

ADD  
Internet-Draft  
Intended status: Standards Track  
Expires: September 5, 2020

M. Boucadair  
Orange  
T. Reddy  
McAfee  
D. Wing  
Citrix  
March 4, 2020

**DoH/DoT Deployment Considerations for Home Networks**  
**draft-btw-add-home-00**

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 5, 2020.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

|                       |  |                    |
|-----------------------|--|--------------------|
| <a href="#">1.</a>    | Introduction . . . . .                           | <a href="#">2</a>  |
| <a href="#">2.</a>    | Terminology . . . . .                            | <a href="#">4</a>  |
| <a href="#">3.</a>    | Sample Deployment Scenarios . . . . .            | <a href="#">4</a>  |
| <a href="#">4.</a>    | DNS Reference Identifier Option . . . . .        | <a href="#">6</a>  |
| <a href="#">4.1.</a>  | DHCPv6 DNS Reference Identifier Option . . . . . | <a href="#">7</a>  |
| <a href="#">4.2.</a>  | DHCP DNS Reference Identifier Option . . . . .   | <a href="#">7</a>  |
| <a href="#">4.3.</a>  | RA DNS Reference Identifier Option . . . . .     | <a href="#">8</a>  |
| <a href="#">5.</a>    | Locating DoH/DoT Servers . . . . .               | <a href="#">9</a>  |
| <a href="#">6.</a>    | Hosting DoH/DoT Forwarder in the CPE . . . . .   | <a href="#">11</a> |
| <a href="#">7.</a>    | Security Considerations . . . . .                | <a href="#">12</a> |
| <a href="#">8.</a>    | IANA Considerations . . . . .                    | <a href="#">13</a> |
| <a href="#">8.1.</a>  | DHCPv6 Option . . . . .                          | <a href="#">13</a> |
| <a href="#">8.2.</a>  | DHCP Option . . . . .                            | <a href="#">13</a> |
| <a href="#">8.3.</a>  | RA Option . . . . .                              | <a href="#">13</a> |
| <a href="#">9.</a>    | Acknowledgements . . . . .                       | <a href="#">14</a> |
| <a href="#">10.</a>   | References . . . . .                             | <a href="#">14</a> |
| <a href="#">10.1.</a> | Normative References . . . . .                   | <a href="#">14</a> |
| <a href="#">10.2.</a> | Informative References . . . . .                 | <a href="#">15</a> |
|                       | Authors' Addresses . . . . .                     | <a href="#">16</a> |

## [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 (Customer Premise Equipment (CPE) or User Equipment (UE)) 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 LAN



are similar in both fixed and cellular CPE-based broadband service offerings.

(a) Fixed Networks



(b) Cellular Networks

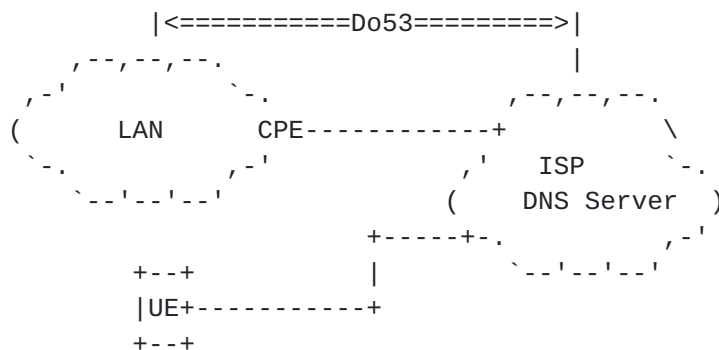


Figure 1: Sample Legacy Deployments

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



resolexpervers 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.

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. This document permits such deployments. It is up to an ISP to decide which list of DNS resolvers to advertise to its serviced 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](#)].

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

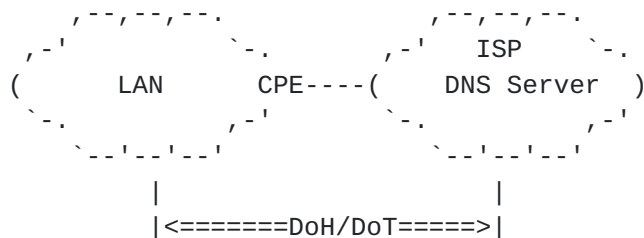
## 3. Sample Deployment Scenarios

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 authentication domain name information (ADN, defined in [[RFC8310](#)]) to managed CPEs if DoH/DoT is supported by a local network similar to what is depicted in Figure 2.

DNS clients may try to establish DoH/DoT sessions with discovered DNS servers to determine whether these servers support DoH and/or DoT ([Section 5](#)). Alternatively, a DNS client may discover whether the DNS server in the local network supports DoH/DoT by using the mechanism discussed in [Section 6](#) of [[I-D.reddy-dprive-dprive-privacy-policy](#)]. If DoH is supported by the DNS server, the DNS client may request the URI resource record type [[RFC7553](#)] to use the HTTPS URI scheme ([Section 3 of](#) [[RFC8484](#)]).



