ADD   M. Boucadair
Internet-Draft   Orange
Intended status: Standards Track   T. Reddy
Expires: September 10, 2020   McAfee
                                                              D. Wing
                                                               Citrix
                                                              N. Cook
                                                         Open-Xchange
                                                        March 9, 2020

DNS-over-HTTPS and DNS-over-TLS Server Discovery and Deployment Considerations for Home and Mobile Networks
draft-btw-add-home-02

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.

   One of the goals of this document is to assess to what extent
   existing tools can be used to provide a DoT/DoH service. As an
   outcome, new DHCP and Router Advertisement Options are specified in
   order to convey a DNS Authentication Domain Name.

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 September 10, 2020.

Copyright Notice

Table of Contents

[1](#). Introduction

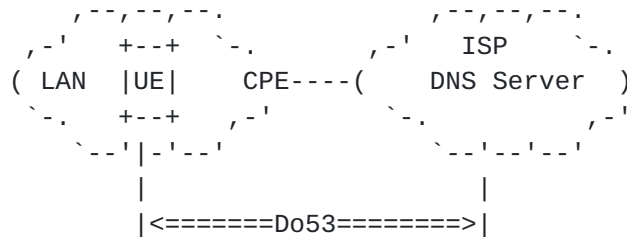   Internet Service Providers (ISPs) traditionally provide DNS resolvers
   to their customers. Typically, ISPs deploy the following mechanisms
   to advertise a list of DNS Recursive DNS server(s) to their
   customers:

   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 (a.k.a., User Equipment
(UE)) (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, connectivity can be
provided to a UE or to 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  |UE|     CPE----(      DNS Server  )
        `-.    +--+    ,-'          `-.             ,-'
          `--'|-'--'                  `--'--'--'
              |                           |
              |<=======Do53========>|


       (b) Cellular Networks


             |<===========Do53=========>|
         ,--,-|,--.                      |
       ,-'    +--+    `-.                ,--,--,--.
      ( LAN  |UE|     CPE-----------+          \
       `-.    +--+    ,-'               ,'   ISP     `-.
         `--'--'--'                    (     DNS Server  )
                         +-----+-.         ,-'
          +--+           |       `--'--'--'
          |UE+-----------+
          +--+
```
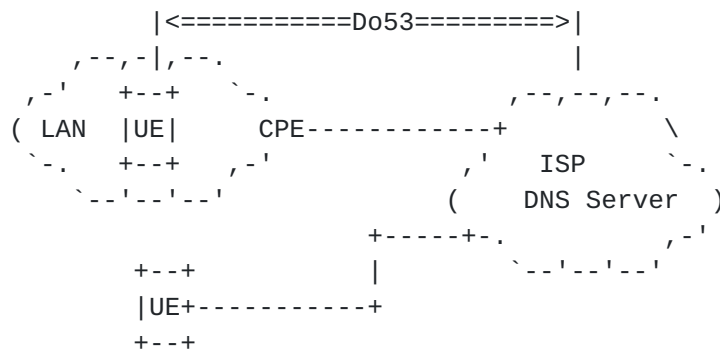
                Figure 1: Sample Legacy Deployments

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. In
particular, 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.

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].

'DoH/DoT' refers to DNS-over-HTTPS and/or DNS-over-TLS.
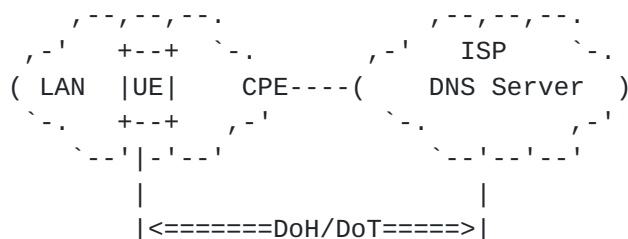
3. Sample Deployment Scenarios

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 DoH) clients establish the DoH (or DoT) session with
the discovered DNS server.

If a DNS client supports both DoT and DoH, the client try to
establish DoH/DoT sessions with the discovered DNS server to
determine whether these servers support DoH and/or DoT (Section 5).
Alternatively, the DNS client may discover whether the DNS server in
the local network supports DoH/DoT by using the mechanism discussed
in Section 6.

