SPEERMING Working Group
Internet-Draft
Intended status: Informational
Expires: February 27, 2009

A. Uzelac, Ed.
Global Crossing
Y. Lee, Ed.
Comcast Cable

August 26, 2008

VoIP SIP Peering Use Cases
draft-ietf-speermint-voip-consolidated-usecases-10

Status of this Memo

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. In describing use cases, the intent is descriptive, not prescriptive.

Table of Contents

1. Introduction

This document attempts to capture Voice over IP (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.

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].

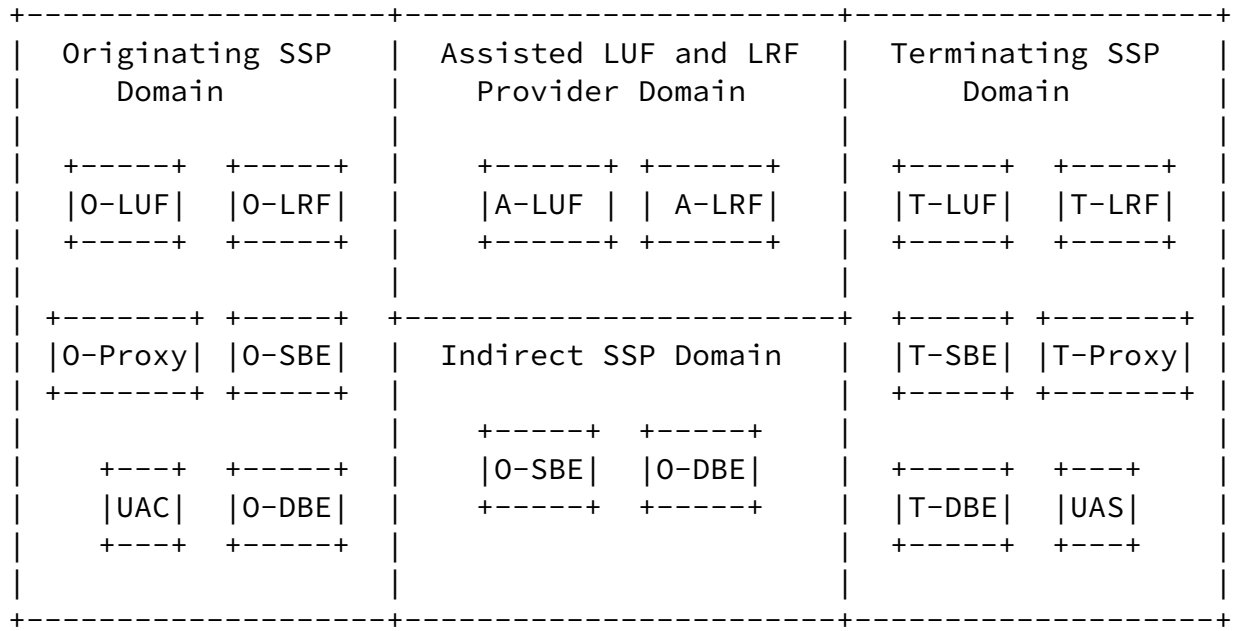
This document also uses terms defined in [I-D.ietf-speermint-terminology]. Please refer to it for definitions.

3. Reference Architecture

The diagram below provides the reader with a context for the VoIP use cases in this document. Terms such as SSP, LUF, LRF, SBE and DBE are defined in [I-D.ietf-speermint-terminology].

Originating SSP (O-SSP) is the SSP originating a request.
Terminating SSP (T-SSP) is the SSP terminating the request

originating from O-SSP. Assisted 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.



General Overview

Figure 1

Note that in Figure 1 - some 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 into Direct Peering and Indirect Peering [I-D.ietf-speermint-terminology]. 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 member when peering.

These can include:

- Peer Discovery - Peer discovery via a Look-Up Function (LUF) to determine the Session Establishment Data (SED) 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 URI [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. The O-SSP may also use the standard procedure

defined in [RFC3263] to discover the next hop.

- 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 Layer-3 network), which TLS client certificate [RFC3546] 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 example, the receiving SBE needs to determine whether the INVITE it received really came from a trusted member possibly via an access control list entry.

