

ADD
Internet-Draft
Intended status: Standards Track
Expires: 6 October 2022

T. Pauly
E. Kinnear
Apple Inc.
C. A. Wood
Cloudflare
P. McManus
Fastly
T. Jensen
Microsoft
4 April 2022

Discovery of Designated Resolvers
draft-ietf-add-ddr-06

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. 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 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 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 October 2022.

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	3
2. Terminology	3
3. DNS Service Binding Records	4
4. Discovery Using Resolver IP Addresses	5
4.1. Use of Designated Resolvers	6
4.2. Verified Discovery	7
4.3. Opportunistic Discovery	8
5. Discovery Using Resolver Names	8
6. Deployment Considerations	9
6.1. Caching Forwarders	9
6.2. Certificate Management	10
6.3. Server Name Handling	10
6.4. Handling non-DDR queries for resolver.arpa	10
6.5. Interaction with Network-Designated Resolvers	10
7. Security Considerations	11
8. IANA Considerations	11
8.1. Special Use Domain Name "resolver.arpa"	12
9. References	12
9.1. Normative References	12
9.2. Informative References	13
Appendix A. Rationale for using SVCB records	15
Authors' Addresses	15

1. Introduction

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

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

1. When only an IP address of an Unencrypted Resolver is known, the client queries a special use domain name (SUDN) [RFC6761] to discover DNS SVCB records associated with one or more Encrypted Resolvers the Unencrypted Resolver has designated for use when support for DNS encryption is requested (Section 4).
2. When the hostname of an Encrypted 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 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 claims ownership over 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 Resolver, designated by another resolver for use in its own place. This designation can be verified with TLS certificates.

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

Unencrypted Resolver: A DNS resolver using 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 )
```

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. The client can still use others 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 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, Designated Resolvers SHOULD follow the guidance in Section 10 of [RFC8484] regarding the avoidance of DNS-based references that block the completion of the TLS handshake.

This document focuses on discovering DoH and DoT Designated Resolvers. Other protocols can also use the format defined by [I-D.ietf-add-svcb-dns]. However, if any 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 Resolver IP address, it SHOULD query the resolver for SVCB records for "dns://resolver.arpa" before making other queries. 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 or used to construct the DoH template MUST be provided.

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 )
```

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 "dns://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 allow the DNS client to make queries over an encrypted connection without waiting to resolve the Encrypted Resolver name per [I-D.ietf-dnsop-svcb-https]. If no A/AAAA records or SVCB IP address hints are included, clients will be forced to delay use of the Encrypted Resolver until an additional DNS lookup for the A and AAAA records can be made to the Unencrypted Resolver (or some other resolver the DNS client has been configured to use).

If the recursive resolver that receives this query has no Designated Resolvers, it SHOULD return NODATA for queries to the "resolver.arpa" SUDN.

4.1. Use of Designated Resolvers

When a client discovers Designated Resolvers from an Unencrypted 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 is accessed using a non-public IP 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 SHOULD NOT automatically use a Designated Resolver without some sort of validation, such as the two methods defined in this document or a future mechanism.

A client MUST NOT use a Designated Resolver designated by one Unencrypted Resolver in place of another Unencrypted Resolver. As these are known only by IP address, this means each unique IP address used for unencrypted DNS requires its own designation discovery. This ensures queries are being sent to a party designated by the resolver originally being used.

Generally, clients also SHOULD NOT reuse the Designated Resolver discovered from an Unencrypted Resolver over one network connection in place of the same Unencrypted Resolver on another network connection. Instead, clients SHOULD repeat the discovery process on the other network connection.

However, if a given Unencrypted Resolver designates a Designated Resolver that uses a public IP address and can be verified using the mechanism described in Section 4.2, it MAY be used on different network connections so long as the subsequent connections over other networks can also be successfully verified using the mechanism described in Section 4.2. This is a tradeoff between performance (by having no delay in establishing an encrypted DNS connection on the new network) and functionality (if the Unencrypted Resolver intends to designate different Designated Resolvers based on the network from which clients connect).

