Network Working Group
Internet-Draft
Expires: August 21, 2006

D. Meyer

February 17, 2006

SPEERMINT Requirements and Terminology
draft-ietf-speermint-reqs-and-terminology-01.txt

Status of this Memo

Copyright Notice

Abstract

This document outlines the solutions space requirements and defines the terminology that is to be used by the Session PEERing for Multimedia INTerconnect Working Group (SPEERMINT). It has as its primary objective to focus the working group during its discussions, and when writing requirements, gap analysis and other solutions oriented documents.

Table of Contents

1. Introduction

The term "VoIP Peering" has historically been used to describe a wide variety of aspects pertaining to the interconnection of service provider networks and to the delivery of SIP call termination over those interconnections. The discussion of these interconnections has at times been confused by the fact that the term "peering" is used in various contexts to relate to interconnection at different levels in a protocol stack. Session Peering for Multimedia Interconnect focuses on how to identify and route real-time sessions (such as VoIP calls) at the application layer, and it does not (necessarily) involve the exchange of packet routing data or media sessions. In particular, "layer 5 network" is used here to refer to the interconnection between SIP servers, as opposed to interconnection at the IP layer ("layer 3"). Finally, the terms "peering" and "interconnect" are used interchangeably throughout this document.

This document introduces standard terminology for use in characterizing real-time session interconnection. Note however, that while this document is primarily targeted at the VoIP interconnect case, the terminology described here is applicable to those cases in which service providers interconnect using SIP signaling for real-time or quasi-real-time communications.

The remainder of this document is organized as follows: Section 2 provides the general context for the SPEERMINT Working Group. Section 3 provides the general definitions for real-time SIP based communication, with initial focus on the VoIP interconnect case, and Section 4 briefly touches on terms from the ENUM Working Group. Finally, Section 5 provides the requirements for SPEERMINT working group solutions.

2. Context

Figure 1 depicts the general VoIP interconnect context. In this case, the caller uses an E.164 number [ITU.E164.1991] as the "name" of the called user. Note that this E.164 number is not an address, since at this point we do not have information about where the named endpoint is located. In the case shown here, an E.164 number is used as a key to retrieve a NAPTR recored [RFC3404] from the DNS, which in turn resolved into a SIP URI. Call routing is based on this SIP URI. The call routing step does not depend on the presence of an E.164 number; the SIP URI can be advertised in various other ways, such as on a web page. Finally, note that the subsequent lookup steps, namely, lookup of SRV, A, and AAAA records (as well as any routing steps below that) are outside the scope of SPEERMINT.

```
E.164 number <--- Peer Discovery
     |
     | <--- ENUM lookup of NAPTR in DNS
     |
     |
     | ENUM Working Group Scope
=====+=======================================
     | SPEERMINT Working Group Scope
     |
     |
SIP URI <--- Call Routing Data (CRD)
     |
     | <--- Service Location (Lookup of SRV in DNS)
     |
     |
Hostname <--- Addressing and session establishment
     |
     | <---- Lookup of A and AAAA in DNS
     |
Ip address
     |
     | <---- Routing protocols, ARP etc
     |
Mac-address
```

Figure 1: Session Interconnect Context

The ENUM Working Group is primarily concerned with the acquisition of Call Routing Data, or CRD (i.e., above the double line in Figure 1), while the SPEERMINT Working Group is focused on the use of such CRD. Importantly, the CRD can be derived from ENUM (i.e., an E.164 DNS entry), or via any other mechanism available to the user.

3. General Definitions

3.1. Call Routing Data

Call Routing Data, or CRD, is a SIP URI used to route a call (real-time, voice or other type) to the called domain's ingress point. A domain's ingress point can be thought of as the location pointed to by the SRV record that resulted from the resolution of the CRD (i.e., a SIP URI).

3.2. Call Routing

Call routing is the set of processes, rules, and CRD used to route a call to its proper (SIP) destination. More generally, call routing

can be thought of as the set of processes, rules and CRD which are used to route a real-time session to its termination (ingress) point.

