Routing SIP Requests with ENUM

draft-kaplan-enum-sip-routing-04

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 April 24, 2012.

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 a mechanism for a source-based query/answer mechanism for such.

Table of Contents

1. Terminology....................................................2
2. Introduction...................................................3
   2.1. Background....................................................3
3. The Problem....................................................5
4. The Proposed Solution.........................................6
   4.1. Generating the ENUM-based DNS Query with Source URI....6
5. Source URI Details.............................................6
   5.1. Providing Trunk Group Information in Source URI....7
6. Examples.........................................................8
   6.1. Basic SIP Scenario............................................8
   6.2. Peering SIP Scenario........................................9
   6.3. Transit SIP Scenario.........................................10
   6.4. Basic PSTN Scenario.........................................11
7. Security Considerations........................................11
8. IANA Considerations............................................12
9. Acknowledgments...............................................12
10. References....................................................12
    10.1. Normative References.....................................12
    10.2. Informative References...................................12
Authors’ Addresses.............................................13
Appendix A. Why ENUM-DNS vs. Other Protocols................13
Appendix B. Alternative Solutions................................13

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 Tel-URI, and potentially other URIs as well.
Source URI: the URI encoded in the EDNS0 Option data field, as described in [draft-edns0-source-info].

ENUM Client: a SIP device or PSTN Gateway which generates a DNS query for E.164 number resolution, per [RFC3761]

ENUM Server: a DNS server which processes DNS queries for E.164 number resolution, per [RFC3761], and is deployed specifically for that purpose

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.

SSP: SIP Service Provider, as per [RFC5486].

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 is still missing one important capability: source-based queries and results, whereby the resultant routes are based on the source of the SIP requests or PSTN calls. This source-based routing problem is described in this document, as well as the solution, which has been implemented by multiple vendors and is in use.

2.1. Background

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" or "Public 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 manageable, 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 over the Internet.

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 are only accessible to specific clients. Such Private ENUM 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", because the private DNS database represents a call routing database.

3. The Problem

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. There are various reasons for this need, a non-exhaustive list of which are itemized as follows:

- 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.

- For interconnection traffic between carriers, where calls coming from a specific region or originating peer need to be routed through specific routes or border elements to the terminating or next-peer, usually due to billing and commercially-related reasons.

- For 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 towards a next-peer, usually due to operational and capacity management issues.

- For Emergency Services destination numbers, where the originating information may affect the chosen emergency center for a call.

- To provide "near-end" or "hot-potato" routing, whereby the nearest transit inter-exchange point is selected, instead of the farthest point (which is "far-end" or "cold-potato" routing).
4. The Proposed Solution

The proposed solution uses a new EDNS0 Option code, defined in [draft-edns0-source-info], to add the source SIP/PSTN URI information into the ENUM DNS query. For example, the Source URI could be based on the P-Asserted-Identity URI of the SIP request to be routed, possibly including [RFC4904] Trunk-group parameters from the received trunk group, if applicable. This Source URI info would be used by the responding DNS server to "filter" its response based on the source information as appropriate.

4.1. Generating the ENUM-based DNS Query with Source URI

When an ENUM client such as a SIP Proxy or PSTN Gateway generates an ENUM-based DNS query following this document’s mechanism, it follows [RFC3761] and transforms the target E.164 number into a reverse-number dotted-format domain name for the DNS query key. The domain-name suffix is defined by local policy, but SHOULD NOT be "e164.arpa" because this mechanism is for purely private use.

The ENUM client then appends an EDNS0 OPT pseudo-RR to the query, with the sender’s maximum UDP length it can handle, as defined in [RFC2761], as well as the EDNS0 Option-Code reserved by [draft-edns0-source-info]. Within the Option-Data field it encodes a SIP or TEL URI, based on the source information of the received SIP request or PSTN call, as defined in the next section.

If the ENUM client needs to recursively resolve the name, by issuing the DNS query multiple times to different servers, it MUST add the same Source URI to each repeated query.

5. Source URI Details

In general, the Source URI can contain whatever the administrator wishes it to, since this mechanism is defined for private use only. However, to aid in multi-vendor interoperability, this section provides guidance for reasonable default behavior. Local policy MAY override behavior defined in this section.

The Source URI for the EDNS0 Option data field conveys source originator and transit information to the ENUM Server(s), and from a logical perspective the Source URI is a brand new URI constructed by the ENUM client. In order to construct the Source URI, the client SHOULD use relevant information from the received SIP or PSTN message fields, as described next.

If the ENUM client received a SIP request which triggered the ENUM query, and the SIP request contained a P-Asserted-Identity header value that it trusts to be accurate, the Source URI SHOULD be based
on the SIP or TEL URI information in the received P-Asserted-Identity header value. If there was no P-Asserted-Identity header value in the request, or it does not trust the URI to be accurate, then the Source URI MAY be based on local policy; for example, it may be a statically defined or default URI representing the peer, or the policy may be to not use the Source URI mechanism in such a case.

If the ENUM client received a PSTN message which triggered the ENUM query, such as an IAM, the Source URI SHOULD be a TEL URI of the calling party number.

