SPEERMINT Working Group
Internet-Draft
Expires: April 26, 2007

J-F. Mule
CableLabs

October 23, 2006

SPEERMINT Requirements for SIP-based VoIP Interconnection
draft-ietf-speermint-requirements-01.txt

Status of this Memo

Copyright Notice

Abstract

This document describes high-level guidelines and general requirements for Session PEERing for Multimedia INTerconnect. It also defines a minimum set of requirements applicable to session peering for Voice over IP interconnects. It is intended to become best current practices based on the use cases discussed in the speermint working group.

Table of Contents

1. Introduction

The Session PEERing for Multimedia INTerconnect (SPEERMINT) Working Group is chartered to focus on architectures to identify, signal, and route delay-sensitive communication sessions. These sessions use the Session Initiation Protocol (SIP) protocol to enable peering between two or more administrative domains over IP networks.

This document describes high-level guidelines and general requirements for session peering; these requirements are applicable to any type of multimedia session peering such as Voice over IP (VoIP), video telephony, and instant messaging. The document also defines a minimum set of requirements for a sub-set of the session peering use cases: VoIP interconnects.

The intent of this version of this document is to describe what mechanisms are used for establishing SIP session peering with a special look at VoIP interconnects, and in doing so, it defines some of requirements associated with the secure establishment of VoIP interconnects between a large number of peers.
The primary focus is on the requirements applicable to the boundaries of layer-5 SIP networks: SIP UA or end-device requirements are considered out of scope.
It is also not the goal of this document to mandate any particular use of any IETF protocols to establish session peering by users or service providers. However, when protocol mechanisms are used, the document aims at providing guidelines or best current practices on how they should be implemented, or configured and enabled in order to facilitate session peering.

Finally, a list of parameters for the definition of a session peering policy is provided in an informative annex. It should be considered as an example of the information a Voice Service Provider, or Application Service Provider may require in order to connect to another using SIP.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [RFC2119].

This specification makes use of terms defined in [I-D.ietf-speermint-terminology], the Session Description Protocol (SDP) [RFC4566] and the Session Initiation Protocol (SIP) [RFC3261]. We also use the terms Voice Service Provider (VSP) and Application Service Provider (ASP) as defined in [I-D.ietf-ecrit-requirements].

3. General Requirements

The following section defines general guidelines and requirements applicable to session peering for multimedia sessions.

- Session peering should be independent of lower layers. The mechanisms used to establish session peering SHOULD accommodate diverse supporting lower layers.

  Motivations:
  Session peering is about layer 5 mechanisms. It should not matter whether lower layers rely on the public Internet or are implemented by private L3 connectivity, using firewalls or L2/L3 Virtual Private Networks (VPNs), IPSec tunnels or Transport Layer Security (TLS) connections [RFC3546]...

- Session Peering Policies and Extensibility:
  Policies developed for session peering SHOULD be flexible and extensible to cover existing and future session peering models. It is also RECOMMENDED that policies be published via local configuration choices in a distributed system like DNS rather than in a centralized system like a 'peering registry'.
  In the context of session peering, a policy is defined as the set of parameters and other information needed by one VSP/ASP to connect to another. Some of the session policy parameters may be statically exchanged and set throughout the lifetime of the peering relationship. Others parameters may be discovered and updated dynamically using by some explicit protocol mechanisms. These dynamic parameters may also relate to a VSP/ASP's session-dependent or session independent policies as defined in [I-D.ietf-sipping-session-policy-framework].

  Motivations:
  It is critical that the solutions be flexible and extensible given the various emerging models: layer 5 peering may involve open federations of SIP proxies, or closed environments with systems that only accept incoming calls from selected peers based on a set of bilateral trust relationships. Federations may also be based on memberships in peering fabrics or voice service provider clubs, etc. Session peering may be direct or indirect.
  The maintenance of the "system" should scale beyond simple lists of peering partners. In particular, it must incorporate aggregation mechanisms which avoid O(n^2) scaling (where n is the number of participating peers). The distributed management of the DNS is a good example for the scalability of this approach.

