Network Working Group	P. Faltstrom	
Internet-Draft	Cisco	
Updates: 3404, 3959	O. Kolkman	
(if approved)	NLNet	
Intended status: Standards Track	October 11, 2010	
Expires: April 14, 2011		

TOC

The Uniform Resource Identifier (URI) DNS Resource Record
draft-faltstrom-uri-06.txt

Abstract

This document defines a new DNS resource record, called the Uniform Resource Identifier (URI) RR, for publishing mappings from hostnames to URIs.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.
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.”
This Internet-Draft will expire on April 14, 2011.

Table of Contents

---

1. Introduction

TOC

This document explains the use of the Domain Name System (DNS) for the storage of URIs, and how to resolve hostnames to such URIs that can be used by various applications. For resolution the application need to know both the hostname and the protocol that the URI is to be used for. The protocol is registered by IANA.
Currently, looking up URIs given a hostname uses the DDDS (Mealling, M., “Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS,” October 2002.) [RFC3401] application framework with the DNS as a database as specified in RFC 3404 (Mealling, M., “Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI),” October 2002.) [RFC3404]. This has a number of implications such as the inability to select what NAPTR records that match the query are interesting. The RRSet returned will always consist of all URIs "connected" with the domain in question.
The URI resource record specified in this document enables the querying party to select which ones of the NAPTR records one is interested in. This because data in the service field of the NAPTR record is included in the owner part of the URI resource record type.

Querying for URI resource records is not replacing querying for NAPTR resource records (or use of S-NAPTR (Daigle, L. and A. Newton, “Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS),” January 2005.) [RFC3958]). Instead, the URI resource record type provides a complementary mechanism to use when one already knows what service field is interesting. With it, one can directly query for the specific subset of the otherwise possibly large RRSet given back when querying for NAPTR resource records.

This document updates RFC 3958 and RFC 3404 by adding the flag "D" to the list of defined terminal flags in section 2.2.3 of RFC 3958 and 4.3 of RFC 3404.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.) [RFC2119].

---

2. Applicability Statement

TOC

In general, it is expected that URI records will be used by clients for applications where the relevant protocol to be used is known, but, for example, an extra abstraction is needed in order to separate a domain name from a point of service (as addressed by the URI). One example of such a situation is when an organisation has many domain names, but only one official web page.

Applications MUST know the specific service fields to prepend the hostname with. Using repetitive queries for URI records MUST NOT be a replacement for querying for NAPTR records according to the NAPTR (DDDS) or S-NAPTR algorithms. NAPTR records serve the purpose to discover the various services and URIs for looking up access points for a given service. Those are two very different kinds of needs.

---

3. DNS considerations

TOC

Using prefix labels, such as underscored service tags, prevents the use of wildcards, as constructs as _s2._s1.*.example.net. are not possible in the DNS, see RFC 4592 (Lewis, E., “The Role of Wildcards in the Domain Name System,” July 2006.) [RFC4592]. Besides, underscored service tags used for the URI RR (based on the NAPTR service descriptions) may have slightly different semantics than service tags used for underscored prefix labels that are used in combination with other (yet unspecified) RR types. This may cause subtle management problems when delegation structure that has developed within the context of URI RRs is also to be used for other RR types. Since the service labels might be overloaded, applications should carefully check that the application level protocol is indeed the protocol they expect.

Subtle management issues may also arise when the delegations from service to sub service label involves several parties and different stake holders.

---

4. The format of the URI RR

TOC

This is the presentation format of the URI RR:

Ownername TTL Class URI Priority Weight Target

The URI RR does not cause any kind of Additional Section processing.

4.1. Ownername, class and type

TOC

The URI ownername is subject to special conventions.
Just like the SRV RR (Gulbrandsen, A., Vixie, P., and L. Esibov, “A DNS RR for specifying the location of services (DNS SRV),” February 2000.) [RFC2782] the URI RR has service information encoded in its ownername. In order to encode the service for a specific owner name one uses service parameters. Valid service parameters used are those used for SRV resource records, or registered by IANA for Enumservice Registrations. The Enumservice Registration parameters are reversed (subtype(s) before type), prepended with an underscore (_) and prepended to the owner name in separate labels. The underscore is prepended to the service parameters to avoid collisions with DNS labels that occur in nature, and the order is reversed to make it possible to do delegations, if needed, to different zones (and therefore providers of DNS).
It should be noted that the usage of a prefix must be described in detail in for example the Enumservice Registration documentation, or in a specific document that clarifies potential overload of parameters in the same URI. Specifically, registered URI schemes are not automatically acceptable as a service. With the HTTP scheme, one can for example have multiple methods (GET, PUT, etc), and this with the same URI.
For example, suppose we are looking for the URI for a service with Service Parameter "A:B:C" for host example.com.. Then we would query for (QNAME,QTYPE)=("_C._B._A.example.com","URI")
The type number for the URI record is TBD1 (to be assigned by IANA).
The URI resource record is class independent.
The URI RR has no special TTL requirements.

