Subject: ATIS/SIP Forum NNI Joint Task Force Draft Documents for Comment

The IP-Network to Network Interface (NNI) Joint Task Force is seeking public comment on two (2) draft documents: (1) IP Interconnection Profile; and (2) IP Interconnection Routing Report. These documents are being provided for public review/feedback; written input is requested by October 29, 2014. However, in light of the short timeframe, written input will be accepted until December 1, 2014.

About the Task Force. The IP-Network to Network Interface (NNI) Joint Task Force is a cooperative effort between the Alliance for Telecommunications Industry Solutions (ATIS) and the SIP Forum that has been meeting regularly for the past ten months to define specification to support SIP-based Service Provider to Service Provider IP Interconnection. The Task Force is comprised of telecommunications technical experts representing a range of telephony service providers and suppliers, both large and small, that serve both consumers and businesses.

In December 2013, the IP-NNI Joint Task Force adopted a charter that included two primary goals:

- Develop a SIP profile defining the "on-the-wire" signaling and media specification at the IP interconnection point between telephony service providers.
- Develop a routing specification defining the data needed to determine IP routing (i.e., telephone number (TN) ownership, porting information, and TN-to-IP address association) and how it will be exchanged to support an all-IP environment.

These deliverables, while still “works in progress”, are now mature enough to solicit feedback from interested parties.

About the Documents. Two documents available for review are:

1. **IP Interconnection Profile.** The IP-NNI Profile Specification defines a reference architecture and specifications for both the protocol and media as it appears “on-the-wire” at interconnect points. The specifications reference commonly used IETF, 3GPP, and other related industry specifications and identify protocol extensions and capability information needed for all-IP telephony peering.

   It is the consensus of the Task Force that this document should be considered Normative.

2. **IP Interconnection Routing Report**. The IP-NNI Routing Technical Report documents mechanisms for identifying the preferred IP interconnection point for a given TN. This report presents multiple views of current IP interconnection mechanisms based on aggregate PSTN constructs, interim solutions based on all-IP routing using a per-TN registry, and a consideration of hybrid approaches across both mechanisms during the transition to all-IP.

It is consensus of the Task Force that this document should be considered Non-Normative because multiple alternatives are presented without a specific recommendation on the use of a single preferred technical approach. Various service providers are in different states of readiness and manage their networks for SIP interconnection in different ways. The Technical Report presented several suggested approaches for interoperability between alternatives that may be implemented in different ways using various technical means.

Though these specifications center on the use of SIP and IMS in service provider voice networks, the task force believes that these recommendations will ultimately be adapted for other multimedia forms of real-time communication including point to point video calling and rich text media.

Feedback. It is the earnest desire of the Task Force to encourage ongoing and informed *technical* feedback on the attached documents, from all segments of the industry. Interested parties are invited to submit technical comments to the Task Force via its mailing list. In order to join the effort, individuals must first be registered as a SIP Forum Participant Member (Free) using the online form located here: http://www.sipforum.org/component/option,com_advanced_registration/task,register/. When completed, subscription to the NNI Task Force mailing list can be performed at: http://sipforum.org/mailman/listinfo/nni.

For further information on the IP Network to Network Interface (NNI) Joint Task Force and these above-referenced documents, please contact:

Jim McEachern <Senior Technical Consultant, ATIS> jmceachern@atis.org

Richard Shockey <Chairman of the Board, SIP Forum> richard@shockey.us

About ATIS

As a leading technology and solutions development organization, the Alliance for Telecommunications Solutions (ATIS) brings together the top global ICT companies to advance the industry's most-pressing business priorities. Through ATIS committees and forums, nearly 200 companies address cloud services, device solutions, emergency services, M2M communications, cyber security, network evolution, quality of service, billing support, operations, and more. These priorities follow a fast-track development lifecycle – from design and innovation through solutions that include standards, specifications, requirements, business use cases, software toolkits, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of oneM2M, a member and major U.S. contributor to the International

Telecommunication Union (ITU) Radio and Telecommunications sectors, and a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

About the SIP Forum

The SIP Forum is an IP communications industry association that engages in numerous activities that promote and advance SIP-based technology, such as the development of industry recommendations, the SIPit, SIPconnect-IT and RTCWeb-it interoperability testing events, special workshops, educational seminars, and general promotion of SIP in the industry. The SIP Forum is also the producer of the annual SIPNOC conferences (for SIP Network Operators Conference), focused on the technical requirements of the service provider community. One of the Forum's notable technical activities is the development of the SIPconnect Technical Recommendation - a standards-based SIP trunking recommendation that provides detailed guidelines for direct IP peering and interoperability between IP PBXs and SIP-based service provider networks. Other important Forum initiatives include work in Fax-over-IP interoperability, User Agent Configuration, Video Relay Service interoperability, security, NNI, and SIP and IPv6. For more information, please visit: http://www.sipforum.org.

Media Contacts

ATIS Contact:

Marcella Wolfe
Phone: +1 202-434-8851
Email: mwolfe at atis.org

SIP Forum Contact:

Marc Robins
Phone : +1 203-829-6307
Email: marc.robins at sipform.org

Contribution

TITLE: IP Interconnection Profile

SOURCE*: Martin Dolly, AT&T, Lead Member Technical Staff

ABSTRACT

This document provides the clean baseline document to the 9/4 meeting.

NOTICE

ATIS-1000063

ATIS Standard on

IP Interconnection

Alliance for Telecommunications Industry Solutions

Approved Month DD, YYYY

Abstract

Abstract text here.

Foreword

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The [COMMITTEE NAME] Committee [INSERT MISSION]. [INSERT SCOPE].

The SIP Forum's mission is to advance the adoption of products and services based on the Session Initiation Protocol and to maintain and serve a global community of commercial SIP based service and technology providers. The primary goals of the SIP Forum are to foster interoperability and adherence to standardization efforts, and provide educational resources and a platform for productive communication among industry participants.

This document was developed by the ATIS/SIP Forum IP-NNI Task Force

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, [COMMITTEE NAME], 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, [COMMITTEE NAME], which was responsible for its development, had the following leadership:

[LEADERSHIP LIST]

The [SUBCOMMITTEE NAME] Subcommittee was responsible for the development of this document.

Table of Contents

[INSERT]

Table of Figures

[INSERT]

Table of Tables

[INSERT]

ATIS Standard on –

IP Interconnection

1 Scope, Purpose, & Application

1.1 Scope

This document was developed under a joint ATIS and SIP Forum collaboration. The document defines an IP NNI Standard with an emphasis on VoIP. Other Multimedia services will be addressed in subsequent releases.

The objective of this document is to:

1. Define a reference architecture that sets forth the common functional entities necessary for Carrier to Carrier Interconnection. This reference architecture will be from the perspective of the interconnection points between carriers and will not deal with implementation details inside the networks on either side of the IP-NNI.
2. Specify the exact specifications (including IETF RFCs, 3GPP, and other existing standards) associated with these protocols that must or should be supported by each element of the reference architecture. Where required, the options that MUST or SHOULD be supported within a given standard will also be specified.
3. Specify customary methods for negotiating protocols, protocol extensions, and exchanging capability information between carriers. Specify consensus methods of formulating SIP protocol messages where multiple options exist in standards.
4. Specify the exact presentations of Fully Qualified Domain Names in “From:” and “To:” fields including use of TEL URI format, including P-Asserted Identity (PAI).
5. For IP originated Calls, specify the preferred header [SHOULD] for Calling Name data [CNAM], and specify how that data is presented to the terminating proxy including format, syntax and processing of such data. Note: The expectation is that the signaling of CNAM would not survive interworking to SS7.
6. Define mandated support for underlying transport [e.g. UDP, TCP, SCTP].
7. Specify an audio codec selection strategy that minimizes the need for transcoding and a transcoding strategy that balances the workload between originating and terminating carrier.
8. Define strategies for DTMF and Fax support.
9. Specify call loop detection and avoidance methods.
10. Define common Quality of Service objectives including network overload and congestion notification and processing mechanisms.
11. Investigate issues surrounding known interoperability problems (e.g. PRACK [RFC 3262], early media, ptime, etc.).

1.2 Purpose

IP Interconnection among service providers is significantly increasing as the transition of the PSTN from SS7/TDM to SIP/IP networks progresses. Current deployments of SIP/IP in the core carrier networks have exposed operational and implementation differences on how IP for SIP traffic works ‘on the wire’. These differences complicate interconnection, and in some cases require ‘protocol normalization’ to achieve full interoperability. The call control protocol SIP [RFC 3261] is defined in the IETF and further refined in profiles developed by 3GPP or ATIS that reflect regional and/or national differences in implementation. There are hundreds of IETF SIP and 3GPP specifications that are open to interpretation, creating ambiguity in the detailed options that are implemented. This often requires Session Border Controllers or I-CSCF proxies reconcile the signaling between service providers and resolving those ambiguities. Time and effort is also required to document the differences and configure the SBC or I-CSCF proxy to implement the necessary changes to the on the wire protocol.

The purpose of this effort is to identify a baseline set of features that should be common to all IP-NNI implementations for voice service, and where gaps or ambiguities are identified in existing standards, request that those gaps be addressed by the responsible Standards Development Organizations [SDOs].

This specification defines which standards and options must be supported. They will provide carriers with a precise description of the IP-NNI in the areas where the standards leave multiple options, or where the existing specifications are ambiguous.

In addition, this specification will increase requirements [i.e. MAY, SHOULD, MUST] where operational experience indicates that such enhancements are necessary to support full interoperability.

1.3 Application

This standard is defined for North America deployments, but may be applicable for deployments outside North America.

1.4 Requirements

<S.1.2.3 R/CR/O – 00010 – Start>

Requirement

Note:

<S.1.2.3 R/CR/O – 00010 – End>

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

ATIS-0x0000x, *Technical Report*.

ATIS-0x0000x.201x, *American National Standard*.

[RFC 4733] IETF RFC 4733 – RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals

[draft-ietf-soc-overload-control-15]

[T.38] ITU-T Recommendation T.38 (09/2010) – Procedures for real-time Group 3 facsimile communication over IP networks

[V.150.1] ITU-T Recommendation V.150.1 (01/2003) – Modem-over-IP networks: Procedures for the end-to-end connection of V-series DCEs

[V.152] ITU-T Recommendation V.152 (09/2010) – Procedures for supporting voice-band data over IP networks

3 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < http://www.atis.org/glossary >.

3.1 Definitions

AAA: xxxx.

Bbbb: xxxx.

3.2 Acronyms & Abbreviations

3GPP	3rd Generation Partnership Project
ALG	Application Level Gateway
ATCF	Access Transfer Control Function
B2BUA	Back to Back user agent
BGCF	Border Gateway Control Function
CSCF	Call Session Control Function
IBCF	Interconnection Border Control Function
I-BGF	Interconnection Border Gateway Function
I-CSCF	Interrogating-Call Session Control Function
ICSS	IMS Centralized Services
IMS	IP Multimedia Subsystem
IMS-ALG	Multimedia Subsystem Application Level Gateway
IP	Internet Protocol
IPSec	IP Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
MGCF	Media Gateway Control Function
MGF	Media Gateway Function
MIME	Multipurpose Internet Mail Extensions
MSC	Mobile Switching Center
NAT	Network Address Translation
NAT-PT	Network Address Translation—Protocol Translation
NNI	Network to Network Interface
P-CSCF	Proxy Call Session Control Function
RTP	Real-Time Protocol
SBC	Session Border Controller
S-CSCF	Serving-Call Session Control Function
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SGF	Signalling Gateway Function
SIP	Session Initiation Protocol
SIP URI	SIP protocol Uniform Resource Identifier
SIP-I	SIP with encapsulated ISUP
SIP-T	SIP for Telephones
SLA	Service Level Agreement
SRVCC	Single Radio Voice Call Continuity
TCP	Transmission Control Protocol

tel-URI	Telephone Uniform Resource Identifier
TRF	Transit and Roaming Function
TrGw	Transition Gateway
TLS	Transport Layer Security
UA	User Agent
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
VoIP	Voice over IP

4 Reference Model for Interconnection

4.1 Current US Telephony PSTN Interconnect Model

The figure below depicts the current US Telephony PSTN architecture and interconnect model. This architecture is characterized by:

- One or more end office local switching systems interconnected within a Local Access and Transport Area (LATA).
- One or more inter-exchange carrier networks providing interconnect services between these LATA based local networks.

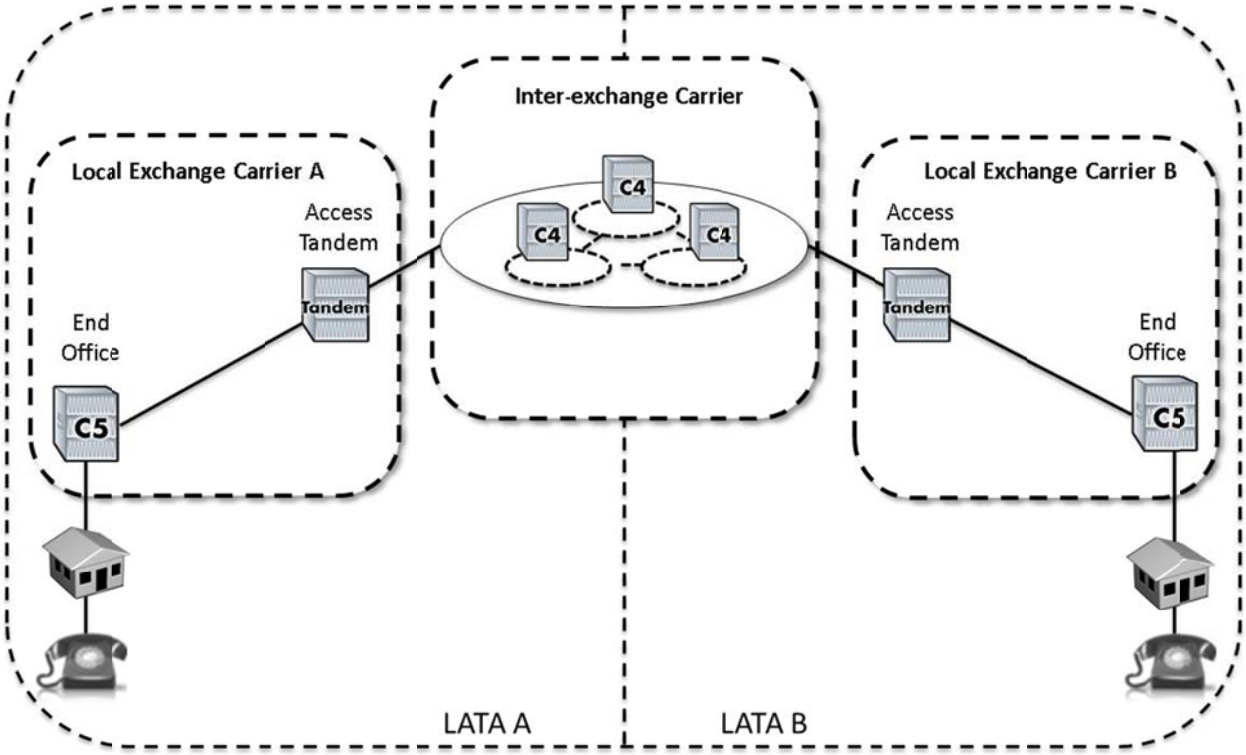

Figure 4. 1 - Current US Telephony PSTN Interconnect Model

The end office switches within the LATA are known as Class 5 (C5) switches. Within the LATA, Class 5 switches interconnect through tandem switches or through direct connections. Class 5 switches connect directly to

customer premises equipment such as telephones and FAX machines, and provide local telephony services to this equipment.

Interconnectivity between LATAs is provided by inter-exchange carrier networks. These networks are comprised of Class 4 (C4) switches that provide interconnect services between other Class 4, Class 5, and tandem switches. An inter-exchange carrier's class 4 switch may connect to an access tandem and/or directly to the class 5 switches within a LATA.

4.2 VoIP Interconnection Basic Configuration

VoIP in this context will coexist with SMS, MMS, Multimedia features, video calling, and other Real Time Communications features that may come available.

VoIP has been introduced into the traditional PSTN network architecture in a variety of places, forming islands of VoIP that must interconnect. For example VoIP could be used in:

- Enterprise PBX networks.
- Local networks.
- Tandem and inter-exchange networks.

The figure below illustrates one example of a bilateral carrier VoIP interconnection wherein VoIP signaling and media are exchanged between carriers. More detail relating to interconnect models is provided in section C.2 of this document.

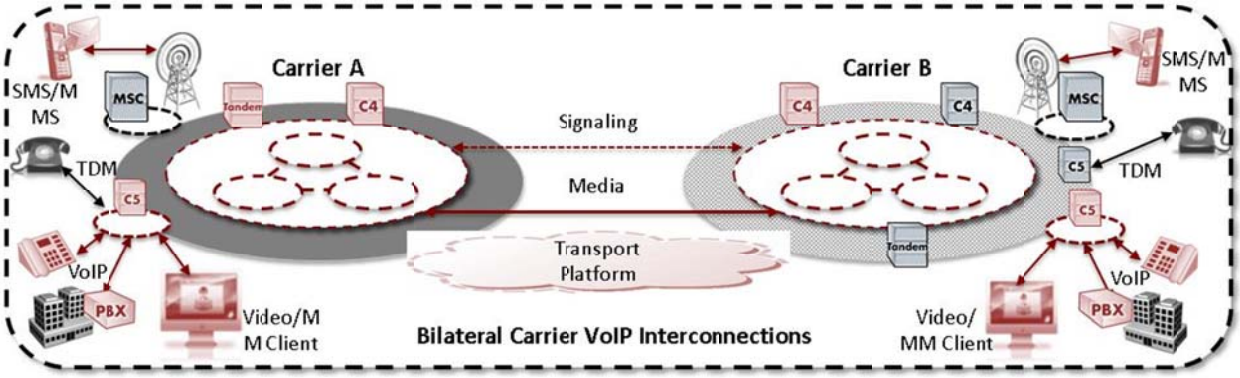

Figure 4. 2 - Bilateral Carrier VoIP Interconnections

4.3 Trust Model

Security trust model

The Carrier functional reference architecture defines Functional Entities (FEs). However, since network security aspects depend heavily on the way that FEs are bundled together, the Carrier security architecture is based on physical Network Elements (NEs), i.e., tangible boxes that contain one or more FEs. The way these FEs are bundled into NEs will vary, depending on the vendor.

This sub-clause defines three security zones;

1. Trusted,
2. Trusted but vulnerable,
3. Un-trusted,

These security zones are dependent on operational control, location, and connectivity to other device/network elements.

When a Carrier is connected to another Carrier, whether the other Carrier is trusted depends on:

- Physical interconnection, where the interconnection can range from a direct connection in a secure building to via shared facilities;
- The peering model, whether the traffic is exchanged directly between the two Carrier service providers, or via one or more untrusted Carrier transport providers;
- Business relationships, where there may be penalty clauses in the SLA agreements, and/or a trust in the other Carrier provider's security policy. The relationship must specify contractual terms stating the obligations each party to the contract agrees to and should also specify any specific security mechanisms, information and procedures also agreed to by the parties.

In general, Carrier providers should view other providers as un-trusted. Figure 3 shows an example when a connected Carrier is judged un-trusted.

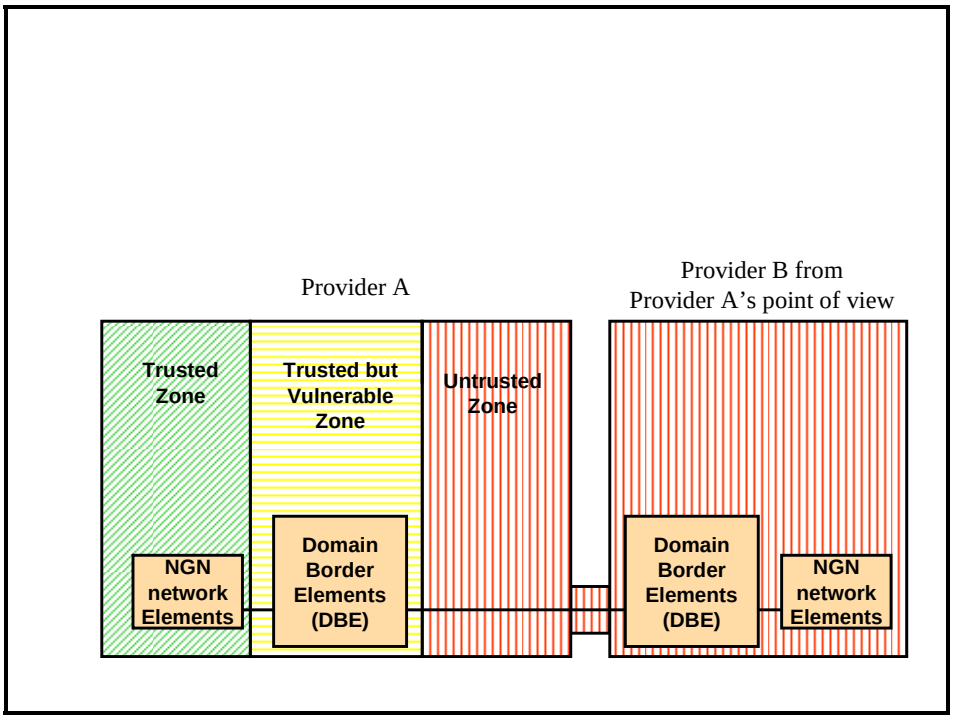

Figure 4. 3 - Carrier Interconnection Trust Relationship

An "internally trusted network security zone" or "trusted zone" in short, is a zone where a Carrier provider's network elements and systems reside and never communicate directly with customer equipment or other domains. The common characteristics of Carrier network elements in this zone are that they are under the full control of the Carrier provider are located in the Carrier provider domain, and they communicate only with elements in the "trusted" zone and with elements in the "trusted-but-vulnerable" zone. It should not be assumed that because it is in a trusted zone it is secure per se.

The "trusted zone" will be protected by a combination of various methods. Some examples are physical security of the Carrier network elements, general hardening of the systems, , use of secure signaling, security for OAMP messages separate VPN within the (MPLS/)IP network for communication within the "trusted" zone and with Carrier network elements in the "trusted-but-vulnerable" zone. See clause 8 for more details.

A "trusted but vulnerable network security zone", or "trusted but vulnerable zone" in short, is a zone where the network elements/devices are operated (provisioned and maintained) by the Carrier provider. The equipment may be under the control by either the customer/subscriber or the Carrier provider. In addition, the equipment may be

located within or outside the Carrier provider's premises. They communicate with elements both in the trusted zone and with elements in the un-trusted zone, which is why they are "vulnerable". Their major security function is to protect the NEs in the trusted zone from the security attacks originated in the un-trusted zone.

Elements that are located on the Carrier provider's domain with connectivity to elements outside the trusted zone are referred to as Network Border Elements (NBEs). Examples of these are the:

- Network Border Elements (NBE), which provide the User-Network Interface service control or transport elements of the Carrier provider in the trusted zone in order to provide the user/subscriber access to the Carrier provider's network for services and/or transport.
- Domain Border Element (DBE) that is the same kind of equipment with network border element except that it resides on the border between domains.
- Device configuration & bootstrap NBE (DCB-NBE) that interface with the Carrier provider's device configuration system in the trusted zone in order to configure the user's/subscriber's device and Carrier provider's equipment in the outside plant.
- Operations, Administration, Maintenance, and Provisioning NBE(OAMP-NBE) that interfaces with the Carrier provider's OAMP systems in the trusted zone in order to provide and maintain the user's/subscriber's device and Carrier provider's equipment in the outside plant.
- Application Server/Web Server NBE (AS/WS-NBE) that interfaces with the Carrier provider's AS/WS-NBE in the trusted zone to provide the user/subscriber access to web based services.

Examples of devices and systems that are operated by an Carrier provider but are not located on the Carrier provider's premises, and that may or may not be under the control of the Carrier provider (and, therefore, may or may not be part of the trusted zone), are:

- Outside plant equipment in the access network/technology;
- Base Station Router (BSR), a wireless network element that integrates the base station, radio network controller and router functionalities;[1]
- Optical Units (ONUs) within a user/subscriber's residence.

The "trusted-but-vulnerable" zone will be protected by a combination of methods. Some examples are physical security of the Carrier network elements, general hardening of the systems, , use of secure signaling for all signaling messages sent to Carrier network elements in the "trusted" zone, security for OAMP messages, and packet filters and firewalls as appropriate. See clause 8 for more details.

An "un-trusted zone" includes all network elements and systems of a customer network, peer network, or other Carrier provider security zone outside of the related Carrier provider domain. These are connected to the Carrier provider's border elements. The elements in the "un-trusted zone" may not be under the control of the Carrier providers and it is effectively impossible to enforce the provider's security policy on the user. Still it is desirable to apply some security measures, and to that end, it is recommended that signaling, media, and OAM&P be secured and that the Terminal Equipment Border Element (TE-BE) located in the "un-trusted zone", is hardened. However, due to the lack of physical security, these measures cannot be considered absolutely safe. See clause 8 for more details.

5 General Procedures

5.1 Extension Negotiation

SIP entities involved in session peering SHOULD be configured in such a way that they do not require any SIP extensions, beyond those mandated by this document, to be supported by the peer Carrier (SIP Service Provider) network. When sending an out-of-dialog request to a peer Carrier network, SIP entities involved in session

[1] This is not CPE.

peering SHOULD include a Supported header field identifying all the extensions supported by the sending network.

SIP entities involved in session peering MAY support configuration controls to disable certain extensions based on bilateral agreement between peer Carrier networks. For example, a SIP entity involved in session peering could be configured to remove 'preconditions' from the Supported header in order to disable the use of reliable provisional response (PRACK).

NOTE: Policies that limit or block the use of SIP extensions should be applied with care, since their application tends to disable SIP's native extension negotiation mechanism, and therefore inhibit the deployment of new services.

When sending a dialog-initiating request to a peer Carrier network, SIP entities involved in session peering MUST identify all supported SIP requests in the Allow header field

5.2 Public User Identities

Users are identified at the peering interface by their Public User Identity. A SIP entity involved in session peering MUST encode Public User Identities as a SIP URI of the telephone-subscriber syntax form of a Tel URI as indicated by the "user=phone" parameter (see [RFC 3261] section 19.1.6), where the user part of the SIP URI contains a global Tel URI as defined in [RFC 3966].

Example:

`sip:+13035551212@example.operator.com;user=phone`

5.2.1 Identifying the Called User

When sending a dialog-initiating request to a peer Carrier network, SIP entities involved in session peering MUST:

- identify the called user in the Request-URI of the request, and
- identify the called user using the telephone-subscriber syntax form of the SIP URI as described above in Section 6.2.

In addition, if Local Number Portability (LNP) information for the called number was obtained, then SIP entities involved in session peering MUST:

- include the LNP data in SIP URI in the Request-URI using the Tel URI "npdi" and "rn" parameters as defined in 6.2, and
- if the called number is ported, identify the routing number using the global form of the "rn" parameter, which is indicated by a leading "+" character followed by the country-code followed by the national number (e.g., "rn=+16132220000").

- On receiving a dialog-initiating request from a peer Carrier network, SIP entities involved in session peering MUST:
- identify the called user based on the contents in the Request-URI, where the Request-URI contains a SIP URI as described above in Section 6.2;
- obtain the LNP data for the called number based on the presence and contents of the "npdi" and "rn" Tel URI parameters contained in the SIP URI in the Request-URI as defined in [RFC 4694].

Table 5.1 summarizes the called Public User Identity that MUST be supported at the peering interface.

