Network Working Group
Internet-Draft
Expires: January 31, 2001

P Faltstrom
Cisco Systems Inc

August 2, 2000

E.164 number and DNS
draft-ietf-enum-e164-dns-03

Status of this Memo

Copyright Notice

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[2][3], 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[4]

2. E.164 numbers and DNS

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 in order to be listed, 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.

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: +46-8-9761234

2. Remove all non-digit characters with the exception of the leading '+'. Example: +4689761234

3. Remove all characters with the exception of the digits. Example: 4689761234

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

5. Reverse the order of the digits. Example: 4.3.2.1.6.7.9.8.6.4

6. Append the string ".e164.arpa" to the end. Example: 4.3.2.1.6.7.9.8.6.4.e164.arpa

3. Fetching URIs given an E.164 number

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 domainname, including phone numbers by the use of the e164.arpa 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.

It is the string which is the result of step 2 in section 2 above which is input to the NAPTR algorithm.

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 that URIs are stored in the regexp field.

3.1.1 Specification for use of NAPTR Resource Records

The input is an E.164 encoded telephone number. The output is a Uniform Resource Identifier in its absolute form according to the

'absoluteURI' production in the Collected ABNF found in RFC2396[5]

An E.164 number, without any characters but leading '+' and digits, (result of step 2 in section 2 above) is the input to the NAPTR algorithm.

The service supported for a call is E2U.

3.1.2 Specification of Service E2U (E.164 to URI)

* Name: E.164 to URI
* Mnemonic: E2U
* Number of Operands: 1
* Type of Each Operand: First operand is an E.164 number.
* Format of Each Operand: First operand is the E.164 number in the form as specified in step 2 in section 2 in this document.
* Algorithm: Opaque
* Output: One or more URLs
* Error Conditions:
  - o E.164 number not in the numbering plan
  - o E.164 number in the numbering plan, but no URLs exist for that number
  - o Service unavailable

* Security Considerations:
  - o Malicious Redirection
    One of the fundamental dangers related to any service such as this is that a malicious entry in a resolver's database will cause clients to resolve the E.164 into the wrong URL. The possible intent may be to cause the client to retrieve a resource containing fraudulent or damaging material.
  - o Denial of Service
    By removing the URL to which the E.164 maps, a malicious intruder may remove the client's ability to access the resource.

This operation is used to map a one E.164 number to a list of URIs. The first well-known step in the resolution process is to remove all non-digits apart from the leading '+' from the E.164 number as described in step 1 and 2 in section 2 of this document.

3.2 Examples

3.2.1 Example 1

```
$ORIGIN 4.3.2.1.6.7.9.8.6.4.e164.arpa.
 IN NAPTR 100 10 "u" "sip+E2U"  "!^.*$!sip:information@tele2.se!"       .
 IN NAPTR 102 10 "u" "mailto+E2U" "!^.*$!mailto:information@tele2.se!"  .
```

This describes that the domain 4.3.2.1.6.7.9.8.6.4.e164.arpa is

preferably contacted by SIP, and secondly by SMTP.

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.

3.2.2 Example 2

```
$ORIGIN 4.3.2.1.6.7.9.8.6.4.e164.arpa.
 IN NAPTR  10 10 "u" "sip+E2U"   "!^.*$!sip:paf@swip.net!"      .
 IN NAPTR 102 10 "u" "mailto+E2U"  "!^.*$!mailto:paf@swip.net!" .
 IN NAPTR 102 10 "u" "tel+E2U"   "!^.*$!tel:+4689761234!"       .
```

Note that the preferred method is to use the SIP protocol, but the result of the rewrite of the NAPTR record is a URI (the "u" 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[6]. In the case of the "tel" URI scheme[7], 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.

3.2.3 Example 3

```
$ORIGIN 6.4.e164.arpa.
 * IN NAPTR 100 10 "u" "ldap+E2U" "!^+46(.*)$!ldap://ldap.example.se/
cn=0\1!" .
```

We see in this example that information about all E.164 numbers in the 46 countrycode (for Sweden) exists in an LDAP server, and the search to do is specified by the LDAP URI[8].