TOC

4.2. Priority

The priority of the target URI in this RR. Its range is 0-65535. A client MUST attempt to contact the URI with the lowest-numbered priority it can reach; URIs with the same priority SHOULD be tried in the order defined by the weight field.

4.3. Weight

TOC

A server selection mechanism. The weight field specifies a relative weight for entries with the same priority. Larger weights SHOULD be given a proportionately higher probability of being selected. The range of this number is 0-65535.

4.4. Target

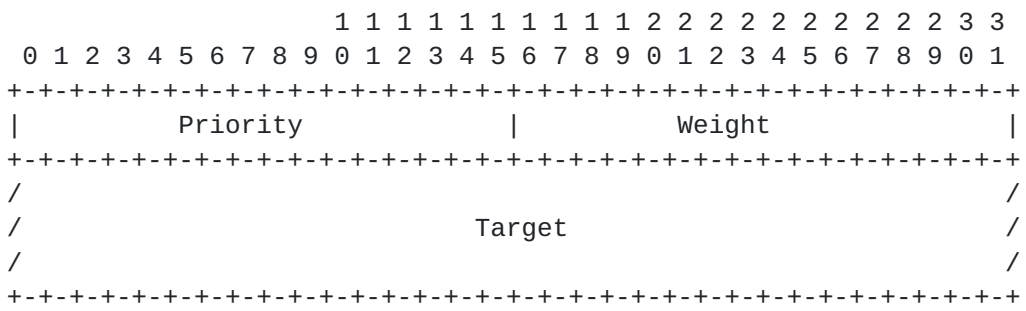
TOC

The URI of the target, enclosed in double-quote characters ('"'). Resolution of the URI is according to the definitions for the Scheme of the URI.
The URI is encoded as one or more <character-string> RFC1035 section 3.3 (Mockapetris, P., "Domain names - implementation and specification," November 1987.) [RFC1035].

4.5. URI RDATA Wire Format

TOC

The RDATA for a URI RR consists of a 2 octet Priority field, a two octet Weight field, and a variable length target field.
Priority and Weight are unsigned integers in network byte order.
The Target field contains the URI (without the enclosing double- quote characters used in the presentation format), encoded as a sequence of one or more <character-string> (as specified in section 3.3 of RFC 1035 (Mockapetris, P., "Domain names - implementation and specification," November 1987.) [RFC1035]), where all but the last <character-string> are filled up to the maximum length of 255 octets.
The Target field can also contain an IRI, but with the additional requirements that it is in UTF-8 (Yergeau, F., "UTF-8, a transformation format of ISO 10646," November 2003.) [RFC3629] and possible to convert to a URI according to section 3.1 of RFC 3987 (Duerst, M. and M. Suignard, "Internationalized Resource Identifiers (IRIs)," January 2005.) [RFC3987] and back again to an IRI according to section 3.2. Other character sets than UTF-8 are not allowed. The domain name part of the IRI can be either an U-LABEL or A-LABEL as defined in RFC 5890 (Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework," August 2010.) [RFC5890].



---

5. Definition of the flag 'D' for NAPTR records

TOC

This document specifies the flag "D" for use as a flag in NAPTR records. The flag indicate a terminal NAPTR record because it denotes the end of the DDDS/NAPTR processing rules. In the case of a "D" flag, the Replacement field in the NAPTR record, prepended with the service flags, is used as the Owner of a DNS query for URI records, and normal URI processing as defined in this document is applied.
The replacement field MUST NOT include any of the service parameters. Those are to be prepended (together with underscore) as described in other places in this document.
The Regexp field in the NAPTR record MUST be empty when the 'D' flag is in use.

---

6. Examples

TOC

6.1. Homepage at one domain, but two domains in use

TOC

An organisation has the domain names example.com and example.net, but the official URI http://www.example.com/. Given the service type "web" and subtype "http" (from the IANA registry), the following URI Resource Records could be made available in the respective zones (example.com and example.net):

```
$ORIGIN example.com.
_http._web    IN URI 10 1 "http://www.example.com/"

$ORIGIN example.net.
_http._web    IN URI 10 1 "http://www.example.com/"
```

---

7. Relation to S-NAPTR

TOC

The URI resource record type is not a replacement for the S-NAPTR. It is instead an extension and the seond step of the S-NAPTR resolution can resolve a URI resource record instead of using SRV records and yet another algorithm for how to use SRV records for the specific protocol.

```
$ORIGIN example.com.
;;       order pref flags
  IN NAPTR 100   10   "s"   "EM:ProtA"              ( ; service
                            ""                       ; regexp
                            _ProtA._tcp.example.com.   ; replacement
_ProtA._tcp IN URI "schemeA:service.example.com/example"
```

---

8. Relation to U-NAPTR

TOC

The URI Resource Record Type, together with S-NAPTR, can be viewed as a replacement for the U-NAPTR. The URI Resource Record Type is though only interesting when one know a base domain name, a protocol and service so that one can compose the record to look up. NAPTR records of any kind are used to look up what services exists for a certain domain, which is one step before the URI resource record is used.