Table 5. 1 - Called Public User Identities

Use Case	Direction	Valid Form	Example
No LNP query	send/receive	SIP URI containing global Tel URI	sip:+13036614567@example.com;user=phone
LNP Query - number not ported	send/receive	Above plus "npdi" parameter	sip:+13036614567;npdi@example.com;user=phone
LNP Query - number ported	send/receive	Above plus global "rn" parameter	sip:+13036614567;npdi,rn=+13036620000@example.com;user=phone

North American supported formats are shown in Table 5.2.

5.2.2 Identifying the Calling User

When sending or receiving a dialog-initiating request, SIP entities involved in session peering MUST identify the calling user in the P-Asserted-Identity header field using the telephone-subscriber syntax form of the SIP URI as described above in Section 6.5.2.3.

5.2.3 Numbering & Addressing

The table below describes the set of URI formats that MUST be supported on the IP-NNI, and the headers in which these formats may appear. This is not intended to preclude the use of tel or sips URIs.

URI	sip:+1NPANXXXXXX@host;user=phone
Description	NANP number
Reference	IETF RFC3966
Headers	R-URI, To, From, Request Contact, 3XX Contact, PAI, Diversion
URI	sip:+18YYXXXXXXX@host;user=phone
Description	NANP 8YY number
Reference	IETF RFC3966
Headers	R-URI, To, 3XX Contact
URI	sip:+1NPANXXXXXX;npdi@host;user=phone
Description	NANP number with Number Portability Dip Indicator
Reference	http://www.ietf.org/internet-drafts/draft-ietf-iptel-tel-np-09.txt
Headers	R-URI, To, 3XX Contact
URI	sip:+1NPANXXXXXX;rn=+1NPANXXXXXX;npdi@host;user=phone

Description	NANP number with Number Portability Dip indicator and LRN
Reference	http://www.ietf.org/internet-drafts/draft-ietf-iptel-tel-np-09 .txt
Headers	R-URI, To, 3XX Contact
URI	sip:+1NPANXXXXXX;cic=+10288@host;user=phone
Description	NANP number with Carrier Identification Code, NPA may be an 8YY
Reference	http://www.ietf.org/internet-drafts/draft-ietf-iptel-tel-np-09.txt
Headers	R-URI, To, 3XX Contact
URI	sip:+1NPANXXXXXX;cic=+10288;dai@host;user=phone
Description	NANP number with Carrier Identification Code and dial around indicator; NPA may be an 8YY
Reference	http://www.ietf.org/internet-drafts/draft-ietf-iptel-tel-np-09.txt
Headers	R-URI, To, 3XX Contact
URI	sip:+1NPANXXXXXX@host;user=phone;isup-oli=0
Description	NANP number with OLI
Reference	IETF RFC3966
Headers	From
URI	sip:+1NPANXXXXXX;rn=+1NPANXXXXXX@host;user=phone
Description	NANP number with JIP (used in a From, PAI, or Diversion header)
Reference	
Headers	From, PAI, Diversion
URI	sip:N11;phone-context=+1@host;user=phone
Description	NANP special service code in local number format
Reference	IETF RFC3966
Headers	R-URI, To, 3XX Contact
URI	sip:613131;phone-context=+1@host;user=phone
Description	NANP directory assistance in local number format

Reference	IETF RFC3966
Headers	R-URI, To, 3XX Contact
URI	sip:+CCNSN@host;user=phone
Description	International number, CC=Country Code, NSN=National Significant Number
Reference	IETF RFC3966
Headers	R-URI, To, From, Request Contact, 3XX Contact, PAI, Diversion
URI	sip:B;phone-context=+33@host;user=phone
Description	Directory assistance in local number format in country with CC 33
Reference	IETF RFC3966
Headers	R-URI, To, 3XX Contact

5.3 IPv4/6 Interworking

It is the responsibility of the IPv6 Carrier network to perform the IPv4/IPv6 interworking function when interworking with an IPv4 Carrier network.

5.4 Fault Isolation and Recovery

5.4.1 Interface Failure Detection

A Carrier network MAY periodically send an OPTIONS request containing a Max-Forwards header field set to a value of '0' to detect the availability of a peer's ingress point. The ping rate is based on bi-lateral agreement (typically every 5 seconds). If the sending Carrier network fails to receive a response to an OPTIONS request, then it will consider that non-responding ingress point into the peer Carrier network to have failed, and will remove the ingress point from the available set of ingress points to the peer Carrier network. When a failure is detected, the Carrier network that detected the failure should attempt to route subsequent calls to the peer Carrier network over an available alternate route, with the final alternate route being the PSTN. In the meantime, the Carrier network that detected the failure will continue to send periodic OPTIONS pings to the failed ingress point, in order to detect when it has been restored and is available for service.

NOTE: A possible enhancement to the OPTIONS ping is to declare a well-known SIP URI in the registry that could be used totest the health of each ingress point in a peer Carrier network. For example, SIP INVITE (with no SDP) to SIP:999999999@mso-a.com would respond with a 200OK (again no SDP), followed by a BYE/200OK.

5.4.2 Congestion Control

Carrier's MUST support SIP Overload Control with mandatory support of the default algorithm [draft-ietf-soc-overload-control-15]. Carrier's MAY optional support the Rate Based algorithm based on bilateral agreement between two carriers.

A Carrier network MAY impose limits on the number of simultaneous calls, and the incoming rate at which it will accept calls, from a peer. On receiving a dialog-initiating request that exceeds such limits, the receiving Carrier network MUST respond with a 503 (Service Unavailable) response. A Carrier network receiving a dialog-initiating request MUST limit the use of the 503 responses to reporting congestion at the ingress point. A terminating Carrier network MUST NOT send a 503 response to an originating Carrier network to report congestion or other

failures that are internal to the terminating Carrier network. For example, a 503 response generated by a SIP signaling entity within a terminating Carrier network should be consumed within the terminating network, and should not be propagated across the peering interface to the originating Carrier network (i.e., avoid sending a 503 response to an originating peer if the same failure is likely to be encountered when the call is retried via an alternate route).

On receiving a 503 (Service Unavailable) response from a peer Carrier network, the receiving Carrier network MUST limit the scope of the response to the call on which it was received (i.e., a 503 response has no affect on the routing of subsequent calls to the peer). Also, the receiving Carrier network MUST attempt to consume the 503 response from a peer as close to the egress signaling point as possible, and avoid propagating the response back toward the originating CMS or E-DVA. Specifically, on receiving a 503 response to a dialog-initiating request that was sent to a peer Carrier network, the receiving Carrier network MUST:

1. terminate the current transaction,
2. ignore the Retry-After header field if one is present, and
3. attempt to route the call via an alternate peering interface (i.e., do not attempt to route the call via the same peering interface since it may encounter and aggravate the same overload condition).

5.4.3 Session Timer

SIP entities involved in session peering SHOULD support Session Timer as defined in [RFC 4028].

5.4.4 RTP Loopback Test

Peer Carrier networks SHOULD support the RTP Loopback Test procedures defined in [E-DVA]. Carrier networks that support the RTP Loopback procedures will provide a SIP URI that identifies a media endpoint within the Carrier network that performs the loopback functions. Ideally, this "loopback" media endpoint would be located near the ingress point of the peer Carrier network.

5.5 Media

5.5.1 RTP

5.5.2 Codecs

Narrow Band codecs reproduce the audio bandwidth of the PSTN. The following codecs, widely used in IP based voice networks, shall be supported as described in the tables below. Codecs in the Group 1 column in each table MUST be supported for both transmission and reception across the NNI. Codecs in the Group 2 columns in each table SHOULD be supported for both transmission and reception across the NNI.

Table 5. 2 - Mandatory and Optional Narrow Band Codecs

Group 1. Mandatory Narrow Band codecs	Group 2. Optional
G.711 μ-law 64 kbit/s	G.711 A-law
	G.723.1 (quality impairments have to be considered using this codec)
G.729, G.729a, G.729b, G.729ab 8kbit/s	G.726
	AMR-NB

When wide band audio is being used, the following wide band codecs, widely used in IP based voice networks, shall be supported as described in the tables below. Codecs in the Group 1 column in each table MUST be supported for both transmission and reception across the NNI. Codecs in the Group 2 columns in each table SHOULD be supported for both transmission and reception across the NNI.

Table 5. 3 - Mandatory and Optional Wideband Codecs

Group 1. Mandatory Wideband codecs (*)	Group 2. Optional Wideband codecs
G.722 (generally used by fixed network operators)	
G.722.2 (AMR-WB, generally used by mobile network operators)	

5.5.3 Codec/Packetization Period Use & Transcoding Guidelines

The packetization periods and payload types shown in the following table MUST be used for each of the associated codecs.

Codec	Packetization Period	Payload type definition
G.711 A-law	20 ms	PT= 8 Static
G.711 μ-law	20 ms	PT= 0 Static
G.729, G.729a,	20 ms	PT= 18 Static
G.729b, G.729ab	20 ms	PT= 18 Static. Optional parameter “annexb” may be used according to RFC 4855
G.723.1	30 ms	PT=4 Static Optional parameters "annexa" and "bitrate" may be used according to RFC3555
G.726	20 ms	PT=Dynamic as defined in RFC 4855
AMR-NB	20 ms	Dynamic as defined in RFC 4867

Bitrates and Modes for mandatory Wideband codecs

The requirements for AMR-WB are taken from GSMA PRD IR.36 [100] and RFC 4867 [39]. The requirements for G.722 are taken from New Generation Dect-ETSI TS 102 527-1; New Generation DECT, Part 1 Wideband Speech

AMR-WB can operate in a 9 modes at source codec bit rate of 23.85 kbit/s, 23.05 kbt/s, 18.25 kbit/s, 15.85 kbit/s, 14.25 kbit/s, 12.65 kbt/s, 8.85 kbt/s,6.60 kbit/s.

The AMR-WB configurations specified for 2G and 3G are:

WB-Set 0 = { 12.65 8.85 6.60}

WB-Set 2 = {15.85 12.65 8.85 6.60}

WB-Set 4 = {23.85 12.65 8.85 6.60}

No other combination of the 9 AMR-WB modes is allowed for voice telephony. The other modes of AMR-WB may be used for other applications.

All these 3 supported configurations are TrFO compatible. However, WB-Set 0 is the guaranteed minimum common denominator mandatory for all configurations and shall be supported. This configuration also includes DTX, i.e. WB-SID frames and no data transmission during inactive speech; support of SID frames in reception is mandatory; generation is optional. All other modes are optional.

G.722 shall be supported at a bit rate of 64 kbit/s.

Packetisation period for mandatory Wideband codecs

- for G.722, packetisation period shall be 20 ms
- for AMR-WB, packetisation period shall be 20 ms

Payload type definition for mandatory Wideband codecs

- G.722 PT=9 Static
- AMR-WB Dynamic as defined in RFC 4867

5.5.4 General Guidelines

The following general guidelines aim to provide default rules for codec choice and transcoding responsibility:

1. Transcoding should generally avoided;
2. If the SDP offer contains a wideband codec, then the wideband codec will always be placed first in order (e.g., if wideband and narrowband are offered, the wideband is first in order).
3. Wideband codec continuity offers the optimal quality; Service Providers should offer a fallback to narrowband codec that is universally supported (e.g. G.711) along with its supported high quality codec(s).
4. Transcoding to narrowband codecs must be avoided unless it is the only way for a call to be successfully established;
5. the order of codec/packetisation period preference is determined by the originating terminal and should be honoured wherever possible;
6. if the call is to be routed to a TDM network, only one transcoding is recommended. If required, it should be performed during the voice over IP/TDM conversion;in case no common codec can be used between both end Service Providers, in the first instance it is the responsibility of Service Providers to support transcoding in order to ensure successful voice interoperability for their services

5.5.5 Voice-band Data Transport Mechanisms

Voice-band data (VBD) includes modem and fax data traditionally carried in circuit-switched voice channels. In a VoIP environment, the presence of VBD sessions will typically come from interworking with circuit-switched networks and CPE. Either packetized G.711 μ-law or A-law or packet-optimized relay mechanisms such as [T.38] fax relay can be used to carry these data streams. Modem relay modes such as in [V.150.1] are not common in the inter-carrier environment. Where NNIs use IP transport engineered for low loss and jitter, VBD without fax/modem relay should normally be sufficient. In the case of VBD without relay mechanisms, VBD may be transparently used over a compatible audio codec. Fax relay modes or explicit VBD-mode negotiation can optionally be used by bilateral agreement.

SIP entities involved in session peering MUST support fax or modem voice-band data (VBD) pass-through in a G.711 μ-law or A-law audio stream.

When a non-G.711 codec is originally negotiated for a session, SIP entities involved in session peering MUST support fallback to G.711 μ-law or A-law for VBD pass-through via SDP audio codec renegotiation without explicit VBD-mode negotiation. It is up to bilateral agreement which network element or elements will be responsible for recognizing fax/modem tones and for initiating a transition.

SIP entities involved in session peering MAY use fax relay mechanisms such as [T.38].

SIP entities involved in session peering MAY use explicit negotiation of transitions to VBD modes such as the following methods:

- Negotiation of support of voice-band data as specified in [V.152]
- Modem/fax events as specified in [RFC 4733]

5.5.6 DTMF Digit Transport Mechanisms

The “named telephone events,” or “telephone-events” RTP payload [RFC 4733] is the preferred mechanism for transport of DTMF digit events between VoIP endpoints and network elements. In limited cases and by bilateral agreement, in-band DTMF tones might be used across the NNI to avoid transcoding from in-band DTMF tones to named telephone events (DTMF relay), for instance if the media stream is expected to originate and terminate on circuit-switched voice channels in both carrier networks. It is assumed that in-band DTMF is only applicable for sessions using the G.711 codecs. The “telephone-events” payload type is negotiated by offering it along with an audio codec in the SDP. If the telephone-events payload is not negotiated, it is assumed that any DTMF digits will be passed across the NNI as in-band tones in the audio RTP channel.

SIP entities involved in session peering MUST support DTMF digits in a named telephone events RTP payload [RFC 4733].

SIP entities involved in session peering MAY support DTMF digits as in-band tones when the negotiated audio codec is G.711 A-law or μ-law.

SIP entities involved in session peering that utilize named telephone events [RFC 4733] for DTMF digit transport MUST support at least the following events (event codes 0-11):

- digits 0-9
- ‘#’ (pound or hash)
- ‘*’ (star)

5.6 IP Packet Marking

The following table describes the traffic classes defined for use across the NNI

Traffic class	Traffic type
Voice Media	Speech / Voice bearer.
Voice Signaling	Voice Control Traffic (SIP, SIP-I signaling protocols)I
Mobile Signaling	SMS and roaming (TCAP signaling protocol)
Other Customer Traffic	Internet traffic, other data traffic

Other control/management traffic such as BGP traffic may also use the interface.

Distinguishing traffic classes

In order to distinguish between traffic classes, the use of the DSCP marking scheme in Behaviour Aggregation mode [9] is recommended.

NOTE: Using classification based on the DSCP value, packet marking is pre-agreed by both operators. The receiving operator assumes that the sending operator has marked the packet correctly according to the pre-agreed scheme described above.

If there is a mix of Internet and VoIP traffic across the interconnection or the recommended marking cannot be guaranteed, an alternative solution is to classify packets using the Multi-Field classification method [9]. Using this

scheme, ingress traffic is classified by the receiving Operator PE Router based on any field in the IP header, e.g. destination address, source address, port numbers or other IP packet header fields.

IP Marking table

The following table illustrates DiffServ IETF RFC and IP Precedence TOS marking scheme plus the coding scheme at the MPLS and Ethernet layers that SHOULD be supported, respectively. It applies to all the traffic to be transmitted.

Traffic Type	DSCP Marking	IP Precedence	802.1Q VLAN
Voice Signaling and Media	DSCP 46/EF (101110).	5	5
	DSCP 46/EF (101110) or DSCP 00/DF (000000).	5 or 0	5 or 0
ETS Voice Signaling and Media	DSCP 44/VOICE-ADMIT (101100).	5	5
	DSCP 44/VOICE-ADMIT (101100).	5	5
Other traffic	DSCP 00/DF (000000).	0	0

The marking for the other control/management traffic depends on the specific network implementation.

Traffic treatment

Voice and media traffic leaving the sending Border Function towards the receiving Border Function should be treated according to the Expedited Forwarding Per-Hop Behavior [10] [11].

ETS voice signaling and media traffic leaving the sending Border Function towards the receiving Border Function should be treated according to the VOICE-ADMIT Forwarding Per-Hop Behaviour [Reference to 5865].

Voice signaling traffic leaving the sending Border Function towards the receiving Border Function should be treated according to the Expedite Forwarding Per-Hop Behavior [10] [11] or alternatively according to the Assured Forwarding Per-Hop Behavior [12].

Signalling traffic leaving the sending Border Function towards the sending PE router MUST be treated according to one of the following schemes:

- the Expedite Forwarding Per-Hop Behavior, as specified in RFC 3246 [10] and RFC 3247 [11] the Assured Forwarding Per-Hop Behavior as specified in RFC 2597 [12].
- the Default forwarding PHB , as specified in IETF RFC 2474 [8].

6 Call Features

6.1 Basic Call Setup

This section describes the procedures at the peering interface required to establish a 2-way session for a basic voice call. In this case it is assumed that no originating or terminating features are applied (no call blocking, forwarding, etc), and that the called line is available to accept the call. Also, this section describes the session establishment procedures when the call is initiated by the originating SIP User Agent itself, and not via a 3rd party in support of features like click-to-call. Two-way call establishment using 3rd Party Call Control (3PCC) procedures is covered in Section 6.6.

SIP entities involved in session peering MUST support the SDP offer/answer procedures specified in [RFC 3264] with the consideration that reliable provisional responses MUST be used as specified in [RFC 3262]. The originating Carrier network SHOULD include an SDP offer in the initial INVITE. The terminating Carrier network

MUST include an SDP answer in the reliable response to an INVITE received with an SDP offer. The terminating Carrier MUST include an SDP offer in the first reliable response to an INVITE received without an SDP offer. Once an SDP answer has been provided in a reliable response, it SHOULD not be repeated in subsequent responses (e.g., 200 OK (INVITE)), but if it is, the SDP in the 200 OK (INVITE) MUST be identical to the SDP in the reliable 183 Session Progress.

The terminating Carrier network MAY also include an SDP body in a provisional 18x response or reliable response (e.g., PRACK).

NOTE: If the provisional and final responses are on different dialogs (say, when the INVITE is forked), the SDPs may be different between the various responses.

SIP entities involved in session peering that advertise support for different but overlapping sets of codecs in the SDP offer/answer exchange for a given call MUST negotiate a single common codec for the call. An SDP answer MUST contain only a single codec (plus additional auxiliary codecs such as DTMF), per media stream, selected from the offered set of codecs.

6.1.1 SDP Requirements

SIP entities involved in session peering MUST support the SDP requirements defined in [RFC 4566]. A SIP entity involved in session peering MUST include only one media (m=) descriptor per desired media stream in an SDP offer to a peer Carrier network.

If a SIP entity involved in session peering receives an SDP offer containing multiple media descriptors, it MUST act on the media descriptors and include all of them in the same order in the response, including non-zero ports and zero ports for the offered media according to its capabilities as specified in [RFC 3264]an Offer/Answer Model with SDP. A SIP entity involved in session peering MUST NOT reject an offered session because it offers more media than the SIP entity can handle.

6.2 Ringback Tone vs. Early Media

During the call setup phase, while the originating Carrier network is waiting for the terminating Carrier network to answer the call, the originating line is either playing local ringback tone to the calling user, or is connected to a receive-only or bi-directional early-media session with the terminating Carrier network. For example, early media can be supplied by the terminating endpoint (e.g., custom ringback tone) while waiting for answer.

SIP entities involved in session peering MUST use the following procedures to control whether the originating line applies local ringback tone or establishes an early media session while waiting for the call to be answered.

1. The terminating Carrier network controls the application of local ringback tone at the originating line or the establishment of an early media session by sending the following provisional response to a call-initiating INVITE.
    - The terminating Carrier Network MUST send a 180 (Alerting) response containing no SDP to the originating SP network, if the call scenario requires the application of local ringback tone at the originating line.
    - The terminating Carrier Network MUST send a 183 (Progressing) response containing SDP that describes the terminating media endpoint to the originating Carrier network, if the call scenario requires an early media session.
    - The provisional response sent for other call scenarios is not be specified, as long as the response is not one of those described above.
2. The originating Carrier network performs the following action on receipt of a provisional response to a call-initiating INVITE.
    - The originating Carrier network MUST apply local ringback tone if it receives a 180 (Alerting) response containing no SDP.
    - The originating Carrier network MUST establish an early media session with the media endpoint described by the SDP when it receives a 18x response containing SDP.
    - The originating Carrier Network MUST do nothing (e.g., continue to apply local ringback tone if it was already being applied when the response was received) if it receives a 18x response other than 180 (Alerting), and the response contains no SDP.

When establishing an early media session, the originating Carrier network MAY immediately remove any local ringback tone currently being applied. Alternatively, the originating Carrier network MAY wait for receipt of RTP that matches the received SDP, and apply other checks/policies to validate the received RTP, before removing any locally applied ringback tone.

6.3 Early-Media

Carrier's MUST support P-Early-Media as defined in RFC 5009.

6.3.1 Terminating Network Procedures

When sending an 18x response and early media will be present, the response MUST include a P-Early-Media header field, as defined in IETF RFC 5009, authorizing early media, except when

- a reliable provisional response including a P-Early-Media header field has already been sent, and
- the most recently sent P-Early-Media header field authorization matches that which would be sent.

When both-way early media is required, the 18x response shall include a P-Early-Media header field authorizing backward and forward early media (i.e., "sendrecv"), otherwise the P-Early-Media header field shall only authorize backward early media (i.e., "sendonly").

When early media will not be present, the 18x response shall include a P-Early-Media header field not authorizing early media (i.e., “inactive”).

In the event that the nature of early media changes after initially signaled in an 18x response, the new authorization may be signaled in the P-Early-Media header field of either a subsequent 18x response or an UPDATE request.

6.3.2 Originating Network Procedures

When sending the initial INVITE request a SIP entity involved in session peering shall include the P-Early-Media header field with the “supported” value to indicate applicability of the P-Early-Media procedures, per IETF RFC 5009.

When an initial or subsequent 18x response or UPDATE request is received containing a P-Early-Media header field, then the following through connection procedures shall occur.

- If a P-Early-Media header field is received authorizing backward early media (i.e., a value of "sendonly"), then through connection in the backward direction shall be performed, if not already done.
- If a P-Early-Media header field is received not authorizing early media (i.e., a value of "inactive"), then through connection shall not be performed or removed if already done. The originating network shall generate alerting once a 180 Ringing response has been received.
- If a P-Early-Media header field is received authorizing both backward and forward early media (i.e., a value of "sendrecv"), then through connection in both directions shall be performed. The bearer path shall be connected in both directions on completion of the bearer setup.

6.4 Forking the INVITE

For each terminating media endpoint that requires an early media session to be established with the originating line, the terminating Carrier network MUST signal the attributes of the terminating media endpoint to the originating Carrier network within the SDP of a 183 (Progressing) response.

If terminating Carrier needs to modify the SDP, the Carrier SHOULD offer the modified SDP in an UPDATE request.

Alternatively, with bi-lateral agreement, the terminating Carrier network MAY utilize forked responses to ensure that 18x/200 responses containing different SDP copies are not sent within the same dialog. This MUST only be used if it had not previously received a Request-Disposition header [RFC 3841] preventing the use of forking, (e.g., Request-Disposition: no-fork). The terminating Carrier network does this by specifying a different tag parameter in the To header field for each provisional response that contains a unique SDP, as if the INVITE had been sequentially forked.

6.5 Redirecting the INVITE

Carrier's MAY support redirection across the NNI, based on bilateral agreement. The redirection MAY be performed with a 3XX or REFER message.

As an alternative to sequentially forking the INVITE, the terminating entity can redirect the originating entity to the next endpoint in the series by sending a 302 (Moved Temporarily) response containing a Contact header field that identifies the next endpoint. The resulting INVITE from the originating Carrier network is sent as a dialog-initiating request, and can therefore establish a new early-media session with the next endpoint in the series. The use of this procedure is based on bilateral agreement between peering operators.

On receiving a 302 (Moved Temporarily) response to an INVITE request, and if this mechanism is enabled based on local policy, the originating Carrier network MUST send a new dialog-initiating INVITE with a Request-URI set to the value returned in the Contact header field of the 302 (Moved Temporarily) response, as described in [RFC 3261].

6.6 Establishing Calls Using 3PCC

Carrier's may support features such as click-to-call, where the call is initiated by a 3rd party such as an Application Server on behalf of the originating user. To support such features, SIP entities involved in session peering MUST support the 3PCC procedures described in [RFC 3725].

6.7 Call Hold

A SIP entity involved in session peering that wishes to place a media stream "on hold" MUST offer an updated SDP to its peer Carrier network with an attribute of "a=inactive" or "a=sendonly" in the media description block. A SIP entity involved in session peering that wishes to place a media stream "on hold" MUST NOT set the connection information of the SDP to a null IP address. For example, the SIP entity involved in session peering MUST NOT set the 'c=' connection line to c=IN IP4 0.0.0.0. A SIP entity involved in session peering that wants to place a media stream "on hold" SHOULD locally mute the media stream.

A SIP entity involved in session peering that receives an SDP offer with an attribute of "a=inactive" in the media block MUST place the media stream "on hold" and send an SDP answer containing a media attribute of "a=inactive". A SIP entity involved in session peering that receives an SDP offer with an attribute of "a=inactive" in the media block MUST NOT set the connection data of the answer SDP to c=0.0.0.0. A SIP entity involved in session peering operating in IPv4 that receives an SDP offer with no directionality attributes but connection data set to c=IN IP4 0.0.0.0 SHOULD place the media stream "on hold".

6.8 Calling Number & Name Delivery

The originating Carrier network MUST provide the calling number of the originating user in the P-Asserted-Identity header field of dialog-initiating requests. Subject to local policies/agreements, the originating Carrier network SHOULD provide the calling name of the originating user in the P-Asserted-Identity header field of dialog-initiating requests. (The mechanism for obtaining the calling name is outside the scope of this document.) The calling number is contained in the telephone-subscriber syntax form of the SIP URI, containing an E.164 number [E.164] as described in Section 6.2. The calling name is contained in the display-name component of the P-Asserted-Identity header field.

If the originating user wants to remain anonymous, the originating Carrier network MUST include a Privacy header field containing the value "id" as specified in [RFC 3323] and [3325]. In addition, the originating Carrier network SHOULD obscure the identity of the originating user in other header fields as follows:

- Set the identity information in the From header field to "Anonymous <sip:anonymous@anonymous.invalid>"
- Set the display-name in the To header field to "Anonymous" (since the To display-name selected by the originating user could provide a hint to the originating user's identity)
- Obscure any information from the Call-ID and Contact header fields, such as the originating FQDN, that could provide a hint to the originating user's identity

The terminating Carrier network MUST obtain the calling name and number for caller-ID display from the contents of the P-Asserted-Identity header field contained in dialog-initiating requests. If the INVITE request contains a Privacy header with the value "id", the terminating Carrier network MUST provide a display of "Private" to the terminating user.

6.9 Call Forwarding

Carrier's MUST support the History-Info Header and SHOULD support of the SIP Diversion header for a period of time in order facilitate interoperability. When both headers are sent, the sender MUST ensure that they are semantically identical.

