Network Working Group   M. Mealling
Request for Comments: 3405   VeriSign
BCP: 65   October 2002
Category: Best Current Practice

            Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA
                          Assignment Procedures

Status of this Memo

   This document specifies an Internet Best Current Practices for the
   Internet Community, and requests discussion and suggestions for
   improvements. Distribution of this memo is unlimited.

Abstract

   This document is fifth in a series that is completely specified in
   "Dynamic Delegation Discovery System (DDDS) Part One: The
   Comprehensive DDDS" (RFC 3401). It is very important to note that it
   is impossible to read and understand any document in this series
   without reading the others.

Table of Contents

1. Introduction

   This document defines the policies and procedures for inserting
   Naming Authority Pointer (NAPTR) records into the 'URI.ARPA' and
   'URN.ARPA' zones for the purpose of resolving Uniform Resource
   Identifiers (URIs) according to "Dynamic Delegation Discovery System
   (DDDS) Part Four: The URI Resolution Application" (RFC 3402) [2],
   which is an Application that uses the Domain Name System (DNS) based
   DDDS Database. All of these concepts are defined in RFC 3401 [1].
   It is very important to note that it is impossible to correctly
   understand this document without reading RFC 3401 and the documents
   it specifies.

   RFC 3403 defines a how DNS is used as a DDDS database that contains
   URI delegation rules (sometimes called resolution hints). That
   document specifies that the first step in that algorithm is to append
   'URI.ARPA' to the URI scheme and retrieve the NAPTR record for that
   domain-name. I.e., the first step in resolving "http://foo.com/"
   would be to look up a NAPTR record for the domain "http.URI.ARPA".
   URN resolution also follows a similar procedure but uses the
   'URN.ARPA' zone as its root. This document describes the procedures
   for inserting a new rule into the 'URI.ARPA' and 'URN.ARPA' zones.

2. URI Resolution vs URN Resolution

   RFC 3402 [2] defines how both URI [7] resolution and URN [6]
   resolution work when DNS is used as the delegation rule (or hint)
   database. Specifically it says that the initial instructions
   ('hints') for DNS-based resolution of URIs are stored as resource
   records in the 'URI.ARPA' DNS zone.

   Since a URN is a URI scheme, a hint for resolution of the URI prefix
   'urn:' will also be stored in the 'URI.ARPA' zone. This rule states
   that the namespace id [6] is extracted, 'URN.ARPA' is appended to the
   end of the namespace id, and the result is used as the key for
   retrieval of a subsequent NAPTR record [4].

3. Registration Policies

   The creation of a given URI scheme or URN namespace id (NID) follows
   the appropriate registration documents for those spaces. URI schemes
   follow "Registration Procedures for URL Scheme Names" (RFC 2717)
   [10]. URN namespace ids follow "URN Namespace Definition Mechanisms"
   (RFC 2611) (or updates thereto) [9].

3.1 URI.ARPA Registration

3.1.1 Only Schemes in the IETF Tree Allowed

   In order to be inserted into the URI.ARPA zone, the subsequent URI
   scheme MUST be registered under the IETF URI tree. The requirements
   for this tree are specified in [10].

3.1.2 Scheme Registration Takes Precedence

   The registration of a NAPTR record for a URI scheme MUST NOT precede
   proper registration of that scheme and publication of a stable
   specification in accordance with [10]. The IESG or its designated
   expert will review the request for

      1. correctness and technical soundness

      2. consistency with the published URI specification, and

      3. to ensure that the NAPTR record for a DNS-based URI does not
          delegate resolution of the URI to a party other than the
          holder of the DNS name. This last rule is to insure that a
          given URI's resolution hint doesn't hijack (inadvertently or
          otherwise) network traffic for a given domain.

3.1.3 NAPTR Registration May Accompany Scheme Registration

   A request for a URI.ARPA registration MAY accompany a request for a
   URI scheme (in accordance with [10]), in which case both requests
   will be reviewed simultaneously by IESG or its designated experts.