The Source URI MAY contain additional information providing routing number (RN) in an ‘rn’ parameter, and/or carrier identification code (CIC) in a ‘cic’ parameter, as defined in [RFC4694]. Note that for a SIP URI these would be user parameters, not URI parameters. Such fields would be used to identify the porting information of the originating number, or the originating carrier.

Although the most common case will be that the Source URI user name is a phone-number, it need not be the only case and ENUM servers supporting this mechanism MUST support non-phone-number cases as valid ENUM queries. In other words, it is not a DNS protocol failure to receive such a query, even though the ENUM server may not have an appropriate answer for the query given such source information, and thus return a DNS Not Found response (as it could for phone number Source URI cases that it does not have any entries for).

If the Source URI’s SIP URI user name is a phone number, or it is a TEL URI, the ENUM client MUST NOT encode any visual-separators (the tokens named visual-separator in [RFC3966]) in it. A Source URI as a SIP URI of a phone number SHOULD contain a ‘user’ URI parameter of the value ‘phone’ (i.e., a ”;user=phone”); however an ENUM server MAY treat any Source URI user portion as a phone number if it follows the syntax of a TEL URI for such.

ENUM servers supporting this mechanism MUST ignore unknown fields in the Source URI, such as unknown parameters or embedded headers.

5.1. Providing Trunk Group Information in Source URI

The Source URI MAY contain trunk group and context information, encoded as the "tgrp" and "trunk-context" parameters within the URI per [RFC4904]. Note that for a SIP URI these would be URI user parameters, not URI parameters.

By definition, trunk group names are scoped to their trunk-context, and are not global in nature. In particular, a trunk group name
used by one SSP typically has no meaning to another SSP, and since it defines a specific trunk of the SSP it is not usable by another SSP. In order for such information in a Source URI to be usable, it needs to be what the local SSP’s ENUM server can understand and have policies for. Therefore, the trunk group information SHOULD identify the PSTN trunk or direct SIP peer trunk from which the SIP/PSTN request was received, and not any trunk group information in the received SIP request. In other words, the trunk group information conveys the local SSP’s defined trunk, not what the previous carrier’s trunk name was.

Note that the previous carrier may be a transit carrier rather than the originating carrier, and thus the trunk group information conveys the transit provider not originating provider.

6. Examples

The following examples are designed to show various Source URI usage possibilities. These are not the only possibilities, however.

6.1. Basic SIP Scenario

In the following example, a SIP UA in the local SSP generates an INVITE to Proxy-1, which performs a private ENUM query using this document’s mechanism.

```
Local Domain
ssp.example.com

+--------+        +--------+
    ENUM   |        | Server |
|SIP|-->| SIP   /        +-------+
|UA |   |Proxy-1|

SIP Proxy-1 receives:
INVITE sip:+17815551212@ssp.example.com SIP/2.0
Via: SIP/2.0/UDP 192.0.10.10:5060;branch=z9hG4bK74b43
Max-Forwards: 69
To: <sip:+17815551212@ssp.example.com>
From: Jenny <sip:7818675309@ssp.example.com>;tag=9fxced76sl
Call-ID: 3848276298220188511
CSeq: 1 INVITE
Contact: <sip:jenny@192.0.1.1>
Content-Type: application/sdp
Content-Length: ...
[SDP omitted from example]
```
Although no P-Asserted-Identity header is received in the request, Proxy-1 authenticates the UA to be authorized for the identity "sip:+17818675309@ssp.example.com", and thus generates a DNS query for the domain:

2.1.2.1.5.5.5.1.8.7.1.priv-enum.ssp.example.com

with an EDNS0 OPT RR with the appropriate Option-Code for Source URI, and the Option-Data Source URI of:
sip:+17818675309@ssp.example.com;user=phone

The ENUM server looks up the query key for the domain, filters the response based on the Source URI information, and returns the appropriate NAPTR entries.

6.2. Peering SIP Scenario

In the following example, a SIP INVITE request originates in orig.example.com from a SIP UA for the destination phone number +17815551212, with a P-Asserted-Identity of "sip:+17818675309@orig.example.com", and reaches the local SSP’s Proxy-2. Proxy-2 receives the request over trunk group "tgl-orig-ssp" in context "ssp.example.com".

SIP Proxy-2 receives:
INVITE sip:+17815551212@ssp.example.com SIP/2.0
Via: SIP/2.0/UDP 192.0.10.10:5060;branch=z9hG4bK74b43
Max-Forwards: 69
To: <sip:+17815551213@ssp.example.com>
From: Jenny <sip:7818675309@orig.example.com>;tag=9fxced76sl
P-Asserted-Identity: "T. Tutone" <sip:+17818675309@orig.example.com>
Call-ID: 3848276298220188511
CSeq: 1 INVITE
Contact: sip:jenny;tgrp=s1;trunk-context=orig.example.net@192.0.1.1
Content-Type: application/sdp
Content-Length: ... [SDP omitted from example]

Proxy-2 generates a DNS query for the domain:
2.1.2.1.5.5.5.1.8.7.1.priv-enum.ssp.example.com
with an EDNS0 OPT RR with the appropriate Option-Code for Source URI, and the Option-Data Source URI of:

sip:+17818675309;tgpr=tg1-orig-ssp;
    trunk-context=ssp.example.com@orig.example.com;user=phone

Note that although the received Contact URI contains trunk group information, this is not what Proxy-2 inserts in the Source URI, since it identifies Proxy-1’s trunk info instead of Proxy-2’s.

