Network Working Group
Internet-Draft
Expires: November 16, 2006

D. Meyer
May 15, 2006

SPEERMINT Terminology
draft-ietf-speermint-terminology-00.txt

Status of this Memo

Copyright Notice

Abstract

This document 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 5 briefly touches on terms from the ENUM Working Group. Finally, Section 6 introduces the concept of federations.

2. SPEERMINT Context

Figure 1 depicts the general VoIP interconnect context. In the case shown here, an E.164 number [ITU.E164.1991] is used as a key by ENUM to retrieve a NAPTR record [RFC3404] from the DNS, which in turn resolved into a SIP URI. Call routing is based on the resulting SIP URI. The call routing step does not depend on the presence of an E.164 number; indeed, the resulting SIP URI may no longer even contain any numbers, and the SIP URI can be advertised in various other ways, such as on a web page. Finally, note that the subsequent lookup steps described in RFC 3263 [RFC3263] used to find the next-hop SIP server from this URI are outside the scope of SPEERMINT.

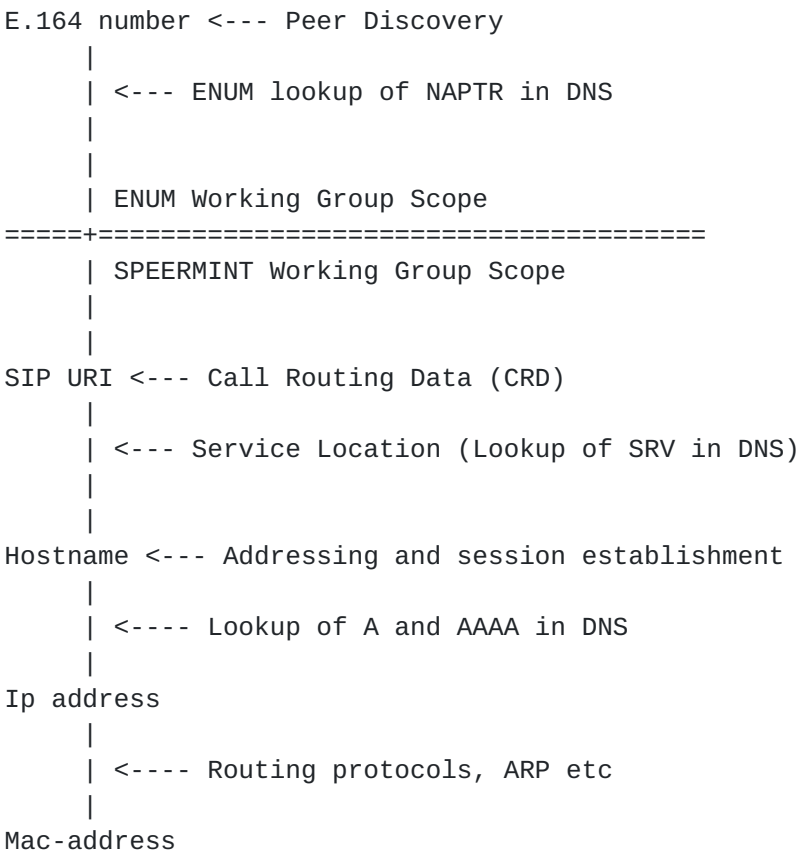

Figure 1: Session Interconnect Context

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. Service Provider

A Service Provider (or SP) is defined to be an entity that controls a "network" as defined in Section 3.4, and provides transport of SIP signaling and media packets.

3.6. Voice Service Provider

A Voice Service Provider (or VSP) 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 VSP 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.

Finally, note that the terms VSP and SP are used interchangeably in this document.

4. Peering

While the precise definition of the term "peering" is the subject of considerable 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.

4.1. 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.

4.2. Layer 5 Peering

Layer 5 peering refers to interconnection of two service providers for the purposes of SIP signaling. Such interconnection may be direct (e.g., in those cases where two SPs interconnect without an intervening Layer 5 network), or indirect (e.g., via some referral network). Of course, in the indirect case, transitive trust must typically be established.

4.3. 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.

4.4. Private Peering

Private Peering is generally regarded as the use of one or more technologies (including DNS/ENUM and, optionally, SIP Redirect) that service providers or enterprises may use to exchange phone number to URI mappings in a private secure manner.