3.3. PSTN

The term "PSTN" refers to the Public Switched Telephone Network. In particular, the PSTN refers to the collection of interconnected circuit-switched voice-oriented public telephone networks, both commercial and government-owned. In general, PSTN terminals are addressed using E.164 numbers, noting that various dial-plans (such as emergency services dial-plans) may not directly use E.164 numbers.

3.4. Network

For purposes of this document and the SPEERMINT and ENUM Working Groups, a network is defined to be the set of SIP servers and end-users (customers) that are controlled by a single administrative domain. The network may also contain end-users who are located on the PSTN.

3.5. VoIP Service Provider

A VoIP service provider is an entity that provides transport of SIP signaling (and possibly media streams) to its customers. Such a service provider may additionally be interconnected with other service providers; that is, it may "peer" with other service providers. A VoIP service provider may also interconnect with the PSTN.

Note that as soon as a ingress point is advertised via a SRV record, anyone can find that ingress point and hence can send calls there. This is very similar to sending mail to a SMTP server based on the existence of a MX record.

3.6. Peering

While the precise definition of the term "peering" is the subject of some debate, peering in general refers to the negotiation of reciprocal interconnection arrangements, settlement-free or otherwise, between operationally independent service providers.

This document distinguishes two types of peering, Layer 3 Peering and Layer 5 peering, which are described below.

3.6.1. Layer 3 Peering

Layer 3 peering refers to interconnection of two service providers for the purposes of exchanging IP packets which destined for one (or

both) of the peer's networks. Layer 3 peering is generally agnostic to the IP payload, and is frequently achieved using a routing protocol such as BGP [RFC1771] to exchange the required routing information.

An alternate, perhaps more operational definition of layer 3 peering is that two peers exchange only customer routes, and hence any traffic between peers terminates on one of the peer's network.

3.6.2. Layer 5 Peering

Layer 5 peering refers to interconnection of two service providers for the purposes of SIP signaling. Note that in the layer 5 peering case, there is no intervening network. That is, for purposes of this discussion, there is no such thing as a "Layer 5 Transit Network".

3.7. Session Peering

Session peering is defined to be a layer 5 peering between two VoIP providers for purposes of routing real-time (or quasi-real time) call signaling between their respective customers. Media streams associated with this signaling (if any) are not constrained to follow the same set of paths.

4. ENUM

ENUM [RFC3761] defines how the Domain Name System (DNS) can be used for identifying available services connected to one E.164 number.

4.1. Carrier of Record

For purposes of this document, "Carrier of Record", or COR, refers to the entity that provides PSTN service for an E.164 number [I-D.lind-infrastructure-enum-reqs]. The exact definition of who and what is a COR is ultimately the responsibility of the relevant National Regulatory Authority.

4.2. Public ENUM

Public ENUM is generally defined as the set administrative policies and procedures surrounding the use of the e164.arpa domain for Telephone Number to URI resolution [RFC3761]. Policies and procedures for the registration of telephone numbers within all branches of the e164.arpa tree are Nation State issues by agreement with the IAB and ITU. National Regulatory Authorities have generally defined Public ENUM Registrants as the E.164 number holder as opposed to the COR that issued the phone number.

4.3. Private ENUM

Private ENUM is generally regarded as one or more technologies (including DNS and SIP Redirect) that service providers or enterprises may use to exchange phone number to URI mappings in a private secure manner. Private ENUM may be used in any mutually agreed upon domain. Records in Private ENUM may be globally visible but in most cases are not visible to the global Internet and are protected using a variety of security technologies such as split-DNS, VPN's or various forms or authentication and authorization. Technical comments on issues surrounding split-DNS can be found in [RFC2826].

4.4. Carrier ENUM

Carrier ENUM is generally regarded as the use of a separate branch the e164.arpa tree, such as 4.4.c.e164.arpa to permit service providers to exchange phone number to URI data in order to find points of interconnection. The current theory of Carrier ENUM is that only the COR for a particular E.164 number is permitted to provision data for that E.164 within that portion of the e164.arpa tree.