(a) Fixed Networks



(b) Cellular Networks

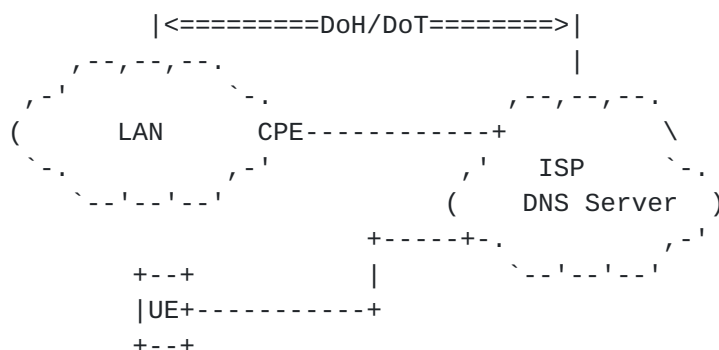


Figure 2: DoH/DoT in the WAN

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).

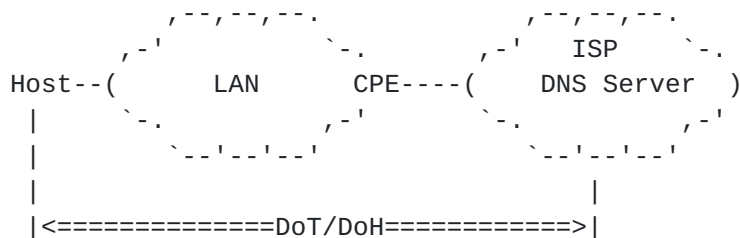


Figure 3: Direct DoH/DoT Sessions

In many deployments, 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.

Also, an ISP that wants to offer DoH/DoT to its customers may enable DoH/DoT in both legs as shown in Figure 4. Additional considerations related to this approach are discussed in [Section 6](#).

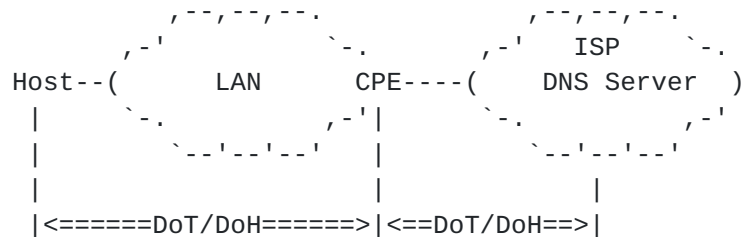


Figure 4: Proxied DoH/DoT Sessions

#### 4. DNS Reference Identifier Option

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 and an IP address 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.

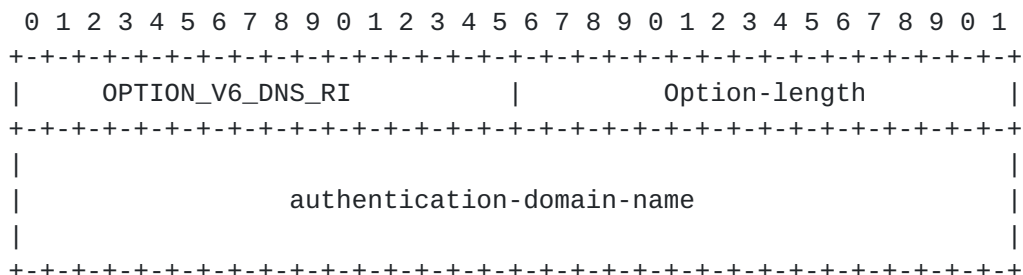


Figure 5: DHCPv6 DNS Reference Identifier Option

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

- o Option-code: OPTION\_V6\_DNS\_RI (TBA1, see [Section 8.1](#))
- 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".

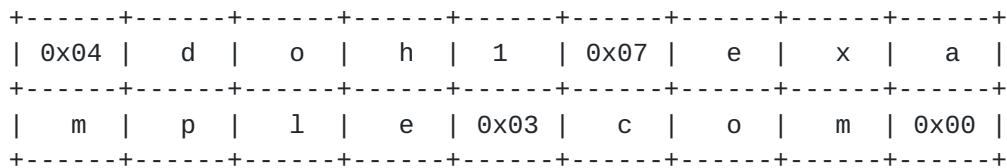


Figure 6: An example of the authentication-domain-name Encoding

#### 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: DHCPv4 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 8.2](#)).
- 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 8.3](#)).
- 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

As mentioned in [Section 1](#), a CPE or a host relies upon discovery mechanisms (such as PCO, DHCP, or RA) to retrieve DoH and DoT servers' reachability information, and hosted by local networks. 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 9). 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, existing discovery mechanisms 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](#).