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 MUST contain the IP address of the designating Unencrypted Resolver in a subjectAltName extension. If the certificate can be validated, the client SHOULD use the discovered Designated Resolver for any cases in which it would have otherwise used the Unencrypted Resolver. If the Designated Resolver has a different IP address than the Unencrypted Resolver and the TLS certificate does not cover the Unencrypted Resolver address, the client MUST NOT automatically use the discovered Designated Resolver. Additionally, the client SHOULD suppress any further queries for Designated Resolvers using this Unencrypted Resolver for the length of time indicated by the SVCB record's Time to Live (TTL).

If the Designated Resolver and the Unencrypted Resolver share an IP address, clients MAY choose to opportunistically use the Designated Resolver even without this certificate check (Section 4.3).

If resolving the name of a Designated Resolver from an SVCB record yields an IP address that was not presented in the Additional Answers section or ipv4hint or ipv6hint fields of the original SVCB query, the connection made to that IP address MUST pass the same TLS certificate checks before being allowed to replace a previously known and validated IP address for the same Designated Resolver name.

4.3. Opportunistic Discovery

There are situations where Verified Discovery of encrypted DNS configuration over unencrypted DNS is not possible. This includes Unencrypted Resolvers on non-public IP addresses such as those defined in [RFC1918] whose identity cannot be confirmed using TLS certificates.

Opportunistic Privacy 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. A client MAY use information from the SVCB record for "dns://resolver.arpa" with this "opportunistic" approach (not validating the names presented in the SubjectAlternativeName field of the certificate) as long as the IP address of the Encrypted Resolver does not differ from the IP address of the Unencrypted Resolver. Clients SHOULD use this mode only for resolvers using non-public IP addresses. This approach can be used for any encrypted DNS protocol that uses TLS.

5. Discovery Using Resolver Names

A DNS client that already knows the name of an Encrypted 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 Resolver, or if a network provisioning protocol (such as DHCP or IPv6 Router Advertisements) provides a name for an Encrypted Resolver alongside the resolver IP address.

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 Resolver itself or to any other resolver. Unlike the case of bootstrapping from an Unencrypted Resolver (Section 4), these records SHOULD be available in the public DNS.

