DRINKS	S. Channabasappa, Ed.	
Internet-Draft	CableLabs	
Intended status: Informational	May 25, 2010	
Expires: November 26, 2010		

TOC

DRINKS Use cases and Protocol Requirements
draft-ietf-drinks-usecases-requirements-03

Abstract

This document captures the use cases and associated requirements for interfaces that provision session establishment data into SIP Service Provider components, to assist with session routing. Specifically, the current version of this document focuses on the provisioning of one such element, termed the registry.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.
Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as “work in progress.”
This Internet-Draft will expire on November 26, 2010.

Copyright Notice

Table of Contents

1. Terminology
2. Overview
3. Registry Use Cases
    3.1. Category: Provisioning Mechanisms
    3.2. Category: Interconnect Schemes
    3.3. Category: SED Exchange and Discovery Models
    3.4. Category: SED Record Content
    3.5. Category: Separation and Facilitation of Data Management
    3.6. Category: Lookup Keys
    3.7. Category: Number Portability
    3.8. Category: Misc
4. Requirements
5. Security Considerations
6. IANA Considerations
7. Acknowledgments
8. References
    8.1. Normative References
    8.2. Informative References

§ Author's Address

---

1. Terminology

TOC

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] (Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.).

This document reuses terms from [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," June 2002.) (e.g., SIP), [RFC5486] (Malas, D. and D. Meyer, "Session Peering for Multimedia Interconnect (SPEERMINT) Terminology," March 2009.) (e.g., LUF, LRF, SED) and [RFC5067] (Lind, S. and P. Pfautz, "Infrastructure ENUM Requirements," November 2007.) (carrier-of-record and transit provider). In addition, this document specifies the following additional terms.

Registry: The authoritative source for provisioned session establishment data (SED) and related information.

Registrar An entity that provisions and manages data into the registry.

Registrant An entity whose data is provisioned into the registry. The registrant can act as its own registrar or - additionally or alternatively - delegate this function to a third party who acts as its registrar.

Local Data Repository: The data store component of an addressing server that provides resolution responses.

Public Identifier: A public identifier refers to a telephone number (TN), an email address, or other identity as deemed appropriate, such as a globally routable URI of a user address (e.g., mailto:john.doe@example.net).

TN Range: A numerically contiguous set of telephone numbers whose SED can be looked up (resolved).

Destination Group: An aggregation of a set of public identifiers, TN Ranges, or RNs that share common SED.

Data Recipient: An entity with visibility into a specific set of public identifiers, the destination groups that contain these public identifiers, and a routing group’s SED records.

Routing Group: An aggregation that contains a related set of SED records, and is associated with a set of destination groups. Routing groups facilitate the management of SED records - which are common to a large number of public identifiers, TN Ranges or RNs - for one or more data recipients.

---

2. Overview

TOC

The SPEERMINT WG specifies Session Establishment Data, or SED, as the data used to route a call to the next hop associated with the called domain's ingress point. More specifically, the SED is the set of parameters that the outgoing signaling path border elements (SBEs) need to establish a session. See [RFC5486] (Malas, D. and D. Meyer, “Session Peering for Multimedia Interconnect (SPEERMINT) Terminology,” March 2009.) for more details.

The specification of the format and protocols to provision SED is a task taken up by the DRINKS WG. This document contains the use cases and requirements that have been proposed in this regard.

SED is typically created by the terminating SSP and consumed by the originating SSP. To avoid a multitude of bilateral exchanges, SED is often shared via intermediary systems - termed registries within this document. Such registries receive SED via provisioning transactions from other SSPs, and then distribute the received data into Local Data Repositories. These local data repositories are used for call routing by outgoing SBEs. This is depicted in Figure 1 (General Diagram).

