Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 27, 2007

D. Schwartz
Kayote Networks
E. Katz
XConnect Global Networks
J. Barkan
Digitalshtick

October 24, 2006

Session Peering Use Cases for Federations
draft-schwartz-speermint-use-cases-federations-00.txt

Status of this Memo

Copyright Notice

Abstract

This document describes a use case involving session peering in Service Provider Federations. The scenario is based on the deployment experience gleaned from one such active federation. The focus in this document is on SIP layer interactions and supporting protocols commonly used in Federation based Layer 5 peering.

Table of Contents

1. Introduction

The purpose of this document is to highlight some of the actual peering models that are in practical use (commercial or other) today. This document should not be seen as a set of requirements for what peering should or should not be; rather, it is a statement of how voice-service provider peering is occurring in the IP world today. It is descriptive, not prescriptive. This document starts with a conceptual framework for understanding peering models. This framework is then mapped into the three identified peering model categories described in the SPEERMINT terminology draft [9]. Finally, a use case containing elements of all models and closely modeling an actual peering instance is presented.

2. Terminology

Terminology in this document follows the conventions listed in [9] with the following additions:

OU: Originating User - User Agent making the call

O-VSP: Originating Voice Service Provider - VSP providing voice services to OU

TU: Terminating User - User Agent receiving the call

T-VSP: Terminating Voice Service Provider - VSP providing voice services to TU

PSP: Peering Service Provider - A logical entity providing 1 or more of the 5 peering functions described in the next section

D-PSP: PSP providing location function or service enabling direct (D) peering [9]relationship

I-PSP: PSP providing peering functions on behalf of a VSP enabling indirect (I) peering [9]. Can include all peering functions or services other than location service

A-PSP: PSP providing all peering functions on behalf of VSP enabling Assisted (A) peering [9]. As opposed to the prior two PSP types, access to A-PSP is restricted to VSPs sharing the same federation as defined in [9]

3. Conceptual Model

A set of functional building blocks is defined for modeling peering. All models discussed in this document are analyzed with respect to six functions or services associated with the call setup across peering networks. Each of these functions presented below has an orthogonal layer of policy associated with it that defines the implementation of the function. The functions are:

L (Location) Location of termination Voice Service Provider

I (Interoperability) Signaling/media compatibility with T-VSP

S (Security) Security of transport, authenticity of O-VSP/T-VSP

T (Trust) Privacy, Identity [6], Authentication management, SPIT

R (Routing) Priority based traffic management

C (Cost) Cost of call

Each of these peering functions should have a policy framework associated with it consisting of the actual content (e.g. TLS vs. IPSec), negotiation and enforcement. Policy can be negotiated via anything from a simple fax to a dynamic, real- time policy exchange engine. Such negotiation is outside the scope of this document. As for policy content, the bullets below give some examples:

Location Function Policy Content:

- Query mechanism and format of data (NAPTR [1] , SIP 3XX [2])
- Location of authoritative information (Remote, Local)
- Type of data returned (Domain, IP)

  if domain - resolution of domain (static, DNS SRV [3])
- Whose location returned (T-VSP, Intermediary)
- O-VSP has access to (All data, Selected peers)
- Data retrieval (Unlimited, Rate limited)

Interoperability Function Policy Content:

- Supported RFCs
- DTMF mechanism [5]
- B2BUA Vs Proxy [2]
- Supported codecs[4]
- Transcoding function

Security Function Policy Content:

- Type (IPSec, TLS)
- Symmetric (IPSec IKE, mutual TLS)
- Asymmetric (TLS + Digest)

Trust Function Policy Content:

- o Peering relationship

  Privacy (signaling, media, location)

  Identity (Authentication server)

  Authentication (OU, O-VSP)

- o Per call

  SPIT (queries/sec, sequential requests, blacklists etc)

Routing Function Policy Content:

- o Priority based limiting

  Concurrent calls

  Call starts / sec

  Congestion

Cost Function Policy Content:

- o Gratis/Fee
- o Type of charge (per query, per call, per minute)
- o Prepaid/Postpaid
- o Currency

Please note that the content just described can exist at a number of overlapping logical entities including:

- At a PSP
- At a PSP, for a given Federation entity
- Static between specific peers O-VSP and T-VSP
- On a call by call basis between the peers

4. Scope

This document does not address the following issues relating to the use cases:

- Provisioning of information by the VSPs to location servers

  (e.g. Zone transfers, EPP, etc.)

