ADD
Internet-Draft
Intended status: Standards Track
Expires: July 26, 2021

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

January 22, 2021

DHCP and Router Advertisement Options for Encrypted DNS Discovery
draft-btw-add-home-12

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 port number to reach such encrypted DNS servers. The discovery of DNS-over-HTTPS URI Templates is also discussed.

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 July 26, 2021.

Copyright Notice

Table of Contents

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-dnsoquic] in local networks.

In particular, the document specifies how a local encrypted DNS server can be discovered and used by connected hosts by means of DHCP [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 optionally a port number. The discovery of DoH URI Templates is discussed in Section 7.

Sample target deployment scenarios are discussed in Appendix A; both managed and unmanaged Customer Premises Equipment (CPEs) are covered. It is out of the scope of this document to provide an exhaustive inventory of deployments where Encrypted DNS Options (Sections 4, 5, and 6) can be used.

Considerations related to hosting a DNS forwarder in a local network are described in Section 8.

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.

Encrypted DNS: refers to a scheme where DNS exchanges are transported over an encrypted channel. Examples of encrypted DNS

are DNS-over-TLS (DoT) [RFC7858], DNS-over-HTTPS (DoH) [RFC8484], or DNS-over-QUIC (DoQ) [I-D.ietf-dprive-dnsoquic].

Managed CPE: refers to a CPE that is managed by an Internet Service Providers (ISP).

Unmanaged CPE: refers to a CPE that is not managed by an ISP.

DHCP: refers to both DHCPv4 and DHCPv6.

3. Overview and Rationale

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

As reported in 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.

In order to allow for PKIX-based authentication between a DNS client and an encrypted DNS server while accommodating the current best practices for issuing certificates, this document allows for configuring an authentication domain name to be presented as a reference identifier for DNS authentication purposes.

To avoid adding a dependency on another server to resolve the ADN, the options return a list of IP addresses to locate the encrypted DNS server. In the various scenarios sketched in Appendix A, encrypted DNS servers may terminate on the same IP address or distinct IP addresses. Terminating encrypted DNS servers on the same or distinct IP addresses is deployment specific. It is RECOMMENDED to return both the ADN and a list of IP addresses to a requesting host.

Note that in order to optimize the size of discovery messages when all servers terminate on the same IP address, a host may rely 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 to probe that list of IP addresses. To avoid such probing, the options defined in the following sections associate an IP address with an encrypted DNS type. No probing is required in such design.

A list of IP addresses to reach an encrypted DNS server can be returned in the option to accommodate current deployments relying upon primary and backup servers. Whether one IP address or more are returned in an option is deployment specific. For example, a router embedding a recursive server or forwarder has to include one single IP address pointing to one of its LAN-facing interfaces. This 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 server option, these addresses are ordered in the preference for use by the client.

Because DoT and DoQ may make use of customized port numbers instead of default ones, the Encrypted DNS server options are designed to return alternate port numbers.

Some ISPs rely upon external resolvers (e.g., outsourced service or public resolvers); these ISPs provide their customers with the IP addresses of these resolvers. These addresses are typically configured on CPEs using dedicated management tools. Likewise, users can modify the default DNS configuration of their CPEs (e.g., supplied by their ISP) to configure their favorite DNS servers. This document permits such deployments.

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.

The DNS client establishes an encrypted DNS session with the discovered DNS IP address(es) and port number, and uses 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.

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.

DHCP/RA options to discover encrypted DNS servers (including, DoH URI Templates should the WG pursue that approach pending feedback) takes precedence over DEER [I-D.pauly-add-deer] since DEER uses unencrypted DNS to an external DNS resolver, which is susceptible to both internal and external attacks whereas DHCP/RA is only vulnerable to internal attacks.

4. DHCPv6 Encrypted DNS Options

This section defines two DHCPv6 options: DHCPv6 Encrypted DNS ADN option (Section 4.1) and DHCPv6 Encrypted DNS Address option (Section 4.2).

4.1. Encrypted DNS ADN Option

The DHCPv6 Encrypted DNS ADN option is used to configure an authentication domain name of the encrypted DNS server. The format of this option is shown in Figure 1.

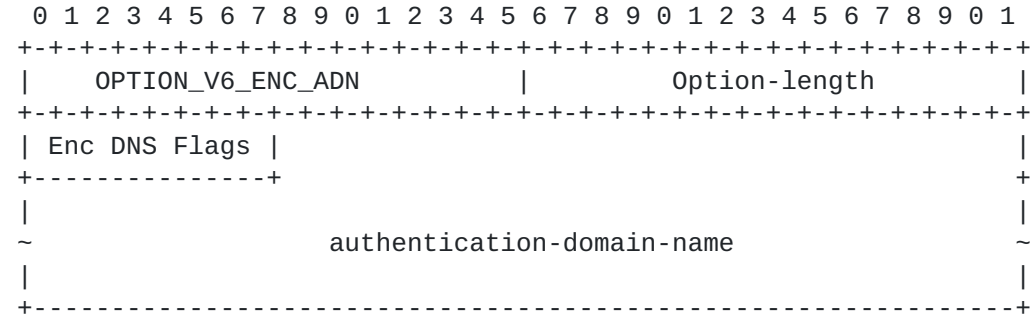


Figure 1: DHCPv6 Encrypted DNS ADN Option

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

Option-code: OPTION_V6_ENC_ADN (TBA1, see Section 11.2)

Option-length: Length of the enclosed data in octets.

Enc DNS Flags (Encrypted DNS Flags): Indicates the type(s) of the encrypted DNS server conveyed in this attribute. The format of this 8-bit field is shown in Figure 2.

Figure 2: Encrypted DNS Flags Field

T: If set, this bit indicates that the server supports DoT [RFC7858].

H: If set, this bit indicates that the server supports DoH [RFC8484].

Q: If set, this bit indicates that the server supports DoQ [I-D.ietf-dprive-dnsoquic].

U: Unassigned bits. These bits MUST be unset by the sender. Associating a meaning with an unassigned bit can be done as per Section 11.1.