---

9. Relation to SRV

TOC

The URI Resource Record Type can be viewed as a replacement for the SRV record. This because it like the SRV record can only be looked up if one know the base domain, the protocol and the service. It has a similar functionality, but instead of returning a hostname and port number, the URI record return a full URI. As such, it can be viewed as a more powerful resource record than SRV.

---

10. IANA Considerations

TOC

10.1. Registration of the URI Resource Record Type

TOC

IANA has assigned Resource Record Type TBD1 for the URI Resource Record Type and added the line depicted below to the registry named Resource Record (RR) TYPEs and QTYPEs as defined in BCP 42 RFC 5395 (Eastlake, D., "Domain Name System (DNS) IANA Considerations," November 2008.) [RFC5395] and located at http://www.iana.org/assignments/dns-parameters.

TYPE	Value and meaning	Reference
URI	TBD1 a URI for a service (per the owner name)	[RFCXXXX]

10.2. Registration of services

TOC

No new registry is needed for the registration of services as the Enumservice Registrations registry is used also for the URI resource record type.

11. Security Considerations

TOC

The authors do not believe this resource record cause any new security problems. Deployment must though be done in a proper way as misconfiguration of this resource record might make it impossible to reach the service that was originally intended to be accessed.
Using the URI resource record together with security mechanisms that relies on verification of authentication of hostnames, like TLS, makes it important to choose the correct domain name when doing the comparison.
The basic mechanism works as follows:

1. Announce the fact example.com is hosted at example.org (with some URL) in DNS

2. Secure the URI resource record with DNSSEC.

3. Verify the TLS (for example) certificate for the connection to example.org matches, i.e. use the hostname in the URI and not the hostname used originally when looking up the URI resource record.

4. If needed, do application layer authentication etc over the then encrypted connection.

What also can happen is that the URI in the resource record type has errors in it. Applications using the URI resource record type for resolution should behave similarly as if the user typed (or copy and pasted) the URI. At least it must be clear to the user that the error is not due to any error from his side.
One SHOULD not include userinfo (see User Information, Section 3.2.1, in RFC 3986 (Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax," January 2005.) [RFC3986]) in a URI that is used in a URI resource record as DNS data must be viewed as publicly available information.

---

12. Acknowledgements

TOC

Ideas on how to split the two different kind of queries "What services exists for this domain name" and "What is the URI for this service" came from Scott Bradner and Lawrence Conroy. Other people that have contributed to this document include Richard Barnes, Leslie Daigle, Olafur Gudmundsson, Ted Hardie, Peter Koch and Penn Pfautz.

Appendix A. RRTYPE Allocation Request

TOC

A. Submission Date:
May 23, 2009

B. Submission Type:
[X] New RRTYPE
[ ] Modification to existing RRTYPE

C. Contact Information for submitter:
Name: Patrik Faltstrom
Email Address: paf@cisco.com
International telephone number: +46-8-6859131
Other contact handles:

(Note: This information will be publicly posted.)

D. Motivation for the new RRTYPE application?
There is no easy way to get from a domain name to a URI (or IRI). Some mechanisms exists via use of the NAPTR (Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database," October 2002.) [RFC3403] resource record. That implies quite complicated rules that are simplified via the S-NAPTR (Daigle, L. and A. Newton, "Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)," January 2005.) [RFC3958] specification. But, the ability to directly look up a URI still exists. This specification uses a prefix based naming mechanism originated in the definition of the SRV (Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)," February 2000.) [RFC2782] resource record, and the RDATA is a URI, encoded as one text field.

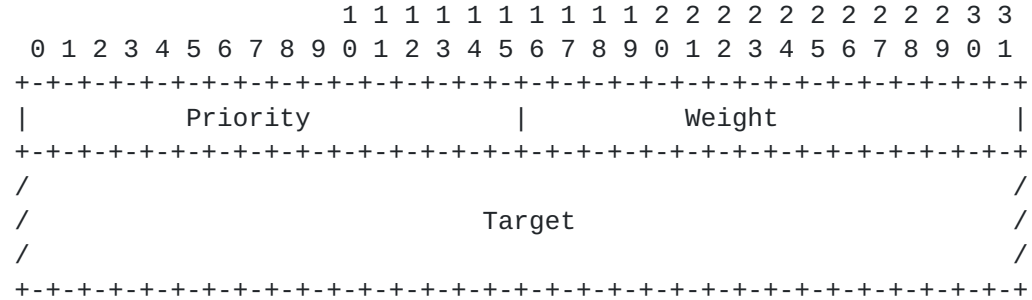
See also above (Introduction).

