ADD
Internet-Draft
Intended status: Standards Track
Expires: 6 February 2023

T. Pauly
E. Kinnear
Apple Inc.
C. A. Wood
Cloudflare
P. McManus
Fastly
T. Jensen
Microsoft

5 August 2022

Discovery of Designated Resolvers
draft-ietf-add-ddr-10

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 6 February 2023.

Copyright Notice

Copyright (c) 2022 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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction 3
1.1. Specification of Requirements 4
2. Terminology 4
3. DNS Service Binding Records 4
4. Discovery Using Resolver IP Addresses 6
4.1. Use of Designated Resolvers 7
4.1.1. Use of Designated Resolvers across network changes . 8
4.2. Verified Discovery 8
4.3. Opportunistic Discovery 9
5. Discovery Using Resolver Names 10
6. Deployment Considerations 11
6.1. Caching Forwarders 11
6.2. Certificate Management 11
6.3. Server Name Handling 11
6.4. Handling non-DDR queries for resolver.arpa 12
6.5. Interaction with Network-Designated Resolvers 12
7. Security Considerations 12
8. IANA Considerations 13
8.1. Special Use Domain Name "resolver.arpa" 14
8.2. Domain Name Reservation Considerations 14

9. References 15
9.1. Normative References 15
9.2. Informative References 17
Appendix A. Rationale for using a Special Use Domain Name . . . 18
Appendix B. Rationale for using SVCB records 18
Authors' Addresses 19

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].

Responses to the SVCB query for the "resolver.arpa" SUDN describe Designated Resolvers. To ensure that different Designated Resolver configurations can be correctly distinguished and associated with A and AAAA records for the resolver, ServiceMode SVCB responses to these queries MUST NOT use the "." or "resolver.arpa" value for the TargetName. Similarly, clients MUST NOT perform A or 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.

2) 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.

3) 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.

4) 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.

5) 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.

6) 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.

7) 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

ADD
Internet-Draft
Intended status: Standards Track
Expires: 29 October 2023

M. Boucadair, Ed.
Orange
T. Reddy, Ed.
Nokia
D. Wing
Citrix
N. Cook
Open-Xchange
T. Jensen
Microsoft

27 April 2023

DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)
draft-ietf-add-dnr-16

Abstract

The document specifies new DHCP and IPv6 Router Advertisement options to discover encrypted DNS resolvers (e.g., DNS-over-HTTPS, DNS-over-TLS, DNS-over-QUIC). Particularly, it allows a host to learn an authentication domain name together with a list of IP addresses and a set of service parameters to reach such encrypted DNS resolvers.

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 29 October 2023.

Copyright Notice

Copyright (c) 2023 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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction 3
2. Terminology 3
3. Overview 4
3.1. Configuration Data for Encrypted DNS 4
3.1.1. ADN as the Reference Identifier for DNS Authentication 4
3.1.2. Avoiding Dependency on External Resolvers 5
3.1.3. Single vs. Multiple IP Addresses 5
3.1.4. Why Not Separate Options for ADN and IP Addresses? . 5
3.1.5. Service Parameters 6
3.1.6. ADN Only Mode 6
3.1.7. Encrypted DNS Options Ordering 7
3.1.8. DNR Validation Checks 7
3.1.9. DNR Information Using Other Provisioning Mechanisms 7
3.2. Handling Configuration Data Conflicts 8
3.3. Validating Discovered Resolvers 8
3.4. Multihoming Considerations 9
4. DHCPv6 Encrypted DNS Option 9
4.1. Option Format 9
4.2. DHCPv6 Client Behavior 12
5. DHCPv4 Encrypted DNS Option 12
5.1. Option Format 12
5.2. DHCPv4 Client Behavior 14
6. IPv6 RA Encrypted DNS Option 15
6.1. Option Format 15
6.2. IPv6 Host Behavior 17
7. Security Considerations 17
7.1. Spoofing Attacks 18
7.2. Deletion Attacks 18
7.3. Passive Attacks 19
7.4. Wireless Security – Authentication Attacks 19
8. Privacy Considerations 19
9. IANA Considerations 20
9.1. DHCPv6 Option 20
9.2. DHCPv4 Option 20
9.3. Neighbor Discovery Option 20

10. Acknowledgements 21
11. Contributing Authors 21
12. References 22
12.1. Normative References 22
12.2. Informative References 23
Authors' Addresses 26

1. Introduction

This document focuses on the discovery of encrypted DNS such as DNS-over-HTTPS (DoH) [RFC8484], DNS-over-TLS (DoT) [RFC7858], or DNS-over-QUIC (DoQ) [RFC9250] in local networks.

In particular, the document specifies how a local encrypted DNS resolver can be discovered by connected hosts by means of DHCPv4 [RFC2132], DHCPv6 [RFC8415], and IPv6 Router Advertisement (RA) [RFC4861] options. These options are designed to convey the following information: the DNS Authentication Domain Name (ADN), a list of IP addresses, and a set of service parameters. This procedure is called Discovery of Network-designated Resolvers (DNR).

The options defined in this document can be deployed in a variety of deployments (e.g., local networks with Customer Premises Equipment (CPEs) that may or may not be managed by an Internet Service Provider (ISP), or local networks with or without DNS forwarders). It is out of the scope of this document to provide an inventory of such deployments.

Resolver selection considerations are out of scope. Likewise, policies (including any interactions with users) are out of scope.

2. Terminology

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.

This document makes use of the terms defined in [RFC8499]. The following additional terms are used:

Authentication Domain Name (ADN): refers to a domain name that is used by a DNS client to authenticate a DNS resolver.

ADN-only mode: refers to a DNS discovery mode where only the ADN of the DNS resolver is retrieved. See Section 3.1.6.

Do53: refers to unencrypted DNS.

DNR: refers to the Discovery of Network-designated Resolvers procedure.

Encrypted DNS: refers to a scheme where DNS exchanges are transported over an encrypted channel. Examples of encrypted DNS are DoT, DoH, or DoQ.

