

add
Internet-Draft
Intended status: Informational
Expires: January 29, 2021

D. Migault
Ericsson
July 28, 2020

DNS Resolving service Discovery Protocol (DRDP)
draft-mglt-add-rdp-03

Abstract

This document describes the DNS Resolver Discovery Protocol (DRDP) that enables a DNS client to discover various available local and global resolving service. The discovery is primarily initiated by a DNS client, but a resolving service may also inform the DNS client other resolving services are available and eventually preferred.

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 <https://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 January 29, 2021.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Internet-Draft

DRDP

July 2020

Table of Contents

1.	Requirements Notation	2
2.	Introduction	2
3.	Terminology	3
4.	Overview	4
5.	Pointer to a list of Resolving Domains	5
6.	Discovery of Resolving Services	6
7.	TTL	7
8.	SvcParamKey	7
9.	Resolver advertising other service sub type	8
10.	Migration to service sub types	8
11.	Security Considerations	8
11.1.	Use of protected channel is RECOMMENDED	8
11.2.	DNSSEC is RECOMMENDED	9
11.3.	TLSA is RECOMMENDED	10
12.	Privacy Considerations	10
13.	IANA Considerations	11
14.	Acknowledgments	11
15.	Appendices	12
15.1.	DRDP Requirements	12
15.2.	Discovery of specific service instance	13
16.	References	14
16.1.	Normative References	14
16.2.	Informative References	14
	Author's Address	15

[1.](#) Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [BCP 14](#) [[RFC2119](#)] [[RFC8174](#)] when, and only when, they appear in all capitals, as shown here.

[2.](#) Introduction

A DNS client can proceed to DNS resolution using various resolving services. These services can be local or global and can use a wide range of DNS transport protocols such as, for example, standard DNS [[RFC1035](#)], DNS over TLS [[RFC7858](#)] or DNS over HTTPS [[RFC8484](#)]. The local scope of these services may take various forms. For example, it could be associated to a network perspective (restricted to the

network the DNS client is connected to) or to an application perspective (restricted to some domain names).

The purpose of the DNS Resolving service Discovery Protocol (DRDP) is to discover resolving services available to the DNS client. These

available resolving services to a given DNS client may highly depend on its location or browsing activity. The number of resolving services available to the DNS client is expected to remain quite consequent and evolve over time. Similarly, characteristics associated to these resolving services may also evolve over time. As a result, the DNS client is unlikely willing to synchronize such a huge data base of resolving services. DRDP proposes an alternative that consists in adaptively discovering the available resolving services based on the DNS client context.

DRDP adopts a hierarchical approach where the DNS client (or DRDP client) discovers the resolving services from resolving domains (RD) or a pointer to a list of resolving domains (Pointer).

The document does not describe how the DNS client is provisioned with RD or RD_list. The DNS client may obtain the contextual resolving domains via various way, including a configuration, via DHCP Options [[I-D.btw-add-home](#)] or derived from specific procedures [[I-D.mglt-add-drdp-isp](#)]. The DNS client is expected to discover resolving services from all RD or RD_list before proceeding to a selection process. The selection process of the resolving service is out of scope of this document.

[3.](#) Terminology

DNS client the client that sends DNS queries fro resolution. In this document the DNS client designates also the end entity that is collecting information about the available Resolving Services and then proceed to the selection of a subset them. The selection is processed according to the DNS client's policy.

Resolving Service designates a service that receives DNS queries from a DNS client and resolves them. A Resolving Service is implemented by one or multiple resolvers.

Resolver: A resolver designates the software or hardware handling the

DNS exchange. See [[RFC7719](#)] for more details.

