E.164 number and DNS

draft-ietf-enum-e164-dns-00

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on October 24, 2000.

Copyright Notice

Copyright (C) The Internet Society (2000). All Rights Reserved.

Abstract

This document discusses the use of DNS for storage of E.164 numbers. More specifically, how DNS can be used for identifying available services connected to one E.164 number. Routing of the actual connection using the service selected using these methods is not discussed.
1. Introduction

Through transformation of E.164 numbers into DNS names and the use of existing DNS services like delegation through NS records, and use of NAPTR[1] records in DNS[4], one can look up what services are available for a specific domainname in a decentralized way with distributed management of the different levels in the lookup process.

1.1 Terminology

The key words "MUST", "REQUIRED", "SHOULD", "RECOMMENDED", and "MAY" in this document are to be interpreted as described in RFC2119[3]
2. E.164 numbers and DNS

The domain "e164.int." 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 in order to be listed, by examining the SOA resource record associated with the zone, just like in normal DNS operations.

To find the DNS names for a specific E.164 number, the following procedure is to be followed:

1. See that the E.164 number is written in its full form, including the countrycode IDDD. Example: +46-8-56264000

2. Remove all non-digit characters part from the leading ‘+’. Example: +4689761234

3. Use this string as input to the NAPTR algorithm.

4. Remove all characters part from the digits. Example: 4689761234

5. Put dots (".") between each digit. Example: 4.6.8.9.7.6.1.2.3.4

6. Change the order of the digits. Example: 4.3.2.1.6.7.9.8.6.4

7. Append the domain "e164.int" to the end. Example: 4.3.2.1.6.7.9.8.6.4.e164.int
3. Identifying available services

For a record in DNS, the NAPTR record is used for identifying available ways of contacting a specific node identified by that name. Specifically it can be used for knowing what services exists for a specific domain name, including phone numbers by the use of the e164.int domain as described above.

The identification is using the NAPTR resource record defined for use in the URN resolution process, but it can be generalized in a way that suits the needs specified in this document.

3.1 The NAPTR record

The key fields in the NAPTR RR are order, preference, service, flags, regexp, and replacement. For a detailed description, see:

- The order field specifies the order in which records MUST be processed when multiple NAPTR records are returned in response to a single query.

- The preference field specifies the order in which records SHOULD be processed when multiple NAPTR records have the same value of "order".

- The service field specifies the resolution protocol and resolution service(s) that will be available if the rewrite specified by the regexp or replacement fields is applied.

- The flags field contains modifiers that affect what happens in the next DNS lookup, typically for optimizing the process.

- The regexp field is one of two fields used for the rewrite rules, and is the core concept of the NAPTR record.

- The replacement field is the other field that may be used for the rewrite rule.

Note that the client applies all the substitutions and performs all lookups, they are not performed in the DNS servers. Note also that it is the belief that regexps should rarely be used. The replacement field seems adequate for the vast majority of situations.

3.1.1 Specific handling of non-terminal NAPTR records

A E.164 number, without any characters but leading ‘+’, is the input to the NAPTR algorithm, and because of this non-terminal NAPTR records (i.e. rewrite rules) operate on this E.164 number.
The service supported for a call is N2R.

3.1.2 Example of use

tele2.se.

```
;;        ord pr fl  service            re replacement
IN NAPTR 100 10 "a" "sip+N2R"       "sip:information@tele2.se"
IN NAPTR 102 10 "a" "smtp+N2R"      "mailto:information@tele2.se"
```

This describes that the domain tele2.se is preferrable contacted via the SIP protocol, secondly via SMTP (for VPIM voicemail over SMTP for example).

In both cases, the next step in the resolution process is to use the resolution mechanism for each of the protocols, (SIP and SMTP) to know what node to contact for each.

3.1.3 When the virtual address is a phone number

When the target address is a phone number, it is first translated into a RR name in the e164.int domain according to the method described above.

Example:

```
4.3.2.1.6.7.9.8.6.4.e164.int.

IN NAPTR 10 10 "a" "sip+N2R"       "sip:paf@swip.net"
IN NAPTR 102 10 "a" "smtp+N2R"      "mailto:paf@swip.net"
IN NAPTR 102 10 "a" "tel+N2R"       "tel:+4689761234"
```

Note that the prefered method is to use the SIP protocol, but the result of the rewrite of the NAPTR record is a URI (the "a" flag in the NAPTR record). In the case of the protocol SIP, the URI might be a SIP URI, which is resolved as described in RFC 2543[5]. In the case of the "tel" URI scheme, the procedure is restarted with this new E.164 number. The client is responsible for loop detection.