Encrypted DNS resolver: refers to a DNS resolver that supports any encrypted DNS scheme.

Encrypted DNS options: refers to the options defined in Sections 4, 5, and 6.

DHCP: refers to both DHCPv4 and DHCPv6.

3. Overview

This document describes how a DNS client can discover local encrypted DNS resolvers using DHCP (Sections 4 and 5) and Neighbor Discovery protocol (Section 6): Encrypted DNS options.

These options configure an authentication domain name, a list of IP addresses, and a set of service parameters of the encrypted DNS resolver. More information about the design of these options is provided in the following subsections.

3.1. Configuration Data for Encrypted DNS

3.1.1. ADN as the Reference Identifier for DNS Authentication

In order to allow for a PKIX-based authentication of the encrypted DNS resolver to the DNS client, the Encrypted DNS options are designed to always include an authentication domain name. This ADN is presented as a reference identifier for DNS authentication purposes. This design accommodates the current best practices for issuing certificates as per Section 1.7.2 of [RFC6125]:

> Some certification authorities issue server certificates based on IP addresses, but preliminary evidence indicates that such certificates are a very small percentage (less than 1%) of issued certificates.

3.1.2. Avoiding Dependency on External Resolvers

To avoid adding a dependency on another server to resolve the ADN, the Encrypted DNS options return the IP address(es) to locate an encrypted DNS resolver. These encrypted DNS resolvers may be hosted on the same or distinct IP addresses. Such a decision is deployment specific.

In order to optimize the size of discovery messages when all DNS resolvers terminate on the same IP address, early versions of this document considered relying upon the discovery mechanisms specified in [RFC2132][RFC3646][RFC8106] to retrieve a list of IP addresses to reach their DNS resolvers. Nevertheless, this approach requires a client that supports more than one encrypted DNS protocol (e.g., DoH and DoT) to probe that list of IP addresses. To avoid such a probing, the options defined in Sections 4, 5, and 6 associate an encrypted DNS protocol with an IP address. No probing is required in such a design.

3.1.3. Single vs. Multiple IP Addresses

A list of IP addresses to reach an encrypted DNS resolver may be returned in an Encrypted DNS option to accommodate current deployments relying upon primary and backup resolvers. Also, DNR can be used in contexts where other DNS redundancy schemes (e.g., anycast as in BCP 126 [RFC4786]) are used.

Whether one or more IP addresses are returned in an Encrypted DNS option is deployment specific. For example, a router embedding a recursive server or a forwarder has to include one single IP address pointing to one of its LAN-facing interfaces. Typically, this IP address can be a private IPv4 address, a link-local address, a Unique Local IPv6 unicast Address (ULA), or a Global Unicast Address (GUA).

If multiple IP addresses are to be returned in an Encrypted DNS option, these addresses are ordered in the preference for use by the client.

3.1.4. Why Not Separate Options for ADN and IP Addresses?

A single option is used to convey both the ADN and IP addresses. Otherwise, a means to correlate an IP address conveyed in an option with an ADN conveyed in another option will be required if, for example, more than one ADN is supported by the network.

3.1.5. Service Parameters

Because distinct encrypted DNS protocols (e.g., DoT, DoH, and DoQ) may be provisioned by a network and that some of these protocols may make use of customized port numbers instead of default ones, the Encrypted DNS options are designed to return a set of service parameters. These parameters are encoded following the same rules for encoding SvcParams in Section 2.1 of [I-D.ietf-dnsop-svcb-https]. This encoding approach may increase the size of the options but it has the merit of relying upon an existing IANA registry and, thus, accommodating new encrypted DNS protocols and service parameters that may be defined in the future.

The following service parameters MUST be supported by a DNR implementation:

alpn: Used to indicate the set of supported protocols (Section 7.1 of [I-D.ietf-dnsop-svcb-https]).

port: Used to indicate the target port number for the encrypted DNS connection (Section 7.2 of [I-D.ietf-dnsop-svcb-https]).

In addition, the following service parameter is RECOMMENDED to be supported by a DNR implementation:

dohpath: Used to supply a relative DoH URI Template (Section 5.1 of [I-D.ietf-add-svcb-dns]).

3.1.6. ADN Only Mode

The provisioning mode in which an ADN, a list of IP addresses, and a set of service parameters of the encrypted DNS resolver are supplied to a host SHOULD be used because the Encrypted DNS options are self-contained and do not require any additional DNS queries. The reader may refer to [RFC7969] for an overview of advanced capabilities that are supported by DHCP servers to populate configuration data (e.g., issue DNS queries).

In contexts where putting additional complexity on requesting hosts is acceptable, returning an ADN only can be considered. The supplied ADN will be passed to a local resolution library (a DNS client, typically) which will then issue Service Binding (SVCB) queries [I-D.ietf-add-svcb-dns]. These SVCB queries can be sent to the discovered encrypted DNS resolver itself or to the network-designated Do53 resolver. Note that this mode may be subject to active attacks, which can be mitigated by DNSSEC.

> How an ADN is passed to a local resolution library is implementation specific.

3.1.7. Encrypted DNS Options Ordering

The DHCP options defined in Sections 4 and 5 follow the option ordering guidelines in Section 17 of [RFC7227].

Likewise, the RA option (Section 6) adheres to the recommendations in Section 9 of [RFC4861].

3.1.8. DNR Validation Checks

On receipt of an Encrypted DNS option, the DHCP client (or IPv6 host) makes the following validation checks:

* The ADN is present and encoded as per Section 10 of [RFC8415].

* If additional data is supplied:

  - the service parameters are encoded following the rules specified in Section 2.1 of [I-D.ietf-dnsop-svcb-https].

  - the option includes at least one valid IP address.

  - the service parameters do not include "ipv4hint" or "ipv6hint" service parameters.

If any of the checks fail, the receiver discards the received Encrypted DNS option.

