ETSI TR 102 055 V1.1.1 (2005-05)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); ENUM scenarios for user and infrastructure ENUM

Reference
DTR/TISPAN-04001

Keywords
ENUM, USER

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document identifies a range of issues which occur if providers of communication services and networks (called Communication Service Providers (CSP) within the present document) consider using the concepts developed in RFC 3761 [16] (ENUM) for infrastructure purposes. Such an approach would result in the application of the ENUM concept to the provision of information for routeing (both internally and for the interconnection of networks - also called peering), including information for number portability, freephone and other number or address translation capabilities, SMS and MMS, etc.

It considers the likely steps along the way and where possible, identifies alternative options and approaches.

It will specifically identify:

- Issues which occur if providers of IMS-based NGNs consider peering traffic with each other via Points-of-Interconnect based on IP technology, by using E.164 numbers to address end-points they are hosting for their subscribers.

- Issues which occur if providers of IMS-based NGNs consider peering traffic with other providers e.g. IMS-based PLMNs and also with providers on the Internet.

Out-of-scope are requirements for using Infrastructure ENUM for peering of transit traffic not targeted for end-points within the providers control.

2 References

For the purposes of this Technical Report (TR), the following references apply:

NOTE: The present document is based additionally on "Work in Progress" at the IETF, documented in Internet Drafts. This is especially valid for the definitions of the "ENUMservices" in the NAPTR RR, which are based on the definitions in RFC 3761 [16].

[1] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[2] ETSI TS 102 051: "ENUM Administration in Europe".

[3] IETF RFC 1034: "Domain Names - Concepts and Facilities".

[4] IETF RFC 1035: "Domain Names - Implementation and Specification".

[5] IETF RFC 1123: "Requirements for Internet Hosts - Application and Support".

[6] IETF RFC 1591: "Domain Name System Structure and Delegation".

[7] IETF RFC 1738: "Uniform Resource Locators (URL)".

[8] IETF RFC 2181: "Clarifications to the DNS Specification".

NOTE: Updates: IETF RFC 1034, IETF RFC 1035, IETF RFC 1123.

[9] IETF RFC 2182: "Selection and Operation of Secondary DNS Servers".

[10] IETF RFC 2255: "The LDAP URL Format".

[11] IETF RFC 2368: "The mailto URL scheme".

[12] IETF RFC 2396: "Uniform Resource Identifiers (URI): Generic Syntax".

[13] IETF RFC 2616: "Hypertext Transfer Protocol - HTTP/1.1".

[14] IETF RFC 3966: "The tel URI for Telephone Numbers".

[15] IETF RFC 2818: "HTTP Over TLS".

[16] IETF RFC 3761: "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".

[17] IETF RFC 3261: "SIP: Session Initiation Protocol".

[18] IETF RFC 3401: "Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS".

[19] IETF RFC 3402: "Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm".

[20] IETF RFC 3403: "Dynamic Delegation Discovery System (DDDS). Part Three: The Domain Name System (DNS) Database".

[21] IETF RFC 3405: "Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA Assignment Procedures".

[22] IETF RFC 3508: "H.323 Uniform Resource Locator (URL) Scheme Registration".

[23] IETF RFC 3762: "Telephone Number Mapping (ENUM) Service Registration for H.323".

[24] IETF RFC 3764: "Enumservice Registration for Session Initiation Protocol (SIP) Addresses-of-Record".

[25] IETF RFC 3861: "Address Resolution for Instant Messaging and Presence".

[26] ETSI TS 102 172: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Minimum requirements for interoperability of ENUM implementations".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Address-of-Record (AoR): within SIP, an address-of-record represents an identity of the user, generally a long-term identity, and it does not have a dependency on any device; users can move between devices or even be associated with multiple devices at one time whilst retaining the same address-of-record

NOTE: A simple URI, generally of the form "sip:egdar@example.com", is used for an address-of-record.

apex: name of a delegation point in the DNS. For example, the zone apex for the public ENUM name space is e164.arpa

border element: generic term used for any device separating intranets, extranets and the public Internet

NOTE: It may consist of firewalls, session border controllers and may provide Network Address Translation (NAT) functions.

Communication Service Provider (CSP): any entity providing communications services using E.164 numbers to "End Users" and using an infrastructure to provide routeing capabilities

NOTE: The "End Users" may be on the Internet, within an IMS based NGN or even on the PSTN.

domain: set of names within the DNS consisting of a single domain name and all the domain names below it

E.164: International Public Telecommunications Numbering Plan

E164 number: number taken from the International Public Telecommunications Numbering Plan

ENUM: protocol developed by the IETF as RFC 3761 [16] to be used within e164.arpa

ENUMservice: parameter held in the Service Field of a NAPTR Resource Record associated with the ENUM DDDS Application that indicates the class of functionality a given URI Scheme offers

NOTE: According to RFC 3761 [16] an "ENUMservice" is defined in an RFC and officially registered with IANA (see http://www.iana.org/assignments/enum-services).

End user: entity using the services provided by the CSP. This may be IP Communication services including Infrastructure ENUM

ENUM End User: entity using ENUM services in e164.arpa

extranet: any IP network within the full control of a group (confederation) of CSPs. It is both separated from the intranets of the participating CSPs and from the public Internet by border elements

NOTE: It may or may not have an IP address space part of the public IP address space. Here only the extranet containing the DNS and Infrastructure ENUM is of concern.

infrastructure ENUM: See clause 4, "Introduction". Other terms used are Carrier ENUM or Operator ENUM.

intranet: any IP network within the full control of an CSP

NOTE: It is separated from other IP networks (extranets or the public Internet) by one or more border elements. It may or may not have an IP address space part of the public IP address space.

Naming Authority Pointer Resource Record (NAPTR): Naming Authority Pointer Resource Record is a DNS Resource Record type specified in RFC 3403 [20] that can be used to generate URIs

Number Portability: ability of an end user to change location within a geographic area, between service providers or services, without changing their number

NOTE: This must be in accordance with the portability requirements pertaining to each specific type of E.164 number.

Point-of-Interconnect (PoI): access point between two networks

NOTE: The PoI may be any type of border element such as session-border-controller, ingress gateways, SIP server, gatekeeper, etc. or the VoIP servers may be reached directly via the Internet.

private name space: name space in the DNS which is private to a CSP and is typically only visible to an organization's internal network

public name space: name space in the DNS that is visible on the public Internet

shared name space: name space in the DNS that is visible to a group of CSPs but not visible to the Internet

tier: delegation point within DNS for administrative or technical purposes. In the present document the Tier 0 is the global Apex for an instance of Infrastructure ENUM

NOTE: Depending on the model and architecture used in an instance of Infrastructure ENUM there may be one or more Tiers.

Uniform Resource Identifier (URI): compact string of characters for identifying an abstract or physical resource (e.g. an application)

NOTE: An URI is used within a NAPTR Resource Record to point to a specific application.

Uniform Resource Identifier (URI) Schemes: in the Uniform Resource Identifier (URI) definition (RFC 2396 [12], RFC 1738 [7]) there is a field, called "scheme", to identify the type of resource

NOTE: URI Schemes are defined in RFCs and officially registered with the IANA (see http://www.iana.org/assignments/uri-schemes).

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AoR	Address-of-Record
CSP	Communication Service Provider
DNS	Domain Name System
IAB	Internet Architecture Board
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISUP	ISDN User Part
MMS	Multi-Media Message Service
NAPTR	Naming Authority PoinTer resource Record
NAT	Network Address Translator
NGN	Next Generation Network
NS	NameServer
PLMN	Public Land Mobile Networks
PoI	Point of Interconnect
PSTN	Public Switched Telephone Network
RFC	Request For Comment (IETF related standard)
RRs	(DNS) Resource Records
SCN	Switched Circuit Network
SIP	Session Initiation Protocol
SMS	Short Message Service
TDM	Time Division Multiplex (a synonym for circuit-switched networks)
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VPN	Virtual Private Network

4 Introduction

It is necessary to understand the fundamental differences between ENUM in e164.arpa and Infrastructure ENUM as discussed in the present document.