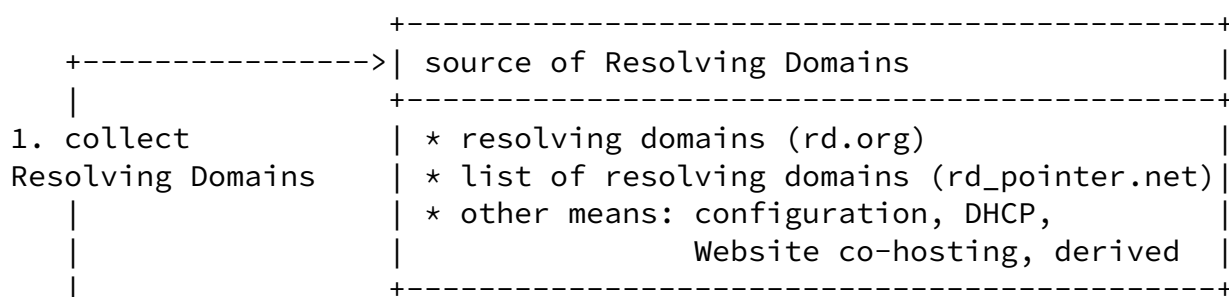
DNS transport designates the necessary parameters a DNS client needs to establish a session with a Resolving Service.

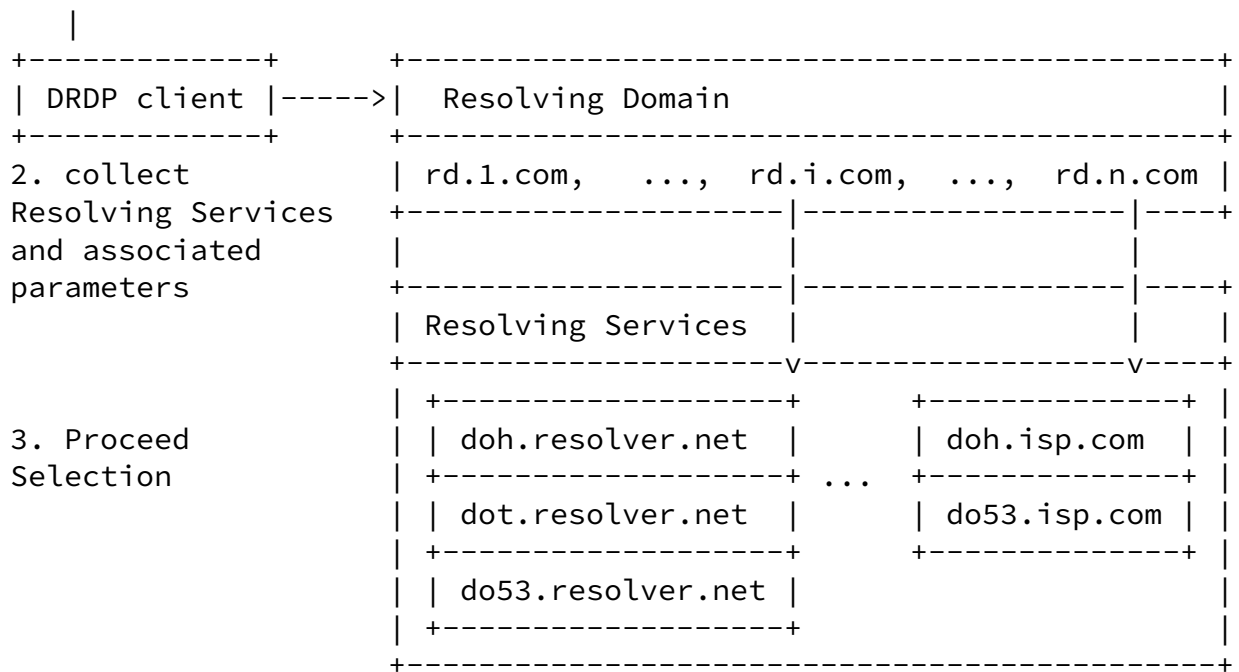
Resolving Domain a DNS domain that hosts one or multiple resolving services.

[4.](#) Overview

DRDP is a DNS based protocol that addresses the requirements listed in [Section 15.1](#). The figure below represents provides a high level description of DRDP.