3.1.9. DNR Information Using Other Provisioning Mechanisms

The provisioning mechanisms specified in this document may not be available in specific networks (e.g., some cellular networks exclusively use Protocol Configuration Options (PCOs) [TS.24008]) or may not be suitable in some contexts (e.g., need for a secure discovery). Other mechanisms may be considered in these contexts for the provisioning of encrypted DNS resolvers. It is RECOMMENDED that at least the following DNR information is made available to a requesting host:

* A service priority whenever the discovery mechanism does not rely on implicit ordering if multiple instances of the encrypted DNS are used.

* An authentication domain name. This parameter is mandatory.

* A list of IP addresses to locate the encrypted DNS resolver.

* A set of service parameters.

3.2. Handling Configuration Data Conflicts

If the encrypted DNS is discovered by a host using both RA and DHCP, the rules discussed in Section 5.3.1 of [RFC8106] MUST be followed.

DHCP/RA options to discover encrypted DNS resolvers (including, DoH URI Templates) takes precedence over Discovery of Designated Resolvers (DDR) [I-D.ietf-add-ddr] since DDR uses Do53 to an external DNS resolver, which is susceptible to both internal and external attacks whereas DHCP/RA is typically protected using the mechanisms discussed in Section 7.1.

If a client learns both Do53 and encrypted DNS resolvers from the same network, and absent explicit configuration otherwise, it is RECOMMENDED that the client uses the encrypted DNS resolvers for that network. If the client cannot establish an authenticated and encrypted connection with the encrypted DNS resolver, it may fall back to using the Do53 resolver.

3.3. Validating Discovered Resolvers

This section describes a set of validation checks to confirm that an encrypted DNS resolver matches what is provided using DNR (e.g., DHCP or RA). Such validation checks do not intend to validate the security of the DNR provisioning mechanisms or the user's trust relationship to the network.

If the local DNS client supports one of the discovered encrypted DNS protocols identified by Application Layer Protocol Negotiation (ALPN) protocol identifiers (or other service parameter that indicates some other protocol disambiguation mechanism), the DNS client establishes an encrypted DNS session following the service priority of the discovered encrypted resolvers.

The DNS client verifies the connection based on PKIX validation [RFC5280] of the DNS resolver certificate and uses the validation techniques as described in [RFC6125] to compare the authentication domain name conveyed in the Encrypted DNS options to the certificate provided (see Section 8.1 of [RFC8310] for more details). The DNS client uses the default system or application PKI trust anchors unless configured otherwise to use explicit trust anchors. ALPN-related considerations can be found in Section 6.1 of [I-D.ietf-dnsop-svcb-https]. Operation considerations to check the revocation status of the certificate of an encrypted DNS resolver are discussed in Section 10 of [RFC8484].

3.4. Multihoming Considerations

Devices may be connected to multiple networks; each providing their own DNS configuration using the discovery mechanisms specified in this document. Nevertheless, it is out of the scope of this specification to discuss DNS selection of multi-interface devices. Such considerations fall under the generic issue of handling multiple provisioning sources and which should not be dealt within each option separately as per the recommendation in Section 12 of [RFC7227].

The reader may refer to [RFC6731] for a discussion of DNS selection issues and an example of DNS resolver selection for multi-interfaced devices. Also, the reader may refer to [I-D.ietf-add-split-horizon-authority] for a discussion on how DNR and Provisioning Domains (PvDs) Key "dnsZones" (Section 4.3 of [RFC8801]) can be used in Split DNS environments (Section 6 of [RFC8499]).

4. DHCPv6 Encrypted DNS Option

4.1. Option Format

The format of the DHCPv6 Encrypted DNS option is shown in Figure 1.

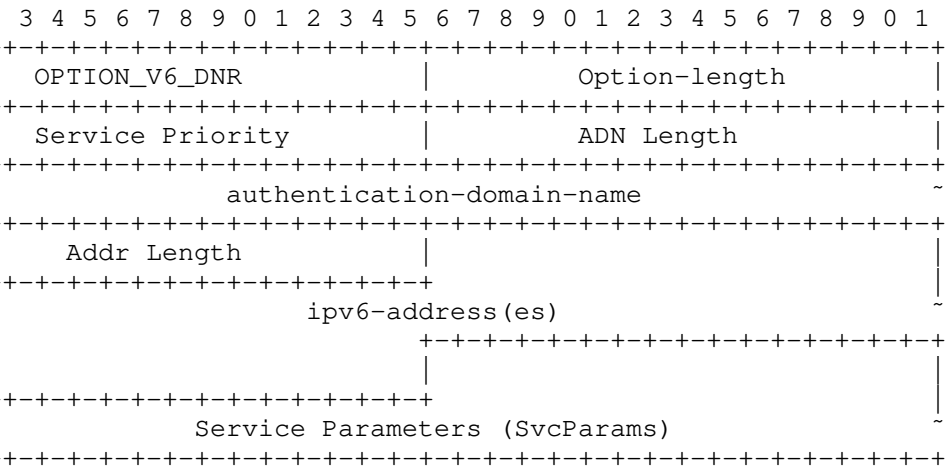

Figure 1: DHCPv6 Encrypted DNS Option

The fields of the option shown in Figure 1 are as follows:

Option-code: OPTION_V6_DNR (TBA1, see Section 9.1)

Option-length: Length of the enclosed data in octets. The option length is ('ADN Length' + 4) when only an ADN is included in the option.

Service Priority: The priority of this OPTION_V6_DNR instance compared to other instances. This 16-bit unsigned integer is interpreted following the rules specified in Section 2.4.1 of [I-D.ietf-dnsop-svcb-https].

ADN Length: Length of the authentication-domain-name field in octets.

authentication-domain-name (variable length): A fully qualified domain name of the encrypted DNS resolver. This field is formatted as specified in Section 10 of [RFC8415].

An example of the authentication-domain-name encoding is shown in Figure 2. This example conveys the FQDN "doh1.example.com.", and the resulting Option-length field is 18.

