Provisioning Protocol Requirements for ENUM-SIP Addressing Servers

draft-mule-peppermint-espp-requirements-01

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of 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 15, 2009.
Abstract

This document presents use cases and protocol requirements for provisioning ENUM-SIP addressing servers. The provisioned data is used by the addressing server to return session establishment data for SIP entities to route SIP requests to the target destinations. An ENUM-SIP addressing server acts as a Lookup Function in session peering to determine the target domain of a given SIP request. It may also act as a Location Routing Function to develop the location of the SIP signaling entity in the target domain.

Table of Contents

1. Introduction ............................................. 3
2. Terminology .............................................. 4
3. Motivations and Use Cases Examples ....................... 5
   3.1. Separation of Responsibility ....................... 5
   3.2. File-based Distribution and Bootstrapping .......... 7
   3.3. Backward Compatibility to Legacy Switch Translations ... 8
4. Protocol Requirements ...................................... 9
   4.1. Connection-Oriented Operation ...................... 9
   4.2. File Oriented Operation ............................. 9
   4.3. Security Requirements: Authentication, Integrity and Confidentiality ............................................. 10
   4.4. Data Model Requirements ............................. 10
   4.5. Data Presentation Requirements ...................... 11
   4.6. Protocol Operations .................................. 11
   4.7. Versioning, Capability Exchange, and Extensibility Requirements ............................................. 11
5. Security Considerations ................................... 12
6. IANA Considerations ...................................... 13
7. Acknowledgments ......................................... 14
8. References ................................................. 15
   8.1. Normative References ............................... 15
   8.2. Informative References ............................. 15
Authors’ Addresses ............................................. 17
Intellectual Property and Copyright Statements ..................... 18
1. Introduction

This document presents a set of use cases and protocol requirements for an ENUM-SIP addressing Server Provisioning Protocol (ESPP). An ENUM-SIP addressing server is a session routing server which resolves telephone numbers or any type of public user addresses into Uniform Resource Identifiers (URIs) based on various rules and routing logic. The data provisioned into an ENUM-SIP addressing server is queried by SIP entities using ENUM [RFC3761] or Session Establishment Protocol (SIP) [RFC3261]. It is intended to provide the necessary information for a querying SIP entity to route a session request to the target destination.

An ENUM-SIP addressing server is a host that acts as a Lookup Function in session peering to determine the target domain of a given SIP request. It may also act as a Location Routing Function to develop the target domain into the location of the SIP signaling entity servicing the target user.

In order to perform address resolution, the addressing server often receives configuration data from various data sources. These data sources may reside in a service provider or enterprise network (intra-office or intra-company back-office systems), or in a peer’s network in the case of bilateral session peering agreements, or in a session peering registry shared by a group of SIP Service Providers (SSPs). These data sources advertise the public user identities they serve (SIP user addresses, telephone numbers, and other types of Uniform Resource Identifiers) along with other data elements like the Signaling path Border Elements (SBEs) to use to reach those user identities.

The ENUM-SIP addressing server Provisioning Protocol (ESPP) is an example of provisioning protocol based on the requirements in this document ([I-D.espp-protocol]). It can be viewed as a provisioning protocol for the lookup and location routing functions defined in session peering.

This document is organized as follows: Section 3 presents some motivations and use cases, and Section 4 defines protocol requirements for a provisioning protocol for the lookup and location routing functions.

This document is provided as input for protocol requirement discussion in the drinks working group.
2. 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 [RFC2119].

This document also reuses the SIP terminology defined in [RFC3261]. The Lookup Function (LUF), Location Routing Functions (LRF) and other session peering terms are defined [I-D.ietf-speermint-terminology].
3. Motivations and Use Cases Examples

The main motivation for defining an open provisioning protocol for ENUM-SIP addressing servers is to allow multiple server vendors to accept provisioning data from multiple data sources (some internal to a SIP service provider, some controlled by one or more session peers) using a common and flexible data model for the data elements that may need to be provisioned.