1. The DRDP client considers the source of resolving domains (RD). This document defines two ways to collect RDs: RD are directly provisioned - in our case rd.org) , or RD are retrieved from a Pointer - in our case rd_pointer.org. In the later case RD are collected from a DNS request of type PTR. In the case of Pointer being rd_pointer.org, the QNAME of the PTR request would be b._dns.rd_pointer.org.
2. The DRDP client collects the resolving services and associated parameters under the umbrella of each RD. The resolving services offered by the RD are collected via a DNS request of type SVCB and the associated parameters are provided through SvcParameters. In the case of the RD being rd.org, the QNAME of the SVCB request would be _dns.rd.org.





5. Pointer to a list of Resolving Domains

A Pointer is a FQDN that points to a list of FQDN that designates RD. If Pointer is represented by rd_pointer.net, the associated RDs are retrieved by the DNS query of type PTR for b._dns.rd_pointer.org.

The zone file below is inspired from DNS-SD where b indicates a browsing domain, _dns indicates the DNS resolving service, rd_pointer.org the Pointer and rd.1.com, ... rd.i.com the associated RDs. Note that they do not necessarily need to share a TLD. The order of the resolving domains is irrelevant, and the zone administrator SHOULD regularly reorder them. The RRsets MUST be signed with DNSSEC.

```
b._dns.rd_pointer.net PTR rd.1.com
[...]
b._dns.rd_pointer.net PTR rd.n.com
```

Using the DNS provides the advantage to retrieve the resolving domain without requiring other libraries than DNS as well as benefit from the DNS caching infrastructure including the use of the TTL.

An EDNS buffer size of 1232 bytes will avoid fragmentation on nearly all current networks. This is based on an MTU of 1280, which is required by the IPv6 specification, minus 48 bytes for the IPv6 and UDP headers. This document RECOMMENDS that the number of RDs associated to a Pointer do not generate fragmentation of the DNS UDP packet. It is believed to address most common needs or expectation from a vast majority of stub DNS client.

When the number of RD exceeds this limit, the DNS client may carry this over TCP which is likely to be supported by DNS client willing to upgrade to DoH or DoT resolving services. However, the transfer of large number of RDs is considered as an application specificity that would benefit from the compression of the transferred data provided by ftp or http. In such case, these application may define there own specific mechanism to provision the RDs.

As of July 27 2020, 1232 bytes correspond to the 94 first most popular FQDN listed by [\[moz.com\]](https://moz.com). The current size of such lists [\[curl\]](https://curl.haxx.se)[\[dnsprivacy.org\]](https://dnsprivacy.org) have less than 50 resolving domains. Other lists such as [\[public-dns.info\]](https://public-dns.info) have as much as 11.000 entries, but such lists seems to contain open resolvers which is out side of the scope of a selection process.

Web browser (Google Chrome) also have lists over 10.000 entries, but in case a significant number of entries seems to be IP addresses that have a very limited network scope (e.g. limited to the ISP). The length of the list in scope to the DNS client is in fact significant

smaller in term of IP addresses and even smaller if resolving domain are able to represent multiple IP addresses. Overall, the size of such lists are currently due to the absence of discovery protocols.

[6.](#) Discovery of Resolving Services

The discovery of resolving services is performed by the RDP client with all the available RDs. Given a RD `rd.org`, a DRDP client sends a DNS request of type SVCB for `_dns.rd.org`.

The example below presents the use of an AliasForm followed by a ServiceForm which allows an indirection. The Alias form is not madatory and instead only ServiceForm associated to `_dns.rd.org` could have been used instead.

The SvcFieldPriority indicates the preference of the RD. It typically enables an operator to indicate that an encrypted DNS is preferred.

The SvcParamKey alpn MUST be present when TLS is used as its presence and value indicates the DNS transport. The absence of the alpn SvcParamKey indicates Do53, alpn set to dot indicates DoT is served while h* indicates DoH is served. Note that the port value (53, 853, 443) is not used to determine the DNS transport as non standard port MAY be used. The example below uses an non standard port 5353 for illustrative purpose.

