Network Working Group
Request for Comments: 5486
Category: Informational

D. Malas, Ed.
CableLabs
D. Meyer, Ed.

March 2009

Session Peering for Multimedia Interconnect (SPEERMINT) Terminology

Status of This Memo

Copyright Notice

Abstract

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

Table of Contents

1. Introduction 2
2. SPEERMINT Context 3
3. General Definitions 4
3.1. Signaling Path Border Element 4
3.2. Data Path Border Element 4
3.3. Session Establishment Data 4
3.4. Call Routing 5
3.5. PSTN 5
3.6. IP Path 5
3.7. Peer Network 5
3.8. Service Provider 5
3.9. SIP Service Provider 6
4. Peering 6
4.1. Layer 3 Peering 6
4.2. Layer 5 Peering 6
4.2.1. Direct Peering 7
4.2.2. Indirect Peering 7
4.2.3. On-Demand Peering 7
4.2.4. Static Peering 7
4.3. Functions 7
4.3.1. Signaling Function 7
4.3.2. Media Function 8
4.3.3. Look-Up Function 8
4.3.4. Location Routing Function 8
5. Federations 8
6. Security Considerations 9
7. Acknowledgments 9
8. Informative References 10

1. Introduction

The term "Voice over IP Peering" (VoIP Peering) has historically been used to describe a wide variety of practices pertaining to the interconnection of service provider networks and to the delivery of Session Initiation Protocol (SIP [2]) 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 describe 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 session layer, and it does not (necessarily) cover 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"). The term "peering" will be used throughout the remainder of the document for the purpose of indicating a layer 5 interconnection.

This document introduces standard terminology for use in characterizing real-time session peering. Note however, that while this document is primarily targeted at the VoIP peering case, the terminology described here is applicable to those cases in which service providers peer using SIP signaling (defined as SIP Service Providers; see Section 3.9) for non-voice or quasi-real-time communications like instant messaging.

The remainder of this document is organized as follows: Section 2 provides the general context for the Session PEERing for Multimedia INTerconnect working group (SPEERMINT). Section 3 provides the general definitions for real-time, SIP-based communication, with initial focus on the VoIP peering case, and Section 4 defines the terminology describing the various forms of peering. Finally, Section 5 introduces the concept of federations.

2. SPEERMINT Context

SPEERMINT provides a peering framework that leverages the building blocks of existing IETF-defined protocols such as SIP [2] and ENUM [4]. While the SPEERMINT working group describes the use of these protocols in peering, it does not redefine how these protocols use input or output variables necessary for creating Session Establishment Data (SED) or the methods in which this data will be used during the peering process. See Section 3.3 for additional detail on SED and its principal variables such as Uniform Resource Identifiers (URIs) [3] and telephone numbers of E.164 numbers [5]. For example, while the SPEERMINT working group is not limited to the use of telephone numbers, an E.164 number may be used as a key in an E.164-to-URI mapping using ENUM. This mapping involves looking up Naming Authority Pointer (NAPTR) records in the DNS, and results in a SIP URI. The process for deriving this information has already been defined in [4], but is used as a building block for SPEERMINT SED, on which the subsequent call routing is based. Note that the call-routing step does not depend on the presence of an E.164 number. Indeed, the URI resulting from an ENUM query may no longer even contain numbers of any type. In particular, the SIP URI can be advertised in various other ways, such as on a web page.

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) is located on the administrative border of a domain through which inter-domain session layer messages will flow. It typically provides signaling functions such as protocol inter-working (for example, H.323 to SIP), identity and topology hiding, and Session Admission Control for a domain.

3.2. Data Path Border Element

A data path border element (DBE) is located on the administrative border of a domain through which flows the media associated with an inter-domain session. It typically provides media-related functions such as deep packet inspection and modification, media relay, and firewall-traversal support. The DBE may be controlled by the SBE.

3.3. Session Establishment Data

Session Establishment Data, or SED, is the data used to route a call to the next hop associated with the called domain's ingress point. A domain's ingress point might, for example, be the location derived from various types of DNS records (NAPTR, SRV, or A record) [1] that resulted from the resolution of the SIP URI.

More specifically, the SED is the set of parameters that the outgoing SBEs need to complete the call, and may include:

- A destination SIP URI
- A SIP proxy or ingress SBE to send the INVITE to, including:
  - Fully Qualified Domain Name (FQDN)
  - Port
  - Transport Protocol (UDP [8], TCP [9], and TLS [7])
- 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 call initiations to a peer
  - Limits on SIP transactions per second

3.4. Call Routing

Call routing is the set of processes and rules used to route a call and any subsequent mid-dialog SIP requests to their proper (SIP) destination. More generally, call routing can be thought of as the set of processes and rules that 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; however, various dial-plans (such as emergency services dial-plans) may not directly use E.164 numbers.

3.6. IP Path

For the 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 user agents (UAs) (customers) that are associated with 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 (SP) is defined to be an entity that provides layer 3 (IP) transport of SIP signaling and media packets. Example services may include, but are not limited to, Ethernet Private Line (EPL), Frame Relay, and IP Virtual Private Network (VPN). An example of this may be an Internet Service Provider (ISP).

