Network Working Group D. Meyer
Internet-Draft August 30, 2006
Intended status: Informational
Expires: March 3, 2007

SPEERMINT Terminology
draft-ietf-speermint-terminology-04.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 "Voice over IP Peering" (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 Session Initial Protocol (SIP [RFC3261]) 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 (SPEERMINT) 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 session interconnect context. In the case shown here, an E.164 number [ITU.E164.2005] is used as a key in an E.164 to Uniform Resource Identifier (URI) mapping (ENUM [RFC3761]) 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.

```
          E.164 number <--- Peer Discovery
                |
                | <--- ENUM lookup of NAPTR in DNS
                |
                |
                | ENUM Working Group Scope
          =====+==========================================================
                | SPEERMINT Working Group Scope
                |
          SIP URI <--- Call Addressing Data (CAD)
                |
                |
                | <--- Federation Detection, Policy
                |      Lookup, and Service Location
                |
                |
          Hostname <--- Addressing and session establishment
                |
                | SPEERMINT Working Group Scope
          =====+==========================================================
                | Out of scope for the SPEERMINT Working Group
                |
                | <--- 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 Addressing Data, or CAD, while the SPEERMINT Working Group is focused on the use of such CAD. Importantly, the CAD can be derived from ENUM (i.e., an E.164 DNS entry) or via any other mechanism available to the user. Finally, note that the term "call" is being used in the most general sense, i.e., call routing and session routing are used interchangeably.

3. General Definitions

3.1. Call Addressing Data

Call Addressing Data, or CAD, 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 [RFC2782] that resulted from the resolution of the CAD (i.e., a SIP URI).

More specifically, the CAD is the set of parameters that the outgoing border elements need to complete the call, and may include:

- A destination SIP URI

- A SIP proxy to send the INVITE to, including

  * Fully Qualified Domain Name (FQDN)

  * Port

  * Transport Protocol (UDP/TCP/TLS)

- Security Parameters, including

  * TLS certificate to use

  * TLS certificate to expect

  * TLS certificate verification setting

- Congestion Control parameters, including

  * Static settings

  * Dynamic protocol to use, if any

3.2. Call Routing

Call routing is the set of processes, rules, and CAD 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 CAD which are used to route a real-time session to its termination 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. Peer Network

For purposes of this document and the SPEERMINT and ENUM Working Groups, a peer network is defined to be the set of SIP servers and end-users (customers) that are controlled by a single administrative domain and can be reached via some IP path. That is, SPEERMINT peer networks are not interconnected only via the PSTN. Note that such a peer network may also contain end-users who are located on the PSTN, as long as they are also reachable via some IP path.

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 route calls there (although this does not mean the call will be accepted). This is very similar to sending mail to a Simple Mail Transfer Protocol (SMTP [RFC0821]) server based on the existence of a mail exchange (MX) record.

Finally, note the concept of a VSP is a subset of the possible SP types. That is, a VSP is an SP, but it is not necessary that an SP be a VSP.

3.7. Internet Telephony Service Provider

An Internet Telephony Service Provider, or ITSP, is a synonym for VSP. The terms ITSP and VSP are used interchangeably, however, this document uses the term VSP.

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' networks 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 (Session) peering refers to interconnection of two service providers for the purposes of routing real-time (or quasi-real time) secure call signaling between their respective customers using SIP methods. Such interconnection may be direct or indirect (see Section 4.3 and Section 4.4 below). Note that media streams associated with this signaling (if any) are not constrained to follow the same set of paths.

4.3. Direct Peering

Direct peering describes those cases in which two service providers interconnect without using an intervening layer 5 network. Both service providers must have a trust relationship established (for example, they may know they belong to the same federation; see Section 6 below) before opening up a secure layer 5 communication path.

4.4. Indirect Peering

Indirect, or transit, peering refers to the establishment of a secure signaling path via one (or more) referral or transit network(s). In this case it is required that a trust relationship is established between the originating service provider and the transit network on one side, and the transit network and the termination network on the other side. Both trust relationships must exist before opening up a secure (layer 5) communication path.

4.5. Assisted Peering

In this case a federation employs a central SIP proxy (which is not itself a VSP) to bridge calls between participating networks.