4.1 ENUM in e164.arpa

RFC 3761 [16] together with RFC 3403 [20] defines the ENUM protocol and the NAPTR records. RFC 3761 [16] discusses the use of the Domain Name System (DNS) [2], [3] for storage of E.164 numbers and how DNS can be used for identifying available services connected to one E.164 number.

Through transformation of E.164 numbers in the international format [1], into DNS names and the use of existing DNS services like delegation through NS records and NAPTR records, one can look up what services are available for a specific E.164 number in a decentralized way with distributed management of the different levels in the lookup process.

RFC 3761 [16] states in the introduction:

"The domain "e164.arpa" is being populated in order to provide the infrastructure in DNS for storage of E.164 numbers. In order to facilitate distributed operations, this domain is divided into subdomains. Holders of E.164 numbers which want to be listed in DNS should contact the appropriate zone administrator according to the policy which is attached to the zone. One should start looking for this information by examining the SOA resource record associated with the zone, just like in normal DNS operations. Of course, as with other domains, policies for such listings will be controlled on a subdomain basis and may differ in different parts of the world."

This implies:

- that for ENUM the domain "e164.arpa" MUST be used as the basis for storing E.164 numbers in the DNS; and
- that the administration of ENUM is a national or regional matter.

The implementation of RFC 3761 [16] has therefore led to specification of the administrative requirements in TS 102 051 [2] "ENUM Administration in Europe" and also to the specification of the minimum requirements for interoperability of ENUM implementations in TS 102 172 [26]. TS 102 051 [2] draws attention to the importance of the opt-in principle in order to preserve users' privacy rights. This means that the "ENUM Subscriber" is providing the data and the information can be retrieved and utilized by "ENUM End Users", but also by Communication Service Providers (CSP). How this information may be retrieved and processed by both ENUM End Users and CSP is described in TS 102 172 [26].

4.2 Infrastructure ENUM

Infrastructure ENUM is basically about publishing the information which E.164 numbers a CSP is hosting to either a group of selected peers or to all other CSPs.

The present document looks at the application of the concepts in ENUM for the different purpose of provision of information for routeing (both internally and between networks), including information for number portability, freephone and other number or address translation capabilities, SMS and MMS, and so on. This information is provided exclusively by and to CSPs, the End User has either no access to this information or may not be able to use it. This is incompatible with the opt-in principle because it may need full population of the information. Hence, it would have to logically be implemented as a separate system. For this reason, the system we are describing in the present document is referred to as "Infrastructure ENUM".

Infrastructure ENUM as described here would be used to facilitate routeing between CSPs to certain entities of other networks (e.g. a switch, an egress gateway, a point-of-interconnect to another network, etc.), within an Extranet or on the public Internet. These entities are called in the rest of the document border elements. It may also provide or replace simple translation-functions e.g. providing routeing numbers for number portability, for freephone numbers, SMS, MMS routeing.

4.3 Major differences between Infrastructure ENUM and ENUM in e164.arpa

Table 1 clearly shows there are major differences between the requirements of Infrastructure ENUM and ENUM.

Table 1: Comparison of attributes of Infrastructure ENUM and ENUM in e164.arpa

Key issues	Infrastructure ENUM	ENUM in e164.arpa
Who decides to participate in the ENUM scheme?	CSP	Country (Administration) ENUM subscribers
By whom is information required?	CSPs only	Optional information
By whom is information supplied?	CSPs	ENUM subscribers
Who can upload information?	CSP serving the E.164 number	Any single ENUM Registrar per E.164 number
How is information populated?	All E.164 numbers inserted, no opt-in for single subscribers	Opt-in for each ENUM subscriber
Who has access to information?	Intended for CSPs only	Any entity
Is retrieval of information controlled?	Yes	No
Is a domain defined?	No	Yes: e164.arpa

There are different methods which can be adopted to implement Infrastructure ENUM.

If a CSP uses DNS functionality within a non-public IP network for internal purposes (Intranet), this is an internal matter. The present document gives some advice how to implement this. This functionality is called CSP-internal Infrastructure ENUM in the rest of the document.

If a group of CSPs uses DNS functionality within the Internet or a non-public IP network (Extranet), this is an internal matter of the group. The present document gives some advice how to implement this. This functionality is called CSP-shared Infrastructure ENUM in the rest of the document.

It is assumed that the information retrieval and processing in Infrastructure ENUM is done in the same way as defined in TS 102 172 [26] for ENUM and that therefore Infrastructure ENUM is technically compatible with all related RFCs, especially regarding RFC 3761 [16], the "enumservices" registered with IANA and defined in TS 102 172 [26].
No additional requirements have been identified yet.

4.4 Choice of an domain apex for Infrastructure ENUM

An additional document will cover the requirements to make Infrastructure ENUM work, operational and policy aspects and issues around the choice of the apex. However, at this stage it is recognized that an additional apex to that used for ENUM (e164.arpa) will be required.

If such an approach is not adopted, a CSPs ability to utilize Infrastructure ENUM would be inhibited unless his Administration had decided to opt-in into e164.arpa. The implementation of Infrastructure ENUM should not be dependant on Administration agreement concerning the delegation of the required domain (c.c.e164.arpa).

Additionally for ENUM the choice of the delegation and the DNS nameservers for the NAPTRs for a given E.164 number lies with the end-user, whereas for Infrastructure ENUM the choice lies with the CSP that currently serves the number. And so the ENUM and Infrastructure ENUM trees are incompatible and have to be separate.

Although the apex of this new tree(s) could be in any domain, .arpa (e.g. "e164i.arpa" or "i.e164.arpa") is preferred because it is defined for infrastructure purposes. The rationale behind this choice is in principle the same as for e164.arpa. Within this approach approval from the IAB is necessary.

As described in step 5b in clause 8, a globally shared namespace approach is required which raises the issue of what domain should be used as the apex. Infrastructure ENUM should be implemented via a different namespace for CSP-populated E.164 numbers to that used for subscriber populated E.164 numbers.

In User ENUM because of the agreements between IAB, ITU-T and RIPE NCC and the interim procedures a tiered approach is defined at least for Tier 0 and Tier 1, where the Tier 0 is defined as the root of the E.164 numbering plan administered by ITU-T and operated by RIPE NCC, and the Tier 1 the implementation of the national numbering plan.

The structure within and below Tier 1 in User ENUM is a national matter.

In a CSP-shared Infrastructure ENUM system the structure of the Tiers is a matter of the participating CSPs. In general there can be assumed that there will be a combined Tier 0/Tier1.

The public e164.arpa name space will not be appropriate for Infrastructure ENUM. There are several reasons for this.

- Firstly, the use of the public e164.arpa domain is constrained by the procedures agreed between ITU, IAB, RIPE NCC and Administrations. CSPs will need to enter E.164 numbers into a name space for Infrastructure ENUM irrespective of whether delegations for country codes have been made in the public e164.arpa tree.

- Secondly, the public e164.arpa space will normally be governed by the opt-in principle. Numbers would only be entered with the explicit consent of the end user. This is clearly impractical for the operation of a CSP's service.

- Finally, it is highly unlikely that the information CSPs publish in the name space for Infrastructure ENUM should be public. It may contain details of border gateways that cannot be reached from the public Internet. Public dissemination of this information could also disclose details about the topology and operation of the CSP's network.