In a request, these bits are assigned to indicate the requested encrypted DNS server type(s) by the client. In a response, these bits are set as a function of the encrypted DNS supported by the server and the requested encrypted DNS server type(s).

To keep the packet small, if more than one encrypted DNS type (e.g., both DoH and DoT) are to be returned to a requesting client and the same ADN is used for these types, the corresponding bits must be set in the 'Encrypted DNS Types' field of the same option instance in a response. For example, if the client requested DoH and DoT and the server supports both with the same ADN, then both T and H bits must be set.

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

An example of the authentication-domain-name encoding is shown in Figure 3. This example conveys the FQDN "doh1.example.com.", and the resulting Option-length field is 18.

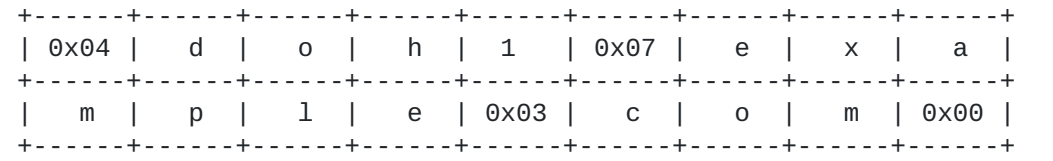


Figure 3: An Example of the DNS authentication-domain-name Encoding

4.2. Encrypted DNS Address Option

The DHCPv6 Encrypted DNS Address option is used to configure a list of IP addresses and a port number of the encrypted DNS server. The format of this option is shown in Figure 4.

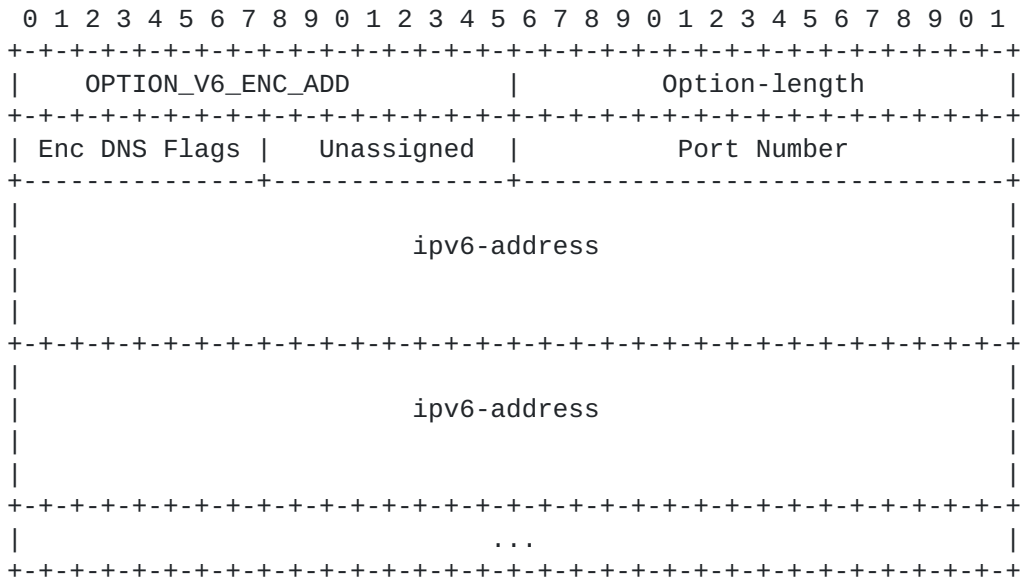


Figure 4: DHCPv6 Encrypted DNS Address Option

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

Option-code: OPTION_V6_ENC_ADD (TBA2, see Section 11.2)

Option-length: Length of the enclosed data in octets.

Enc DNS Flags (Encrypted DNS Flags): Indicates the type(s) of the encrypted DNS server conveyed in this attribute. The format of this 8-bit field is shown in Figure 2. In a request, these bits are set to indicate the requested encrypted DNS server type(s) by the client. In a response, these bits are set as a function of the encrypted DNS supported by the server and the requested encrypted DNS server type(s).

Unassigned: These bits MUST be unset by the sender. Associating a meaning with an unassigned bit can be done via Standards Action [RFC8126].

Port Number: If not null, it indicates the port number to be used for the encrypted DNS. If this field is set to zero, this indicates that default port numbers should be used. As a reminder, the default port number is 853 for DoT and 443 for DoH.

ipv6-address(es): Indicates one or more IPv6 addresses to reach the encrypted DNS server. An address can be link-local, ULA, or GUA.

Multiple instances of OPTION_V6_ENC_ADN (or OPTION_V6_ENC_ADD) may be returned to a DHCPv6 client; each pointing to a distinct encrypted DNS server type.

If more than one encrypted DNS server types is supported on the same IP address and default port numbers are used, one instance of OPTION_V6_ENC_ADD option with the appropriate bits set in "Encr DNS Types" field should be returned by the DHCP server.

4.3. DHCPv6 Client Behavior

To discover an encrypted DNS server, the DHCPv6 client MUST include OPTION_V6_ENC_ADN and OPTION_V6_ENC_ADD 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 sets the Encrypted DNS Types field to the requested encrypted DNS server type(s).

If the DHCPv6 client requested more than one encrypted DNS server type, the DHCP client MUST be prepared to receive multiple OPTION_V6_ENC_ADN (or OPTION_V6_ENC_ADD) options; each option is to be treated as a separate encrypted DNS server.

The DHCPv6 client MUST silently discard multicast and host loopback addresses conveyed in OPTION_V6_ENC_ADD.

5. DHCPv4 Encrypted DNS Option

5.1. Encrypted DNS Option

The DHCPv4 Encrypted DNS option is used to configure an authentication domain name, a list of IP addresses, and a port number of the encrypted DNS server. The format of this option is illustrated in Figure 5.