The remaining of this section provides a couple of use cases.

3.1. Separation of Responsibility

A SIP Service Provider’s business practices may impose a separation of roles and responsibilities such that:

(a) network engineering and planning personnel are responsible for establishing points-of-interconnect (at layer 3 for IP internetworking and layer 5 for SBEs),

(b) for telephony services, telephony personnel are responsible for provisioning telephone numbers, and telephone number prefixes,

(c) other personnel or back-office application systems are responsible for provisioning other forms of resolvable user addresses (e.g., email addresses, instant messaging addresses via self-provisioned web applications, etc.).

The above separation of roles and responsibilities imply that multiple data sources may concurrently add, modify or delete data elements that often must be "combined" for an ENUM-SIP addressing server to return session establishment data.

For example, two SIP service providers agree to exchange SIP traffic by establishing a session peering relationship for voice services first, and they decide to first exchange traffic for a sub-set of their customer base; two destination groups, the New York-Manhattan and New York-Queens groups are peered. Note that the destination groups used in this example are geographical to facilitate the understanding of destination groups but in many cases, peers will establish peering relationships independent of any geographical considerations (user groups, im groups, etc.).

In unison, the network engineering personnel of each company establish physical inter-connect in the New York City 60 Hudson Street facility. Each SIP service provider commissions redundant Signaling path Border Elements that are used to secure the interconnect located at 60 Hudson Street. Then through the use of the ESPP protocol, the network engineering departments publish IP and
SIP addressing information to each other’s ENUM-SIP addressing servers – provisioning NAPTRs for each Ingress SBE and through Route objects associating them with the logical Destination Groups of each metropolitan area.

Once the Destination Groups and Routes are established, the telephony personnel manage the telephony addressing by adding telephone numbers, routing numbers or prefixes to the respective Destination Groups.

Some of the data (SBEs, Destination Groups, Routes and their respective priorities) is usually provisioned once for each SIP Service Provider with occasional subsequent updates as interconnect points are added or changed. It is provisioned independently from the provisioning of the elements contained in Destination Groups (TNs, TN Ranges, LRNs, or public identities such as IM identifiers). This allows the rare process of provisioning SBEs, destination groups, etc. to be distinctly separate from the continuous process of adding subscribers. This also applies to non-voice applications where subscribers are added independently of the underlying Layer-5 entities that service those users.

Note that the exchange of this information may be done directly between peers or via an entity representing a group of SIP service providers. Today, in some VoIP networks, this information is often exchanged in a static manner using email and spreadsheets.

Figure 1 illustrates how telephone numbers may be grouped logically into destination groups (which may not necessarily be based on geographical boundaries). It also shows how each destination group may be reachable via a domain or a list of signaling path border elements.
Destination Groups:

<table>
<thead>
<tr>
<th>Destination Group</th>
<th>TN or TN Ranges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manhattan</td>
<td>212-203-0000 -&gt; 212-203-9999</td>
</tr>
<tr>
<td>Bronx</td>
<td>347-876-1000 -&gt; 347-876-1999</td>
</tr>
<tr>
<td>Queens</td>
<td>347-354-6000 -&gt; 347-354-6999</td>
</tr>
</tbody>
</table>

Routes:

<table>
<thead>
<tr>
<th>Route Name</th>
<th>Nodes</th>
<th>Destination Group</th>
<th>( Manhattan )</th>
</tr>
</thead>
<tbody>
<tr>
<td>118th Ave</td>
<td>NYC-SBE-1</td>
<td>Manhattan/Bronx</td>
<td>--&gt;(SBE)</td>
</tr>
<tr>
<td>60 Hudson</td>
<td>NYC-SBE-2</td>
<td>Queens</td>
<td>++ '-------' ( Queens )</td>
</tr>
</tbody>
</table>

Nodes:

<table>
<thead>
<tr>
<th>Node Name</th>
<th>Host/Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>NYC-SBE-1</td>
<td>sbe-1.nyc-sp1.example.com</td>
</tr>
<tr>
<td>NYC-SBE-2</td>
<td>sbe-2.nyc-sp2.example.com</td>
</tr>
</tbody>
</table>

Figure 1: Protocol Data Elements

3.2. File-based Distribution and Bootstrapping

The process of downloading large quantities of data to an ENUM-SIP addressing server should be carried out as quickly as possible with minimum resources. It involves the generation and transfer of a bulk file between the client and server. It may be used in cases where the loading a newly commissioned ENUM-SIP addressing server or reloading an existing server data due to a complete shutdown or loss of memory has occurred.

For example, a SIP service provider has decided to opt into a federation of service providers that collectively service over one hundred million (100M) subscribers, choosing to establish session peering with every member of the federation. Once commissioned, the SIP service provider’s addressing server needs to immediately receive all 100M registered user addresses (SIP addresses, TNs, etc.). Rather than stream the 100M TNs over a network connection in real-time, the administrator of the federation registry and SIP service
provider choose to utilize the file-based distribution mechanism (as described in [I-D.espp-protocol]).

3.3.  Backward Compatibility to Legacy Switch Translations

The underlying data schema used to provision ENUM-SIP addressing servers should be backward compatible with today’s legacy VoIP server translations and PSTN. This requirement arises from the fact that some SIP service providers may wish to utilize the same number translation data employed by their SIP servers handling subscribers.

For example, a SIP service provider’s switch translation personnel, who are responsible for managing SIP to telephone number address translations, are given responsibility for managing the ENUM data. Rather than provisioning complete numbers to a peer’s addressing server some may choose to provision telephone number prefixes or routing numbers. For example, an enterprise’s branch office may wish to provision the first n number of digits it can serve. As another example, in North America, some may not wish to provision the complete 10-digit numbers but opt for the provisioning Routing Numbers (RNs) as prefixes. This decision is, in large part, due to the fact that, in some enterprise and SIP service provider networks today, the trunk selection algorithm are based on prefix (e.g. NPA-NXX in North America). The translation personnel choose to reuse prefixes rather than taking responsibility for keeping a complete set of the service provider’s numbers up to date.
4. Protocol Requirements

This section describes the high-level requirements for the ENUM-SIP server provisioning protocol.

4.1. Connection-Oriented Operation

- The protocol MUST support a file-based, bulk delivery mechanism where the Client writes one or more update requests to one or more files and the file(s) are delivered to and consumed by the Server.

- The protocol MUST also support real-time, transaction-based operations where the Client requests one operation over a reliable transport and the ESPP server processes the request upon receipt and then responds to the Client with an indication of the transaction’ status (success, warning or error).

- All Clients and Servers MUST use HTTP 1.1 as defined in [RFC2616] for the transport mechanism of real-time operations.

- All Clients and Servers SHOULD support HTTP Keep-Alive to allow long lived connections, where multiple request and response pairs are exchanged across a single network connection.

4.2. File Oriented Operation

- The protocol MUST support a file-based mechanism (bulk load) where the Client writes one or more requests to a file and the file is delivered to and consumed by the Server.

- The delivery or transmission of bulk files MAY be triggered by a manual process out-of-band of the protocol.

- During bulk loading the Server SHOULD NOT accept new records through the real-time, connection-oriented interface.

- The maximum size of a bulk load file SHOULD NOT exceed 500 MB.

- The name of a bulk file SHOULD identify the Client, Server, file sequence number, and transaction ID(s) for which the bulk file was generated.

- The bulk load interface MUST be capable of supporting the download of an entire address space of the order of the PSTN.

- The format of the bulk load file MUST be compatible with the XML definitions of the real-time interface.
The Server MUST maintain an error log that identifies transactions that resulted in an error when being applied to the database of the Server. The errors codes of the bulk load interface SHOULD comply with the error codes of the real-time interface.