Private Peering may use any mutually agreed upon domain name as an ENUM root, which may be a public or private root or domain. Records in such an ENUM root 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].

5. ENUM

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

5.1. 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. More specifically, the COR can be defined can defined as follows [I-D.ietf-enum-infrastructure-enum-reqs]:

- If the number in question has not been ported, then the COR is the Service Provider to which the E.164 number was allocated for end user assignment (either the National Regulatory Authority (NRA) or the International Telecommunication Union (ITU) makes these assignments), or

- If the number has been ported, the COR is the service provider to which the number was ported, or

- If the number is assigned directly to end users, the COR is the service provider that the end user number assignee has chosen to provide a Public Switched Telephone Network/Public Land Mobile Network (PSTN/PLMN) point-of-interconnect for the number.

Finally, note that the exact definition of who and what is a COR is ultimately the responsibility of the relevant NRA.

5.2. User ENUM

User 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]. In the User ENUM case, the entity (or person) having the right to use a number has the controls the content of the associated domain and thus the zone content (at the very least, there is local control over the content of the zone). From a domain registration perspective, the end user number assignee is thus the registrant [I-D.ietf-enum-infrastructure-enum-reqs].

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 Internet Architecture Board (IAB) and ITU. National Regulatory Authorities have generally defined User ENUM

Registrants as the E.164 number holder as opposed to the COR that issued the phone number.

5.3. Infrastructure ENUM

Infrastructure ENUM (also called Carrier ENUM) is generally regarded as the use of a separate branch the e164.arpa tree, such as i.e164.arpa to permit service providers to exchange phone number to URI data in order to find points of interconnection. The current theory of Infrastructure 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 infrastructure ENUM, only the COR may enter data in the corresponding domain. The COR may also enter CRD (i.e., a SIP URI) to allow other VSPs to 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.

6. Federations

The domain policy DDDS application [I-D.lendl-domain-policy-ddds] defines a method with which a domain owner can announce the policy it will use to accept incoming calls. This section introduces a policy type for use with that framework, known as federations [I-D.lendl-speermint-federations].

Briefly, a federation is a group of VSPs which agree:

- To receive calls from each other via SIP,
- On a set of administrative rules for such calls (settlement, abuse-handling, ...), and
- On specific rules for the technical details of the interconnection.

[I-D.lendl-domain-policy-ddds] does not define what these rules can be or how they might be communicated to the members of a federation. Further, there is no requirement that such rules are in any way public.

Example federation rules might include the following:

- A set of VSPs form an association and agree to accept calls from each other via the public Internet as long as the SIP call uses TCP/TLS as transport protocol and presents a X.509 cert which was signed by the association's own CA.

- A set of VSPs build a L3 network dedicated to VoIP peering (e.g., the 3GPP GRX). The further agree to accept calls from all participants in that network and bill each other via a clearinghouse.

- A set of VSPs agree to accept calls originating from within the same country. They use a set of firewall rules to block calls from abroad.

- A company sets up a SIP proxy which acts as a forwarding proxy between the SIP proxies of all participating VSPs. The group of these VSP form a federation whose technical rules state that calls have to be routed via that central proxy.

7. Acknowledgments

Many of the definitions were gleaned from detailed discussions on the SPEERMINT, ENUM, and SIPPING mailing lists. Scott Brim, Mike Hammer, Jason Livingood, Jean-Francois Mule, David Schwartz, Richard Shocky, Henry Sinnreich, Richard Stastny, and Dan Wing 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.

8. Security 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.

9. IANA Considerations

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

10. References

10.1. Normative References

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

[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.

10.2. 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.ietf-enum-infrastructure-enum-reqs] Lind, S. and P. Pfautz, "Infrastrucure ENUM Requirements", draft-ietf-enum-infrastructure-enum-reqs-00 (work in progress), March 2006.

[I-D.lendl-speermint-federations] Lendl, O., "Federations for the Domain Policy DDDS Application", draft-lendl-speermint-federations-00 (work in progress), March 2006.

[I-D.lendl-domain-policy-ddds] Lendl, O., "The Domain Policy DDDS Application",

draft-lendl-domain-policy-ddds-00 (work in progress), February 2006.

Author's Address

David Meyer

Email: dmm@1-4-5.net

Full Copyright Statement

Intellectual Property

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 currently provided by the Internet Society.