Workgroup: ADD
Internet-Draft: draft-ietf-add-ddr-09
Published: 3 August 2022
Intended Status: Standards Track
Expires: 4 February 2023
Authors: T. Pauly
Apple Inc.
E. Kinnear
Apple Inc.
C. A. Wood
Cloudflare
P. McManus
Fastly
T. Jensen
Microsoft

Discovery of Designated Resolvers

Abstract

This document defines Discovery of Designated Resolvers (DDR), a mechanism for DNS clients to use DNS records to discover a resolver's encrypted DNS configuration. An encrypted DNS resolver discovered in this manner is referred to as a "Designated Resolver". This mechanism can be used to move from unencrypted DNS to encrypted DNS when only the IP address of a resolver is known. This mechanism is designed to be limited to cases where unencrypted DNS resolvers and their designated resolvers are operated by the same entity or cooperating entities. It can also be used to discover support for encrypted DNS protocols when the name of an encrypted DNS resolver is known.

Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the Adaptive DNS Discovery Working Group mailing list (add@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/add/.

Source for this draft and an issue tracker can be found at https://github.com/ietf-wg-add/draft-ietf-add-ddr.

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 4 February 2023.

Copyright Notice

Table of Contents

1. Introduction

When DNS clients wish to use encrypted DNS protocols such as DNS-over-TLS (DoT) [RFC7858], DNS-over-QUIC (DoQ) [RFC9250], or DNS-over-HTTPS (DoH) [RFC8484], they can require additional information beyond the IP address of the DNS server, such as the resolver's hostname, alternate IP addresses, non-standard ports, or URI templates. However, common configuration mechanisms only provide the resolver's IP address during configuration. Such mechanisms include network provisioning protocols like DHCP [RFC2132] [RFC8415] and IPv6 Router Advertisement (RA) options [RFC8106], as well as manual configuration.

This document defines two mechanisms for clients to discover designated resolvers that support these encrypted protocols using DNS server Service Binding (SVCB, [I-D.ietf-dnsop-svcb-https]) records:

1. When only an IP address of an Unencrypted DNS Resolver is known, the client queries a special use domain name (SUDN) [RFC6761] to discover DNS SVCB records associated with one or more Encrypted DNS Resolvers the Unencrypted DNS Resolver has designated for use when support for DNS encryption is requested (Section 4).

2. When the hostname of an Encrypted DNS Resolver is known, the client requests details by sending a query for a DNS SVCB record. This can be used to discover alternate encrypted DNS protocols supported by a known server, or to provide details if a resolver name is provisioned by a network (Section 5).

Both of these approaches allow clients to confirm that a discovered Encrypted DNS Resolver is designated by the originally provisioned resolver. "Designated" in this context means that the resolvers are operated by the same entity or cooperating entities; for example, the resolvers are accessible on the same IP address, or there is a certificate that contains the IP address for the original designating resolver.

1.1. Specification of Requirements

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. Terminology

This document defines the following terms:

DDR:
Discovery of Designated Resolvers. Refers to the mechanisms defined in this document.

Designated Resolver: A resolver, presumably an Encrypted DNS Resolver, designated by another resolver for use in its own place. This designation can be verified with TLS certificates.

Encrypted DNS Resolver: A DNS resolver using any encrypted DNS transport. This includes current mechanisms such as DoH, DoT, and DoQ, as well as future mechanisms.

Unencrypted DNS Resolver: A DNS resolver using a transport without encryption, historically TCP or UDP port 53.

3. DNS Service Binding Records

DNS resolvers can advertise one or more Designated Resolvers that may offer support over encrypted channels and are controlled by the same entity.

When a client discovers Designated Resolvers, it learns information such as the supported protocols and ports. This information is provided in ServiceMode Service Binding (SVCB) records for DNS Servers, although AliasMode SVCB records can be used to direct clients to the needed ServiceMode SVCB record per [I-D.ietf-dnsop-svcb-https]. The formatting of these records, including the DNS-unique parameters such as "dohpath", are defined by [I-D.ietf-add-svcb-dns].