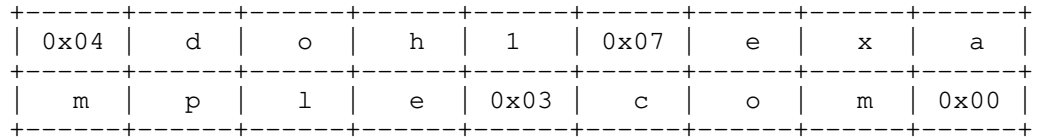

Figure 2: An Example of the DNS authentication-domain-name Encoding

Addr Length: Length of enclosed IPv6 addresses in octets. When present, it MUST be a multiple of 16.

ipv6-address(es) (variable length): Indicates one or more IPv6 addresses to reach the encrypted DNS resolver. An address can be link-local, ULA, or GUA. The format of this field is shown in Figure 3.

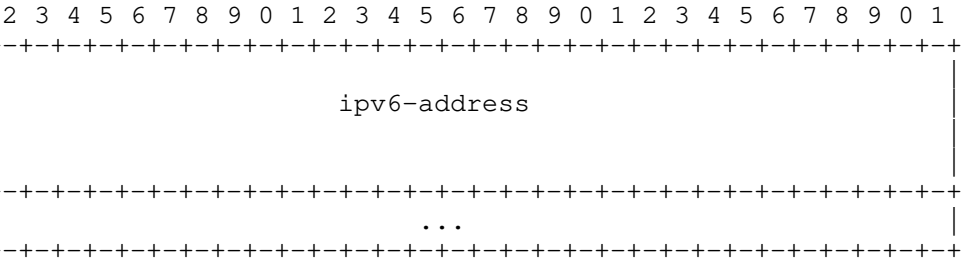

Figure 3: Format of the IPv6 Addresses Field

Service Parameters (SvcParams) (variable length): Specifies a set of service parameters that are encoded following the rules in Section 2.1 of [I-D.ietf-dnsop-svcb-https]. Service parameters may include, for example, a list of ALPN protocol identifiers or alternate port numbers. This field SHOULD include at least "alpn" SvcParam. The "alpn" SvcParam may not be required in contexts such as a variant of DNS over CoAP where messages are encrypted using Object Security for Constrained RESTful Environments (OSCORE) [RFC8613]. The service parameters MUST NOT include "ipv4hint" or "ipv6hint" SvcParams as they are superseded by the included IP addresses.

If no port service parameter is included, this indicates that default port numbers should be used. As a reminder, the default port number is 853 for DoT, 443 for DoH, and 853 for DoQ.

The length of this field is ('Option-length' - 6 - 'ADN Length' - 'Addr Length').

Note that "Addr Length", "ipv6-address(es)", and "Service Parameters (SvcParams)" fields are not present if the ADN-only mode is used (Section 3.1.6).

4.2. DHCPv6 Client Behavior

To discover an encrypted DNS resolver, the DHCPv6 client MUST include OPTION_V6_DNR in an Option Request Option (ORO), as in Sections 18.2.1, 18.2.2, 18.2.4, 18.2.5, 18.2.6, and 21.7 of [RFC8415].

The DHCPv6 client MUST be prepared to receive multiple instances of the OPTION_V6_DNR option; each option is to be treated as a separate encrypted DNS resolver. These instances MUST be processed following their service priority (i.e., smaller service priority indicates a higher preference).

The DHCPv6 client MUST silently discard any OPTION_V6_DNR that fails to pass the validation steps defined in Section 3.1.8.

The DHCPv6 client MUST silently discard multicast and host loopback addresses conveyed in OPTION_V6_DNR.

5. DHCPv4 Encrypted DNS Option

5.1. Option Format

The format of the DHCPv4 Encrypted DNS option is illustrated in Figure 4.

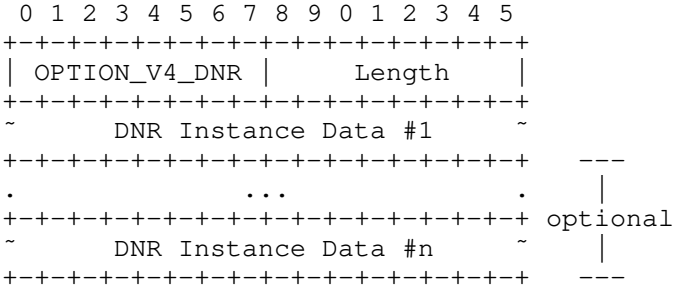

Figure 4: DHCPv4 Encrypted DNS Option

The fields of the option shown in Figure 4 are as follows:

Code: OPTION_V4_DNR (TBA2, see Section 9.2).

Length: Indicates the length of the enclosed data in octets.

DNR Instance Data: Includes the configuration data of an encrypted DNS resolver. The format of this field is shown in Figure 5.

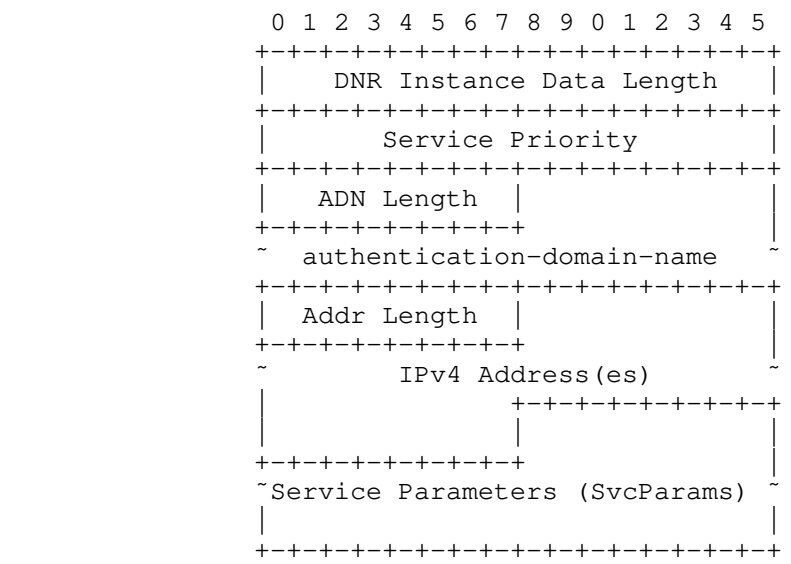

Figure 5: DNR Instance Data Format

When several encrypted DNS resolvers are to be included, the "DNR Instance Data" field is repeated.

