INTERNATIONAL INTERCONNECTION FORUM
FOR SERVICES OVER IP

(i3 FORUM)

(www.i3forum.org)

Workstream "Technical Aspects"

White Paper

Techniques for Carriers' Advanced Routing and Addressing Schemes

(Release 1.0) May 2010

Table of Contents

Executive Summary

As carrier voice interconnection evolves to an IP based architecture, carriers need to route the voice traffic based on the IP routable addresses rather than the direct E.164 format address (telephone number) for routing in the traditional PSTN network. Therefore, a solution is required to map the E.164 format address to an IP routable address that can be used for routing the call to its destination network in an IP environment. The destination network can be either the far-end user's service provider network or an intermediate network (carrier network) to transit the call.

An added complexity is introduced with number portability. Number portability allows a user to change its service provider while retaining the telephone number. A carrier prefers the number portability corrected data to make routing decision to effectively minimize the traffic transiting cost and increase the end-to-end quality level where possible.

The initial i3 Forum Technical Interconnection Requirements for International Voice Services document assumed route selection based on Country Code (and perhaps number block assignment within the CC) rather than the full E.164 number. It did not support definitive identification of the terminating service provider in the face of number portability, nor did it support routing decisions based on other individual number characteristics, e.g., supported services.

This document discusses what is required to enable carrier routing decisions to take into account number portability and other service/capability aspects of destination numbers. Two service categories to be supported are the International Carrier Traffic Routing based on the carrier bilateral/multilateral agreements and the Specific Service Based Routing considering the services supported by the far-end user and the underlying carrier supporting capability. Although recommendations are provided for query and provisioning interfaces for carriers to exchange and access the required information, a number of challenges in achieving an implementation are also identified.

At the initial stage of the i3 Forum routing and addressing discussion, any routing policy, i.e. the least cost routing, is left to each carrier to manage based on the information made available via the mechanisms detailed in this document. Likewise the integration of the information into each carrier's Least Cost Routing (LCR) infrastructure along with the bilateral/multilateral agreement management is an individual carrier's responsibility.

1 Scope of the Document

International carriers traditionally exchange traffic, mainly for voice calls, based on the user dialed numbers. The traffic is routed to the selected carriers by the carrier dial code breakout considering both commercial and technical arrangements. Unlike the service providers who own the end users and the telephone numbers within their networks, international carriers usually don't consider the assignment of a number to a network when making routing decisions. When an end user telephone number is ported from one service provider network to another network, international carriers traditionally don't route the traffic based on the number portability corrected address.

The i3 Forum foresees an increasing demand for the carriers to route traffic intelligently to the other carriers who have the best quality and cost structure for terminating the traffic. This requires the carrier to receive the number portability corrected data in order to make the routing decision combined with other business considerations, e.g. least cost routing, etc. There are solutions available in the market for service providers routing their peering traffic by identifying the terminating service provider network directly. In the scope of this document, the term "terminating Service Provider" is to be understood as either a service provider network providing the local service to the destination user, or an exclusive carrier network that represents the underlying service provider. However, the existing solutions may not always work for the international carrier community as the international carriers prefer to manage the routing decision within their own domains, often via the existing Interconnect Business Optimization (IBO) system to factor the cost, quality, network capacity, service capability, e.g. CLI delivery capability, into the routing decisions.

This white paper provides an overview of the carrier interconnection techniques for advanced routing and addressing schemes. It specifies the technical requirements for the provisioning and query interfaces and a set of the minimum information required in the addressing database that will allow carriers to exchange number portability corrected data. The main purpose is to set a standard for the carriers to develop their own routing and addressing solution and to promote the carriers' exchange of the number portability corrected data in order to identify the terminating network. The interface and database requirements are relatively independent of the solution architecture.

2 Objective of the Document

The objective of this document is to allow the participating carriers to exchange addressing (and routing) and service attribute information to facilitate effective and flexible bilateral/multilateral traffic exchange.

The solutions to be adopted by carriers should be able to achieve the following goals.

- Be able to share their number portability corrected data;
- Be able to provide all necessary information for each carrier to decide the routing when such information is not available by other means;
- Be able to provide the information to support service based routing, e.g. far-end user characteristics and/or applications supported, including non-voice service, e.g. SMS, MMS. FAX etc.
- Be able to provide a smooth evolution path for the participating carriers with forward looking considerations;
    - The solution architecture should be flexible, scalable and evolvable;
    - Be able to inter-work or incorporate with other industry carrier federations/consortiums;
    - Start with focus on E.164 addressing, but evolvable to accommodate Non E.164 addressing.

The initial document focuses on the provisioning and the query interface requirements. Further research and analysis is required on the data exchange architecture, which subsequently will determine the detailed interface requirements to each participating carrier.

3 Acronyms

AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
CC	Country Code
CIC	Carrier Identification Code
CLI	Calling Line Identification
CPU	Central Processing Unit
DNS	Domain Name System
DRINKS	Data for Reachability of Inter/tra-NetworK SIP
ENUM	E.164 Number Mapping
EPP	Extensible Provisioning Protocol
ESPP	ENUM Server Provisioning Protocol
FAX	Facsimile
FTPS	File Transfer Protocol over SSL
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
IBO	Interconnect Business Optimization
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IFAX	Facsimile Using Internet Mail
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISP	Internet Service Provider
ITU	International Telecommunications Union
LCR	Least Cost Routing
MMS	Multimedia Messaging Service
NAPTR	Naming Authority Pointer
NDC	National Destination Code
NECA	National Exchange Carrier Association
NNI	Network to Network Interface
NP	Number Portability
NPDB	Number Portability Database
NPDI	Number Portability Dip Indicator
OCN	Operating Company Number
OID	Object Identifier
P-FTP	Passive File Transfer Protocol
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RN	Routing Number
SCP	Secure Copy Protocol
SCSCF	Serving Call Session Control Function
SCTP	Stream Control Transmission Protocol
SFTP	SSH File Transfer Protocol
SMS	Short Message Service
SPID	Service Provider Identification
SPN	Service Provider Number
SS7	Signalling System 7
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TN	Telephone Number
URI	Uniform Resource Identifier
VPN	Virtual Private Network
XMPP	Extensible Messaging and Presence Protocol