5 Types of Infrastructure ENUM

In the following clause the different types of Infrastructure ENUM are explained in more detail.

5.1 CSP-internal Infrastructure ENUM

CSP-internal Infrastructure ENUM uses DNS data existing and accessible only within the CSPs environment (Intranet).

CSP-internal Infrastructure ENUM is intended to be used by a given CSP to reach the border elements within his Intranet to other CSPs, the gateways within his Intranet providing Point-of-Interconnect to different Telephony Service Providers on the PSTN, and also to reach the end-users connected in his Intranet.

NOTE: Reaching the End User means that the Address-of-Record (AoR) of the End-User (the address of the server where the user is registered) is provided in Infrastructure ENUM. This does never mean to provide directly the contact address of the End-User's device (see ENUM SIP RFC 3764 [24]).

CSP-internal Infrastructure ENUM may be used in any suitable DNS domain. The DNS may be a private namespace or part of the public namespace. One solution is the use of split DNS using the same domain names as the public namespace used for global or CSP-shared Infrastructure ENUM, but providing a different view in the private namespace.

It is a CSP decision if it uses a separate tree for CSP-internal Infrastructure ENUM or uses the same tree as the preferred Infrastructure ENUM system with Split DNS.

The intended use for CSP-internal Infrastructure ENUM is:

1) to find users and their services for routeing within the own network (Intranet);

2) to find the border elements connected to other CSPs, the public Internet and the gateways to the PSTN within the own network (Intranet);

3) to access translation databases belonging to this CSP from inside the network (Intranet) using ENUM technology;

4) to hide the users and the infrastructure behind border elements and give outside CSPs only access to these border elements.

5.2 CSP-shared Infrastructure ENUM

CSP-shared Infrastructure ENUM uses DNS data accessible at least by all CSP participating in the system. It is a policy decision whether the data for the Infrastructure ENUM system is in the public DNS and if it is accessible by the public (see below).

CSP-shared Infrastructure ENUM is intended to be used by Communication Service Providers (CSP) to reach the border elements of other CSPs, it is not intended to be used by end-users and the end-users of other CSPs directly. End-users (ENUM End users) will only use ENUM within e164.arpa to reach other end-users directly.

NOTE: If the CSPs network is open to the shared Infrastructure and directly accessible by other CSPs, the CSP may also chose to provide the location of his end-users (AoR) directly.

Shared Infrastructure ENUM may be used in any suitable DNS domain (apex), a group of CSP mutually agrees upon. It is recommended by ETSI (for a rationale see clause 4.4) that CSPs agree on a common domain tree, preferable in .arpa, for Infrastructure ENUM use, although the use of a limited number of different domains by different groups of CSPs is also possible. A given CSP may also access more than one Infrastructure ENUM domain and also propagate his data in different Infrastructure ENUM domains.

It is of course the choice of the participating CSPs if this system is using the public namespace or not.

5.3 Global (or Common) Infrastructure ENUM

If all CSPs using Infrastructure ENUM would agree to share ONE common Infrastructure ENUM system containing all E.164 numbers hosted by the participating CSPs, this system would be able to provide potentially global and common connectivity between all CSPs. Additional Infrastructure ENUM systems would not be necessary.

This would ensure global access to the latest information that remains under the control the CSP responsible for that part of the infrastructure, basically which provider is hosting which E.164 number including up-to-date information about ported/ceased numbers, etc. on a global scale.

It is of course the choice of the CSPs if this system is using the public namespace or not.

6 Authentication aspects

Unlike User ENUM, all the participants in an Infrastructure ENUM environment are considered to be trusted parties, so it may not be necessary to implement any authentication (validation) process when a communications provider wishes to populate a given number or number range. This is particularly the case where the group is a series of co-operating communications providers.

However, the concept of Infrastructure ENUM will expand so that the participants are merely communications providers who have agreed that it would be mutually beneficial to share information via ENUM, but who, at a commercial level, are competitors. In this situation, it will be necessary to address whether some form of authentication is appropriate, e.g. to prevent situations where call hijacking could occur.

The likelihood is that in this situation a mechanism will be required to confirm that a given communications provider has been assigned a given number or number range. However, it is assumed that this process could be very basic when compared to that for user-ENUM, and also that there will not be any necessity to confirm the identity of the service provider.

It may be necessary to safeguard the integrity of DNS data from attacks on the DNS infrastructure. These threats include the accidental or deliberate publication of bogus DNS data, DNS spoofing attacks and tampering with DNS responses to hijack traffic. Possible defensive measures could include the use of Secure VPNs or DNS security protocols such as Transaction Signatures and Secure DNS.

7 Architectural options

A number of architectures can be adopted by a group of communications providers for infrastructure ENUM. No single approach will be optimal in all cases. The most appropriate architecture should be selected according to the particular circumstances. It should be noted that the different models could be mixed in one group, e.g. different models for different number ranges.

In a CSP-shared Infrastructure ENUM system the structure of the Tiers is a matter for the participating CSPs. In general it can be assumed that there will be a combined Tier 0/Tier1. The models described here therefore assume that only one Tier equivalent to the Tier 1 is existing on the apex.

Regardless of the model chosen, careful consideration needs to be given, particularly in the start-up phase, as to how networks should behave when an Infrastructure ENUM query does not result in NAPTR records being returned. This could be because the serving operator has not entered any information into Infrastructure ENUM, or because the operator has entered data, but the particular number is not in service. In the former case, alternate routeing procedures should be followed, but in the latter, the call should be dropped. Measures need to taken so the two scenarios can be distinguished between. One solution could be the usage of the "enumservice" void as described in TS 102 172 [26] and defined draft-ietf-enum-void-01.txt.

Annex A provides a non-exhaustive set of examples of architectures which could be adopted, setting out the advantages and disadvantages of each.

8 A possible evolution path

The following steps are likely to occur if a natural progression towards a global implementation of Infrastructure ENUM takes place although any step can be implemented at any time as a stand alone scenario.

Step 0: Current Situation on the PSTN

- Communication Service Providers (CSP) on the PSTN using TDM technology are interconnected on the PSTN via TDM Points-of-Interconnect (PoI) and use conventional routeing of calls (the existing scenario).

Step 1: CSP Islands connected via PSTN

- Communication Service Providers (CSP) migrate within their networks partially or completely from TDM to IP based technology.
- Connectivity to other CSPs is via IP/TDM gateways using conventional signalling (e.g. ISUP). So from the outside they still look like CSPs using only TDM technology.
- All calls originating or terminating in the IP-based network are routed to the PSTN/ISDN or incoming via the PSTN/ISDN.
- The IP network used for signalling and media-stream has no connectivity to any other IP networks or the Internet. This is called an Intranet.

  This is completely under each individual operator's control and would require no additional public infrastructure.

Step 2: Private Infrastructure ENUM only

- CSPs will use initially Infrastructure ENUM for routeing within their own networks (intranet approach).
- The CSP is setting up the complete DNS infrastructure required for Infrastructure ENUM within his own Intranet. This includes an internal apex, Tier 0, Tier 1 and Tier 2 (which will be in most cases combined in one database), so there is an internal registry function.
- The information contained in the NAPTR RR gives either internal destination points to end-users or PSTN/ISDN routeing information.
- Infrastructure ENUM may or may not indicate routeings to other networks.
- There is no "single" common, external apex required.
- The connectivity with other CSPs is still via the PSTN/ISDN/PLMN, as in Step 1.
- The IP network used for signalling and media-stream has no connectivity to any other IP network or the Internet. This is called an Intranet.

  This is completely under each individual CSPs control and would require no additional public infrastructure.

