Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 06, 2013

M. Blanchet
Viagenie

June 04, 2013

Finding the Authoritative Registration Data (RDAP) Server draft-blanchet-weirds-bootstrap-00.txt

Abstract

This document specifies a method to find which Registration Data Access Protocol (RDAP) server is authoritative to answer queries for a requested scope, such as domain names, IP addresses or Autonomous System numbers.

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 December 06, 2013.

Copyright Notice

Table of Contents

1. Introduction 2
2. Domain Name Registry 2
3. Internet Numbers Registry 3
3.1. IPv4 Address Space 3
3.2. IPv6 Address Space 3
3.3. Autonomous Systems 3
4. Nameserver 4
5. Entity 4
6. A and AAAA Queries 4
7. Processing NXDOMAIN Considerations 4
8. Querying to the Authoritative Server 4
9. Deployment Considerations 5
10. Security Considerations 5
11. IANA Considerations 5
12. Acknowledgements 6
13. References 6
13.1. Normative References 6
13.2. Informative References 6
Author's Address 7

1. Introduction

Querying and retrieving registration data from registries are defined in the Registration Data Access Protocol(RDAP)[I-D.ietf-weirds-rdap-query][I-D.ietf-weirds-using-http][I-D.ietf-weirds-json-response]. These documents do not specify where to send the queries. This document specifies a method to find which server is authoritative to answer queries for the requested scope.

(author note: should it have some text on various possibilities that have been discussed, such as IETF84...?)

The proposed mechanism starts with a well-known domain suffix (rdap.arpa) managed by IANA. Below the suffix, each scope is delegated to the entity responsible for the registration data. A RDAP client constructs a DNS query based on the scope of the user query and receives from the DNS the address(es) of the servers to contact to send the registration data query using the RDAP protocol.

The use of DNS provides the scaling and delegation properties needed for this large scale registration data access.

2. Domain Name Registry

The domain names authoritative registration data servers are found by concatenating the queried FQDN to the domain suffix:

"domain.rdap.arpa." and then generating DNS address queries for that concatenated domain.

For example, a RDAP query for example.com generates a DNS request to example.com.domain.rdap.arpa. IDN labels are in their A-label form[RFC5891].

3. Internet Numbers Registry

3.1. IPv4 Address Space

The IPv4 address space authoritative registration data servers are found by concatenating the reversed IPv4 address to the domain suffix: "ip4.rdap.arpa." and then generating A/AAAA DNS address queries for that concatenated domain. The reversed IPv4 address method is identical to the in-addr.arpa. tree method ([RFC1035] section 3.5).

For example, a query for 192.9.200.0/24 generates a DNS request to 200.9.192.ip4.rdap.arpa.

3.2. IPv6 Address Space

The IPv6 address space authoritative registration data servers are found by concatenating the reversed full IPv6 address to the domain suffix: "ip6.rdap.arpa." and then generating A/AAAA DNS address queries for that concatenated domain. The reversed full IPv6 address method is identical to the ip6.arpa. tree method ([RFC1886] section 2.5).

For example, a query for 2001:db8::/32 generates a DNS request to 8.b.d.0.1.0.0.2.ip6.rdap.arpa.

3.3. Autonomous Systems

The Autonomous Systems (AS) authoritative registration data servers are found by concatenating the AS number to the domain suffix: "autnum.rdap.arpa." and then generating A/AAAA DNS address queries for that concateneted domain.

For example, a query for AS 65411 generates a DNS request to 65411.autnum.rdap.arpa.

4. Nameserver

TBD

5. Entity

TBD

6. A and AAAA Queries

The RDAP client SHOULD not decide which of A and/or AAAA queries is sent as the DNS RR query. The client should use standard IP-independent APIs such as [RFC3493].

7. Processing NXDOMAIN Considerations

When a RDAP client receives a NXDOMAIN answer for the query, which means the queried domain does not exist, then the client removes the leftmost label of the domain and restart the query. The client redo this until either a positive answer or the domain to query is the root of the scope (i.e. {domain,ip4,ip6,autnum}.rdap.arpa). In this case, there is no such registration server available for the requested data and an error should be pushed to the end user.

For example, if the initial query is 8.b.d.0.1.0.0.2.ip6.rdap.arpa. and the answer is NXDOMAIN, then the new query is b.d.0.1.0.0.2.ip6.rdap.arpa. and if the answer is still NXDOMAIN, then a new query to b.d.0.1.0.0.2.ip6.rdap.arpa. is tried. The removal of leftmost labels continues until either a positive answer is received or the root of the scope (ip6.rdap.arpa in this example) is reached.