E. Description of the proposed RR type.
The format of the URI resource record is as follows:

```
Ownername TTL Class URI Priority Weight Target
```

The URI RR has service information encoded in its ownername. In order to encode the service for a specific owner name one uses service parameters. Valid service parameters used are either Enumservice Registrations registered by IANA, or prefixes used for the SRV resource record.

The wire format of the RDATA is as follows:



F. What existing RRTYPE or RRTYPEs come closest to filling that need and why are they unsatisfactory?

The RRTYPE that come closest is the NAPTR resource record. It is for example used in the DDDS and S-NAPTR algorithms. The main problem with the NAPTR is that selection of what record (or records) one is interested in is based on data stored in the RDATA portion of the NAPTR resource record. This, as explained in RFC 5507 (IAB, Faltstrom, P., Austein, R., and P. Koch, "Design Choices When Expanding the DNS," April 2009.) [RFC5507], is not optimal for DNS lookups. Further, most applications using NAPTR resource records uses regular expression based rewrite rules for creation of the URI, and that has shown be complicated to implement.

The second closest RRTYPE is the SRV record that given a prefixed based naming just like is suggested for the URI resource record, one get back a port number and domain name. This can also be used for creation of a URI, but, only URIs without path components.

G. What mnemonic is requested for the new RRTYPE (optional)?
URI

H. Does the requested RRTYPE make use of any existing IANA Registry or require the creation of a new IANA sub-registry in DNS Parameters?
Yes, partially.

One of the mechanisms to select a service is to use the Enumservice Registry managed by IANA. Another is to use services and protocols used for SRV records.

I. Does the proposal require/expect any changes in DNS servers/ resolvers that prevent the new type from being processed as an unknown RRTYPE (see [RFC3597])?
No

J. Comments:
None

13. References

TOC

13.1. Normative References

TOC

[E164]

	ITU-T, “The International Public Telecommunication Number Plan,” Recommendation E.164, May 1997.
[RFC1035]	Mockapetris, P., “Domain names - implementation and specification,” STD 13, RFC 1035, November 1987 (TXT).
[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC3629]	Yergeau, F., “UTF-8, a transformation format of ISO 10646,” STD 63, RFC 3629, November 2003 (TXT).
[RFC3958]	Daigle, L. and A. Newton, “Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS),” RFC 3958, January 2005 (TXT).
[RFC3987]	Duerst, M. and M. Suignard, “Internationalized Resource Identifiers (IRIs),” RFC 3987, January 2005 (TXT).
[RFC5395]	Eastlake, D., “Domain Name System (DNS) IANA Considerations,” BCP 42, RFC 5395, November 2008 (TXT).
[RFC5890]	Klensin, J., “Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework,” RFC 5890, August 2010 (TXT).

13.2. Non-normative references

TOC

[RFC2782]	Gulbrandsen, A., Vixie, P., and L. Esibov, “A DNS RR for specifying the location of services (DNS SRV),” RFC 2782, February 2000 (TXT).
[RFC3401]	Mealling, M., “Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS,” RFC 3401, October 2002 (TXT).
[RFC3403]	Mealling, M., “Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database,” RFC 3403, October 2002 (TXT).
[RFC3404]	Mealling, M., “Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI),” RFC 3404, October 2002 (TXT).
[RFC3986]	Berners-Lee, T., Fielding, R., and L. Masinter, “Uniform Resource Identifier (URI): Generic Syntax,” STD 66, RFC 3986, January 2005 (TXT, HTML, XML).
[RFC4592]	Lewis, E., “The Role of Wildcards in the Domain Name System,” RFC 4592, July 2006 (TXT).
[RFC4848]	Daigle, L., “Domain-Based Application Service Location Using URIs and the Dynamic Delegation Discovery Service (DDDS),” RFC 4848, April 2007 (TXT).
[RFC5507]	IAB, Faltstrom, P., Austein, R., and P. Koch, “Design Choices When Expanding the DNS,” RFC 5507, April 2009 (TXT).

Authors' Addresses

TOC

	Patrik Faltstrom
	Cisco Systems
Email:	paf@cisco.com
	Olaf Kolkman
	NLnet Labs
Email:	olaf@NLnetLabs.nl