```
       (a) Fixed Networks


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


       (b) Cellular Networks


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

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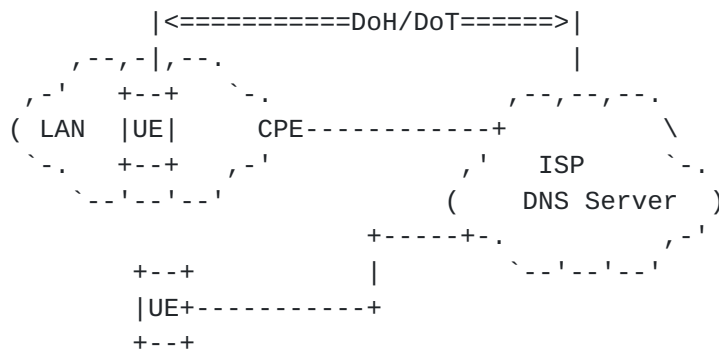
Figure 2 shows the scenario where the CPE relays the list of DoT/DoH
servers it learns for the network by using mechanisms like DHCP or a
specific Router Advertisement message. In such context, direct DoH/
DoT sessions will be established between a host serviced by a CPE and
an ISP-supplied DoT/DoH server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

```
           ,--,--,--.                    ,--,--,--.
        ,-'          `-.            ,-'   ISP     `-.
   UE----(      LAN      CPE----(     DNS Server   )
     |     `-.        ,-'       `-.            ,-'
     |        `--'--'--'           `--'--'--'
     |                                    |
     |<=============DoT/DoH============>|
```
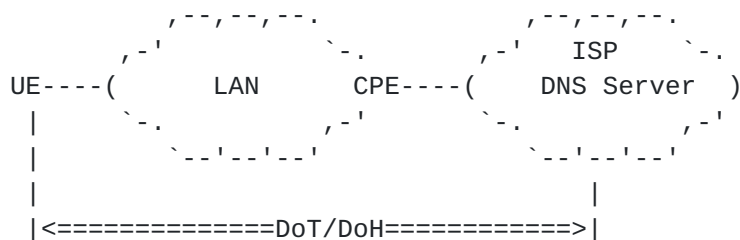
                  Figure 3: Direct DoH/DoT Sessions

   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     `-.
   UE----(      LAN      CPE----(     DNS Server   )
     |     `-.        ,-'|       `-.            ,-'
     |        `--'--'--'   |       `--'--'--'
     |                     |           |
     |<======DoT/DoH======>|<==DoT/DoH==>|
```
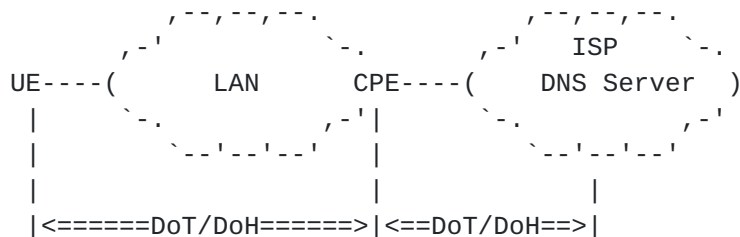
                  Figure 4: Proxied DoH/DoT Sessions

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 5) 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 5.

```
 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         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                  Authentication Domain Name                   |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
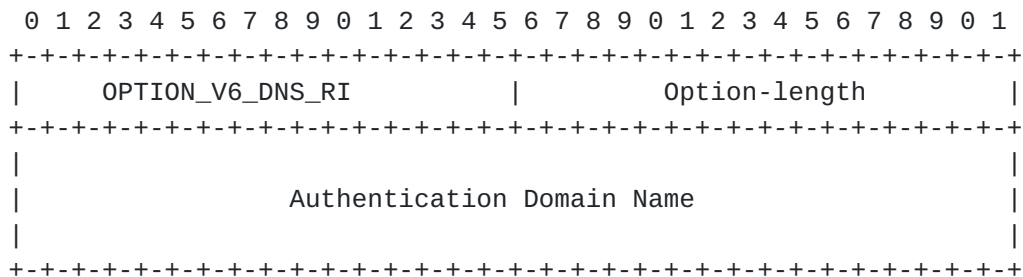
Figure 5: DHCPv6 DNS Reference Identifier Option

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

o Option-code: OPTION_V6_DNS_RI (TBA1, see Section 9.1)
o Option-length: Length of the Authentication Domain Name field in
   octets.