4 References

[1] i3 Forum Workstream "Services" – Routing and Addressing Services for International Interconnections over IP (V 1) May 2010

[2] IETF RFC 5526 The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application for Infrastructure ENUM – April 2009

[3] IETF RFC 3761 The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM) – April 2004

[4] GSMA PRD IR.67 - DNS/ENUM Guidelines for Service Providers & GRX/IPX Providers – April 2007

[5] IETF RFC 4769 IANA Registration for an Enumservice Containing Public Switched Telephone Network (PSTN) Signaling Information – November 2006

[6] IETF RFC 3261 SIP: Session Initiation Protocol – June 2002

[7] IETF RFC 4694 Number Portability Parameters for the "tel" URI – Oct 2006

[8] IETF Internet Draft E.164 to MetaData (E2MD) Dynamic Delegation Discovery System (DDDS) Application (draft-hoeneisen-e164-to-metadata-02) – February 2010

[9] IETF RFC 3730-3735 Extensible Provisioning Protocol (EPP) Guidelines – March 2004

[10] IETF RFC 4114 E.164 Number Mapping for Extensible Provisioning Protocol (EPP) – June 2005

[11] PacketCable ENUM Server Provisioning Protocols (ESPP) CableLabs PKT-SP-ENUM-PROV-I03-090630

[12] ITU Recommendation M.1400 - Designations for interconnections among operators' networks

[13] IETF RFC 2578 Structure of Management Information Version 2 – April 1999

[14] IETF RFC 3588 Diameter Base Protocol – September 2003

[15] IETF RFC 4740 Diameter Session Initiation Protocol (SIP) Application – November 2006

[16] IETF RFC 4904 Representing Trunk Groups in tel/sip Uniform Resource Identifiers (URIs) – June 2007

5 Supported Services

The purpose of this document is to define the query and provisioning interfaces as well as the general solution requirement for carriers to exchange the addressing and the service attribute information to support the following two service categories:

- International carrier traffic routing

The received addressing information from other carriers will allow a carrier to route the traffic to its international bilateral/multilateral carrier of choice and avoid expensive charges and quality degradation from the extra transiting hops. Many Mobile Network Operators and Cable Network Operators have already established the peering relationships within the network operator community. However, there are some additional requirements from the carrier perspective to support the carrier bilateral/multilateral traffic exchange and essentially move from country-to-country to carrier-to-carrier routing. One of the requirements is for carriers to manage the final routing decision based on other business considerations, i.e. least cost routing, bilateral overage traffic cost etc. Other requirements involve quality considerations driven by the far-end user service attributes and the underlying carrier capability.

- Service based routing

Specific service based routing will allow a carrier to make the routing decision based on the services supported by the far-end user and the underlying carrier service supporting capability. For instance, a carrier could choose another carrier A as its default interconnect provider but carrier B for some specific service types, e.g. FAX/IFAX.

At the initial stage of the i3 Forum routing and addressing discussion, the focus is for the carrier to obtain the number portability corrected data based on E.164 address to support routing in the IP environment. The actual routing policy, e.g. the least cost routing, the specific service based routing, is left to each carrier to manage. This offers a simple solution for participating carriers to benefit before a full set of the services, e.g. the routing policy management gets supported.

5.1 Information Elements to be Exchanged

The document [1] by i3 Forum Services Workstream covers the routing and addressing market requirements from the carrier community's perspective.

Based on the requirements identified by the i3 Services Workstream, two types of information about E.164 numbers are desired to enhance carriers' routing decisions are:

- Terminating service provider identity. The information to identify the terminating service providers network, e.g. a unique service provider ID (SP ID) or a domain name in the SIP URI that contains the network identity;
- Services and capabilities associated with a number.

The information provided is the input to carriers' routing decisions; routing decisions remain with each carrier. Thus, what is desired are information elements to be input to carriers Least Cost Routing mechanism rather than URIs to be directly utilized by carrier's call control elements to initiate a SIP INVITE. Each carrier's least cost routing mechanism provides the mapping from a terminating service provider identity to a carrier or a group of carriers for routing.

5.2 Information Sources

5.2.1 Terminating Service Provider Identity

There are four sources that can potentially provide the terminating service provider identity to a given E.164 number.

- Carriers who have the knowledge of their represented service provider E.164 number database; These carriers may benefit the most from this solution and are more likely to provide this address data than other potential sources;
- Service providers who own the end user and their E.164 numbers; It might be a challenge finding incentives for these service providers to supply their E.164 numbers as they may not directly benefit from the carrier solution;
- National or regional number registries and Number Portability Databases (NPDB);
- Other existing industry carrier federations/consortiums address databases.

Authoritative SP ID information is in some, but not all cases available from national number registries and number portability databases where they exist, e.g. in the USA and Canada. These sources may not provide information about the entity maintaining the retail relationship with the end users.

Carrier or service provider sourced SP ID information cannot be regarded as authoritative unless verified again authoritative sources. Without the authoritative verification, the SP ID can still be used, at the carrier's discretion, for the carriers who have the bilateral/multilateral routing relationship.

As of today, there is no global standard for SP ID. Therefore, Number portability databases cannot provide a standard SP ID. They may provide a national SP ID or a routing number (rn) and may continue to do so even after a world-wide SP ID is standardized. Deriving a global SP ID, may require a mapping table in a registry and, in the rn case requires a further translation. Mapping could also be done by the querying carrier, although that would require each carrier to develop mappings for each country.