The fields shown in Figure 5 are as follows:

DNR Instance Data Length: Length of all following data in octets. This field is set to ('ADN Length' + 3) when only an ADN is provided for a DNR instance.

Service Priority: The priority of this instance compared to other DNR instances. This 16-bit unsigned integer is interpreted following the rules specified in Section 2.4.1 of [I-D.ietf-dnsop-svcb-https].

ADN Length: Length of the authentication-domain-name in octets.

authentication-domain-name (variable length): The authentication domain name of the encrypted DNS resolver. This field is formatted as specified in Section 10 of [RFC8415]. An example is provided in Figure 2.

Addr Length: Length of included IPv4 addresses in octets. When present, it MUST be a multiple of 4.

IPv4 Address(es) (variable length): Indicates one or more IPv4

addresses to reach the encrypted DNS resolver. Both private and public IPv4 addresses can be included in this field. The format of this field is shown in Figure 6. This format assumes that an IPv4 address is encoded as a1.a2.a3.a4.

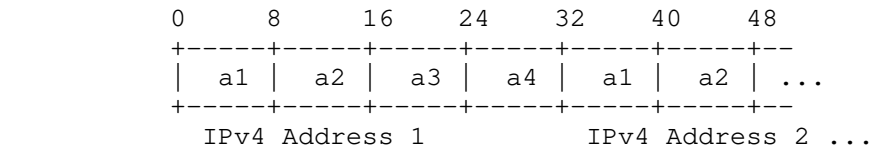

Figure 6: Format of the IPv4 Addresses Field

Service Parameters (SvcParams) (variable length): Specifies a set of service parameters that are encoded following the rules in Section 2.1 of [I-D.ietf-dnsop-svcb-https]. Service parameters may include, for example, a list of ALPN protocol identifiers or alternate port numbers. This field SHOULD include at least "alpn" SvcParam. The "alpn" SvcParam may not be required in contexts such as a variant of DNS over CoAP where messages are encrypted using OSCORE. The service parameters MUST NOT include "ipv4hint" or "ipv6hint" SvcParams as they are superseded by the included IP addresses.

If no port service parameter is included, this indicates that default port numbers should be used.

The length of this field is ('DNR Instance Data Length' - 4 - 'ADN Length' - 'Addr Length').

Note that "Addr Length", "IPv4 Address(es)", and "Service Parameters (SvcParams)" fields are not present if the ADN-only mode is used (Section 3.1.6).

OPTION_V4_DNR is a concatenation-requiring option. As such, the mechanism specified in [RFC3396] MUST be used if OPTION_V4_DNR exceeds the maximum DHCPv4 option size of 255 octets.

5.2. DHCPv4 Client Behavior

To discover an encrypted DNS resolver, the DHCPv4 client requests the encrypted DNS resolver by including OPTION_V4_DNR in a Parameter Request List option [RFC2132].

The DHCPv4 client MUST be prepared to receive multiple DNR instance data in the OPTION_V4_DNR option; each instance is to be treated as a separate encrypted DNS resolver. These instances MUST be processed following their service priority (i.e., smaller service priority indicates a higher preference).

The DHCPv4 client MUST silently discard any OPTION_V4_DNR that fails to pass the validation steps defined in Section 3.1.8.

The DHCPv4 client MUST silently discard multicast and host loopback addresses conveyed in OPTION_V4_DNR.

6. IPv6 RA Encrypted DNS Option

6.1. Option Format

This section defines a new Neighbor Discovery option [RFC4861]: IPv6 RA Encrypted DNS option. This option is useful in contexts similar to those discussed in Section 1.1 of [RFC8106].

The format of the IPv6 RA Encrypted DNS option is illustrated in Figure 7.

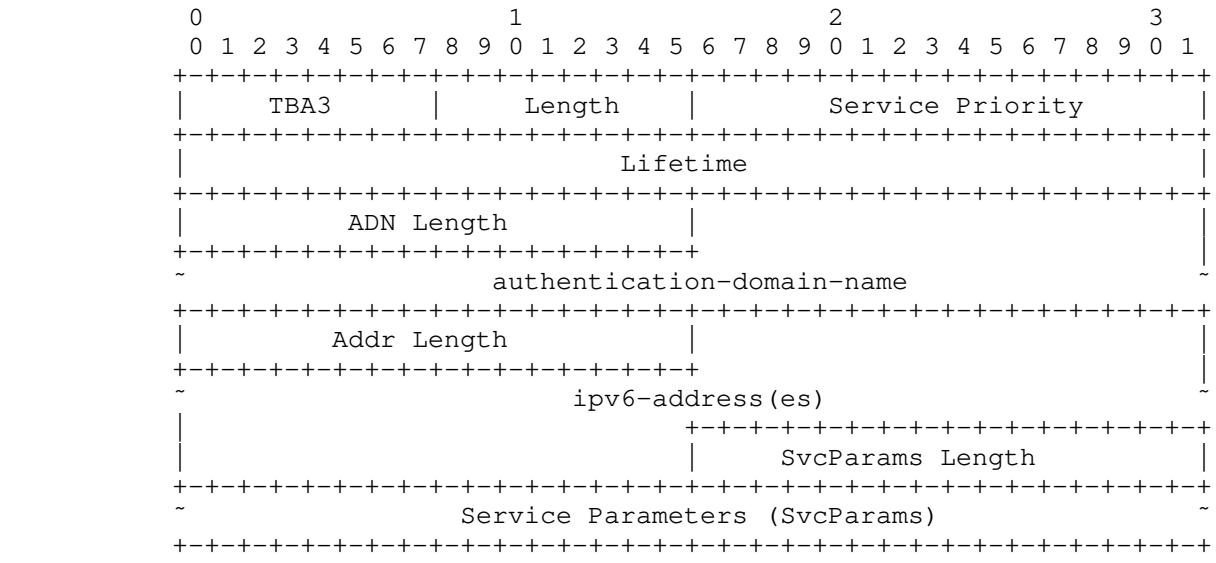

Figure 7: RA Encrypted DNS Option

The fields of the option shown in Figure 7 are as follows:

Type: 8-bit identifier of the Encrypted DNS option as assigned by IANA (TBA3, see Section 9.3).