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 1 resolver.example.com. (
  alpn=dot )
```


Clients MUST validate that for any Encrypted 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 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" 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 blind forwarder MAY choose to forward these queries when the operator expects that this does not apply, either because the operator knows the upstream resolver does have the forwarder's IP address in its TLS certificate's SAN field or that the operator expects clients of the unencrypted resolver to use the SVCB information opportunistically.

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 or DoH connections, or in the URI host for DoH requests.

When performing discovery using resolver IP addresses, clients MUST use the IP address 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 both DoT and DoH.

6.4. Handling non-DDR queries for resolver.arpa

DNS resolvers that support DDR by responding to queries for `_dns.resolver.arpa` SHOULD 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.

The designated resolver information in DNR might not contain a full set of SvcParams needed to connect to an encrypted 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 packets. 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.

DoH resolvers that allow discovery using DNS SVCB answers over unencrypted DNS MUST NOT provide differentiated behavior based on the HTTP path alone, since an attacker could modify the "dohpath" parameter.

While the IP address of the Unencrypted 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 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 Resolver, clients applying Verified Discovery (Section 4.2) MUST validate that the IP address of the Unencrypted Resolver is covered by the SubjectAlternativeName of the Designated Resolver's TLS certificate.

Clients using Opportunistic Discovery (Section 4.3) MUST be limited to cases where the Unencrypted Resolver and Designated Resolver have the same IP address.

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]. This will allow resolvers to respond to queries directed at themselves rather than a specific domain name. While this document uses "resolver.arpa" to return SVCB records indicating designated encrypted capability, the name is generic enough to allow future reuse for other purposes where the resolver wishes to provide information about itself to the client.

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 Resolver much like "ipv4only.arpa" allows for client-to-middlebox communication. For more context, see the rationale behind "ipv4only.arpa" in [RFC8880].

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.

9. References

9.1. Normative References

- [I-D.ietf-add-svcb-dns]
Schwartz, B., "Service Binding Mapping for DNS Servers", Work in Progress, Internet-Draft, draft-ietf-add-svcb-dns-02, 1 February 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-add-svcb-dns-02>>.
- [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-08, 12 October 2021, <<https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-svcb-https-08>>.
- [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>>.

- [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>>.
- [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>>.

9.2. Informative 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-06, 22 March 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-add-dnr-06>>.
- [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>>.
- [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>>.

- [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>>.
- [RFC5507] IAB, Faltstrom, P., Ed., Austein, R., Ed., and P. Koch, Ed., "Design Choices When Expanding the DNS", RFC 5507, DOI 10.17487/RFC5507, April 2009, <<https://www.rfc-editor.org/rfc/rfc5507>>.
- [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>>.
- [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>>.
- [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 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 Resolver (using a SUDN) or another Encrypted 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 resolver 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 Resolvers or another Encrypted 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.
- * Clients that support SVCB will generally send out three queries when accessing web content on a dual-stack network: A, AAAA, and HTTPS queries. Discovering a Designated Resolver as part of one of these queries, without having to add yet another query, minimizes the total number of queries clients send. While [RFC5507] recommends adding new RRTypes for new functionality, SVCB provides an extension mechanism that simplifies client behavior.