Step 3: Private Infrastructure with IP based Interconnect

- CSPs will interconnect their IP-based networks with other IP-based networks on a bilateral basis via Border Elements. Border Elements may do NAT, firewalls, protocol and code conversion between the two intranets, as required.
- The connectivity with CSPs not providing IP-based Points of Interconnect may still be via the PSTN/ISDN/PLMN, as in Step 1 and 2.
- The CSP is setting up the complete DNS infrastructure required for Infrastructure ENUM within his own intranet. This includes internal apex, Tier 0, Tier 1 and Tier 2, so there is an internal registry function.
- The information contained in the Tier 2 (NAPTRs) gives either internal destination points, IP based routeing information or PSTN/ISDN/PLMN routeing information.
- Infrastructure ENUM may or may not indicate routeings to other networks.

- There is no "single" common, external apex required.

  This is completely under each individual CSPs control and would require no additional public infrastructure.

Step 4: CSP-shared Infrastructure ENUM with extranet between a group of service providers

- CSPs will require connectivity between groups of CSPs via a shared extranet.
- The intranets are connected in addition to the existing connections to the PSTN/ISDN/PLMN and to the bilateral IP connections also to the extranet via additional Border Elements. These Border Elements may do NAT, firewalls, protocol and code conversion between the intranet and the CSP-shared extranet, as required.
- Within this CSP-shared extranet a CSP-shared Infrastructure ENUM is also set up.
- This CSP-shared Infrastructure ENUM requires a CSP-shared apex within the extranet, a CSP-shared Tier 0/1 and therefore also a CSP-shared external registry. The NS records in the common Tier 1 are pointing to the Tier 2 Nameserver of the CSPs participating in the extranet. The participating CSPs may also decide to host all NAPTR RR in the CSP-shared Tier 1 by uploading (exporting) the data.
- The Tier 2 Nameservers of the CSP are connected to the extranet and are holding NAPTR records for the E.164 number range this specific CSP is hosting and these NAPTR records hold URIs pointing to the ingress gateways (border elements) connected to the extranet to be used for these numbers.
- It should be noted that the CSP still has the complete DNS infrastructure required for Infrastructure ENUM within his own intranet as in Step 2 and 3. The only difference is that he now may keep only the entries belonging to numbers which are hosted by himself. All other entries belonging to numbers not hosted by himself may be deleted or replaced with default entries, e.g. pointing to the border elements from the inside.
- The infrastructure ENUM DNS in the CSP's intranet is overlaid to the CSP-shared infrastructure ENUM DNS in the extranet. So if an CSP A queries ENUM in his intranet, he is always querying his own Infrastructure ENUM. If he is querying a number he is hosting himself, he gets the answer from his own Infrastructure ENUM database, if he is querying a number he is not hosting, the Infrastructure ENUM DNS is passing the query through to the extranet and getting an answer from the Tier 2 operated by the CSP B hosting this number. (in case of split DNS). Note: If the CSP is not using split DNS, he needs to query his private DNS first to get to the border element and then query the common Infrastructure DNS to get the routeing to CSP B.
- If another CSP B is querying a number hosted by CSP A, he gets an answer from the ENUM Tier 2 Nameserver connected to the extranet. This answer may differ from the answer CSP A may get if he is querying the Infrastructure ENUM DNS from the intranet. This is called split DNS.

  The Infrastructure ENUM DNS in the intranet is still completely under the control of the CSP, the Infrastructure ENUM Tier 0 and Tier 1 Registry is under CSP-shared control, the ENUM Tier 2 Nameserver in the extranet is again under the control of the CSPs.

  This implementation requires the provision of a CSP-shared Tier 0/1 and requires prior agreements as to how this is set up.

Step 5a: Common Infrastructure ENUM within a global shared extranet

If the above extranet is created by a group of CSPs, independent extranets may be created by other groups of CSPs.

If these groups now decide to make a common "shared" extranet, there exist two possibilities:

a) The groups decide to keep their CSP-shared extranets and overlay a new common shared extranet on top. The procedure to do this is in principle the same as in step 4 creating a CSP-shared extranet between a group of CSPs. In principle the procedure is recursive, but definitely not recommended.

b) The groups decide to merge their CSP-shared extranets. This is the more simplistic way in terms of complexity, but may cause problems with duplicate IP addresses and duplicate registries and/or namespaces.

It is therefore strongly recommended to plan for a common, global "shared" extranet from the beginning.

In all of the above cases no single shared namespace is required for Infrastructure ENUM, because all implementations are within private networks.

Step 5b: Public Infrastructure ENUM on the Internet

A group of CSPs could decide to use the public Internet as CSP-shared network from the beginning, or if two extranets are to be merged, the two groups may decide to use the Internet for a common public "shared" Infrastructure ENUM.

In principle any domain can be taken as Infrastructure ENUM Tier 0/1 apex.

There could be one or more public Infrastructure ENUM systems.

9 Likely Infrastructure ENUM usage scenarios

IMS-based NGN providers may either control/manage their own communications network, being also a communication network provider, or provide their service as an application on the Internet.

The subscribers may have access to the above mentioned end-points either via the Internet, via dedicated networks or even via the PSTN.

The primary questions are, depending on the peering architecture chosen by IMS-based NGNs providers:

- How do I find the ingress PoI (or IMS servers) of a IMS-based NGN provider hosting a certain E.164 number, if a common network infrastructure is used?
- How do I find the egress PoI from within the own network if no common infrastructure is used?
- What are the options available for the Infrastructure ENUM architecture for the above mentioned cases?
- What are the Identifiers used to address the ingress or egress PoIs within ENUM?
(URIs used within NAPTR)

Some examples are shown below of the likely infrastructure ENUM usage scenarios as introduced in clause 9.

9.1 Private Infrastructure ENUM only (Step 2)

A CSP is using Private Infrastructure ENUM only within his own network (Intranet). There are only connections to the PSTN via IP-Gateways.

Infrastructure ENUM is used to find end-users in the own network (Intranet) and the proper gateway for calls routed to the PSTN.

All E.164 numbers not assigned to end-users are routed to the PSTN gateways.

The Infrastructure ENUM database may be implemented in any DNS domain at the CSP discretion and holds the following information:

For every end-user within the CSP's network a zone entry in ENUM exists for the related E.164 number.

For numbers ported out to other operators also a zone entry exists for the related E.164 number. It contains an "sip" or "h323" URI pointing to the gateway serving either directly the ported out number or a transit network. The zone entry may also contain a "tel" URI with a routeing number. The NAPTR RR containing the "tel" URI will then be used by the gateway. If only one gateway exists to the PSTN, the zone entry may only contain the "tel" URI and the routeing to the gateway may be done by default.

Numbers out of the number range assigned to this network but not assigned to end-users (unassigned numbers) must contain a NAPTR with enumservice "void" as all numbers will be entered in the DNS. This could be handled with a common NAPTR at the zone related to the whole number range as described in TS 102 172 [26].

Number ranges not assigned within this network may contain a "wild card" NAPTR at the zone related to the number range pointing to a PSTN gateway serving this number range.

Number ranges not assigned to any operator should contain a NAPTR RR with enumservice "void".