If the History-Info header and the Diversion header are both received by a carrier supporting both headers, the History-Info header MUST take precedence.

If a Carrier offers call-forwarding services to its users, then the forwarding Carrier network MAY remain in the signaling path of the forwarded call in order to support separate billing for forward-from and forward-to legs. A Carrier network that is required to remain in the signaling path of a forwarded call based on local policy MUST do so using one of the following procedures:

1. forward the INVITE to the forward-to-user while remaining in the signaling path as a SIP Proxy or B2BUA, or
2. respond to the initial INVITE with a 302 (Moved Temporarily) response with a Contact header field containing a private URI that points back to the forwarding Carrier network.

6.10 National Security/Emergency Prepardness (NS/EP)

Resource Priority Header (RPH) MUST be supported by NS/EP compliant networks, and MUST be transparently passed by non-NS/EP compliant networks.

7 NNI Signaling Profile

7.1 SIP Methods & Header Fields

Notations of the codes

For the purpose of the present document clause 6.1.1.4 TS 29.165 v11.5.0 (2012-12) applies as follows:

In the Table 7.1 the status codes "m", "o", "c" and "n/a" have the following meanings:

Table 7. 1 - Key to notation codes for SIP messages

Notation code	*Notation name*	*Sending side*	*Receiving side*
m	*mandatory*	*The message shall be supported at NNI. Supporting sending a SIP message at the NNI means that this message shall be sent over the NNI if received from the serving network. It does not imply that network elements inside the serving network or user equipment connected to this network shall support this message.*	*Supporting receiving a SIP message at the NNI means that this message shall be forwarded to the serving network. It does not imply that network elements inside the served network or user equipment connected to this network are supporting this message.*
o	*optional*	*The message may or may not be supported at NNI. The support of the method is provided based on bilateral agreement between the operators.*	*Same as for sending side.*
n/a	*not applicable*	*It is impossible to use/support the message.*	*It is impossible to use/support the message. This message will be discarded by the IBCF.*
c <integer>	*conditional*	*The requirement on the message ("m", "o" or "n/a") depends on the support of other optional or conditional items. <integer> is the identifier of the conditional expression.*	*Same as for sending side.*

7.1.1 SIP Methods

For the purpose of the present document clause 6.1.1.2 TS 29.165 v11.5.0 (2012-12) with the following changes applies.

3GPP TS 24.229 [5] defines the methods allowing an IBCF to interconnect to an IBCF placed in another IM CN subsystem.

The following SIP methods are supported on the NNI as defined in Table 7.2

The following table is based on table A.5 and table A.163 of 3GPP TS 24.229 [5] and endorsed for this document:

Table 7. 2 - Supported SIP methods

Item	*Method*	*Ref.*	*IP-NNI*	
			Sending	*Receiving*
1	*ACK request*	*IETF RFC 3261 [13]*	*m*	*m*
2	*BYE request*	*IETF RFC 3261 [13]*	*m*	*m*
3	*BYE response*	*IETF RFC 3261 [13]*	*m*	*m*
3	*BYE response*	*IETF RFC 3261 [13]*	*m*	*m*
4	*CANCEL request*	*IETF RFC 3261 [13]*	*m*	*m*
5	*CANCEL response*	*IETF RFC 3261 [13]*	*m*	*m*
5A	*INFO request*	*IETF RFC 6086 [39]*	*o*	*o*
5B	*INFO response*	*IETF RFC 6086 [39]*	*o*	*o*
8	*INVITE request*	*IETF RFC 3261 [13]*	*m*	*m*
9	*INVITE response*	*IETF RFC 3261 [13]*	*m*	*m*
9A	*MESSAGE request*	*IETF RFC 3428 [19]*	*o*	*o*
9B	*MESSAGE response*	*IETF RFC 3428 [19]*	*o*	*o*
10	*NOTIFY request*	*IETF RFC 3265 [20]*	*oo*	*oo*
11	*NOTIFY response*	*IETF RFC 3265 [20]*	*oo*	*oo*
12	*OPTIONS request*	*IETF RFC 3261 [13]*	*x1*	*x1*
13	*OPTIONS response*	*IETF RFC 3261 [13]*	*x1*	*x1*
14	*PRACK request*	*IETF RFC 3262 [18]*	*m*	*m*
15	*PRACK response*	*IETF RFC 3262 [18]*	*m*	*m*
15A	*PUBLISH request*	*IETF RFC 3903 [21]*	*oo*	*oo*
15B	*PUBLISH response*	*IETF RFC 3903 [21]*	*oo*	*oo*
16	*REFER request*	*IETF RFC 3515 [22]*	*o*	*o*
17	*REFER response*	*IETF RFC 3515 [22]*	*o*	*o*
18	*REGISTER request*	*IETF RFC 3261 [13]*	*n/an/a*	*n/an/a*
19	*REGISTER response*	*IETF RFC 3261 [13]*	*n/an/a*	*n/an/a*
20	*SUBSCRIBE request*	*IETF RFC 3265 [20]*	*oo*	*oo*
21	*SUBSCRIBE response*	*IETF RFC 3265 [20]*	*oo*	*oo*
22	*UPDATE request*	*IETF RFC 3311 [23]*	*m*	*m*
23	*UPDATE response*	*IETF RFC 3311 [23]*	*m*	*m*
on/aNOTE: In the above table, m, o and c and n/a have the meanings indicated in table 7.1. *x1: Support of OPTIONS in a SIP dialog is mandatory, where support of OPTIONS out of a SIP dialog is optional. Use of OPTIONS outside the dialogue may be used as a keep alive mechanism only based on bilateral agreement.*				

7.1.2 SIP Header Fields

7.1.2.1 General

For the purpose of the present document clause 6.1.1.3.0 of TS 29.165 v11.5.0 (2012-12) applies as follows:

The IBCF shall provide the capabilities to manage and modify SIP header fields according to subclause 5.10 and Annex A of 3GPP TS 24.229 [5] with modifications as described in the following subclauses.

7.1.2.2 Trust & No Trust Relationship

For the purpose of the present document clause 6.1.1.3.1 of TS 29.165 v11.5.0 (2012-12) applies with the following changes of Table 7.3 as follows:

The IBCF acting as exit point applies the procedures described in clause 5.10.2 of 3GPP TS 24.229 [5] before forwarding the SIP signalling to the IBCF acting as entry point. The IBCF acting as entry point applies the procedures described in clause 5.10.3 of 3GPP TS 24.229 [5].

Additionally, in case there is no trust relationship between the two IM CN subsystems connected by NNI, the IBCF acting as exit point applies the procedures described in clause 4.4 of 3GPP TS 24.229 [5], before forwarding the SIP signalling.

These procedures may be utilized on a per header field basis to realize overall trust as well as per service level screening of header fields. Trust relationships and trust domains may be defined by inter-operator agreements for individual services and/or individual SIP header fields.

The management of the SIP header fields (if present) over NNI in case of a presence or not of a trust relationship between the two interconnected IM CN subsystems is wrapped up in the following table.

Table 7. 3 - Management of SIP header fields over NNI in presence or not of a trust relationship

Item	*Header field*	*Reference*	*Trust relationship*	*Not trust relationship*
1	*P-Asserted-Identity*	*IETF RFC 3325 [44]*	*As specified in 3GPP TS 24.229 [5], clause 4.4 (NOTE 5)*	*As specified in 3GPP TS 24.229 [5], clause 4.4 (NOTE 5)*
2	*P-Access-Network-Info* (NOTE 2)	*IETF RFC 3455 [24]*	*As specified in 3GPP TS 24.229 [5], clause 4.4*	*As specified in 3GPP TS 24.229 [5], clause 4.4*
3	*Resource-Priority*	*IETF RFC 4412 [78]*	As specified in 3GPP TS 24.229 [5], clause 4.4	As specified in 3GPP TS 24.229 [5], clause 4.4
4	*History-Info*	*RFC 4244 [25]*	*As specified in 3GPP TS 24.229 [5], clause 4.4*	*As specified in clause 4.3.3 of RFC 4244 [25] and in 3GPP TS 24.229 [5], clause 4.4*
5	*Reason (in a response)*	*IETF RFC 6432 [49]*	*As specified in 3GPP TS 24.229 [5], clause 4.4*	*As specified in 3GPP TS 24.229 [5], clause 4.4*
6	*P-Early-Media*	*IETF RFC 5009 [74]*	*As specified in 3GPP TS 24.229 [5], clause 4.4*	

NNINOTE 2: This header field is only applicable on a roaming NNI whereas for the interconnect NNI it is left unspecified.
NOTE 3: In addition, value-dependent operator policies may be applied.
NOTE 4: This header field is not applicable at NNI.
NOTE 5: The handling of the URI parameters "cpc" and "oli", defined in 3GPP TS 24.229 [5] subclause 7.2A.12, is specified in 3GPP TS 24.229 [5], clause 4.4.

Items stroke out in the table above are not in scope of this i3 Forum Release, and items underlined are modifications or additions.

7.1.2.3 Derivation of Applicable SIP Header Fields from 3GPP TS 24.229 [5]

For the purpose of the present document clause 6.1.1.3.2 of TS 29.165 v11.5.0 (2012-12) applies as follows:

For any method in table 7.1, the SIP header fields applicable on the NNI are detailed in the corresponding method tables for the UA role and proxy role sending behavior in Annex A of 3GPP TS 24.229 [5]. Unless other information is specified in the normative part of the present specification, the applicability of header fields at the NNI can be derived for each method from the corresponding tables in annex A of 3GPP TS 24.229 [5] as follows:

- *All header fields not present in the corresponding tables in Annex A of 3GPP TS 24.229 or marked as "n/a" in both the "RFC status" and "profile status" columns for the UA role and proxy role sending behaviour of that tables are not applicable at the NNI.*

NOTE 1: Operators could choose to apply header fields for other SIP extensions on an NNI based on bilateral agreements, but this is outside the scope of the present specification.

- *All header fields which are marked as "o" in at least one of the "RFC status" or the "profile status" profile columns for the sending behaviour in the corresponding UA role and proxy role tables in annex A of 3GPP TS 24.229 [5] and as "n/a" or "o" in the other such columns are applicable at NNI based on bilateral agreement between operators.*
- *All header fields which are marked as "m" in at least one of the "RFC status" or the "profile status" columns for the sending behaviour in the corresponding UA role or proxy role table in annex A of 3GPP TS 24.229 [5] and as "n/a", "o", or "m" in the other such columns are applicable at the NNI.*
- *If conditions are specified, they are also applicable at the NNI and the above rules are applicable to the "n/a", "o" and "m" values within the conditions.*

NOTE 2: In the above rules, the RFC profile columns are taken into account in order to enable interworking with non-3GPP networks,

7.1.2.4 Applicability of SIP Header Fields on a Non-Roaming NNI

For the purpose of the present document clause 6.1.1.5 of TS 29.165 v11.5.0 (2012-12) applies as follows:

The following SIP header fields are only applicable on a non-roaming NNI or for the loopback traversal scenario:

- *P-Refused-URI-List*

7.1.2.5 Modes of Signalling

Enbloc signaling MUST be supported.

7.1.3 SDP Protocol

7.1.3.1 General

For the purpose of the present document clause 6.1.2.1 of TS 29.165 v11.5.0 (2012-12) applies as follows:

The functional entity closest to the border of an NNI (see reference model in Clause 5) shall provide the capabilities specified for that network element in Annex A.3 of 3GPP TS 24.229 [5].

The SDP bodies shall be encoded as described in IETF RFC 3261 [13] and in IETF RFC 4566 [147]. The offer/answer model with the SDP as defined in IETF RFC 3264 [146] shall be applied.

7.1.4 Major Capabilities

For the purpose of the present document clause 6.1.3 of TS 29.165 v11.5.0 (2012-12) applies with the following changes in Table 7.4 and Table 7.5. as follows:

This subclause contains the major capabilities to be supported over the NNI.

The table 7.4 specifies which capabilities are applicable for NNI. The profile status codes within table 7.4 are defined in table 6.1.3.2. For the "Basic SIP" capabilities part of table 6.1.3.1, the last column "Profile status over NNI" specifies the general status of applicability of the IETF RFC 3261 [13] main mechanisms described in the 2nd column "Capability over the Ici".

For the "Extensions to basic SIP" capabilities part, the last column "Profile status over NNI" specifies the general status of applicability of the RFC referenced in the 2nd column "Capability over the Ici". If necessary, the applicability of RFCs at the NNI level is further detailed in the present Technical Specification.

The columns "Reference item in 3GPP TS 24.229 [5] for the profile status" provide informative references for comparison purposes into the UA and Proxy role major capabilities tables in 3GPP TS 24.229 [5], where the capabilities are defined via additional references.

Table 7. 4 - Major capabilities over NNI

Item	***Capability over the Ici***	***Profile status over IP-NNI***
	Basic SIP (IETF RFC 3261 [13])	
1	*registrations*	*n/a*
2	*initiating a session*	*m*
3	*terminating a session*	*m*
4	*General proxy behaviour*	*n/a*
5	*Managing several responses due to forking*	*m*
6	*support of indication of TLS connections in the Record-Route header*	*n/a*
7	*Support of authentication*	*n/a*
8	*Timestamped requests (Timestamp header field)*	*m*
9	*Presence of date in requests and responses (Date header field)*	*m*
10	*Presence of alerting information data (Alert-info header field)*	*o*
11	*Support and handling of the Require header field for REGISTER and other requests or responses for methods other than REGISTER*	*m*
12	*Support and reading of the Supported and Unsupported header fields*	*m*
13	*Support of the Error-Info header field in 3xx - 6xx responses*	*o*
14	*Support and handling of the Organization header field*	*m*
15	*Support and handling of the Call-Info header field*	*m*
16	*Support of the Contact header field in 3xx response*	*m*
16A	*Proxy reading the contents of a body or including a body in a request or response*	*n/a*
	Extensions to basic SIP	
16B	*3GPP TS 24.237 [131]: proxy modifying the content of a body*	*n/a*
17	*IETF RFC 6086[39]: SIP INFO method and package framework*	*o*
17A	*IETF RFC 6086 [39]: legacy INFO usage*	*o*
18	*IETF RFC 3262 [18]: reliability of provisional responses in SIP (PRACK method)*	*m*
19	*IETF RFC 3515 [22]: the SIP REFER method*	*o*
20	*IETF RFC 3312 [40] and RFC 4032 [41]: integration of resource management and SIP (Preconditions framework)*	*o*
21	*IETF RFC 3311 [23]: the SIP UPDATE method*	*m*
22	*IETF RFC 3313 [42]: SIP extensions for media authorization (P-Media-Authorization header field)*	*m*
23	*IETF RFC 3265 [20]: SIP specific event notification (SUBSCRIBE/NOTIFY methods)*	*o*
24	*IETF RFC 3327 [43]: session initiation protocol extension header field for registering non-adjacent contacts (Path header field)*	*n/a*
25	*IETF RFC 3325 [44]: private extensions to the Session Initiation Protocol (SIP) for network asserted identity within trusted networks*	*c4*
26	*IETF RFC 3325 [44]: the P-Preferred-Identity header field extension*	*n/a*
27	*IETF RFC 3325 [44]: the P-Asserted-Identity header field extension*	*m*
28	*IETF RFC 3323 [34]: a privacy mechanism for the Session Initiation Protocol (SIP) (Privacy header field)*	*m*
29	*IETF RFC 3428 [19]: a messaging mechanism for the Session Initiation Protocol (SIP) (MESSAGE method)*	*o*
30	*IETF RFC 3608 [45]: session initiation protocol extension header field for service route discovery during registration (Service-Route header field)*	*n/a*
31	*IETF RFC 3486 [46]: compressing the session initiation protocol*	*n/a*
32	*IETF RFC 3455 [24]: private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP)*	*o*
32A	*IETF RFC 3325 [44]: act as first entity within the trust domain for asserted identity*	*n/a*
32B	*IETF RFC 3325 [44]: act as entity within trust network that can route outside the trust*	*n/a*

	network	
32C	*IETF RFC 3325: act as entity passing on identity transparently independent of trust domain*	*n/a*
33	*IETF RFC 3455 [24]: the P-Associated-URI header field extension*	*n/a*
34	*IETF RFC 3455 [24]: the P-Called-Party-ID header field extension*	*n/a*
35	*IETF RFC 3455 [24]: the P-Visited-Network-ID header field extension*	*n/a*
36	*IETF RFC 3455 [24]: the P-Access-Network-Info header field extension*	*c4*
37	*IETF RFC 3455 [24]: the P-Charging-Function-Addresses header field extension*	*n/a*
38	*IETF RFC 3455 [24]: the P-Charging-Vector header field extension*	*m*
39	*IETF RFC 3329 [47]: security mechanism agreement for the session initiation protocol*	*n/a*
39A	*draft-dawes-dispatch-mediasec-parameter-03 [137]: Capability Exchange for Media Plane Security*	*n/a*
40	*IETF RFC 3326 [48]: the Reason header field for the session initiation protocol*	*m*
41	*IETF RFC 6432 [49]: carrying Q.850 codes in reason header fields in SIP (Session Initiation Protocol) responses*	*c4*
42	*IETF RFC 3581 [50]: an extension to the session initiation protocol for symmetric response routeing*	*o*
43	*IETF RFC 3841 [51]: caller preferences for the session initiation protocol (Accept-Contact, Reject-Contact and Request-Disposition header fields)*	*m*
44	*IETF RFC 3903 [21]: an event state publication extension to the session initiation protocol (PUBLISH method)*	*o*
45	*IETF RFC 4028 [52]: SIP session timer (Session-Expires and Min-SE headers)*	*m*
46	*IETF RFC 3892 [53]: the SIP Referred-By mechanism*	*m*
47	*IETF RFC 3891 [54]: the Session Initiation Protocol (SIP) "Replaces" header*	*o*
48	*IETF RFC 3911 [55]: the Session Initiation Protocol (SIP) "Join" header*	*o*
49	*IETF RFC 3840 [56]: the callee capabilities*	*o*
50	*IETF RFC 4244 [25]: an extension to the session initiation protocol for request history information (History-Info header field)*	*o*
51	*IETF RFC 5079 [57]: Rejecting anonymous requests in the session initiation protocol*	*o*
52	*IETF RFC 4458 [58]: session initiation protocol URIs for applications such as voicemail and interactive voice response (NOTE 3)*	*o*
53	*IETF RFC 4320 [59]: Session Initiation Protocol's (SIP) non-INVITE transactions*	*m*
54	*IETF RFC 4457 [60]: the P-User-Database private header field extension*	*n/a*
55	*IETF RFC 5031 [61]: a uniform resource name for services*	*n/a*
56	*IETF RFC 5627 [62]: obtaining and using GRUUs in the Session Initiation Protocol (SIP)*	*o*
	Void	
58	*IETF RFC 4168 [27]: the Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)*	*o*
59	*IETF RFC 5002 [64]: the SIP P-Profile-Key private header field extension*	*n/a*
60	*IETF RFC 5626 [65]: managing client initiated connections in SIP*	*o*
61	*IETF RFC 5768 [66]: indicating support for interactive connectivity establishment in SIP*	*n/a*
62	*IETF RFC 5365 [67]: multiple-recipient MESSAGE requests in the session initiation protocol*	*o if 29, else n/a*
63	*draft-ietf-sipcore-location-conveyance-08 [68]: SIP location conveyance (Geolocation header)*	*m*
64	*IETF RFC 5368 [69]: referring to multiple resources in the session initiation protocol*	*o if 19, else n/a*
65	*IETF RFC 5366 [70]: conference establishment using request-contained lists in the session initiation protocol*	*o*
66	*IETF RFC 5367 [71]: subscriptions to request-contained resource lists in the session initiation protocol*	*o if 23, else n/a*
67	*IETF RFC 4967 [72]: dialstring parameter for the session initiation protocol uniform resource identifier*	*n/a*

68	*IETF RFC 4964 [73]: the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular*	*o*
69	*IETF RFC 5009 [74]: the SIP P-Early-Media private header field extension for authorization of early media*	*c4*
70	*IETF RFC 4694 [75]: number portability parameters for the 'tel' URI*	*o*
72	*IETF RFC 4411 [77]: extending the session initiation protocol Reason header for preemption events*	*o*
73	*IETF RFC 4412 [78]: communications resource priority for the session initiation protocol? (Resource-Priority header field)*	*o*
74	*IETF RFC 5393 [79]: addressing an amplification vulnerability in session initiation protocol forking proxies*	*m*
75	*IETF RFC 5049 [80]: the remote application identification of applying signalling compression to SIP*	*n/a*
76	*IETF RFC 5688 [81]: a session initiation protocol media feature tag for MIME application sub-types*	*o*
77	*IETF RFC 6050 [26]: Identification of communication services in the session initiation protocol*	*o*
78	*IETF RFC 5360 [82]: a framework for consent-based communications in SIP?*	*o*
79	*draft-johnston-sipping-cc-uui-09 [83]: transporting user to user information for call centers using SIP?*	*o*
79A	*draft-ietf-cuss-sip-uui-isdn [83A]: Interworking ISDN Call Control User Information with SIP*	*o*
80	*draft-vanelburg-dispatch-private-network-ind-01 [84]: The SIP P-Private-Network-Indication private-header (P-Header)*	*o*
81	*IETF RFC 5502 [85]: the SIP P-Served-User private header*	*n/a*
83	*draft-dawes-sipping-debug-04 [87]: the P-Debug-ID header extension*	*o*
84	*IETF RFC 6228 [88]: the 199 (Early Dialog Terminated) response code*	*m*
85	*IETF RFC 5621 [89]: message body handling in SIP*	*m*
86	*IETF RFC 6223 [90]: indication of support for keep-alive*	*o*
87	*IETF RFC 5552 [91]: SIP Interface to VoiceXML Media Services*	*n/a*
88	*IETF RFC 3862 [92]: common presence and instant messaging (CPIM): message format*	*o*
89	*IETF RFC 5438 [93]: instant message disposition notification*	*o*
90	*IETF RFC 5373 [94]: requesting answering modes for SIP (Answer-Mode and Priv-Answer-Mode header fields)*	*o*
	Void	
92	*IETF RFC 3959 [96]: the early session disposition type for SIP*	*o*
93	*IETF RFC 4244 [97]: delivery of Request-URI targets to user agents*	*n/a*
94	*draft-kaplan-dispatch-session-id-00 [124]: The Session-ID header*	*o*
95	*IETF RFC 6026 [125]: correct transaction handling for 200 responses to Session Initiation Protocol INVITE requests*	*m*
96	*IETF RFC 5658 [126]: addressing Record-Route issues in the Session Initiation Protocol (SIP)*	*o*
97	*IETF RFC 5954 [127]: essential correction for IPv6 ABNF and URI comparison in IETF RFC 3261 [13]*	*m*
98	*IETF RFC 4488 [135]: suppression of session initiation protocol REFER method implicit subscription*	*m if 19, else n/a*
99	*draft-ietf-salud-alert-info-urns [136]: Alert-Info URNs for the Session Initiation Protocol*	*o*
100	*Subclause 3.1 of 3GPP TS 24.229: multiple registrations*	*n/a*
101	*IETF RFC 5318 [141]: the SIP P-Refused-URI-List private-header*	*c5*
102	*IETF RFC 4538 [140]: request authorization through dialog Identification in the session initiation protocol (Target-Dialog header field)*	*o*
103	*draft-holmberg-sipcore-proxy-feature [143]: indication of features supported by proxy*	*o*
104	*IETF RFC 6140: registration of bulk number contacts*	*n/a*

105	*IETF RFC 6230: media control channel framework*	*o*
105A	*3GPP TS 24.229 [5]: S-CSCF restoration procedures*	*n/a*
106	*RFC 6357 [164] SIP overload control*	*m*
107	*draft-ietf-soc-overload-control [165] feedback control*	*m*
c4: m in case of trust relationship between the interconnected networks, else n/a *c5: o in case of non-roaming NNI and loopback traversal scenario, else n/a* *NOTE 1: The item numbering corresponds to the one provided in table A.4 in [5].* *NOTE 2: The item numbering corresponds to the one provided in table A.162 in [5].* *NOTE 3: A common URI namespace is required to apply this feature on the NNI.* *NOTE i3F-1: Needed to support CONF service as specified within TS 24.147 [106] Section 5.3.1.5.3* *NOTE i3F-2:.* *Item 9: Date header is of no use for basic voice service, which is the scope of the document, as it is globally considered less reliable with regards to locally registered timestamp. Furthermore it's not commonly used for any post-processing (charging, reporting, …) so it's more appropriate to leave it as an optional item.* *Item 36; this capability is optional due to possible unsecure relationship via public Internet,* *Item: 44: as shown is Sec. 6.1.1.2.the PUBLISH method is out-of-scope at Interconnection NNI* *Item 45: SIP Session Timer as specified in RFC 4028 is meant to be an end-to-end per-session keepalive mech meaningless if there is any node (B2BUA, ASs,...) in the chain, re-generating SIP signalling so interrupting the sig it is common in real environments. It's more appropriate not to mandate it.*		

Table 7. 5 - Key to notation codes for major capabilities

Notation code	***Notation name***	***Explanation***
M	*mandatory*	*The capability shall be supported at NNI.* *SIP message relating to this capability shall be sent over the NNI if received from the serving network, unless they also make use of other unsupported capabilities.* *SIP headers or other information elements relating to this capability shall be passed over the NNI if received from the sending side.* *This does not imply that network elements inside the serving network or served network or user equipment connected to these networks shall support this capability.*
O	*optional*	*The capability may or may not be supported at NNI. The support of the capability is provided based on bilateral agreement between the operators (i.e. Service Provider and/or carriers according to i3Forum terminology).*
n/a	*not applicable*	*It is impossible to use/support the capability at the NNI.*
c <integer>	*conditional*	*The support of the capability ("m", "o" or "n/a") depends on the support of other optional or conditional items. <integer> is the identifier of the conditional expression.*

7.2 Control Plane Transport

The SIP protocol can be transported over UDP [31], TCP or SCTP. IETF RFC 3261 [17] defines that UDP is the default for SIP.

In the scope of this document UDP shall be used as default. If a non-reliable transport implementation is used then TCP may be used based on bilateral agreements.

There is also the possibility to use the newer transport protocol SCTP. Since support from vendors is not widely available at the date when this document is published, the use of SCTP is left as part of the specific bilateral agreement.*NNINNI.*

7.3 SIP Timers

The support of IETF RFC 4028 [21], which addresses SIP Timers specification, is optional. The carrier receiving the INVITE message shall comply with IETF RFC 3261 [17] section 16.8 if IETF RFC 4028 [21] is not supported**.**

8 Security

The VoIP traffic, from the border element in one carrier's domain to the border element in another carrier's domain, shall be secured, either physically or logically, from Internet Transit traffic. This security can be achieved:

- *physically*: by implementing separated and dedicated networks for the traffic.
- *logically*: by implementing mechanism such as Virtual Private Networks (either layer 2, e.g., VLANs, or layer 3, e.g., MPLS-VPN) and Tunneling (e.g. IP Sec).

Appendix A – Response Codes

(informative)

This annex documents the semantics for the common response codes that appear on the peering interface so an Carrier network that receives a response code from a peer will take the correct action.

Table A.1 lists response codes for some of the common call failures. For many of the 4xx error cases, the response code would only be generated for the stated condition if the call wasn't handled in some manner by the terminating Carrier network (e.g., call routed to voice mail).