The following is an example of an SVCB record describing a DoH server discovered by querying for _dns.example.net:

```
_dns.example.net.  7200  IN SVCB 1 example.net. (
     alpn=h2 dohpath=/dns-query{?dns} )
```

The following is an example of an SVCB record describing a DoT server discovered by querying for _dns.example.net:

```
_dns.example.net.  7200  IN SVCB 1 dot.example.net (
     alpn=dot port=8530 )
```

The following is an example of an SVCB record describing a DoQ server discovered by querying for _dns.example.net:

```
_dns.example.net.  7200  IN SVCB 1 doq.example.net (
     alpn=doq port=8530 )
```

If multiple Designated Resolvers are available, using one or more encrypted DNS protocols, the resolver deployment can indicate a

preference using the priority fields in each SVCB record [I-D.ietf-dnsop-svcb-https].

If the client encounters a mandatory parameter in an SVCB record it does not understand, it MUST NOT use that record to discover a Designated Resolver, in accordance with Section 8 of [I-D.ietf-dnsop-svcb-https]. The client can still use other records in the same response if the client can understand all of their mandatory parameters. This allows future encrypted deployments to simultaneously support protocols even if a given client is not aware of all those protocols. For example, if the Unencrypted DNS Resolver returns three SVCB records, one for DoH, one for DoT, and one for a yet-to-exist protocol, a client which only supports DoH and DoT should be able to use those records while safely ignoring the third record.

To avoid name lookup deadlock, clients that use Designated Resolvers need to ensure that a specific Encrypted Resolver is not used for any queries that are needed to resolve the name of the resolver itself or to perform certificate revocation checks for the resolver, as described in Section 10 of [RFC8484]. Designated Resolvers need to ensure this deadlock is avoidable as described in Section 10 of [RFC8484].

This document focuses on discovering DoH, DoT, and DoQ Designated Resolvers. Other protocols can also use the format defined by [I-D.ietf-add-svcb-dns]. However, if any such protocol does not involve some form of certificate validation, new validation mechanisms will need to be defined to support validating designation as defined in Section 4.2.

4. Discovery Using Resolver IP Addresses

When a DNS client is configured with an Unencrypted DNS Resolver IP address, it SHOULD query the resolver for SVCB records of a service with a scheme of "dns" and an Authority of "resolver.arpa" before making other queries. This allows the client to switch to using Encrypted DNS for all other queries, if possible. Specifically, the client issues a query for _dns.resolver.arpa. with the SVCB resource record type (64) [I-D.ietf-dnsop-svcb-https].

Because this query is for an SUDN, which no entity can claim ownership over, the ServiceMode SVCB response MUST NOT use the "." value for the TargetName. Instead, the domain name used for DoT/DoQ or used to construct the DoH template MUST be provided. This ensures that different designated resolver configurations can be correctly associated with IP addresses in A and AAAA records. As such, clients MUST NOT perform A and AAAA queries for "resolver.arpa".

The following is an example of an SVCB record describing a DoH server discovered by querying for _dns.resolver.arpa:

```
_dns.resolver.arpa.  7200  IN SVCB 1 doh.example.net (
     alpn=h2 dohpath=/dns-query{?dns} )
```

The following is an example of an SVCB record describing a DoT server discovered by querying for _dns.resolver.arpa:

```
_dns.resolver.arpa.  7200  IN SVCB 1 dot.example.net (
     alpn=dot port=8530 )
```

The following is an example of an SVCB record describing a DoQ server discovered by querying for _dns.resolver.arpa:

```
_dns.resolver.arpa.  7200  IN SVCB 1 doq.example.net (
     alpn=doq port=8530 )
```

If the recursive resolver that receives this query has one or more Designated Resolvers, it will return the corresponding SVCB records. When responding to these special queries for "resolver.arpa", the recursive resolver SHOULD include the A and AAAA records for the name of the Designated Resolver in the Additional Answers section. This will save the DNS client an additional round trip to retrieve the address of the designated resolver; see Section 5 of [I-D.ietf-dnsop-svcb-https].

Designated Resolvers SHOULD be accessible using the IP address families that are supported by their associated Unencrypted DNS Resolvers. If an Unencrypted DNS Resolver is accessible using an IPv4 address, it ought to provide an A record for an IPv4 address of the Designated Resolver; similarly, if it is accessible using an IPv6 address, it ought to provide a AAAA record for an IPv6 address of the Designated Resolver. The Designated Resolver MAY support more address families than the Unencrypted DNS Resolver, but it SHOULD NOT support fewer. If this is not done, clients that only have connectivity over one address family might not be able to access the Designated Resolver.