- Administrative and Technical Policies:
  Various types of policy information may need to be discovered or

exchanged in order to establish session peering. At a minimum, a policy SHOULD specify information related to call addressing data in order to avoid session establishment failures. A policy MAY also include information related to QoS, billing and accounting, layer-3 related interconnect requirements which are out of the scope of this document.

Motivations:
The reasons for declining or accepting incoming calls from a prospective peering partner can be both administrative (contractual, legal, commercial, or business decisions) and technical (certain QoS parameters, TLS keys, domain keys, ...). The objectives are to provide a baseline framework to define, publish and optionally retrieve policy information so that a session establishment does not need to be attempted to know that imcompatible policy parameters will cause the session to fail (this was originally referred to as "no blocked calls").

- URIs and Domain-Based Peering Context:
  Call Addressing Data SHOULD rely on URIs (Uniform Resource Identifiers, RFC 3986 [RFC3986]) for call routing and SIP URIs SHOULD be preferred over tel URIs (RFC 3966 [RFC3966]). Although the initial call addressing data may be based on E.164 numbers for voice interconnects, a generic peering methodology SHOULD NOT rely on such E.164 numbers.

  Motivations:
  Telephone numbers commonly appear in the username portion of a SIP URI. When telephone numbers are in tel URIs, SIP requests cannot be routed in accordance with the traditional DNS resolution procedures standardized for SIP as indicated in RFC 3824 [RFC3824]. Furthermore, we assume that all SIP URIs with the same domain-part share the same set of peering policies, thus the domain of the SIP URI may be used as the primary key to any information regarding the reachability of that SIP URI.

- URI Reachability and Minimal additional cost on call initiation:
  Based on a well-known URI (for e.g. sip, pres, or im URIs), it MUST be possible to determine whether the domain servicing the URI (VSP/ASP) allows for session peering, and if it does, it SHOULD be possible to locate and retrieve the domain's policy and signaling functions. For example, an originating service provider must be able to determine whether a SIP URI is open for direct interconnection without requiring to initiate a SIP request. Furthermore, since each call setup implies the execution of any proposed algorithm, the establishment of a SIP session via peering SHOULD incur minimal overhead and delay, and employ caching wherever possible to avoid extra protocol round trips.

Motivations:
This requirement is important as unsuccessful call attempts are highly undesirable since they can introduce high delays due to timeouts and can act as an unintended denial of service attack (e.g., by repeated TLS handshakes). There should be a high probability of successful call completion for policy-conforming peers.

- Variability of the Call Address Data:
  A terminating VSP/ASP or user SHOULD be able to indicate its domain ingress points (Signaling Path Border Element(s)) based on the identity of the originating VSP/ASP or user.
  The mechanisms recommended for the use and resolution of the call addressing data SHOULD allow for variability or customization of the response(s) depending on various elements, such as the identity of the originating or terminating user or user domain.

4. Requirements for SIP-based VoIP Interconnection

This section defines some requirements for SIP-based VoIP Interconnection. It should be considered as the minimal set of requirements to be implemented to perform SIP VoIP interconnects.

4.1. DNS, Call Addressing Data (CAD) and ENUM

Call Addressing Data can be derived from various mechanisms available to the user, such as ENUM when the input is a telephone number, or other DNS queries using SRV and NAPTR resource records when the entry is a SIP URI for example. The SPEERMINT Working Group is focused on the use of CAD.

The following requirements are best current practices for VoIP session peering:

- SIP URIs SHOULD be preferred over tel URIs when establishing a SIP session for voice interconnects.

- The recommendations defined in [RFC3824] SHOULD be followed by implementers when using E.164 numbers with SIP, and by authors of NAPTR records for ENUM for records with an 'E2U+sip' service field. Other ENUM implementation issues and experiences are described in [I-D.ietf-enum-experiences] that may be relevant for VoIP interconnects using ENUM.

