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.

Table of Contents

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.

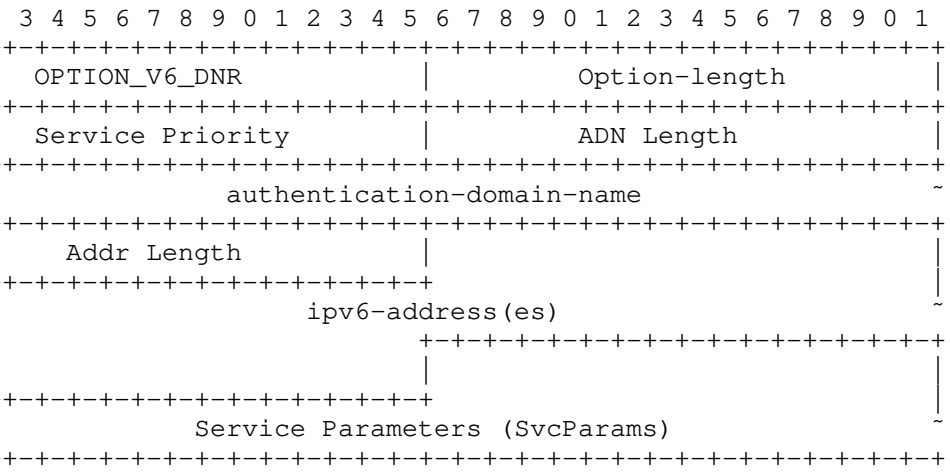

Figure 1: DHCPv6 Encrypted DNS Option

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.

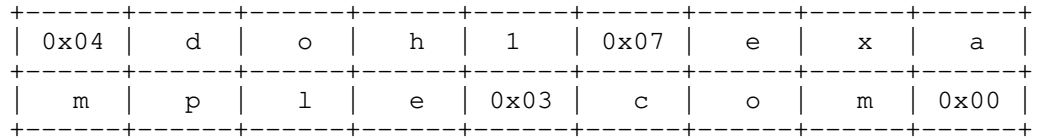

Figure 2: An Example of the DNS authentication-domain-name Encoding

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.

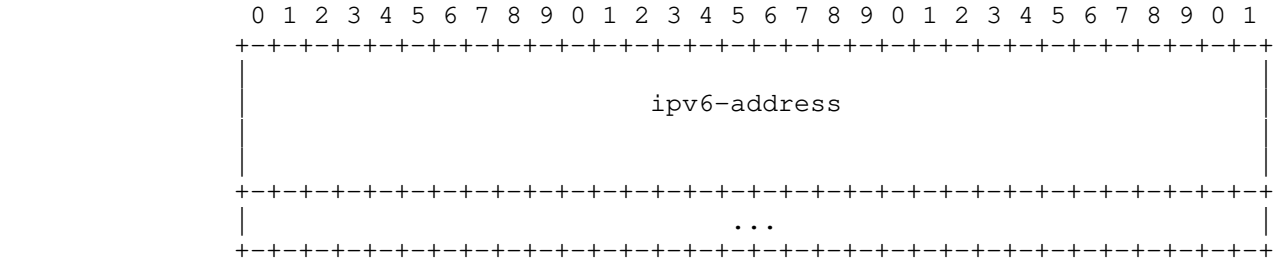

Figure 3: Format of the IPv6 Addresses Field

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.

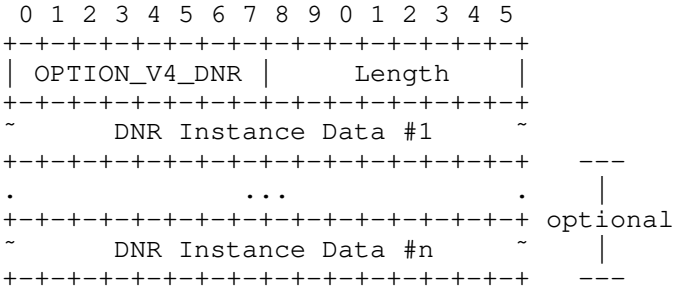

Figure 4: DHCPv4 Encrypted DNS Option

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.