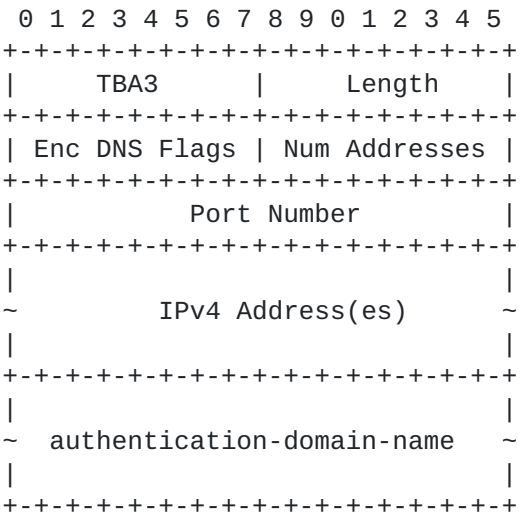


Figure 5: DHCPv4 Encrypted DNS Option

The fields of the option shown in Figure 5 are as follows:

Code: OPTION_V4_ENC_DNS (TBA3, see Section 11.3).

Length: Length of the enclosed data in octets.

Enc DNS Flags (Encrypted DNS Flags): Indicates the type(s) of the encrypted DNS server conveyed in this attribute. The format of this field is shown in Figure 2.

Num Addresses: Indicates the number of included IPv4 addresses.

Port Number: If not null, it indicates the port number to be used for the encrypted DNS. A null value indicates that default port numbers are used. As a reminder, the default port number is 853 for DoT and 443 for DoH.

IPv4 Address(es): 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.

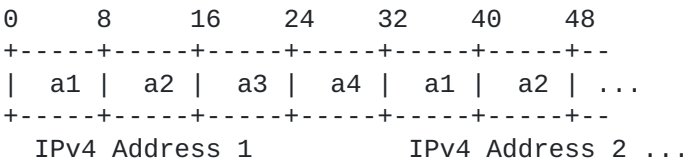


Figure 6: Format of the IPv4 Addresses Field

authentication-domain-name: The 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 7. The values s1, s2, s3, etc. represent the domain name labels in the domain name encoding.

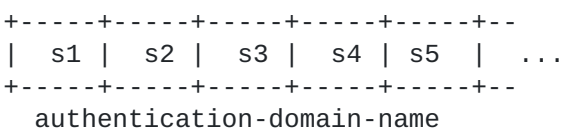


Figure 7: Format of the Authentication Domain Name Field

OPTION_V4_ENC_DNS is a concatenation-requiring option. As such, the mechanism specified in [RFC3396] MUST be used if OPTION_V4_ENC_DNS 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_ENC_DNS in a Parameter Request List option [RFC2132]. The DHCPv4 client sets the Encrypted DNS Types field to the requested encrypted DNS server.

If the DHCPv4 client requested more than one encrypted DNS server type, the DHCPv4 client MUST be prepared to receive multiple DHCP OPTION_V4_ENC_DNS options; each option is to be treated as a separate encrypted DNS server.

The DHCPv4 client MUST silently discard multicast and host loopback addresses conveyed in OPTION_V4_ENC_DNS.

6. IPv6 RA Encrypted DNS Options

This section defines two Neighbor Discovery [RFC4861]: IPv6 Router Advertisement (RA) Encrypted DNS ADN option (Section 6.1) and IPv6 RA Encrypted DNS Address option (Section 6.2). These options are useful in contexts similar to those discussed in Section 1.1 of [RFC8106].

6.1. Encrypted DNS ADN Option

The IPv6 RA Encrypted DNS ADN option is used to configure an authentication domain name of the encrypted DNS server. The format of this option is illustrated in Figure 8.

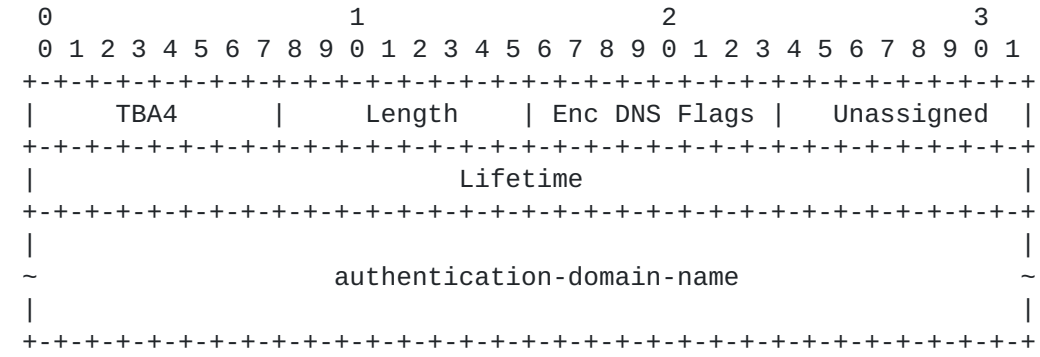


Figure 8: RA Encrypted DNS ADN Option

The fields of the option shown in Figure 8 are as follows:

Type: 8-bit identifier of the Encrypted DNS Option as assigned by IANA (TBA4, see Section 11.4).

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

Enc DNS Flags (Encrypted DNS Flags): Indicates the type(s) of the encrypted DNS server conveyed in this attribute. The format of this field is shown in Figure 2.

Unassigned: This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

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.

authentication Domain Name: The domain name of the encrypted DNS server. This field is formatted as specified in Section 10 of [RFC8415].

This field MUST be padded with zeros so that its size is a multiple of 8 octets.

6.2. Encrypted DNS Address Option

The IPv6 RA Encrypted DNS Address option is used to configure a port number and a list of IPv6 addresses of the encrypted DNS server. The format of this option is illustrated in Figure 9. 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 Address options may be used.