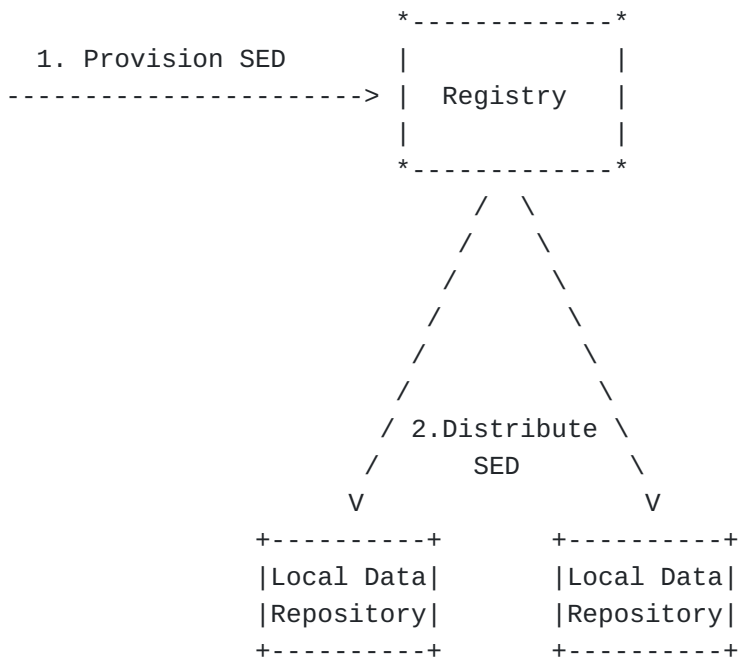

Figure 1: General Diagram

In this version of the document, we primarily address the use cases and requirements for provisioning registries. Future revisions may include

data distribution to local data repositories. The resulting provisioning protocol can be used to provision data into a registry, or between registries. This is depicted in Figure 2 (Functional Overview).

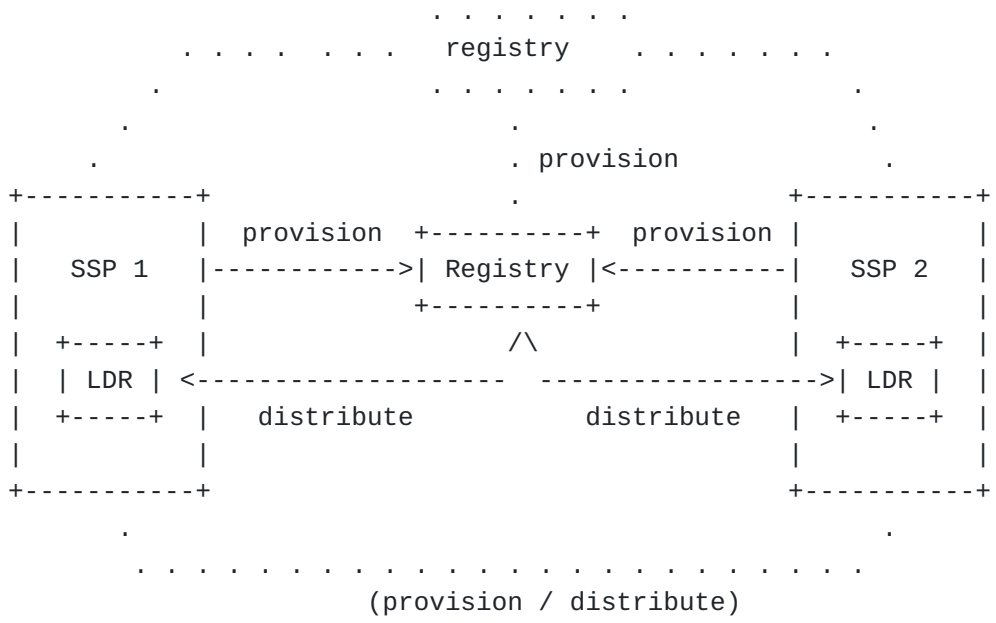

Figure 2: Functional Overview

In addition, this document proposes the following aggregation groups with regards to SED (refer to the use cases in Section 3.5 (Category: Separation and Facilitation of Data Management) for the rationale):

*Aggregation of public Identifiers into a destination group.

*Aggregation of SED records into a Routing Group.

The data model depicted in Figure 3 (Data Model Diagram) shows the various entities, aggregations and the relationships between them.