4.3. Security Requirements: Authentication, Integrity and Confidentiality

- All Clients and Servers MUST support Transport Layer Security (TLS) as defined in [RFC4346] as the secure transport mechanism.
- All Clients and Servers MUST use HTTP Digest Authentication as defined in [RFC2617] as the secure authentication mechanism.
- Transfer of bulk files MUST use Secure Copy (SCP), which relies on Secure Shell (SSH) for security, as the secure file transport mechanism.

4.4. Data Model Requirements

- The provisioning protocol MUST be capable of supporting the following data elements as part of user addresses: any type of user addresses or Uniform Resource Identifiers that can be used to establish SIP sessions, and telephone number related elements (TNs, TN prefixes, TN ranges, and Routing Numbers).
- The protocol data model MUST provide means to logically group public user addresses into Destination Groups.
- The protocol data model MUST allow the data separation between public user addresses (and their logical groupings) and the domain or routes that can be used to reach those user addresses.
- The protocol data model MUST support the data elements required for the SPEERMINT Lookup Function and allow the Location Routing Function to dynamically determine the target’s SIP server outside the provisioning framework. This is the case of dynamic SIP location determination based on a domain name of the SSP and mechanisms like [RFC3263].
- The protocol data model MUST also allow the data elements required for the Location Routing Function to be provisioned within this provisioning framework.
- Because of the above requirement, the protocol MUST be capable of supporting the following data elements as part of Routes associated with Destination Groups: ingress and egress Signaling
path border elements (SBE FQDNs, SIP transport protocol and ports), priority of routes, etc.

4.5. Data Presentation Requirements

- The protocol MUST utilize SOAP 1.1 [SOAP], WSDL 1.1 [WSDL], and XML 1.0 [XML].
- The protocol MUST support efficient transportation of a large number of data model objects from the client to the server.

4.6. Protocol Operations

- The protocol MUST support the ability to add, modify, and delete the objects defined in the protocol data model.
- The protocol MUST support the ability to query for a specific instance of each type of object defined in the data model by using the object identifier.
- The protocol MUST support the ability for multiple Clients to provision objects into the same Server.
- The protocol MUST support the ability for objects created by one Client to refer to objects created by another Client.

4.7. Versioning, Capability Exchange, and Extensibility Requirements

- The protocol MUST support schema versioning such that major version changes are defined as any change that breaks backward compatibility and minor version changes are defined as any change that does not break backward compatibility.
- The protocol MUST allow, but not require, a server to expose multiple concurrent major versions and/or minor versions of the protocol concurrently.
- The protocol MUST make the major version identification of a request message detectable by schema validation and the minor version identification of a request message detectable by the application.
- The protocol MUST be extensible such that new operations and objects can be added to the protocol in a systematic manner.
5. Security Considerations

Provisioning data and other configuration information in scope of this ENUM-SIP Server Provisioning protocol include public identities, telephone number ranges, signaling path border elements and NAPTRs. This information is sensitive and its transmission in the clear and without integrity checking leaves servers exposed to eavesdropping attacks.

If the object values such as TNs, Routes, or Destination Groups are set maliciously, it may result in sessions being misrouted or an over-allocation of signaling resources in an attempt to create denial of service attacks.

An initial set of security requirements for such a provisioning protocol are defined in Section 4.3.
6. IANA Considerations

This document does not register any values in IANA registries.
7. Acknowledgments

This document is based on the work of participants in the CableLabs PacketCable ENUM Server vendor focus team and initial feedback from the Peppermint/Drinks working groups.

The authors wish to thank the following participants for their contributions and efforts:
8. References

8.1. Normative References


8.2. Informative References


[WSDL] W3C, "W3C Recommendation, Web Services Description
Authors’ Addresses

Tom Creighton
Comcast Cable Communications
One Comcast Center
Philadelphia, PA  19103
USA

Email: tom_creighton@cable.comcast.com

Jean-Francois Mule
CableLabs
858 Coal Creek Circle
Louisville, CO  80027
USA

Email: jfm@cablelabs.com
Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.