If the recursive resolver that receives this query has no Designated Resolvers, it SHOULD return NODATA for queries to the "resolver.arpa" zone, to provide a consistent and accurate signal to clients that it does not have a Designated Resolver.

4.1. Use of Designated Resolvers

When a client discovers Designated Resolvers from an Unencrypted DNS Resolver IP address, it can choose to use these Designated Resolvers either automatically, or based on some other policy, heuristic, or user choice.

This document defines two preferred methods to automatically use Designated Resolvers:

- Verified Discovery (Section 4.2), for when a TLS certificate can be used to validate the resolver's identity.

- Opportunistic Discovery (Section 4.3), for when a resolver's IP address is a private or local address.

A client MAY additionally use a discovered Designated Resolver without either of these methods, based on implementation-specific policy or user input. Details of such policy are out of scope of this document. Clients MUST NOT automatically use a Designated Resolver without some sort of validation, such as the two methods defined in this document or a future mechanism. Use without validation can allow an attacker to direct traffic to an Encrypted Resolver that is unrelated to the original Unencrypted DNS Resolver, as described in Section 7.

A client MUST NOT re-use a designation discovered using the IP address of one Unencrypted DNS Resolver in place of any other Unencrypted DNS Resolver. Instead, the client needs to repeat the discovery process to discover the Designated Resolver of the other Unencrypted DNS Resolver. In other words, designations are per-resolver and MUST NOT be used to configure the client's universal DNS behavior. This ensures in all cases that queries are being sent to a party designated by the resolver originally being used.

4.1.1. Use of Designated Resolvers across network changes

If a client is configured with the same Unencrypted DNS Resolver IP address on multiple different networks, a Designated Resolver that has been discovered on one network SHOULD NOT be reused on any of the other networks without repeating the discovery process for each network, since the same IP address may be used for different servers on the different networks.

4.2. Verified Discovery

Verified Discovery is a mechanism that allows automatic use of a Designated Resolver that supports DNS encryption that performs a TLS handshake.

In order to be considered a verified Designated Resolver, the TLS certificate presented by the Designated Resolver needs to pass the following checks made by the client:

1. The client MUST verify the chain of certificates up to a trust anchor as described in Section 6 of [RFC5280]. This SHOULD use

the default system or application trust anchors, unless otherwise configured.

2. The client MUST verify that the certificate contains the IP address of the designating Unencrypted DNS Resolver in an iPAddress entry of the subjectAltName extension as described in Section 4.2.1.6 of [RFC5280].

If these checks pass, the client SHOULD use the discovered Designated Resolver for any cases in which it would have otherwise used the Unencrypted DNS Resolver, so as to prefer Encrypted DNS whenever possible.

If these checks fail, the client MUST NOT automatically use the discovered Designated Resolver if this designation was only discovered via a _dns.resolver.arpa. query (if the designation was advertised directly by the network as described in Section 6.5, the server can still be used). Additionally, the client SHOULD suppress any further queries for Designated Resolvers using this Unencrypted DNS Resolver for the length of time indicated by the SVCB record's Time to Live (TTL) in order to avoid excessive queries that will lead to further failed validations. The client MAY issue new queries if the SVCB record's TTL is excessively long (as determined by client policy) to minimize the length of time an intermittent attacker can prevent use of encrypted DNS.

If the Designated Resolver and the Unencrypted DNS Resolver share an IP address, clients MAY choose to opportunistically use the Designated Resolver even without this certificate check (Section 4.3). If the IP address is not shared, opportunistic use allows for attackers to redirect queries to an unrelated Encrypted Resolver, as described in Section 7.

Connections to a Designated Resolver can use a different IP address than the IP address of the Unencrypted DNS Resolver, such as if the process of resolving the SVCB service yields additional addresses. Even when a different IP address is used for the connection, the TLS certificate checks described in this section still apply for the original IP address of the Unencrypted DNS Resolver.

4.3. Opportunistic Discovery

There are situations where Verified Discovery of encrypted DNS configuration over unencrypted DNS is not possible. This includes Unencrypted DNS Resolvers on private IP addresses [RFC1918], Unique Local Addresses (ULAs) [RFC4193], and Link Local Addresses [RFC3927] [RFC4291], whose identity cannot be safely confirmed using TLS certificates under most conditions.