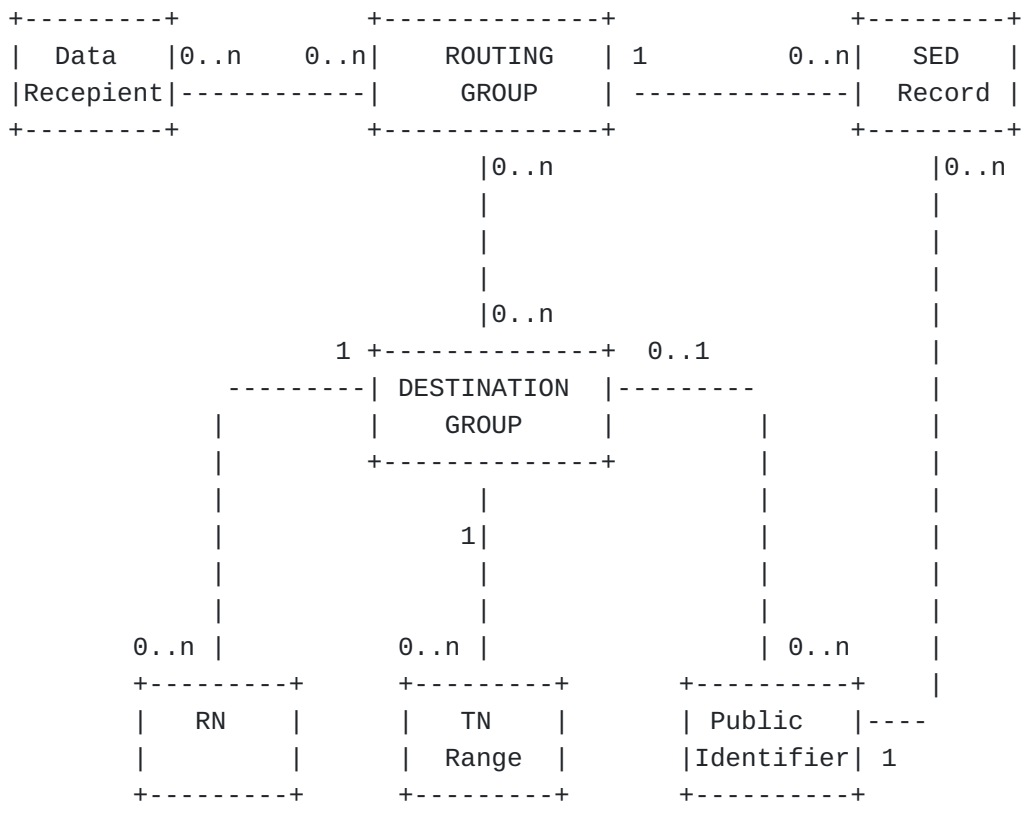

Figure 3: Data Model Diagram

The relationships are as described below:

- A Data Recipient object can be associated with zero or more Routing Group objects, and a Routing Group object can refer to zero or more Data Recipient objects.

- A Routing Group object can contain zero or more SED Record objects, and a SED Record object can be contained in exactly one

Routing Group object.

- A Routing Group object can be associated with zero or more Destination Group objects, and a Destination Group object can be associated with zero or more Routing Group objects.

- A Destination Group object can contain zero or more RN objects, and an RN object can be contained in exactly one Destination Group object.

- A Destination Group object can contain zero or more TN Range objects, and a TN Range object can be contained in exactly one Destination Group object.

- A Destination Group object can contain zero or more Public Identifier objects, and a Public Identifier object can be contained in exactly one Destination Group object.

---

3. Registry Use Cases

TOC

This Section documents use cases related to the provisioning of the registry. Any request to provision, modify or delete data is subject to authorization. However, the act of authorization is considered to be out of scope within this document.

3.1. Category: Provisioning Mechanisms

TOC

UC PROV #1 Real-Time Provisioning: Registrars have operational systems that provision public identifiers, in association with their SED. These systems often function in a manner that expect or require that these provisioning activities be completed immediately, as apposed to an out-of-band or batch provisioning scheme that can occur at a later time. This type of provisioning is referred to as real-time, or on-demand provisioning.