In nations that allow number portability but do not implement a central number portability database there may be no direct authoritative source for SP ID. Existing number plan information may identify the provider that originally served a ported number but only that entity may be able to identify the current service provider.

5.2.2 Services & Capabilities

Service and capability information, on the other hand, is generally not available in national number portability databases but is only known to the serving providers.

When the terminating service providers are represented by an exclusive carrier, the carrier may provide the service and capability information.

6 Routing and Addressing Data Exchange Architectures

6.1 Call Model

Before considering candidate architectures for the exchange of routing and addressing data, it is useful to consider how such data will be employed in the route selection process during session setup. A call control element (such as an SCSCF) presumably queries some server to determine a route. The routable URI returned reflects the outcome of an LCR decision. The

data discussed in this document (SP ID, Services/Capabilities) are inputs to the LCR decision. Carriers (or their LCR vendors) need to carefully consider how to most efficiently structure information flow. For example, should the registries (or local copies or data stores) envisioned in this document be queried by the call control element or by the routing server? In the former case, the call control element will have to pass the info to the routing server for processing. Alternatively, the routing server could perform the query in response to the request from the call control element. This would also allow the query to be bypassed in cases where the server does not need additional information to make a decision (e.g., the carrier has only one route to a particular country or NDC.)

6.2 Architecture Types

Exchange of routing and addressing data may take place bilaterally between carriers or mediated by a shared registry. While certain exchanges might take place bilaterally, they can become complex as the number of carriers involved increases. Thus at the international level, carriers are and will continue to make use of shared addressing registries, mostly supported by third party registry service providers.

- It has been recognized that a variety of IP routing and addressing architectures could exist in the industry.
    - Public
    - Private
    - Fully meshed
    - Centralized
    - Distributed

The final architecture selection is driven by the business model and its requirements. However, it will support the following functions as the minimal requirements:

- Data sharing based on bilateral/multilateral agreement and defined authorization policy;
- Automatic data replication among authorized carriers with bilateral/multilateral agreement;
- Near-real time data update for data to be number portability corrected;
    - Each carrier is responsible for providing and updating the addressing data that the carrier represents;
    - Data is directly or indirectly synchronized with each country's national, regional or carrier based Number Portability Database (NPDB) to prevent false ownership declaration.
- Interoperability with other industry carrier federations/consortiums.

6.3 Public vs. Private Architectures

In this document, public registries are those sanctioned by some authority such as the ITU-T. Private registries are those operated by a commercial party or parties. (Note: A public registry implementation of a carrier ENUM, e.g., as in RFC 5526 [2], where the service provider controls registrations for a number is different from End User ENUM as contemplated in RFC 3761 [3] where the telephone number assignee controls registration.) It is presumed that initially private registries will be used to meet the needs outlined in this document.

6.4 Fully Meshed vs. Centralized vs. Distributed Architectures

A fully meshed architecture is one in which each carrier exchanges routing and addressing data directly with each other carrier on a bilateral basis. While such architectures are feasible for a small number of carriers, they are not effectively scalable. Therefore, where needed, it is expected that addressing & routing registries will be employed.

Such registries are managed by third parties. They may be either centralized or distributed. In the centralized case all data is contained in a single registry while in the distributed case, the data is distributed across multiple databases. For example, in an ENUM implementation, the routing data for all numbers could be held in one central registry or different portions (segmented by Country Code and/or by serving service provider) could be held in multiple databases with pointer from a top level registry indicating where to find data for a specific E.164 number. The GSMA PathFinder registry discussed below provides examples of both concepts.

6.5 Industry Existing Architecture - GSMA

There are vendor specific routing and addressing solutions available in the market as well as some solutions proposed by the industry service operator associations. One of the existing architectures proposed by GSMA is an implementation of Carrier ENUM as detailed in GSMA document IR.67 [4].

The GSMA defines one tree, where the root is identified by the domain e164enum.net with a flexible tiered structure below it. Below the root (tier-0) is a tier-1 level, which is at a country level. As an example, a UK tier-1 would be responsible for the sub-domain 4.4.e164enum.net (UK = +44 prefix). Number portability is also managed at the tier-1 level. Below the tier-1 level is the retail operator level at tier-2 level. Tier-2s are responsible for providing the NAPTR records.

Tier 0 – Global level (e.g. Root DNS server)
- Authoritative for the top level domain ("e164enum.net");
- Under this domain are pointers to the Tier 1 authoritative servers.

Tier 1 – Country level (CC)
- Authoritative for country code (e.g. "4.4.e164enum.net" for country code +44);
- Under this domain are pointers to the Tier 2 authoritative servers (portability corrected).

Tier 2 – Operator level (NDC)
- Provide NAPTR records;
- Under this domain are the individual Subscriber Numbers each with one or more NAPTR records.

The GSMA proposal recognizes that the tier structure will vary on a national basis. For example, where number portability has been implemented carriers may no longer be authoritative for an NDC and the Tier 1 may contain delegations for individual subscriber numbers. Alternatively, some providers may wish to provision their NAPTR records onto a common server, resulting in a combined Tier 1 and 2.

7 Query Interface

The query interface is for carriers to obtain Service Providers' identities and service capabilities information. Such information can be acquired from a shared registry or via a carrier-to-carrier bilateral relationship.