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 6. 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 6: An example of the authentication-domain-name Encoding

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 7.

```
     Code  Length   Authentication Domain Name
    +-----+-----+-----+-----+-----+-----+-----+--
    |TBA2 |  n  |  s1 |  s2 |  s3 |  s4 | s5  |  ...
    +-----+-----+-----+-----+-----+-----+-----+--
```

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

        Figure 7: DHCP DNS Reference Identifier Option

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

o Code: OPTION_V4_DNS_RI (TBA2, see Section 9.2).
o Length: Includes the length of the Authentication Domain Name
   field in octets.
o Authentication Domain Name: The domain name of the DoH/DoT server.
   This field is formatted as specified in Section 10 of [RFC8415].

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 8.

```
 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     |            Reserved           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            Lifetime                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
:                   Authentication Domain Name                  :
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

              Figure 8: RA DNS Reference Identifier Option

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

   o Type: 8-bit identifier of the DNS Reference Identifier Option as
      assigned by IANA (TBA3, see Section 9.3).
   o Length: 8-bit unsigned integer. The length of the option
      (including the Type and Length fields) is in units of 8 octets.
   o Reserved: 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].

5. 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 as
   depicted in Figure 10). 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
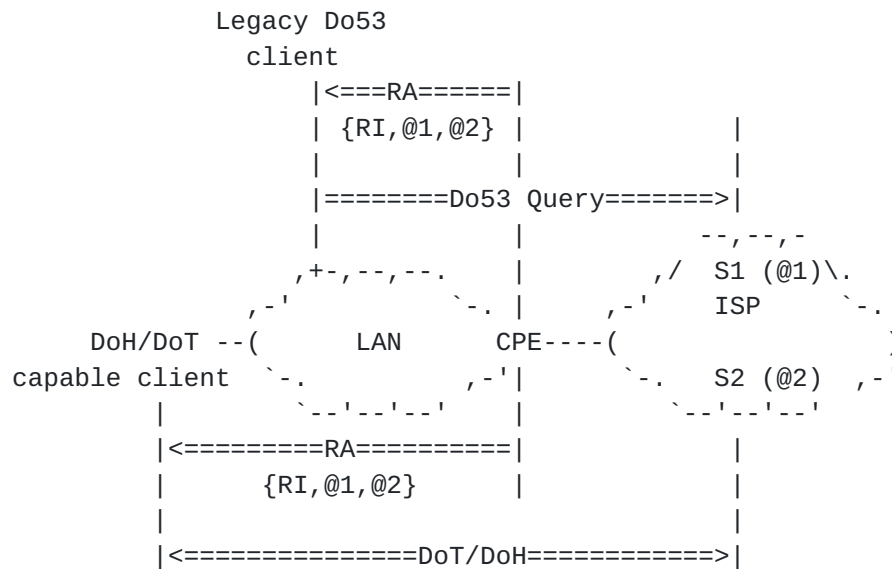domain name is supplied by one of the options discussed in Section 4.
An example is depicted in Figure 9.

```
                  Legacy Do53
                    client
                      |<===DHCP===>|
                      |    {@1}     |        |
                      |             |        |
                      |======Do53 Query===>|
                      |             |        |    --,--,-
                    ,+-,--,--.      |        |,/   ISP   \.
                 ,-'          `-. |      ,-'           `-.
         DoH/DoT --(       LAN      CPE----( S (@1)          )
     capable client  `-.          ,-'|       `-.          ,-'
             |          `--'--'--'     |        | `--'--'--'
             |<=======DHCP=======>|        |
             |         {RI, @1}         |        |
             |                         |        |
             |<========DoT/DoH===========>|
```
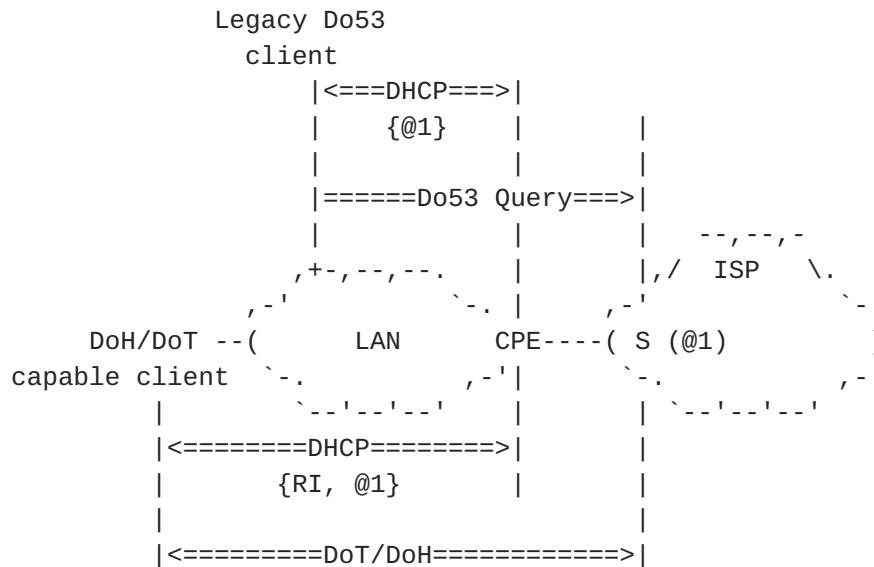
Legend:
  * S: DNS server
  * {@1}: IP address of S; returned in a DHCP
    Domain Name Server option
  * RI: DNS Reference Identifier

         Figure 9: Locating DoH/DoT/Do53 (Same DNS Server)