- The use of DNS domain names and hostnames is RECOMMENDED in SIP URIs and they MUST be resolvable on the public Internet.

- The DNS procedures specified in [RFC3263] SHOULD be followed to resolve a SIP URI into a reachable host (IP address and port), and transport protocol. Note that RFC 3263 relies on DNS SRV [RFC2782] and NAPTR Resource Records [RFC2915].

4.2. Minimum set of SIP-SDP-related requirements

The main objective of VoIP interconnects being the establishment of successful SIP calls between peer VSPs/ASPs, this section provides a minimum set of SIP-related requirements.

- The Core SIP Specifications as defined in [RFC3261] and [I-D.ietf-sip-hitchhikers-guide] MUST be supported by Signaling Path Border Elements and any other SIP implementations involved in session peering.
  Justifications:
  The specifications contained in the Core SIP group provide the fundamental and basic mechanisms required to enable VoIP

interconnects. This includes: the SIP protocol for session establishment and its updates such as RFC 3853 and RFC 4320, SDP [RFC4566] and its Offer/Answer model [RFC3264] for VoIP media session descriptions and codec negotiations, SIP Asserted Identity for caller ID services, and various other extensions to support NAT traversal, etc.

- The following RFCs SHOULD be supported: Reliability of Provisional Responses in SIP - PRACK [RFC3262], the SIP UPDATE method (for e.g. for codec changes during a session) [RFC3311], the Reason header field [RFC3326].

In the context of session peering where peers desire to maximize the chances of successful call establishment, the recommendations contained in RFC 3261 regarding the use of the Supported and Require headers MUST be followed. Signaling Path Border Elements SHOULD include the supported SIP extensions in the Supported header and the use of the Require header must be configurable on a per target domain basis in order to match a network peer policy and to maximize interoperability.

4.3. Media-related Requirements

VSPs engaged in session peering SHOULD support of compatible codecs and include media-related parameters in their domain's policy. Transcoding SHOULD be avoided by proposing commonly agreed codecs.

Motivations: The media capabilities of a VSP's network are either a property of the SIP end-devices, or, a combination of the property of end-devices and Data Path Border Elements that may provide media transcoding. The choice of one or more common codecs for VoIP sessions between VSPs is therefore outside the scope of speermint. Indeed, as stated in introduction, requirements applicable to end-devices of a VSP are considered out of scope. A list of media-related policy parameters are provided in the informative Section 5.

4.4. Security Requirements

4.4.1. Security in today's VoIP networks

In today's VoIP deployments, various approaches exist to secure exchanges between VSPs/ASPs. Signaling and media security are the two primary topics for consideration in most deployments. A number of transport-layer and network-layer mechanisms are widely used by some categories of VSPs: TLS in the enterprise networks for applications such as VoIP and secure Instant Messaging, IPSec and L2/L3 VPNs in some VSP networks where there is a desire to secure all signaling and media traffic at or below the IP layer. Media level

security is not widely deployed for RTP, even though it is in use in few deployments where the privacy of voice communications is critical.
A detailed security threat analysis of session peering exchanges should provide more guidance on what scalable and efficient methods should be used to help mitigate the the main security risks in large-scale session peering.

A recent IETF BoF at IETF 66 (rtpsec) was organized to analyze SIP requirements for SRTP keying; a number of security requirements for VoIP were discussed. A few Internet-Drafts have since been released and focus on media security requirements for SIP sessions ([I-D.ietf-wing-media-security-requirements]). Some of these scenarios may be applicable to interdomain VSP/ASP session peering or they may be augmented in the future by interdomain scenarios.

4.4.2. TLS Considerations for session peering

The remaining of Section 4 covers some details on how TLS could be deployed and used between 2 VSPs/ASPs to secure SIP exchanges. The intent is to capture what two VSPs/ASPs should discuss and agree on in order to establish TLS connections for SIP session peering.