7.1 Existing Alternatives

Four candidate query protocols have been identified:

- ENUM/DNS (RFC 3761 [3] & 4769 [5])
- SIP Redirect (RFC 3261 [6] & 4694 [7])
- SS7 MAP/TCAP
- DIAMETER

The following table provides an overview of benefits and limitations within each protocol:

Query Interface Options	Pros	Cons
ENUM	Light weight, Service Agnostic, Re-use of existing DNS infrastructure; captures service information	Limited information contained in the query; ENUM is currently focused on delivering URIs. Use of TXT records or enhancements in progress may be required if carrier network elements and IBO systems cannot make use of URIs for LCR
SIP Redirect	Has more place holders for call information in the request	Call processing intensive, cannot effectively convey service information
SS7 MAP/TCAP	Allows service available to legacy TDM switches with MAP/TCAP support. As a result, this protocol support in the soft switch is widely available	Heavy weight protocol; call processing intensive
DIAMETER	used within IMS based networks, suitable for database related services; light weight; service agnostic; extendable; could be long term preference to support	Lack of industry standard as it is not widely deployed in the intended use for IP routing and addressing

Note: It is recognized that SIP is not a query protocol, although in this document it is used as a query resolution mechanism.

7.2 Recommended Query Interface Protocols

It is recommended either ENUM or SIP Redirect be the protocol of the query interface. SS7 and DIAMETER will not be discussed further within this document. Carriers can choose to implement SS7 and/or DIAMETER for routing and addressing within their networks at their discretion.

Carriers with local address resolvers can define their own query interface; Carriers who do not have local address resolvers query an external addressing registry database; countries that disallow local replication of the number portability data require the carrier query the national registry.

The IETF is considering formation of an E2MD Working Group to work on proposals for using the Domain Name System (DNS) to resolve E.164 numbers into metadata (E2MD) to provide information about E.164 numbers in cases where E.164 Number to URI Mapping (ENUM) can not be used [8]. Such proposal, when it becomes mature and widely supported by the industry will be further looked into as i3 future work.

7.2.1 ENUM Query Protocol

It's recommended ENUM be one of the supported query protocols. An ENUM query returns portability corrected information (including PSTN number portability parameters) and can convey service information via the *enumservice* field as detailed below and in the section 10 of this document.

ENUM Query and Response

The ENUM query interface supports a standard DNS query as defined in RFC 3761 [3]. An ENUM query returns a NAPTR (Naming Authority Pointer) record. ENUM is inherently number portability corrected, meaning that the records returned reflect the current service provider of record.

Information on the current service provider for a PSTN number may be reflected in at least three ways:

- A NAPTR record may resolve to a SIP URI that identifies the service provider's ingress point, e.g., in the hostname, for example

```
$ORIGIN 3.2.1.0.5.5.5.5.1.2.1.e164.arpa. NAPTR 10 100 "u" "E2U+pstn:sip"
        "!^.*$!sip:+12155550123@gw.serviceprovider1.com;user=phone!".
```

- A NAPTR record may resolve to a tel URI that includes number portability information per RFC 4769

```
$ORIGIN 3.2.1.0.5.5.5.5.1.2.1.e164.arpa. NAPTR 10 100 "u" "E2U+pstn:tel"
        "!^.*$!tel:+12155550123;npdi;rn=2155550199!"
```

- As discussed below, ENUM queries may eventually return an SP ID that directly identifies the terminating service provider without providing any routing information.

The NAPTRs for pstn service will contain either tel URI or sip URI.

ENUM is focused on returning URIs via NAPTR records. This may complicate the task of the carrier's LCR platform in extracting the service provider and service/capability information it needs for routing. On the other hand, nothing prevents an ENUM query from returning TXT records that could contain arbitrary information to be defined by the i3 to support its needs.

Presentation of Number Portability

An ENUM query response that returns the number portability (NP) information does so by populating multiple parameters as detailed in RFC 4769 [5]. The carrier that receives the query response can route the call based on the NP information. The NP parameters are Routing Number (rn), rn-context, Number Portability Dip Indicator (npdi), cic, cic-context and Service Provider Identifier (SP ID). Another option is to use SIP URI to capture the routing information in the domain name.

Considering the i3's position to promote the inter-carrier bilateral/multilateral traffic exchange, the SP ID is recommended to present the number portability corrected address data. Unlike a service provider peering agreement where the parties simply exchange each other's organic traffic, the carrier bilateral/multilateral agreement has other factors to consider:

1. A carrier bilateral/multilateral agreement assumes a commercial value, often rate per minute or rate per message to the traffic being exchanged. The imbalance traffic is usually given a higher overage rate that could result in the carrier choosing to route the imbalance traffic through other hubbing agreements.
2. A carrier can claim its representation of any service providers based on the cost structure, i.e. via a service provider peering agreement. In such situations, the traffic originating carrier requires the flexibility to route the traffic outside of the bilateral/multilateral agreement as needed.

At the current stage of the analysis, the carrier will manage the routing within its own network based on the addressing information received from the query response. The service provider information for any given E.164 address is sufficient for the carrier to make the routing decision based on various bilateral/multilateral and hubbing agreements, which often is managed via the carrier owned Interconnect Business Optimization (IBO) system. The IBO system usually factors the vendor dial code breakouts, underlying carrier cost, quality and service capability as well as network capacity into the routing decisions. The carriers would encourage the IBO system vendors or the carrier's own developers to enhance the IBO solutions to accommodate the advanced routing and addressing requirements outlined in this document towards a fully integrated solution for the carriers in the near future.

Please note that the rn and SP ID are not world-wide industry standard and require some customization before they can be used.

7.2.2 SIP Re-direct Query Protocol

It is recommended SIP Redirect be one of the supported query protocols beside ENUM.

The response to the SIP INVITE serving as a query returns the URI information containing the number portability corrected address data. Upon receiving the data, the originating carrier identifies the proper routing information based on the address and sends another SIP INVITE to complete the call routing. The SIP Re-direct query interface complies with the RFC 3261 [6].