```
                    Legacy Do53
                      client
                         |<===RA======|
                         | {RI,@1,@2} |              |
                         |            |              |
                         |=======Do53 Query======>|
                         |            |          --,--,-
                    ,+-,--,--.        |        ,/   S1 (@1)\.
                  ,-'         `-. |      ,-'      ISP     `-.
        DoH/DoT --(      LAN      CPE----(                   )
     capable client  `-.         ,-'|       `-.   S2 (@2)   ,-'
              |        `--'--'--'    |         `--'--'--'
              |<========RA==========|              |
              |       {RI,@1,@2}       |              |
              |                        |              |
              |<==============DoT/DoH===========>|
```

   Legend:
     * S1: Do53 server
     * S2: DoH/DoT server
     * @1: IP address of S1
     * @1: IP address of S2
     * RI: DNS Reference Identifier

           Figure 10: Locating DoH/DoT/Do53 (Distinct Servers)

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

5.1. 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 check 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.

5.2. 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-dprive-bootstrap-dns-server] 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.

6. DoT and DoH DNS-SD Considerations

As an alternative to probing discovered DNS servers in order to check
(1) whether they support DoT and/or DoH, and (2) whether customized
port numbers are used (instead of 443/853 port numbers), a DNS client
MAY use DNS-based Service Discovery (DNS-SD) [RFC6763].

DNS-SD defines a set of naming rules for certain DNS record types
that they use for advertising and discovering services. Section 4.1

of [RFC6763] specifies that a service instance name in DNS-SD has the
following structure:

<Instance> . <Service> . <Domain>

The <Domain> portion specifies the authentication domain name
(Section 4). The <Service> portion of the DNS service instance name
MUST be "_domain-s._tcp" (Section 6 of [RFC7858]) or "_doh._tcp"
(Section 9.4). If no DNS-SD records can be retrieved by the DNS
client, it MUST wait a time period that is appropriate for the
encountered error (e.g., NXDOMAIN, timeout, etc.).

If DoH is supported by the DNS server, the DNS client may request the
URI resource record type [RFC7553] using the domain name discovered
using DNS Reference Identifier DHCP/RA option (Section 4) to use the
HTTPS URI scheme (Section 3 of [RFC8484]).

7. Hosting DoH/DoT Forwarder in the CPE

The following mechanisms can be used to host a DoH/DoT forwarder in
the CPE:

ACME: If a CPE is co-located with security services (e.g., malware
   filtering, parental control, MUD), 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 to
   automate certificate management functions such as domain
   validation procedure, certificate issuance and certificate
   revocation.

   Alternatively, the security service provider can assign a unique
   FQDN to the managed CPE. DNS requests to the forwarder are sent
   to the internal IP address, not the external one. The DoH/DoT
   forwarder will act like a private DoT/DoH server only be
   accessible from within the home network.

Redirection: An ISP-managed CPE can be configured with the ISP's
   DoH/DoT resolver IP addresses and ADN, which it will communicate
   to internal hosts using DHCP/RA. Upon joining the network, a DoH/
   DoT client follows the procedure specified in Section 5.1 to
   upgrade to DoT/DoH.

   Once the DoH session is established, the ISP DoH/DoT server uses
   HTTP redirection (Section 6.4.4 in [RFC7231]) to redirect the DNS
   client to the DoH forwarder hosted on the CPE (e.g.,
   cpe1-internal.example.net). The DNS client either uses Do53 or
   opportunistic privacy profile (Section 7.2 of [RFC8310]) to

resolve the domain name in the redirected URI and eventually
establishes DoH session with the DoH forwarder in the CPE
reachable on the LAN interface. A simplified example is
illustrated in Figure 11.

PKIX authentication [RFC6125] based upon the domain name in the
redirected URI will detect rogue DNS servers.

A DNS client that successfully connects to a redirected DoH server
may choose to locally cache the server host IP addresses in order
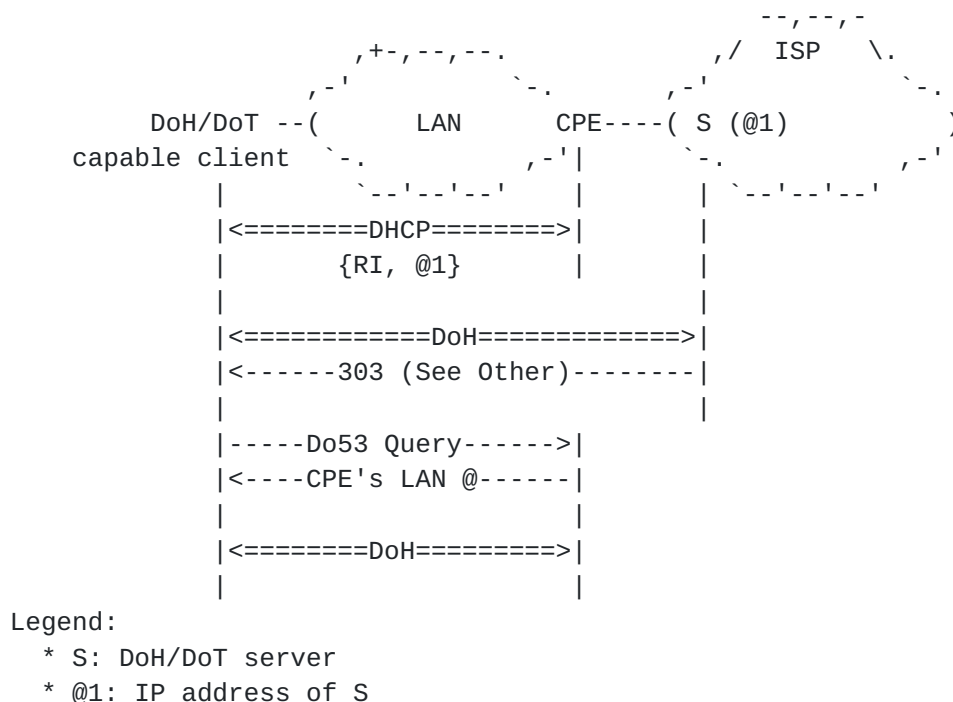to not have to repeat the Do53 query.