Table A. 1 - Response Codes

Condition	Response Code	Example Action when Received
Endpoint is unavailable • UEUE powered down • UE removed from service by OS • Line in lockout	480 Temporarily Unavailable	Reorder tone, or announcement "Your call cannot be completed at this time. Please hang up and try again later."
Line is "busy" • Line doesn't have call waiting and is busy in a call • Line has call waiting, but is already busy with two calls, busy in an emergency call, is in a transient state with another call (ringing, origination glare, etc)	486 Busy Here	Busy tone
Call times out waiting for user action • Ringing timeout waiting for answer • Timeout waiting to accept call-waiting call • Timeout waiting for caller to enter digits after solicitor-call-blocking prompt	480 Temporarily Unavailable	Reorder tone, or announcement "Your call cannot be completed at this time. Please hang up and try again later."
Call blocked by a feature • Terminating call blocking • Do not disturb	403 Forbidden	Announcement: "Due to network difficulties, your call cannot be completed at this time. Please try your call again later."
Call blocked because called user not authorized to receive calls • Temporarily disconnected due to late payment • Recently deleted	404 Not Found	Announcement: "Your call cannot be completed as dialed. Please check the number and try again."
Call blocked due to resource limitation • No QoS • UE resource exhaustion (e.g., no DSP resources)	480 Temporarily Unavailable	Reorder tone, or announcement "Your call cannot be completed at this time. Please hang up and try again later."
Call Forward loop detected	Depends on type of call forwarding: • CFBL: 486 Busy Here • CFDA, CFV, SCF: 480 Temporary Failure	Reorder tone, or announcement "Your call cannot be completed at this time. Please hang up and try again later."

Condition	Response Code	Example Action when Received
During call-transfer, transfer-to user agent can't find dialog identified in Replaces header	481 Call/Transaction Doesn't Exist	Application dependent
Called endpoint can not support SDP offer • Does not support IP version in SDP c= line • Does not support any offered codec • Not authorized for authored media	488 Not Acceptable Here	Reorder, or announcement
Called address does not exist • Target routing number not owned by this network • Called user does not exist in this network	404 Not Found	Announcement: "Your call cannot be completed as dialed. Please check the number and try again."
Congestion encountered at the peering interface	503 Service Unavailable	Retry call via PSTN (see Section 6.5.2 for more details).

IPNNI- 2014-00083R14

Contribution

TITLE: IP Interconnection Routing Report

SOURCE*: Editor

ABSTRACT

This document provides a marked up version of the changes agreed to at the IP NNI Task Force 9/30/2014 Meeting.

Contributions Added:

- IPNNI-2014-00097R000
- IPNNI-2014-00100R001

NOTICE

* CONTACT:

ATIS-1000062

Technical Report on

IP Interconnection Routing

Alliance for Telecommunications Industry Solutions

Approved Month DD, YYYY

Abstract

As Service Providers introduce and expand IP-based service offerings, there is increasing interest in identifying the opportunities for the industry to facilitate IP routing of VoIP traffic using E.164 addresses. The ATIS/SIP Forum IP-NNI Task Force has taken on the initiative to develop a Technical Document and is publishing a draft report to describe the candidate proposals for circulation and comment. Recognizing that IP traffic exchange is developing as an overlay to existing TDM interconnection and will be implemented by different service providers with varying timelines, the purpose of this draft report is to:

1. Provide an overview of in-use and proposed architectures with the provisioning processes and calls flows to facilitate the exchange of VoIP traffic associated with IP-based services using E.164 addresses.
2. Present comparative characteristics that may be useful in understanding the approaches.
3. Consider how such in use and proposed solution(s) may be adopted and/or coexist, and evolve for transition to a future integrated registry envisioned at the FCC Numbering Testbed Workshop.

Foreword

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The [COMMITTEE NAME] Committee [INSERT MISSION]. [INSERT SCOPE].

The SIP Forum's mission is to advance the adoption of products and services based on the Session Initiation Protocol and to maintain and serve a global community of commercial SIP based service and technology providers. The primary goals of the SIP Forum are to foster interoperability and adherence to standardization efforts, and provide educational resources and a platform for productive communication among industry participants.

This document was developed by the ATIS/SIP Forum IP-NNI Task Force

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, [COMMITTEE NAME], 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, [COMMITTEE NAME], which was responsible for its development, had the following leadership:

[LEADERSHIP LIST]

The [SUBCOMMITTEE NAME] Subcommittee was responsible for the development of this document.

Table of Contents

[INSERT]

Table of Figures

[INSERT]

Table of Tables

[INSERT]

Technical Report on –

IP Interconnection Routing

1 Scope, Purpose, & Application

1.1 Scope

This document was developed under a joint ATIS/SIP Forum collaboration. The document discusses existing in-use and proposed routing solutions to facilitate the exchange of traffic associated with IP-based services between North American service providers.

Many options and issues were previously investigated by an ATIS Inter-Carrier VoIP Call Routing Focus Group (IVCR-FG), which issued its final report in February 2008. At that time, the IVCR-FG report noted that a number of vendor proposals have been made, but no initiative exists to develop the necessary standards needed to enable VoIP call interconnectivity [1].

The initial objectives of the ATIS/SIP Forum IP-NNI Task Force as memorialized in the agreement between ATIS and the SIP Forum included defining "the architecture and requirements for a shared "Thin" registry of NNI interconnection data." The Task Force was unable to reach consensus on a single registry architecture. Accordingly, this report summarizes the various proposals for IP interconnection routing that have been discussed by the Task Force, both registry and non-registry based, and how they may interoperate.

Subsequent to the formation of the ATIS/SIP Forum IP-NNI Task Force, the Federal Communications Commission authorized the creation of a Numbering Testbed to "spur the research and development of the next generation standards and protocols for number allocation, verification, and call routing."[2] The Commission also held a workshop to initiate a Numbering Testbed on March 25, 2014. Discussion at the Workshop focused on ideas for a "future integrated registry" that would support number allocation, verification, and call routing across all types of NANP numbers in a post TDM environment.

It should be noted that this initial report of the ATIS/SIP Forum IP-NNI Task Force report does not address the development of such an integrated registry, but instead focuses on the identification of existing in-use and proposed solutions to facilitate call routing across IP interconnections between now and the deployment of the future integrated registry envisioned at the Workshop.

1.2 Purpose

As Service Providers introduce and expand IP-based service offerings, there is increasing interest in identifying the opportunities for the industry to facilitate IP routing of VoIP traffic using E.164 addresses. The ATIS/SIP Forum IP-NNI Task Force has taken on the initiative to develop a Technical Report and is publishing a draft report to describe the candidate proposals for circulation and comment. Recognizing that IP traffic exchange is developing as an overlay to existing TDM interconnection and will be implemented by different service providers with varying timelines, the purpose of this draft report is to:

1. Provide an overview of in-use and proposed architectures with the provisioning processes and calls flows to facilitate the exchange of VoIP traffic associated with IP-based services using E.164 addresses.
2. Present comparative characteristics that may be useful in understanding the approaches.
3. Consider how such in use and proposed solution(s) may be adopted and/or coexist, and evolve for transition to a future integrated registry envisioned at the FCC Workshop.

Based upon the output and feedback on this draft report, further analysis will be required including but not limited to:

1. Refine solution(s) that includes consideration of feedback obtained from the draft report.

2. Detail how existing in-use and proposed interim solution(s) may be adopted and/or coexist, and evolve.
3. Finalize comparative characteristics

1.3 Application

This is a Technical Report.

2 References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[1] ATIS-I-0000017, ATIS Inter-Carrier VoIP Call Routing (IVCR) Assessment and Work Plan, February 2008

[X] FCC 14-5, January 2013

[2] ATIS-0x0000x, Technical Report.

[3] ATIS-0x0000x.201x, American National Standard.

[4] ATIS-1000039

[5] RFC 4904

[6] RFC 4694

[7] RFC 6116

[8] RFC 5067

3 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the ATIS Telecom Glossary, which is located at < http://www.atis.org/glossary >.

3.1 Definitions

For the purposes of this document the following descriptions apply

3.1.1 The Business Integrated Routing and Rating Database System (BIRRDS)- is a database system used for inputting service provider call routing/rating and interconnection information for all telephone numbers within the North American numbering plan. BIRRDS data is entered by Service Providers (SPs) and/or their agents. It consists of a collection of input databases from which the **LERG™ Routing Guide** is generated.

3.1.2 LERG™ Routing Guide - is the North American telecom industry's recognized, authoritative database used for the exchange of PSTN routing information that is obtained from BIRRDS.

3.1.3 Common Language® CLONES Database – is the authoritative database used for the development and exchange of Common Language Location Codes (CLLITM Codes) per ATIS-0300253, *Identification of Location Entities for the North American Telecommunications System*. CLONES reference data is used in BIRRDS/LERG for the identification of switch and interface locations.

3.1.4 NPAC –is the authoritative industry PSTN database for local number portability routing information as mandated by the FCC in 1996. It is currently administered by Neustar who was awarded the initial contract by the FCC. NPAC is governed by the NANC/LNPA Working Group which is a Federal Advisory Committee to the FCC.

3.2 Acronyms & Abbreviations

3GPP	3rd Generation Partnership Project
ALG	Application Level Gateway
ATCF	Access Transfer Control Function
B2BUA	Back to Back user agent
BIRRDS	Business Integrated Routing and Rating Database System
BGCF	Border Gateway Control Function
CSCF	Call Session Control Function
GSM	Global System for Mobile
IBCF	Interconnection Border Control Function
I-BGF	Interconnection Border Gateway Function
I-CSCF	Interrogating-Call Session Control Function
ICSS	IMS Centralized Services
II-NNI	Inter-IMS Network to Network Interface
IM-CN	IP Multimedia Core Networks
IMS	IP Multimedia Subsystem
IMS-ALG	Multimedia Subsystem Application Level Gateway
IP	Internet Protocol
IPSec	IP Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
LERG	Local Exchange Routing Guide
LTE	Long-Term Evolution
MGCF	Media Gateway Control Function
MGF	Media Gateway Function
MIME	Multipurpose Internet Mail Extensions
MSC	Mobile Switching Center
NAT	Network Address Translation
NAT-PT	Network Address Translation—Protocol Translation
NECA	National Exchange Carriers Association
NNI	Network to Network Interface
NPAC	Number Portability Administration Center
OCN	Operating Company Number
P-CSCF	Proxy Call Session Control Function
PE	Provider Edge
RTP	Real-Time Protocol
SBC	Session Border Controller

S-CSCF	Serving-Call Session Control Function
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SGF	Signalling Gateway Function
SIP	Session Initiation Protocol
SIP URI	SIP protocol Uniform Resource Identifier
SIP-I	SIP with encapsulated ISUP
SIP-T	SIP for Telephones
SLA	Service Level Agreement
SPID	Service Provider ID
SRVCC	Single Radio Voice Call Continuity
TCP	Transmission Control Protocol
tel-URI	Telephone Uniform Resource Identifier
TRF	Transit and Roaming Function
TrGw	Transition Gateway
TLS	Transport Layer Security
UA	User Agent
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
VoIP	Voice over IP
VoLTE	Voice of LTE

4 Aggregate Approaches Based on Existing NANP Data Structures

Some service providers are already exchanging voice traffic over IP facilities. This section details how routing for such exchanges has been implemented based on existing data in the LERG and NPAC supplemented with the bilateral exchange of information to map LERG and/or NPAC identifiers to IP connection information.

Existing approaches to IP interconnection routing discussed in this Section rely on NANP constructs that already aggregate telephone numbers into groups and then associate a route (SBC URI or IP address) with the TN group. Common methods of aggregation are Location Routing Number (LRN) in the NPAC, and OCNs, CLLIs, and central office codes (NPA-NXXs) in the LERG.

4.1 In-Use Method Using Existing LERG & NPAC Data

4.1.1 Introduction

This section describes how some SPs have already implemented an internal IP routing service using data available from the LERG and NPAC. This is possible because when SPs obtain numbering resources they are associated with the SP's OCN, the serving switch's CLLI code, an NPA-NXX, as well as a 10-digit LRN for those TNs which are ported or pooled. These "identifiers" are shared among SPs through existing NPAC and LERG feeds and no new industry systems development or standards were required to implement this solution. Sometimes referred to as the "aggregation method," the use of these existing identifiers to efficiently represent (or

aggregate) large groups of TNs significantly reduces the quantity of routing records, and avoids the need for SPs to provision multiple instances of the same routing data for each of its customers' TNs. During the development of the interconnection agreement, SPs exchange these "identifiers" (aka "TN group identifiers") and ingress SBC IP addresses to establish routes between their networks via an IP interconnection.

4.1.2 Use Cases

The makeup of an SP's switching infrastructure and the degree to which customer TNs are served via IP will influence which identifier(s) may be used to represent the groups of TNs to which traffic should be sent via an IP interconnect. The following use case examples are not intended to serve as an exhaustive list of possible scenarios:

- A SP may specify calls to all of their customers' TNs on all of their switches should be sent over an IP interconnection. Here, the SP can simply specify their Operating Company Number (OCN) as the identifier since all the TNs associated in the LERG and NPAC with their switches are related to their OCN. This is likely attractive if the SP is a VoIP provider or a cable company if all of their customers are served via IP.
- If an SP has specific switches to which calls should be sent via IP, they could simply identify those switches by their switch CLLI code. This is likely attractive for SPs with a mixed TDM and IP switching infrastructure that prefer traffic associated with certain or all of their IP switches be sent via an IP interconnect. Also, SPs transitioning their TDM interconnects to IP can manage the rate of transition by adding switch CLLI codes to the list of identifiers as it grows its IP interconnection capacity.
- The 10-digit LRN is a flexible vehicle for identifying a subset of TNs associated with a particular switch that, for example, serves both TDM and IP customer endpoints. Although SPs are required to establish at least one LRN per switch per LATA, they can create additional 10-digit LRNs to uniquely identify those TNs to which calls should be sent over an IP interconnection. This is likely attractive where one IP switch is used to serve both TDM and IP customer endpoints where the SP establishes second unique LRN to identify those TNs served via IP for which traffic should be sent over the IP interconnection. For example, an LTE wireless carrier may choose to establish unique LRNs to identify TNs belonging to VoLTE customers. Another example is where a CLEC provides TNs to an OTT VoIP provider and creates a unique LRN to identify those TNs assigned to customers of the OTT VoIP provider (that should be sent via and IP interconnection).

Below is a table summarizing the group of TNs represented by a "group identifier" as described in the above examples:

Group Identifier	Group of TNs Represented By the Identifier
OCN	All TNs associated with all SP switches
Switch CLLI	All TNs associated with an single SP's switch
LRN	A subset of TNs associated with a single switch
NPA-NXX	A subset of TNs associated with a single switch

4.1.3 Implementation

Many SP core networks are IP based and utilize an internal "routing service" to determine how to forward service requests. SIP redirect and DNS capabilities common in IP core networks provide the basic building blocks to implement real-time call processing for external NNI routing applications using "group identifiers." This solution can be accommodated by commercially available routing (DNS and ENUM) infrastructure and each SP is free to determine when and how to implement a "routing service" solution appropriate for their business and operational needs. SPs have options given vendors are actively engaged in providing solutions of this nature and the following general description is provided for illustrative purposes only.

4.1.4 Provisioning

A Provisioning diagram is shown below in Figure 4.1:

In this provisioning example, SP1 provisions its Routing Service and DNS based upon information provided by SP2. In this example, group identifiers (LRNs) are correlated with SBC interconnect IP addresses and domain names provided by SP2.

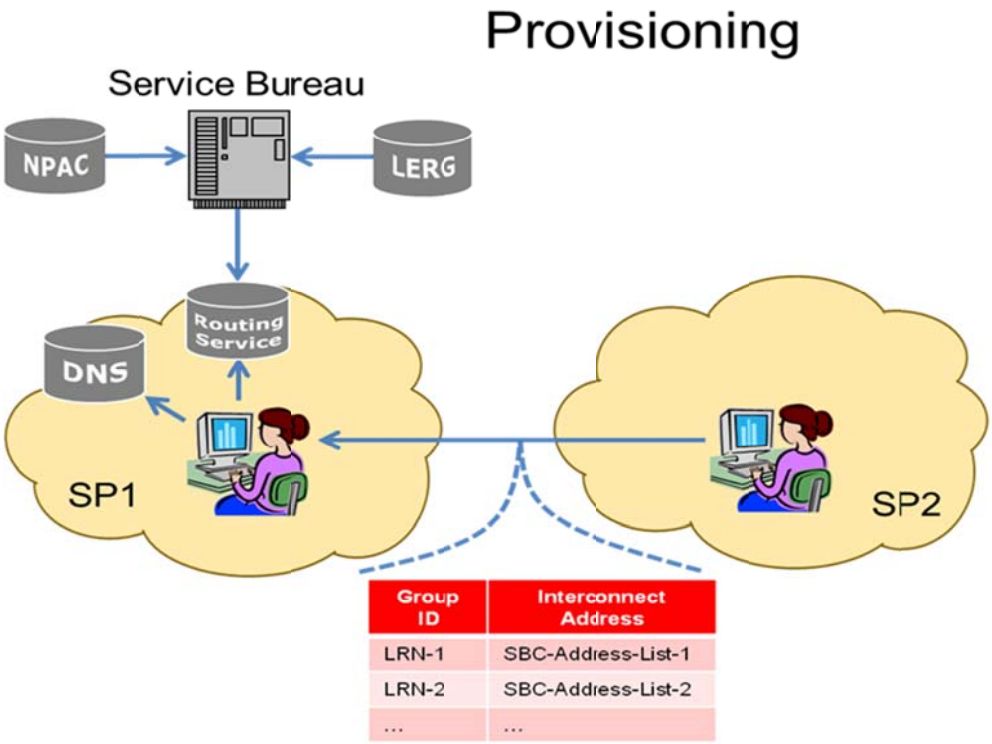

Figure 4. 1 - Provisioning - In-Use Method Using Existing LERG and NPAC Data

4.1.5 Call Flow

One example of the Call Flow is shown below in Figure 4.2. Other methods of implementation are also consistent with this approach:

1. Pat (non-roaming subscriber of SP1) makes a session request (e.g., places a call) to Mike (subscriber of SP2). SP1's network provides originating services based on Pat's subscription.
2. SP1's application server queries its routing service in real time using the called number to determine how to forward the request. The routing service first portability corrects the called number, and then determines that it is not subscribed to SP1. It then checks to see whether a group identifier is associated with the telephone number and covered by an IP interconnection agreement. If so, the SP1 routing service supplies[1] the application server with the ingress point through which SP2 has requested that session requests directed to members of this group enter its network.

[1] How this is accomplished is implementation specific. Messages from an application server to a routing service is typically an ENUM query, but in some networks a SIP message is sent to a proxy collocated with the ENUM service, which sends back a 302 "redirect" response.

3. The application server identifies SBC-2 and (if applicable) SBC-1 in SIP ROUTE headers, and forwards the resulting session request onward. SP 1's L3 processing resolves the host portion of the topmost ROUTE header (using DNS) to the IP address of SBC-1.
4. SBC-1 removes the topmost ROUTE header (which identifies itself) and forwards the session request based on the next one (which identifies SBC-2). To do so it resolves (using DNS) the host portion of that header, yielding the IP address of SBC-2.
5. SBC-2 removes the topmost ROUTE header (which identifies itself) and admits the message to SP2's network, forwarding it to an application server, and eventually to Mike. How SP2 performs these functions is SP specific.

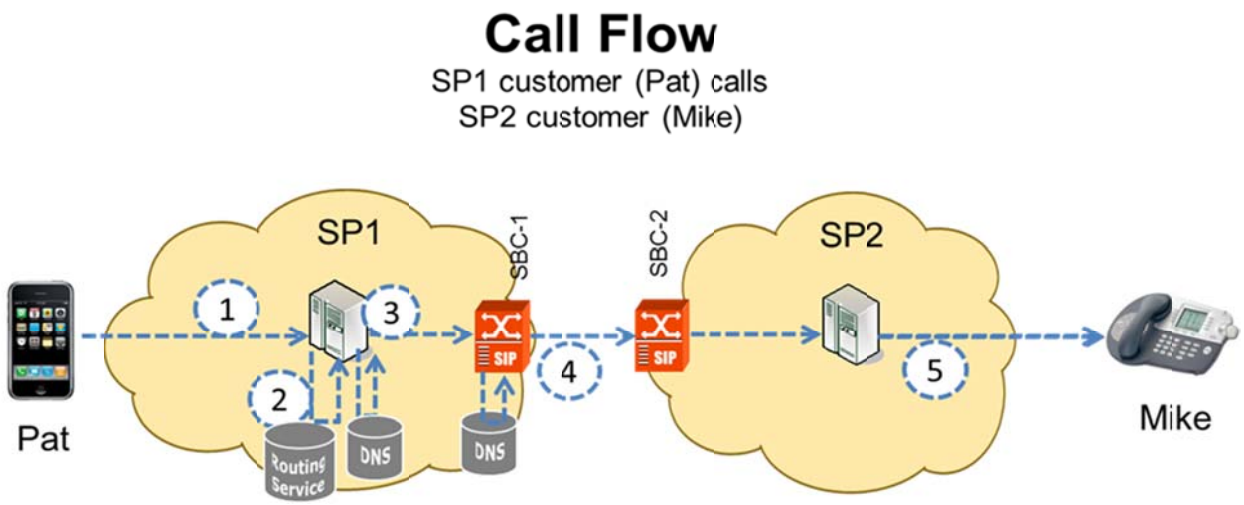

Figure 4. 2 - Call Flow -In-Use Method Using Existing LERG and NPAC Data

4.2 In-Use Method with LERG Enhancements

This section describes the exchange of data for IP routing and interconnection using existing industry database systems, architectures and processes, with LERG enhancements as needed for routing of E.164 Addressed Communications over IP Network-to-Network Interconnection (NNI).

This approach would allow existing downstream systems and processes to be utilized and enhanced, as may be needed, with minimal impact to service providers. The LERG and NPAC have evolved since their inception to support new technologies and industry processes. These systems have embedded governance processes that allow the industry to facilitate system process enhancements as required by service providers. Consequently, a solution to utilize existing database systems would allow the industry to continue to manage process evolution as it pertains to IP routing and interconnection within established industry forums that are proven, efficient, cost effective, and are balanced across industry segments.

Utilizing LERG for support of IP interconnection could maintain consistency of data exchange across the multi-carrier ecosystem. Additionally, utilization of the LERG routing data allows the originating provider to retain control of egress route selection through management of its own translations and routing tables.

Service providers can continue to leverage NPAC and existing Local Number Portability (LNP) system processes, such as Service Order Administration (SOA) and the LSMS framework, with minimal impact to their business processes for ported and pooled numbers that are serviced by IP technology.

The existing industry framework supports the evolution of TDM to IP routing and interconnection, however, existing database systems would need to be enhanced according to the industry requirements. The following items require further study and are possible areas of enhancement to these industry databases in support of IP routing for both PSTN transition and all IP networks. Upon industry consensus, BIRRDS/LERG can be enhanced to support:

- service provider exchange of Uniform Resource Identifier (URI) to identify I-SBCs (session border controllers) or other IP interconnect equipment.
- service provider exchange of location data for I-SBCs or other IP interconnect equipment. For example, Session Border Controller Location Entities could still be specified per ATIS-0300253, Identification of Location Entities for the North American Telecommunications and exchanged between service providers.
- a process for service providers to exchange service types and attribute parameters (e.g., Classes of Service, CODEC capabilities, Transcode Free Operation (TrFO), facsimile support, etc.) that are associated with a specific Session Border Controller (SBC)/IP interconnection point. This can be similar to the current process in BIRRDS/LERG to identify TDM switch attributes known as Switch Office Functionality indicators (SOFs).
- a process for flagging specific LRNs, as defined by the service provider, to be "related to" IP interconnection.
- a process to support service provider exchange of per service type (e.g., SIP, PSTN, mailto, etc.) Uniform Resource Identifier (URI) and parameter exchange.
- a process to exchange potential PSTN and IP routes simultaneously.
- a process to retain policy control for selection of primary and alternate egress routes and all the associated business processes.
- a process to validate Domain Names and potentially full URIs associated with an IP interconnection point prior to accepting such routing information for exchange.
- a process to have routing/interconnection database systems support alternative number conservation methods (e.g., use of 100 or other number block sizes); BIRRDS/LERG can be enhanced to meet this need, all while maintaining compatibility with routing on existing NPA/NXX and thousands blocks assignments. Support for a "Just In Time" number allocation model at a single TN level warrants further evaluation; however, in that case an industry requirement for coexistence with block level assignments should also be evaluated.
- more frequent routing data exchanges than daily, then BIRRDS/LERG can be enhanced to meet this need.

4.2.1 Call Flow

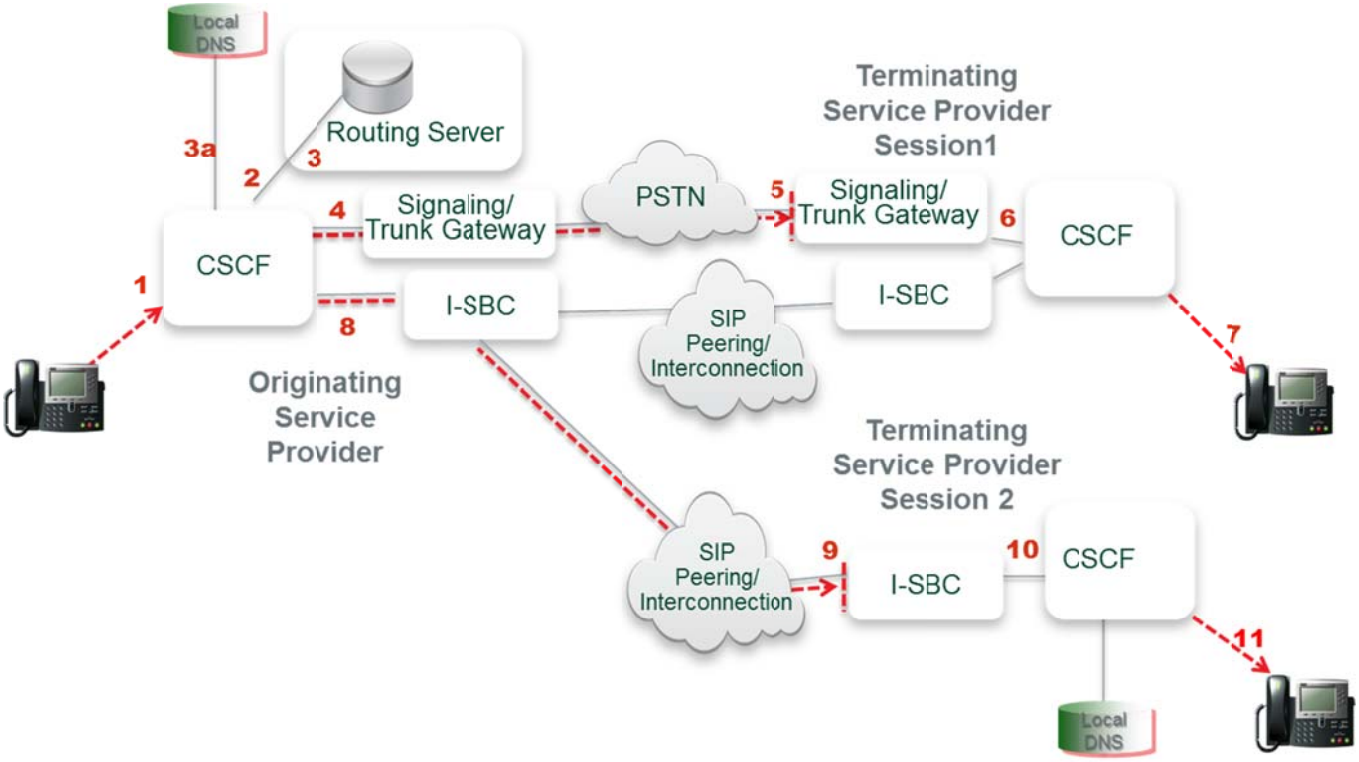

Figure 4. 3 - Call Flow – In-Use Method using LERG Enhancements

Session 1 – IP Session via PSTN Interconnection

(1) A session is originated and sent to the Call Session Control Function (CSCF).

