ADD M. Boucadair
Internet-Draft Orange
Intended status: Standards Track T. Reddy
Expires: November 16, 2020 McAfee
D. Wing
Citrix
N. Cook
Open-Xchange
May 15, 2020

Encrypted DNS Discovery and Deployment Considerations for Home Networks

draft-btw-add-home-06

Abstract

This document discusses DoT/DoH deployment considerations for home networks. It particularly sketches the required steps to use DoT/DoH capabilities provided by local networks.

The document specifies new DHCP and Router Advertisement Options to convey a DNS Authentication Domain Name.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction 2
2. Terminology 4
3. Sample Deployment Scenarios 5
3.1. Managed CPEs 5
3.2. Unmanaged CPEs 7
4. DNS Reference Identifier Option 8
4.1. DHCPv6 DNS Reference Identifier Option 9
4.2. DHCP DNS Reference Identifier Option 11
4.3. RA DNS Reference Identifier Option 12
5. DoH URI Templates 13
6. Locating DoH/DoT Servers 13
6.1. DoT/DoH Auto-Upgrade 14
6.2. Other Deployment Options 14
7. Hosting DoH/DoT Forwarder in the CPE 15
7.1. Managed CPEs 15
7.1.1. ACME 15
7.1.2. Auto-Upgrade based on Domains and their Sub-domains . 15
7.2. Unmanaged CPEs 16
8. Legacy CPEs 17
9. Security Considerations 17
10. IANA Considerations 18

10.1. DHCPv6 Option 18
10.2. DHCP Option 19
10.3. RA Option 19
11. Acknowledgements 19
12. References 20
12.1. Normative References 20
12.2. Informative References 21
Authors' Addresses 23

1. Introduction

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

o Protocol Configuration Options in cellular networks [TS.24008].

- o DHCP [RFC2132] (Domain Name Server Option) or DHCPv6 [RFC8415][RFC3646] (OPTION_DNS_SERVERS).
- o 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, [I-D.ietf-dnsop-terminology-ter]). Some examples are depicted in Figure 1. 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.

```
           (a) Fixed Networks
                      ,--,--,--.             ,--,--,--.
                   ,-'   +--+  `-.       ,-'   ISP    `-.
                  ( LAN  |H |    CPE----(                 )
                   `-.   +--+   ,-'       `-.          ,-'
                      `--'|-'--'             `--'--'--'
                          |                     |
                          |<=======Do53========>|

           (b) Cellular Networks
                           |<===========Do53=========>|
                      ,--,-|,--.                      |
                   ,-'   +--+   `-.               ,--,--,--.
                  ( LAN  |H |     CPE------------+          \
                   `-.   +--+   ,-'            ,'   ISP     `-.
                      `--'--'--'              (                )
                                         +-----+-.          ,-'
                         +--+            |        `--'--'--'
                         |H +------------+
                         +--+
           Legend:
            * H: refers to a host.
```

Figure 1: Sample Legacy Deployments

ISPs use DNS to provide additional services such as (but not limited to) malware filtering, parental control, or VoD (Video on Demand) optimization. DNS is also a central component for mastering the quality of experience for current latency-sensitive services, but also emerging ones (such as those services that pertain to the Ultra Reliability and Low Latency Communications (uRLLC) or Enhanced Mobile Broadband (eMBB).

For example, the latency targets set in the context of 5G are 1ms (uRLLC) and 4ms (eMBB). An ISP will be able to address such demanding latency requirements assuming the corresponding services rely upon resources (network, compute, storage) that are located as close to the user as possible (e.g., by means of Edge Computing techniques and resources). Such latency requirements are likely to be addressed by means of optimized designs (DNS, in particular), too.

Relying upon local DNS resolvers will therefore contribute to meet the aforementioned service requirements. The use of external resolvers is likely to induce an extra service delay which exceeds by far the service target.