6.3. Transit SIP Scenario

In the following example, a SIP INVITE request originates in orig.example.com from a SIP UA for the destination phone number +17815551212, with a P-Asserted-Identity of "sip:+17818675309@orig.example.com", goes through a transit carrier trans.example.net, and reaches the local SSP’s Proxy-3. Proxy-3 receives the request over trunk "tg1-strans-ssp" in context "ssp.example"com".

<table>
<thead>
<tr>
<th>Originating Domain</th>
<th>Transit Domain</th>
<th>Local Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>orig.example.com</td>
<td>trans.example.net</td>
<td>ssp.example.com</td>
</tr>
</tbody>
</table>

SIP Proxy-3 receives:
INVITE sip:+17815551212@ssp.example.com SIP/2.0
Via: SIP/2.0/UDP 192.0.10.10:5060;branch=z9hG4bK74b43
Max-Forwards: 69
To: <sip:+17815551213@ssp.example.com>
From: Jenny <sip:7818675309@orig.example.com>;tag=9fxced76sl
P-Asserted-Identity: "T. Tutone" <sip:+17818675309@orig.example.com>
Call-ID: 3848276298220188511
CSeq: 1 INVITE
Contact: sip:jenny;tgrp=s1;trunk-context=trans.example.net@192.0.1.1
Content-Type: application/sdp
Content-Length: ... [SDP omitted from example]

Proxy-3 generates a DNS query for the domain:
    2.1.2.1.5.5.1.8.7.1.priv-enum.ssp.example.com
with an EDNS0 OPT RR with the appropriate Option-Code for Source URI, and the Option-Data Source URI of:
Note that although the received Contact URI contains trunk group information, this is not what Proxy-3 inserts in the Source URI, since it identifies Proxy-2’s trunk info instead of Proxy-3’s.

6.4. Basic PSTN Scenario

In the following example, a PSTN Gateway in the local SSP receives an IAM message, and performs a private ENUM query using this document’s mechanism.

```
Local
Domain
ssp.example.com
   +--------+
   | ENUM   |
   +--------+ / | Server |
 | PSTN   / +--------+
 | Gateway / +--------+
```

PSTN Gateway receives an IAM with a Called Party Number parameter indicating the international number 17815551212, and a Calling Party Number parameter indicating the international number of 17818675309, over PSTN trunk "tg1-pri" in context "ssp.example.com".

The Gateway generates a DNS query for the domain:

```
2.1.2.1.5.5.1.8.7.1.priv-enum.ssp.example.com
```

with an EDNS0 OPT RR with the appropriate Option-Code for Source URI, and the Option-Data Source URI of:

```
tel:+17818675309;tgrp=tg1-pri;trunk-context=ssp.example.com
```

The ENUM server looks up the query key for the domain, filters the response based on the Source URI information, and returns the appropriate NAPTR entries.

7. Security Considerations

Conveying source information in DNS queries exposes the source information to eavesdropping and modification by intermediaries. Furthermore, DNS has no default authorization nor authentication mechanism for client queries, and thus any device can issue such queries, using any source information it wishes to generate. Therefore, the mechanism described in this document MUST only be used in controlled, restricted environments. It is not appropriate for the general Internet, and will not function correctly with public Internet DNS servers.
8. IANA Considerations

This document makes no request of IANA.

9. Acknowledgments

Thanks to Tom Creighton (Comcast), James Yu (Neustar), Nick Russell (Vodafone), and Timothy Dwight (Verizon) for their feedback and support. Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).

10. References

10.1. Normative References


10.2. Informative References


Appendix A. Why ENUM-DNS vs. Other Protocols

A common question raised in the IETF regarding using DNS for SIP routing is why use DNS to begin with, instead of another database query protocol or even SIP itself (through SIP redirect servers). In the authors’ opinions, the following are the major advantages of DNS which are driving the market for Private-ENUM:

1. Performance - DNS queries and responses are single-transaction, compact size, efficiently parsed, and can be used over a connectionless transport (UDP). Compared to SIP Redirect and other protocols, the performance gains can be drastic.
2. Scalability - DNS has an underlying database scalability model built into the protocol itself, and taken advantage of by ENUM’s naming scheme, which does not natively exist in other database protocols nor for SIP Redirect.
3. Resiliency - since DNS uses a single request-response transaction model and runs over UDP, it can be deployed using an anycast addressing model.
4. Interoperability - DNS is a simple, well-understood protocol with significant maturity and developer experience.
5. Time-to-market - most SIP devices and PSTN gateways already have DNS libraries, and can leverage them for ENUM use fairly quickly.

Appendix B. Alternative Solutions

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 when multiple vendors are used.
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 source North American Numbering Plan (NANP) area codes and local-exchange prefixes, for the same destination number.