UC PROV #2 Non-Real-Time Bulk Provisioning: Operational systems that provision public identifiers and associated SED sometimes expect that these provisioning activities be batched up into large sets. These batched requests are then processed using a provisioning mechanism that is out-of-band and occurs at a later time.

UC PROV #3

Multi-Request Provisioning: Regardless of whether a provisioning action is performed in real-time or not, SSPs often perform several provisioning actions on several objects in a single request or transaction. This is done for performance and scalability reasons, and for transactional reasons, such that the set of provisioning actions either fail or succeed atomically, as a complete set.

3.2. Category: Interconnect Schemes

TOC

UC INTERCONNECT #1 Inter-SSP SED: SSPs create peering relationships with other SSPs in order to establish interconnects. Establishing these interconnects involves, among other things, communicating and enabling the points of ingress and other SED used to establish sessions to a set of public identifiers.

UC INTERCONNECT #2 Direct vs Indirect Peering: Some inter-SSP peering relationships are created to enable the establishment of sessions to the public identifiers for which an SSP is the carrier-of-record. This is referred to as direct peering. Other inter-SSP peering relationships are created to enable the establishment of sessions to public identifiers for which an SSP is a transit provider. This is referred to as indirect peering. Some SSPs take into consideration an SSP’s role as a transit or carrier-of-record provider when selecting a route to a public identifier.

UC INTERCONNECT #3 Intra-SSP SED: SSPs support the establishment of sessions between their own public identifiers, not just to other SSPs public identifiers. Enabling this involves, among other things, communicating and enabling intra-SSP signaling points and other SED that can differ from inter-SSP signaling points and SED.

UC INTERCONNECT #4 Selective Peering (a.k.a. per peer policies): SSPs create peering relationships with other SSPs in order to establish interconnects. However, SSPs peering relationships often result in different points of ingress or other SED for the same set of public identifiers.

UC INTERCONNECT #5

Provisioning of a delegated name server: An SSP maintains a Tier 2 name server that contains the NAPTR records that constitute the terminal step in the LUF. The SSP needs to provision a registry to direct queries for the SSP's numbers to the Tier 2 name server. Usually queries to the registry should return NS records, but in cases where the Tier 2 uses a different domain suffix from that used in the registry, CNAME and NS records may be employed instead.

3.3. Category: SED Exchange and Discovery Models

TOC

UC SED EXCHANGE #1 SED Exchange and Discovery using unified LUF/ LRF: When establishing peering relationships some SSPs wish to communicate or receive points of ingress and other SED that contain LUF and LRF.

UC SED EXCHANGE #2 SED Exchange and Discovery using LUF’s Domain Name: When establishing peering relationships some SSPs may not wish to communicate or receive points of ingress and other SED using a registry. They wish to only communicate or receive domain names resolvable via [RFC3263], and this query will then return the points of ingress or other SED that form the LUF.

UC SED EXCHANGE #3 SED Exchange and Discovery using LUF’s Administrative Domain Identifier: When establishing peering relationships some SSPs may not wish to communicate or receive points of ingress and other SED using a registry. They wish to only communicate or receive an administrative domain identifier, which is not necessarily resolvable via DNS. The subsequent process of using that administrative domain identifier to select points of ingress or other SED can be SSP specific and occurs outside the context of this protocol.

UC SED EXCHANGE #4 Co-existent SED Exchange and Discovery Models: When supporting multiple peering relationships some SSPs have the need to concurrently support all three of the SED Exchange and Discovery Models described above, for the same set of lookup keys.

3.4. Category: SED Record Content

TOC

UC SED RECORD #1 SED Record Content: Establishing interconnects between SSPs involves, among other things, communicating points of ingress, the service types (SIP, SIPS, etc) supported by each point of ingress, and the relative priority of each point of ingress for each service type.

UC SED RECORD #2 Time-To-Live (TTL): For performance reasons, querying SSPs sometimes cache SED that had been previously looked up for a given public identity. In order to accomplish this, SSPs sometimes specify the TTL associated with a given SED record.