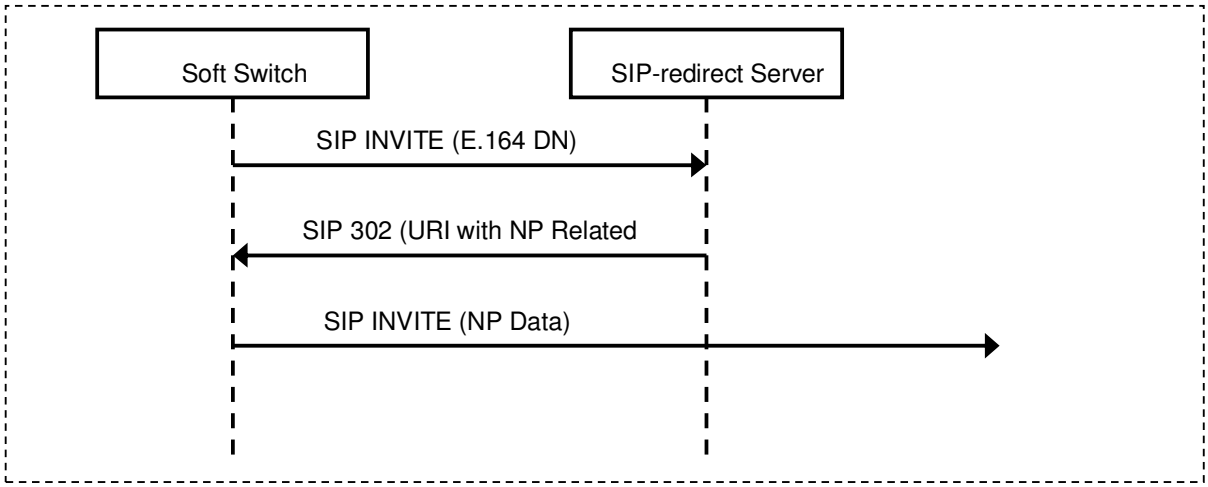

Figure 1 SIP Redirect Call Flow

Unlike the ENUM query, SIP redirect lacks of the support of multiple service types of the terminating device but it provides an alternative option when ENUM is not an option to the carrier. This happens in the situation where the carrier uses a soft switch lacking ENUM capability to query the number portability information.

As per the signalling flow shown in Figure 1, a SIP INVITE returns a redirect response including a URI with number portability related information. RFC 4694 – Number Portability Parameters for the "tel" URI - defines how tel URI contains the number portability related information [7]. It recommends use of routing number (rn) combined with the npdi parameter in the tel URI to carry the number portability information, or carrier identification code (cic) to carry the long-distance carrier information. Both rn and cic are not ideal parameters to carry the service provider identity information which is the preference for carrier communities to contain the number portability data.

Protocol customization is required to contain the service provider identity into the redirect response with sip URI or tel URI as the input to the carrier routing decision. Challenges arise not only from the protocol customization to support SP ID but also from the capability of the soft switch, which is likely the entity that initiates the SIP INVITE, to route based on SP ID. Alternatively, the service provider identity can be integrated into the dialed number as the digit prefix in the redirect response. Prefix based routing is generally supported by a soft switch translations scheme but it adds the complexity to the switch dial code management and might not be scalable depending on the deployed soft switches capability. Also, this adds a requirement that the SP ID must be in numeric format.

In addition, when the redirect response is received by the soft switch, it requires the capability to re-translate based on the additional information received in the response to apply further routing considerations, e.g. least cost routing. SIP redirect could create billing issues by way of multiple CDR generations within the switch due to multiple SIP INVITEs.

Therefore, SIP redirect is recommended as a query protocol only when ENUM query protocol is not supported. The same considerations with respect to the number portability presentation as per the discussion in section 7.2.1, apply to SIP Redirect.

7.3 Transport and IP Security for Query Interface

Three transport options have been identified to provide IP connectivity for the query interface. The following discusses each of these three options:

- Private Line
  A dedicated transport link will be deployed between carrier and the addressing database. The link provides:
  - IP connectivity for Query interface;
  - A dedicated physical link to prevent any potential security risk from other networks;
  - Guaranteed bandwidth to offer good QoS control for Query traffic.

  However this option also has some limitations:
  - Scalability issue for building private line to each individual carrier requiring query access to the addressing registry database;
  - High cost for implementing and maintaining those links.

- VPN over Shared Facility
  This option takes advantage of a Virtual Private Network (VPN) service from third party provider to offer IP connectivity for Query Interface.
  - Traffic in the virtual network is tunneled through the underlying transport network (Layer3, Layer2, IPSec etc.)
    - The proposed solution is to transfer query information on a multipoint-to-multipoint environment;
    - This makes the addressing database query available for all carriers who join the VPN;
    - It reduces the complexity of having dedicated VPN for each carrier.

  Although the nature of VPN makes most security threats from public network impossible, some additional security measurements are still required in a multipoint-to-multipoint environment:

        - A security device, e.g. stateful firewall etc., should be deployed in front of the addressing database server farm to protect the system from potential security threats from other operators;
        - Each individual operator may also want to deploy their own security device based on internal security policies to prevent the VPN gaining access to its entire corporate network.
    - End to end QoS policy is available for query traffic;
    - VPN service is generally available internationally from various VPN providers;
    - Easy to manage and maintain a single network to handle all query traffic.

The limitations of this option are:

- VPN service from one provider might not be available at certain International locations;
- To maintain a consistent end to end QoS policy might prove challenging for the multiple VPN providers required to cover all locations. The multiple VPN providers will have multiple NNIs among them to limit end to end QoS policy.

- Public Internet
  This option utilizes the Public Internet to provide IP connectivity for Query Interface. It has following benefits:
    - Addressing database could be accessible from most of area in the world;
    - Most carriers would have a reliable internet access in place based on the IP peering links with many other carriers from the ISP perspective;
    - The lowest cost solution to offer IP connectivity for Query interface.

  The concerns for this option are:
    - Both carrier and addressing database infrastructure are exposed under all security attacks on the public Internet;
    - QoS is not available on the public Internet;
    - Security mechanisms have to be in place to protect both carrier and addressing database infrastructure and the transactions between them:
        - Stateful Firewall / ACL (Access Control List) to only allow particular hosts and applications to communicate each other;
        - IPS/IDS (Intrusion Prevention System and Intrusion Detection System) to prevent any security threats on Public Internet;
        - Encryption (TLS – SSL, IPSec, Kerberos etc.) to protect the confidentiality of messages.