Other SvcParam are detailed in [Section 8](#) and are optional. A SvcParam not understood by the DNS client MUST be ignored.

The RRsets MUST be protected with DNSSEC and when alpn is provided a TLSA RRset SHOULD be present. These RRsets have been omitted for clarity.

```
## Discovery of all service instances
_dns.rd.org. 7200 IN SVCB 0 svc.example.com.
svc.example.com.      7200 IN SVCB 12 ( svc0.example.net.
                                port="5353" user-display="Legacy Resolver
svc.example.com.      7200 IN SVCB 1 ( svc1.example.net.  alpn="dot"
                                port="5353" esniconfig="..."
                                user-display="Preferred Example's Choice"
svc.example.com.      7200 IN SVCB 3 ( svc2.example.net.  alpn="h2"
                                port="5353" esniconfig="..." user-displa
svc.example.com.      7200 IN SVCB 2 ( svc3.example.net.  alpn="h3"
                                port="5353" esniconfig="..." user-displa
```

Note that [Section 15.2](#) provides another variant to perform RDP. Such variant is left for further discussion and address the need to be able to narrow down the discovery to a subset of resolving services such as DoH-only or DoT-only services.

Some notes:

1. _domain uses SVCB but does not have TLS. While SVCB has been

created essentially for TLS based service, this does not appear to be mandatory.

2. Should we have some constraints regarding the SvcDomainName and QNAME ?
3. do we need the service subsets

7. TTL

The DNS client SHOULD perform DRDP at regular intervals as indicated by its policy.

The selection process MAY remove resolving services with short TTL lower than a day as it indicates some source of instability. Given a subset of selected resolving services, the DNS client may perform DRDP 1 hour before an SVB RRset expires.

8. SvcParamKey

This section defines a set of SvcParamKey that MAY be use to carry the necessary informations for the selection process.

alpn :

esniconfig :

port :

user-display indicates a strings in UTF-8 that is expected to be representative to a potential end user. Though there is no restriction in the scope of that string. The string is likely to represent the service within the resolving domain.

uri_template designates the URI template for DoH. This key MUST NOT be present on non DoH services and MUST be ignored by the DNS client on non DoH resolving Services.

auth_domain indicates the list of authoritative domain name the resolving service has strong relation with. It is expected that a

resolving service may prefer to perform DNS resolution over these

domains to that specific resolving service as to preserve its privacy. This information **MUST** be verified and validated.

`scope_domain` indicates the limitation of resolved domains. When present DNS request sent to the resolution service **MUST** belong to that domain.

`filtering` indicates the presence of a filtering service

`ip_subnet` indicates a subnetwork restriction. This is mostly useful for resolving services that are not globally.

`dnssec` indicates whether dnssec is enabled or not.

[9.](#) Resolver advertising other service sub type

A resolving service receiving a DNS request over a service sub type **MAY** be willing to advertise the DNS client that other sub service type are available. This is especially useful, when, for example, a resolver wants that the DNS resolver switches to other service sub types that are more secure.

In order to do so the resolver **MAY** provide in the additional data field the `_dns SRVCB` of `ServiceForm`.

[10.](#) Migration to service sub types

The principle of the discovery mechanism is that the resolver indicates the available service sub types and let the DNS client chose which sub type it prefers. On the other hand, the resolver **MAY** also indicate a preference using the priority and weight fields. Redirection **MAY** especially be needed when a DNS client is using the Do53 and the resolver would like to upgrade the DNS client session to a more secure session. This **MAY** require a specific `ERROR` code that will request the DNS client to perform service discovery.

It is expected that `DRDP` **MUST** always be available via Do53. However, this does not mean that a resolver is expected to implement the Do53 sub type service for a resolving service.