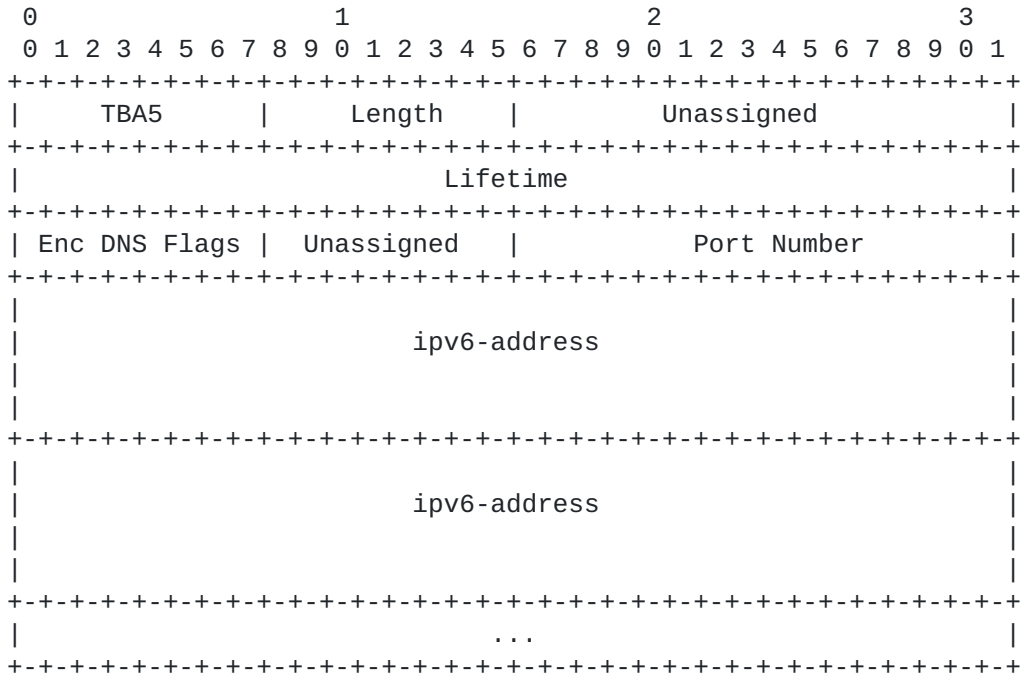


Figure 9: RA Encrypted DNS Address Option

The fields of the RA Encrypted DNS Address option shown in Figure 9 are as follows:

Type: 8-bit identifier of the Encrypted DNS Address Option as assigned by IANA (TBA5, see Section 11.4).

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

Unassigned: This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Lifetime: 32-bit unsigned integer. The maximum time in seconds (relative to the time the packet is received) over which the discovered encrypted DNS IPv6 addresses are 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 these IPv6 addresses MUST no longer be used.

Enc DNS Flags (Encrypted DNS Flags): Indicates the type(s) of the encrypted DNS server conveyed in this attribute. The format of this field is shown in Figure 2.

Port Number: If not null, it indicates the port number to be used for the encrypted DNS. A null value indicates that default port numbers must be used. As a reminder, the default port number is 853 for DoT and 443 for DoH.

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

7. DoH URI Templates

DoH servers may support more than one URI Template [RFC8484]. Also, if the resolver hosts several DoH services (e.g., no-filtering, blocking adult content, blocking malware), these services can be discovered as templates. The following discusses a mechanism for a DoH client to retrieve the list of supported templates by a DoH server.

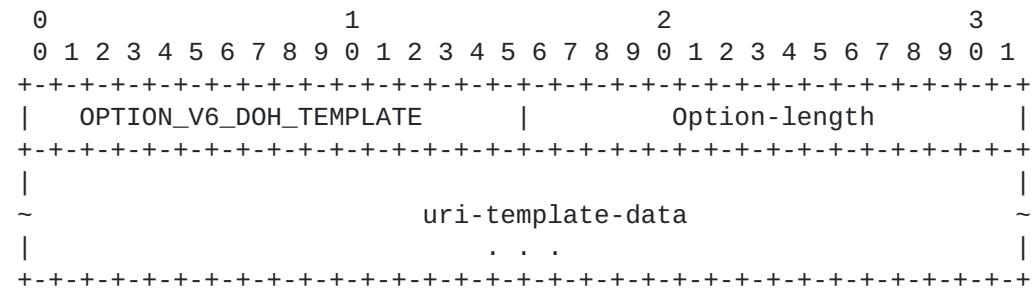
Upon discovery of a DoH resolver (Sections 4, 5, and 6), the DoH client may contact that DoH resolver to retrieve the list of supported DoH services using DEER [I-D.pauly-add-deer]. This will allow the client to discover the resolver's supported DoH templates or DoH resolvers that the discovered resolver designates using DNS SVCB queries [I-D.schwartz-svcb-dns]. The designated DoH resolvers and DoH resolver discovered using DHCP/RA may be hosted on the same or distinct IP addresses.

Let's suppose that a host has discovered an encrypted DNS server that is DoH-capable. The host has also discovered the following information:

- ADN: doh.example.com
- Locator: 2001:db8:1::1

The client will use DEER [I-D.pauly-add-deer] to discover the DoH templates supported by the DNS server at the Locator (2001:db8:1::1). In addition to the checks included in DEER, clients should verify the ADN (doh.example.com) is valid for the certificate provided by the DoH resolver. However, the IP address of the DEER-discovered resolver may differ from the Locator field value. This will allow the ISP to offer different DoH services to the endpoints attached to local networks.

Alternatively, dedicated DHCP/RA options may be defined to convey an URI template in order to avoid additional network traffic to bootstrap DoH configuration. An example of the format of such an option is depicted in Figure 10.



Each instance of the uri-template-data is formatted as follows:

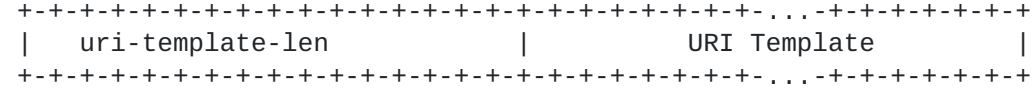


Figure 10: Example of a DHCPv6 URI Template Option

Note: More feedback from the WG is needed to decide which approach(es) to follow.

How a DoH client makes use of the configured DoH services is out of the scope of this document.

8. Hosting Encrypted DNS Forwarder in Local Networks

This section discusses some deployment considerations (not recommendations) to host an encrypted DNS forwarder within a local network.