3.1.4 Registration or Changes after Scheme Registration

   A request for a NAPTR record (or an request to change an existing
   NAPTR record) MAY be submitted after the URI prefix has been
   registered. If the specification for the URI prefix is controlled by
   some other party than IETF, IESG will require approval from the
   owner/maintainer of that specification before the registration will
   be accepted. This is in addition to any technical review of the
   NAPTR registration done by IESG or its designated experts.

3.2 URN.ARPA Registration

3.2.1 NID Registration Takes Precedence

   The registration of a NAPTR record for a URN NID MUST NOT precede
   proper registration of that NID and publication of a stable
   specification in accordance with [9]. This is to prevent the
   registration of a NAPTR record in URN.ARPA from circumventing the NID
   registration process.

3.2.2 NAPTR Registration May Accompany NID Registration

   A request for a URN.ARPA registration MAY accompany a request for a
   NID (in accordance with [9]), in which case both requests will be
   reviewed at the same time.

3.2.3 Registration or Changes after Scheme Registration

   A request for a NAPTR record (or an request to change an existing
   NAPTR record) MAY be submitted after the NID has been registered. If
   the specification for the NID is controlled by some other party than
   IETF, IESG will require approval from the owner/maintainer of that
   specification before the registration will be accepted. This is in
   addition to any technical review of the NAPTR registration done by
   IESG or its designated experts.

   Note that this applies to all NAPTR records for a particular NID,
   even though a NAPTR record might affect only part of the URN space
   assigned to an NID

4. Requirements on hints

   Delegation of a namespace can happen in two ways. In the case of
   most URIs, the key being delegated to is hard-coded into the
   identifier itself (e.g., a hostname in an HTTP URI). The syntax of
   where this new key is located is predetermined by the syntax of the
   scheme. In other cases, the new key can be part of the hint itself.
   This is the functional equivalent of saying, "if this rule matches
   then this is always the key."

   In order to minimize the query load on the URI.ARPA and URN.ARPA
   zones, it is anticipated that the resource records in those zones
   will have extremely long "times to live" (TTLs), perhaps measured in
   years.

Thus, for any URI prefix or URN namespace for which the resolution
hints are likely to change, the actual rule should be stored in some
other (less stable) DNS zone, and within URI.ARPA or URN.ARPA a
stable NAPTR record should be used to delegate queries to that less
stable zone.

For example, the 'foo' URN namespace has flexible rules for how
delegation takes place. Instead of putting those rules in the
URN.ARPA zone, the entry instead punts those rules off to a
nameserver that has a shorter time to live. The record in URN.ARPA
would look like this:

```
    foo     IN NAPTR 100 10  ""  "" "" urn-resolver.foo.com.
```

Thus, when the client starts out in the resolution process, the first
step will be to query foo.URN.ARPA to find the above record, the
second step is to begin asking 'urn-resolver.foo.com' for the NAPTR
records that contain the resolution rules. The TTL at the root is
very long. The TTL at the 'urn-resolver.foo.com' is much shorter.

Conversely, the 'http' URI scheme adheres to a particular syntax that
specifies that the host to ask is specified in the URI in question.
Since this syntax does not change, that rule can be specified in the
URI.ARPA zone. The record would look like this:

```
    http    IN NAPTR 100 100 "" ""  "/http:\\/\\/([^\\/:]+)/\\2/i" .
```

Thus, the second step of resolution is to use the domain-name found
in the URI as the next key in the cycle. If, for example, that NAPTR
was terminal and contains some hostname in the replacement field,
then the client could contact that host in order to ask questions
about this particular URI.

5. Submission Procedure

Using the MIME Content-Type registration mechanism [8] as a model
for a successful registration mechanism, the 'URI.ARPA' and
'URN.ARPA' procedures consist of a request template submitted to an
open mailing list made up of interested parties. If no objections
are made within a two week period, a representative of the
registration authority considers the submission to be accepted and
enters that submission into the nameserver.

   o Registrations for the 'URI.ARPA' zone are sent to
      'register@URI.ARPA'.

o Registrations for the 'URN.ARPA' zone are sent to
   'register@URN.ARPA'.

The registration authority is the Internet Assigned Numbers
Authority (IANA).