Length: 8-bit unsigned integer. The length of the option (including the Type and Length fields) is in units of 8 octets.

Service Priority: 16-bit unsigned integer. The priority of this Encrypted DNS option instance compared to other instances. This field is interpreted following the rules specified in Section 2.4.1 of [I-D.ietf-dnsop-svcb-https].

Lifetime: 32-bit unsigned integer. The maximum time in seconds (relative to the time the packet is received) over which the discovered Authentication Domain Name is valid.

The value of Lifetime SHOULD by default be at least 3 * MaxRtrAdvInterval, where MaxRtrAdvInterval is the maximum RA interval as defined in [RFC4861].

A value of all one bits (0xffffffff) represents infinity.

A value of zero means that this Authentication Domain Name MUST no longer be used.

ADN Length: 16-bit unsigned integer. This field indicates the length of the authentication-domain-name field in octets.

authentication-domain-name (variable length): The authentication domain name of the encrypted DNS resolver. This field is formatted as specified in Section 10 of [RFC8415].

Addr Length: 16-bit unsigned integer. This field indicates the length of enclosed IPv6 addresses in octets. When present, it MUST be a multiple of 16.

ipv6-address(es) (variable length): One or more IPv6 addresses of the encrypted DNS resolver. An address can be link-local, ULA, or GUA.

All of the addresses share the same Lifetime value. Similar to [RFC8106], if it is desirable to have different Lifetime values per IP address, multiple Encrypted DNS options may be used.

The format of this field is shown in Figure 3.

SvcParams Length: 16-bit unsigned integer. This field indicates the length of the Service Parameters field in octets.

Service Parameters (SvcParams) (variable length): Specifies a set of service parameters that are encoded following the rules in Section 2.1 of [I-D.ietf-dnsop-svcb-https]. Service parameters may include, for example, a list of ALPN protocol identifiers or alternate port numbers. This field SHOULD include at least "alpn" SvcParam. The "alpn" SvcParam may not be required in contexts such as a variant of DNS over CoAP where messages are encrypted using OSCORE. The service parameters MUST NOT include "ipv4hint" or "ipv6hint" SvcParams as they are superseded by the included IP addresses.

If no port service parameter is included, this indicates that default port numbers should be used.

Note that "Addr Length", "ipv6-address(es)", and "Service Parameters (SvcParams)" fields are not present if the ADN-only mode is used (Section 3.1.6).

The option MUST be padded with zeros so that the full enclosed data is a multiple of 8 octets (Section 4.6 of [RFC4861]).

6.2. IPv6 Host Behavior

The procedure for DNS configuration is the same as it is with any other Neighbor Discovery option [RFC4861]. In addition, the host follows the same procedure as the one described in Section 5.3.1 of [RFC8106] for processing received Encrypted DNS options with the formatting requirements in Section 6.1 and validation checks in Section 3.1.8 substituted for the length and fields validation.

The host MUST be prepared to receive multiple Encrypted DNS options in RAs. These instances MUST be processed following their service priority (i.e., smaller service priority indicates a higher preference).

The host MUST silently discard multicast and host loopback addresses conveyed in the Encrypted DNS options.

7. Security Considerations

7.1. Spoofing Attacks

DHCP/RA messages are not encrypted or protected against modification within the LAN. Unless mitigated (described below), the content of DHCP and RA messages can be spoofed or modified by active attackers, such as compromised devices within the local network. An active attacker (Section 3.3 of [RFC3552]) can spoof the DHCP/RA response to provide the attacker's encrypted DNS resolver. Note that such an attacker can launch other attacks as discussed in Section 22 of [RFC8415]. The attacker can get a domain name with a domain-validated public certificate from a CA and host an encrypted DNS resolver.

Attacks of spoofed or modified DHCP responses and RA messages by attackers within the local network may be mitigated by making use of the following mechanisms:

* DHCPv6-Shield [RFC7610]: the network access node (e.g., a border router, a CPE, an Access Point (AP)) discards DHCP response messages received from any local endpoint.

* RA-Guard [RFC7113]: the network access node discards RAs messages received from any local endpoint.

* Source Address Validation Improvement (SAVI) solution for DHCP [RFC7513]: the network access node filters packets with forged source IP addresses.

The above mechanisms would ensure that the endpoint receives the correct configuration information of the encrypted DNS resolvers selected by the DHCP server (or RA sender), but cannot provide any information about the DHCP server or the entity hosting the DHCP server (or RA sender).

Encrypted DNS sessions with rogue resolvers that spoof the IP address of a DNS resolver will fail because the DNS client will fail to authenticate that rogue resolver based upon PKIX authentication [RFC6125], particularly the authentication domain name in the Encrypted DNS Option. DNS clients that ignore authentication failures and accept spoofed certificates will be subject to attacks (e.g., redirect to malicious resolvers, intercept sensitive data).

7.2. Deletion Attacks

If the DHCP responses or RAs are dropped by the attacker, the client can fall back to use a preconfigured encrypted DNS resolver. However, the use of policies to select resolvers is out of the scope of this document.

Note that deletion attack is not specific to DHCP/RA.

7.3. Passive Attacks

A passive attacker (Section 3.2 of [RFC3552]) can identify a host is using DHCP/RA to discover an encrypted DNS resolver and can infer that host is capable of using DoH/DoT/DoQ to encrypt DNS messages. However, a passive attacker cannot spoof or modify DHCP/RA messages.