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 to which an E.164 number has been assigned to (or ported to). More specifically, the COR can be defined can defined as follows [I-D.ietf-enum-infrastructure-enum-reqs]:

- o If the number in question has not been ported, then the COR is the entity 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

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

- o 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 of 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 control over 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 (I-ENUM) is defined to be the use of a separate branch the .arpa tree (in particular, ie164.arpa [I-D.ietf-enum-infrastructure]) to permit service providers to exchange phone number to URI data in order to find points of interconnection. The salient property of I-ENUM is that only the COR for a particular E.164 number is permitted to provision data for that E.164 number within the I-ENUM portion of the .arpa tree.

In I-ENUM, then, only the COR may enter data in the corresponding domain. The COR may also enter CAD (i.e., a SIP URI) to allow other SPs to to route sessions to its network.

Finally, note that ENUM is not constrained to carry only data (CAD) as defined by SPEERMINT. In particular, an important class of CAD, 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 CAD 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]. Importantly, [I-D.lendl-speermint-federations] does not define federation rules or how they are communicated to the members of a federation, and does not require such rules be publicly visible.

Briefly, a federation is a group of SPs 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.

6.1. Federation Functionality

A federation may provide some or all of the following functionality:

* Common policies

  + Policy might be ad-hoc, and published in the DNS (e.g., [I-D.lendl-domain-policy-ddds], or

  + Policy might also be managed by a federation entity

* A federated ENUM root

* Address resolution mechanisms

* Session signaling (via federation policy)

* Media streams (via federation policy)

* Federation security policies

* Interconnection policies

* Other layer 2 and layer 3 policies

Finally, note that a SP can be a member of

* No federation (e.g., the SP has only bilateral peering agreements)

* A single federation

* Multiple federations

and an SP can have any combination of bi-lateral and multi-lateral (i.e., federated) interconnections.

6.2. Announcement of Federation Membership

Announcement of federation membership is typically made by the terminating SP, using one or more of the following mechanisms:

* I-ENUM

   * A Private ENUM Federation discovery mechanism

   * DNS

6.3. Example Federation Rules

Example federation rules might include the following:

- o A set of SPs 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 [ITU.X509.2000] certificate which was signed by the association's own Certificate Authority (CA).

- o A set of SPs build a layer 3 network dedicated to VoIP peering (e.g., the GPRS Roaming eXchange network, or GRX). Further, they agree to accept calls from all participants in that network and bill each other via a clearinghouse.

- o A group of VSPs agree to accept calls originating from each other. They use firewall rules to block calls from all other networks.

- o A company sets up a SIP proxy which acts as a forwarding proxy between the SIP proxies of all participating SPs (see, e.g., Section 4.5). This group of SPs forms 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, Eli Katz, Mike Hammer, Gaurav Kulshreshtha, Otmar Lendl, Jason Livingood, Alexander Mayrhofer, Jean-Francois Mule, David Schwartz, Richard Shockey, Henry Sinnreich, Richard Stastny, Dan Wing, and Adam Uzelac all made valuable contributions to early versions 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

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

[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.E164.2005] International Telecommunications Union, "The International Public Telecommunication Numbering Plan", ITU-T Recommendation E.164, 02 2005.

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

10.2. Informative References

[RFC0821] Postel, J., "Simple Mail Transfer Protocol", STD 10, RFC 821, August 1982.

[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.

[I-D.ietf-enum-infrastructure-enum-reqs]

Lind, S. and P. Pfautz, "Infrastrucure ENUM Requirements", draft-ietf-enum-infrastructure-enum-reqs-02 (work in progress), April 2006.

[I-D.lendl-speermint-federations]
Lendl, O., "A Federation based VoIP Peering Architecture", draft-lendl-speermint-federations-01 (work in progress), June 2006.

[I-D.lendl-domain-policy-ddds]
Lendl, O., "The Domain Policy DDDS Application", draft-lendl-domain-policy-ddds-01 (work in progress), June 2006.

[I-D.ietf-enum-infrastructure]
Livingood, J., "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application for Infrastructure ENUM", draft-ietf-enum-infrastructure-00 (work in progress), April 2006.

[ITU.X509.2000]
International Telecommunications Union, "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", ITU-T Recommendation X.509, ISO Standard 9594-8, March 2000.

Author's Address

David Meyer

Email: dmm@1-4-5.net

Full Copyright Statement

Intellectual Property

Acknowledgment

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