An Opportunistic Privacy Profile is defined for DoT in Section 4.1 of [RFC7858] as a mode in which clients do not validate the name of the resolver presented in the certificate. This Opportunistic Privacy Profile similarly applies to DoQ [RFC9250]. For this profile, Section 4.1 of [RFC7858] explains that clients might or might not validate the resolver; however, even if clients choose to perform some certificate validation checks, they will not be able to validate the names presented in the SubjectAlternativeName field of the certificate for private and local IP addresses.

A client MAY use information from the SVCB record for "_dns.resolver.arpa" with this Opportunistic Privacy Profile as long as the IP address of the Encrypted DNS Resolver does not differ from the IP address of the Unencrypted DNS Resolver. Clients SHOULD use this mode only for resolvers using private or local IP addresses, since resolvers that use other addresses are able to provision TLS certificates for their addresses.

5. Discovery Using Resolver Names

A DNS client that already knows the name of an Encrypted DNS Resolver can use DDR to discover details about all supported encrypted DNS protocols. This situation can arise if a client has been configured to use a given Encrypted DNS Resolver, or if a network provisioning protocol (such as DHCP or IPv6 Router Advertisements) provides a name for an Encrypted DNS Resolver alongside the resolver IP address, such as by using Discovery of Network Resolvers (DNR) [I-D.ietf-add-dnr].

For these cases, the client simply sends a DNS SVCB query using the known name of the resolver. This query can be issued to the named Encrypted DNS Resolver itself or to any other resolver. Unlike the case of bootstrapping from an Unencrypted DNS Resolver (Section 4), these records SHOULD be available in the public DNS if the same domain name's A or AAAA records are available in the public DNS to allow using any resolver to discover another resolver's Designated Resolvers. When the name can only be resolved in private namespaces, these records SHOULD be available to the same audience as the A and AAAA records.

For example, if the client already knows about a DoT server resolver.example.com, it can issue an SVCB query for _dns.resolver.example.com to discover if there are other encrypted DNS protocols available. In the following example, the SVCB answers indicate that resolver.example.com supports both DoH and DoT, and that the DoH server indicates a higher priority than the DoT server.

```
_dns.resolver.example.com.  7200  IN SVCB 1 resolver.example.com. (
     alpn=h2 dohpath=/dns-query{?dns} )
_dns.resolver.example.com.  7200  IN SVCB 2 resolver.example.com. (
     alpn=dot )
```

Clients MUST validate that for any Encrypted DNS Resolver discovered using a known resolver name, the TLS certificate of the resolver contains the known name in a subjectAltName extension. In the example above, this means that both servers need to have certificates that cover the name resolver.example.com. Often, the various supported encrypted DNS protocols will be specified such that the SVCB TargetName matches the known name, as is true in the example above. However, even when the TargetName is different (for example, if the DoH server had a TargetName of doh.example.com), the clients still check for the original known resolver name in the certificate.

Note that this resolver validation is not related to the DNS resolver that provided the SVCB answer.

As another example, being able to discover a Designated Resolver for a known Encrypted DNS Resolver is useful when a client has a DoT configuration for foo.resolver.example.com but is on a network that blocks DoT traffic. The client can still send a query to any other accessible resolver (either the local network resolver or an accessible DoH server) to discover if there is a designated DoH server for foo.resolver.example.com.

6. Deployment Considerations

Resolver deployments that support DDR are advised to consider the following points.

6.1. Caching Forwarders

A DNS forwarder SHOULD NOT forward queries for "resolver.arpa" (or any subdomains) upstream. This prevents a client from receiving an SVCB record that will fail to authenticate because the forwarder's IP address is not in the upstream resolver's Designated Resolver's TLS certificate SAN field. A DNS forwarder which already acts as a completely transparent forwarder MAY choose to forward these queries when the operator expects that this does not apply, either because the operator knows that the upstream resolver does have the forwarder's IP address in its TLS certificate's SAN field or that the operator expects clients to validate the connection via some future mechanism.

Operators who choose to forward queries for "resolver.arpa" upstream should note that client behavior is never guaranteed and use of DDR

by a resolver does not communicate a requirement for clients to use the SVCB record when it cannot be verified.

6.2. Certificate Management

Resolver owners that support Verified Discovery will need to list valid referring IP addresses in their TLS certificates. This may pose challenges for resolvers with a large number of referring IP addresses.