5. Use Cases

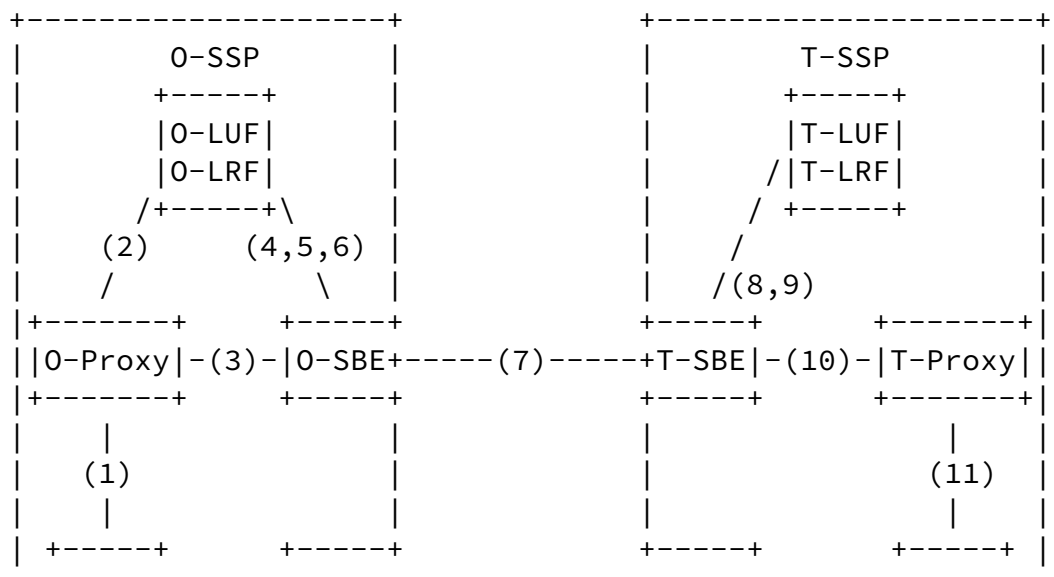
Please note there are intra-domain message flows within the use cases to serve as supporting background information. Only inter-domain communications are germane to Speermint.

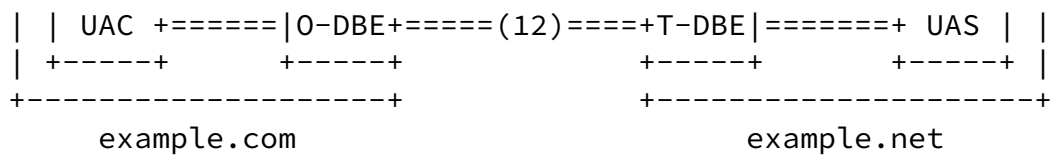
5.1. Static Peering Use Cases

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 an identification method (remote proxy IP address) and 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 is direct between the connected SSPs. 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.





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@client.example.com
CSeq: 1 INVITE
Contact: <sip:+19175550100@client.example.com;user=phone
  ;transport=tcp>
```

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. In the deployment where UAC does not have its own FQDN, UAC may insert IP address into the headers.

2. UAC only knows UAS's TN but not 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'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 [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 discover 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 s<ip+19175550100@example.com;user=phone>
Call-ID: abcde@client.example.com
CSeq: 1 INVITE
Contact: <sip:+19175550100@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 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 form 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 transport protocol, so it sends a SRV DNS query for the SRV record [RFC2782] for "_sip._tcp.t-sbe.example.net".

```
;;     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   192.2.0.100
  t-sbe1.example.net.   IN A   192.2.0.101
```

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 Back-to-Back User Agent (B2BUA) [RFC3261], 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:+19175550100@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:+14085550101@example.com;user=phone>
  ;tag=54321
To: Bob <sip:+19175550100@example.net;user=phone>
Call-ID: abcde-osbe1@o-sbe1.example.com
CSeq: 1 INVITE
Contact: <sip:+19175550100@o-sbe1.example.com;user=phone
  ;transport=tcp>
```

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 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. 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 query DNS for the A record of domain "t-proxy.example.net.". The DNS returns an A record:

```
;; DNS ANSWER
t-proxy.example.net.   IN A   192.2.1.2
```