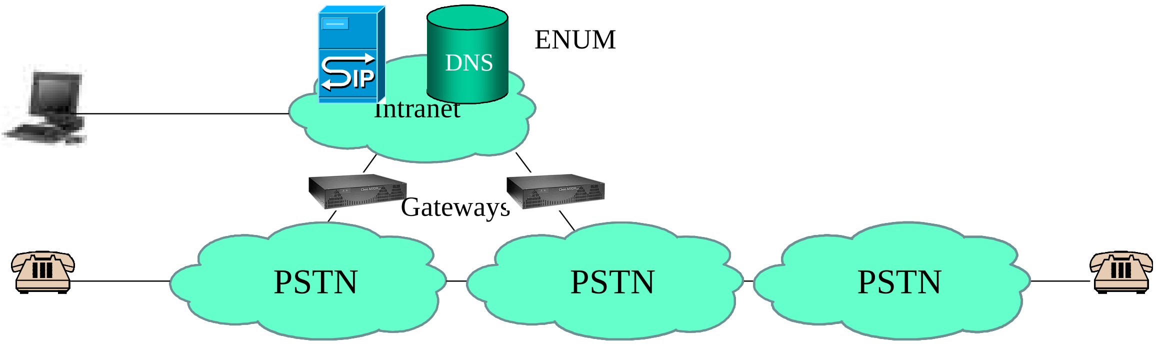

Figure 1

9.2 Private Infrastructure ENUM with IP-based Interconnect (Step 3)

A CSP is using Private Infrastructure ENUM only within his own network (Intranet), there are connections to the PSTN via IP-Gateways and in addition there are direct IP-based connections to other CSP via border elements.

Infrastructure ENUM is used to find end-users in the own network (Intranet), the proper gateway for calls routed to the PSTN and the proper border element for calls to number ranges hosted by the other CSP.

Numbers out of the number range assigned to this network but not assigned to end-users (unassigned numbers) must contain a NAPTR RR with enumservice "void" as all numbers will be entered in the DNS. This could be handled with a common NAPTR RR at the zone related to the whole number range as described in TS 102 172 [26].

Number ranges not assigned within this network should be routed either to SCN Gateways or to the border elements.

In this step, the Infrastructure ENUM database may be implemented in any DNS domain at the CSP's discretion and holds in addition to the information described in the above clause also NAPTR RRs pointing to the border elements.

These NAPTR RR contain "sip" or" h323" URIs indicating the IP-address or domain name of the border element and the E.164 number as the user-info, e.g. sip:+4319793321@border1.prov.net

The border elements in the other CSPs are querying their own private Infrastructure ENUM database to route the call further in their own Intranets.

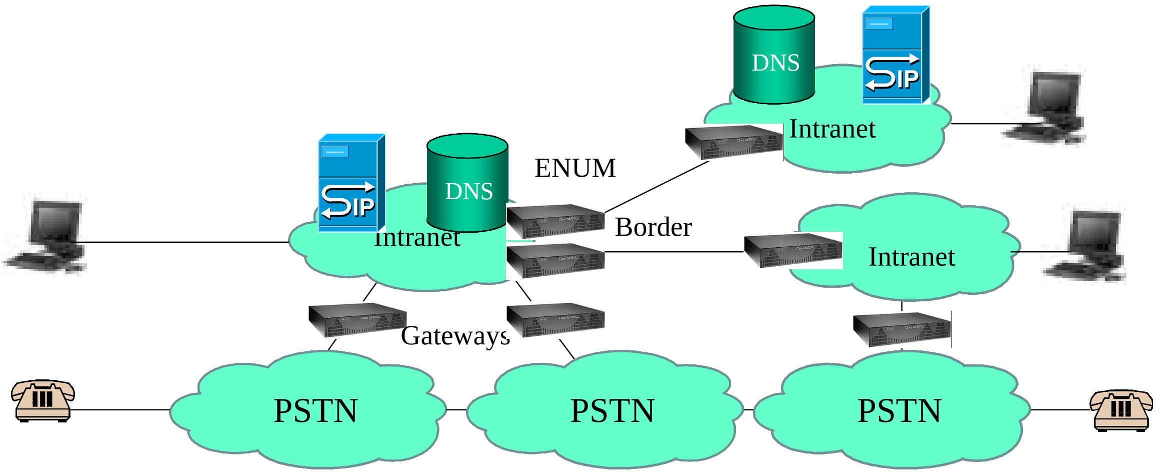

Figure 2

9.3 Shared Infrastructure ENUM with Extranet (Step 4)

A CSP is using Private Infrastructure ENUM within his own network (Intranet), there are connections to the PSTN via IP-Gateways and in addition there are IP-based connections to other CSP via border elements and via an Extranet.

Private Infrastructure ENUM is used to find end-users in the own network (Intranet), the proper gateway for calls routed to the PSTN and the proper border element for calls to number ranges hosted by the other CSP.

The routeing in the Extranet is done via the Shared (or Common) Infrastructure ENUM database in the Extranet.

For the routeing of calls to and within the Extranet two options exist:

1) The Extranet and the Intranet is completely separate. In this case the calls are routed in the Intranet to the Border Element and the Common Infrastructure ENUM database in the Extranet is queried by the Border Element to find the proper routeing information within the Extranet. The Private ENUM Infrastructure database and the Shared ENUM Infrastructure Databases may be in different domain trees, and only the border elements need access to the shared database. In this case three Infrastructure ENUM queries may be necessary to complete a call between CSP A and CSP B. First CSP A need to query his private Infrastructure ENUM database to find the Border Element to the CSP shared extranet. The Border Element from CSP A needs to query the CSP-shared Infrastructure ENUM database to find the address of the ingress Border Element of CSP B, and the Border Element of CSP B needs to query the private Infrastructure ENUM database of CSP B to finally find the AoR of the End-User.

2) The Private and the Shared Infrastructure DNS are using the same domain tree and the data in the CSP-shared Infrastructure ENUM are visible from within the Intranet (Split DNS). In this case the Border element of the other CSP may be addressed directly, thus saving the second query and also saving the separate administration of the different trees.

All E.164 numbers not assigned to end-users are routed either to PSTN gateways or to the border elements. In this scenario, unassigned numbers may, at the sole discretion of the CSP responsible for these numbers, be indicated in the shared database. If these are so indicated, the querying CSP can choose to process the call failure, without passing it onwards.

The Private ENUM database may be implemented in any DNS domain at the CSP discretion and holds in addition to the information described in the above clause also NAPTR RR pointing to the border elements (option1) or is derived directly from the Public Infrastructure ENUM (in option 2).

These NAPTR RRs contain "sip" or "h323" URIs indicating the IP-address or domain name of the border element and the E.164 number as the user-info, e.g. +4319793321@border1.prov.net.