6.3. Server Name Handling

Clients MUST NOT use "resolver.arpa" as the server name either in the TLS Server Name Indication (SNI) ([RFC8446]) for DoT, DoQ, or DoH connections, or in the URI host for DoH requests.

When performing discovery using resolver IP addresses, clients MUST use the original IP address of the Unencrypted DNS Resolver as the URI host for DoH requests.

Note that since IP addresses are not supported by default in the TLS SNI, resolvers that support discovery using IP addresses will need to be configured to present the appropriate TLS certificate when no SNI is present for DoT, DoQ, and DoH.

6.4. Handling non-DDR queries for resolver.arpa

DNS resolvers that support DDR by responding to queries for _dns.resolver.arpa MUST treat resolver.arpa as a locally served zone per [RFC6303]. In practice, this means that resolvers SHOULD respond to queries of any type other than SVCB for _dns.resolver.arpa with NODATA and queries of any type for any domain name under resolver.arpa with NODATA.

6.5. Interaction with Network-Designated Resolvers

Discovery of network-designated resolvers (DNR, [I-D.ietf-add-dnr]) allows a network to provide designation of resolvers directly through DHCP [RFC2132] [RFC8415] and IPv6 Router Advertisement (RA) [RFC4861] options. When such indications are present, clients can suppress queries for "resolver.arpa" to the unencrypted DNS server indicated by the network over DHCP or RAs, and the DNR indications SHOULD take precedence over those discovered using "resolver.arpa" for the same resolver if there is a conflict, since DNR is considered a more reliable source.

The designated resolver information in DNR might not contain a full set of SvcParams needed to connect to an encrypted DNS resolver. In such a case, the client can use an SVCB query using a resolver name, as described in Section 5, to the authentication-domain-name (ADN).

7. Security Considerations

Since clients can receive DNS SVCB answers over unencrypted DNS, on-path attackers can prevent successful discovery by dropping SVCB queries or answers, and thus prevent clients from switching to use encrypted DNS. Clients should be aware that it might not be possible to distinguish between resolvers that do not have any Designated Resolver and such an active attack. To limit the impact of discovery queries being dropped either maliciously or unintentionally, clients can re-send their SVCB queries periodically.

Section 8.2 of [I-D.ietf-add-svcb-dns] describes a second downgrade attack where an attacker can block connections to the encrypted DNS server. For DDR, clients need to validate a Designated Resolver using a connection to the server before trusting it, so attackers that can block these connections can prevent clients from switching to use encrypted DNS.

Encrypted DNS Resolvers that allow discovery using DNS SVCB answers over unencrypted DNS MUST NOT provide differentiated behavior based solely on metadata in the SVCB record, such as the HTTP path or alternate port number, which are parameters that an attacker could modify. For example, if a DoH resolver provides a filtering service for one URI path, and a non-filtered service for another URI path, an attacker could select which of these services is used by modifying the "dohpath" parameter. These attacks can be mitigated by providing separate resolver IP addresses or hostnames.

While the IP address of the Unencrypted DNS Resolver is often provisioned over insecure mechanisms, it can also be provisioned securely, such as via manual configuration, a VPN, or on a network with protections like RA-Guard [RFC6105]. An attacker might try to direct Encrypted DNS traffic to itself by causing the client to think that a discovered Designated Resolver uses a different IP address from the Unencrypted DNS Resolver. Such a Designated Resolver might have a valid certificate, but be operated by an attacker that is trying to observe or modify user queries without the knowledge of the client or network.

If the IP address of a Designated Resolver differs from that of an Unencrypted DNS Resolver, clients applying Verified Discovery (Section 4.2) MUST validate that the IP address of the Unencrypted DNS Resolver is covered by the SubjectAlternativeName of the Designated Resolver's TLS certificate. If that validation fails, the client MUST NOT automatically use the discovered Designated Resolver.

Clients using Opportunistic Discovery (Section 4.3) MUST be limited to cases where the Unencrypted DNS Resolver and Designated Resolver

have the same IP address, which SHOULD be a private or local IP address. Clients which do not follow Opportunistic Discovery (Section 4.3) and instead try to connect without first checking for a designation run the possible risk of being intercepted by an attacker hosting an Encrypted DNS Resolver on an IP address of an Unencrypted DNS Resolver where the attacker has failed to gain control of the Unencrypted DNS Resolver.