(2&3) The CSCF performs an internal query to its routing server to retrieve routing data for the called number.

(4) If the CSCF determines that the called number requires interconnection via the PSTN to Terminating Service Provider 1, then the session is routed to the appropriate trunk gateway where it is converted to TDM.

(5) The session is routed internally to the trunk gateway and point of interconnection for Terminating Service Provider 1. The call is converted back to IP within the terminating service provider network.

(6&7) Terminating Service Provider 1 then signals the terminating CSCF to complete the call. Terminating Service Provider 1 may be an IP network but the means of interconnection is still via the PSTN. It is probable, per the illustration, that the terminating service provider offers both media gateways and I-SBCs to accept sessions during the IP transition phase.

Session 2 – IP Session via IP-IP Interconnection

(1) A session is originated and sent to the Call Session Control Function (CSCF).

(2) The CSCF performs an internal query to its routing server to retrieve routing data for the called number.

(3) The routing server returns a URI and the CSCF determines that the called number can accommodate an IP-NNI to the Terminating Service Provider,

(3a) The CSCF will then query its local DNS to resolve the URI to the IP address of the I-SBC of the terminating network.

(8) A SIP invite is sent to the egress I-SBC of the originating network that has connectivity to the ingress I-SBC of the terminating service provider.

(9) A SIP Invite is forwarded to the terminating service providers ingress I-SBC. Route selection is based on IP peering agreement between SPs as well as service attributes, least cost routing, etc.

(10&11) Terminating Service Provider 2 signals to the appropriate CSCF and the end-to-end session is established.

4.2.2 Provisioning

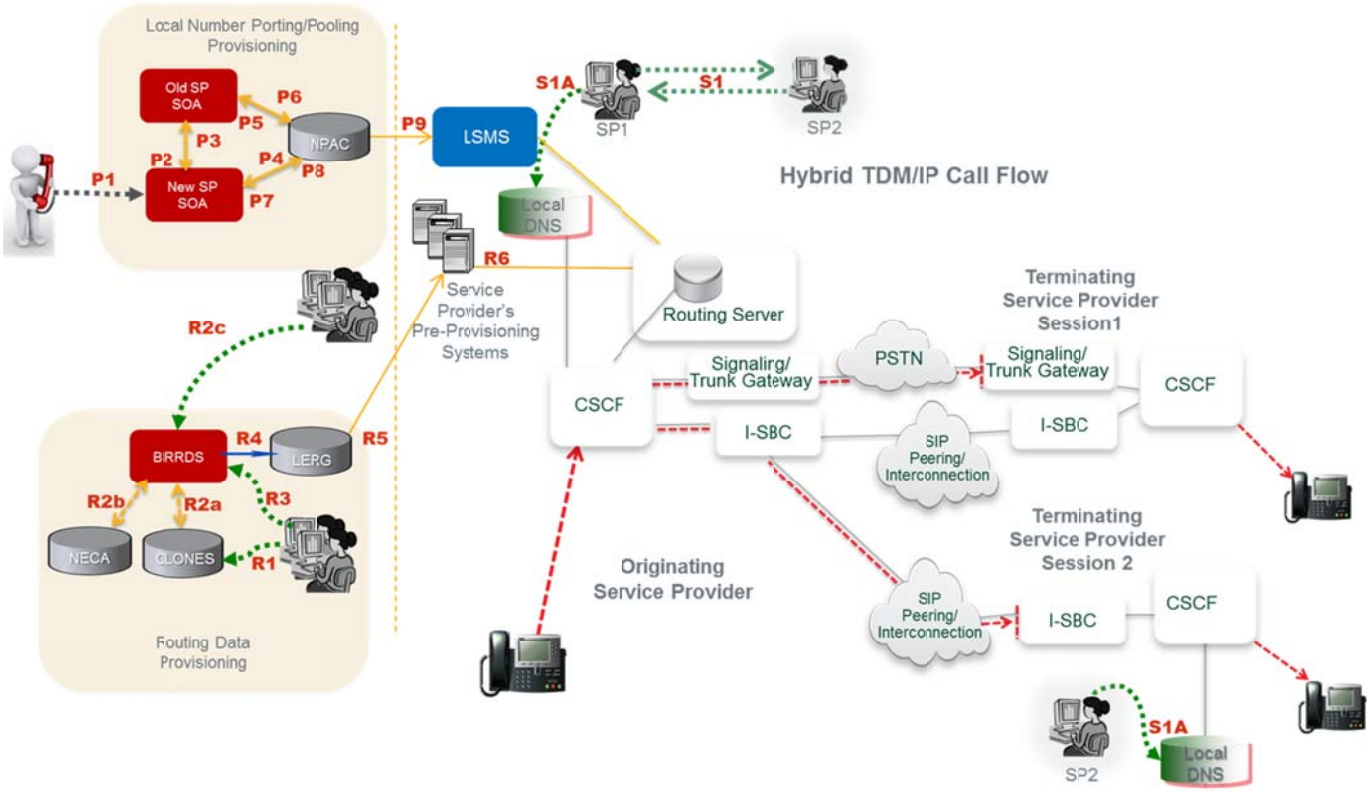

Figure 4. 4 - Provisioning – In-Use Method using LERG Enhancements

Routing Data Provisioning:

(R1) Service provider develops a switch/point-of-interface (POI) CLLI Code and associated location attributes in the CLONES database.

(R2a) The CLONES database provides newly developed CLLI Code and location reference data to BIRRDS. The location reference information is used by service providers in support of developing new BIRRDS switch/POI records.

(R2b) The National Exchange Carrier Association (NECA), provides new Company Codes (a subset of Operating Company Numbers (OCNs)), as they are assigned, to BIRRDS.

(R2c) National CO Code (NXX) Administrators and the Thousands-Block Pooling Administrator (US only) establish base CO Code and block assignment records in BIRRDS.

(R3) Service provider updates BIRRDS with switch/POI information (e.g., actual switch, points of interface, trunk gateways, call agents, Signaling Transfer Points (STPs), etc.), homing arrangements, Location Routing Numbers (LRNs), and detailed information supporting the CO Code NPA/NXX, NPA/NXX-X. This data is integrated with other BIRRDS data elements (e.g., Rate Centers) maintained by the BIRRDS administrator. URIs can potentially be associated with OCN, at the highest order, or can be associated with other LERG data, e.g., NPA-NXX level. The URI association would need to be agreed upon by the service providers.

(R4) The LERG is generated from current BIRRDS data and is provided to service providers monthly for their pre-provisioning systems. As an option, augmented daily activity may be provided nightly.

(R5) Based on service providers' local methods and procedures, the LERG data is loaded into service providers' pre-provisioning systems and is used for switch translations and routing.

(R6) Based on service providers' local methods and procedures, the LERG data in service providers' pre-provisioning systems is made accessible to switch translations engineers to configure the switch translation and routing tables.

Local Number Porting/Pooling Provisioning:

The following process involves a pre-port validation (PPV) process as well as an NPAC Service Order Administration (SOA) process.

(P1) A customer/subscriber requests to port his/her telephone number to the new/recipient service provider.

(P2) Pre-port validation - The new/recipient server provider requests validation of the port from the old /donor service provider.

(P3) Confirmation - verification of subscriber information is sent from the old/donor service provider to the new/recipient service provider.

(P4) The new/recipient service provider sends a creation of a pending port to NPAC.

(P5) NPAC sends a notification of port to the old/donor service provider.

(P6) An approval of the pending port is sent by the old/donor service provider to NPAC.

(P7) NPAC sends a notification of the old service provider's port approval to the new/ recipient service provider.

(P8) Activation of the port is sent from the new/recipient service provider to the NPAC.

(P9) NPAC broadcasts the new routing information for the port to the Local Service Management Systems (LSMSs) for all service providers to update their local databases – generally a service control point (SCP) or STP.

Service Provider Provisioning:

(S1) Service providers negotiate interconnection and exchange DNS Address (A/AAAA) records for their ingress interconnection POI's.

(S1A) Each service provider provisions the records received from the other service provider in its internal DNS. These IP addresses correspond to the destination service provider's I-SBCs that constitute the application layer POIs.

4.2.3 Summary

As industry requirements develop, and if they direct a solution to utilize existing database systems to support IP routing and interconnection information exchange, the capabilities of BIRRDS/LERG and NPAC database systems and their existing processes can be leveraged and enhanced to meet this need. There are several advantages for utilizing the existing database systems and infrastructure to support IP routing and interconnection. In particular, and at a minimum, this approach:

- Retains egress routing policy at the originating provider and allows QoS, least cost routing and other operational and commercial considerations to continue to play a role in determining primary and alternate routes for interconnection.
- Provides simultaneous PSTN and IP routes in an efficient manner should both options be available for a particular session including resiliency during the transition phase should one method be unavailable at a given moment.
- Leverages existing vehicles and processes for industry-wide routing information exchange of new IP parameters, URIs, and locations on a per service type basis.
- Avoids additional carrier overhead and costs that would result from adding network gear (hardware, software, and associated engineering, provisioning, monitoring, and security processes) for external

queries (e.g., ENUM) in per call/session setup. Likewise it avoids additional points of network failure and potential performance degradation.

- Can coexist with an ENUM approach to routing data exchange should that be adopted between two service providers who agree to do so.
- Retains and leverages existing process management for the evolution of IP information exchange and is governed by established neutral industry forums and based on specific requirements developed by the industry.

BIRRDS/LERG and NPAC database systems and processes have efficiently evolved to support new network routing and interconnection data exchange for the past many years. These systems are likewise deeply imbedded into service provider operations and business processes for billing, reporting, network engineering, least cost routing, and service activation, among others. Such factors are equally as important to service providers as deploying IP interconnection technology itself. Utilizing existing industry database systems and processes for IP routing data exchange would minimize potentially broad impacts to service providers and will support a more cost effective, reliable, seamless, and accelerated transition from TDM to an all IP environment.

In addition, enhancements allowing SPs the option to mechanize the distribution of their list of IP group identifiers including OCNs, LRN, and NXXs using existing BIRRDS/LERG distribution capabilities is under consideration by the Common Interest Group on Routing and Rating (CIGRR).

4.3 Enhancing LERG to Provide a Tier 1 ENUM Registry

This section describes how the LERG can be enhanced to support Tier 1 ENUM Registry information exchange for routing of E.164 Addressed Communications over IP Network-to-Network Interconnection (NNI). To accommodate this capability the existing LERG would need to be enhanced to include Tier 2 Name Server information.

The LERG was initially designed for routing of interLATA Time Division Multiplex (TDM) calls by interexchange carriers but has effectively evolved since its inception to support new networks and technologies. It continues to evolve with governance processes that allow the industry to facilitate system process enhancements as required by service providers. For example, the LERG has also evolved to provide support for information exchange between all types of service providers including Incumbent Local Exchange Carriers, Competitive Local Exchange Carriers, Wireless Service Providers, and Voice over IP (VoIP) Providers, etc. In addition, the LERG evolved to support the exchange of hybrid TDM/IP routing and interconnection architectures, Call Agent/Media Gateway homing arrangements and NPA/NXX assignments, to name a few.

Consequently, a solution to utilize LERG to provision Tier 2 Name Server information as well as any other IP data elements would allow the industry to continue to effectively manage process evolution as it pertains to IP routing and interconnection. This management would reside within interactive industry processes that have proven efficient, cost effective, and balanced in regards to all industry segments.

The LERG, functioning as a Tier 1 Registry, would also maintain consistency of data exchange across the multi-service provider ecosystem as opposed to a third party's tiered solution that might be difficult to maintain a consistent quality of service benchmark across service providers.

4.3.1 Call Flow

A high level reference architecture is provided below that illustrates how the ENUM Domain Name System (DNS) query sequence would function during a session. In this example a Session Initiation Protocol (SIP) session is depicted.

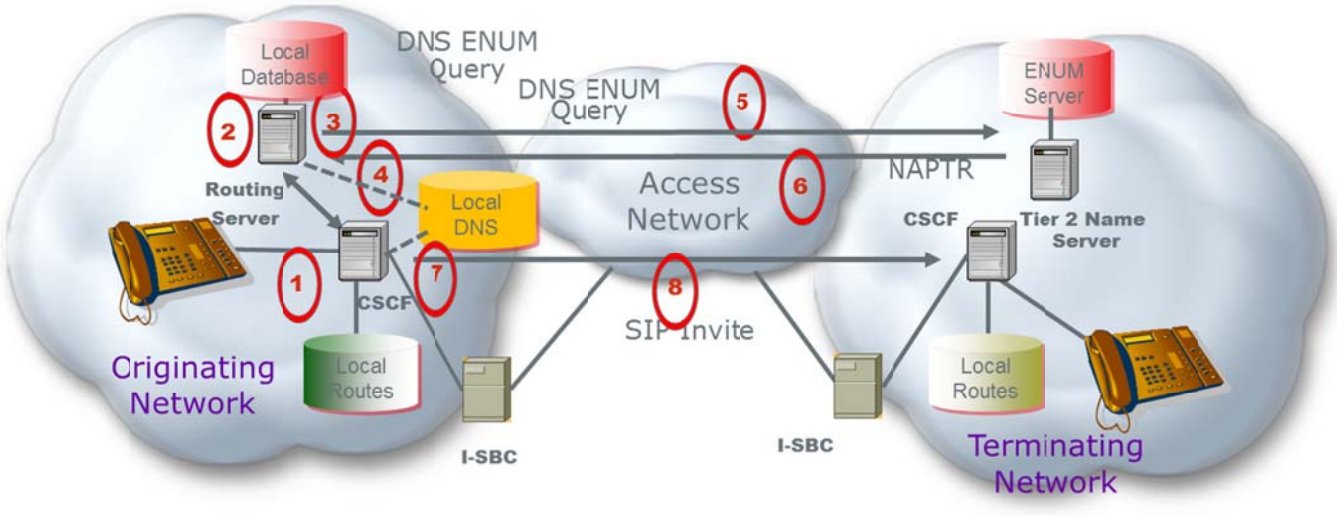

Figure 4. 5 - Call Flow – Enhancing LERG to Provide Tier 1 ENUM Registry

1. A session is initiated
2. The Call Session Control Function (CSCF) initiates a query to the Routing Server for a routing lookup (potentially using ENUM) in its local database
3. The local database returns an NS record with the host name of a Delegated Tier 2 Name Server where specific VoIP routing information can be found. The number may need to be port corrected to get the authorized service provider of record. The NS record for that provider was pre-provisioned by the LERG download.
4. The originating Service Provider resolves the FQDN in the NS record to the IP address of the terminating service provider's Tier 2 ENUM server
5. The Routing Server sends an ENUM query to the terminating network's Tier 2 Name Server
6. The terminating network's Tier 2 Name Servicer returns interconnect information in the form of one or more Naming Authority Pointer (NAPTR) records within the ENUM response.
7. The originating Service Provider resolves a NAPTR to a SIP URI and thhen the hostname in the SIP URI to obtain the IP address of an agreed upon terminating Service Provider's ingress SBC
8. Based in the information received, the originating network initiates a SIP invite to the terminating network to initiate a SIP session

By implementing an ENUM approach, the network infrastructure needs to be enhanced to accommodate the additional queries as depicted in sequences 5-6.

Additionally, the network needs to standardize the information, content, and format in the Uniform Resource Identifier (URI). This includes standardizing the service parameters that are going to be supported for when the originating service provider receives the NAPTR records there is an agreed to and standardized process for how to use them for egress routing and session set up.

It should be pointed out that the initiation of a SIP session, sequence 8 above, has additional cross-network messages that are not depicted in this reference architecture but need to be supported by all service providers. From an originating service provider perspective, there are at least 1 additional ENUM query messages to accompany the 3 or 4 SIP set up messages, meaning the originating CSCF, and likely their I-SBC, must process more messaging in an ENUM architecture.

4.3.2 Provisioning Flow

A high level reference architectures is proposed below that illustrates the provisioning sequence that could be implemented.

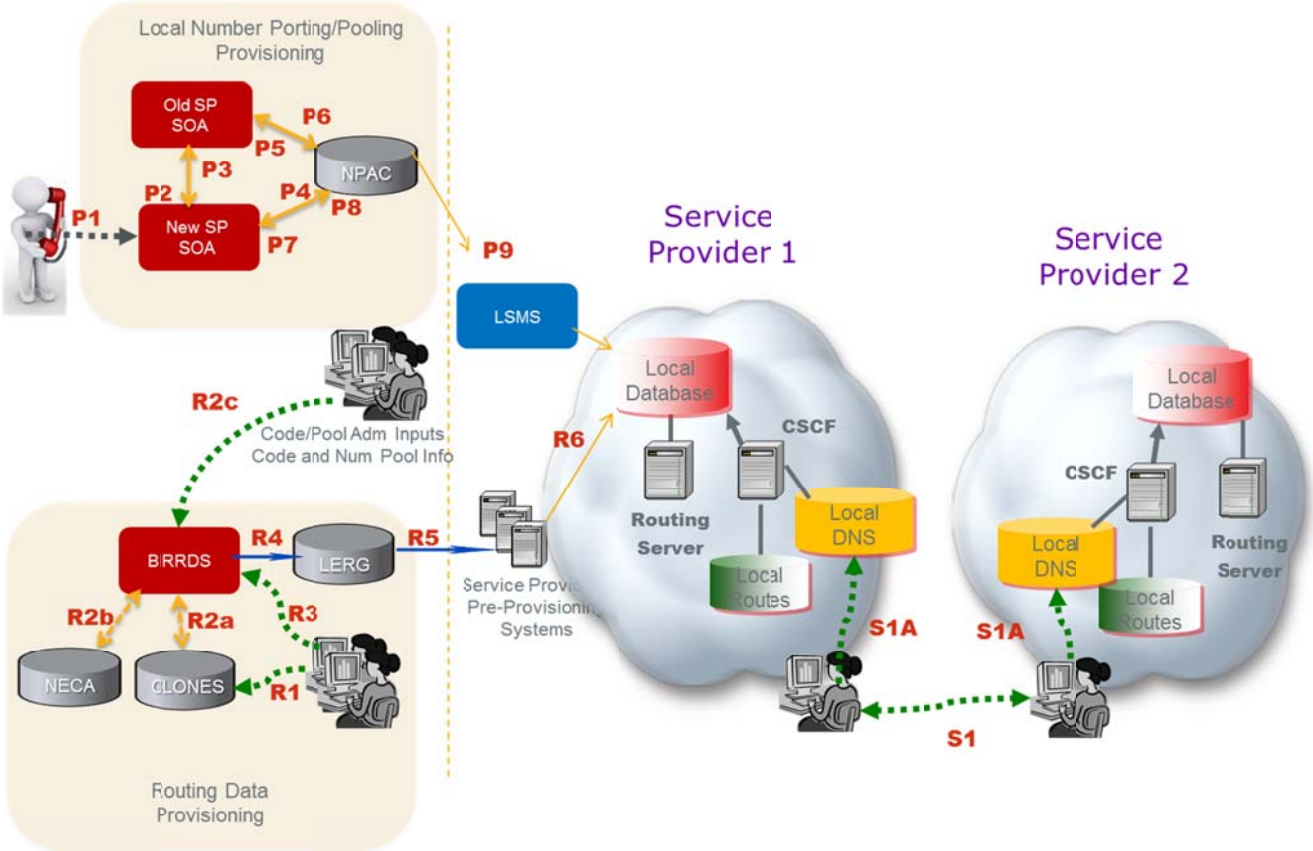

Figure 4. 6 - Provisioning - Enhancing LERG to Provide Tier 1 ENUM Registry

As depicted in Figure 4.6, service providers would obtain the Tier 2 Name Server information from the LERG to enable a functional IP Network to Network Interconnection. This figure illustrates a logical view that may be realized by different operations systems.

Steps R1 and R2 provision Public Switched Telephone Network (PSTN) information while R3 through R6 includes both new IP information (i.e., the Name Server info) and existing PSTN data. Essentially, the current provisioning and routing data exchange systems and methodology for the PSTN can be applied directly to service provider Name Server data exchange. Also note that the number port provisioning flow is unchanged from today's methodology.

Routing Data Provisioning:

(R1) Service provider develops a switch/point-of-interface (POI) CLLI Code and associated location attributes in the Common Language® CLONES database.

(R2a) The CLONES database provides newly developed CLLI Code and location reference data to the Business Integrated Routing and Rating Database System (BIRRDS). The location reference information is used by service providers in support of developing new BIRRDS switch/POI records.

(R2b) The National Exchange Carrier Association (NECA), provides new Company Codes (a subset of Operating Company Numbers (OCNs)), as they are assigned, to BIRRDS.

(R2c) National CO Code (NXX) Administrators and the Thousands-Block Pooling Administrator (US only) establish base CO Code and block assignment records in BIRRDS.

(R3) Service provider updates BIRRDS with Tier 2 Name Server information, switch/POI information (e.g., actual switch, points of interface, trunk gateways, call agents, signaling transfer points (STPs), etc.), homing arrangements, Location Routing Numbers (LRNs), and detailed information supporting the CO Code NPA/NXX and Thousands-Blocks that they have been assigned. This data is integrated with other BIRRDS data elements (e.g., Rate Centers) maintained by the BIRRDS administrator. At this time, BIRRDS can perform domain validations to validate Tier 2 Name Server accuracy. Name Server records can potentially be associated with OCN, at the highest order, or can be associated with other LERG data, e.g., CO level. That Name Server association would need to be agreed upon by the service providers.

(R4) The LERG is generated from current BIRRDS data and is provided to service providers monthly for their pre-provisioning systems. As an option, augmented daily activity may be provided nightly.

(R5) Based on service providers' local methods and procedures, the LERG data is loaded into service providers' pre-provisioning systems and is used for both PSTN and IP interconnection and routing covering switch translations and routing.

(R6) Based on service providers' local methods and procedures, the LERG data in service providers' pre-provisioning systems is made accessible to switch translations engineers to configure the switch translation, routing tables and data elements used for both PSTN and IP interconnection and routing, e.g., Tier 2 Name Server information for IP.

Local Number Porting/Pooling Provisioning:

The following process involves a pre-port validation (PPV) process as well as a Number Pooling Administration Center (NPAC) Service Order Administration (SOA) process

(P1) A customer/subscriber requests to port his/her telephone number to the new/recipient service provider.

(P2) Pre-port validation - The new/recipient server provider requests validation of the port from the old/donor service provider.

(P3) Confirmation - verification of subscriber information is sent from the old/donor service provider to the new/recipient service provider.

(P4) The new/recipient service provider sends a creation of a pending port to NPAC.

(P5) NPAC sends a notification of port to the old/donor service provider.

(P6) An approval of the pending port is sent by the old/donor service provider to NPAC.

(P7) NPAC sends a notification of the old service provider's port approval to the new/ recipient service provider.

(P8) Activation of the port is sent from the new/recipient service provider to the NPAC.

(P9) NPAC broadcasts the new routing information for the port to the Local Service Management Systems (LSMSs) for all service providers to update their local databases likely a Routing Server.

Service Provider Provisioning:

Service providers negotiate interconnection and exchange and provide Address records for their Tier 2 name servers (S1). In addition, address (A/AAAA) records for the hostname FQDNs in URIs derived from the NAPTR records that will be provided in the responses from their Tier 2 name servers. These IP addresses correspond to the destination service provider's I-SBCs that constitute the application layer POIs. Each service provider provisions the records received from the other service provider in its internal DNS (S1A).

In this reference architecture, BIRRDS/LERG would need to be modified/enhanced to allow the administrators to provide the registration of the Tier 2 name server information.

4.3.3 Summary

A solution that utilizes the LERG as the thin Tier 1 Registry would allow the industry to continue to leverage existing processes for data exchange of the ENUM Name Server records with caching in local databases to avoid external NS queries.

The existing industry framework supports the exchange of TDM and IP routing and interconnection, however, existing data base systems would need to be enhanced according to the industry requirements in order to exchange Tier 2 NS records and other IP routing information. The following items are possible areas of enhancement to LERG functioning as the Tier 1 Registry for IP routing and interconnection:

- Adopt an ENUM architecture but avoid the overhead and complexity of external NS queries by supporting service provider exchange (i.e., local downloads) of Tier 2 Name Server information.
- Assign and exchange a single Name Server record for a given service provider (e.g., an OCN) or a set of Name Server Records depending on the NPA/NXX or other considerations (such as East vs. West). It is worth discussing what granularity a Name Server will need to support including what requirement would drive Name Servers at a full 10 digit TN level.
- Validate Domain Names and potentially full URIs associated with a Name Server address prior to accepting such routing information for exchange.
- Support more frequent routing data exchanges than daily.
- Global access to the NS information requires further evaluation.

5 Per-TN Overview & Approaches

A number of service providers have identified that they have a need for more molecular routing than that based on NANP aggregation elements as discussed in the previous section.

In general these needs arise where TNs may share common point of interconnection (PoI) for TDM interconnection (and are thus associated with the same LRN or CLLI) but need to be treated differently for IP interconnection.

For example, wireless SPs are migrating their existing 2G/3G subscribers to VoLTE – from TDM to IP based user equipment (UE). For VoLTE to VoLTE calls, IP interconnection makes sense for a number of reasons – support for high definition (HD) voice and other Rich Communication Services (RCS) features and elimination of needless IP-TDM and TDM-IP conversions as would be required for TDM interconnection. SPs must still offer TDM interconnection for VoLTE TNs since not all SPs are capable or willing to provide IP interconnection. And because the migration will be gated by customer adoption of VoLTE capable UE, SPs may want to maintain existing TDM PoIs for both 2G/3G and VoLTE TNs and maintain existing TDM routing to those PoIs. Moreover, it may be desirable not to use the IP interconnection serving VoLTE TNs for 2G/3G TNs. First, additional network equipment must be deployed sooner than if IP interconnection scales with VoLTE adoption and, second, 2G/3G calls will be forced to go through unnecessary TDM/IP and IP/TDM conversions. These issues can be avoided if an SP can specify IP interconnection routing for VoLTE TNs separately from the associated LRNs.

A related case cited during IP-NNI Task Force discussions occurs in the deployment of RCSe capabilities outside North America in situations where voice calls and sessions using other RCS features need to be routed differently. This may be particularly the case where number portability methods may not support aggregation via methods like porting to different LRNs.

There may be other use cases for TN routing as well. It has been suggested that per-TN routing could be used to either avoid routing calls to fax numbers over IP interconnections using incompatible compression or taking other measures to insure adequate transmission quality.

The remainder of this section discusses different approaches to providing per-TN routing information. The first three make use of an authoritative industry registry for the exchange of per-TN data while the fourth and fifth discusses the exchange of per-TN information on a bilateral basis or via ad hoc service bureaus without the use of shared industry infrastructure. Of the registry-based solutions, the first uses the registry to provide routing data (SIP URIs) directly while the other two are based on a tiered ENUM approach in which the registry provides name server (NS) records that direct the interconnect partner how to query the terminating service provider for specific

routing data (NAPTR records resolving to SIP URIs). Two of the registry solutions use the NPAC to perform the registry function while the other proposes an independent registry.