This document focuses on the support of DNS-over-HTTPS (DoH) [RFC8484] or DNS-over-TLS (DoT) [RFC7858] in local networks. In particular, the document describes how a local DoH/DoT server can be discovered and used by connected hosts. This document specifies options that allow DNS clients to discover local DoT/DoH servers. Section 4 describes DHCP, DHCPv6, and RA options to convey the Authentication Domain Name (ADN, defined in [RFC8310]).

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 the same mechanisms listed above. 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.

Both managed and unmanaged CPEs are discussed in the document (Section 3). Also, considerations related to hosting a DNS forwarder in the CPE are described (Section 7).

Hosts and/or CPEs 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.

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] and [I-D.ietf-dnsop-terminology-ter].

Do53 refers to unencrypted DNS.

'DoH/DoT' refers to DNS-over-HTTPS and/or DNS-over-TLS.

3. Sample Deployment Scenarios

3.1. Managed CPEs

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 authentication domain name information (ADN) to managed CPEs if DoH/DoT is supported by a local network similar to what is depicted in Figure 2.

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 by using a dedicated field in the discovery message:
Encrypted DNS Types (Section 4).

```
           (a) Fixed Networks

                      ,--,--,--.             ,--,--,--.
                   ,-'   +--+  `-.       ,-'   ISP    `-.
                  ( LAN  |H |    CPE----(    DNS Server  )
                   `-.   +--+   ,-'       `-.          ,-'
                      `--'|-'--'             `--'--'--'
                          |                     |
                          |<=======DoH/DoT=====>|


           (b) Cellular Networks

                           |<===========DoH/DoT======>|
                      ,--,-|,--.                      |
                   ,-'   +--+    `-.                ,--,--,--.
                  ( LAN  |H |     CPE---------------+          \
                   `-.   +--+    ,-'             ,'   ISP     `-.
                      `--'--'--'                (    DNS Server  )
                                         +-----+-.           ,-'
                          +--+           |          `--'--'--'
                          |H +-----------+
                          +--+
```

Figure 2: DoH/DoT in the WAN

Figure 2 shows the scenario where the CPE relays the list of DoT/DoH servers it learns for the network by using mechanisms like DHCP or a specific Router Advertisement message. In such context, direct DoH/DoT sessions will be established between a host serviced by a CPE and an ISP-supplied DoT/DoH server (see the example depicted in Figure 3 for a DoH/DoT-capable host).

```
                         ,--,--,--.             ,--,--,--.
                      ,-'           `-.       ,-'   ISP    `-.
              Host---(      LAN      CPE----(    DNS Server  )
                |     `-.           ,-'       `-.          ,-'
                |        `--'--'--'             `--'--'--'
                |                                    |
                |<==============DoT/DoH=============>|
```

Figure 3: Direct DoH/DoT Sessions

Figure 4 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., [I-D.ietf-v6ops-rfc7084-bis]) or for supporting advanced services within the home (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:

o The leg between an internal host and the CPE.

o The leg between the CPE and an upstream DNS resolver.

An ISP that offers DoH/DoT to its customers may enable DoH/DoT in both legs as shown in Figure 4. Additional considerations related to this deployment are discussed in Section 7.

```
                 ,--,--,--.             ,--,--,--.
              ,-'          `-.       ,-'   ISP    `-.
       Host---(      LAN      CPE----(    DNS Server  )
         |     `-.          ,-'|       `-.          ,-'
         |        `--'--'--'   |          `--'--'--'
         |                     |             |
         |<======DoT/DoH======>|<==DoT/DoH==>|
```

Figure 4: Proxied DoH/DoT Sessions

3.2. 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 Section 3.1. A host can thus establish DoH/DoT session with a DoH/DoT server similar to what is depicted in Figure 3.