```
                                                --,--,-
                     ,+-,--,--.              ,/  ISP   \.
                  ,-'          `-.        ,-'          `-.
         DoH/DoT --(       LAN      CPE----( S (@1)          )
      capable client   `-.           ,-'|      `-.          ,-'
              |          `--'--'--'    |       | `--'--'--'
              |<=======DHCP=======>|        |
              |          {RI, @1}        |        |
              |                        |        |
              |<===========DoH============>|
              |<------303 (See Other)--------|
              |                        |        |
              |-----Do53 Query------>|
              |<----CPE's LAN @------|
              |                        |        |
              |<=======DoH========>|
              |                        |        |
    Legend:
      * S: DoH/DoT server
      * @1: IP address of S
```

Figure 11: A Simplified Example of Redirection to the DNS Forwarder
                          in the CPE

8. 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 primary attacks against the methods described in Section 6 are
the ones that would lead to impersonation of a DNS server and
spoofing the DNS response to indicate that the DNS server does not
support DoH or DoT. To protect against DNS-vectored attacks, secured
DNS (DNSSEC) can be used to ensure the validity of the received DNS
records received. Impersonation of a DoH/DoT server is prevented by
validating the certificate presented by the DoH/DoT server. If DHCP/
RA conveys an ADN, but the DNS-SD lookup indicates that the DNS
server does not support DoH/DoT, the DNS client can detect the DNS
response is spoofed.

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. The DNS client must 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. Sections 5.1 and
5.2 identify 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, its policy information must be cryptographically
attested by the ISP (e.g., [I-D.reddy-dprive-dprive-privacy-policy]);
user consent is required to use the locally-discovered DoH/DoT
server. Such consent may be part of the generic policies discussed
above.

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.

9. IANA Considerations

9.1. 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 | Singleton | Reference |
		ORO	Option	
TBA1	OPTION_V6_DNS_RI	Yes	Yes	[ThisDocument]

9.2. 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 | Meaning | Reference |
		Length		
TBA2	OPTION_V4_DNS_RI	N	DoT/DoH server	[ThisDocument]
			authentication	
			domain name	

9.3. 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]

9.4. Service Name

IANA is requested to allocate the following service name from the
registry available at: https://www.iana.org/assignments/service-
names-port-numbers/service-names-port-numbers.xhtml.