5.1 NPAC TN Registry

This approach makes use of the existing Voice URI field in the NPAC subscription version, essentially as originally contemplated. This field provides a SIP URI that, in conjunction with bilaterally exchanged IP connection information as in the aggregate approaches discussed in section 4, resolves to the traffic exchange route(s) agreed to between the interconnection partners.

Service providers wishing to provide per-TN routing perform the following provisioning activities:

1. As part of bilateral traffic exchange negotiations provide mappings for SIP URI hostnames to SBC IP addresses.
2. Populate the Voice URI field in the NPAC subscription version for TNs available for IP interconnection with the appropriate SIP URI. The URI will be a full SIP URI (e.g., sip:+13036614567@example.mso-a.com;user=phone) but without the tel URI number portability parameters as defined in RFC 4694..

   NPAC provisioning is carried out through Change Orders 429 and 442, compliant SOAs. If a TN is not pooled or ported, the pseudo LRN capability is used to create a subscription version.

Service providers electing to use the per-TN routing information provided by their interconnect partner will:

1. Provision the hostname – IP address mappings into their internal DNS (A/ AAAA records).
2. Provision TN-URI mappings from the NPAC into their internal routing servers using Change Orders 429, and 442 compliant LSMS to obtain the NPAC data. If the routing server is accessed via a SIP query, the SIP URI may be directly populated. If the routing server is accessed via an ENUM query, the SIP URI is encapsulated into a NAPTR record.

5.1.1 Provisioning

This provisioning process is illustrated in Figure 5.1 below.

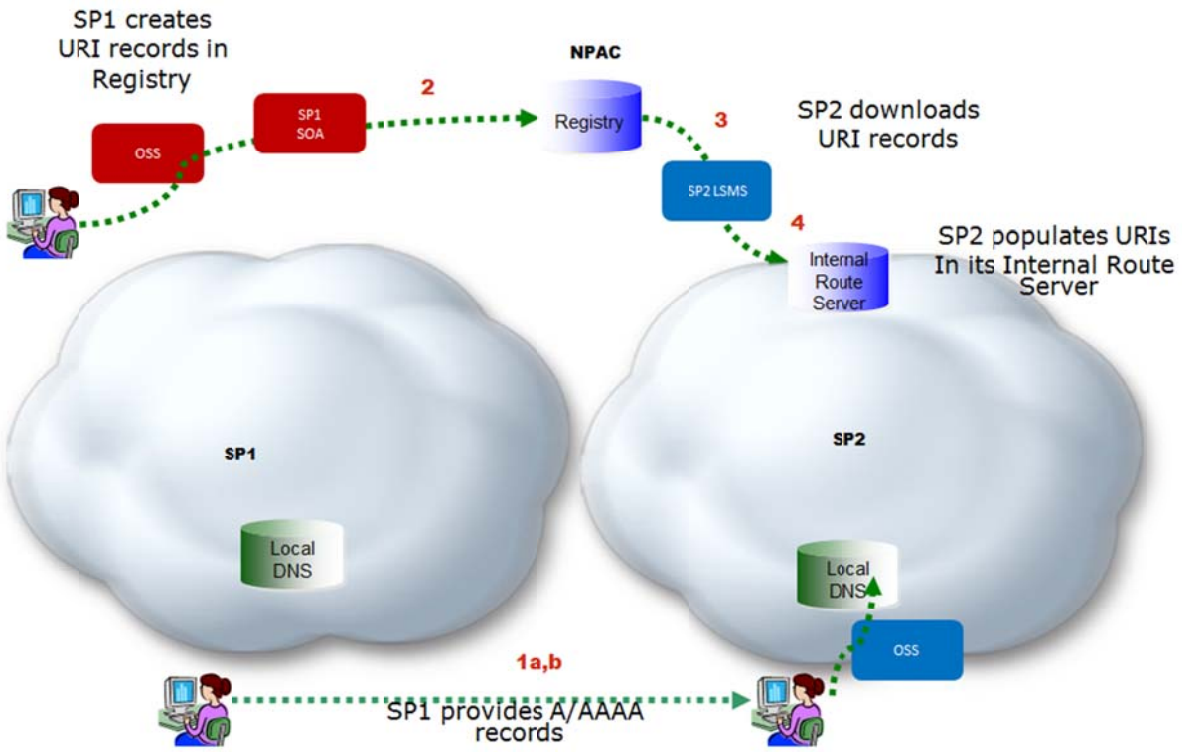

Figure 5. 1- Provisioning - NPAC TN Registry

5.1.1.1 Provisioning the NPAC Registry with Non-compliant SOA & LSMS

The provisio ning app roach introdu ced in this se ction levera ges the NP AC and app roved No rth American Numbering Council (NANC) governance change orders designed to facilitate routing transition to next generation networks. The approach further draws on established practices and commercial third part y offerings which have been enabling ubiquitous Short Message Service (SMS) routing, for example, across a broad range of specialized use cases. Specifically, this approach focuses on the provisioning of per-TN level routing data into the NPAC and distributing it at a per-T N level for con sumption by any authorized s ervice p rovider whe re th eir existi ng Service Order A ctivation (SOA) a nd/or Local Service Man agement Sy stem (LSMS) do not yet support the previously approved NANC change orders that are required.

SOA is on e of s everal w ays to provis ion ro uting d ata into the NPAC. In addition to m ultiple third party SOA options, there are other ways to directly provision routing data into the NPAC or indirectly provision data through a Service Bureau entity. For the remainder of this description, a compliant SOA (or equivalent) is one that supports the following two previously approved NANC change orders: NANC 429, “Uniform Resource Identifier (URI) Field for Voice” and NANC 442, “Pseudo Location Routing Number (LRN)”.

LSMS is us ed to receiv e information from the N PAC and i s the se rvice provider’s d atabase con taining all information r equired for c orrect c all ro uting w hen a customer c hanges from one se rvice provider to a nother. In addition to multiple third party LSMS options, there are other ways to directly receive routing data from the NPAC or indirectly receive data through a Service Bureau entity. For the remainder of this description, a compliant LSMS (or equivalent) is one that supports NANC 429 and NANC 442.

It should be noted that NANC 372, “SOA/LSMS Interface Protocol Alternatives”, supports the addition of an XML-based i nterface along with the exi sting, but g enerally m ore co mplex C MIP-based interface. Implementations of NANC 3 72 could be one way fo r exi sting SOA/LS MS to ad dress full indust ry c ompliance wit h NAN C 4 29 and NANC 442. However, this is not assumed in the remainder of this description.

The following description does a ssume that certai n one-time a ctivities previ ously di scussed have already taken place betwe en servi ce providers (e. g., IP c onnectivity estab lished). It should fu rther be noted that this provisioning approach ca n su pport th e NPAC in t he role of eit her a Tie r 1 (i.e., routing data in a format that

identifies service provider Tier 2 servers – see also Section 5.2) or Tier 2 (i.e., routing data in a format that identifies an interconnect SBC, or I- SBC, domain, where the specific "trunk group" or "route" is ultimately designed through a bi-lateral service provider information exchange – this Section 5.1). The remainder of this description assumes a Tier 2 role, where the routing data to be exchanged in the NPAC is in the form of a SIP URI like "sip:<telephone number>@sbc1.sp1.com". However, the approach doesn't rely on just this specific URI format.

Generally, the NPAC Location Routing Number (LRN) for ported telephone numbers or NANP NPA-NXX for native telephone numbers is used to route calls between service providers. Similarly, the NPAC Service Provider IDentification (SPID) or NANP Operating Company Number (OCN) is typically used to route text messages between service providers. Over the past five years or so, multiple commercial wireless use cases have arose where the SPID or OCN associated with a particular telephone number in these recognized authoritative databases (after port-correction) was not sufficient for routing within the ecosystem. Further, these authoritative databases, at the time, were limited in their support of such use cases. Consequently, several commercial third party services were introduced to support these use cases while they work hand-in-hand with the recognized authoritative databases.

The key constraint in the NPAC has since been removed through NANC 442 that allows native telephone numbers and associated information to be stored in the NPAC. The PSTN to IP transition use case and others being discussed are analogous to those that have naturally evolved around text messaging where additional information beyond an NPAC LRN or NANP NPA-NXX is required in support of routing. The provisioning flow summarized below uses the NPAC in support of the use case(s) minimally discussed within this ATIS SIP Forum IP- NNI Task Force. Specifically, it proposes to use the industry-approved VOICE URI field (NANC 429) that is one field of many in the existing, standard NPAC database record. Further, it leverages at least one established commercial third party service to provision and distribute NPAC database records with URI field data.

Figure 5.2 below highlights the provisioning and distribution aspects of the approach. The routing data input is assumed to be in the form of an NPA-NXX-XXXX. Further, SP1 has both a compliant SOA and LSMS while SP2 does not.

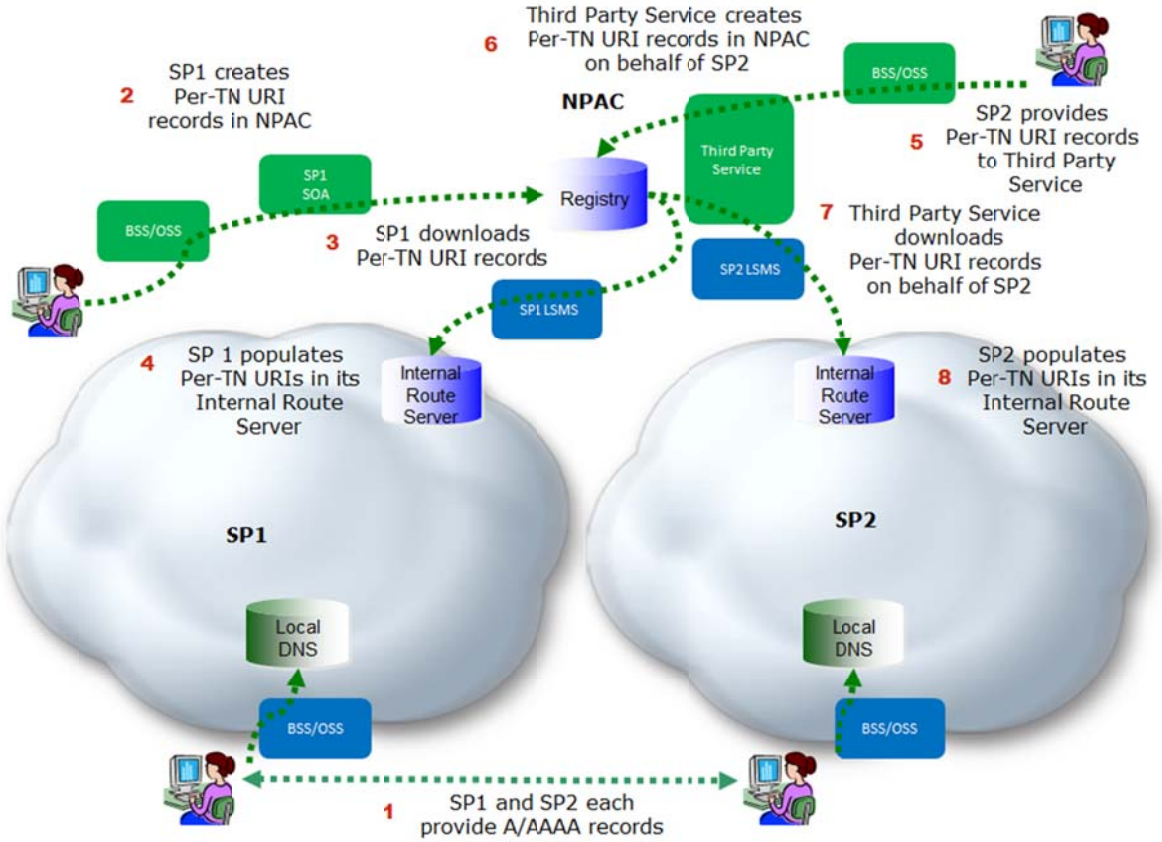

Figure 5. 2 - Provisioning NPAC as a TN Registry for Non-compliant SOA and LSMS

1. SP1 and SP2 negotiate bilateral IP interconnection and exchange. In support of routing data exchange, each provides an agreed to mapping of IP address records (A/AAAA records) to FQDNs (or URI domains) corresponding to their respective I-SBCs. Each SP then provisions these records into their respective local DNS. An example of such a mapping for one URI domain could be:

URI Domain	IP Address
sbc1.sp1.com	138.34.23.3
sbc1.sp1.com	182.36.12.1
sbc1.sp1.com	58.23.12.90

2. SP1 populates the NPAC VOICE URI field in the associated subscription version (SV) record through its SOA (or equivalent) as new numbers are provisioned or existing numbers become available for IP interconnection. Again, the routing data to be exchanged is assumed, for this description, to be in the form of a SIP URI like “sip:<telephone number>@sbc1.sp1.com”.
3. SP1 downloads per-TN VOICE URI field data from SP2 (along with other existing NPAC data for number portability) through its LSMS (or equivalent).
4. SP1 extracts per-TN VOICE URI field data from SP2 (along with other existing NPAC data for number portability) and provisions it into their internal route server. Note that the details of how this routing data gets represented and used are specific to SP1.
5. SP2 shares per-TN VOICE URI routing data with an established third party service. For example,
   a. SP2 designates existing TN 508-332-2319 for IP interconnection.
   b. The associated ingress SBC domain is “sbc1.sp2.com”.
   c. SP2 establishes a Letter of Authorization (LOA) with the third party supporting this approach (if such an LOA doesn’t already exist).
   d. The TN/ingress SBC domain/Action is then shared with the third party service over one of several published APIs (e.g., a flat file with a row “5083322319,sbc1.sp2.com,A” where “A”=Add).
6. The third party service for SP2 manages as per-TN VOICE URI field data in the NPAC on behalf of SP2. For one example use case,
   a. Third party service interprets row “5083322319,sbc1.sp2.com,A” in a shared flat file and generates the associated NPAC provisioning actions. For example,
      i. Modify action is generated to add sip:5083322319@sbc1.sp2.com to the VOICE URI field for this existing SV record in the NPAC
7. At a configured interval (e.g., every 15 minutes), the third party service checks for changes in SP1 VOICE URI field data and distributes them over a pre-configured SP2 interface separate from the non-compliant LSMS interface which continues to receive existing NPAC data for number portability.
8. SP2 extracts per-TN VOICE URI field data from SP1 (along with other existing NPAC data for number portability) and provisions it into their internal route server. Note that the details of how this routing data gets represented and used are specific to SP2.

This sub-section expands on sections 5.1.1 (above) and 5.2.1 (to be discussed in the next section) where the NPAC is proposed for supporting per-TN routing. Specifically, it focuses on an approach for supporting the provisioning of per-TN level routing data into the NPAC and distributing it at a per-TN level for consumption by any authorized service provider where their existing SOA and/or LSMS may not yet be compliant with the previously approved NANC change orders that are required. The provisioning approach is transparent to service providers who have compliant SOA and LSMS. For service providers who do not, their per-TN level routing data can be shared through an established third party and provisioned (on their behalf) into the NPAC. This per-TN routing data can then be directly consumed by any participating service provider with a compliant LSMS or distributed through an established third party over a pre-configured interface.

5.1.2 Call Flow

On call origination, the originating service provider will query their routing server and obtain the corresponding SIP URI for numbers available for IP interconnect. They will resolve the hostname from the URI in their internal DNS to obtain the IP address of the terminating provider's ingress SBC.[2] The call flow is shown in Figure 5.3 below:

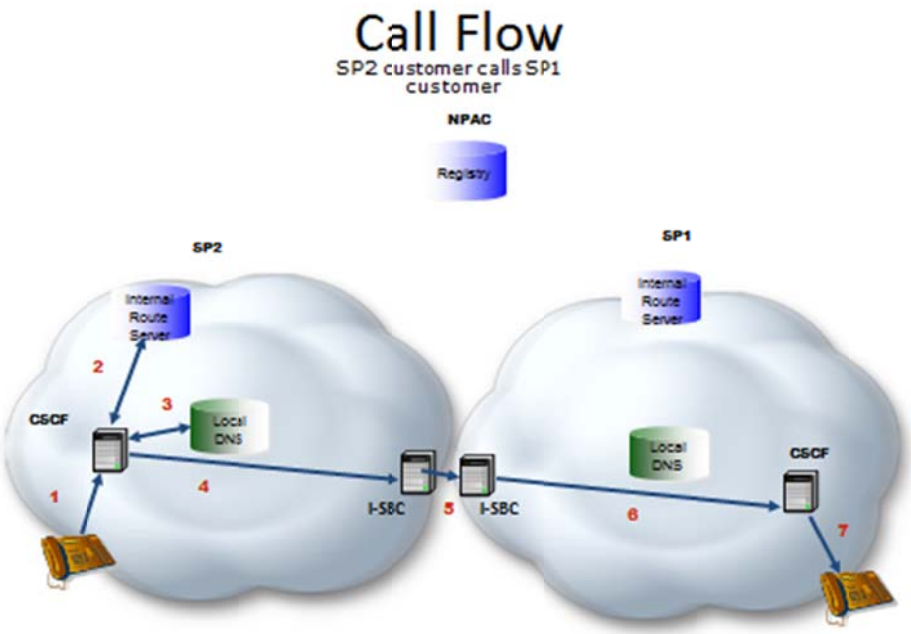

Figure 5. 3 - Call Flow - NPAC TN Registry

1. SP2 Caller dials destination number
2. SP2 S-CSCF queries internal route server and SP2 route server responds with a URI passed back to S-CSCF
3. SP2 S-CSCF resolves the hostname in the SIP URI to obtain the IP address of an agreed upon SP1 ingress SBC
4. A SIP INVITE is sent to egress SBC of SP2 that has layer 3 connectivity to the ingress SBC of SP1
5. The SIP INVITE is forwarded to the SP1 ingress SBC.
6. and 7. SP1 terminates the call to its end user.

Note that although the NPAC URI approach is proposed primarily in support of per-TN information exchange, the Voice URI can also be populated on thousands block level, thus providing some level of aggregation where appropriate.

5.2 The NPAC as a Tier 1 ENUM Registry

Consistent with 3GPP IMS recommendations for inter-carrier routing, an ENUM-based architecture is proposed for routing across the IP NNI. The essence of this architecture is a query using the protocol described in RFC 6116. 3GPP recommendations do not specify, however, the details of the ENUM data repository to be queried nor the source of the data in that repository. This proposal includes recommendations for these matters, the

[2] There may be alternate approaches to combining the bilaterally exchanged URI-IP address mappings and the TN-URI mappings obtained from the Registry and combining them in a routing server for session establishment.

corresponding data formats, and the manner in which the results of ENUM queries are processed to resolve responses to the IP address(es) toward which a SIP INVITE to the destination network Session Border Controller are to be directed.

The classic ENUM "golden tree" architecture assumed a tiered structure in which a Tier 0 registry (such as the one currently managed by RIPE for the e164.arpa user ENUM domain) contains name server (NS) records pointing to the Tier 1 name servers authoritative for individual E.164 country codes. The Tier 1 registries in turn consist of NS records pointing to the authoritative Tier 2 server for a specific E.164 number. The Tier 2 servers, maintained by or for the assignee of the number, contained NAPTR records that resolved to the URIs needed to establish communication to the number in question.

As the industry has yet to establish a universally recognized Tier 0 for infrastructure ENUM (RFC 5067) as opposed to user ENUM, a combined Tier 0/1 registry is proposed for the US portion of Country Code 1.[3] This Tier 0/1 registry is in principle extensible to other portions of Country Code 1 if desired by the competent authorities and may eventually be linked to registries for other country codes or to a global Tier 0 when and if consensus on such a Tier 0 emerges. In the interim the registry simply contains NS records for individual numbers in the US portion of CC1.

To speed deployment and leverage existing infrastructure it is proposed that the Number Portability Administration Center (NPAC), the local number portability database of record, serve as the Tier 0/1 registry. Unlike the Tier 0 and Tier 1 registries in the classic ENUM architecture, the NPAC is not a DNS name server and is not queried during call processing. It can however download data for NS records to service providers or service bureaus for them to provision in their name servers to be queried on call origination.

As in the classic ENUM model, the NS records will point to Tier 2 name servers that respond with NAPTR records containing the actual routing data. Service Providers will maintain themselves or have service bureaus provide for Tier 2 name servers for the numbers they serve. Based on the NS records obtained from the Tier 0/1 query, the originating service provider will query the Tier 2 name server to obtain the NAPTR record for call routing. Together the SIP URI obtained from the NAPTR record and the bilaterally exchanged URI hostname to IP address mapping instantiate the routing agreed to by the interconnect partners.

5.2.1 Call Flow

The following is the inter-service provider call flow as shown in the Figure below:

[3] In infrastructure ENUM, the Tier 1 servers point to Tier 2 servers maintained by or for the service provider of record for the number.

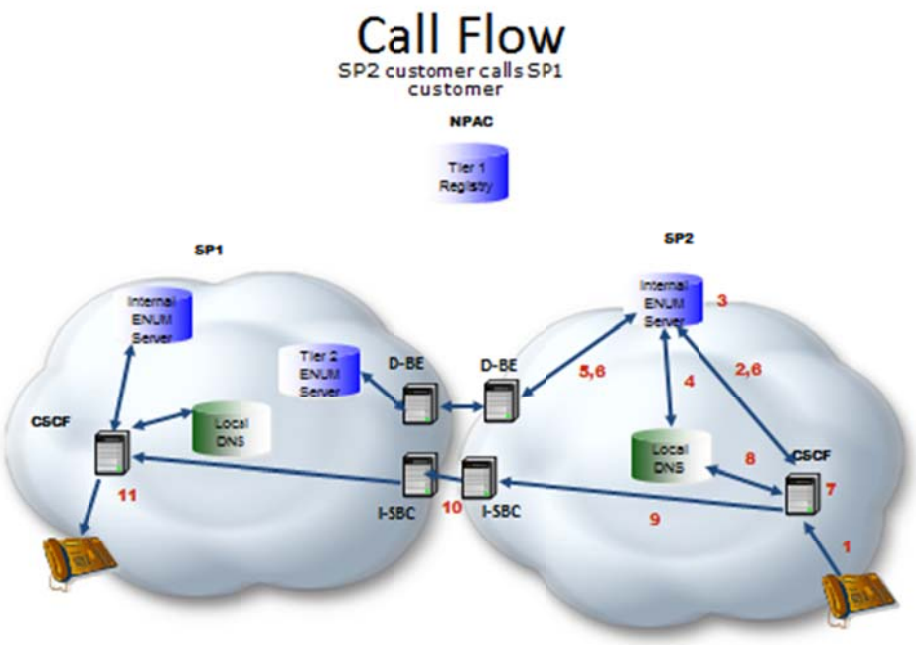

Figure 5. 4 - Call Flow –NPAC as a Tier 1 ENUM Registry

1. SP2 Caller dials destination number
2. SP2 S-CSCF queries internal ENUM server
3. SP2 ENUM server finds an NS record
4. SP2 internal ENUM server resolves the FQDN in the NS record to the IP address of SP1's Tier 2 ENUM server.[4]
5. An ENUM query is forwarded to SP1's Tier 2 ENUM server.[5]
6. SP1's Tier 2 ENUM server responds with a NAPTR record(s) passed back to S-CSCF
7. SP2 S-CSCF processes the NAPTR record set returned resulting in a SIP URI
8. SP2 S-CSCF resolves the hostname in the SIP URI to obtain the IP address of an agreed upon SP1 ingress SBC
9. A SIP INVITE is sent to egress SBC of SP2 that has layer 3 connectivity to the ingress SBC of SP1
10. The SIP INVITE is forwarded to the SP1 ingress SBC.
11. SP1 terminates the call to its end user.

5.2.2 Provisioning

Provisioning is shown in the Figure below:

[4] Resolution is shown in recursive mode. It could also take place in iterative mode with the NS record being returned to the S-CSCF for the S-CSCF to resolve the FQDN in the NS record and then issue a query to the SP1 Tier 2.

[5] Use of separate Data Border Element is shown.

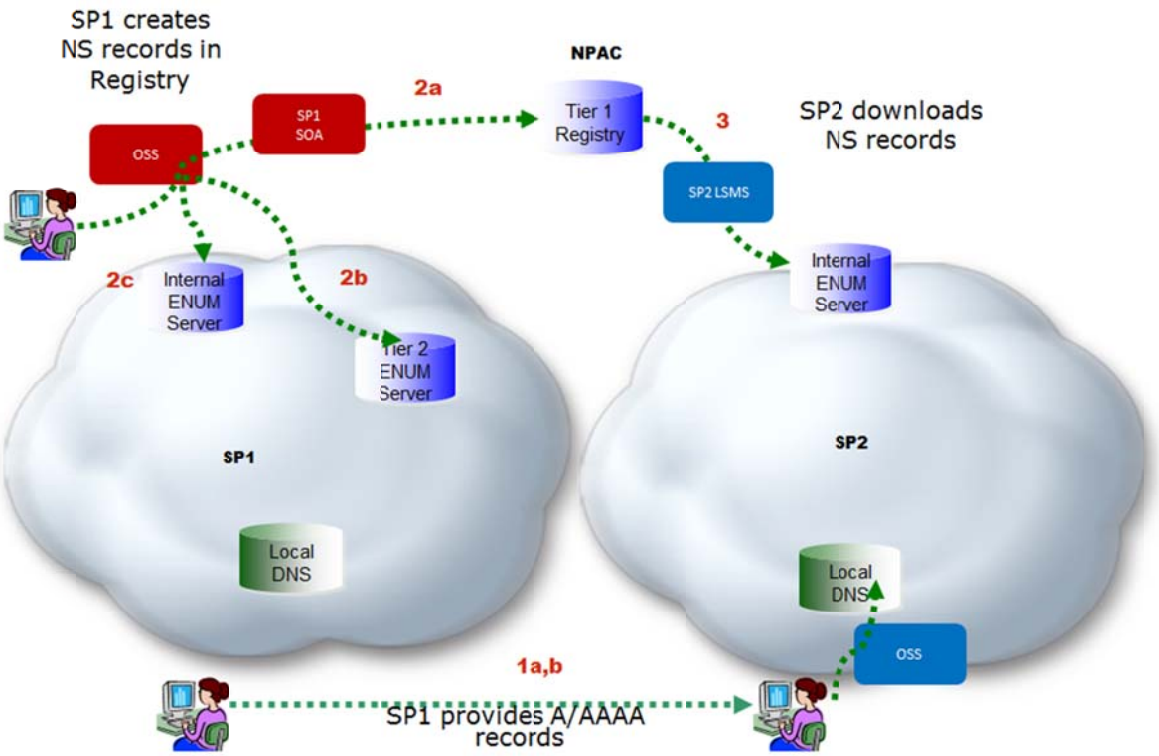

Figure 5. 5 - Provisioning –NPAC as a Tier 1 ENUM Registry

1. Servi ce providers negotiate i nterconnection an d exc hange, as part of the interconnect technical negotiation process,
   a. Address (A/AAAA) records for their Tier 2 name servers
   b. Address (A/AAAA) records for the hos tname FQDNs in URIs de rived from th e NAPTR records that will provided in the responses from their Tier 2 name servers. These IP addresses correspond to the destination service provider's I-SBCs that constitute the application layer POIs.[6]

   Each service provider provisions the records received from the other carrier in its internal DNS.

2. Whe n new numbers are provisioned or existing numbers made available for IP interconnection by an SP, the SP
   a. P rovisions NS record information for the numb er into the NPAC Voice URI field of the s ubscription version (SV) of the numb er th rough i ts SOA. (If t here is no e xisting sub scription ve rsion on e is added.)[7]

---

[6] There are alternate approaches to the resolution of Tier 2 name servers and interconnection URI FQDNs. These include a) exchange of SRV instead of A/AAAA records, b) resolution in the internet DNS, c) sharing through some controlled access industry system including but not necessarily limited to a private DNS.