8 Provisioning Interface

Provisioning/replication interfaces are required for carriers to update the addressing data into the addressing registry database as well as for carriers to download the authorized addressing data to the local resolver, when such registry database exists.

The defined addressing Data Replication interface/protocol should support both incremental replication and bulk replication.

The defined addressing Data Replication interface/protocol also needs to support the additional reference interfaces to connect other carrier federations/consortium registry service providers and the selected country national or regional based number portability databases, when required. The other carrier federations/consortium registry service providers, e.g. GSMA etc. could provide the extra address data coverage if such data is required but not available from the participating carriers. The national or regional based number portability database access offers not only an authoritative source to verify the carrier provided E.164 number owner of record, but also an

alternative data source to gain the full E.164 numbers of a nation or region covered by the number portability database.

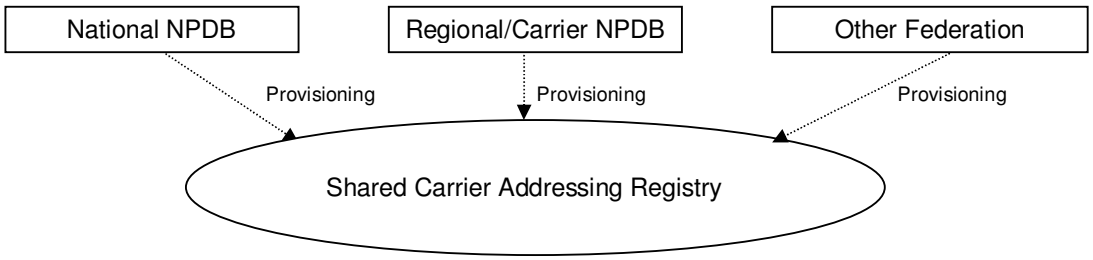

Figure 2 Addressing Data Provisioning Sources

The query objective is to obtain address data, i.e. SP ID and service/capability information. Routing decisions should be managed by the originating carrier based on the address data and on any other available information, e.g. using Least Cost Routing data.

8.1 Interface Requirements

Provisioning interface requirements consist of both interface requirements and database requirements.

Interface Requirements

- Support a file-based data transfer mechanism;
- Support both incremental updates (real time, connection oriented) and bulk update (trigger from manual process);
- During bulk updates the server should not accept incremental updates from the same source (client ID);
- Authentication, integrity and confidentiality;
- Support efficient transportation of a large number of data model objects;
- Ability to add, modify and delete the objects defined in the data model;
- Data storage and transfer optimization, simplify the distribution of redundant information or records, i.e. TN to SP ID mapping, support block of TN's transfer;
- Support uploading and downloading policy control to allow or disallow a carrier to download another carrier addressing data and/or to query the data.

Database Requirements

- Support a large addressing space – same magnitude as the PSTN (registry requirement);
- Data uploading and downloading policy control as well as the query authorization information are linked to the source of the address information;
- Alert object data conflicts received from multiple clients;
- Support multiple uploading streams into same server from different sources simultaneously;
- Data storage and transfer optimization, simplify the distribution of redundant information or records, i.e. TN to SP ID mapping, support block of TNs storage;
- Manage conflicting uploading streams into the registry from different sources simultaneously.

Potential Provisioning Interfaces

The provisioning interface may depend upon the query interface chosen. For servers using the ENUM query interface, there are some candidates available in addition to vendor proprietary interfaces:

- Extensible Provisioning Protocol (EPP) as defined in RFCs 3730-3735 [9] and RFC 4114 [10].
- ENUM Server Provisioning Protocol (ESPP) defined by CableLabs PKT-SP-ENUM-PROV-I03-090630 [11].
- The IETF drinks (Data for Reachability of Inter/tra-NetworK SIP) working group is currently pursuing specification of a protocol for such provisioning.

The i3 Forum will need to track ongoing developments before specifying a protocol.

The servers supporting the SIP redirect query interface can leverage the similar provisioning interface requirements because the information to be stored in the address database is the same with the ENUM server. The carrier who does not support ENUM might not be able to support the provisioning interface specifically designed for the ENUM server. In this situation, the carrier can choose to be a query user only without supporting the provisioning interface and contributing the address data.

8.2 Transport and IP Security for Provisioning Interface

The IP connectivity requirements for Provisioning are similar with the query interface requirements. It also has three transport options – Private Line, VPN over Shared Facility and Public Internet which have been discussed in the previous sections. The proposed approach is to share the same IP infrastructure for both Provisioning and Query interfaces.

In addition, the data replication function of the Provisioning interface requires a mechanism to pass the bulk data in a fast and secure method. The following protocols, as examples, can be implemented for file transfer with the security consideration:

- Secure Copy Protocol (SCP);
- Passive File Transfer Protocol (P-FTP);
- SSH File Transfer Protocol (SFTP);
- File Transfer Protocol over SSL (FTPS).

9 Service Provider Identity

A service provider ID schema needs to be standardized as part of the solution. There are some recommendations available from the registry service providers and other addressing and routing data consortiums. The i3 Forum could either follow an existing recommendation or propose its own standard.

Some factors to be considered in selecting an ID schema include:

- Since the i3 service requirements have tentatively indicated a desire to be able to use SP ID in carrier routing logic, careful consideration of the constraints this need imposes is required.
- Some linkage with number portability is required for SP ID to be authoritative (at least the data must be portability corrected) but NP schema and corresponding SP ID formats vary on a national basis.
- The party that would administer the schema may be a consideration. Vendor proprietary schemes are, all things being equal, less desirable than industry controlled ones.
- Some have argued that SP ID schemas need to be linked to authentication. While this does not yet appear to apply to the use cases so far defined, clarity on this point would be useful as well.