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: 15 October 2022

M. Boucadair, Ed.
Orange
T. Reddy, Ed.
Akamai
D. Wing
Citrix
N. Cook
Open-Xchange
T. Jensen
Microsoft
13 April 2022

DHCP and Router Advertisement Options for the Discovery of Network-
designated Resolvers (DNR)
draft-ietf-add-dnr-07

Abstract

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

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 15 October 2022.

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	2
2. Terminology	3
3. Overview	3
3.1. Configuration Data for Encrypted DNS	4
3.2. Handling Configuration Data Conflicts	6
3.3. Connection Establishment	6
3.4. Multihoming Considerations	7
4. DHCPv6 Encrypted DNS Option	7
4.1. Option Format	7
4.2. DHCPv6 Client Behavior	9
5. DHCPv4 Encrypted DNS Option	9
5.1. Option Format	9
5.2. DHCPv4 Client Behavior	11
6. IPv6 RA Encrypted DNS Option	12
6.1. Option Format	12
6.2. IPv6 Host Behavior	14
7. Security Considerations	14
7.1. Spoofing Attacks	14
7.2. Deletion Attacks	15
7.3. Passive Attacks	15
7.4. Wireless Security - Authentication Attacks	15
8. IANA Considerations	16
8.1. DHCPv6 Option	16
8.2. DHCPv4 Option	16
8.3. Neighbor Discovery Option	17
9. Acknowledgements	17
10. Contributing Authors	17
11. References	18
11.1. Normative References	18
11.2. Informative References	18
Authors' Addresses	21

1. Introduction

This document focuses on the support of encrypted DNS such as DNS-over-HTTPS (DoH) [RFC8484], DNS-over-TLS (DoT) [RFC7858], or DNS-over-QUIC (DoQ) [I-D.ietf-dprive-dnsquic] in local networks.

In particular, the document specifies how a local encrypted DNS server 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), local networks with or without DNS forwarders). It is out of the scope of this document to provide an inventory of such deployments.

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:

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 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 servers 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 IPv6 addresses, and a set of service parameters of the encrypted DNS server. More information about the design of these options is provided in the following subsections.

3.1. Configuration Data for Encrypted DNS

In order to allow for PKIX-based authentication between a DNS client and an encrypted DNS server, the Encrypted DNS options are designed to 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.

To avoid adding a dependency on another server to resolve the ADN, the Encrypted DNS options return the IP address(es) to locate the encrypted DNS server. These encrypted DNS servers 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 servers 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 servers. 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 IP address with an encrypted DNS protocol. No probing is required in such a design.

A list of IP addresses to reach an encrypted DNS server may be returned in an Encrypted DNS option to accommodate current deployments relying upon primary and backup servers. 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. 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 more than one IP address are to be returned in an Encrypted DNS option, these addresses are ordered in the preference for use by the client.

Because distinct encrypted DNS protocols may be provisioned by a network (e.g., DoT, DoH, and DoQ) 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 to rely upon an existing IANA registry and, thus, to accommodate new encrypted DNS protocols and service parameters that may be defined in the future. At least the following service parameters are RECOMMENDED to 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]).

ech: Used to enable Encrypted ClientHello (ECH) (Section 7.3 of [I-D.ietf-dnsop-svcb-https]).

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

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

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].

ServiceMode (Section 2.4.3 of [I-D.ietf-dnsop-svcb-https]) 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 processed by a host following the procedure in Section 5 of [I-D.ietf-add-ddr]. Note that this mode may be subject to active attacks, which can be mitigated by DNSSEC.

Other mechanisms may be considered in other contexts (e.g., secure discovery) for the provisioning of encrypted DNS servers. 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.
- * A list of IP addresses to locate the encrypted DNS server.
- * 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 servers (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.

3.3. Connection Establishment