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: 10
From: Alice <sip:+14085550101@example.com;user=phone>
  ;tag=54321
To: Bob <sip:+19175550100@t-proxy.example.net;user=phone>
Call-ID: abcde-tsbe1@t-sbe1.example.com
CSeq: 1 INVITE
Contact: <sip:+19175550100@t-sbe1.example.net;user=phone
  ;transport=tcp>
```

11. 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: 9
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@t-sbe1.example.com
CSeq: 1 INVITE
Contact: <sip:+19175550100@t-sbe1.example.net;user=phone
  ;transport=tcp>
```

12. RTP is established between UAC and UAS. Note that the media passes through O-DBE and T-DBE in the . This 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 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

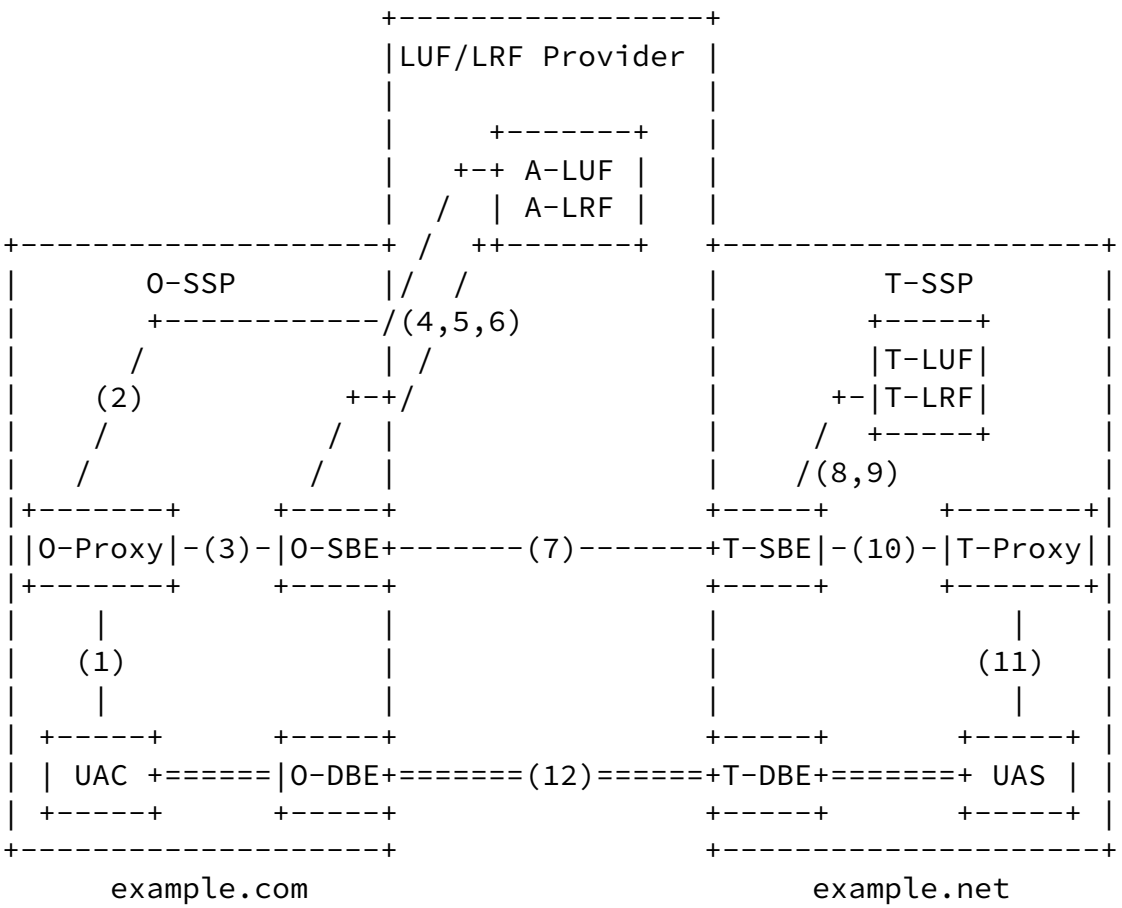
eases the operation cost for deploying or removing Layer-5 network elements. Consider the deployment architecture where multiple proxies connect to a single SBE. An operator can add or remove a proxy without coordinating with the peer operator. The peer operator "sees" only the SBE. As long as the SBE 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 administrative domain or both administrative domains can decide to deploy SBE(s). 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.