1. Peers SHOULD agree on one or more Certificate Authorities (CAs) to trust for securing session peering exchanges.
Motivations:
A VSP/ASP should have control over which root CA it trusts for SIP communications. This may imply creating a certificate trust list and including the peer's CA for each authorized domain. This requirement allows for the initiating side to verify that the server certificate chains up to a trusted root CA. This also means that SIP servers SHOULD allow the configuration of a certificate trust list in order to allow a VSP/ASP to control which peer's CAs are trusted for TLS connections. Note that these considerations seem to be around two themes: one is trusting a root, the other is trusting intermediate CAs.

2. Peers SHOULD indicate whether their domain policies require proxy servers to inspect and verify the identity provided in SIP requests as defined in [RFC4474].

3. SIP servers involved in the secure session establishment over TLS MUST have valid X.509 certificates and MUST be able to receive a TLS connection on a well-known port.

4. The following TLS/SIP Protocol parameters SHOULD be agreed upon as part of session peering policies: the version of TLS supported by Signaling Border Elements (TLSv1, TLSv1.1), the SIP

TLS port (default 5061), the server-side session timeout (default 300 seconds), the list of supported or recommended ciphersuites, and the list of trusted root CAs.

5. SIP servers involved in the session establishment over TLS MUST verify and validate the client certificates: the client certificate MUST contain a DNS or URI choice type in the subjectAltName which corresponds to the domain asserted in the host portion of the URI contained in the From header. It is also recommended that VSPs/ASPs convey the domain identity in the certificates using both a canonical name of the SIP server(s) and the SIP URI for the domain as described in section 4 of [I-D.gurbani-sip-domain-certs]. On the client side, it is also critical for the TLS client to authenticate the server as defined in [RFC3261] and in section 9 of draft-ietf-sip-certs-01.txt.

6. A session peering policy SHOULD include details on SIP session establishment over TLS if TLS is supported.

5. Annex A - List of Policy Parameters for VoIP Interconnections

This informative annex lists the various types of parameters that should be considered when discussing the technical aspects of a VoIP Peering policy .

5.1. Categories of parameters and Justifications

It is intended as an initial list of topics that should be addressed by peers when establishing a VoIP peering relationship.

- IP Network Connectivity:
  It is assumed that IP network connectivity exists between peers. While this is out of scope of session peering, VSPs must agree upon a common mechanism for IP transport of Layer 5 session signaling and media. This may be accomplish via private (e.g. IPVPN, IPSEC, etc.) or public IP networks.

- Media-related Parameters:

  * Media Codecs: list of supported media codecs for audio, real-time fax (version of T.38, if applicable), real-time text (RFC 4103), DTMF transport, voice band data communications (as applicable) along with the supported or recommended codec packetization rates, level of RTP paylod redundancy, audio volume levels, etc.

  * Media Transport: level of support for RTP-RTCP [RFC3550], RTP Redundancy (RTP Payload for Redundant Audio Data - [RFC2198]) , T.38 transport over RTP, etc.

  * Other: support of the VoIP metric block as defined in RTP Control Protocol Extended Reports [RFC3611] , etc.

- SIP:

  * A session peering policy SHOULD include the list of supported and required SIP RFCs, supported and required SIP methods (including p headers if applicable), error response codes, supported or recommended format of some header field values , etc.

  * It should also be possible to describe the list of supported SIP RFCs by various functional groupings. A group of SIP RFCs may represent how a call feature is implemented (call hold, transfer, conferencing, etc.), or it may indicate a functional grouping as in [I-D.ietf-sip-hitchhikers-guide].

- Accounting:
  Call accounting may be required for tracking session usage on a peer's network. It is critical for peers to determine whether the support of any SIP extensions for accounting is a pre-requisite for SIP interoperability. In some cases, call accounting may feed data for billing purposes but not always: some operators may decide to use accounting as a 'bill and keep' model to track session usage and monitor usage against service level agreements. [RFC3702] defines the terminology and basic requirements for accounting of SIP sessions. A few private SIP extensions have also been defined and used over the years to enable call accounting between VSP domains such as the P-Charging* headers in [RFC3455], the P-DCS-Billing-Info header in [RFC3603], etc.