[7] The VOICE URI field was originally defined to contain a URI that would be used to provide for IP routing of voice calls, but it is currently little used and has no explicit typing. It simply allows up to 255 characters.

It is proposed that NS record information be populated in the VOICEURI field in the form

tier2enum.serviceprovider.com

(i.e., just the nameserver name as an FQDN) as opposed to the full NS form:

3.8.0.0.6.9.2.3.6.4.1.e164enum.net IN NS tier2enum.serviceprovider.net

The full record form would be reconstituted by the service provider for provisioning in its ENUM server. Note that an NS record or records are generally provisioned for each individual number.

b. Provisions NAPTR records for number in its Tier 2 name server[8].
c. Provisions internal NAPTR records in its internal ENUM server for use within network calls.

3. Service providers download SVs from the NPAC, extract the NS information from the Voice URI field and provision it as NS records into their internal ENUM server. Note that a record is provisioned for each TN.

Please note that the provisioning approach previously described in Section 5.1.1.1 can also support the proposed solution above where the NPAC is used as a Tier 1 ENUM Registry. Specifically, any authorized service provider whose SOA and/or LSMS does not support NANC Change Orders 429, and 442 can have their per-TN NS record information shared through an established third party and provisioned (on their behalf) into the NPAC. This per-TN NS record information can then be directly consumed by any participating service provider with a compliant LSMS or distributed through an established third party over a pre-configured interface.

5.2.3 Summary

A Tiered ENUM approach using the NPAC as the Tier 0/1 registry populates NS records into existing fields in the subscription version that already contains TDM routing elements. SVs are populated in the NPAC for each TN for which IP interconnection is offered. (If a TN is not otherwise ported or pooled an SV with a pseudo LRN is created). This approach simply enhances the existing interfaces (direct or via service bureaus) that all SPs have with the NPAC, requiring no new governance structures.

5.3 Independent ENUM Registry

This section describes an independent ENUM Registry, for the exchange of data for IP routing and interconnection for routing of E.164 Addressed Communications over IP Network-to-Network Interconnection (NNI).

An ENUM Tier 1 Registry can enable authorized Service Providers to start directly exchanging routing information dynamically to enable session setup end-to-end over IP networks. Listed below are some requirement considerations and benefits of having a Registry:

- The Tier 1 Registry could vastly reduce the NS record set by supporting policy-based NS provisioning. For example, an NS record value could be assigned to each Operating Company Number (OCN)/Service Provider ID (SPID) rather than to each telephone number, and/or NPA/NXX or Location Routing Number (LRN). This could also differ by TN and be at the discretion of the number holder.
- The Tier 1 Registry needs to incorporate the existing NPAC Local Service Management System (LSMS) feed to provide Tier 2 NS records that are corrected for porting and pooled numbers when applicable.
- Optimize session setup time; the Tier 1 ENUM query to the external registry could be avoided by using Zone Transfer protocol to download the NS records to local cache at each originating service provider. If

---

Multiple NS records could be populated in the NPAC VOICEURI field through the use of some agreed upon separator character. This would allow for redundancy as it is expected that carriers would want to have multiple name server instances.

Note that an apex domain, for example, *e164enum.net*, needs to be agreed upon.

[8] The ENUM query may return multiple NAPTR records with different order, preference, and enumservice fields as defined in RFC 6116. Thus multiple options for interconnection can be provided including different gateways for different service types (e.g., voice versus video) where appropriate. A NAPTR for general SIP interconnection might look like

NAPTR 10 100 "u" "E2U+sip" "!^.$!sip:\1@gw02.serviceprovider.net; user=phone!" .*

its resolution would result in the URI

sip:+14632963800@gw02. serviceprovider.net; user=phone

The querying service provider would then resolve the hostname

gw02.serviceprovider.net to obtain an IP address for the terminating provider's ingress SBC.

this results in too many NS records for a simple Zone Transfer, then the NS data could be transferred in stages using a series of Zone Transfers.

- Support service providers who did not have the capability for locally caching the Tier 1 NS records, then ENUM or another query protocol could be used by originating service providers to request the NS record from the Tier 1 Registry.
- Optimize external queries whenever possible, then the Tier 0/1 Registry could optionally be used by service providers to capture and exchange NAPTR records instead of NS records thereby combining Tier 2 functionality in the Tier 1 Registry. This could be optional according to terminating service provider discretion and would be transparent to the originating service provider.
- Allow for different NS records depending on the originating & terminating service provider combination, then the Tier 0/1 Registry could be configured with policy for source based resolution.. For example, some authorized Service Providers might input Name Server information for the same TN that in one case refers to the Tier 2 Name Server of a transit operator or IP eXchange (IPX) and in another case refers to their own terminating Tier 2 Name Server when they are peering or interconnecting directly with the originating service provider. While more powerful in the Tier 2 Name Server platform, this feature has potential application at the Tier 0/1 Registry level and could be used for either per session queries as well as to customize the data download to local cache.
- Accommodate ENUM on a global basis, such as for incoming and outgoing international calls, then the Registry addresses for each country could be communicated to the global service provider community.
- Support multiple Tier 0/1 Registries in order to avoid a sole supplier environment, then a mechanism, system processes and interfaces could be established to replicate data across participating registries. Technology exists to support such a requirement. Database peering has been formally endorsed by the FCC to support a competitive market of TV Whitespace geolocation databases.
- Support source-based routing logic which can be used for services which require it.[9]
- Support source-based routing logic which can use location to optimize physical transport path.[9]

5.3.1 Call Flow

A session set-up is shown in Figure 5.6 that illustrates how the ENUM query sequence would function during a session. In this example a SIP session set up is depicted.

[9] This could also be supported in other solutions that include an ENUM query to the terminating network.

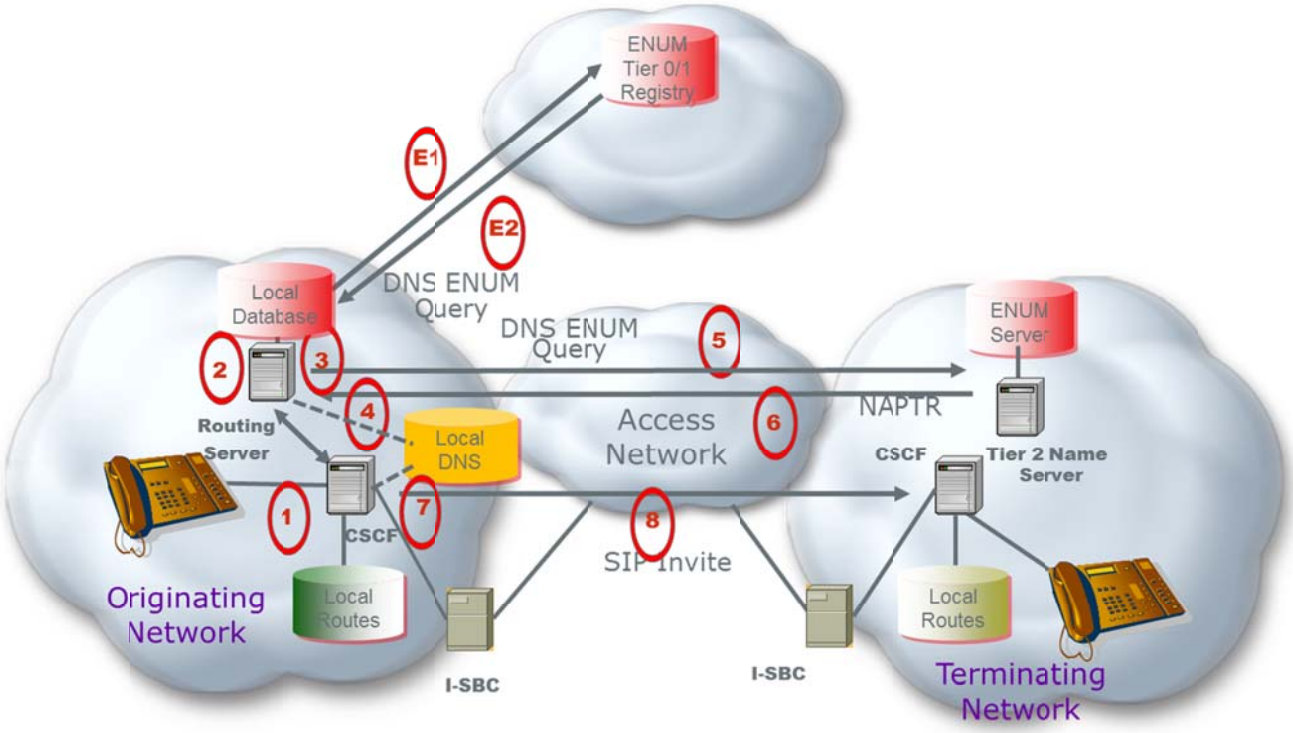

Figure 5. 6 - Call Flow - Independent ENUM Registry

In Figure 5.6 a call is being initiated (1). The Call Session Control Function (CSCF) initiates a query to the Routing Server for a routing lookup (potentially using ENUM) in its local database (2). The local database returns an NS record with the host name of a Delegated Tier 2 Name Server where specific VoIP routing information can be found (3).

If not cached locally, the CSCF would initiate an ENUM DNS Query to the Tier 0/1 Registry (E1). The Tier 0/1 Registry returns an NS record (E2) for the service provider that holds the number. Steps (E1) and (E2) allow for the case where an originating service provider does not support receiving the Tier 0/1 Registry data in a local cache and must send a query to request the NS record at call setup.

The NS record indicates the host name of a Delegated Tier 2 Name Server where specific VoIP routing information can be found. The originating service provider resolves the FQDN in the NS record to the IP address of the terminating Service Provider's Tier 2 ENUM server (4). This NS information is used by the originating network to send a query to the terminating network's Tier 2 Name Server (5).

The terminating network's Tier 2 Name Server returns specific routing information identifying the I-SBC in the form of one or more Naming Authority Pointer (NAPTR) records (6). The originating service provider resolves the domain name from the NAPTR URI to obtain the IP address of an agreed upon terminating network's ingress I-SBC (7). Based on the information received, the originating network initiates a SIP invite (8) to the terminating network I-SBC in order to initiate a SIP session. .

By implementing an ENUM approach, the network infrastructure needs to be enhanced to accommodate the additional queries as depicted in sequences 2-6 as well as potentially E1 and E2. Additionally, the network needs to standardize the information, content, and format in the URI including what service parameters are going be supported so when the originating service provider receives the NAPTR records there is an agreed to and standardized process for how to use them for egress routing and session set up.

It should be pointed out that the initiation of a SIP session, sequence 8 above, has additional cross-network messages that are not depicted in this reference architecture but need to be supported by all service providers. A representative example of the message set, presuming the calling and called devices are SIP end-points, is shown in the Figure below.

5.3.2 Provisioning Flow

A high level provisioning reference architecture is shown in Figure 5.7 below to illustrate the high level process that would be required for service providers to configure the ENUM Tier 0/1 Registry to support routing data exchange.

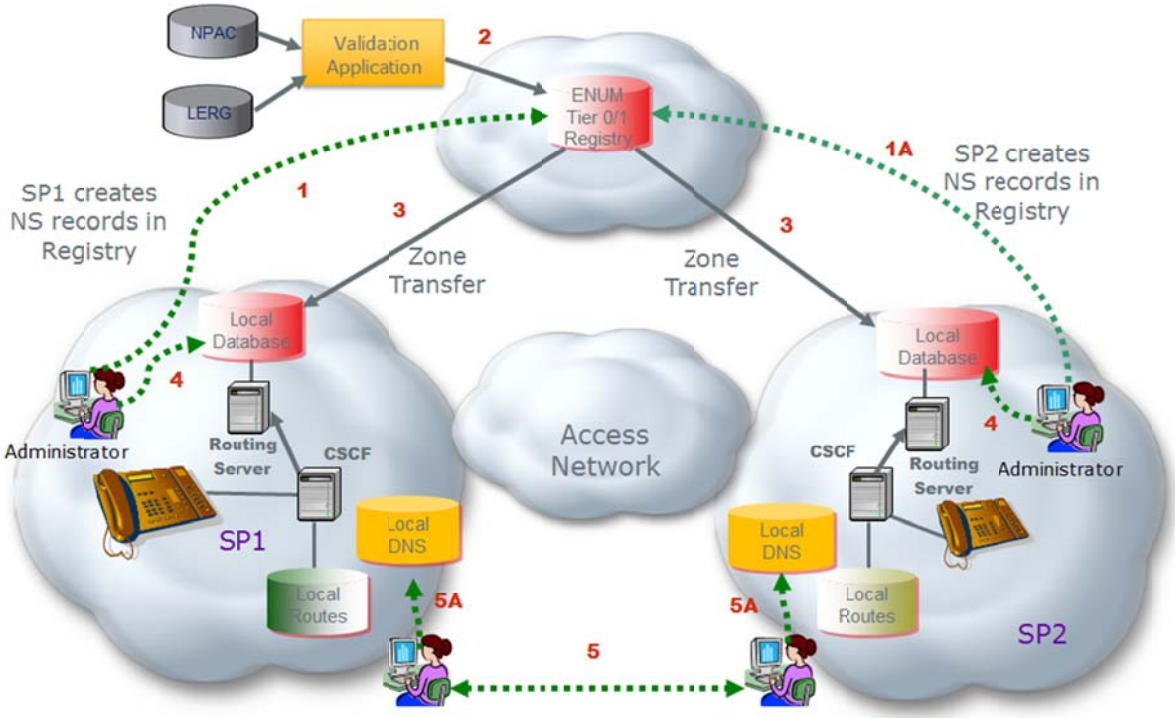

Figure 5. 7 - Provisioning - Independent ENUM Registry

As depicted in Figure 5.7, the ENUM Tier 0/1 Registry can obtain data from all authorized Service Providers to enable routing data exchange for a functional IP Network to Network Interconnection service. One of the functions of the Registry is to allow authorized Service Providers to create, change, and/or modify ENUM domain name registrations in the Tier 0/1 Registry Database (1 and 1A).

Further it validates registrations via access to the authoritative LERG and Number Portability Administration Center (NPAC) data sources (2).

The NS records (Authoritative Name Server, DNS records), are sent via Zone Transfer protocol to local cache at all service providers (3). The local administration also provisions internal routing information into its own database (4). This includes providing the NS record resolution to an IP address. Service providers negotiate interconnection and exchange and provide Address (A/AAAA) records for their Tier 2 name servers (5). In addition, address records for the hostname FQDNs in URIs derived from the NAPTR records that will be provided in the responses from their Tier 2 name servers. These IP addresses correspond to the destination service provider's I-SBCs that constitute the application layer POIs. Each service provider provisions the records received from the other service provider in its internal DNS (5A).

5.3.3 Summary

This option proposes using a purpose-built ENUM solution as the data exchange mechanism for an IP routing industry framework. An ENUM Tier 1 Registry can enable authorized Service Providers to start directly exchanging routing information dynamically to enable session setup end-to-end over IP networks.

5.4 Bulk Transfer using Independent Service Bureaus

Some SPs have shown interest in the per-TN approach to exchanging routing data, whereas some others have plans to or have already implemented the Aggregation Method described in Section 4.1. Yet, there are many more SPs that have yet to determine what method best fits their operational capabilities and business interests. These varying needs among SPs are indicative of how the industry is still evolving, and why a per-TN solution SPs can implement without impacting other SPs is warranted. Three approaches allowing SPs to implement a per-TN solution independently and in cooperation with like-minded SPs is described in this section.

5.4.1 Implementation

No new industry systems development or standards are required to implement this method. SPs can maintain their existing internal core network IP routing service, and develop/evolve their provisioning systems autonomously based upon their operational and business needs. In general, per-TN SPs can agree to correlate some or all of their TNs with routing data to create a per-TN database that is shared with other SPs, either directly or indirectly using one or more Service Bureaus.

Referring to Figure 5.8, each set of arrows lettered A thru C (and color coded) represent three possible per-TN implementations. The black arrows represent the manual exchange of domain names and IP address for use when resolving per-TN routing data, e.g., SIP URIs. Note that this manual bilateral exchange is required for all the solutions discussed in this document.

The green arrows (lettered A) depict the direct exchange where each SP obtains a copy of the others per-TN routing database. This may be attractive to SPs having the operational capability that prefer not to outsource the data exchange functionality.

The blue arrows (lettered B) depict the use of a common Service Bureau to exchange per-TN routing data where both SPs have chosen the same Service Bureau to outsource data exchange functionality.

The red arrows (lettered C) depict how SPs may use a Service Bureau to exchange routing data on their behalf with SPs subscribed to a different Service Bureau. Here again, Service Bureaus may provide additional functionality based upon the needs of their SP subscribers.

5.4.2 Provisioning

A Provisioning diagram is shown below in Figure 5.8.

In this provisioning example, SP1 provisions (black arrows) its Routing Service and DNS based upon information provided by SP2. SIP URIs are correlated with SBC interconnect IP addresses and domain names provided by SP2.

The SP1 and SP2 exchange (either directly or via Service Bureaus as described above) its per-TN database and periodic updates based upon an agreed frequency. For example, TNs can be correlated with a URI that is a full SIP URI (e.g., sip:+13036614567@example.mso-a.com;user=phone) but without the tel URI number portability parameters as defined in RFC 4694. How SP1 designs its routing service to use per-TN routing data is specific to SP1's implementation.

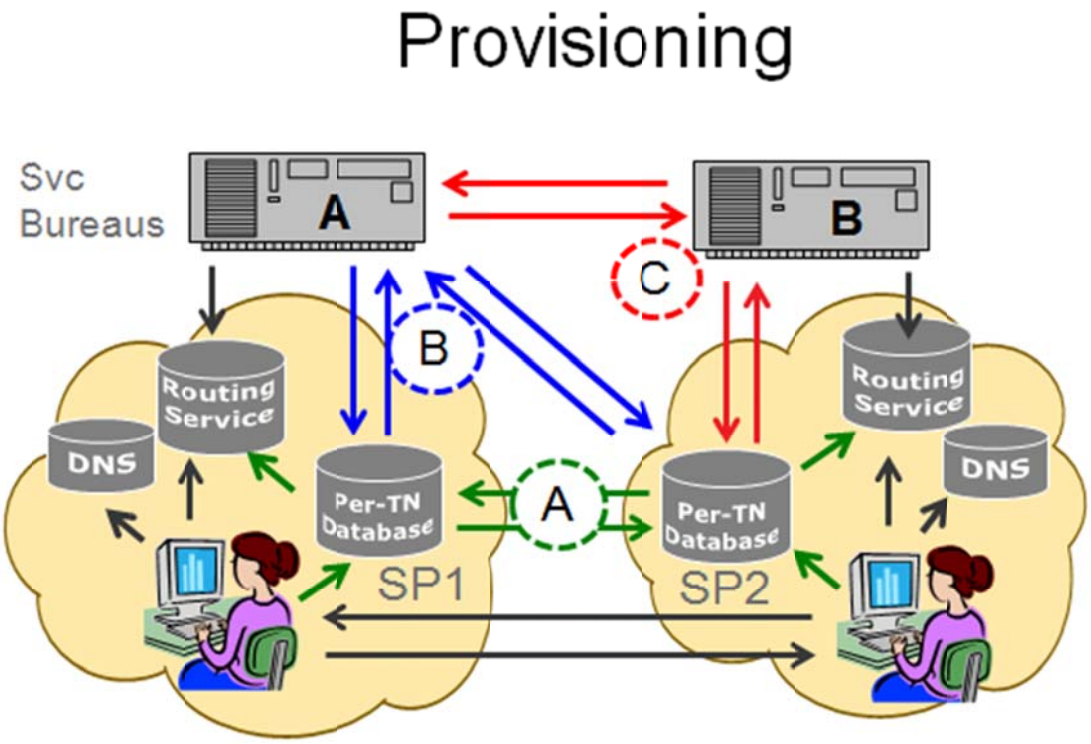

Figure 5. 8 - Provisioning- Bulk Transfer using Independent Service Bureaus

5.4.3 Call Flow

An example of the Call Flow is shown below in Figure 5.9:

1. Pat (non-roaming subscriber of SP1) makes a session request (e.g., places a call) to Mike (subscriber of SP2). SP1's network provides originating services based on Pat's subscription.
2. SP1's application server queries its routing service in real time using the called number to determine how to forward the request. The routing service first portability corrects the called number, and then determines that it is not subscribed to SP1. It then checks to see whether the code holder associated with the telephone number[10] is covered by an IP interconnection agreement. If so, the SP1 routing service supplies[11] the application server with the ingress point through which SP2 has requested that session requests directed to this telephone number enter its network.
3. The application server identifies SBC-2 and (if applicable) SBC-1 in SIP ROUTE headers, and forwards the resulting session request onward. SP1's L3 processing resolves the host portion of the topmost ROUTE header (using DNS) to the IP address of SBC-1.
4. SBC-1 removes the topmost ROUTE header (which identifies itself) and forwards the session request based on the next one (which identifies SBC-2). To do so it resolves (using DNS) the host portion of that header, yielding the IP address of SBC-2.
5. SBC-2 removes the topmost ROUTE header (which identifies itself) and admits the message to SP2's network, forwarding it to an application server, and eventually to Mike. How SP2 performs these functions is SP specific.

---

[10] The "code holder" is a term used to refer to the SP serving the TN, which can be identified in LERG data using the LRN or the NPA-NXX of the telephone number (if not shown in the NPAC, e.g., ported or pooled).

[11] How this is accomplished is implementation specific. Messages from an application server to a routing service is typically an ENUM query, but in some networks a SIP message is sent to a proxy collocated with the ENUM service, which sends back a 302 "redirect" response.

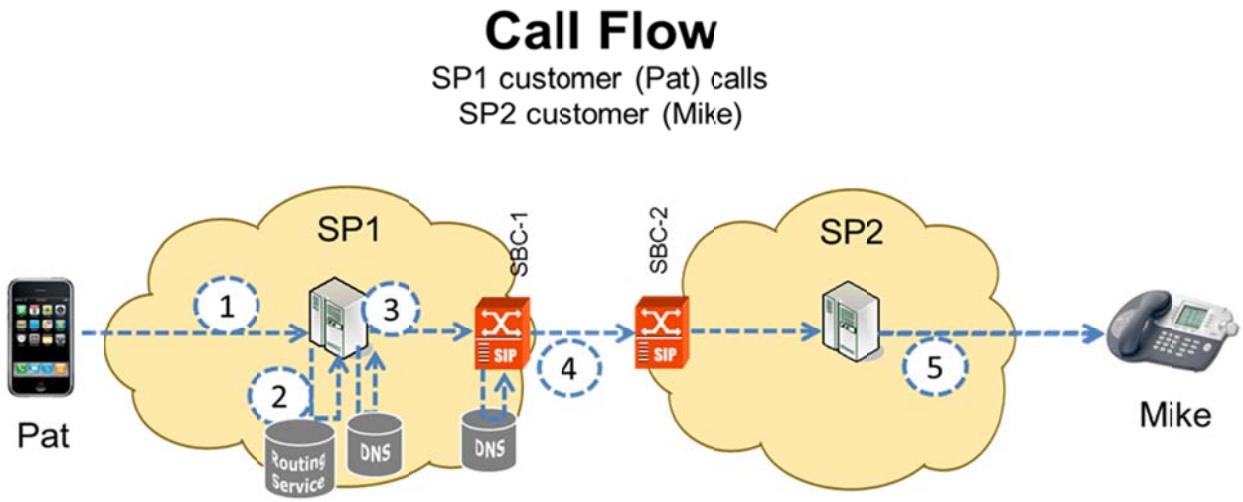

Figure 5. 9 - Call Flow - Bulk Transfer using Independent Service Bureaus

5.5 Query Using Independent Service Bureaus

Some SPs have shown interest in the per-TN approach to exchanging routing data, whereas some others have plans to or have already implemented the Aggregation Method described in Section 4.1. Yet, there are many more SPs that have yet to determine what method best fits their operational capabilities and business needs. These varying needs among SPs are indicative of how the industry is still evolving a routing paradigm, and why a per-TN solution SPs can implement by "opting-in" without impacting other SPs is warranted.

Three approaches allowing SPs to implement a per-TN solution independently and in cooperation with like-minded SPs by "sharing copies of their per-TN database" is described in Section 5.4. This Section describes three additional per-TN approaches where SPs agreeing to employ the per-TN method do so by "querying an external database" hosted by a Service Bureau or directly with the interconnecting SP.

5.5.1 Implementation

Some SPs subscribe to products offered by Service Bureaus to facilitate IP routing. For example, a Service Bureau subscribing to the LERG and NPAC feeds can manipulate and format data based upon the needs of an SP's internal routing service. SPs choosing the per-TN method can "opt-in" by sharing routing data with a Service Bureau, so that interconnecting SPs choosing to employ the per-TN method can perform a real-time per-TN query to obtain routing information. Alternatively, SPs may agree to query each others' per-TN database directly, but this is expected to be the exception. It is expected that Service Bureaus will synchronize the routing data of their subscribing SPs so that each will have authoritative routing information.

These three solutions do not require the development of existing or new shared industry infrastructure, but the database and query /response protocol should be uniform to facilitate interoperability. Also, uniformity as to how multiple registry providers may synchronize with each other so they can offer the same authoritative data to their respective SPs is also warranted.

Referring to Figure 5.10, each set of arrows lettered A thru C (and color coded) represent three possible per-TN implementations. (The black arrows represent the manual bilateral exchange of URI and IP addresses to resolve SIP URIs obtained via query. Note that this manual exchange of a limited quantity of routing data is commonplace among per-TN and Aggregation methods describe elsewhere in this document.)

- The green arrows (lettered A) depict the case where SPs directly query each other's per-TN database. This may be attractive to SPs having the operational capability that prefer not to outsource the query functionality to a Service Bureau.
- The blue arrows (lettered B) depict the case where SPs query a common Service Bureau, an example of where SPs have chosen the same Service Bureau to outsource query functionality.

- The red arrows (lettered C) depict the case where SPs do not use a common Service Bureaus, but allow their chosen Service Bureaus to exchange routing data on their behalf for query by SPs (subscribed to a different Service Bureau).

Note that each of the below three cases may be implemented simultaneously, allowing SPs to selected a Service Bureau that best meets their operational needs. It is expected that SPs would gain access to multiple Service Bureaus for interconnection purposes and that an ecosystem of Service Bureaus may evolve. The ability for Service Bureaus to provide both a query and bulk transfer service as discussed in Section 5.4 – coupled with the synchronization of routing data among multiple registries – would provide SPs with a broad range of options.

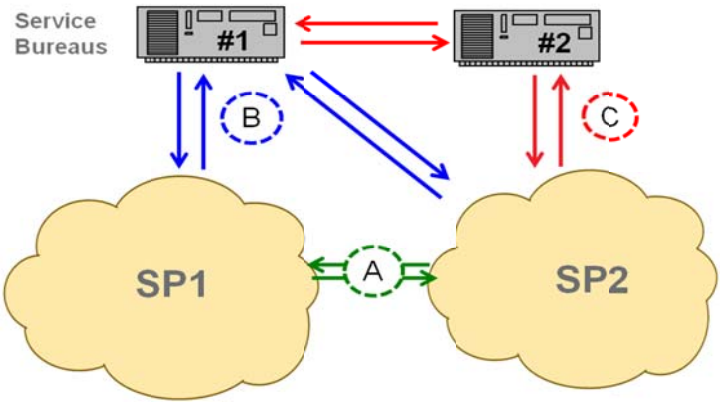

Figure 5. 10 - Service Bureau Implementation Examples

5.5.2 Provisioning

A Provisioning diagram is shown below in Figure 5.11. Note that only the case where both SPs employ a common Service Bureau is shown for simplicity.