The rest of the resolution of the routing is done as described above.
4. Security Considerations

As this system is built on top of DNS, one can not be sure that the information one get back from DNS is more secure than any DNS query. To solve that, the use of DNSSEC for securing and verifying zones is to be recommended.

The caching in DNS can make the propagation time for a change take the same amount of time as the time to live for the NAPTR and SRV records in the zone that is changed. The TTL should because of that be kept to a minimum. The use of this in an environment where IP-addresses are for hire (i.e. DHCP) must therefore be done very carefully.
5. Acknowledgement

Support and ideas has come from people at Ericsson, especially Bjorn Larsson, especially the group which implemented this scheme in their lab to see that it worked. Input has also come from ITU-T SG2, Working Party 1/2 (Numbering, Routing, Global Mobility and Service Definition), the ENUM working group in the IETF, and Leif Sunnegardh at Tele2 for information about how SS7 really works.
References


Author’s Address

Patrik Faltstrom
Tele2
Borgarfjordsgatan 16
127 61 Kista
Sweden

EMail: paf@swip.net
URI: http://www.tele2.se
Appendix A. Example 1

ITU has delegated the country code 46, and the zone 6.4.e164.int to the regulator of telephony in Sweden. Because of that, the content of the e164.int zone is.

$ORIGIN e164.int.
6.4 IN NS ns.regulator-e164.example.se.

The regulator has in turn given a series of 10000 numbers to the telco with the name Telco-A. The regulator because of that has in his DNS.

$ORIGIN 6.4.e164.int.
6.7.9.8 IN NS ns.telco-a.example.se.

A user named Sven Svensson has from Telco A got the phone number +46-8-9761234. The user gets the service of running DNS from the company Redirection Service. Sven Svensson has asked Telco A to point out Redirection Service as the authoritative source for information about the number +46-8-9761234. Telco A because of this puts in his DNS the following.

$ORIGIN 6.7.9.8.6.4.e164.int.
4.3.2.1 IN NS ns.redirection-service.example.se.

Sven Svenssson has already plain telephony from Telco A, but also a SIP service from the company Sip Service which provides Sven with the SIP URI "sip:sven@sipservice.example.se". The ISP with the name ISP A runs email and webpages for Sven, under the emailaddress sven@ispa.example.se, and URL http://svensson.ispa.example.se.

The DNS for the redirection service because of this contains the following.

$ORIGIN 4.3.2.1.6.7.9.8.6.4.e164.int.
IN NAPTR 10 10 "a" "sip+N2R" "sip:sven@sipservice.example.se"
IN NAPTR 10 10 "a" "smtp+N2R" "mailto:sven@ispa.example.se"
IN NAPTR 10 10 "a" "http+N2R" "http://svensson.ispa.example.se"
IN NAPTR 10 10 "a" "tel+N2R" "tel:+46-8-9761234"

A user, John Smith, want to contact Sven Svensson, he to start with only has the E.164 number of Sven, i.e. +46-8-9761234. He takes the number, and enters the number in his communication client, which happen to know how to handle the SIP protocol. The client removes
the dashes, and ends up with the E.164 number +4689761234. That is what is used in the algorithm for NAPTR records, which is as follows.

The client converts the E.164 number into the domainname 4.3.2.1.6.7.9.8.6.4.e164.int., and queries for NAPTR records for this domainname. Using DNS mechanisms which includes following the NS record referals, the following records are returned:

```
$ORIGIN 4.3.2.1.6.7.9.8.6.4.e164.int.
IN NAPTR 10 10 "a" "sip+N2R" "sip:sven@sipservice.example.se"
IN NAPTR 10 10 "a" "smtp+N2R" "mailto:sven@ispa.example.se"
IN NAPTR 10 10 "a" "http+N2R" "http://svensson.ispa.example.se"
IN NAPTR 10 10 "a" "tel+N2R" "tel:+46-8-9761234"
```

Because this client know sip, the first record above is selected, and the SIP URI is extracted, and used according to SIP resolution.
Full Copyright Statement

Copyright (C) The Internet Society (2000). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC editor function is currently provided by the Internet Society.