- Performance Metrics:
  Layer-5 performance metrics should be defined and shared between peers. The performance metrics apply directly to signaling or media; they may be used pro-actively to help avoid congestion, call quality issues or call signaling failures, and as part of monitoring techniques, they can be used to evaluate the performance of peering exchanges.
  Examples of SIP performance metrics include the maximum number of SIP transactions per second on per domain basis, Session Completion Rate (SCR), Session Establishment Rate (SER), etc.
  Some SIP end-to-end performance metrics are defined in [I-D.Malas-sip-performance]; a subset of these may be applicable to session peering and interconnects.
  Some media-related metrics for monitoring VoIP calls have been defined in the VoIP Metrics Report Block, in Section 4.7 of [RFC3611].

- Security:
  A VSP/ASP SHOULD describe the security requirements that other peers must meet in order to terminate calls to its network. While such a list of security-related policy parameters often depends on the security models pre-agreed to by peers, it is expected that these parameters will be discoverable or signaled in the future to allow session peering outside VSP clubs. The list of security parameters may be long and composed of high-level requirements (e.g. authentication, privacy, secure transport) and low level protocol configuration elements like TLS parameters.
  The following list is not intended to be complete, it provides a preliminary list in the form of examples:

  * Call admission requirements: for some providers, sessions can only be admitted if certain criteria are met. For example, for some providers' networks, only incoming SIP sessions signaled over established IPSec tunnels or presented to the well-known

TLS ports are admitted. Other call admission requirements may be related to some performance metrics as descrived above. Finally, it is possible that some requiremetns be imposed on lower layers, but these are considered out of scope of session peering.

* Call authorization requirements and validation: the presence of a caller or user identity MAY be required by a VSP/ASP. Indeed, some VSPs/ASPs may further authorize an incoming session request by validating the caller's identity against white/black lists maintained by the service provider or users (traditional caller ID screening applications or IM white list).

* Privacy requirements: a VSP/ASP MAY demand that its SIP messages be securely transported by its peers for privacy reasons so that the calling/called party information be protected. Media sessions may also require privacy and some ASP/VSP policies may include requirements on the use of secure media transport protocols such as sRTP, along with some contraints on the minimum authentication/encryption options for use in sRTP.

* Network-layer security parameters: this covers how IPSec security associated may be established, the IPSec key exchange mechanisms to be used and any keying materials, the lifetime of timed Security Associated if applicable, etc.

* Transport-layer security parameters: this covers how TLS connections should be established as described in Section 4.4.2

5.2. Summary of Parameters for Consideration in Session Peering Policies

The following is a summary of the parameters mentioned in the previous section. They may be part of a session peering policy and appear with a level of requirement (mandatory, recommended, supported, ...).

- IP Network Connectivity (assumed, requirements out of scope of this document)

- Media session parameters:

  * Codecs for audio, video, real time text, instant messaging media sessions

    * Modes of communications for audio (voice, fax, DTMF), IM (page mode, MSRP)

    * Media transport and means to establish secure media sessions

- SIP

    * SIP RFCs, methods and error responses

    * headers and header values

    * possibly, list of SIP RFCs supported by groups (e.g. by call feature)

- Accounting

- Performance Metrics: SIP signaling performance metrics; media-level VoIP metrics.

- Security: Call admission control, call authorization, network and transport layer security parameters, media security parameters

6. Acknowledgments

This document is a work-in-progress and it is based on the input and contributions made by a large number of people in the SPEERMINT working group, including: Scott Brim, Mike Hammer, Richard Shocky, Henry Sinnreich, Richard Stastny, Patrik Faltstrom, Otmar Lendl, Daryl Malas, Dave Meyer, Jason Livingood, Bob Natale, Brian Rosen, Eric Rosenfeld and Adam Uzelac.