8. Querying to the Authoritative Server

After finding the authoritative server IP address, the client connects using the appropriate transport and application protocol to do the RDAP query[I-D.ietf-weirds-rdap-query]. The following is a non-normative example of the processing.

If the query is to find the registration data for "example.com", and the autoritative server is reachable by 2001:db8:1:1::1 over HTTP[I-D.ietf-weirds-using-http], then the following steps will happen:

- client sends A and AAAA DNS requests for example.com.domain.rdap.arpa.

- NXDOMAIN is received.

- client sends A and AAAA DNS requests for com.domain.rdap.arpa.
- 2001:db8:1:1:1 is received as the AAAA
- client sends an HTTP request to 2001:db8:1:1::1 with the following url: http://com.domain.rdap.arpa/domain/example.com
- client receives registration data for that domain[I-D.ietf-weirds-json-response]

9. Deployment Considerations

RDAP clients SHOULD not cache any server information, since that caching(and related expiration processing) is already happening at the DNS level. Therefore, the RDAP clients SHOULD always process a new RDAP request by querying the DNS to find the authoritative RDAP server as specified in this document.

RDAP server operators may use various techniques such as anycast[RFC4786] to manage the load on their servers.

To avoid walking up the tree, DNS wildcards may be used by the zone operators with the considerations discussed in [RFC4592]. Using the previous example, if the wildcard is defined for 1.0.0.2.ip6.rdap.arpa., the query to 8.b.d.0.1.0.0.2.ip6.rdap.arpa. will receive a positive answer instead of a negative answer. Therefore, no walking up the tree will be done to find the authoritative server.

This specification makes no assumption on how the authorities of registration data may work together on sharing their information for a common service. For example, the autnum zone may be wholly delegated to a single entity that acts on behalf of all regional registries for that space. The registration information of all autnum space can be provided by all registries to that single entity or redirection may be used at the HTTP level by the single operating entity to the servers of the authoritative registries.

10. Security Considerations

TBD

11. IANA Considerations

IANA is requested to do the following:

- delegation of rdap.arpa as a zone file managed by IANA

- creation of the domain,ip4,ip6,autnum zones under rdap.arpa.

- process by which an authoritative registration data registry requests addition/modification/removal of delegation of the zone for the scope the registry owns.

- author note: more details needed

12. Acknowledgements

The weirds working group had multiple discussions on this topic, including a session during IETF 84. All the people involved in these discussions are herin acknowledged. Simon Perreault, Jean-Philippe Dionne, John Levine, have provided input and suggestions to this document.

13. References

13.1. Normative References

[I-D.ietf-weirds-json-response]
Newton, A. and S. Hollenbeck, "JSON Responses for the Registration Data Access Protocol (RDAP)", draft-ietf-weirds-json-response-03 (work in progress), April 2013.

[I-D.ietf-weirds-rdap-query]
Newton, A. and S. Hollenbeck, "Registration Data Access Protocol Lookup Format", draft-ietf-weirds-rdap-query-04 (work in progress), April 2013.

[I-D.ietf-weirds-using-http]
Newton, A., Ellacott, B., and N. Kong, "HTTP usage in the Registration Data Access Protocol (RDAP)", draft-ietf-weirds-using-http-05 (work in progress), May 2013.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC1886] Thomson, S. and C. Huitema, "DNS Extensions to support IP version 6", RFC 1886, December 1995.

[RFC5891] Klensin, J., "Internationalized Domain Names in Applications (IDNA): Protocol", RFC 5891, August 2010.

13.2. Informative References

[RFC3493] Gilligan, R., Thomson, S., Bound, J., McCann, J., and W. Stevens, "Basic Socket Interface Extensions for IPv6", RFC 3493, February 2003.

[RFC4592] Lewis, E., "The Role of Wildcards in the Domain Name System", RFC 4592, July 2006.

[RFC4786] Abley, J. and K. Lindqvist, "Operation of Anycast Services", BCP 126, RFC 4786, December 2006.

Author's Address

Marc Blanchet
Viagenie
246 Aberdeen
Quebec, QC G1R 2E1
Canada

Email: Marc.Blanchet@viagenie.ca
URI: http://www.viagenie.ca