Customers may also decide to deploy internal home 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. DoH/DoT sessions can be established by a host with the DoH/DoT servers of the ISP

(see
Figure 5).

```
                   ,--,--,--.                    ,--,--,--.
                ,-'          Internal         ,-'    ISP   `-.
         Host--(    Network#A   CPE----CPE---(    DNS Server   )
          |     `-.          ,-'              `-.           ,-'
          |        `--'--'--'                    `--'--'--'
          |                                          |
          |<==================DoT/DoH=============>|
```

Figure 5: Direct DoH/DoT 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. DoH/DoT sessions can be established directly between a
host
and a 3rd Party DNS server (see Figure 6).

```
                ,--,--,--.                 ,--,
              ,'         Internal        ,-'    '-     3rd Party
       Host--(  Network#A  CPE----CPE---(   ISP   )--- DNS Server
        |     `.          ,-'            `-.    -'          |
        |       `-'--'--'                   `--'            |
        |                                                   |
        |<====================DoT/DoH==================>|
```

Figure 6: Direct DoH/DoT Sessions with a Third Party DNS Resolver

Section 7.2 discusses considerations related to hosting a forwarder
in the Internal CPE.

4. DNS Reference Identifier Option

This section describes how a DNS client can discover the ADN of
local
DoH/DoT server(s) using DHCP (Sections 4.1 and 4.2) and Neighbor
Discovery protocol (Section 4.3).

As reported in Section 1.7.2 of [RFC6125]:

> "few 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 a DoH/DoT 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.

The DNS client establishes a DoH/DoT session with the discovered DNS IP address(es) (Section 6) and uses the mechanism discussed in Section 8 of [RFC8310] to authenticate the DNS server certificate using the authentication domain name conveyed in the DNS Reference Identifier.

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

4.1. DHCPv6 DNS Reference Identifier Option

The DHCPv6 DNS Reference Identifier option is used to configure an authentication domain name of the DoH/DoT server. The format of this option is shown in Figure 7.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     OPTION_V6_DNS_RI          |         Option-length         |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    | Encr DNS Types|                                               |
    +-+-------------+                                               |
    |                                                               |
    ~                 Authentication Domain Name                    ~
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 7: DHCPv6 DNS Reference Identifier Option

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

- o Option-code: OPTION_V6_DNS_RI (TBA1, see Section 10.1)
- o Option-length: Length of the enclosed data in octets.
- o Encr DNS Types (Encrypted DNS Types): Indicates the type(s) of the encrypted DNS server conveyed in this attribute. The format of this 8-bit field is shown in Figure 8.

```
                      +-+-+-+-+-+-+-+-+
                      |U|U|U|U|U|U|H|T|
                      +-+-+-+-+-+-+-+-+
```

Figure 8: Encrypted DNS Types

T: If set, this bit indicates that the server supports DoT [RFC7858].
H: If set, this bit indicates that the server supports DoH [RFC8484].

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

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 DoTand the server supports both, then both T and H bits must be set.

o Authentication Domain Name: A fully qualified domain name of the DoH/DoT server. This field is formatted as specified in Section 10 of [RFC8415].

An example of the Authentication Domain Name encoding is shown in Figure 9. This example conveys the FQDN "doh1.example.com.".

```
        +------+------+------+------+------+------+------+------+------+
        | 0x04 |   d  |   o  |   h  |  1   | 0x07 |   e  |   x  |   a  |
        +------+------+------+------+------+------+------+------+------+
        |   m  |   p  |   l  |   e  | 0x03 |   c  |   o  |   m  | 0x00 |
        +------+------+------+------+------+------+------+------+------+
```

Figure 9: An example of the authentication-domain-name Encoding

Multiple instances of OPTION_V6_DNS_RI may be returned to a DHCPv6 client; each pointing to a distinct encrypted DNS server type.

To discover an encrypted DNS server, the DHCPv6 client including OPTION_V6_DNS_RI 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 DHCP OPTION_V6_DNS_RI options; each option is to be treated as a separate encrypted DNS server.