3.5. Category: Separation and Facilitation of Data Management

TOC

UC DATA #1 Separation of Provisioning Responsibility: An SSP's operational practices often separate the responsibility of provisioning the points of ingress and other SED, from the responsibility of provisioning public identifiers (or TN ranges or RNs). For example, a network engineer can establish a physical interconnect with a peering SSP's network and provision the associated domain name, host, and IP addressing information. Separately, for each new subscriber, the SSP's provisioning systems provisions the associated public identifiers.

UC DATA #2 Destination Groups: SSPs often provision identical SED for large numbers of public identifiers. Groups of public identifiers that have the same SED are created. This grouping is know as Destination Group. SED is then indirectly associated with that group rather than to each individual public identity.

UC DATA #3 Route Groups: SSPs often provision identical SED for large numbers of public identifiers, and then expose that relationship between a group of SED records and a group of public identifiers to one or more SSPs. This combined grouping of SED records and Destination Groups facilitates management of public identity SED relationships and the list of peers (data recipients) that can lookup those public identifiers and receive that SED. This dual set of SED Records and Destination Groups is termed as a Route Group.

3.6. Category: Lookup Keys

TOC

UC LOOKUP #1 Additions and deletions: SSPs often allocate and de-allocate specific public identifiers to and from end-users. This involves, among other things, activating or deactivating specific public identifiers (or TN ranges or RNs), and directly (or indirectly) associating them with the appropriate points of ingress and other SED.

UC LOOKUP #2 Carrier-of-Record vs Transit Lookup Key Provisioning: Some inter-SSP peering relationships are created to enable the establishment of sessions to the lookup keys for which an SSP is the carrier-of-record. Other inter-SSP peering relationships are created to enable the establishment of sessions to lookup keys for which an SSP is a transit provider. Some SSPs take into consideration an SSP’s role as a transit or carrier-of-record provider when selecting a route to a public identifier.

UC LOOKUP #3 Multiplicity of Identical Lookup Keys: As described in previous use cases, SSPs provision lookup keys and their associated SED for multiple peering SSPs, and as both the carrier-of-record and transit provider. As a result, a given lookup key can reside in multiple destination groups at any given time.

UC LOOKUP #4 Lookup Key Destination Group Modification: SSPs often change the SED associated with a given lookup key. This involves, among other things, directly or indirectly associating them with a different point of ingress, different services, and/or different other SED.

UC LOOKUP #5 Lookup Key Carrier-Of-Record vs Transit Modification: SSPs may have the need to change their Carrier-Of-Record vs Transit role for lookup keys they previously provisioned.

UC LOOKUP #6 Modification of authority: An SSP indicates that it is the carrier-of-record for an existing public identity or TN Range. If the public identity or TN Range was previously associated with a different carrier-of-record then there are

multiple possible outcomes, such as: a) the previous carrier-of-record is disassociated, b) the previous carrier-of-record is relegated to transit status, or c) the new carrier-of-record is placed in inactive mode. The choice may be dependent on the deployment scenario, and is out of scope for this document.

3.7. Category: Number Portability

TOC

UC NP #1 EDITOR's NOTE: Need to clarify this further.

The SSP wishes to provide in query response to public identifiers an associated routing number or RN. This is the case when a set of public identifiers is no longer associated with original SSP but have been ported to a recipient SSP who provides access to these identifiers via a switch on the SS7 network identified by the RN. In this case a destination group containing all numbers that should be routed to this RN needs to be created and the route group associated with this DG needs to contain the RN

3.8. Category: Misc

TOC

UC MISC #1 Data Recipient Offer and Accept: When a peering relationship is established (or invalidated) SSPs provision (or remove) data recipients in the registry. However, a peer may first need to accept it's role (as a data recipient) before such a change is made effective. Alternatively an auto-accept feature can be configured for a given data recipient.

UC MISC #2 Open numbering plans: In several countries, an "open numbering plan" is used, which is such that the carrier-of-record does not in fact know the complete number, but instead only knows a portion of the E.164 number. The rest of the digits are handled by a PBX off of that carrier-of-record, and even the number of those digit is not fixed. For example, an SSP can be the carrier-of-record for "+123456789", and is also the carrier-of-record for every possible expansion of that number such as "+12345678901" and "+123456789012", even though the SSP does not know what those expansions could be, because the PBX decides that. This can be

described as the carrier-of-record effectively being authoritative for a "prefix".