```
    Service Name:           doh
    Port Number:            N/A
    Transport Protocol(s):  TCP
    Description:            DNS-over-HTTPS
    Assignee:              IESG <iesg@ietf.org>
    Contact:               IETF Chair <chair@ietf.org>
    Reference:             [ThisDocument]
```

10. Acknowledgements

Many thanks to Christian Jacquenet for the review.

Thanks to Tommy Jensen for the comments.

11. References

11.1. 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>.

[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>.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service
           Discovery", RFC 6763, DOI 10.17487/RFC6763, February 2013,
           <https://www.rfc-editor.org/info/rfc6763>.

[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>.

   [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>.

11.2. 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/download.php?file=/sites/default/files/private/
               Device_Provisioning_Protocol_Specification_v1.1_1.pdf>.

   [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-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.reddy-dprive-bootstrap-dns-server]
          Reddy.K, T., Wing, D., Richardson, M., and M. Boucadair,
          "A Bootstrapping Procedure to Discover and Authenticate
          DNS-over-(D)TLS and DNS-over-HTTPS Servers", draft-reddy-
          dprive-bootstrap-dns-server-07 (work in progress),
          February 2020.

[I-D.reddy-dprive-dprive-privacy-policy]
          Reddy.K, T., Wing, D., Richardson, M., and M. Boucadair,
          "DNS Server Privacy Statement and Filtering Policy with
          Assertion Token", draft-reddy-dprive-dprive-privacy-
          policy-03 (work in progress), March 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>.

[RFC7231] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer
          Protocol (HTTP/1.1): Semantics and Content", RFC 7231,
          DOI 10.17487/RFC7231, June 2014,
          <https://www.rfc-editor.org/info/rfc7231>.

[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>.

[RFC7553] Faltstrom, P. and O. Kolkman, "The Uniform Resource
          Identifier (URI) DNS Resource Record", RFC 7553,
          DOI 10.17487/RFC7553, June 2015,
          <https://www.rfc-editor.org/info/rfc7553>.

   [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>.

   [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. Customized DHCP Configuration

   In deployment where DoH/DoT/Do53 are not co-located, an ISP may
   return a list of servers that is composed of DoH (and/or DoT) and
   Do53 servers. A host that is also DoH-capable (and/or DoT-capable),
   will try to establish a DoH (and/or DoT) session to that list. DoT
   and/or DoH are supported if the client succeeds to establish a
   session.

   Let's consider that the DoH server is reachable at
   2001:db8:122:300::2 while the Do53 server is reachable at
   2001:db8:122:300::1. The DHCP server will then return a list that
   includes both 2001:db8:122:300::1 and 2001:db8:122:300::2 to a
   requesting DNS client. That list is passed to the DNS client. A
   legacy Do53 client will select 2001:db8:122:300::1 while a DoH client
   will select 2001:db8:122:300::2.

   Alternatively, the DHCP server may return a customized DNS
   configuration ([RFC7969]) as a function of the requested DHCP
   options. For example, if the DHCP client does not include a DNS

Reference Identifier option in its request, the DHCP server will
return the IP address of the Do53 server (2001:db8:122:300::1). If a
DNS Reference Identifier option is present in the request, the DHCP
server returns the IP address(es) of the DoH server
(2001:db8:122:300::2) (or 2001:db8:122:300::2 and 2001:db8:122:300::1
in this order).

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