4.2. DHCP DNS Reference Identifier Option

The DHCP DNS Reference Identifier option is used to configure an authentication domain name of the DoH/DoT server. The format of this option is illustrated in Figure 10.

```
            0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
           +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           |     TBA2      |     Length    |
           +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           | Encr DNS Types|               |
           +-+-+-+-+-+-+-+-+               |
           |                               |
           ~  Authentication Domain Name   ~
           |                               |
           +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

  with:

            Authentication Domain Name
           +-----+-----+-----+-----+-----+--
           |  s1 |  s2 |  s3 |  s4 | s5  |  ...
           +-----+-----+-----+-----+-----+--

     The values s1, s2, s3, etc. represent the domain name labels in the
     domain name encoding.
```

Figure 10: DHCP DNS Reference Identifier Option

The fields of the option shown in Figure 10 are as follows:

- o Code: OPTION_V4_DNS_RI (TBA2, see Section 10.2).
- o Length: Length of the enclosed data in octets.
- o Encr DNS Types (Encrypted DNS Types): Indicates the type(s) of the encrypted DNS server conveyed in this attribute. The format of this field is shown in Figure 8.
- o Authentication Domain Name: The domain name of the DoH/DoT server. This field is formatted as specified in Section 10 of [RFC8415].

OPTION_V4_DNS_RI is a concatenation-requiring option. As such, the mechanism specified in [RFC3396] MUST be used if OPTION_V4_DNS_RI exceeds the maximum DHCP option size of 255 octets.

To discover an encrypted DNS server, the DHCP client requests the Encrypted DNS Reference Identifier by including OPTION_V4_DNS_RI in a Parameter Request List option [RFC2132]. The DHCP client sets the

Encrypted DNS Types field to the requested encrypted DNS server.

   If the DHCP client requested more than one encrypted DNS server
type,
   the DHCP client MUST be prepared to receive multiple DHCP
   OPTION_V4_DNS_RI options; each option is to be treated as a separate
   encrypted DNS server.

4.3. RA DNS Reference Identifier Option

   The IPv6 Router Advertisement (RA) DNS Reference Identifier option
is
   used to configure an authentication domain name of the DoH/DoT
   server. The format of this option is illustrated in Figure 11.

```
        0                   1                   2                   3
        0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
+
       |     Type      |     Length    | Encr DNS Types|   Unassigned
|
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
+
       |                           Lifetime
|
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
+
       |
|
       :                  Authentication Domain
Name                  :
       |
|
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
+
```

               Figure 11: RA DNS Reference Identifier Option

   The fields of the option shown in Figure 11 are as follows:

   o Type: 8-bit identifier of the DNS Reference Identifier Option as
      assigned by IANA (TBA3, see Section 10.3).
   o Length: 8-bit unsigned integer. The length of the option
      (including the Type and Length fields) is in units of 8 octets.
   o Encr DNS Types (Encrypted DNS Types): Indicates the type(s) of
the
      encrypted DNS server conveyed in this attribute. The format of
      this field is shown in Figure 8.
   o Unassigned: This field is unused. It MUST be initialized to zero
      by the sender and MUST be ignored by the receiver.
   o Lifetime: 32-bit unsigned integer. The maximum time in seconds
      (relative to the time the packet is received) over which the
      authentication domain name MAY be used as a DNS Reference
      Identifier.

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 the DNS Reference Identifier MUST no longer be used.

o Authentication Domain Name: The domain name of the DoH/DoT 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.

5. DoH URI Templates

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

Upon discovery of a DoH resolver (Section 4), the DoH client contacts that DoH resolver to retrieve the list of supported DoH services using the RESINFO RRtype [I-D.pp-add-resinfo]. DoH clients re-iterates that request regularly to retrieve an updated list of supported DoH services. Note that a "push" mode can be considered using the mechanism defined in [I-D.ietf-dnssd-push].

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

6. Locating DoH/DoT Servers

A CPE or a host relies upon discovery mechanisms (such as PCO, DHCP, or RA) to retrieve DoH/DoT servers' reachability information. In the various scenarios sketched in Section 3, Do53, DoH, and DoT may terminate on the same IP address or distinct IP addresses. Terminating Do53/DoH/DoT on the same or distinct IP addresses is deployment-specific.