[11.](#) Security Considerations

[11.1.](#) Use of protected channel is **RECOMMENDED**

When available, it is recommended to chose a protected version of the `rdns` service. More specifically, the use of end-to-end protection ensures that the DNS client is connected to the expected platform and

that its traffic cannot be intercepted on path. Typically, the selection of resolver on the Internet (and not on your ISP network) and the use of a non protected channel enables an attacker to monitor your DNS traffic. The similar observation remains true if you are connected to the resolver of your ISP. It is commonly believed that trusting your ISP (that is your first hop) makes encryption unnecessary. Trusting your ISP is mandatory in any case, but the associated level of trust with an protected channel is restricted to the operation of the DNS platform. With non protected channel the trust is extended to any segment between the DNS client and the resolver, which is consequently larger. The use of a protected channel is recommended as it will prevent anyone on path to monitor your traffic.

11.2. DNSSEC is RECOMMENDED

The exchanges SHOULD be protected with DNSSEC to ensure integrity of the information between the authoritative servers and the DNS client. Without DNSSEC protection, DNS messages may be tampered typically when they are transmitted over an unprotected channel either between the DNS client and the resolver or between the resolver and the authoritative servers. The messages may be tampered by an online attacker intercepting the messages or by the intermediary devices. It is important to realize that protection provided by TLS is limited to the channel between the DNS client and the resolver. There are a number of cases where the trust in the resolver is not sufficient which justify the generalization of the use of DNSSEC. The following examples are illustrative and are intended to be exhaustive.

First, the discovery exchanges may happen over an unprotected channel, in which case, the messages exchanged may be tampered by anyone on-path between the DNS client and the resolver as well as between the resolver and the authoritative servers - including the resolver. When TLS is used between the DNS client and the resolver, this does not necessarily mean the DNS client trusts the resolver. Typically, the TLS session may be established with a self-signed certificate in which case the session is basically protected by a proof-of-ownership. In other cases, the session may be established based on Certificate Authorities (CA) that have been configured into the TLS client, but that are not necessarily trusted by the DNS client. In such cases, the connected resolver may be used to discover resolvers from another domain. In this case, the resolver is probably interacting with authoritative servers using untrusted and unprotected channels. Integrity protection relies on DNSSEC.

[11.3.](#) TLSA is RECOMMENDED

When TLS is used to protect the DNS exchanges, certificates or fingerprint SHOULD be provided to implement trust into the communication between the DNS client and the resolver. The TLS session and the association of the private key to a specific identity can be based on two different trust model. The Web PKI that will rely on CA provisioned in the TLS library or the TA provided to the DNS client. A DNS client SHOULD be able to validate the trust of a TLS session based on the DNSSEC trust model using DANE.

When the DNS client is protecting its session to the resolver via TLS, the DNS client may initiate an TLS session that is not validated by a CA or a TLSA RRsets. The DNS client MUST proceed to the discovery process and validate the certificate match the TLSA RRset. In case of mismatch the DNS client MUST abort the session.

[12.](#) Privacy Considerations

When the discovery protocol is performed using a resolver that belongs to one domain for another domain, or over an unprotected channel, the DNS client must be conscious that its is revealing to the resolver its intention to use another resolver. More specifically, suppose an resolver is complying some legal requirements that DNS traffic must be unencrypted. Using this resolver to perform a resolver discovery reveals the intention of potentially using alternative resolvers. Alternatively, narrowing down the discovery over a specific sub type of resolver (DoT, or DoH) may reveal to that resolver the type of communication. As result, when performing a discovery over a domain that differs to the domain the resolver belongs to, it is RECOMMENDED to request the SRV RRsets associated to all different sub type of proposed services.

The absence of traffic that results from switching completely to a newly discovered resolver right after the discovery process provides an indication to the resolver the DNS client is switching to. It is hard to make that switch unnoticed to the initial resolver and the DNS resolver MUST assume this will be noticed. The information of switching may be limited by sharing the traffic between different

resolvers, however, the traffic pattern associated to each resolver may also reveal the switch. In addition, when the initial resolver is provided by the ISP, the ISP is also able to monitor the IP traffic and infer the switch. As a result, the DNS client SHOULD assume the switch will be detected.