8.1. Managed CPEs

The section discusses mechanisms that can be used to host an encrypted DNS forwarder in a managed CPE (Appendix A.1).

8.1.1. DNS Forwarders

The managed CPE should support a configuration parameter to instruct the CPE whether it has to relay the encrypted DNS server received from the ISP's network or has to announce itself as a forwarder within the local network. The default behavior of the CPE is to supply the encrypted DNS server received from the ISP's network.

8.1.2. ACME

The ISP can assign a unique FQDN (e.g., "cpe1.example.com") and a domain-validated public certificate to the encrypted DNS forwarder hosted on the CPE. Automatic Certificate Management Environment (ACME) [RFC8555] can be used by the ISP to automate certificate management functions such as domain validation procedure, certificate issuance and certificate revocation.

8.1.3. Auto-Upgrade Based on Domains and their Subdomains

If the ADN conveyed in DHCP/RA (Sections 4, 5, and 6) is preconfigured in popular OSes or browsers as a verified resolver and the auto-upgrade (Appendix B) is allowed for both the preconfigured ADN and its sub-domains, the encrypted DNS client will learn the local encrypted DNS forwarder using DHCP/RA and auto-upgrade because the preconfigured ADN would match the subjectAltName value in the server certificate. For example, if the preconfigured ADN is "*.example.com" and the discovered encrypted DNS forwarder is "cpe1.example.com", auto-upgrade will take place.

In this case, the CPE can communicate the ADN of the local DoH forwarder (Section 8.1.2) to internal hosts using DHCP/RA (Sections 4, 5, and 6).

Let's suppose that "*.example.net" is preconfigured as a verified resolved in the browser or OS. If the encrypted DNS client discovers a local forwarder "cpe1-internal.example.net", the encrypted DNS client will auto-upgrade because the preconfigured ADN would match

subjectAltName value "cpe1-internal.example.net" of type dNSName. As shown in Figure 11, the auto-upgrade to a rogue server advertising "rs.example.org" will fail because it does not match "*.example.net".

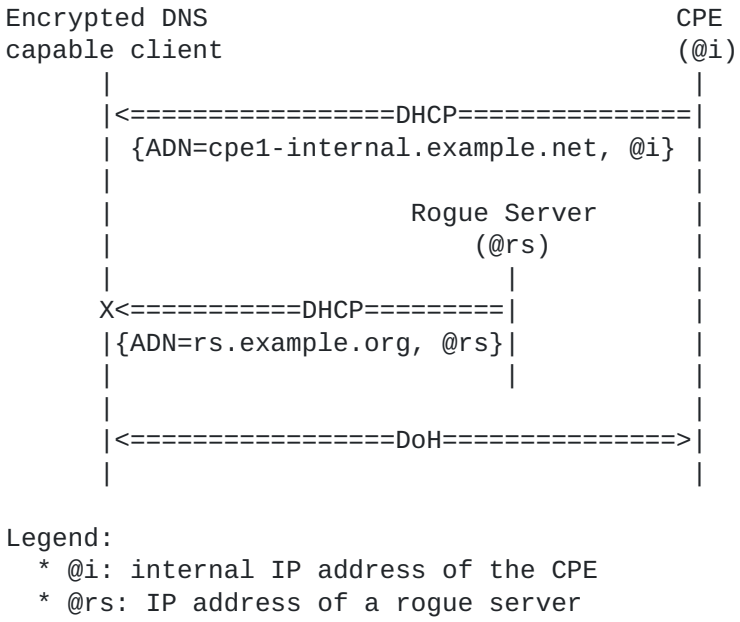


Figure 11: A Simplified Example of Auto-upgrade based on Subdomains

8.2. Unmanaged CPEs

The approach specified in Section 8.1 does not apply for hosting a DNS forwarder in an unmanaged CPE.

The unmanaged CPE administrator (referred to as administrator) can host an encrypted DNS forwarder on the unmanaged CPE. This assumes the following:

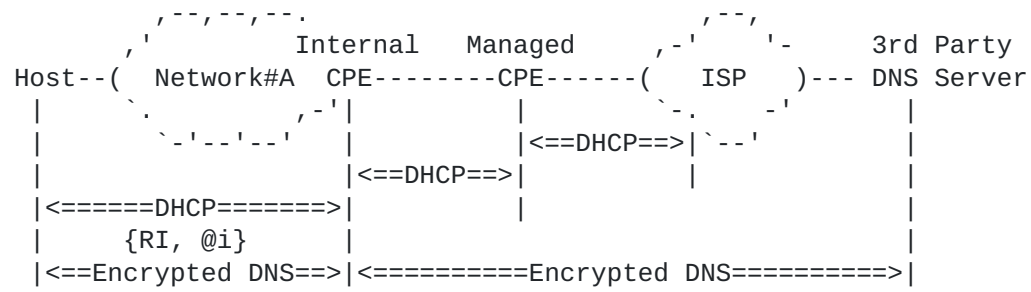
- The encrypted DNS server certificate is managed by the entity in-charge of hosting the encrypted DNS forwarder.

  Alternatively, a security service provider can assign a unique FQDN to the CPE. The encrypted DNS forwarder will act like a private encrypted DNS server only be accessible from within the the local network.

- The encrypted DNS forwarder will either be configured to use the ISP's or a 3rd party encrypted DNS server.

- The unmanaged CPE will advertise the encrypted DNS forwarder ADN using DHCP/RA to internal hosts.

Figure 12 illustrates an example of an unmanaged CPE hosting a forwarder which connects to a 3rd party encrypted DNS server. In this example, the DNS information received from the managed CPE (and therefore from the ISP) is ignored by the Internal CPE hosting the forwarder.



Legend:
* @i: IP address of the DNS forwarder hosted in the Internal CPE.