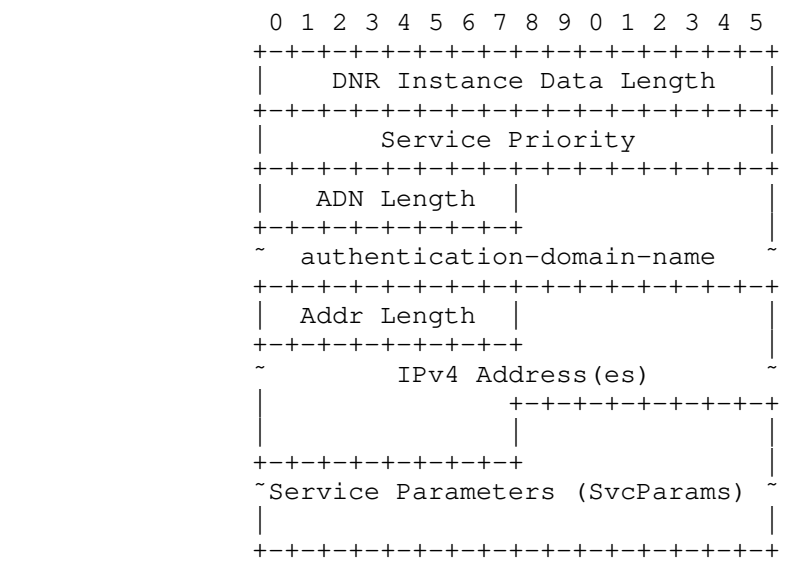

Figure 5: DNR Instance Data Format

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.

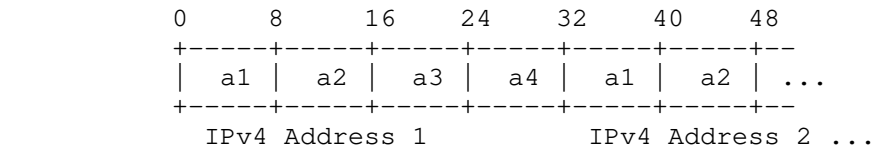

Figure 6: Format of the IPv4 Addresses Field

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.

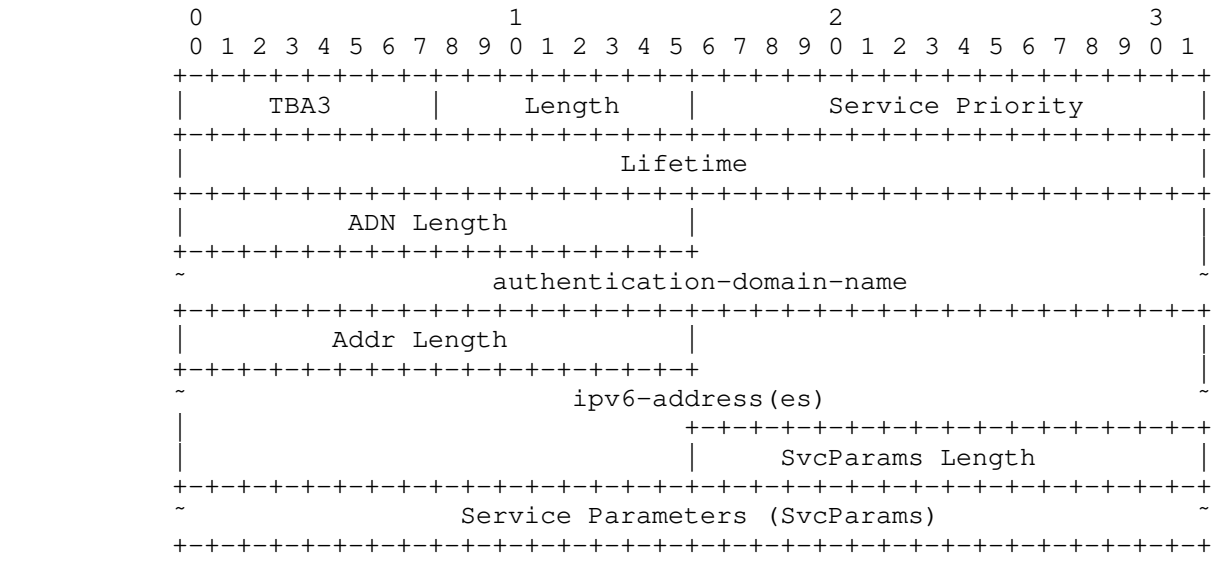

Figure 7: RA Encrypted DNS Option

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