From an IP reachability standpoint, DoH/DoT servers SHOULD be located by their address literals rather than their names. This avoids adding a dependency on another server to resolve the DoH/DoT name. Concretely, if Do53/DoH/DoT terminate on same IP addresses, existing discovery mechanisms [RFC2132][RFC3646][RFC8106] can be leveraged to learn the IP addresses of DoT/DoH servers while an authentication domain name is supplied by one of the options discussed in Section 4.

The following sub-sections discusses the conditions under which discovered DoT/DoH server can be used.

6.1. DoT/DoH Auto-Upgrade

Additional considerations are discussed below for the use of DoH and DoT servers provided by local networks:

o If the DNS server's IP address discovered by using DHCP/RA is pre-configured 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 pre-configured DoH/DoT 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 DoH server are owned and operated by the same organisation.

o Similarly, if the ADN conveyed in DHCP/RA (Section 4) is pre-configured in the OS or browser as a verified resolver, the DNS client auto-upgrades to establish a DoH/DoT session with the ADN.

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

6.2. Other Deployment Options

Some deployment options to securely configure hosts are discussed below. These options are provided for the sake of completeness.

o If Device Provisioning Protocol (DPP) [DPP] is used, the configurator can securely configure devices in the home network with the local DoT/DoH server using DPP. If the DoT/DoH servers use raw public keys [RFC7250], the Subject Public Key Info (SPKI) pin set [RFC7250] of raw public keys may be encoded in a QR code. The configurator (e.g., mobile device) can scan the QR code and provision SPKI pin set in OS/Browser. The configurator can in-turn securely configure devices (e.g., thermostat) in the home network with the SPKI pin set using DPP.

o If a CPE is co-located with security services within the home network, the CPE can use WPA-PSK but with unique pre-shared keys for different endpoints to deal with security issues. In such networks, [I-D.reddy-add-iot-byod-bootstrap] may be used to securely bootstrap endpoint devices with the authentication domain name and DNS server certificate of the local network's DoH/DoT server.

The OS would not know if the WPA pre-shared-key is the same for all clients or a unique pre-shared key is assigned to the host.

Hence, the user has to indicate to the system that a unique pre-shared key is assigned to trigger the bootstrapping procedure.

If the device joins a home network using a single shared password among all the attached devices, a compromised device can host a fake access point, and the device cannot be securely bootstrapped with the home network's DoH/DoT server.

7. Hosting DoH/DoT Forwarder in the CPE

7.1. Managed CPEs

The following mechanisms can be used to host a DoH/DoT forwarder in a managed CPE (Section 3.1).

7.1.1. ACME

The ISP can assign a unique FQDN (e.g., cpe1.example.com) and a domain-validated public certificate to the DoH/DoT 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.

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.

7.1.2. Auto-Upgrade based on Domains and their Sub-domains

If the ADN conveyed in DHCP/RA (Section 4) is pre-configured in popular OSes or browsers as a verified resolver and the auto-upgrade (Section 6.1) is allowed for both the pre-configured ADN and its sub-domains, the DoH/DoT client will learn the local DoH/DoT forwarder using DHCP/RA and auto-upgrade because the left-most label of the pre-configured ADN would match the subjectAltName value in the server certificate. Concretely, the CPE can communicate the ADN of the local DoH forwarder (Section 7.1.1) to internal hosts using DHCP/RA (Section 4).