5.3. 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. In other words, LUF/LRF provider stores the SED to reach T-SSP and provides to O-SSP when O-SSP queries it.


LUF/LRF Provider
A-LUF
A-LRF
O-SSP
T-SSP
(4,5,6)
T-LUF
T-LRF
(2)
(8,9)
(1)
(11)
O-Proxy
(3)
O-SBE
(7)
T-SBE
(10)
T-Proxy
UAC
(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 LUF/LRF provider remotely instead of happening in O-SSP domain.

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

5.3.1. Administrative Characteristics

The LUF/LRF provider provides the LUF and LRF services for the O-SSP. As such , LUF/LRF provider, 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. Layer-5 policy is maintained in the O-SSP and T-SSP domains, and LUF/LRF provider may not aware any Layer-5 policy between 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 granted.

5.3.2. Options and Nuances

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 LUF/LRF provider which query method it will use prior to sending query to LUF/LRF 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.ietf-drinks-cons-rqts] lists the problem statements.

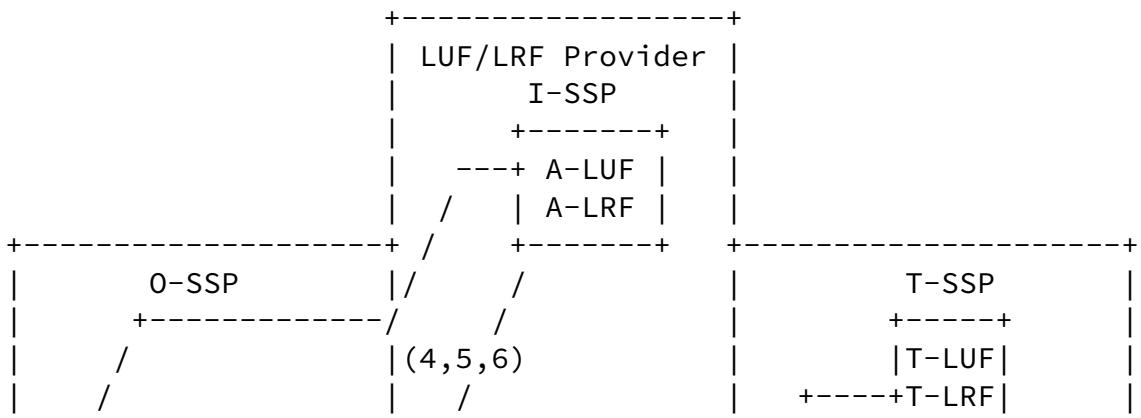
5.4. Static Indirect Peering Use Case - Assisted LUF and LRF

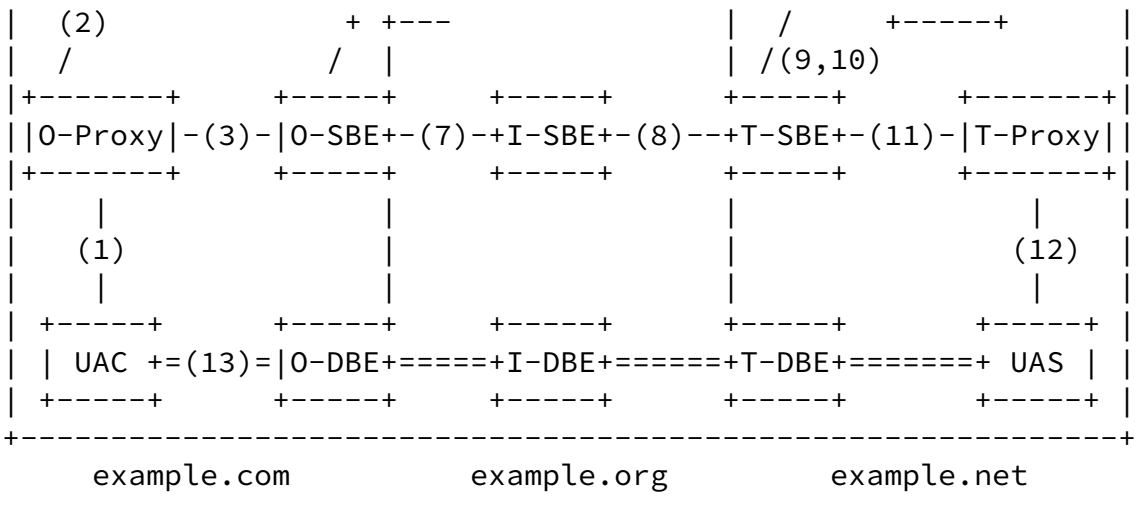
The difference between Static Direct Use Case and Static Indirect Use Case lies within the Layer-5 relationship of which O-SSP and T-SSP maintain. In the Indirect use case, the O-SSP and T-SSP do not have direct Layer-5 connectivity. They require one or multiple Indirect Domains to assist routing the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