- Negotiation of Policy
- Financial/business Motivations
- Issues discussed extensively in other documents including:

  ENUM NAPTR query [1]

SIP redirect mechanism

SRV "decoding" query [3]

Trust or security mechanisms [7],[8]

5. Peering Service Providers (PSPs)

PSPs as defined as follows:

> A PSP is a logical network entity providing one or more of the six peering functions described above. It may be co-located at one or both of the peered VSPs, or it may be a separate, independent entity.

The following matrix presents the functionality associated with each PSP type

	D-PSP	I-PSP	A-PSP
Location	Yes	No	Yes
Interoperability	No	Optional	Yes
Security	No	Optional	Yes
Trust	No	Optional	Yes
Routing	No	Optional	Optional
Cost	Optional	Optional	Optional

Figure 1: PSP functionality matrix

PSPs will be represented in the diagrams as circles containing the relevant functional elements. As noted above in the terminology section, access to PSP functionality may be limited to members of a federation. In this document membership in a federation will be denoted with the word "member" associated with a link to a PSP.

6. High-Level Peering Models

The three models described below are defined in the SPEERMINT terminology draft [9]. These models are reviewed here in the context of our conceptual framework. Short examples are provided for the

sake of completeness and clarity.

6.1. Bi-Lateral or direct peering

The figure below depicts a typical Bi-Lateral or direct peering relationship. While there may not be a need for a location service to provide remote lookup (i.e. in the case where all T-VSP user information is known by O-VSP) this is usually not the case. More often than not, the T-VSP user list is not known remotely and there is a need for T-VSP to be queried via either SIP redirect mechanism or ENUM to attain the required information. For the purposes of this document, VSPs upload their numbers to an externally reachable location service denoted as D-PSP. While in almost all cases of Bi-lateral relationships both O-VSP and T-VSP share a D-PSP (and could technically be considered members of this D-PSP "federation" - as shown in the figure below), depending on D-PSP policy, O-VSP may not need to be a member (e.g. share any of his own user base) in order to retrieve information about other members serviced by this D-PSP.

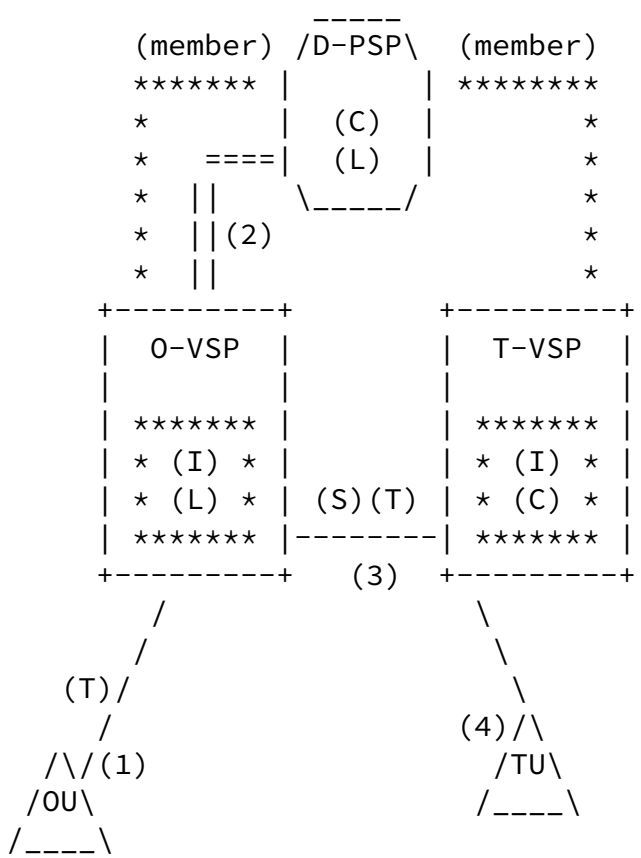


Figure 2: Direct peering example

The flow in this figure is as follows:

(1) OU sends signaling request containing TU username to O-VSP. Note the (T) depicting the need for trust between OU and O-VDP. As mentioned above, there are two popular protocols in use for purposes of querying the location service (2), namely ENUM and SIP INVITE (resulting in 3XX redirect message). In either case the resulting call routing data (CRD) [9] containing next hop routing information for this particular call is in the form "sip:TU@ T-VSP". This next hop domain name resolution service provided by D-PSP is denoted by the (L) enclosed in the D-PSP.