If the local DNS client supports one of the discovered Encrypted DNS protocols identified by Application Layer Protocol Negotiation (ALPN) protocol identifiers, the DNS client establishes an encrypted DNS session following the order of the discovered servers. The client follows the mechanism discussed in Section 8 of [RFC8310] to authenticate the DNS server certificate using the authentication domain name conveyed in the Encrypted DNS options. ALPN-related considerations can be found in Section 6.1 of [I-D.ietf-dnsop-svcb-https].

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. The reader may refer to [RFC6731] for a discussion of issues and an example of DNS server selection for multi-interfaced devices.

4. DHCPv6 Encrypted DNS Option

4.1. Option Format

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

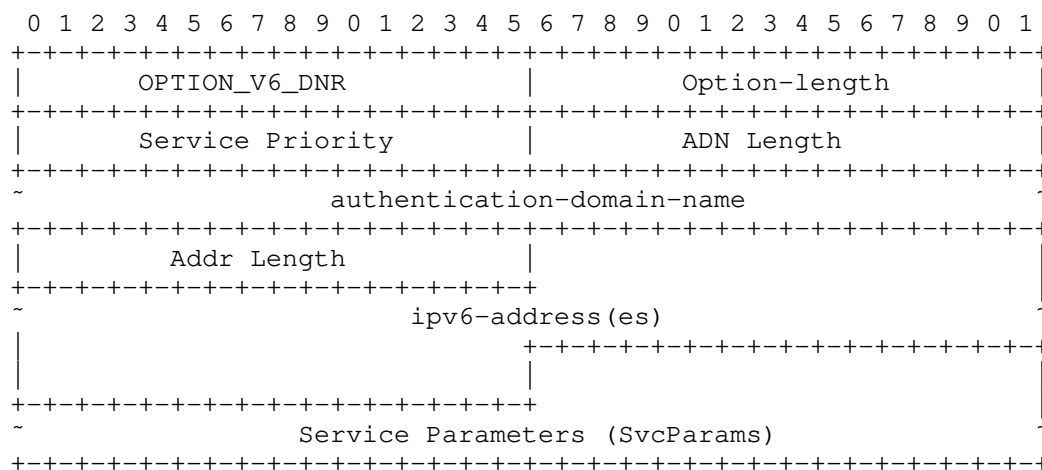


Figure 1: DHCPv6 Encrypted DNS Option

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

Option-code: OPTION_V6_DNR (TBA1, see Section 8.1)

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 field is encoded 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

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').

4.2. DHCPv6 Client Behavior

To discover an encrypted DNS server, 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 server. These instances SHOULD be processed following their service priority (i.e., smaller service priority indicates a higher preference).

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.

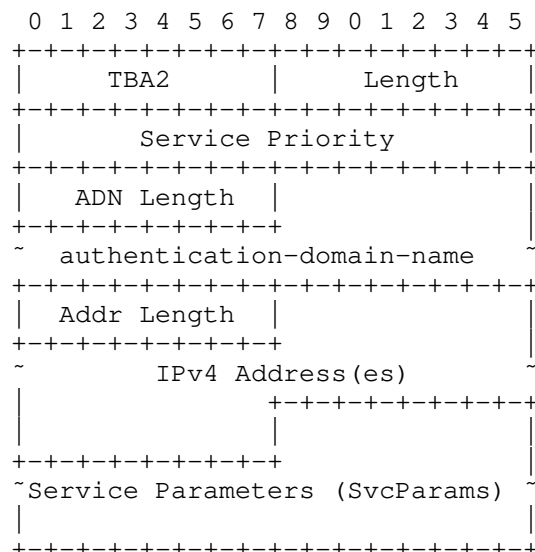


Figure 4: DHCPv4 Encrypted DNS Option

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

Code: OPTION_V4_DNR (TBA2, see Section 8.2).

Length: Indicates the length of the enclosed data in octets. The option length is ('ADN Length' + 3) when only an ADN is included in the option.

Service Priority: The priority of this OPTION_V4_DNR instance compared to other instances. This field is encoded following the rules specified in Section 2.4.1 of [I-D.ietf-dnsop-svcb-https].

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

authentication-domain-name (variable length): Includes the authentication domain name of the encrypted DNS server. This field is formatted as specified in Section 10 of [RFC8415]. The format of this field is shown in Figure 5. The values s1, s2, s3, etc. represent the domain name labels in the domain name encoding.

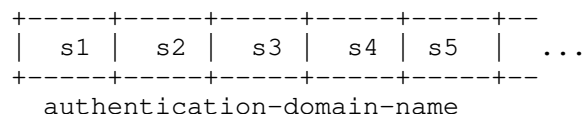


Figure 5: Format of the Authentication Domain Name Field

Addr Length: Indicates the length of included IPv4 addresses in octets. It MUST be a multiple of 4 for ServiceMode.

IPv4 Address(es) (variable length): Indicates one or more IPv4 addresses to reach the encrypted DNS server. 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.

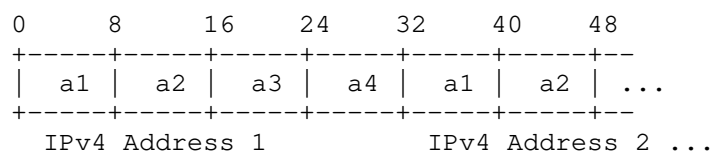


Figure 6: Format of the IPv4 Addresses Field

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. 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 ('Option-length' - 4 - 'ADN Length' - 'Addr Length').

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 server, the DHCPv4 client requests the Encrypted DNS server by including OPTION_V4_DNR in a Parameter Request List option [RFC2132].

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

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.

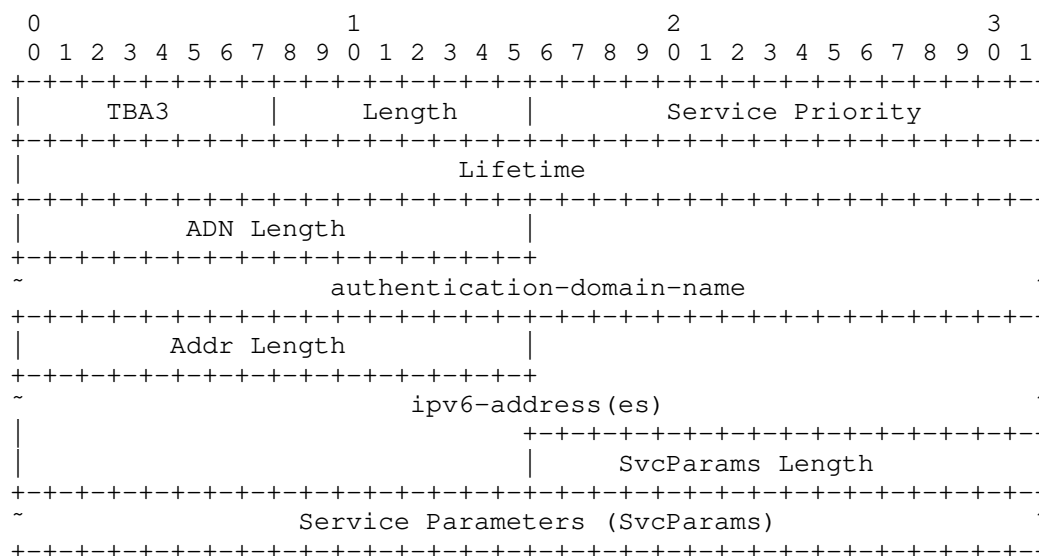


Figure 7: RA Encrypted DNS Option

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 8.3).

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

Service Priority: The priority of this Encrypted DNS option instance compared to other instances. This field is encoded 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 $3 * \text{MaxRtrAdvInterval}$, 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 domain name of the encrypted DNS server. 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. It MUST be a multiple of 16 for ServiceMode.

ipv6-address(es) (variable length): One or more IPv6 addresses of the encrypted DNS server. 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 Paramters (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. 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 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 procedure described in Section 5.3.1 of [RFC8106] with the formatting requirements in Section 6.1 substituted for the length validation.

The host MUST be prepared to receive multiple Encrypted DNS options in RAs. These instances SHOULD 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 server. 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 server.

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 described in [RFC7610], the router (e.g., a border router, a CPE) discards DHCP response messages received from any local endpoint.