Figure 12: Example of an Internal CPE Hosting a Forwarder

9. Legacy CPEs

Hosts serviced by legacy CPEs that can't be upgraded to support the options defined in Sections 4, 5, and 6 won't be able to learn the encrypted DNS server hosted by the ISP, in particular. If the ADN is not discovered using DHCP/RA, such hosts will have to fallback to use DEER as defined in [I-D.pauly-add-deer] to discover the encrypted DNS server and to retrieve the list of supported DoH services using the SVCB RRtype [I-D.schwartz-svcb-dns] without verifying the hostname of discovered templates with the ADN. Other guidance in DEER relating to resolver verification must be followed in this case. This will prevent an unencrypted resolver on a local address from referring to an encrypted resolver at a different address without an out-of-band configuration in the client beyond the scope of this document or DEER.

10. Security Considerations

10.1. 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. Also, an attacker can use a public IP address and get an 'IP address'-validated public certificate from a CA to 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 CPEs discards DHCP response messages received from any local endpoint.
- RA-Guard described in [RFC7113], the CPE discards RAs messages received from any local endpoint.
- Source Address Validation Improvement (SAVI) solution for DHCP described in [RFC7513], the CPE filters packets with forged source IP addresses.

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.

10.2. 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.

10.3. 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.

10.4. Wireless Security - Authentication Attacks

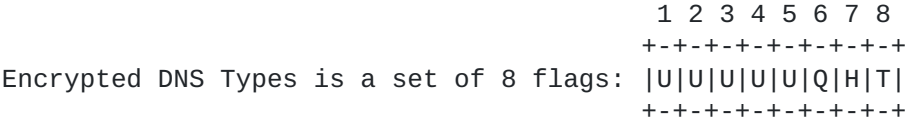
Wireless LAN (WLAN) as frequently deployed in local networks (e.g., home networks) is vulnerable to various attacks (e.g., [Evil-Twin], [Krack], [Dragonblood]). Because of these attacks, only cryptographically authenticated communications are trusted on WLANs. This means information provided by such networks via DHCP, DHCPv6, or RA (e.g., NTP server, DNS server, default domain) are untrusted because DHCP and RA 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, so 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 of 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]).

11. IANA Considerations

11.1. Encrypted DNS Flag Bits



where flag bits in positions 1-5 are for future assignment as additional flag bits.

This document requests IANA to create a new registry called "Encrypted DNS Types". The initial values of the registry are as follows:

Bit Position	Label	Description	Reference
1	U	Unassigned	
2	U	Unassigned	
3	U	Unassigned	
4	U	Unassigned	
5	U	Unassigned	
6	Q	DNS-over-QUIC (DoQ)	[ThisDocument]
7	H	DNS-over-HTTP (DoH)	[ThisDocument]
8	T	DNS-over-TLS (DoT)	[ThisDocument]

New flag bits are assigned via Standards Action [RFC8126].

11.2. DHCPv6 Options

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_ENC_ADN	Yes	No	[ThisDocument]
TBA2	OPTION_V6_ENC_ADD	Yes	No	[ThisDocument]

11.3. 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
TBA3	OPTION_V4_ENC_DNS	N	Encrypted DNS Server	[ThisDocument]

11.4. Neighbor Discovery Options

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
TBA4	DNS Encrypted DNS ADN Option	[ThisDocument]
TBA5	DNS Encrypted DNS Address Option	[ThisDocument]

12. Acknowledgements

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

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

Thanks to Mark Nottingham for the feedback on HTTP redirection.

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].

13. Contributing Authors

Nicolai Leymann
Deutsche Telekom
Germany

Email: n.leymann@telekom.de

14. References

14.1. Normative References

[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>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[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>.

14.2. Informative References

[Auto-upgrade] The Unicode Consortium, "DoH providers: criteria, process for Chrome", <docs.google.com/document/d/128i2YTV2C7T6Gr3I-81zlQ-_Lprnsp24qzy_20Z1Psw/edit>.

[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-dprive-dnsoquic]
Huitema, C., Mankin, A., and S. Dickinson, "Specification of DNS over Dedicated QUIC Connections", draft-ietf-dprive-dnsoquic-01 (work in progress), October 2020.

[I-D.ietf-v6ops-rfc7084-bis]
Palet, J., "Basic Requirements for IPv6 Customer Edge Routers", draft-ietf-v6ops-rfc7084-bis-04 (work in progress), June 2017.

[I-D.pauly-add-deer]
Pauly, T., Kinnear, E., Wood, C., McManus, P., and T. Jensen, "Discovery of Equivalent Encrypted Resolvers", draft-pauly-add-deer-00 (work in progress), November 2020.

[I-D.pusateri-dhc-dns-driu]
Pusateri, T. and W. Toorop, "DHCPv6 Options for private DNS Discovery", draft-pusateri-dhc-dns-driu-00 (work in progress), July 2018.

[I-D.schwartz-svcb-dns]
Schwartz, B., "Service Binding Mapping for DNS Servers", draft-schwartz-svcb-dns-01 (work in progress), August 2020.

[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>.

[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>.

[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>.

[RFC8520] Lear, E., Droms, R., and D. Romascanu, "Manufacturer Usage Description Specification", RFC 8520, DOI 10.17487/RFC8520, March 2019, <https://www.rfc-editor.org/info/rfc8520>.

[RFC8555] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", RFC 8555, DOI 10.17487/RFC8555, March 2019, <https://www.rfc-editor.org/info/rfc8555>.

[TR-069] The Broadband Forum, "CPE WAN Management Protocol", December 2018, <https://www.broadband-forum.org/technical/download/TR-069.pdf>.

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

Appendix A. Sample Target Deployment Scenarios

Internet Service Providers (ISPs) traditionally provide DNS resolvers to their customers. To that aim, ISPs deploy the following mechanisms to advertise a list of DNS Recursive DNS server(s) to their customers:

- Protocol Configuration Options in cellular networks [TS.24008].
- DHCPv4 [RFC2132] (Domain Name Server Option) or DHCPv6 [RFC8415][RFC3646] (OPTION_DNS_SERVERS).
- IPv6 Router Advertisement [RFC4861][RFC8106] (Type 25 (Recursive DNS Server Option)).