Once the next hop domain is retrieved there is a need for resolution into a routable address. This is performed by O-VSP (hence the (L) in the O-VSP) and can be done either statically based on preconfigured values or dynamically via DNS SRV. In either case, the call is then routed to T-VSP (3) over a secure channel and finally onto TU (4). Note that both O-VSP and T-VSP contain the interoperability function (I) as in most cases the Session Border Controller (SBCs) in each is responsible for this functionality. Note also that the link connecting the two VSPs has both (S) and (T) denoting the need for both transport layer security (S) and trust (T) in the form of Authenticated Identity. Finally, note the cost functions (C) located both at D-PSP and at T-VSP indicating possible charges associated with traffic (query or signaling) arriving at these entity.

6.2. Assisted peering

As described in the speerming-terminology draft, assisted peering involves the deployment by the federation of centralized SIP elements. These elements provide SIP proxy functionality, and are often implemented in practice by Session Border Controllers (SBCs), which may "filter" "normalize" and provide network-hiding for incoming messages en route to their final destination. Fear and distrust coupled with continued interoperability and security concerns have revived the need for the neutral central element role enabled by this peering model.

The figure below depicts a simplified assisted peering scenario containing two VSPs in an A-PSP assisted peering (A.K.A spoke and hub) federation. Note that as opposed to the case of the D-PSP federation where "membership" of the querying party is optional, in this model it is mandatory.

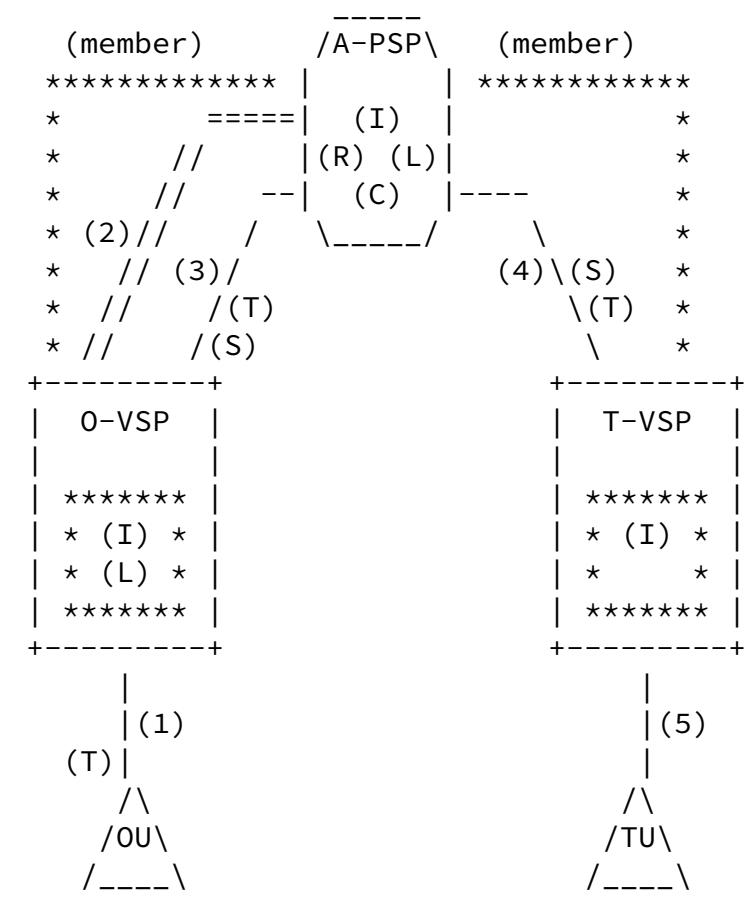


Figure 3: Assisted peering example

The flow being presented in this figure is one where end user OU is trying to call end user TU with both end users receiving services from different VSPs belonging to an assisted peering federation. The flow is as follows:

(1) OU sends a signaling request containing the TU username to O-VSP. O-VSP cannot resolve the TU on its own, and in order to determine the reachability of TU, must send a location query (2) to the federation (note the (L) function in A-PSP). Since this is an assisted peering federation, the response is in the form TU@ A-PSP signifying that the signaling needs to traverse the A-PSP. Once the A-PSP domain is retrieved there is a need for translation

into a routable address. This can be done statically (hence the (L) in the O-VSP) or dynamically via DNS SRV. In either case, the call is then routed to the A-PSP (3) over a secure channel. (note that step 2 can be eliminated by sending signaling directly to A-PSP).

The reason for the popularity of this model can be attributed to the concentration of functions provided by A-PSP. As an external element, A-PSP can provide the full set of services for VSPs, and

through its own relationships with the VSP, eliminate the need of all VSPs for pair-wise trust and service relationships. A-PSP can potentially encompass a large namespace of users that is accessible in one query (L) to external VSP members (or not - depending on policy). In addition there is an interoperability function (I) usually performed by a SIP Proxy, almost guaranteeing interoperability and protocol interchangeability between member VSPs. As part of the interoperability there is also is media sub-function enabling the federation to enforce a standard set of codecs or alternatively provide transcoding functionality to make sure there is media interoperability as well. Finally, A-PSP can implement the routing function (R) enabling traffic shaping and throttling across the federation.

In this flow A-PSP looks up the next hop for this call, receives an answer of the form sip:TU@T-VSP and translates to a routable next hop using either statically configured information or dynamically using DNS SRV. Next, A-PSP runs through additional logic before deciding if call can be routed to its destination. If no rules prevent the completion of the call it is then routed (4) to T-VSP and finally to TU (5). Here too note the possible cost function associated with A-PSP.

6.3. Indirect peering

The "Indirect" model defines a peering relationship that utilizes transient peering networks or VSPs that assist in connecting the OU to the TU. It is hard to implement this model without the additional use of one of the other models as the relationship of the O-VSP with the I-PSP will be either direct or assisted. For the sake of simplicity, this section will discuss a relatively simple model and leave a more complicated one for the next section. A simplistic

model appears in the figure below. Note that in this figure O-VSP is not a "member" of the same D-PSP as T-VSP. For this reason he is not granted direct access to T-VSP. Instead, the query (2) yields the address of an intermediary I-PSP that T-VSP does have a relationship with. In this scenario I-PSP and T-VSP are both "members" of a D-PSP.