GSMA:

For GSM mobile networks the host name in the URI contains the 3-digit mobile network code and the 3-digit mobile country code followed by “3gppnetwork.org” "!^.*$!sip:+447802345678@mnc001.mcc234.3gppnetwork.org!". For operators without assigned E.212 numbering resources such as fixed network operators GSMA IR.67 recommends use of a domain name assigned in the Internet to the operator [4] in place of the mnc-mcc string, i.e., <Internet_assigned_domain_name>.3gppnetwork.org.

ITU Recommandation M.1400M Carrier Codes:

Recommendation M.1400 [12] is “Designations for interconnections among operators’ networks,” and part of it defines codes for identifying network operators. These codes are 6-character alphanumeric identifiers of operators recognized by their ITU Member State’s Administration. In the North America, NECA assigns these as OCNs. A complicating factor is that a single carrier may have multiple ITU carrier codes as shown, for example, on the NECA web site. Thus, a process to identify the single code per carrier may be needed if a single identifier per carrier is required. The i3 Forum also needs to carefully consider whether all the entities it might wish to identify are eligible for ITU carrier codes under their national regulatory structures.

Enterprise OID:

Object Identifiers (OIDs) are a hierarchical scheme standardized in ITU-T X.660 and ISO/IEC 9835 and used in ISO standards, ITU Recommendations, and IETF RFCs. IANA Enterprise Numbers as defined in RFC 2578 [13] are the specific instantiation of OID that would be appropriate.

ITU Study Group 2 Effort
In response to a contribution from NeuStar, SG2 has chartered a correspondence group to examine the issue of a standardized Service Provider Identifier or SP ID. The correspondence group is still awaiting inputs, and SG2 does not meet again until November 2010, no decision on a standard could take place before then.

Vendor specific carrier IDs

As noted, vendors might define their own proprietary code set as some already have. Each vendor will perform the carrier ID normalization if it needs to inter-work with other federations/consortium registry service providers.

Number Portability Databases

As noted, some national number portability implementations include an SP ID parameter. It is not clear that such IDs will be universally consistent.

Recommendation

At this point, either ITU carrier codes or IANA Enterprise Numbers appear to be the most appropriate resource. i3 members should consider the impact of these alternatives in their own infrastructures.

10 Information to be stored in IP routing directory

The data model objects should include:

- Public Identity: TN or TN range
- Service Provider Identity
  - SP ID is suggested
  - Alternatively, the number portability parameter rn (routing number), from RFC 4769 where an appropriate national standard has been defined [5].
- For shared databases, Source Identity: Carrier or federation ID to show the data source, this could be a carrier identification or a carrier federations/consortium ID. This source identity information is required to trace any data in the registry to its original source. When a data conflict occurs, e.g. two sources provide different SP IDs on a same E.164 number, the source of data can be identified to manage the conflict.
- End user service objects: far-end user characteristics and/or applications supported. For ENUM a set of the *enumservice* registrations triggering different URI schemes has been defined (http://www.iana.org/assignments/enum-services) as per the below table. The service types can be identified and returned to the originating carrier upon ENUM query. Such information is optional for the originating carrier to use during the routing decision making.

Service	URI Scheme	Related RFC
H323	h323	RFC3762
SIP	sip or sips	RFC3764
IFAX	mailto	RFC4143
PRES	Pres	RFC3953
WEB	http or https	RFC4002
FT	ftp	RFC4002
EMAIL	mailto	RFC4355
FAX	Tel	RFC4355
SMS	Tel	RFC4355
EMS	Tel	RFC4355
MMS	tel, mailto	RFC4355
E.164 to VPIM	mailto	RFC4238
E.164 to VPIM LDAP	mailto	RFC4238
VOICE	Tel	RFC4415
PSTN	Tel	RFC4694
PSTN	Sip	RFC4769
VCARD	http or https	RFC4969
XMPP	Xmpp	RFC4979
IM	XMPP	RFC4969
VOICEMSG	sip, sips, tel, http or https	RFC5278
VIDEOMSG	sip, sips, http or https	RFC5278
UNIFMSG	sip, sips, http or https	RFC5278
ICAL-SCHED	http or https	RFC5333
ICAL-ACCESS	http or https	RFC5333

When a terminating device supports multiple services, e.g. both pstn and mms, an ENUM query can return multiple NAPTR records as per the following example.

```
$ORIGIN 3.2.1.0.5.5.5.5.1.2.1.e164.arpa.
    NAPTR 10 100 "u" "E2U+pstn:sip"
    "!^.*$!sip:+12155550123;npdi;spn=5xxxx@gw.example.com;user=phone!".
    NAPTR 100 10 "u" "E2U+MMS:mailto"
            "!^.*$!mailto:+12155550123@gw.example.com!"
```

As noted in Section 7.2.1 embedding of service information in NAPTRS/URIs may raise some issues and alternative DNS Resource Record (RR) types might also be considered.

11 IP Routing Directory Security and Accounting Requirements

The proposed solution should cover the following security requirements:

- Protect against malicious attacks (e.g. Denial of Service, man-in-the-middle) at IP and session layer protocols (e.g., ENUM/DNS, SIP, Diameter);
- Provide AAA (Authorization, Authentication, Accounting) for user login, provisioning and service query:
  - Query permission or data replication permission;
  - Carrier based authorization on selected service provider data view and update;
  - Service data access permission;
  - Usage reports, e.g. number of the total queries, percentage of the successful queries, number of network list updates in predefined common format.
- Support transaction security:
  - Provisioning transaction;
  - Querying transaction;
  - Transport and IP security has been discussed in the query interface and provisioning interface sections.
- Data integrity;
  - Integrity check while data is being exchanged between parties.
- Provide user administration.