The communication between a customer's device (possibly via Customer Premises Equipment (CPE)) and an ISP-supplied DNS resolver takes place by using cleartext DNS messages (Do53). Some examples are depicted in Figure 13. In the case of cellular networks, the cellular network will provide connectivity directly to a host (e.g., smartphone, tablet) or via a CPE. Do53 mechanisms used within the Local Area Network (LAN) are similar in both fixed and cellular CPE-based broadband service offerings.

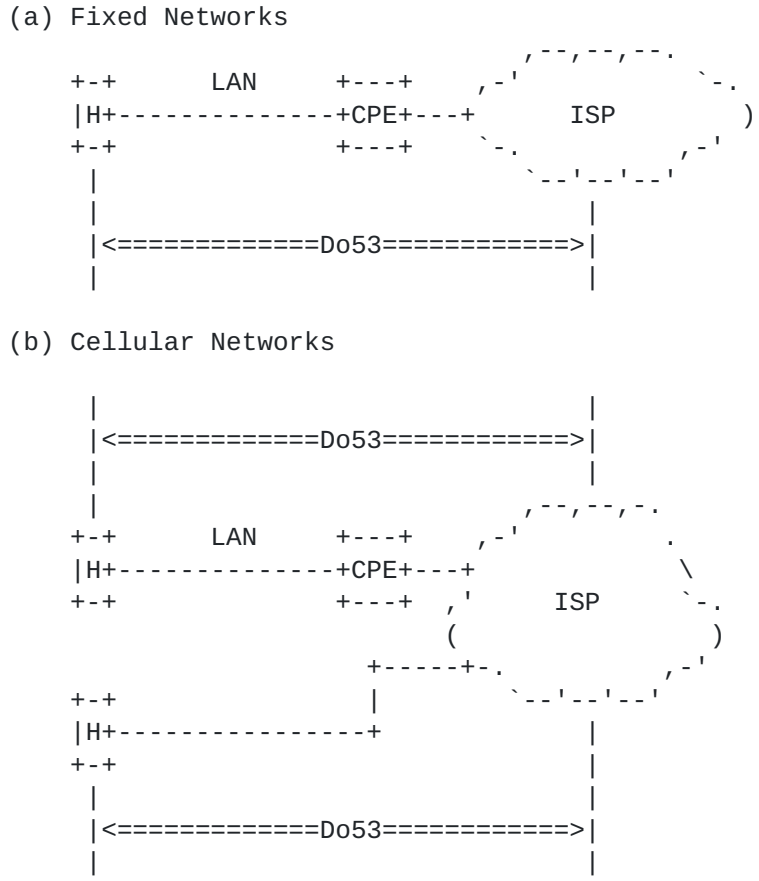


Figure 13: Sample Legacy Deployments

A.1. Managed CPEs

This section focuses on CPEs that are managed by ISPs.

A.1.1. Direct DNS

ISPs have developed an expertise in managing service-specific configuration information (e.g., CPE WAN Management Protocol [TR-069]). For example, these tools may be used to provision the DNS server's ADN to managed CPEs if an encrypted DNS is supported by a local network similar to what is depicted in Figure 14.

For example, DoH-capable (or DoT) clients establish the DoH (or DoT) session with the discovered DoH (or DoT) server.

The DNS client discovers whether the DNS server in the local network supports DoH/DoT/DoQ by using a dedicated field in the discovery message: Encrypted DNS Types (Sections 4, 5, and 6) .

(a) Fixed Networks

(b) Cellular Networks

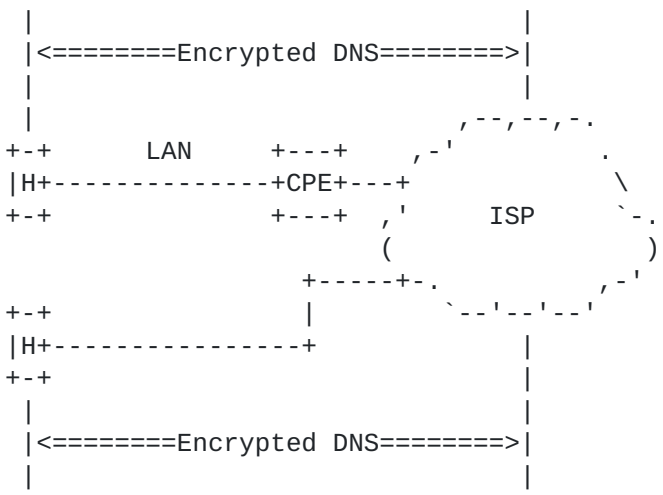


Figure 14: Encrypted DNS in the WAN

Figure 14 shows the scenario where the CPE relays the list of encrypted DNS servers it learns for the network by using mechanisms

like DHCP or a specific Router Advertisement message. In such context, direct encrypted DNS sessions will be established between a host serviced by a CPE and an ISP-supplied encrypted DNS server (see the example depicted in Figure 15 for a DoH/DoT-capable host).

Figure 15: Direct Encrypted DNS Sessions

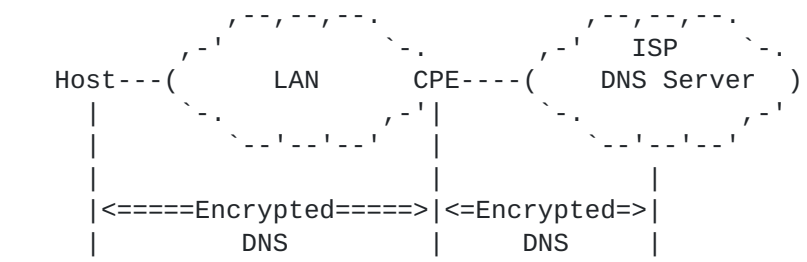
A.1.2. Proxied DNS

Figure 16 shows a deployment where the CPE embeds a caching DNS forwarder. The CPE advertises itself as the default DNS server to the hosts it serves. The CPE relies upon DHCP or RA to advertise itself to internal hosts as the default DoT/DoH/Do53 server. When receiving a DNS request it cannot handle locally, the CPE forwards the request to an upstream DoH/DoT/Do53 resolver. Such deployment is required for IPv4 service continuity purposes (e.g., Section 5.4.1 of [I-D.ietf-v6ops-rfc7084-bis]) or for supporting advanced services within a local network (e.g., malware filtering, parental control, Manufacturer Usage Description (MUD) [RFC8520] to only allow intended communications to and from an IoT device). When the CPE behaves as a DNS forwarder, DNS communications can be decomposed into two legs:

- The leg between an internal host and the CPE.
- The leg between the CPE and an upstream DNS resolver.