---

4. Requirements

TOC

This Section lists the requirements based on the use cases in Section 3 (Registry Use Cases). Unless explicitly stated as optional, the registry provisioning interface must support these requirements.

REQ1: a) Real-time, b) non-real-time bulk, and c) multi-request provisioning.

REQ2: Inter-SSP SED with support for direct and indirect peering.

REQ3: Intra-SSP SED.

REQ4: Selective peering.

REQ5: Provisioning of a delegated name server.

REQ6: The following SED Exchange and discovery models (concurrently for the same public identifier): a) unified LUF/LRF, b) LUF-only with domain name, and c) LUF-only with administrative domain.

REQ7: Provisioning of SED Record content

REQ8: (Optional) Communicate the TTL for a given SED Record.

REQ9: Separation of responsibility of provisioning the points of ingress and other SED, from the responsibility of provisioning public identifiers.

REQ10: Additions and deletions of public identifiers, TN ranges and RNs.

REQ11:
Provisioning of, and modifications to, the following aggregations: destination group and route groups.

REQ12: Support the distinction between an SSP as a carrier-of-record provider versus transit provider.

REQ13: Support for lookup keys having identical business keys (the public identity string, the digits that comprise an RN, the start and end point of a TN range's range) that concurrently exist across multiple destination groups and where each destination group may be managed by different SSPs.
Editor's note: We need to simplify the above requirement.

REQ14: Modification of lookup keys by allowing them to be moved to a different destination group via an atomic operation.

REQ15: SSPs to change their Carrier-Of- Record vs Transit role.

REQ16: Support for modification of authority with the conditions described in UC LOOKUP #6.

REQ17: Destination group offer and acceptance (optionally support auto-acceptance).

REQ18: Open numbering plans.

---

5. Security Considerations

TOC

Session establishment data allows for the routing of SIP sesions within, and between, SIP Service Providers. Access to this data can compromise the routing of sessions and expose a SIP Service Provider to attacks such as service hijacking and denial of service. The data can be compromised by vulnerable functional components and interfaces identified within the use cases.

---

6. IANA Considerations

TOC

This document does not register any values in IANA registries.

---

7. Acknowledgments

TOC

This document is a result of various discussions held by the DRINKS requirements design team, which is comprised of the following individuals, in alphabetical order: Deborah A Guyton (Telcordia), Gregory Schumacher (Sprint), Jean-Francois Mule (CableLabs), Kenneth Cartwright (TNS, Inc.), Manjul Maharishi (TNS, Inc.), Penn Pfautz (AT&T Corp), Ray Bellis (Nominet), the co-chairs (Richard Shockey, Nuestar; and Alexander Mayrhofer, enum.at GmbH), and the editors of this document.

This specific version of the document is a result of contributions from, primarily, David Schwartz (XConnect), Kenneth Cartwright (TNS, Inc.) and Syed Ali (Neustar, Inc.). Other participants who reviewed and provided comments include: Alexander Mayrhofer (enum.at GmbH), Jean-Francois Mule (CableLabs), Manjul Maharishi (TNS, Inc.), Hadriel Kaplan (Acme Packet) and other participants on the DRINKS mailing list.

---

8. References

TOC

8.1. Normative References

TOC

[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).

8.2. Informative References

TOC

[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 (TXT).
[RFC3263]	

	Rosenberg, J. and H. Schulzrinne, “Session Initiation Protocol (SIP): Locating SIP Servers,” RFC 3263, June 2002 (TXT).
[RFC5067]	Lind, S. and P. Pfautz, “Infrastructure ENUM Requirements,” RFC 5067, November 2007 (TXT).
[RFC5486]	Malas, D. and D. Meyer, “Session Peering for Multimedia Interconnect (SPEERMINT) Terminology,” RFC 5486, March 2009 (TXT).

Author's Address

TOC

	Sumanth Channabasappa
	CableLabs
	858 Coal Creek Circle
	Louisville, CO 80027
	USA
Email:	sumanth@cablelabs.com