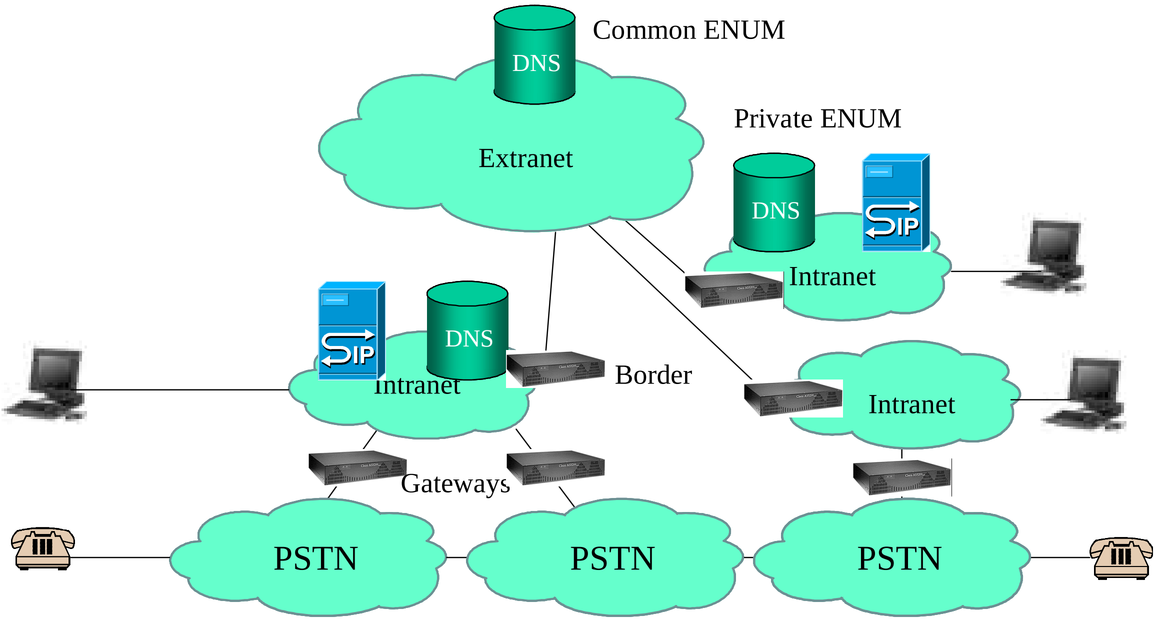

Figure 3

9.4 Shared Infrastructure ENUM on the Internet (Step 5b)

A CSP is using Private Infrastructure ENUM within his own network (Intranet), there are connections to the PSTN via IP-Gateways and IP-based connections to other CSP via border elements and the Public Internet. In addition there may also be connections via border elements and an Extranet or dedicated connections.

Private Infrastructure ENUM is used to find end-users in the own network (Intranet), the proper gateway for calls routed to the PSTN and the proper border element for calls to number ranges hosted by the other CSP.

The routeing on the Public Internet is done via the Shared Infrastructure ENUM database in the Public Internet.

The CSP may also be part of the Public Internet, so that their end-users and the SIP-Servers are reachable on the Public Internet.

For the routeing of calls to and within the public Internet the following options exist:

1) The public Internet and the Intranet is completely separate. In this case the calls are routed in the Intranet to the Border Element and the shared Infrastructure ENUM database on the Internet is queried by the Border Element to find the proper routeing information within the Internet. The Private ENUM Infrastructure database and the shared ENUM Infrastructure Databases may be in different domain trees. As described in the clause above, up to three Infrastructure ENUM queries may be necessary to complete a call.

2) The Private and the shared Infrastructure DNS are using the same domain tree and the data in the shared ENUM Infrastructure are visible form within the Intranet (Split DNS). In this case the Border element of the other CSP may be addressed directly, thus saving the second query and also saving the administration of the routeing to other CSPs.

3) Since CSPs may also have their end-users on the public Internet and do not want to hide these users behind a border element, CSP may populate the Public Infrastructure ENUM database also with end-user data. In this case it is recommended that this data is not visible to other end-users directly.

All E.164 numbers not contained in Infrastructure ENUM may be routed via the PSTN by default. This can be prohibited by using NAPTR RR with the enumservice "void".

The Private ENUM database may be implemented in any DNS domain at the CSP discretion and holds in addition to the information described in the above clause also NAPTR RR pointing to the border elements (option 1) or is derived directly from the Public Infrastructure ENUM (in option 2).

These NAPTR RR contain "sip" or "h323" URIs indicating the IP-address or domain name of the border element and the E.164 number as the user-info, e.g. +4319793321@border1.prov.net.

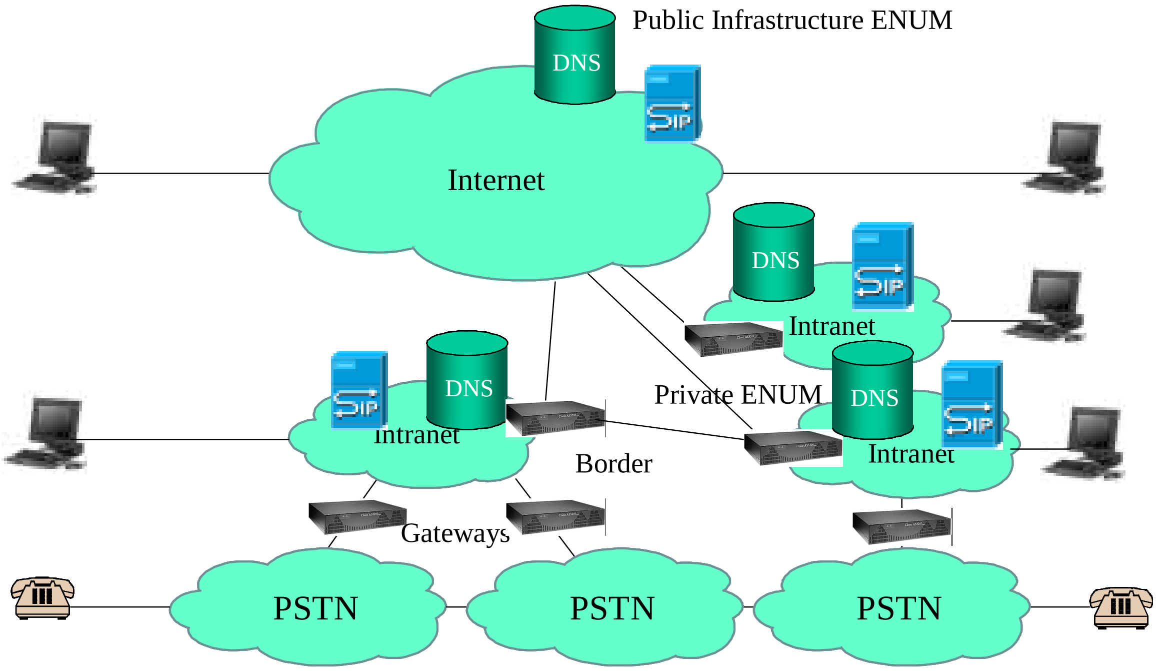
Public Infrastructure ENUM
DNS
SIP
Internet
DNS
SIP
Intranet
SIP
DNS
Intranet
Private ENUM
DNS
SIP
Intranet
Border
Gateways
PSTN
PSTN
PSTN

Figure 4

Annex A: Architectural models

This clause provides a non-exhaustive set of examples of architectures and models which could be adopted, setting out the advantages and disadvantages of each.

In order to highlight the issues, an example confederation with the following parameters is considered:

- Total volume of number ranges: 75 000.
- Size of number ranges: 10 K.
- Total theoretical numbers: 750 M.
- Total active numbers: 125 M.

Volume of numbers ported: 10 %, i.e. 12,5 M.

A.1 Model A

In a CSP-shared Infrastructure ENUM system the structure of the Tiers is a matter of the participating CSPs. In general there can be assumed that there will be a combined Tier 0/Tier1. The models described here therefore assume that only a Tier 1 is existing on the top level.

If the group of CSPs setting up a shared Infrastructure ENUM decide to use only a database system, the NAPTRs would also be in this Tier and the participating CSPs would provide their data to this database via a common provisioning interface. This structure would be very similar to a centralized NP database.

This would obviously also be the natural model for any CSP-internal Infrastructure ENUM.

A.2 Model B

Model B is depicted in figure A.1, and mimics the approach which has been widely adopted for user-ENUM. In this model, the Tier 0/1 contains entries of all of the active numbers, with pointers to the Tier 2 nameservers which contain the actual NAPTRs.

