Network Working Group D. Meyer
Internet-Draft September 18, 2006
Intended status: Informational
Expires: March 22, 2007

SPEERMINT Terminology
draft-ietf-speermint-terminology-06.txt

Abstract

This document defines the terminology that is to be used in describing Session PEERing for Multimedia INTerconnect (SPEERMINT).

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 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 non-voice 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 defines the terminology describing the various forms of peering. Finally, Section 5 introduces the concept of federations.

2. SPEERMINT Context

Figure 1 depicts the general session interconnect context. Note that vertical axis in this figure describes the layering of identifiers, while the horizontal lines indicate working group scope. While the SPEERMINT working group is not limited (or coupled in any way) to the use of E.164 numbers, 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]). That URI is in turn used to retrieve a NAPTR record [RFC3404], which is in turn resolved into a SIP URI. Call routing is based on the resulting SIP URI. Note that 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 of any type. In particular, 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

Note that in Figure 1, Call Addressing Data (CAD), is the data used to route a call to the called domain's ingress point (see Section 3.3 for additional detail).

As illustrated in Figure 1, 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 in routing session signaling requests. 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 here in the most general sense, i.e., call routing and session routing are used interchangeably.

3. General Definitions

3.1. Signaling Path Border Element

A signaling path border element (SBE) provides signaling functions such as protocol inter-working (for example, H.323 to SIP), identity and topology hiding, and Call Admission Control (CAC) for a domain. Such an SBE is frequently (but need not be) deployed on a domain's border.

3.2. Data Path Border Element

A data path border element (DBE) provides media-related functions such as deep packet inspection and modification, media relay, and firewall support under SBE control. As was the case with the SBE, a DBE is frequently deployed on a domain's border.

3.3. Call Addressing Data

Call Addressing Data, or CAD, is the data used to route a call 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 SBEs 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
- Optional resource control parameters such as

* Limits on the total number of calls to a peer

* Limits on SIP transactions/second

* Limits on the total amount of bandwidth used on a peering link

* In addition, lower layer parameters (such as DSCP markings on SIP and/or media packets [RFC4594]) might also be included.

3.4. 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.

3.5. 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; various dial-plans (such as emergency services dial-plans), however, may not directly use E.164 numbers.

3.6. IP Path

For purposes of this document, an IP path is defined to be a sequence of zero or more IP router hops.

3.7. Peer Network

This document defines a peer network as the set of SIP UASs and SIP UACs (customers) that are controlled by a single administrative domain and can be reached via some IP path. Note that such a peer network may also contain end-users who are located on the PSTN (and hence may also be interconnected with the PSTN), as long as they are also reachable via some IP path.

3.8. Service Provider

A Service Provider (or SP) is defined to be an entity that provides layer 3 (IP) transport of SIP signaling and media packets.

3.9. Voice Service Provider

A Voice Service Provider (or VSP) is an entity that provides transport of SIP signaling to its customers. In the event that the

VSP is also an SP, it may also provide 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.

3.10. Internet Telephony Service Provider

An Internet Telephony Service Provider, or ITSP, is a synonym for VSP. While the terms ITSP and VSP are frequently used interchangeably, 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 4.2.1 and Section 4.2.2 below). Note that media streams associated with this signaling (if any) are not constrained to follow the same set of IP paths.

4.2.1. Direct Peering

Direct peering describes those cases in which two service providers interconnect without using an intervening layer 5 network.

4.2.2. 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 generally 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.

4.2.3. Assisted Peering

In this case, some entity (usually a federation, see Section 5) employs a central SIP proxy (which is not itself a VSP) to bridge calls between participating networks.

5. Federations

A federation is a group of VSPs which agree to receive calls from each other via SIP, and who agree on a set of administrative rules for such calls (settlement, abuse-handling, ...) and the specific rules for the technical details of the interconnection.

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. Acknowledgments

Many of the definitions were gleaned from detailed discussions on the SPEERMINT, ENUM, and SIPPING mailing lists. Scott Brim, Mike Hammer, Eli Katz, Gaurav Kulshreshtha, Otmar Lendl, Jason Livingood, Alexander Mayrhofer, Jean-Francois Mule, Jonathan Rosenberg, David Schwartz, Richard Shockey, Henry Sinnreich, Richard Stastny, Hannes Tschofenig, 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.

7. 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.

8. IANA Considerations

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

9. Informative 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.

[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.

[RFC4594] Babiarz, J., Chan, K., and F. Baker, "Configuration Guidelines for DiffServ Service Classes", RFC 4594, August 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.

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).