In carrier ENUM case, only the COR may enter data in the corresponding domain. The COR may also enter CRD (i.e., a SIP URI) to allow other VoIP Service Providers to route calls to its network.

Finally, note that ENUM is not constrained to carry only data (CDR) as defined by SPEERMINT. In particular, an an important class of CRD, the tel URIs [RFC3966] may be carried in ENUM. Such tel URIs are most frequently used to interconnect with the PSTN directly, and are out of scope for SPEERMINT. On the other hand, PSTN endpoints served by a COR and reachable via CDR and networks as defined in Section 3.1 and Section 3.4 are in scope for SPEERMINT.

5. Requirements

A system for real-time session interconnection must satisfy the following requirements:

5.1. Unified solution for all peering policies

Policies developed in the context of the SPEERMINT working group must be extensible and flexible enough to cover existing and future peering policies. These start by a closed system which accepts only incoming calls from selected peers (i.e. a set of bilateral peerings) and include the model of membership in a number of peering fabrics or

carrier clubs. The case of an open SIP proxy should be covered as a special case as well.

5.2. Domain Based

Although the initial call routing may be based on E.164 numbers, a generic peering methodology should not rely on such numbers. Rather, call routing should rely on URIs. 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.

5.3. No blocked calls

An originating service provide must be able to determine whether a SIP URI is open for direct interconnection without actually sending a SIP INVITE. This 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).

5.4. Scaling

The maintenance of the system needs to 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 service providers). Per-service provider opt-in without consultation of a centralized 'peering registry', but rather by publishing local configuration choices only is highly desirable. The distributed management of the DNS is a good example for the scalability of this approach.

5.5. Independence of lower layers

The system needs to be independent of details on what technologies are used route the call and which are used to ensure that only approved peering partner actually connect to the destination SIP proxy. It should not matter whether restrictions are implemented by private L3 connectivity ("walled gardens"), firewalls, TLS policies or SIP proxy configuration.

5.6. Administrative and technical policies

The reasons for declining vs. 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, ...). Methodologies developed by the SPEERMINT working group should accommodate all policies.

5.7. Minimal additional cost on call initiation

Since each call setup implies execution of any proposed algorithm it should incur minimal overhead and delay, and employ caching wherever possible to avoid extra protocol round trips.

5.8. Look beyond SIP

The problem of selective peering is not limited to SIP-based communication. Other protocols may benefit from a generic framework as well, such as SMTP mail. Any solutions proposed by the SPEERMINT working group must be generic enough to encompass other protocols as well.

6. Acknowledgments

Many of the definitions were gleaned from detailed discussions on the SPEERMINT, ENUM, and SIPPING mailing lists. Scott Brim, Mike Hammer, Jean-Francois Mule, Richard Shocky, Henry Sinnreich, and Richard Stastny all made valuable contributions to early revisions of this document. Patrik Faltstrom also made many insightful comments to early versions of this draft, and contributed the basis of Figure 1. Finally, Otmar Lendl contributed much of the text found in the Requirements section.

7. Security Considerations

This document itself 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.

8. IANA Considerations

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

9. References

9.1. Normative References

[RFC3404] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI)",

RFC 3404, 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.

[ITU.E164.1991] International Telecommunications Union, "The International Public Telecommunication Numbering Plan", ITU-T Recommendation E.164, 1991.

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

9.2. Informative References

[RFC1771] Rekhter, Y. and T. Li, "A Border Gateway Protocol 4 (BGP-4)", RFC 1771, March 1995.

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

[RFC2826] Internet Architecture Board, "IAB Technical Comment on the Unique DNS Root", RFC 2826, May 2000.

[I-D.lind-infrastructure-enum-reqs] Lind, S., "Infrastructure ENUM Requirements", draft-lind-infrastructure-enum-reqs-00 (work in progress), July 2005.

Author's Address

David Meyer

Email: dmm@1-4-5.net

Full Copyright Statement

Intellectual Property

Acknowledgment

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