In this provisioning example, SP1 provisions (black arrows) its Routing Service and DNS based upon information provided by SP2. SIP URIs are correlated with SBC interconnect IP addresses provided by SP2.

The SP1 and SP2 query each other's database or employ a Service Bureau to offer its per-TN database for query. For example, TNs can be correlated with a URI that is a full SIP URI (e.g., sip:+13036614567@example.mso-a.com;user=phone) but without the tel URI number portability parameters as defined in RFC 4694. How SP1 designs its routing service to use per-TN routing data is specific to SP1's implementation.

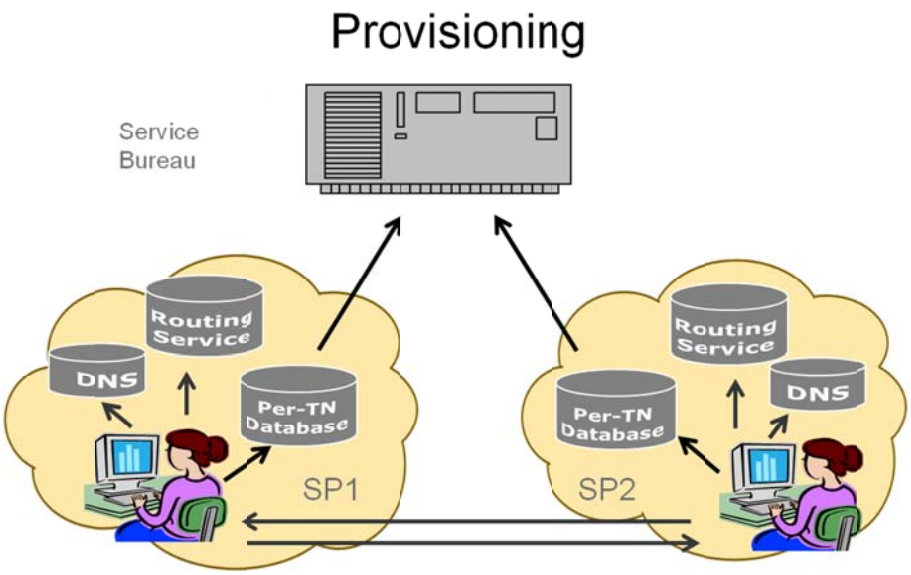

Figure 5. 11 - Provisioning - Query using Independent Service Bureau Call Flow

5.5.3 Call Flow

An example of the Call Flow is shown below in Figure 5.12:

1. Pat (non-roaming subscriber of SP1) makes a session request (e.g., places a call) to Mike (subscriber of SP2). SP1's network provides originating services based on Pat's subscription.
2. SP1's application server queries (2A) its routing service in real time using the called number to determine how to forward the request. The routing service first portability corrects the called number, and then determines that it is not subscribed to SP1. It then checks to see whether the code holder associated with the telephone number[12] is covered by an IP interconnection agreement. If so, SP1 queries (2B) the Service Bureau specified by SP2, and the SP1 routing service (2A) supplies[13] the application server with the ingress point through which SP2 has requested that session requests directed to this telephone number enter its network.
3. The application server identifies SBC-2 and (if applicable) SBC-1 in SIP ROUTE headers, and forwards the resulting session request onward. SP1's L3 processing resolves the host portion of the topmost ROUTE header (using DNS) to the IP address of SBC-1.
4. SBC-1 removes the topmost ROUTE header (which identifies itself) and forwards the session request based on the next one (which identifies SBC-2). To do so it resolves (using DNS) the host portion of that header, yielding the IP address of SBC-2.
5. SBC-2 removes the topmost ROUTE header (which identifies itself) and admits the message to SP2's network, forwarding it to an application server, and eventually to Mike. How SP2 performs these functions is SP specific.

[12] The "code holder" is a term used to refer to the SP serving the TN, which can be identified in LERG data using the LRN or the NPA-NXX of the telephone number (if not shown in the NPAC, e.g., ported or pooled).

[13] How this is accomplished is implementation specific. Messages from an application server to a routing service is typically an ENUM query, but in some networks a SIP message is sent to a proxy collocated with the ENUM service, which sends back a 302 "redirect" response.

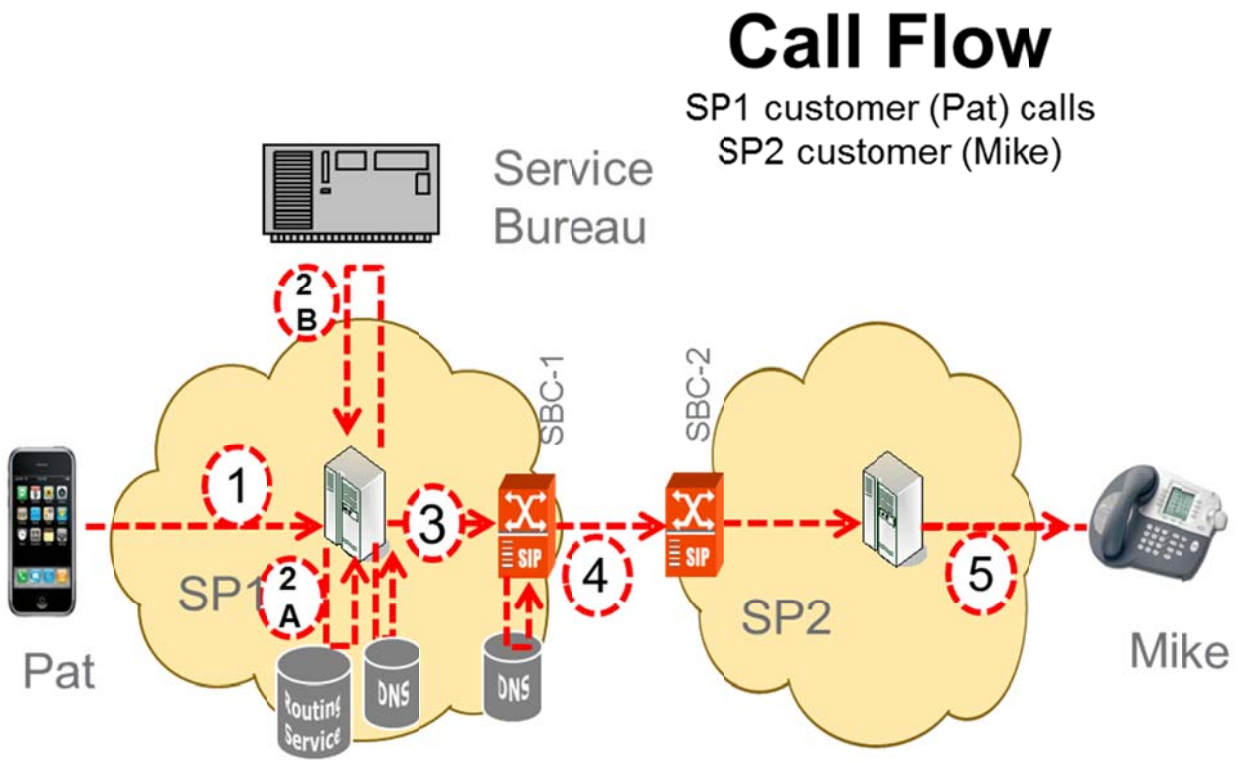

Figure 5. 12 - Call Flow - Query using Independent Service Bureau

6 Interoperability Between Aggregate & Per-TN Routing Data Approaches

This section discusses how the two previously discussed carrier routing approaches can co-exist (or potentially interoperate) with each other.

When considering interoperating between carriers it is important to recognize that the interconnection process has a number of steps that are common. For example:

1. Interconnection agreements are formally negotiated between carriers on a bilateral basis. This negotiation process will lead to a formal agreement between the carriers on a number of key points related to the interconnection, including an agreed to mechanism for exchanging routing data. As a result, there is no need to define an approach where two carriers with arbitrary preferences interconnect and exchange data without first agreeing on the approach each will use.
2. Under all scenarios being considered, carriers will use data from a variety of sources as input to their internal BSS/OSS to build and maintain an internal database for routing calls/sessions. Each carrier uses their own system, with their own algorithm(s), for this, and it is therefore out of scope for this IP_NNI Task Force. The routing data defined in this document is an important enabler for interconnection, but it is just one of the data sources used by the carrier to construct their own routing tables.

The key thing that differs between the proposed solutions is what specific data is to be exchanged between carriers as part of interconnection negotiation. This is an important aspect that has already been discussed in this document and it is assumed for this interoperability section.

Specifically, this section covers the case where carriers prefer to use different approaches and outlines a series of intermediate options that discuss potential industry “middle ground” positions.

6.1 Routing Data From an Aggregate SP To a Per-TN SP

There are several possibilities for how the per-TN SP may arrange to route to the Aggregate SP.

First, the Per-TN SP may simply agree to implement aggregate-based routing as described in Section 4.

The second alternative is to transform the aggregate routing data into a per-TN representation. In the basic case, a per-TN SP receives the aggregate data and then creates individual TN records in its routing server based on that data. For example, if an OCN to SBC IP address mapping is provided, the per-TN SP uses associated industry data to map the OCN into the set of TNs the aggregate SP is offering for IP traffic exchange. This involves determining the set of NPA-NXXs and/or thousands blocks under the OCN, creating a record for each TN, and then continuously removing records for numbers that have ported or pooled away from the aggregate SP and adding records for numbers ported or pooled into an LRN that is associated with the OCN (i.e., has an NPA-NXX with the code holder OCN of the aggregate SP). Thus, it is the responsibility of the Per-TN SP to update the record set based on changes industry data. Note that the expanded data set may include records for unallocated numbers. Except for misdials, these records would not be accessed.

The expansion described above could also be performed by a third party, either on behalf of the per-TN SP or the aggregate SP depending on business arrangements.

In the third party case the aggregate data could be delivered to a service bureau by the aggregate provider. Because the service bureau could distribute data to multiple per-TN providers records would not include IP addresses as these would be target service provider specific. The records however could map TNs to a supplied SIP URI with a generic host name keyed to the aggregation element provided in the bilateral exchange. For example, a SIP URI containing the hostname OCN “<ocn>.<spname>”.net might be used in the service bureau records. The per-TN provider could then populate the TN records in its routing server as described in Section 5 and resolve the host name in its local DNS, with records that match the host name to the IP address associated with the corresponding OCN in the bilateral data exchange.

6.2 Routing Data From a Per-TN SP To an Aggregate SP

There are likewise several possibilities for how an aggregate SP may route to the per-TN SP.

First, the per-TN provider may simply agree to provide aggregate routing data. Aggregate data may include TNs beyond those for which the per-TN SP prefers for IP interconnection. For example, a wireless SP that has both VoLTE (IP) and GSM/UMTS (non-IP) subscribers that are not distinguished from a NANP data construct view may simply provide mappings from, for example, its OCNs to its SBC IP addresses. This will result in some VoLTE originated calls transiting the IP interconnection even though they are destined for GSM/UMTS subscribers.

A second possibility is that the aggregate SP will accept per-TN information to populate its routing server even though it prefers to provide routing information for its own TNs on an aggregate basis. The per-TN data could be provided through a service bureau.

6.3 Registry Supporting Both Aggregate & Expanded per-TN Routing Data

In this case the aggregate input would map a NANP construct to a SIP URI rather than a set of IP addresses (as discussed in Section 6.1 above). Bilateral negotiation would then provide the URI to IP address mapping. A Registry could retain this aggregate input and make it available to SPs that prefer aggregate input via an interface to be defined. It could also expand this aggregate input and make it available to SPs that prefer per-TN data.

6.4 Using the NPAC to interoperate on a per-TN and aggregate basis

6.4.1 Overview

The solution introduced in this section assumes that some service providers will agree to use an aggregate routing data approach and others a per-TN routing data approach. The solution identifies just one potential

"middle ground" for industry consideration. It leverages the NPAC and approved North American Numbering Council (NANC) governance change orders designed to facilitate routing transition to next generation networks. The solution further draws on established practices and commercial third party offerings which have been enabling ubiquitous Short Message Service (SMS) routing, for example, across a broad range of specialized use cases. Specifically, this solution focuses on an approach for supporting the provisioning of both aggregate and per-TN level routing data into the NPAC and distributing it all at a per-TN level for consumption by any authorized service provider.

6.4.2 High Level Description

A key difference between the two currently proposed routing data approaches in Sections 4 and 5 is the granularity of information to be provisioned (shared) and managed by each service provider's routing service. However, once some service providers agree to use a per-TN data approach, then all other participating service providers will most likely need the capability to manage the associated per-TN data in their respective routing services.

The following solution is just one way to support the provisioning of both per-TN and aggregate routing data in the NPAC and builds on various third party services and published APIs that primarily support ubiquitous industry SMS routing today. The following description assumes that certain one-time activities previously discussed and common across both proposed routing data approaches have already taken place between service providers (e.g., IP connectivity established). This solution supports both per-TN and aggregate routing data input and expands the latter for direct provisioning into the NPAC.

It should be noted that this solution can support the NPAC in the role of either a Tier 1 (i.e., routing data in a format that identifies service provider Tier 2 servers – see also Section 5.2) or Tier 2 (i.e., routing data in a format that identifies an interconnect SBC, or I-SBC, domain, where the specific "trunk group" or "route" is ultimately designed through a bi-lateral service provider information exchange – see also Section 5.1). The remainder of this solution description assumes a Tier 2 role, where the routing data to be exchanged in the NPAC is in the form of a SIP URI like "sip: <telephone number>@sbc1.sp1.com". However, the solution doesn't rely on just this specific URI format.

6.4.3 Provisioning

Generally, the NPAC Location Routing Number (LRN) for ported telephone numbers or NANP NPA-NXX for native telephone numbers is used to route calls between service providers. Similarly, the NPAC Service Provider Identification (SPID) or NANP Operating Company Number (OCN) is typically used to route text messages between service providers. Over the past five years or so, multiple commercial wireless use cases have arose where the SPID or OCN associated with a particular telephone number in these recognized authoritative databases (after port-correction) was not sufficient for routing within the ecosystem. Further, these authoritative databases, at the time, were limited in their support of such use cases. Consequently, several commercial third party services were introduced to support these use cases while they work hand-in-hand with the recognized authoritative databases.

The key constraint in the NPAC has since been removed through one NANC governance change order that allows native telephone numbers and associated information to be stored in the NPAC. The PSTN to IP transition use case and others being discussed are analogous to those that have naturally evolved around text messaging where additional information beyond an NPAC LRN or NANP NPA-NXX is required in support of routing. The provisioning flow summarized below uses the NPAC in support of the use case(s) minimally discussed within this ATIS/SIP Forum IP-NNI Task Force. Specifically, it proposes to use the industry-approved VOICE URI field that is one field of many in the existing, standard NPAC database record. Further, it leverages at least one established commercial third party service to provision and maintain NPAC database records with URI field data inherently synchronized with aggregate routing data input.

Figure 6.1 below highlights the provisioning and distribution aspects of the solution. For illustrative purposes and in an attempt to just give the reader an introduction to how the solution can work, the aggregate routing data input is assumed to be in the form of an NPA-NXX (a native NANP 6-digit code or 6-digit LRN). Further, SP1 has agreed to use the per-TN routing data approach while SP2 wants to provision routing data at an aggregate level.

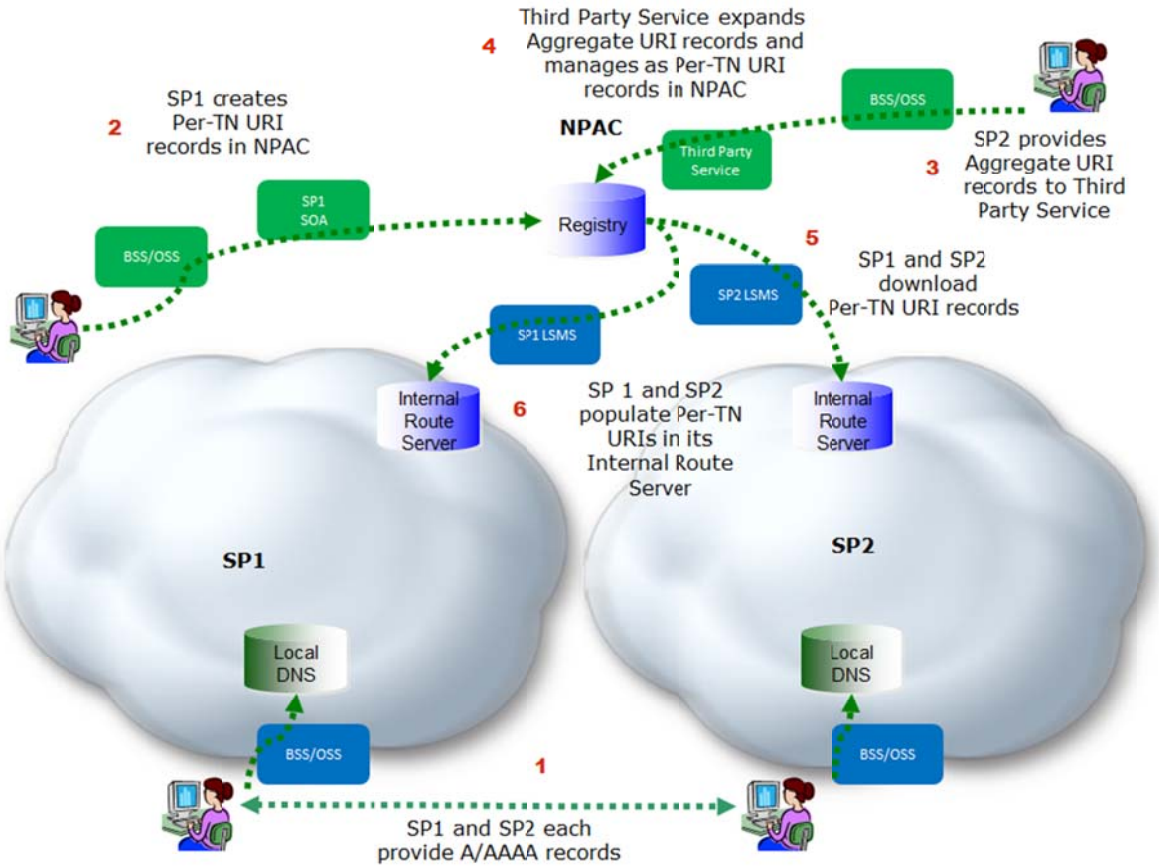

Figure 6. 1 - Provisioning

Using the NPAC to Interoperate on a per-TN and Aggregate Basis

1. SP1 and SP2 negotiate bilateral IP interconnection and exchange. In support of routing data exchange, each provides an agreed to mapping of IP address records (A/AAAA records) to FQDNs (or URI domains) corresponding to their respective I-SBCs. Each SP then provisions these records into their respective local DNS. An example of such a mapping for one URI domain could be:

URI Domain	IP Address
sbc1.sp1.com	138.34.23.3
sbc1.sp1.com	182.36.12.1
sbc1.sp1.com	58.23.12.90

2. SP1 populates the NPAC VOICE URI field in the associated subscription version (SV) record through its SOA (or equivalent) as new numbers are provisioned or existing numbers become available for IP interconnection. Again, the routing data to be exchanged is assumed, for this description, to be in the form of a SIP URI like “sip:<telephone number>@sbc1.sp1.com”.
3. SP2 shares aggregate routing data with an established third party service. For example,
   a. SP2 designates LRN 508-332 for IP interconnection.
   b. The associated ingress SBC domain is “sbc1.sp2.com”.

c. SP2 establishes a Letter of Authorization (LOA) with the third party supporting this solution (if such an LOA doesn't already exist).
d. The LRN/ingress SBC domain/Action is then shared with the third party service over one of several published APIs (e.g., a flat file with a row "508332,sbc1.sp2.com,A" where "A"=Add).

4. The third party service for SP2 expands aggregate routing data input and manages as per-TN VOICE URI field data in the NPAC on behalf of SP2. For one example use case,
   a. Third party service interprets row "508332,sbc1.sp2.com,A" in a shared flat file and generates the associated NPAC provisioning actions. For example,
      i. 15 numbers (SV records) were found to exist in the NPAC with LRN 508332XXXX
      ii. 15 Modify actions are then generated to add "sip:<telephone number>@sbc1.sp2.com" to the VOICE URI field for these SV records
   b. At a configured interval (e.g., every 15 minutes), check for new numbers with LRN 508332XXXX and generate associated Modify actions. Note that there is no action required for those numbers that are no longer associated with this LRN.
5. SP1 and SP2 download per-TN VOICE URI field data from each other (along with other existing NPAC data for number portability) through its LSMS (or equivalent).
6. SP1 and SP2 extract per-TN VOICE URI field data from each other (along with other existing NPAC data for number portability) and provision it into their respective internal route servers. Note that the details of how this routing data gets represented and used are specific to SP1 and SP2.

6.4.4 Call Flow

Figure 6.2 below illustrates a call flow with the proposed solution. For illustrative purposes, SP2 initiates a call (session) to SP1:

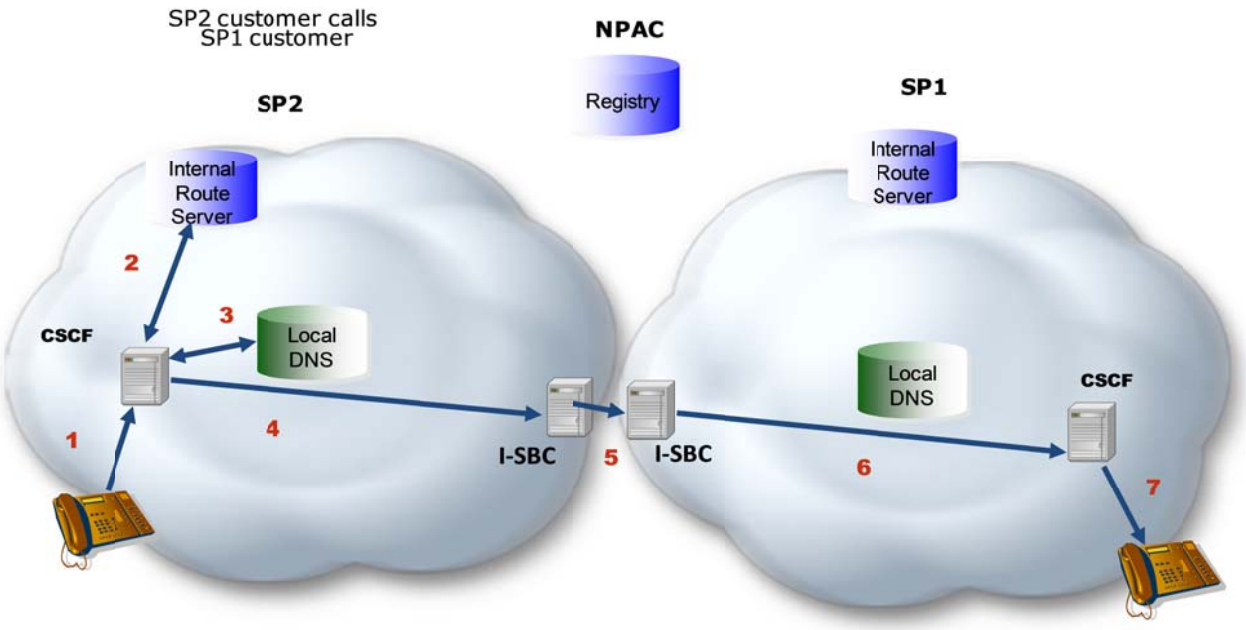

Figure 6. 2 - Call Flow - Using the NPAC to Interoperate on a per-TN and Aggregate Basis

1. SP2 customer dials destination number on SP1 network.
2. SP2 S-CSCF queries internal route server and SP2 route server responds back to S-CSCF with a port-corrected SIP URI containing the hostname of an agreed upon SP1 interconnect SBC.
3. SP2 S-CSCF resolves this hostname in the SIP URI through its local DNS to obtain the IP address of the SP1 interconnect SBC.
4. A SIP INVITE is sent to SP2 interconnect SBC that has layer 3 connectivity to the SP1 interconnect SBC.

5. The SIP INVITE is forwarded to the SP1 interconnect SBC.
6. SP1 interconnect SBC forwards the SIP INVITE to the SP1 S-CSCF.
7. SP1 S-CSCF terminates the call to its customer.

6.4.5 Summary

The solution proposed above is just one potential "middle ground" for industry consideration. It is instantiated over existing NPAC infrastructure and conforms to approved/adopted change orders. Using the NPAC to support the PSTN to IP transition use case (and others being discussed) also allows inherent data synchronization with number portability information. Further, the solution has built-in support for local downloads/caches of routing data. The solution is transparent to service providers who agree to use the per-TN routing data approach. For service providers who agree to use the aggregate routing data approach, the associated aggregate routing data (e.g., native NPA-NXX, LRN) can be shared through an established third party, expanded, provisioned and updated (on their behalf) as per-TN routing data in the NPAC. This per-TN routing data can then be directly consumed by any participating service provider.

Appendix A - Comparative Characteristics Matrix

The ATIS SIP FORUM IP-NNI Task Force developed the following list of comparative characteristics that may be useful in understanding the approaches discussed in this document.

#	Characteristics Group	Characteristics	Information type
1	Performance	Scalability	List issues & quantify
2		Reliability	List issues & quantify
3		Call setup time	Value range & conditions
4		Impact on signaling traffic	Quantify
5	Service requirements	Ability to specify interconnection information with finer granularity than at the service provider level	Yes/No
6		Ability to specify different interconnection attributes for different groupings of a service providers' numbers	Yes/No
7		Provides a mechanism for aggregation of routing information above the individual number level.	Yes/No
8		Provides a mechanism to get some insight into the service capabilities of destinations before routing a call.	Yes/No
9		Supports the ability to provide GETS.	Yes/No
10		Provide a mechanism for interconnecting carriers to identify different interconnection points (for a given group of TNs) depending on the originating carrier.	Yes/No
11		Enables the service provider connecting to the terminating provider to select the interconnect point, consistent with the preferences identified by the terminating carrier.	Yes/No
12		Provides the ability to exchange routing data between carriers in bulk.	Yes/No
13		Provides the ability to query a locally cached copy within each carrier, rather than always having to query the terminating carrier.	Yes/No
14		Provides a clear path to a global solution	Yes/No
15		Provides a good solution for the end-state all-IP network	Yes/No or degree?
16		Maintains backwards compatibility or method to interoperate during the transition to an all-IP network	Yes/No
17		Ability to support non-E.164 public user identities	Yes/No

18		Solution synchronized to number portability	Yes/No
19		Solution not tied to historical geography of numbering plan	Yes/No
20		Support for open Internet routing	Yes/No
21	Solution complexity	Time to implement – common infrastructure	Quantify
22		Impact on core network elements?	Enumerate & quantify
23		Impact on existing service provider systems	Enumerate & quantify
24		What external bodies are required to modify existing arrangements, systems, etc.?	Enumerate
25		Impact on existing industry systems	Quantify
26		Level of dependence on "CO codes", even during the transition?	Quantify
27		Need for additional industry systems & interfaces?	Quantify
28	Security	Increase in vulnerability	Quantify
29		Support for secure tunnels	Yes/No