The constraints on the use of Designated Resolvers specified here apply specifically to the automatic discovery mechanisms defined in this document, which are referred to as Verified Discovery and Opportunistic Discovery. Clients MAY use some other mechanism to verify and use Designated Resolvers discovered using the DNS SVCB record. However, use of such an alternate mechanism needs to take into account the attack scenarios detailed here.

8. IANA Considerations

8.1. Special Use Domain Name "resolver.arpa"

This document calls for the addition of "resolver.arpa" to the Special-Use Domain Names (SUDN) registry established by [RFC6761].

IANA is requested to add an entry in "Transport-Independent Locally-Served DNS Zones" registry for 'resolver.arpa.' with the description "DNS Resolver Special-Use Domain", listing this document as the reference.

8.2. Domain Name Reservation Considerations

In accordance with Section 5 of [RFC6761], the answers to the following questions are provided relative to this document:

1. Are human users expected to recognize these names as special and use them differently? In what way?

No. This name is used automatically by DNS stub resolvers running on client devices on behalf of users, and users will never see this name directly.

1. Are writers of application software expected to make their software recognize these names as special and treat them differently? In what way?

No. There is no use case where a non-DNS application (covered by the next question) would need to use this name.

1. Are writers of name resolution APIs and libraries expected to make their software recognize these names as special and treat them differently? If so, how?

Yes. DNS client implementors are expected to use this name when querying for a resolver's properties instead of records for the name itself. DNS servers are expected to respond to queries for this name with their own properties instead of checking the matching zone as it would for normal domain names.

1. Are developers of caching domain name servers expected to make their implementations recognize these names as special and treat them differently? If so, how?

Yes. Caching domain name servers should not forward queries for this name to avoid causing validation failures due to IP address mismatch.

1. Are developers of authoritative domain name servers expected to make their implementations recognize these names as special and treat them differently? If so, how?

No. DDR is designed for use by recursive resolvers. Theoretically, an authoritative server could choose to support this name if it wants to advertise support for encrypted DNS protocols over plain-text DNS, but that scenario is covered by other work in the IETF DNSOP working group.

1. Does this reserved Special-Use Domain Name have any potential impact on DNS server operators? If they try to configure their authoritative DNS server as authoritative for this reserved name, will compliant name server software reject it as invalid? Do DNS server operators need to know about that and understand why? Even if the name server software doesn't prevent them from using this reserved name, are there other ways that it may not work as expected, of which the DNS server operator should be aware?

This name is locally served, and any resolver which supports this name should never forward the query. DNS server operators should be aware that records for this name will be used by clients to modify the way they connect to their resolvers.

1. How should DNS Registries/Registrars treat requests to register this reserved domain name? Should such requests be denied? Should such requests be allowed, but only to a specially-designated entity?

IANA should hold the registration for this name. Non-IANA requests to register this name should always be denied by DNS Registries/ Registrars.

9. References

9.1. Normative References

[I-D.ietf-add-dnr] Boucadair, M., Reddy, T., Wing, D., Cook, N., and T. Jensen, "DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)", Work in Progress, Internet-Draft, draft-ietf-add-dnr-12, 24 July 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-add-dnr-12>.

[I-D.ietf-add-svcb-dns] Schwartz, B., "Service Binding Mapping for DNS Servers", Work in Progress, Internet-Draft, draft-ietf-add-svcb-dns-06, 5 July 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-add-svcb-dns-06>.

[I-D.ietf-dnsop-svcb-https] Schwartz, B., Bishop, M., and E. Nygren, "Service binding and parameter specification via the DNS (DNS SVCB and HTTPS RRs)", Work in Progress, Internet-Draft, draft-ietf-dnsop-svcb-https-10, 24 May 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-svcb-https-10>.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <https://www.rfc-editor.org/rfc/rfc1918>.

[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/rfc/rfc2119>.

[RFC3927] Cheshire, S., Aboba, B., and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses", RFC 3927, DOI 10.17487/RFC3927, May 2005, <https://www.rfc-editor.org/rfc/rfc3927>.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005, <https://www.rfc-editor.org/rfc/rfc4193>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/rfc/rfc4291>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation

List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/rfc/rfc5280>.

[RFC6303] Andrews, M., "Locally Served DNS Zones", BCP 163, RFC 6303, DOI 10.17487/RFC6303, July 2011, <https://www.rfc-editor.org/rfc/rfc6303>.