7.4. Wireless Security - Authentication Attacks

Wireless LAN (WLAN) as frequently deployed in local networks (e.g., home networks) is vulnerable to various attacks (e.g., [Evil-Twin], [Krack], [Dragonblood]). Because of these attacks, only cryptographically authenticated communications are trusted on WLANs. This means that any information (e.g., NTP server, DNS resolver, domain search list) provided by such networks via DHCP, DHCPv6, or RA is untrusted because DHCP and RA messages are not authenticated.

If the pre-shared key (PSK) is the same for all clients that connect to the same WLAN (e.g., WPA-PSK), the shared key will be available to all nodes, including attackers. As such, it is possible to mount an active on-path attack. On-path attacks are possible within local networks because such a WLAN authentication lacks peer entity authentication.

This leads to the need for provisioning unique credentials for different clients. Endpoints can be provisioned with unique credentials (username and password, typically) provided by the local network administrator to mutually authenticate to the local WLAN AP (e.g., 802.1x Wireless User Authentication on OpenWRT [dot1x], EAP-pwd [RFC8146]). Not all endpoint devices (e.g., IoT devices) support 802.1x supplicant and need an alternate mechanism to connect to the local network. To address this limitation, unique pre-shared keys can be created for each such devices and WPA-PSK is used (e.g., [IPSK]).

8. Privacy Considerations

Privacy considerations that are specific to DNR provisioning mechanisms are discussed in Section 23 of [RFC8415] or [RFC7824]. Anonymity profiles for DHCP clients are discussed in [RFC7844]. The mechanism defined in this document can be used to infer that a DHCP client or IPv6 host support encrypted DNS options, but does not explicitly reveal whether local DNS clients are able to consume these options or infer their encryption capabilities. Other than that, this document does not expose more privacy information compared to Do53 discovery options.

As discussed in [RFC9076], the use of encrypted DNS does not reduce the data available in the DNS resolver. For example, the reader may refer to Section 8 of [RFC8484] or Section 7 of [RFC9250] for a discussion on specific privacy considerations to encrypted DNS.

9. IANA Considerations

9.1. DHCPv6 Option

IANA is requested to assign the following new DHCPv6 Option Code in the registry maintained in [DHCPV6].

Value	Description	Client ORO	Singleton Option	Reference
TBA1	OPTION_V6_DNR	Yes	No	[ThisDocument]

Table 1: DHCPv6 Encrypted DNS Option

9.2. DHCPv4 Option

IANA is requested to assign the following new DHCP Option Code in the registry maintained in [BOOTP].

Tag	Name	Data Length	Meaning	Reference
TBA2	OPTION_V4_DNR	N	Encrypted DNS Server	[ThisDocument]

Table 2: DHCPv4 Encrypted DNS Option

9.3. Neighbor Discovery Option

IANA is requested to assign the following new IPv6 Neighbor Discovery Option type in the "IPv6 Neighbor Discovery Option Formats" sub-registry under the "Internet Control Message Protocol version 6 (ICMPv6) Parameters" registry maintained in [ND].

Type	Description	Reference
TBA3	Encrypted DNS Option	[ThisDocument]

Table 3: Neighbor Discovery Encrypted DNS Option

10. Acknowledgements

Many thanks to Christian Jacquenet and Michael Richardson for the review.

Thanks to Stephen Farrell, Martin Thomson, Vittorio Bertola, Stephane Bortzmeyer, Ben Schwartz, Iain Sharp, and Chris Box for the comments.

Thanks to Mark Nottingham for the feedback on HTTP redirection that was discussed in previous versions of this specification.

The use of DHCP to retrieve an authentication domain name was discussed in Section 7.3.1 of [RFC8310] and in an Internet-Draft authored by Tom Pusateri and Willem Toorop [I-D.pusateri-dhc-dns-driu].

Thanks to Bernie Volz for the review of the DHCP part.

Christian Amsuess reported a case where ALPN service parameter cannot be used.

Thanks to Andrew Campling for the Shepherd review and Eric Vyncke for the AD review.

Thanks to Rich Salz for the secdir reviews, Joe Clarke for the ops-dir review, Robert Sparks for the artart review, and David Blacka for the dnsdir review.

Thanks to Lars Eggert, Roman Danyliw, Erik Kline, Martin Duke, Robert Wilton, Paul Wouters, and Zaheduzzaman Sarker for the IESG review.

11. Contributing Authors

Nicolai Leymann
Deutsche Telekom
Germany
Email: n.leymann@telekom.de

Zhiwei Yan
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing
100190
China
Email: yan@cnnic.cn

12. References

12.1. Normative References

[I-D.ietf-add-svcb-dns]
Schwartz, B. M., "Service Binding Mapping for DNS Servers", Work in Progress, Internet-Draft, draft-ietf-add-svcb-dns-08, 14 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-add-svcb-dns-08>.

[I-D.ietf-dnsop-svcb-https]
Schwartz, B. M., 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-12, 11 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-svcb-https-12>.

[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>.

[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/info/rfc2132>.

[RFC3396] Lemon, T. and S. Cheshire, "Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)", RFC 3396, DOI 10.17487/RFC3396, November 2002, <https://www.rfc-editor.org/info/rfc3396>.

[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/info/rfc4861>.

[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/info/rfc8106>.

[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>.

[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/info/rfc8415>.

12.2. Informative References

[BOOTP] "BOOTP Vendor Extensions and DHCP Options", <https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml#options>.

[DHCPV6] "DHCPv6 Option Codes", <https://www.iana.org/assignments/dhcpv6-parameters/dhcpv6-parameters.xhtml#dhcpv6-parameters-2>.

[dot1x] Cisco, "Basic 802.1x Wireless User Authentication", <https://openwrt.org/docs/guide-user/network/wifi/wireless.security.8021x>.

[Dragonblood] The Unicode Consortium, "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd", <https://papers.mathyvanhoef.com/dragonblood.pdf>.