- * RA-Guard described in [RFC7113], the router discards RAs messages received from any local endpoint.
- * Source Address Validation Improvement (SAVI) solution for DHCP described in [RFC7513], the router filters packets with forged source IP addresses.

The above mechanisms would ensure that the endpoint receives the correct configuration information of the encrypted DNS servers 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 servers that spoof the IP address of a DNS server will fail because the DNS client will fail to authenticate that rogue server 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 servers, intercept sensitive data).

Encrypted DNS connections received from outside the local network MUST be discarded by the encrypted DNS forwarder in the CPE. This behavior adheres to REQ#8 in [RFC6092]; it MUST apply for both IPv4 and IPv6.

7.2. Deletion Attacks

If the DHCP responses or RAs are dropped by the attacker, the client can fallback to use a preconfigured encrypted DNS server. However, the use of policies to select servers 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 server 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 an information (e.g., NTP server, DNS server, default domain) provided by such networks via DHCP, DHCPv6, or RA are untrusted because DHCP and RA messages are not authenticated.

If the pre-shared key is the same for all clients that connect to the same WLAN, the shared key will be available to all nodes, including attackers. As such, it is possible to mount an active on-path attack. Man-in-the-middle attacks are possible within local networks because such 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 Access Point (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 device and WPA-PSK is used (e.g., [PSK]).

8. IANA Considerations

8.1. 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

8.2. 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]

8.3. 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	DNS Encrypted DNS Option	[ThisDocument]

Table 2

9. 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 [I-D.pusateri-dhc-dns-driu].

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

10. 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

11. References

11.1. Normative References

- [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-08, 12 October 2021, <<https://www.ietf.org/archive/id/draft-ietf-dnsop-svcb-https-08.txt>>.
- [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>>.

11.2. Informative References

- [BOOTP] "BOOTP Vendor Extensions and DHCP Options",
<[https://www.iana.org/assignments/bootp-dhcp-parameters/
bootp-dhcp-parameters.xhtml#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](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](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_\(wireless_networks\)](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-06, 4 April
2022, <[https://www.ietf.org/archive/id/draft-ietf-add-ddr-
06.txt](https://www.ietf.org/archive/id/draft-ietf-add-ddr-06.txt)>.
- [I-D.ietf-add-svcb-dns]
Schwartz, B., "Service Binding Mapping for DNS Servers",
Work in Progress, Internet-Draft, draft-ietf-add-svcb-dns-
02, 1 February 2022, <[https://www.ietf.org/archive/id/
draft-ietf-add-svcb-dns-02.txt](https://www.ietf.org/archive/id/draft-ietf-add-svcb-dns-02.txt)>.
- [I-D.ietf-dprive-dnssoquic]
Huitema, C., Dickinson, S., and A. Mankin, "DNS over
Dedicated QUIC Connections", Work in Progress, Internet-
Draft, draft-ietf-dprive-dnssoquic-11, 21 March 2022,
<[https://www.ietf.org/archive/id/draft-ietf-dprive-
dnssoquic-11.txt](https://www.ietf.org/archive/id/draft-ietf-dprive-dnssoquic-11.txt)>.
- [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://www.ietf.org/archive/id/draft-pusateri-dhc-dns-
driu-00.txt](https://www.ietf.org/archive/id/draft-pusateri-dhc-dns-driu-00.txt)>.

- [Krack] The Unicode Consortium, "Key Reinstallation Attacks", 2017, <<https://www.krackattacks.com/>>.
- [ND] "IPv6 Neighbor Discovery Option Formats", <<http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml#icmpv6-parameters-5>>.
- [PSK] 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>.
- [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>>.
- [RFC6092] Woodyatt, J., Ed., "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service", RFC 6092, DOI 10.17487/RFC6092, January 2011, <<https://www.rfc-editor.org/info/rfc6092>>.
- [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>>.
- [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>>.

Authors' Addresses

Mohamed Boucadair (editor)
Orange
35000 Rennes
France

Email: mohamed.boucadair@orange.com

Tirumaleswar Reddy (editor)
Akamai
Embassy Golf Link Business Park
Bangalore 560071
Karnataka
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