[RFC6761] Cheshire, S. and M. Krochmal, "Special-Use Domain Names", RFC 6761, DOI 10.17487/RFC6761, February 2013, <https://www.rfc-editor.org/rfc/rfc6761>.

[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/rfc/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/rfc/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/rfc/rfc8484>.

[RFC9250] Huitema, C., Dickinson, S., and A. Mankin, "DNS over Dedicated QUIC Connections", RFC 9250, DOI 10.17487/RFC9250, May 2022, <https://www.rfc-editor.org/rfc/rfc9250>.

9.2. Informative References

[I-D.ietf-tls-esni] Rescorla, E., Oku, K., Sullivan, N., and C. A. Wood, "TLS Encrypted Client Hello", Work in Progress, Internet-Draft, draft-ietf-tls-esni-14, 13 February 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-esni-14>.

[I-D.schinazi-httpbis-doh-preference-hints] Schinazi, D., Sullivan, N., and J. Kipp, "DoH Preference Hints for HTTP", Work in Progress, Internet-Draft, draft-schinazi-httpbis-doh-preference-hints-02, 13 July 2020, <https://datatracker.ietf.org/doc/html/draft-schinazi-httpbis-doh-preference-hints-02>.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, DOI 10.17487/RFC2132, March 1997, <https://www.rfc-editor.org/rfc/rfc2132>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861,

DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/rfc/rfc4861>.

[RFC6105] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., and J. Mohacsi, "IPv6 Router Advertisement Guard", RFC 6105, DOI 10.17487/RFC6105, February 2011, <https://www.rfc-editor.org/rfc/rfc6105>.

[RFC8106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 8106, DOI 10.17487/RFC8106, March 2017, <https://www.rfc-editor.org/rfc/rfc8106>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/rfc/rfc8415>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

[RFC8880] Cheshire, S. and D. Schinazi, "Special Use Domain Name 'ipv4only.arpa'", RFC 8880, DOI 10.17487/RFC8880, August 2020, <https://www.rfc-editor.org/rfc/rfc8880>.

Appendix A. Rationale for using a Special Use Domain Name

The "resolver.arpa" SUDN is similar to "ipv4only.arpa" in that the querying client is not interested in an answer from the authoritative "arpa" name servers. The intent of the SUDN is to allow clients to communicate with the Unencrypted DNS Resolver much like "ipv4only.arpa" allows for client-to-middlebox communication. For more context, see the rationale behind "ipv4only.arpa" in [RFC8880].

Appendix B. Rationale for using SVCB records

This mechanism uses SVCB/HTTPS resource records [I-D.ietf-dnsop-svcb-https] to communicate that a given domain designates a particular Designated Resolver for clients to use in place of an Unencrypted DNS Resolver (using a SUDN) or another Encrypted DNS Resolver (using its domain name).

There are various other proposals for how to provide similar functionality. There are several reasons that this mechanism has chosen SVCB records:

* Discovering encrypted DNS resolvers using DNS records keeps client logic for DNS self-contained and allows a DNS resolver operator to define which resolver names and IP addresses are related to one another.

* Using DNS records also does not rely on bootstrapping with higher-level application operations (such as [I-D.schinazi-httpbis-doh-preference-hints]).

* SVCB records are extensible and allow definition of parameter keys. This makes them a superior mechanism for extensibility as compared to approaches such as overloading TXT records. The same keys can be used for discovering Designated Resolvers of different transport types as well as those advertised by Unencrypted DNS Resolvers or another Encrypted DNS Resolver.

* Clients and servers that are interested in privacy of names will already need to support SVCB records in order to use Encrypted TLS Client Hello [I-D.ietf-tls-esni]. Without encrypting names in TLS, the value of encrypting DNS is reduced, so pairing the solutions provides the largest benefit.

Authors' Addresses

Tommy Pauly
Apple Inc.
One Apple Park Way
Cupertino, California 95014,
United States of America

Email: tpauly@apple.com

Eric Kinnear
Apple Inc.
One Apple Park Way
Cupertino, California 95014,
United States of America

Email: ekinnear@apple.com

Christopher A. Wood
Cloudflare
101 Townsend St
San Francisco,
United States of America

Email: caw@heapingbits.net

Patrick McManus
Fastly

Email: mcmanus@ducksong.com

Tommy Jensen
Microsoft

Email: tojens@microsoft.com