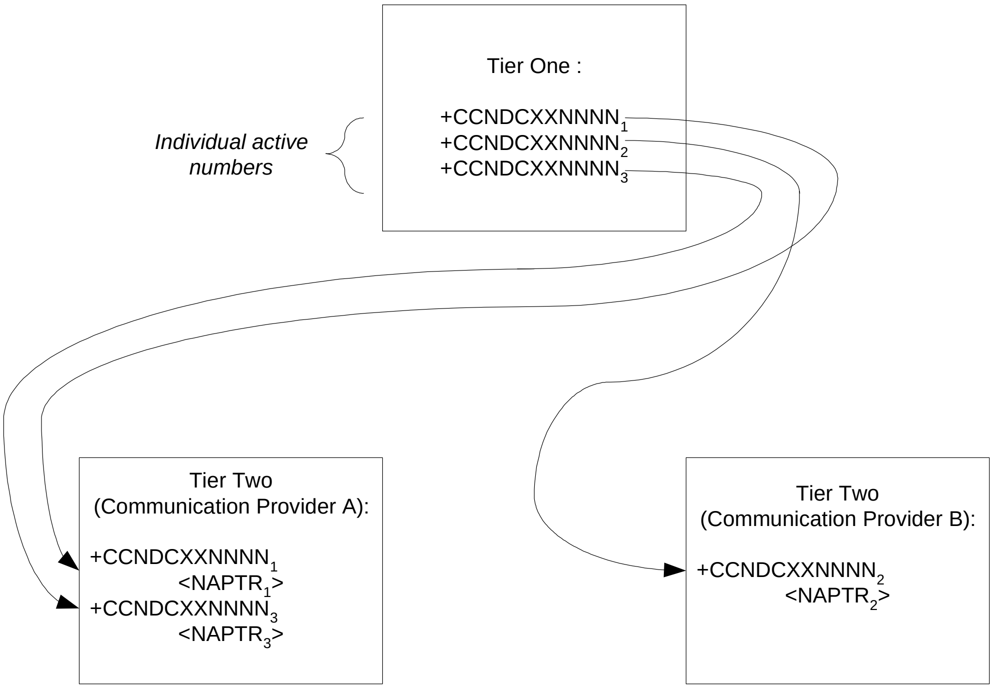

Figure A.1: Model B

For the example group, this means that the Tier 1 database would contain 125M entries, relating to each active individual number.

Model B has the large advantage that it readily accommodates number portability in that the authoritative nameserver for each individual number can be entered into the Tier 1. Where the group has adopted an administration approach which requires authentication, right of use of the number can readily be confirmed so long as there is a central number portability database. However, in locations where there is no onward routeing solution, it would be impossible to authenticate right of use without recourse to the donor CSP (e.g. in figure A.1, where the number +CCNDCXXNNNN$_2$ has been ported from CSP A to CSP B, the Tier 1 provider could not confirm this without consulting CSP A).

Model B is probably the simplest architecture where only a limited proportion of CSPs are participating. For example, CSP B could participate without CSP A being involved (excluding authentication issues), which is not necessarily the case for other options.

Set against this, Model B has disadvantages. Firstly, the Tier 1 database must be of a significant size, as it will contain entries for all active numbers: in the example case this means 125M entries. Although this may not cause any technical issues, there may be cost implications for the Tier 1, and participating CSPs will be seeking to minimize the cost of this entity.

Further, this model implies that every time a new number is provisioned, the Tier 1 must be involved in the process to populate that individual number: this may not be acceptable to the participating CSPs.

Where changes are required to the nameserver hosting the NAPTRs for a given number range, it will be necessary to make multiple amendments in the Tier 1 (i.e. an amendment for each individual number).

A.3 Model C

Model C seeks to overcome some of the issues around Tier 1 by incorporating all numbers into the Tier 1, whether or not they are active. When a CSP is assigned a particular number range, all of the possible numbers will be populated into the Tier 1, with a default entry of the relevant CSPs. Should any of the numbers subsequently be ported, then the entry against the individual number would be amended to point to the appropriate authoritative nameserver. This architectural model is depicted in figure A.2.

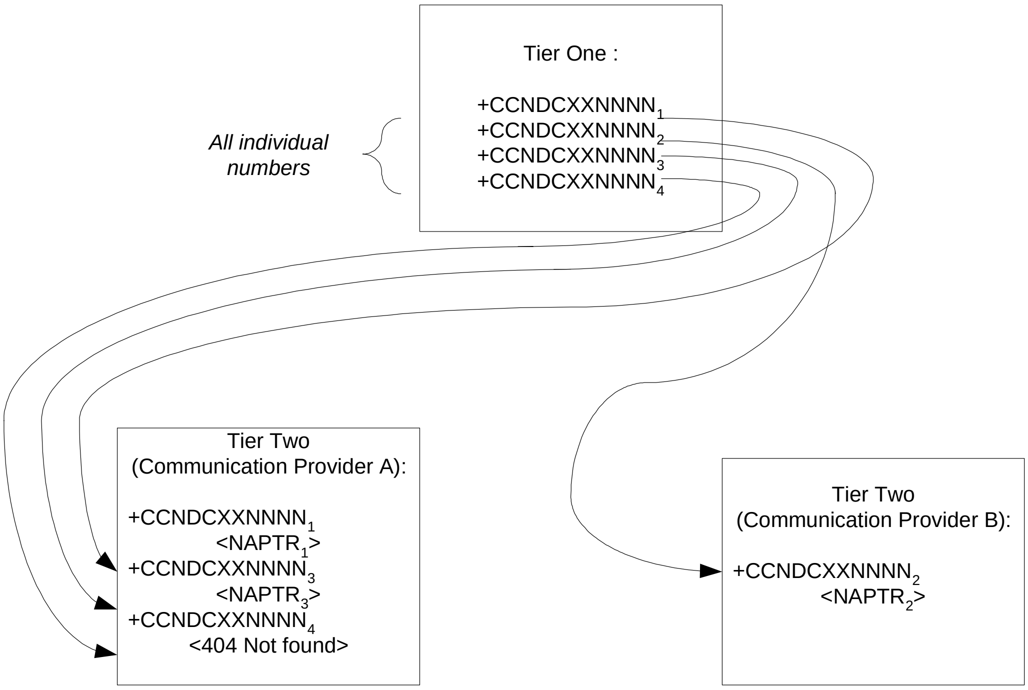

Figure A.2: Model C

This model shares all of the advantages of Model B, with the additional advantage that the Tier 1 is no longer involved in the process of assigning numbers to an individual customer.

Set against this, the Tier 1 database will be considerably larger: in the example group, it will contain some 750M entries. This will inevitably increase costs.

A.4 Model D

Model D adopts an alternative approach, and seeks to minimize the cost of the Tier 1 function. Rather than be broken out at the individual number level, the Tier 1 database would only contain number range information, pointing each range to an authoritative CSP nameserver. Clearly, this presents an issue with respect to ported numbers: this would be overcome by this nameserver redirecting any queries regarding exported numbers to the relevant recipient CSP's nameserver. This model is depicted in figure A.3.