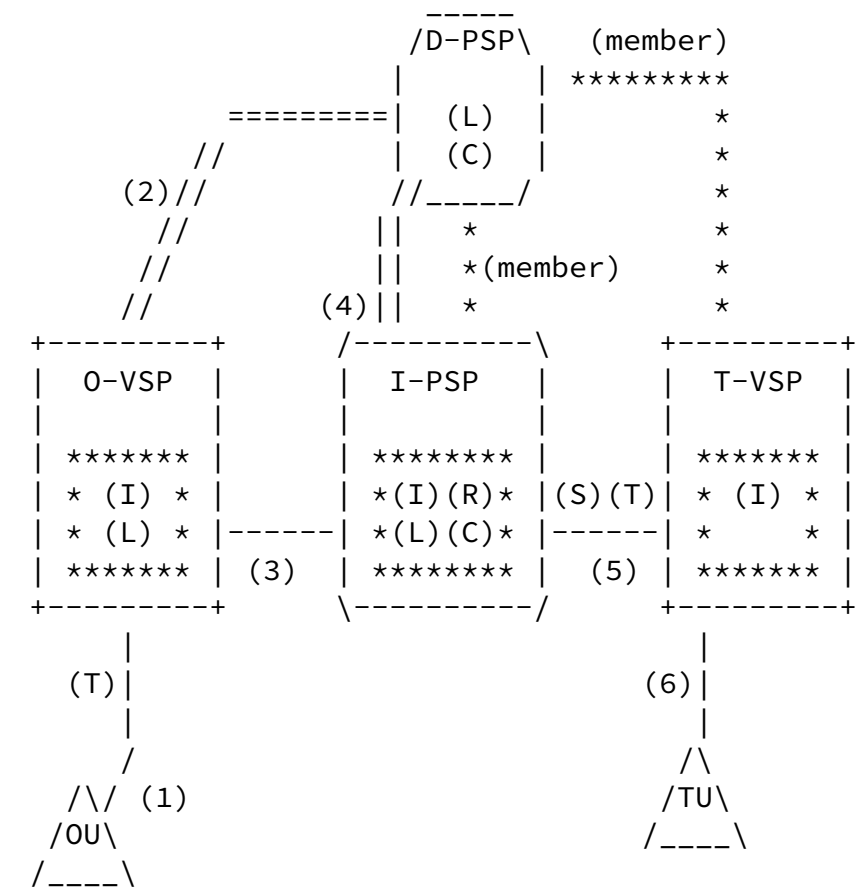


Figure 4: Indirect peering example

The flow in this scenario is as follows:

(1) OU sends signaling request containing TU username to O-VSP. O-VSP does not know who the user is and decides to query (2) D-PSP (which may be a public or private ENUM tree) about TU. Since T-VSP does not know or trust O-VSP, T-VSP does not want to accept any traffic directly from O-VSP and wants I-PSP to process call first to make sure it will not cause any trouble to T-VSP. T-VSP thus registers TU as belonging to I-PSP so that response to query in (2) is in the form sip:TU@I-PSP. O-VSP sends (3) the request to I-PSP. Note that there may be no trust relationship (T) or security relationship (S) between the two VSPs. Depending on policy at I-PSP this lack of security may cause call to be rejected. I-PSP has many peering functions available to it and after finding out where to route the call (4) and decoding the next hop domain information I-PSP can enforce policy for T-VSP prior to sending off to T-VSP (5) for its final destination (6). Note cost functions (C).

7. Use case combining different peering models

Actual real world peering models often contain more complexities than can be described by the individual models described above. However, by combining and composing these models, a more faithful representation can be found.

Consider a case where T-VSP has the flowing three relationships with other VSPs. The first relationship is an open one whereby T-VSP accepts traffic from anyone. The second relationship is as a member of a closed federation or premier club providing a higher class of service to all its members. In this federation there are no business, trust or technical issues preventing peering amongst members as the strict membership requirements reduce these risks for all members. The third relationship consists of premier type peers who are technically incapable of peering with all other members of the premier federation. They may have protocol or codec issues denying them equal access to all members of the premier federation.

The three relationships shall be denoted for the sake of this example OPEN, PREM and R-PREM. Incoming traffic from OPEN is accepted providing the following conditions are met:

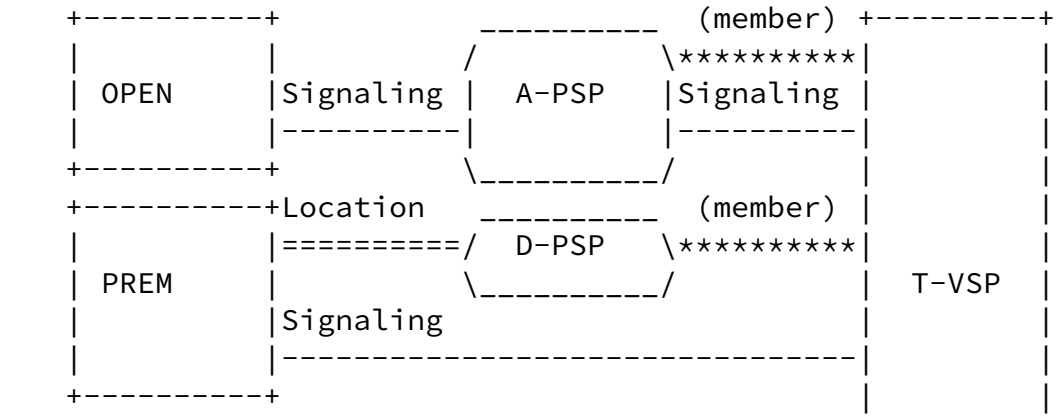
Complete anonymity of termination routing information is preserved preventing possibility of direct outside contact and bypassing of policy

