct-peering-02 (work in progress), July 2007.

[I-D.schwartz-speermint-use-cases-federations]
Schwartz, D., "Session Peering Use Cases for Federations", draft-schwartz-speermint-use-cases-federations-00 (work in progress), November 2006.

[I-D.uzelac-speermint-use-cases]
Uzelac, A., "SIP Peering Use Case for VSPs", draft-uzelac-speermint-use-cases-00 (work in progress), October 2006.

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

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets",

BCP 5, RFC 1918, February 1996.

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

[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.

[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.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

11.2. Informative References

[I-D.lewis-peppermint-enum-reg-if]
Lewis, E., "ENUM Registry Interface Requirements", draft-lewis-peppermint-enum-reg-if-01 (work in progress), November 2007.

[I-D.newton-peppermint-problem-statement]
Newton, A., "Provisioning Extensions in Peering Registries for Multimedia Interconnection (PEPPERMINT) Problem Statement", draft-newton-peppermint-problem-statement-00 (work in progress), January 2007.

[I-D.schwartz-peppermint-problem-statement]
Schwartz, D., Mahy, R., Duric, A., and E. Lewis, "Consolidated Provisioning Problem Statement", draft-schwartz-peppermint-problem-statement-00 (work in progress), February 2008.

[RFC3219] Rosenberg, J., Salama, H., and M. Squire, "Telephony Routing over IP (TRIP)", RFC 3219, January 2002.

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

[RFC4271] Rekhter, Y., Li, T., and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[RFC4366] Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, "Transport Layer Security (TLS) Extensions", RFC 4366, April 2006.

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