Note: It is unlikely that DoH and DoT will be offered simultaneously, but we need to indicate which one wins if DoH and DoT are supported.





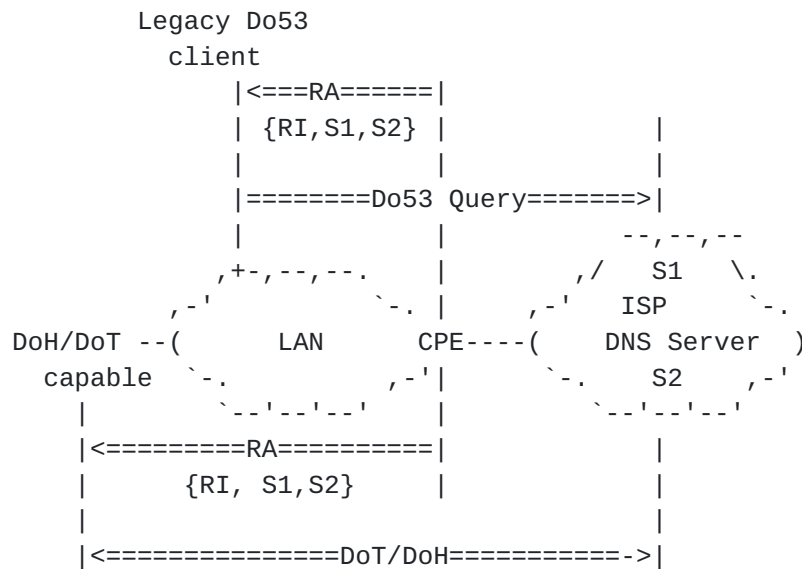


Figure 9: Locating DoH/DoT/Do53 using [RFC8106](#)

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 trusted resolver, the DNS client auto-upgrades to use the discovered DoH/DoT server.
- o If the DNS reference identity ([Section 4](#)) is provided by means of DHCP/RA, 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.
- o If the DNS reference identity is provided by means of DHCP/RA and the DNS client uses these IP addresses as a reference identity, the DNS client matches the IP address in the DNS DHCP/RA option with the 'ipAddress' stored in the subjectAltName entry in the server certificate conveyed in the TLS handshake.

Additional options are discussed below:

- o The Wi-Fi Alliance has released the Device Provisioning Protocol (DPP). If DPP is used, the configurator can securely configure devices in the home network with the local DoT/DoH server 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 (ADN) 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. Hosting DoH/DoT Forwarder in the CPE**

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

- o 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 to the CPE.

Alternatively, the ISP can assign a unique FQDN to the managed CPE. The DoT/DoH forwarder will act like a public DoT/DoH server but will only be accessible from within the home network. DNS queries received outside the home network must be discarded by the DoH/DoT forwarder. This behavior adheres to REQ#8 in [[RFC6092](#)], and must apply for both IPv4 and IPv6.

- o 'ACME IP Identifier Validation Extension' [[RFC8738](#)] can be used to issue a public certificate for the public IP address of the DoH/DoT forwarder. This mechanism requires the issuance of the certificate and the management of the certificate's renewal to be supported by the CPE itself. The HTTP Challenge (HTTP-01) or TLS with Application Level Protocol Negotiation (TLS ALPN) challenge (TLS-ALPN-01) are used to prove the IP address ownership during the issuance of the certificate. This certificate will carry a public IP address in `iPAddress subjectAltName` extension.

The disadvantages of this mechanism are: (1) the certificate needs to be re-issued every time the subscriber's IPv6 prefix or the public IPv4 address changes and (2) the CPE needs to run an HTTP- or HTTPS server (on the default ports) while the ACME server is



validating the challenge; the CPE might have those ports forwarded to an internal host for other purposes.

## 7. 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. The DNS client must adhere to these policies.

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.

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., [\[I-D.redddy-dprive-dprive-privacy-policy\]](#)); user consent is required to use the locally-discovered DoH/DoT server.

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 [\[RFC6125\]](#), and which relies 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).



## 8. IANA Considerations

### 8.1. 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] |

### 8.2. 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 authentication | [ThisDocument] |
|      |                  |        | domain name                   |                |

### 8.3. 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. Acknowledgements

Many thanks to Christian Jacquenet for the review.

## 10. References

### 10.1. 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>>.
- [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>>.

## **10.2. Informative References**

- [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>>.



- [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>>.
- [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>>.
- [RFC8738] Shoemaker, R., "Automated Certificate Management Environment (ACME) IP Identifier Validation Extension", [RFC 8738](#), DOI 10.17487/RFC8738, February 2020, <<https://www.rfc-editor.org/info/rfc8738>>.
- [TR-069] The Broadband Forum, "CPE WAN Management Protocol", March 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](mailto:dwing-ietf@fuggles.com)