With DoT or DoH, the selection of port 443 will make the traffic indistinguishable from HTTPS traffic. This means that an observer will not be able to tell whether the traffic carries web traffic or

DNS traffic. Note that it presents an interest if the server offers both a web service as well as a resolution service. Note that many resolvers have a dedicated IP address for the resolution service, in which case, the information will be inferred from the IP address. Note also that traffic analysis may infer this as well. Typically suppose an IP address hosts one or multiple web sites that are not popular as well as a resolving service. If this IP address is associated frequent short size exchanges, it is likely that these exchanges will be DNS exchanges rather than Web traffic. The size of the packet may also be used as well as many other patterns. As a result, the use port 443 to hide the DNS traffic over web traffic should be considered as providing limited privacy.

13. IANA Considerations

This document requests the IANA the creation of the following underscored node names in the Underscored and Globally Scoped DNS Node Names registry <https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-14>

RR Type	_NODE NAME	Reference
-----+-----+-----		
SRVCB	_dns	RFC-TBD

SvcParamKey	NAME	Meaning	Reference
-----+-----+-----+-----			
7	user-display	User friendly string (UTF8)	RFC-TBD
		to represent the resolver	
	uri_template	URI template	
	auth_domain	Domains the resolving	
		service is authoritative	
	filetring	Filetring services provided	

ip_subnet	ip ranges accepted.	
dnssec	DNSSEC validation enabled	

[14.](#) Acknowledgments

We would like thank Mirja Kuehlewind as well as the GSMA IG for their comments. We also thank Ted Hardie and Paul Hoffman for their feed backs regarding the dns schemes for DoT and DoH.

We thank Ben Schwartz for the comments on the list size. We thank Harald Alvestrand for its recommendation on having a model that enable multiple third party providers to provide their own list of resolving domains. We thank Stephan Bortzmeyer, Ralf Weber, Chris Box for its clarifications.

Migault

Expires January 29, 2021

[Page 11]

Internet-Draft

DRDP

July 2020

[15.](#) Appendices

[15.1.](#) DRDP Requirements

This section lists the DRDP requirements.

REQ 1: DRDP MUST enable a DNS client to discover the available resolving services with their associated characteristics in order to proceeds to a selection process. The selection process takes resolving services identities and associated parameters and proceed to the selection.

Any sort of resolving service selection is outside the scope of DRDP.

REQ 2: While the discovery process is triggered by the DNS client, a third party MUST be able to provide necessary input information so a resolving service discovery process can be triggered within a specific context.

Provisioning protocols to provide this information is not as per say in scope of DRDP. DRDP defines the format of the format for such input as well as a set of such inputs.

REQ 3: Any information used in DRDP MUST be authenticated by its owner. In particular, the characteristics associated to the resolving service MUST be certified by the resolving service operator / owner and MUST be associated a validity period. In addition, a

third party providing a set of inputs MUST authenticate that set.

REQ 4: Information associated to the resolving services is intended to enable the selection process that is assumed to match the end user or application policy. The selection process is out of scope of DRDP. Information may carry some characteristics of a resolving service or hints that will help the selection. In particular an operator of multiple resolving service MUST be able to associate a preference to the proposed resolving services. To ease automation of the selection as well as to make multiple applications benefit from DRDP the information MUST be carried over a standardized format.

REQ 5: DRDP MUST be designed to be used indifferently by a DNS client using any DNS transport protocol (Do53, DoT, DoH, ...). However, DRDP SHOULD be able to restrict the information retrieved to a certain type of resolving service, i.e. Do53, DoT, DoH.

REQ 6: DRDP deployment MUST NOT be disruptive for the legacy DNS client or infrastructure and legacy client SHOULD be able to incrementally include DRDP.