An ISP that offers encrypted DNS to its customers may enable encrypted DNS in one or both legs as shown in Figure 16. Additional considerations related to this deployment are discussed in Section 8.

(a)



(b)

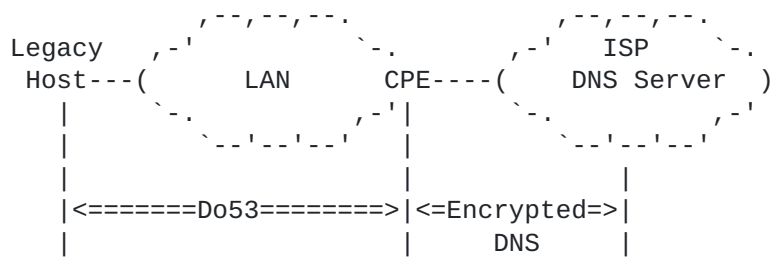


Figure 16: Proxied Encrypted DNS Sessions

A.2. Unmanaged CPEs

A.2.1. ISP-facing Unmanaged CPEs

Customers may decide to deploy unmanaged CPEs (assuming the CPE is compliant with the network access technical specification that is usually published by ISPs). Upon attachment to the network, an unmanaged CPE receives from the network its service configuration (including the DNS information) by means of, e.g., DHCP. That DNS information is shared within the LAN following the same mechanisms as those discussed in Appendix A.1. A host can thus establish DoH/DoT session with a DoH/DoT server similar to what is depicted in Figure 15 or Figure 16.

A.2.2. Internal Unmanaged CPEs

Customers may also decide to deploy internal routers (called hereafter, Internal CPEs) for a variety of reasons that are not detailed here. Absent any explicit configuration on the internal CPE to override the DNS configuration it receives from the ISP-supplied CPE, an Internal CPE relays the DNS information it receives via DHCP/RA from the ISP-supplied CPE to connected hosts. Encrypted DNS sessions can be established by a host with the DNS servers of the ISP (see Figure 17).

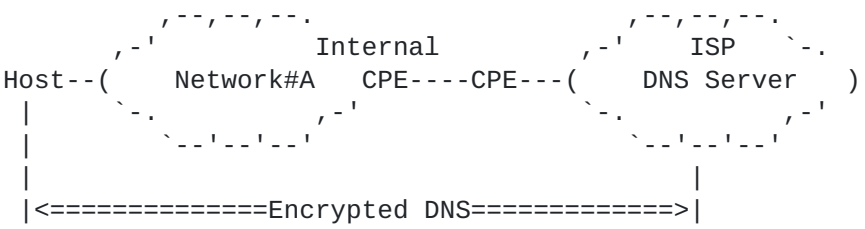


Figure 17: Direct Encrypted DNS Sessions with the ISP DNS Resolver (Internal CPE)

Similar to managed CPEs, a user may modify the default DNS configuration of an unmanaged CPE to use his/her favorite DNS servers instead. Encrypted DNS sessions can be established directly between a host and a 3rd Party DNS server (see Figure 18).

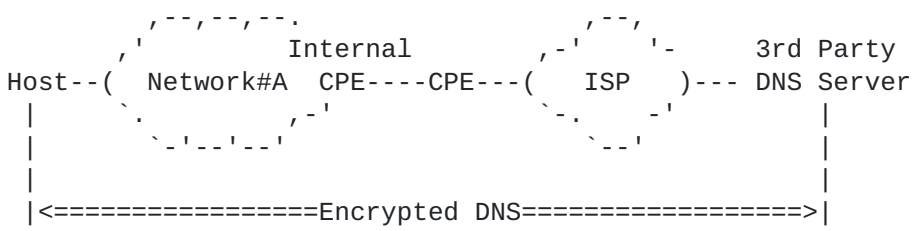


Figure 18: Direct Encrypted DNS Sessions with a Third Party DNS Resolver

Section 8.2 discusses considerations related to hosting a forwarder in the Internal CPE.

Appendix B. Make Use of Discovered Encrypted DNS Servers

Even if the use of a discovered encrypted DNS server is beyond the discovery process and falls under encrypted server selection, the following discusses typical conditions under which discovered encrypted DNS server can be used.

- If the DNS server's IP address discovered by using DHCP/RA is preconfigured in the OS or Browser as a verified resolver (e.g., part of an auto-upgrade program such as [Auto-upgrade]), the DNS client auto-upgrades to use the preconfigured encrypted DNS server tied to the discovered DNS server IP address. In such a case the DNS client will perform additional checks out of band, such as confirming that the Do53 IP address and the encrypted DNS server are owned and operated by the same organisation.

- Similarly, if the ADN conveyed in DHCP/RA (Sections 4, 5, and 6) is preconfigured in the OS or browser as a verified resolver, the

DNS client auto-upgrades to establish an encrypted a DoH/DoT/DoQ session with the ADN.

In such case, the DNS client matches the domain name in the Encrypted DNS DHCP/RA option with the 'DNS-ID' identifier type within subjectAltName entry in the server certificate conveyed in the TLS handshake.

Authors' Addresses

Mohamed Boucadair
Orange
Rennes 35000
France

Email: mohamed.boucadair@orange.com

Tirumaleswar Reddy
McAfee, Inc.
Embassy Golf Link Business Park
Bangalore, Karnataka 560071
India

Email: TirumaleswarReddy_Konda@McAfee.com

Dan Wing
Citrix Systems, Inc.
USA

Email: dwing-ietf@fuggles.com

Neil Cook
Open-Xchange
UK

Email: neil.cook@noware.co.uk

Tommy Jensen
Microsoft
USA

Email: tojens@microsoft.com