Let's suppose that "example.net" is pre-configured as a verified resolved in the browser or OS. If the DoH/DoT client discovers a local forwarder "cpe1-internal.example.net", the DoH/DoT client will auto-upgrade because the pre-configured ADN would match subjectAltName value "cpe1-internal.example.net" of type dNSName. As

shown in Figure 12, the auto-upgrade to a rogue server advertising "rs.example.org" will fail.

```
                            Rogue Server
                |              |
                X<==DHCP=======|
                | {ADN=        |
                |  rs.example.org, @rs}
                |              |                  --,--,-
                |        ,+-,--+--.             ,/  ISP   \.
                |     ,-'          `-.       ,-'            `-.
            DoH/DoT --(      LAN      CPE----( S (@1)          )
       capable client  `-.          ,-'|       `-.          ,-'
                |        `--'--'--'    |         `--'--'--'
                |<========DHCP========>|
                |{ADN=                 |
                |  cpe1-internal.example.net, @i}
                |
                |<========DoH=========>|
                |                      |
```

Legend:
  * S: DoH/DoT server
  * @1: IP address of S
  * @i: internal IP address of the CPE
  * @rs: IP address of a rogue server

Figure 12: A Simplified Example of Auto-upgrade based on Sub-domains

7.2. Unmanaged CPEs

The approach specified in Section 7.1 does not apply for hosting a DNS forwarder in an unmanaged CPE.

The unmanaged CPE administrator (referred to as administrator) can host a DoH/DoT forwarder on the unmanaged CPE. This assumes the following:

o The DoH/DoT server certificate is managed by the entity in-charge of hosting the DoT/DoH forwarder.

   Alternatively, a security service provider can assign a unique FQDN to the CPE. The DoH/DoT forwarder will act like a private DoT/DoH server only be accessible from within the home network.

o The DoH/DoT forwarder will either be configured to use the ISP's or a 3rd party DoH/DoT server.

o The unmanaged CPE will advertise the DoH/DoT forwarder ADN using
   DHCP/RA to internal hosts.

Figure 13 illustrates an example of an unmanaged CPE hosting a forwarder which connects to a 3rd party DoH/DoT 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.

```
              ,--,--,--.                         ,--,
            ,'         Internal   Managed     ,-'    '-     3rd Party
     Host--(  Network#A  CPE--------CPE------(   ISP   )--- DNS Server
      |     `.         ,-'|          |        `-.    -'       |
      |       `-'--'--'   |          |<==DHCP==>|`--'         |
      |                   |<==DHCP==>|          |             |
      |<======DHCP=======>|          |                        |
      |     {RI, @i}      |                                   |
      |<=====DoT/DoH=====>|<=============DoT/DoH=============>|
```

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

Figure 13: Example of an Internal CPE Hosting a Forwarder

8. Legacy CPEs

Hosts serviced by legacy CPEs that can't be upgraded to support the options defined in Section 4 won't be able to learn the DoH/DoT server hosted by the ISP, in particular. Such hosts will have to fallback to use the special-use domain name defined in [I-D.pp-add-resinfo] to discover the DoH/DoT server.

9. Security Considerations

An attacker can get a domain name, domain-validated public certificate from a CA, host a DoT/DoH server and claim the best DNS privacy preservation policy. Also, an attacker within the home network can use the public IP address, get an 'IP address'-validated public certificate from a CA, host a DoT/DoH server and claim the best DNS privacy preservation policy.

Because DHCP/RA messages are not encrypted or protected against modification in any way, their content can be spoofed or modified by compromised devices within the home network. An attacker can spoof the DHCP/RA response to provide the attacker's DoT/DoH server. Note that such an attacker can launch other attacks as discussed in Section 22 of [RFC8415]. Furthermore, if the browser or the OS is

pre-configured with a list of DNS servers and some of which perform malware filtering while others do not, an attacker can prevent contacting the preferred filtering DNS servers causing a downgrade attack to a non-filtering DNS server, which the attacker can leverage to deliver malware.

The use of DoH/DoT also depends on the user's policies. For example, the user may indicate his/her consent to use (or not) the locally-discovered DoH/DoT server or request to review human-readable privacy policy information of a selected DNS server and to assess whether that DNS server performs DNS-based content filtering (e.g., [I-D.reddy-add-server-policy-selection]). The DNS client is assumed to adhere to these policies. This document does not make any assumption about the structure of such policies nor mandates specific requirements. Such policies and their handling is out of scope.