Objections are restricted to those that point out impacts on the zone
itself or to DNS in general. Objections to the URI scheme or to the
URN namespace-id are not allowed, as these should be raised in their
respective forums. The logical conclusion of this is that ANY
sanctioned URI scheme or URN namespace MUST be allowed to be
registered if it meets the requirements specified in this document as
regards times to live and general impact to the DNS.

6. Registration Template

The template to be sent to the appropriate list MUST contain the
following values:

6.1 Key

This is the URN NID or URI scheme, which is used as the domain
portion of the DNS entry. It must be valid according to the
procedures specified in the URN namespace-id assignment document and
any future standards for registering new URI schemes.

6.2 Authority

This is the individual or organization (entity) which has authority
for registering the record. It must be an authority recognized as
either the IESG or any authority defined in the URN NID [9] or URI
scheme registration [10] documents.

6.3 Records

The actual DNS records representing the rule set for the key. The
required values are Preference, Order, Flags, Services, Regex, and
Replacement as defined by RFC 3404 [4].

7. Example Template

To: register@URN.ARPA
From: joe@foo.com

Key: foo
Authority: Foo Technology, Inc as specified in RFCFOO
Record: foo   IN NAPTR 100 100 "" "" "" urn.foo.com.

8. The URN Registration in the URI.ARPA zone

   Since this document discusses the URI.ARPA and URN.ARPA zones and the
   URN rule that exists in the URI.ARPA zone, it makes sense for the
   registration template for the URN URI rule to be specified here:

         To: register@URI.ARPA
         From: The IETF URN Working Group

         Key: urn
         Authority: RFC2141
         Record: urn   IN NAPTR 0 0 "" "" "/^urn:([^:]+)/\\2/i" .

9. IANA Considerations

   The IANA has created the zones URN.ARPA and URI.ARPA. The
   hierarchical name structure, and the only names to be assigned within
   these zones, are the "keys" as described in Section 6.1 of this
   document. The administrative and operational management of these
   zones are to be undertaken by the IANA. The DNS records to be
   inserted in these zones are subject to the review process described
   in this document.

   The IANA has also created two discussion lists, register@uri.arpa and
   register@urn.arpa, for the purposes described in this document. The
   IANA will manage these mailing lists.

10. Security Considerations

   The 'uri.arpa' and 'urn.arpa' zones will be a common point of attack
   both for Denial of Service and for spoofing entries in order to
   redirect delegation paths. Any entity running nameservers that
   contain these zones should take appropriate action for securing an
   infrastructure level component of the Internet. When it becomes
   possible for a nameserver to reliably sign the records in its zone it
   should do so.

11. Acknowledgements

   The author would like to thank Ron Daniel who was originally co-
   author of these documents. Ron's original insite into the intricate
   nature of delegation rules made these procedures and the DDDS itself
   possible.

12. References

   [1]   Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part
          One: The Comprehensive DDDS", RFC 3401, October 2002.

   [2]   Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part
          Two: The Algorithm", RFC 3402, October 2002.

   [3]   Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part
          Three: The Domain Name System (DNS) Database", RFC 3403,
          October 2002.

   [4]   Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part
          Four: The Uniform Resource Identifiers (URI) Resolution
          Application", RFC 3404, October 2002.

   [5]   Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part
          Five: URI.ARPA Assignment Procedures", RFC 3405, October 2002.

   [6]   Moats, R., "URN Syntax", RFC 2141, November 1998.

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

   [8]   Freed, N., Klensin, J. and J. Postel, "Multipurpose Internet
          Mail Extensions (MIME) Part Four: Registration Procedures", BCP
          13, RFC 2048, November 1996.

   [9]   Faltstrom, P., Iannella, R., Daigle, L. and D. van Gulik, "URN
          Namespace Definition Mechanisms", BCP 33, RFC 2611, October
          1998.

   [10]   Petke, R. and I. King, "Registration Procedures for URL Scheme
          Names", BCP 35, RFC 2717, January 1999.

13. Author's Address

   Michael Mealling
   VeriSign
   21345 Ridgetop Circle
   Sterling, VA 20166
   US

   EMail: michael@neonym.net
   URI: http://www.verisignlabs.com

14. Full Copyright Statement

   Copyright (C) The Internet Society (2002). 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.