Routing SIP Requests with ENUM
draft-kaplan-enum-sip-routing-00

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on January 5, 2011.

Copyright and License Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the BSD License.
Abstract

A common ENUM use-case is for hop-by-hop or domain-by-domain "routing" of SIP requests, using private DNS trees and servers. This document describes this use-case and the need for a source-based query/answer mechanism for such.

Table of Contents

1. Terminology..................................................2
2. Introduction................................................2
3. Security Considerations....................................5
4. IANA Considerations........................................5
5. References..................................................5
  5.1. Normative References................................5
  5.2. Informative References................................6
Authors’ Addresses............................................6
Full Copyright Statement......................................7
Intellectual Property Statement................................7
Acknowledgment...............................................7

1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119. The terminology in this document conforms to RFC 2828, "Internet Security Glossary".

For the purposes of this document and sake of simplicity, only the ENUM/DNS NAPTR URI result for a SIP URI is discussed, but it applies to H.323 and other URIs as well.

Prefix: in this document, the term "prefix" is just some arbitrary number of the leading digits of an E.164 number, such as the country code, or country plus region, or even including the local exchange portion. It does not mean additional pre-pended digits used only for internal routing but which are not part of the called/calling number, for which the term "prefix" is also commonly used.

2. Introduction

The E.164 number to URI DDDS (ENUM) application provides a mapping from E.164-based "names" to various URIs, including SIP, H.323, and others, as defined in [RFC3761]. The reader is assumed to be familiar with ENUM and its normative documents.
The goal of this document is to describe one of the common uses of ENUM today: SIP Request Routing. SIP Routing using ENUM generally works very well, but it still missing one important capability: source-based results. This source-based routing problem is described in this document, without describing the solution. A solution has been proposed in another draft, [source-uri], which has since expired but has been implemented by multiple vendors and is in use. A forthcoming draft is expected to propose the same mechanism again.

When it was originally created, ENUM DNS entries were intended to be under the authority of the entity or person identified by the E.164 number, and be something the end user could populate. For example, for SIP the resultant URI would be the user’s global SIP Address-of-Record URI, or even a specific SIP Contact URI of the user’s SIP User-Agent host. This model is sometimes called "End User ENUM". In practice, this model has seen fairly limited deployment or use, for numerous reasons which will not be enumerated in this document.

Another model called "Infrastructure ENUM" or "Carrier ENUM", described in [RFC5526], changes the authority model of the ENUM DNS entries to make the registrant be the carrier-of-record, as opposed to the end user. In the Infrastructure ENUM model, the returned URI was intended to represent a "point of interconnection" into the carrier-of-record’s SIP domain, such as an SBE.

While there are deployments of Infrastructure ENUM, in practice it is not often deployed as originally defined. The public DNS database cannot reasonably be usable for URIs which represent specific points of interconnection or ingress, because such URIs are rarely usable in a global context; only carriers with direct access to the interconnection points can use such URIs to reach the carrier-of-record, and even then the interconnection points would be different per originating carrier.

One could use specific DNS "views" for Infrastructure ENUM, to return different answers per querying carrier IP Address range, but that is difficult to accomplish in the public DNS, in a scalable manner. A more reasonable URI to return from the public DNS database would be a globally reachable SIP Address-of-Record, but one for which the carrier-of-record is the registrant. Unfortunately, even that type of URI is difficult to use; both because many carriers do not wish to publish such data in a public database, and because in practice few Address-of-Records are actually globally, directly, and publicly reachable.

An alternative model, often called "Private ENUM", is widely deployed. Private ENUM uses the DNS Protocol, but not the public DNS Database. Instead, the database either uses a private domain...
suffix/apex reserved for this purpose and known to all participants, or is provided by local DNS servers which do not tie into the public IANA-based tree, or more commonly both privacy tactics are used. The Private ENUM DNS servers typically reside in a private or restricted IP network, and only accessible to specific clients. Such clients are typically constrained to be ones owned and managed by the carrier, such as SIP Proxies, Application Servers, PSTN Gateways, Soft-switches, and Session Border Controllers.

Unlike Infrastructure ENUM, Private ENUM DNS database entries are not registered and populated by the carrier-of-record for a given E.164 number. Instead, the private database’s administrator (the local carrier) directly provisions the entries for all E.164 numbers it cares about, based on various indirect information data sources, and sets the entry URI values relative to their specific "view".

In some cases the resolved URI still does not represent a point of interconnection, such as when it is just used for Number Portability or Calling Name resolution; in other cases it represents a specific interconnection point: either for the peering SBE(s) or tandem PSTN Gateway(s). The interconnection URI identifies either a host, or possibly also a Trunk Group. When Private ENUM is used for local interconnection point resolution for SIP requests, it is typically described as providing an "ENUM Routing" service, or as "SIP Routing using ENUM".

SIP routing based on private-ENUM resolution has been gaining ground in some large SIP operator networks. However, a need has arisen to respond with different ENUM responses based on the source originating number or domain of the SIP request. For example, it is often cheaper to route calls from local source prefix numbers to other local prefixes numbers in a given region directly, whereas out-of-region sources going to the same destination numbers of the same carrier may be cheaper or even legally required to be sent through an interexchange or transit provider, or even the PSTN. Another example is in transit and federation carriers, where calls coming from specific previous-peers need to be routed to different next-peers, for the same destination number, usually due to regulatory or billing-related reasons.

Another example is in interconnection traffic between carriers, where calls coming from a specific region need to be routed through specific routes or border elements to the terminating or next-peer, usually due to billing and commercial-related reasons. Another example is with specific destination numbers, such as premium rate numbers, where calls towards these specific destination numbers need to be routed, based on the originating region or ingress border element, to a specific destination node or a specific
border element to a next-peer, usually due to operational and capacity management issues.

Today such source-based routing with ENUM is performed through various means, which are usually cumbersome and error-prone. These mechanisms typically require the Private ENUM clients and servers to agree on a common scheme, and thus require every SIP Proxy to know and use the same proprietary scheme, which leads to interoperability problems.

A common example is where the SIP Proxies performing the lookup change the ENUM base domain name suffix based on the source E.164 number leading digits, and thus the ENUM-DNS servers have a separate zone per source prefix. Such a scheme needs to be fixed and common; for example that a 7-digit prefix length always be used for the name suffix, instead of for only specific source or destination numbers; the relevant source prefix cannot be a different length for different numbers, prefixes, or call flows.

Another example is where the ENUM server returns all possible NAPTR entries in the DNS response, with proprietary indicators in the NAPTR URIs for the client SIP Proxy to choose from, using the SIP source information it has. The problem with this approach is that the same selection algorithm needs to be supported by all clients, and the DNS response size can grow very, very large. For example, some routing tables in North America need to have entries for hundreds of North American Numbering Plan (NANP) area codes and local-exchange prefixes, for the same destination number.

3. Security Considerations

There are no specific security issues for this mechanism, beyond those already applicable to DNS and ENUM.

4. IANA Considerations

This document makes no request of IANA.

5. References

5.1. Normative References

5.2. Informative References


Authors’ Addresses

Hadriel Kaplan
Acme Packet

Email: hkaplan@acmepacket.com

Colin Pons
KPN

Email: colin.pons@kpn.com
Acknowledgment

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