4. IANA considerations

This memo requests that the IANA delegate the E164.ARPA domain following instructions to be provided by the IAB. Names within this zone are to be delegated to parties according to the ITU recommendation E.164. The names allocated should be hierarchic in accordance with ITU Recommendation E.164, and the codes should assigned in accordance with that Recommendation.

Delegations should be done after Expert Review, and the IESG will appoint a designated expert.

5. 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[9] 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[10] 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 (for example when using DHCP[11]) must therefore be done very carefully.

There are a number of countries (and other numbering environments) in which there are multiple providers of call routing and number/name-translation services. In these areas, any system that permits users, or putative agents for users, to change routing or supplier information may provide incentives for changes that are actually unauthorized (and, in some cases, for denial of legitimate change requests). Such environments should be designed with adequate mechanisms for identification and authentication of those requesting changes and for authorization of those changes.

6. Acknowledgement

Support and ideas has come from people at Ericsson, Bjorn Larsson and 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, John Klensin and Leif Sunnegardh.

References

[1] Mealling, M and R Daniel, "The Naming Authority Pointer (NAPTR) DNS Resource Record", draft-ietf-urn-naptr-rr-03.txt (work in progress), June 1998.

[2] Mockapetris, P.V., "Domain names - concepts and facilities", RFC 1034, STD 13, Nov 1987.

[3] Mockapetris, P.V., "Domain names - implementation and specification", RFC 1035, STD 13, Nov 1987.

[4] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, BCP 14, March 1997.

[5] Berners-Lee, T., Fielding, R.T. and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

[6] Handley, M., Schulzrinne, H., Schooler, E. and J. Rosenberg, "SIP: Session Initiation Protocol", RFC 2543, March 1999.

[7] Vaha-Sipila, A., "URLs for Telephone Calls", RFC 2806, April 2000.

[8] Howes, T. and M. Smith, "An LDAP URL Format", RFC 1959, June 1996.

[9] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

[10] Gulbrandsen, A., Vixie, P. and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[11] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

Author's Address

Patrik Faltstrom
Cisco Systems Inc
170 W Tasman Drive SJ-13/2
San Jose CA 95134
USA

EMail: paf@cisco.com
URI: http://www.cisco.com

Appendix A. Scenario

Say that the content of the e164.arpa zone is the following:

```
$ORIGIN e164.arpa.
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.arpa.
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.arpa.
4.3.2.1 IN NS ns.redirection-service.example.se.
```

Sven Svensson 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.

```
$ORIGIN 4.3.2.1.6.7.9.8.6.4.e164.arpa.
 IN NAPTR 10 10 "u" "sip+E2U"  "!^.*$!sip:sven@sipservice.example.se!"  .
 IN NAPTR 10 10 "u" "mailto+E2U" "!^.*$!mailto:sven@ispa.example.se!"   .
 IN NAPTR 10 10 "u" "http+E2U" "!^.*$!http://svensson.ispa.example.se!" .
 IN NAPTR 10 10 "u" "tel+E2U"  "!^.*$!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.arpa., and queries for NAPTR records for this domainname. Using DNS mechanisms which includes following the NS record referals, the following records are returned:

```
$ORIGIN 4.3.2.1.6.7.9.8.6.4.e164.arpa.
 IN NAPTR 10 10 "u" "sip+E2U"  "!^.*$!sip:sven@sipservice.example.se"  .
 IN NAPTR 10 10 "u" "mailto+E2U" "!^.*$!mailto:sven@ispa.example.se"   .
 IN NAPTR 10 10 "u" "http+E2U" "!^.*$!http://svensson.ispa.example.se" .
 IN NAPTR 10 10 "u" "tel+E2U"  "!^.*$!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

Acknowledgement

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