In this use case, O-SSP and T-SSP want to form a peer relationship. For some reason, 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 signalling will traverse from O-SSP to one or multiple I-SSP(s) to reach T-SSP.

In addition, O-SSP decides to use a LUF/LRF provider. This LUF/LRF provider stores the SED pre-populated by T-SSP. One important motivation to use the 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 rather difficult 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 environment.

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





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:+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@client.example.com
CSeq: 1 INVITE
Contact: <sip:+19175550100@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 Request-URI and To header. O-Proxy checks the Request-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:

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

Note that the response shows the next-hop is the SBE in 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. O-Proxy routes the INVITE request to O-SBE and adds a Route header which contains 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@client.example.com
CSeq: 1 INVITE
Contact: <sip:+19175550100@client.example.com;user=phone
  ;transport=tcp>
```

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.".

```
;;     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   192.3.0.100
i-sbe1.example.org.   IN A   192.3.0.101
```

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:+19175550100@example.org;user=phone SIP/2.0
Via: SIP/2.0/TCP o-sbe1.example.com:5060
  ;branch= z9hG4bK2d4zzz;
Max-Forwards: 10
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@o-sbe1.example.com
CSeq: 1 INVITE
Contact: <sip:+19175550100@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:+19175550100@.example.net;user=phone SIP/2.0
Via: SIP/2.0/TCP i-sbe1.example.org:5060
  ;branch= z9hG4bK2d4777;
Max-Forwards: 10
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@i-sbe1.example.org
CSeq: 1 INVITE
Contact: <sip:+19175550100@i-sbe1.example.org;user=phone
  transport=tcp>
```

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 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. 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 query DNS for the A record of "t-proxy.example.net". The DNS returns an A record:

```
;; DNS ANSWER
t-proxy.example.net.   IN A   192.2.1.2
```

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: 10
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@t-sbe1.example.com
CSeq: 1 INVITE
```

```
Contact: <sip:+19175550100@t-sbe1.example.com;user=phone
  transport=tcp>
```

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: 9
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@t-sbe1.example.com
CSeq: 1 INVITE
Contact: <sip:+19175550100@t-sbe1.example.com;user=phone
  transport=tcp>
```

13. RTP is established between UAC and UAS.

5.4.1. 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 Layer-5 connectivity. Instead, O-SSP connects to T-SSP indirectly via I-SSP.

O-SSP employs this use case when it uses different I-SSP to reach

different T-SSPs. 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 for the SED, LUF/LRF provider is out of the picture. Second trust relationship is between O-SSP and I-SSP. I-SSP provides Layer-5 connectivity to assist O-SSP to reach T-SSP. O-SSP and I-SSP have a pre-association for policy before peering happens. Although Figure 4 shows a single provider to provide both LUR/LRF and I-SSP, O-SSP can choose two different providers.