[15.2.](#) Discovery of specific service instance

To reduce the size of the messages, the DNS client MAY also prefer to query information of resolving services using a specific transport (DNS, DoT, DoH) that are designated as sub sets. A DNS client MAY list the different subsets of that resolving domain with a PTR query. This document defines the following subsets `_53._dns` for DNS, `_853._dns` for DoT and `_443._dns` for DoH. Other subsets MAY be defined in the future. A DNS client that does not understand a subset SHOULD ignore it and maybe proceed to the discovery as defined in [Section 6](#).

All subsets MUST share the same resolving domain and be listed with a PTR RRsets. The DNS client MAY NOT performed a DNS query of type PTR, for example, if it has a previous knowledge of the existence of the subset or if indicated by its policy. In this it MAY directly proceed to the SRVCB resolution.

The same restrictions as defined in section [Section 6](#) apply.

Note that while the SvcFieldPriority indicates the priority within a subservice, this field MUST have a coherence across subservices. The priority provided SHOULD be coherent with the case of a _dns SRVCB query of section [Section 6](#).

The figure below illustrates an example of zone file. RRSIG and TLSA have been omitted for the purpose of clarity.

```
### Definition of the resolving service subsets
_dns.example.com PTR _53._dns.example.com
_dns.example.com PTR _853._dns.example.com
_dns.example.com PTR _443._dns.example.com

### services instances per service subset
_53._dns.example.com. 7200 IN SVCB 0 svc0.example.com.
svc0.example.com.      7200 IN SVCB 12 ( svc0.example.net.
                                port="5353" user-display="Legacy Resolve
_853._dns.example.com. 7200 IN SVCB 0 svc1.example.com.
svc1.example.com.      7200 IN SVCB 1 ( svc1.example.net. alpn="dot"
                                port="5353" esniconfig="..."
                                user-display="Preferred Example's Choice"

_443._dns.example.com. 7200 IN SVCB 0 svc4.example.net.
svc4.example.com.      7200 IN SVCB 3 ( svc2.example.net. alpn="h2"
                                port="5353" esniconfig="..." user-displa
svc4.example.com.      7200 IN SVCB 2 ( svc3.example.net. alpn="h3"
                                port="5353" esniconfig="..."
                                user-display="Testing QUIC")
```

[16.](#) References

[16.1.](#) Normative References

- [RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, [RFC 1035](#), DOI 10.17487/RFC1035, November 1987, <<https://www.rfc-editor.org/info/rfc1035>>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997,

<<https://www.rfc-editor.org/info/rfc2119>>.

- [RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", [RFC 7858](#), DOI 10.17487/RFC7858, May 2016, <<https://www.rfc-editor.org/info/rfc7858>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.
- [RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", [RFC 8484](#), DOI 10.17487/RFC8484, October 2018, <<https://www.rfc-editor.org/info/rfc8484>>.

16.2. Informative References

- [curl] "Publicly available servers", n.d., <<https://github.com/curl/curl/wiki/DNS-over-HTTPS#publicly-available-servers>>.
- [dnsprivacy.org] "DNS Privacy Test Servers", n.d., <<https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Test+Servers#DNSPrivacyTestServers-Publicresolvers>>.
- [I-D.btw-add-home] Boucadair, M., Reddy, K. T., Wing, D., and N. Cook, "Encrypted DNS Discovery and Deployment Considerations for Home Networks", [draft-btw-add-home-07](#) (work in progress), July 2020.
- [moz.com] "The Moz Top 500 Websites", n.d., <<https://moz.com/top500>>.

- [public-dns.info] "Public DNS Server List", n.d., <<https://public-dns.info/>>.

[RFC7719] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", [RFC 7719](https://www.rfc-editor.org/info/rfc7719), DOI 10.17487/RFC7719, December 2015, <<https://www.rfc-editor.org/info/rfc7719>>.

Author's Address

Daniel Migault
Ericsson
8275 Trans Canada Route
Saint Laurent, QC 4S 0B6
Canada

EMail: daniel.migault@ericsson.com