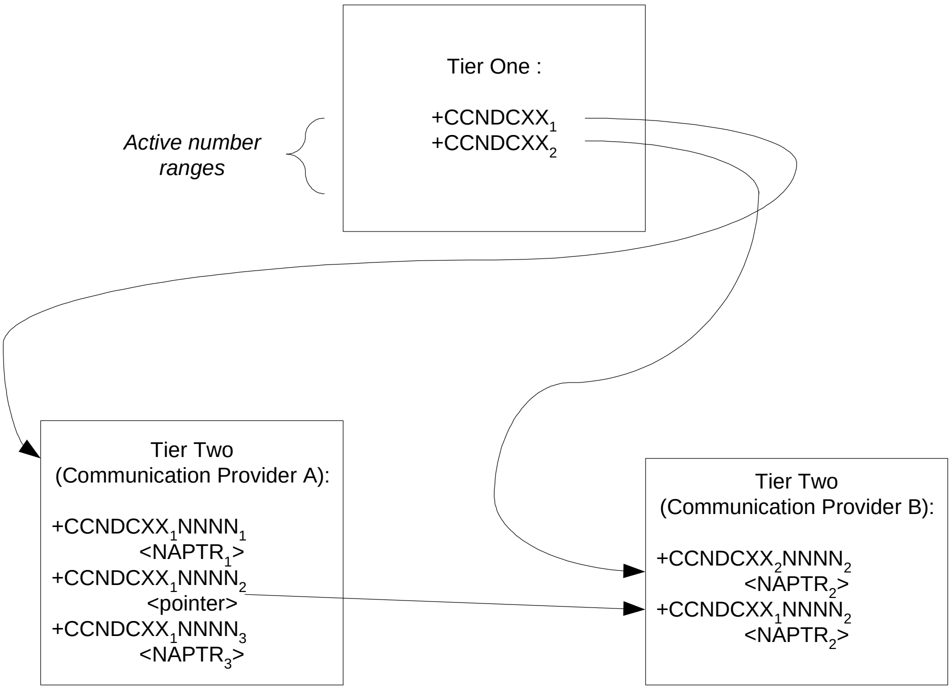

Figure A.3: Model D

Model D has the advantage that it minimizes the size of the Tier 1 database. For the example group, the Tier 1 database would contain only 75K entries, relating to each active individual number range. In principle, this should reduce the cost of this function.

Where authentication is implemented, then the Tier 1 would have a readily available database to utilize, i.e. typically the numbering database available from the relevant regulator.

The Tier 1 would not be involved in day-to-day numbering administration, i.e. would not need to be involved when a number was assigned to an individual customer. Further, should there be a need to change the nameservers dealing with a given number range, only one entry at the Tier 1 would need to be amended.

Set against this, Model D has disadvantages, largely arising as a result of number portability considerations. Firstly, the model perpetuates the situation where the performance of a recipient CSP is in some way influenced by the performance of the donor CSP, because the latter's nameservers are involved in a query for the former's numbers. In general, this does not present a practical issue since as portability is a mutual activity, so where B may port from A for some numbers, A will inevitably port from B for other numbers: as such there is an incentive to maintain a reasonable quality of service. However, difficulties can arise where CSPs suffer financial distress: if the donor CSP goes bankrupt, the nameserver will no longer exist to redirect the query. This could be circumvented via a requirement to escrow data from the nameservers in order that a third party could take over operation if this occurs.

Additionally it would be the responsibility of the original range holder to point to the receiving provider when number portability occurs. Whilst this is manageable if the number is first ported, it becomes increasingly difficult with subsequent porting. A user who changes his provider a number of times for whatever reason, would place a heavy responsibility on the original range holder.

Issues also arise in a start-up phase where only a limited number of CSPs are participating. For example, in figure A.3 if only CSP B is participating, clearly there is an issue that it is impossible to provision any numbers ported from CSP A. There are two potential ways around this:

1) In Tier 1, entries against CSP A are pointed to CSP B until such a time that CSP A decides to participate. At CSP B's nameserver, only numbers imported to them would be populated, with the remaining non-ported numbers not being populated. Whilst this would retain the small size of the Tier 1, it could present process issues as and when CSP A opts to participate. Additionally, this approach would be complex where another CSP C has imported numbers from CSP A; the implication is that CSP B will need to host both its own NAPTRs and pointers to CSP C's nameserver.

2) The Tier 1 becomes a hybrid, containing the number ranges for CSP B, and the individual numbers for those numbers exported from CSP A. In the example, in the hypothetical situation where *all* numbers which are ported are ported from CSP A to B (e.g. A is the incumbent), then this would imply that the Tier 1 would contain 12.5M entries. Once again, process issues could arise as and when CSP A opts to participate. Further, it may be the case that the complexity of the Tier 1 will be greater than otherwise will be the case (entries will be of mixed length), thus increasing costs.

A.5 Model E

The final model presented in this clause is based upon Model D, but seeks to overcome the issues around the performance of a recipient network being dependent upon the performance of a donor. In this model, depicted in figure A.4, the actual nameserver operation is outsourced to an escrow agency.

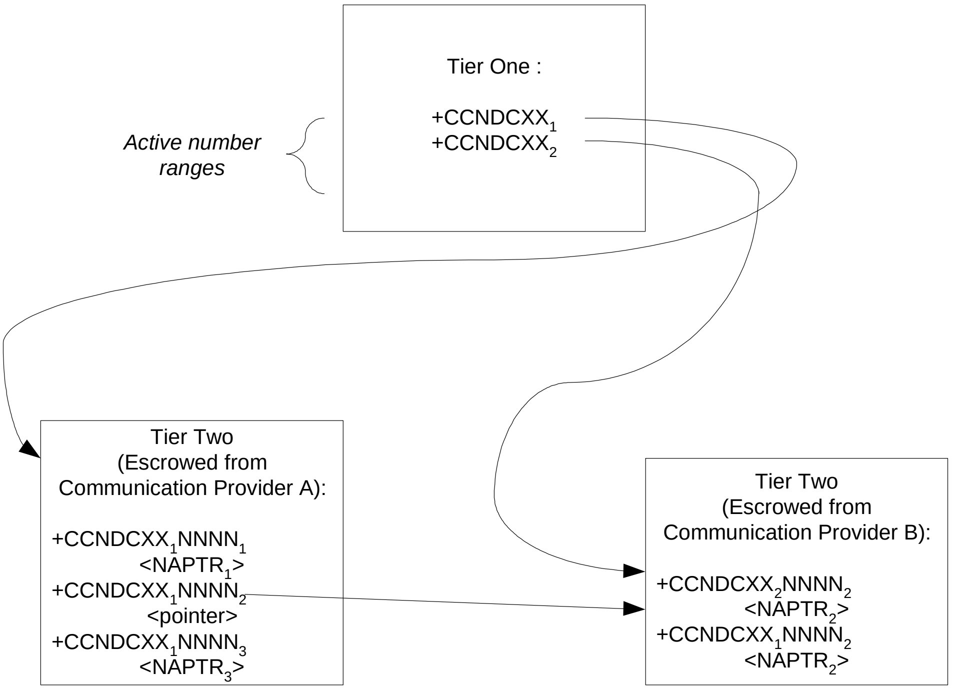
Tier One :
+CCNDCXX$_1$
+CCNDCXX$_2$
Active number ranges
Tier Two (Escrowed from Communication Provider A):
+CCNDCXX$_1$NNNN$_1$ <NAPTR$_1$>
+CCNDCXX$_1$NNNN$_2$ <pointer>
+CCNDCXX$_1$NNNN$_3$ <NAPTR$_3$>
Tier Two (Escrowed from Communication Provider B):
+CCNDCXX$_2$NNNN$_2$ <NAPTR$_2$>
+CCNDCXX$_1$NNNN$_2$ <NAPTR$_2$>

Figure A.4: Model E

The advantages of this model are those of Model D, with the addition that a recipient CSP no longer depends upon the performance of the donor CSP.

Set against this, it may not be acceptable to CSPs to outsource the operation of their nameservers. Further, although the recipient is no longer dependent upon the performance of the donor, they are still dependent upon an agency appointed by the donor: it could be argued that this amounts to the same thing. However, there is a difference in that should the donor CSP face bankruptcy, the escrow nameserver would exist, whereas in Model D only the data would be escrowed, meaning it would be necessary to appoint a new nameserver manager and populate the nameserver.

As with Model D, issues arise around any start-up phase where not all CSPs participate. These issues and the potential solutions have been described earlier and additionally the issues with subsequent explained model D also applies.

History

Document history		
V1.1.1	May 2005	Publication