3.9. SIP Service Provider

A SIP Service Provider (SSP) is an entity that provides session services utilizing SIP signaling to its customers. In the event that the SSP is also a function of the SP, it may also provide media streams to its customers. Such an SSP may additionally be peered with other SSPs. An SSP may also interconnect with the PSTN. An SSP may also be referred to as an Internet Telephony Service Provider (ITSP). While the terms ITSP and SSP are frequently used interchangeably, this document and other subsequent SIP peering-related documents should use the term SSP. SSP more accurately depicts the use of SIP as the underlying layer 5 signaling protocol.

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 that are 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 the Border Gateway Protocol (BGP) [6] 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 peers' networks or the peer's customer's network.

4.2. Layer 5 Peering

Layer 5 (session) peering refers to interconnection of two SSPs for the purposes of routing real-time (or quasi-real-time) call signaling between their respective customers using SIP methods. Such peering 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 SSPs peer without using an intervening layer 5 network.

4.2.2. Indirect Peering

Indirect, or transit, peering refers to the establishment of either a signaling and media path or a signaling path alone via one (or more) layer 5 transit network(s). In this case, it is generally required that a trust relationship is established between the originating SSP and the transit SSP on one side, and between the transit SSP and the termination SSP on the other side.

4.2.3. On-Demand Peering

SSPs are said to peer on-demand when they are able to exchange SIP traffic without any pre-association prior to the origination of a real-time transaction (like a SIP message) between the domains. Any information that needs to be exchanged between domains in support of peering can be learned through a dynamic protocol mechanism. On-demand peering can occur as direct or indirect.

4.2.4. Static Peering

SSPs are said to peer statically when pre-association between providers is required for the initiation of any real-time transactions (like a SIP message). Static peering can occur as direct or indirect. An example of static peering is a federation. Each of the peers within the federation must first agree on a common set of rules and guidelines for peering, thus pre-associating with each other prior to initiating session requests.

4.3. Functions

The following are terms associated with the functions required for peering.

4.3.1. Signaling Function

The Signaling Function (SF) performs routing of SIP requests for establishing and maintaining calls, and to assist in the discovery or exchange of parameters to be used by the Media Function (MF). The SF is a capability of SIP processing elements such as SIP proxies, SBEs, and user agents.

4.3.2. Media Function

The Media Function (MF) performs media-related functions such as media transcoding and media security implementation between two SSPs. The MF is a capability of SIP-session-associated media end-points such as DBEs and user agents.

4.3.3. Look-Up Function

The Look-Up Function (LUF) determines for a given request the target domain to which the request should be routed. An example of an LUF is an ENUM [4] look-up or a SIP INVITE request to a SIP proxy providing redirect responses for peers.

In some cases, some entity (usually a 3rd party or federation) provides peering assistance to the originating SSP by providing this function. The assisting entity may provide information relating to direct (Section 4.2.1) or indirect (Section 4.2.2) peering as necessary.

4.3.4. Location Routing Function

The Location Routing Function (LRF) determines for the target domain of a given request the location of the SF in that domain, and optionally develops other SED required to route the request to that domain. An example of the LRF may be applied to either example in Section 4.3.3. Once the ENUM response or SIP 302 redirect is received with the destination's SIP URI, the LRF must derive the destination peer's SF from the FQDN in the domain portion of the URI.

In some cases, some entity (usually a 3rd party or federation) provides peering assistance to the originating SSP by providing this function. The assisting entity may provide information relating to direct (Section 4.2.1) or indirect (Section 4.2.2) peering as necessary.

5. Federations

A federation is a group of SSPs that agree to exchange calls with each other via SIP and who agree on a set of administrative rules for such calls (settlement, abuse-handling, etc.) and specific rules for the technical details of the peering.

The following provides examples of rules that the peers of a federation may agree to and enforce upon all participants:

- Common domain for all federation peers (e.g., bob@peer1.federation.example.com)

- Codec rules (e.g., all peers must use the ITU-T G.711 codec [10])
- Authentication preference (e.g., all peers must use TLS when requesting to establish sessions with other peers)
- Transport protocol (e.g., all peers must use TCP)
- SIP address resolution mechanisms (e.g., all peers must use ENUM for resolving telephone numbers to SIP URIs)

Finally, note that an SSP can be a member of:

- No federation (e.g., the SSP has only bilateral peering agreements)
- A single federation
- Multiple federations

Also, an SSP can have any combination of bilateral and multilateral (i.e., federated) peers.

6. Security Considerations

This document introduces no new security considerations. However, it is important to note that session peering, as described in this document, has a wide variety of security issues that should be considered in documents addressing both protocol and use-case analysis.

7. Acknowledgments

Many of the definitions were gleaned from detailed discussions on the SPEERMINT, ENUM, and SIPPING mailing lists. Scott Brim, John Elwell, 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, Adam Uzelac, and Dan Wing all made valuable contributions to early versions of this document. Patrik Faltstrom also made many insightful comments to early versions of this document.

8. Informative References

[1] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 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] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI)", RFC 3404, October 2002.

[4] Faltstrom, P. and M. Mealling, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", RFC 3761, April 2004.

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

[6] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[7] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[8] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[9] Postel, J., "DoD standard Transmission Control Protocol", RFC 761, January 1980.

[10] ITU Recommendation G.711 (11/88) - Pulse code modulation (PCM) of voice frequencies.

Authors' Addresses

Daryl Malas (editor)
CableLabs
858 Coal Creek Circle
Louisville, CO 80027
USA
EMail: d.malas@cablelabs.com

David Meyer (editor)
EMail: dmm@1-4-5.net