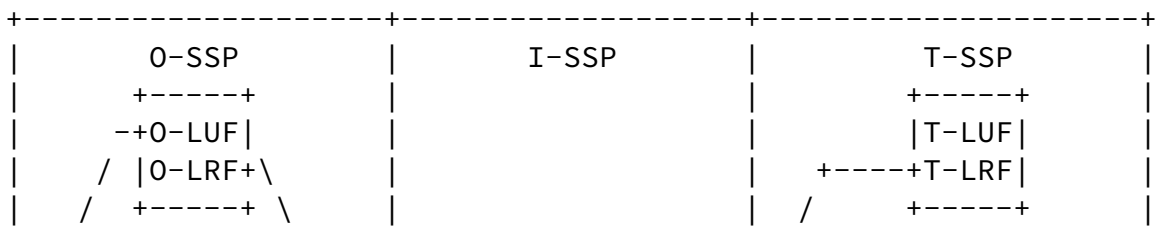
5.4.2. Options and Nuances

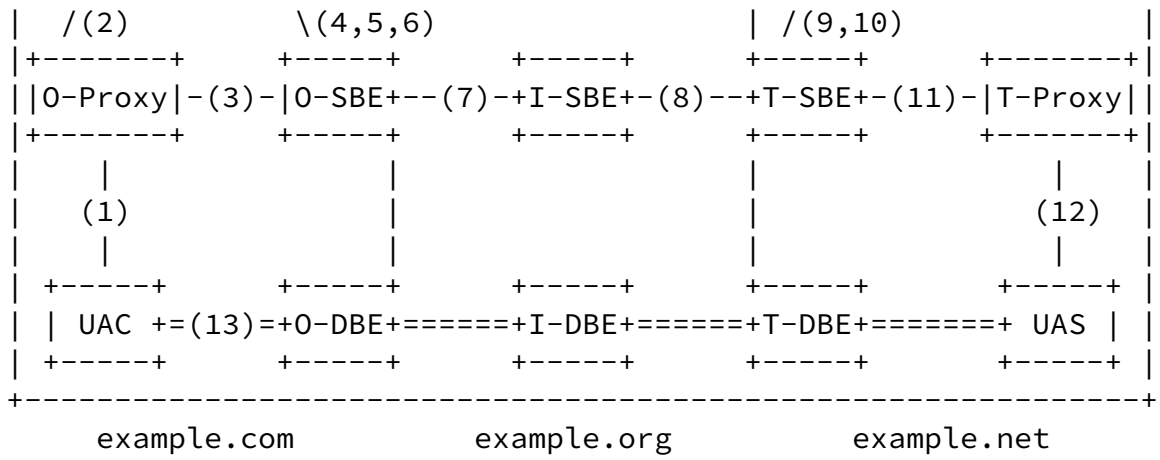
Similar to the Static Direct Peering Use Case, O-SSP and T-SSP may deploy SBE and DBE for NAT traversal, security, transcoding, etc. I-SSP can also deploy SBE and DBE for similar reasons. (as depicted

in Figure 4)

5.5. 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. Note that there could be multiple I-SSPs and multiple SIP routes to reach the same T-SSP; this is out of scope of speermint and has become a focus in the drinks working group.





Indirect Peering via I-SSP (SIP and media)

Figure 5

5.5.1. 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.

5.5.2. Options and Nuances

In Figure 5, we show I-DBE. One scenario the I-DBE can be used is

when O-SSP and T-SSP do not have a common codec. 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.

5.6. 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.

The basis of this use case is built on the fact that there is no 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 Request-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.

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. 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.

5.6.2. 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 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 launch by untrusted O-SSP.

6. Acknowledgments

This document is a consolidation of many early individual drafts (Please refer to the Section Informative References). Michael Haberler, Mike Mammer, Otmar Lendl, Rohan Mahy, David Schwartz, Eli Katz and Jeremy Barkan are the authors of the early individual 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 document.

7. Security and Privacy 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. [I-D.niccolini-speermint-voipthreats] discuss the different security threats related to VoIP peering.

8. IANA Considerations

This document creates no new requirements on IANA namespaces [RFC2434].

9. References

9.1. Normative References

[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.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[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.

9.2. Informative References

[I-D.ietf-drinks-cons-rqts]
Schwartz, D., Mahy, R., Duric, A., and E. Lewis, "Consolidated Provisioning Problem Statement", draft-ietf-drinks-cons-rqts-00 (work in progress), July 2008.

[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.niccolini-speermint-voipthreats]
Niccolini, S., Chen, E., and J. Seedorf, "SPEERMINT Security Threats and Suggested Countermeasures", draft-niccolini-speermint-voipthreats-04 (work in progress), July 2008.

[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.

[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.

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

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

Authors' Addresses

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

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

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

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

Full Copyright Statement

Intellectual Property

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.