[Evil-Twin] The Unicode Consortium, "Evil twin (wireless networks)", <https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks)>.

[I-D.ietf-add-ddr] Pauly, T., Kinnear, E., Wood, C. A., McManus, P., and T. Jensen, "Discovery of Designated Resolvers", Work in Progress, Internet-Draft, draft-ietf-add-ddr-10, 5 August 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-add-ddr-10>.

[I-D.ietf-add-split-horizon-authority]
Reddy.K, T., Wing, D., Smith, K., and B. M. Schwartz, "Establishing Local DNS Authority in Validated Split-Horizon Environments", Work in Progress, Internet-Draft, draft-ietf-add-split-horizon-authority-04, 8 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-add-split-horizon-authority-04>.

[I-D.pusateri-dhc-dns-driu]
Pusateri, T. and W. Toorop, "DHCPv6 Options for private DNS Discovery", Work in Progress, Internet-Draft, draft-pusateri-dhc-dns-driu-00, 2 July 2018, <https://datatracker.ietf.org/doc/html/draft-pusateri-dhc-dns-driu-00>.

[IPSK] Cisco, "Identity PSK Feature Deployment Guide", <https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-5/b_Identity_PSK_Feature_Deployment_Guide.html>.

[Krack] The Unicode Consortium, "Key Reinstallation Attacks", 2017, <https://www.krackattacks.com/>.

[ND] "IPv6 Neighbor Discovery Option Formats", <https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml#icmpv6-parameters-5>.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <https://www.rfc-editor.org/info/rfc3552>.

[RFC3646] Droms, R., Ed., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, DOI 10.17487/RFC3646, December 2003, <https://www.rfc-editor.org/info/rfc3646>.

[RFC4786] Abley, J. and K. Lindqvist, "Operation of Anycast Services", BCP 126, RFC 4786, DOI 10.17487/RFC4786, December 2006, <https://www.rfc-editor.org/info/rfc4786>.

[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/info/rfc5280>.

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, DOI 10.17487/RFC6125, March 2011, <https://www.rfc-editor.org/info/rfc6125>.

[RFC6731] Savolainen, T., Kato, J., and T. Lemon, "Improved Recursive DNS Server Selection for Multi-Interfaced Nodes", RFC 6731, DOI 10.17487/RFC6731, December 2012, <https://www.rfc-editor.org/info/rfc6731>.

[RFC7113] Gont, F., "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)", RFC 7113, DOI 10.17487/RFC7113, February 2014, <https://www.rfc-editor.org/info/rfc7113>.

[RFC7227] Hankins, D., Mrugalski, T., Siodelski, M., Jiang, S., and S. Krishnan, "Guidelines for Creating New DHCPv6 Options", BCP 187, RFC 7227, DOI 10.17487/RFC7227, May 2014, <https://www.rfc-editor.org/info/rfc7227>.

[RFC7513] Bi, J., Wu, J., Yao, G., and F. Baker, "Source Address Validation Improvement (SAVI) Solution for DHCP", RFC 7513, DOI 10.17487/RFC7513, May 2015, <https://www.rfc-editor.org/info/rfc7513>.

[RFC7610] Gont, F., Liu, W., and G. Van de Velde, "DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers", BCP 199, RFC 7610, DOI 10.17487/RFC7610, August 2015, <https://www.rfc-editor.org/info/rfc7610>.

[RFC7824] Krishnan, S., Mrugalski, T., and S. Jiang, "Privacy Considerations for DHCPv6", RFC 7824, DOI 10.17487/RFC7824, May 2016, <https://www.rfc-editor.org/info/rfc7824>.

[RFC7844] Huitema, C., Mrugalski, T., and S. Krishnan, "Anonymity Profiles for DHCP Clients", RFC 7844, DOI 10.17487/RFC7844, May 2016, <https://www.rfc-editor.org/info/rfc7844>.

[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>.

[RFC7969] Lemon, T. and T. Mrugalski, "Customizing DHCP Configuration on the Basis of Network Topology", RFC 7969, DOI 10.17487/RFC7969, October 2016, <https://www.rfc-editor.org/info/rfc7969>.

[RFC8146] Harkins, D., "Adding Support for Salted Password Databases to EAP-pwd", RFC 8146, DOI 10.17487/RFC8146, April 2017, <https://www.rfc-editor.org/info/rfc8146>.

[RFC8310] Dickinson, S., Gillmor, D., and T. Reddy, "Usage Profiles for DNS over TLS and DNS over DTLS", RFC 8310, DOI 10.17487/RFC8310, March 2018, <https://www.rfc-editor.org/info/rfc8310>.

[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>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

[RFC8613] Selander, G., Mattsson, J., Palombini, F., and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)", RFC 8613, DOI 10.17487/RFC8613, July 2019, <https://www.rfc-editor.org/info/rfc8613>.

[RFC8801] Pfister, P., Vyncke, É., Pauly, T., Schinazi, D., and W. Shao, "Discovering Provisioning Domain Names and Data", RFC 8801, DOI 10.17487/RFC8801, July 2020, <https://www.rfc-editor.org/info/rfc8801>.

[RFC9076] Wicinski, T., Ed., "DNS Privacy Considerations", RFC 9076, DOI 10.17487/RFC9076, July 2021, <https://www.rfc-editor.org/info/rfc9076>.

[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/info/rfc9250>.

[TS.24008] 3GPP, "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (Release 16)", December 2019, <https://www.3gpp.org/DynaReport/24008.htm>.

Authors' Addresses

Mohamed Boucadair (editor)
Orange
35000 Rennes
France
Email: mohamed.boucadair@orange.com

Tirumaleswar Reddy (editor)
Nokia
India
Email: kondtir@gmail.com

Dan Wing
Citrix Systems, Inc.
United States of America
Email: dwing-ietf@fuggles.com

Neil Cook
Open-Xchange
United Kingdom
Email: neil.cook@noware.co.uk

Tommy Jensen
Microsoft
United States of America
Email: tojens@microsoft.com