DoH/DoT servers discovered using insecure discovery mechanisms like DHCP/RA are used by a DNS client if the insecurely discovered DoH/DoT server is pre-configured in the OS or the browser. Section 6.1 identifies a set of deployment options under which DHCP/RA RI options can be used.

If the insecurely discovered DoH/DoT server is not pre-configured in the OS or browser, the client may validate the signatory (e.g., cryptographically attested by the ISP). However, as discussed above, the use of policies to select servers is out of scope of this document.

DoT/DoH sessions with rogue servers spoofing 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] based upon the authentication domain name in the Reference Identifier 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).

TCP connections received outside the home network MUST be discarded by the DoH/DoT forwarder in the CPE. This behavior adheres to REQ#8 in [RFC6092]; it MUST apply for both IPv4 and IPv6.

10. IANA Considerations

10.1. DHCPv6 Option

IANA is requested to assign the following new DHCPv6 Option Code in the registry maintained in: https://www.iana.org/assignments/dhcpv6-parameters/dhcpv6-parameters.xhtml#dhcpv6-parameters-2.

Value	Description	Client ORO	Singleton Option	Reference
TBA1	OPTION_V6_DNS_RI	Yes	Yes	[ThisDocument]

10.2. DHCP Option

IANA is requested to assign the following new DHCP Option Code in the registry maintained in: https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml#options.

Tag	Name	Data Length	Meaning	Reference
TBA2	OPTION_V4_DNS_RI	N	DoT/DoH server authentication domain name	[ThisDocument]

10.3. RA 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 http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml#icmpv6-parameters-5.

Type	Description	Reference
TBA3	DNS Reference Identifier Option	[ThisDocument]

11. Acknowledgements

Many thanks to Christian Jacquenet for the review.

Thanks to Tommy Jensen, Stephen Farrell, Martin Thomson, Vittorio Bertola, and Iain Sharp for the comments.

Thanks to Mark Nottingham for the feedback on HTTP redirection.

12. References

12.1. 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>.

[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>.

[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>.

[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>.

[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>.

[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>.

12.2. Informative References

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

[DPP] The Wi-Fi Alliance, "Device Provisioning Protocol Specification", <https://www.wi-fi.org/file/device-provisioning-protocol-specification>.

[I-D.ietf-dnsop-terminology-ter]
Hoffman, P., "Terminology for DNS Transports and Location", draft-ietf-dnsop-terminology-ter-01 (work in progress), February 2020.

[I-D.ietf-dnssd-push]
Pusateri, T. and S. Cheshire, "DNS Push Notifications", draft-ietf-dnssd-push-25 (work in progress), October 2019.

[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.pp-add-resinfo]
Sood, P. and P. Hoffman, "DNS Resolver Information Self-publication", draft-pp-add-resinfo-01 (work in progress), May 2020.

[I-D.reddy-add-iot-byod-bootstrap]
Reddy.K, T., Wing, D., Richardson, M., and M. Boucadair, "A Bootstrapping Procedure to Discover and Authenticate DNS-over-TLS and DNS-over-HTTPS Servers for IoT and BYOD Devices", draft-reddy-add-iot-byod-bootstrap-00 (work in progress), May 2020.

[I-D.reddy-add-server-policy-selection]
Reddy.K, T., Wing, D., Richardson, M., and M. Boucadair, "DNS Server Selection: DNS Server Information with Assertion Token", draft-reddy-add-server-policy-selection-01 (work in progress), April 2020.

[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>.

[RFC7250] Wouters, P., Ed., Tschofenig, H., Ed., Gilmore, J., Weiler, S., and T. Kivinen, "Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", RFC 7250, DOI 10.17487/RFC7250, June 2014, <https://www.rfc-editor.org/info/rfc7250>.

[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>.

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