Filtering of message for malicious content is performed prior to acceptance of call by T-VSP

Calls suspected as SPIT messages are flagged or blocked before acceptance

Dynamic throttling of outside traffic is available to give higher priority to premier traffic

The scenario described above is presented in the figure below



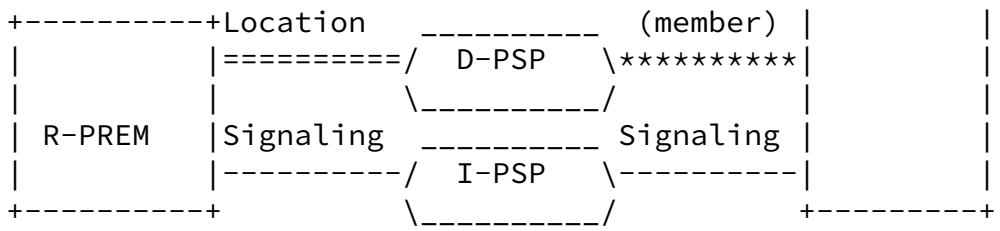


Figure 5: Hybrid peeering example

As can be seen in the figure above, the open provider OPEN must traverse an assisted peering federation A-PSP before being allowed to reach T-VSP. The premier peer PREM shares a D-PSP with T-VSP and as this relationship is just a Bi-Lateral one there is no need for intermediaries. The reduced premier provider R-PREM shares both a D-PSP and an I-PSP with T-VSP. As opposed to the OPEN that requires a full blown A-PSP, since the R-PREM does not require anonymity, the I-PSP is enough to bridge the technical divide.

8. Comparison of Models

In real world peering deployments, VSPs are players and stakeholders in the global VoIP space. As such, peering entities must consider financial and technical tradeoffs between the different models. Financial tradeoffs include capital and operational expenses associated with each model and technical tradeoffs include scalability and reliability of each model. Future versions of this document will present these tradeoffs in a detailed fashion.

9. Security Considerations

All Security considerations related to the SIP protocol are also applicable in peering relationships.

10. IANA Considerations

NA

11. Acknowledgements

This document is based on contributions made by Baruch Sterman, Mike Berkowitz and Brocha Strous of Kayote Networks and Natan Tiefenbrun of XConnect Global Networks.

12. References

12.1. Normative References

[1] Mealling, M. and R. Daniel, "The Naming Authority Pointer (NAPTR) DNS Resource Record", RFC 2119, September 2000.

[2] 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.

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

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

[5] Petrack, S. and H. Schulzrinne, "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals", RFC 2833, May 2000.

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

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

[8] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

12.2. Informative References

[9] Mayer, D., "SPEERMINT Terminology", draft-ietf-speermint-terminology-06.txt, September 2006.

[10] Mule, J., "SPEERMINT Requirements for SIP-based VoIP Interconnection", draft-ietf-speermint-requirements-00.txt, June 2006.

[11] Mahy, R., "A Minimalist Approach to Direct Peering", draft-mahy-speermint-direct-peering-00.txt, June 2006.

[12] Malas, D., Kahn, S., Peno, R., and A. Uzelac, "SPEERMINT Routing Architecture Message Flows", draft-ietf-speermint-flows-00.txt, September 2006.

[13] Haberler, M., Hammer, M., and O. Lendl, "A Federation based VOIP Peering Architecture", draft-lendl-speermint-federations-03.txt, September 2006.

Authors' Addresses

David Schwartz
Kayote Networks
Malcha Technology Park
Building # 1
Jerusalem 90961
Israel

Phone: +972 52 347 4656
Email: david.schwartz@kayote.com
URI: www.kayote.com

Eli Katz
XConnect Global Networks
1 Ballards Lane
London N3 1LQ
United Kingdom

Phone: +44 (0) 870 794 9990
Fax: +44 (0) 870 794 9991
Email: ekatz@xconnect.net
URI: www.xconnect.net

Jeremy Barkan
Digitalshtick
Shalom Yehuda 6
Jerusalem 93395
Israel

Phone: +972 2 6728069
Email: jeremyb@digitalshtick.com
URI: www.digitalshtick.com

Full Copyright Statement

Intellectual Property

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.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).