12 IP Routing Directory Data Partitioning Requirements

The proposed solution should support logical partitioning (not necessarily physical partitioning) of data as follows:

- “Vertical partitioning” to allow different querying parties to receive different responses with respect to numbers/addresses stored in the registry. For example, only permitted parties may replicate the data of a given service provider’s E.164 numbers to their own domains, or only permitted parties may query but not replicate a given service provider’s E.164 numbers.
- “Horizontal partitioning” to allow different subsets of the service attributes data to be presented for a specific number/address. For example, a registry might contain data for a set of service attributes of a given E1.64 number but a given party may only be permitted to query or replicate a subset of those attributes. The subset can be defined as none, selected, or all service attributes available.

13 IP Routing Directory Scalability Requirements

The proposed solution should cover the following scalability requirements:

- To accommodate the transaction traffic growth and avoid a single point of overload;
- The routing directory architecture is implemented in a way to avoid network wide directory registry changes due to a single point of data registry change or addition (e.g. change to an existing member’s data registry or addition of a new member);
- The adopted IP addressing directory architecture shall be vendor and protocol independent;
- Additional business rules can be introduced without impacting the existing business rules and functions.

14 IP Routing Directory QoS Requirements

The following statistics are recommended to be used to measure the QoS of the IP routing directory:

- Operational Statistics for monitoring usage and forecasting the possible exhaustion of hardware, software and system resources with the traffic volume growth trend:
  - Example of resources are CPU, Memory, Disk Space, Software Threads, Software Usage based Licenses (Right-To-Use).
- Query Transaction Statistics (e.g. ENUM, DNS, Diameter, SIP redirect etc):
  - Total Transactions (successful, failed, aborted etc.);
  - Transaction per destination code, destination code can be either a destination service provider ID or an information source ID to identify the owner of the addressing data;
  - Transaction per carrier origination;
  - Referral transactions to other carrier federations/consortium registry service providers.
- Database update / provisioning statistics.

15 Summary

This White Paper outlines the requirements to supply the carrier community with advanced routing and addressing schemes. The solutions discussed in this document aim to support the international carrier traffic exchange based on the number portability corrected data and the service based routing by considering the terminating device service characteristics and the underlying carriers' service supporting capabilities.

This White Paper specifically recommends:

- Terminating service provider identity and the service attributes of a given E.164 number need to be supported by the data registry;
- Carrier makes the final routing decision within its own domain based on the terminating service provider and service attributes data received from the query;
- ENUM is recommended as the query protocol. When ENUM is not supported, SIP Redirect can be used as an alternative query protocol;
- When a shared registry is used, data required in the shared registry can be provisioned from the sources of the participating carriers who have the knowledge of their represented service provider E.164 numbers, the service providers who own the end user and their E.164 numbers, the national or regional number portability databases, or other existing industry carrier federations/consortiums address databases.

Some of the challenges have been identified and require a joint effort from the industry standards bodies, the carriers, and the vendors to ultimately reach an optimized solution that works best for the international carriers. These challenges include but are not limited to:

- Development of a world-wide standard for service provider ID;
- Definition of required service and capability information to support carriers' routing needs;
- Sourcing and integration of SP ID, number portability, and service/capability information into a form suitable for use by carriers' IBO systems;
- A suitable architecture or architectures for carriers to exchange the above information.

Appendix - DIAMETER Query Protocol

The Diameter protocol, [14], is intended to provide, but is not limited to providing, a mechanism for Authentication, Authorization and Accounting (AAA) framework for applications such as network access or IP mobility. Over time it has been adopted and extended for many additional uses, including the manipulation of various network based informational services. Its use in the IMS architecture is an example.

Diameter is not recommended as one of the query protocols for the inter-carrier routing and addressing solution. This recommendation could be revisited if Diameter is widely adopted by the industry for inter-carrier applications.

Being conceived as an AAA protocol, the basic Diameter protocol attempts to address several topics, including the following that would seem to be relevant to its use for Routing and Addressing purposes:

- Failover Behavior
- Transmission level security
- Reliable transport
- Defined Agent behaviour
- Defined Server Behaviours (including initiation of Messages)
- Auditability
- Extensibility
- Capability negotiation
- Peer Discovery
- Roaming support

Diameter is typically run over TCP and/or SCTP to support reliable transport. IPSec and TLS are typically utilized for authentication, confidentiality and security purposes.

The base framework defines the notion of Clients and Servers, which carry the standard connotations, as well as the concept of Relays, Proxies, Redirectors and Translation agents. Again, these typically operate in a fashion the names imply, but in summary they provide for the following (paraphrased from RFC 3588):

- They can distribute administration of systems to a configurable grouping, including the maintenance of security associations;
- They can be used for concentration of requests from an number of co-located or distributed equipment sets to a set of like user groups;
- They can do value-added processing to the requests or responses;
- They can be used for load balancing;
- A complex network will have multiple information sources, and they can sort requests and forward towards the correct target.

It should be noted that there are several applications defined already based on Diameter that would hold examples as to how Network Routing and Addressing could be achieved. For instance, RFC 4740 [15] defines a Diameter SIP application that not only does authentication and authorization, but also defines rudimentary routing functions that allow one SIP entity to find another server that is allocated to a given user in the network.

Examples may also be drawn from the IMS. Take for example the Home Subscriber Server (HSS). The HSS is the main store for all subscriber and service related data, including user identities, access parameters, user permitted service definitions and registration information. It also contains

a portion of the HLR/AUC functionality that enables access to the mobile and circuit switched networks.

The interfaces (reference points) to the HSS are all Diameter based (e.g. Sh, Si and Cx interfaces). Within the definition of the Cx for instance, you have among other things the ability to do location management, which enables you to identify the server in the network serving a particular user. This is similar to the functionality provided by DNS and the type of capability we would want to support for Routing and Addressing.