7. Security Considerations

Securing session peering communications involves numerous protocol exchanges, first and foremost, the securing of SIP signaling and media sessions. The security considerations contained in RF 3261, RFC 4474 are applicable to the SIP protocol exchanges. A number of security considerations are also described in Section 4.4 for VoIP Interconnects.

8. References

8.1. Normative References

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

8.2. Informative References

[I-D.Malas-sip-performance]
Malas, D., "SIP End-to-End Performance Metrics", September 2006.

[I-D.gurbani-sip-domain-certs]
Gurbani, V., Jeffrey, A., and S. Lawrence, "Domain Certificates in the Session Initiation Protocol (SIP)", draft-gurbani-sip-domain-certs-03 (work in progress), August 2006.

[I-D.ietf-ecrit-requirements]
Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies", August 2006.

[I-D.ietf-enum-experiences]
Conroy, L. and K. Fujiwara, "ENUM Implementation Issues and Experiences", June 2006.

[I-D.ietf-sip-hitchhikers-guide]
Rosenberg, J., "A Hitchhikers Guide to the Session Initiation Protocol (SIP)", October 2006.

[I-D.ietf-sipping-session-policy-framework]
Hilt, V., "A Framework for Session Initiation Protocol (SIP) Session Policies", draft-ietf-sipping-session-policy-framework-01 (work in progress), June 2006.

[I-D.ietf-speermint-terminology]
Meyer, R., "SPEERMINT Terminology", September 2006.

[I-D.ietf-wing-media-security-requirements]
Wing, D., Fries, S., and H. Tschofenig, "A Framework for Session Initiation Protocol (SIP) Session Policies", draft-wing-media-security-requirements-00 (work in progress), October 2006.

[RFC2198] Perkins, C., Kouvelas, I., Hodson, O., Hardman, V.,

Handley, M., Bolot, J., Vega-Garcia, A., and S. Fosse-Parisis, "RTP Payload for Redundant Audio Data", RFC 2198, September 1997.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[RFC2915] Mealling, M. and R. Daniel, "The Naming Authority Pointer (NAPTR) DNS Resource Record", RFC 2915, September 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.

[RFC3262] Rosenberg, J. and H. Schulzrinne, "Reliability of Provisional Responses in Session Initiation Protocol (SIP)", RFC 3262, June 2002.

[RFC3263] Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

[RFC3264] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, June 2002.

[RFC3311] Rosenberg, J., "The Session Initiation Protocol (SIP) UPDATE Method", RFC 3311, October 2002.

[RFC3326] Schulzrinne, H., Oran, D., and G. Camarillo, "The Reason Header Field for the Session Initiation Protocol (SIP)", RFC 3326, December 2002.

[RFC3455] Garcia-Martin, M., Henrikson, E., and D. Mills, "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)", RFC 3455, January 2003.

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

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003.

[RFC3603] Marshall, W. and F. Andreasen, "Private Session Initiation Protocol (SIP) Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture", RFC 3603, October 2003.

[RFC3611] Friedman, T., Caceres, R., and A. Clark, "RTP Control Protocol Extended Reports (RTCP XR)", RFC 3611, November 2003.

[RFC3702] Loughney, J. and G. Camarillo, "Authentication, Authorization, and Accounting Requirements for the Session Initiation Protocol (SIP)", RFC 3702, February 2004.

[RFC3824] Peterson, J., Liu, H., Yu, J., and B. Campbell, "Using E.164 numbers with the Session Initiation Protocol (SIP)", RFC 3824, June 2004.

[RFC3966] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, December 2004.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, August 2006.

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.

Author's Address

Jean-Francois Mule
CableLabs
858 Coal Creek Circle
Louisville, CO 80027
USA

Email: jf.mule@cablelabs.com

Full Copyright Statement

Intellectual Property

Acknowledgment

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