ADD
Internet-Draft
Intended status: Informational
Expires: November 18, 2021

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

May 17, 2021

Discovery of Encrypted DNS Resolvers: Deployment Considerations
draft-boucadair-add-deployment-considerations-00

Abstract

The document discusses some deployment considerations of the various options to discover encrypted DNS servers (e.g., DNS-over-HTTPS, DNS-over-TLS, DNS-over-QUIC).

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

[I-D.ietf-add-dnr] specifies how a local encrypted DNS server can be discovered by connected hosts by means of DHCP [RFC2132], DHCPv6 [RFC8415], and IPv6 Router Advertisement (RA) [RFC4861] options. These options are designed to convey the following information: the DNS Authentication Domain Name (ADN), a list of IP addresses, and a set of service parameters.

This document discusses deployment considerations for the discovery of encrypted DNS servers such as DNS-over-HTTPS (DoH) [RFC8484], DNS-over-TLS (DoT) [RFC7858], or DNS-over-QUIC (DoQ) [I-D.ietf-dprive-dnsoquic] in local networks.

Sample target deployment scenarios are discussed in Section 3; both managed and unmanaged Customer Premises Equipment (CPEs) are covered.

It is out of the scope of this document to provide an exhaustive inventory of deployments where Encrypted DNS options can be used.

Considerations related to hosting a DNS forwarder in a local network are described in Section 4.

2. Terminology

This document makes use of the terms defined in [RFC8499]. The following additional terms are used:

Do53: refers to unencrypted DNS.

Encrypted DNS: refers to a scheme where DNS exchanges are transported over an encrypted channel. Examples of encrypted DNS are DNS-over-TLS (DoT) [RFC7858], DNS-over-HTTPS (DoH) [RFC8484], or DNS-over-QUIC (DoQ) [I-D.ietf-dprive-dnsoquic].

Encrypted DNS options: refers to the options defined in [I-D.ietf-add-dnr].

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

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

DHCP: refers to both DHCPv4 and DHCPv6.

3. Sample Target Deployment Scenarios

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

- o Protocol Configuration Options in cellular networks [TS.24008].
- o DHCPv4 [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). 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.

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

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

          (b) Cellular Networks

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

          Legend:
           * H: refers to a host.
```

Figure 1: Sample Legacy Deployments

3.1. Managed CPEs

This section focuses on CPEs that are managed by ISPs.

3.1.1. Direct DNS

ISPs have developed an expertise in managing service-specific configuration information (e.g., CPE WAN Management Protocol [TR-069]). For example, these tools may be used to provision the DNS server's ADN to managed CPEs if an encrypted DNS is supported by a local network similar to what is depicted in Figure 2.

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

The DNS client discovers whether the DNS server in the local network supports DoH/DoT/DoQ by using the service paramters (ALPN).

```
          (a) Fixed Networks

                                           ,--,--,--.
              +-+      LAN     +---+    ,-'           `-.
              |H+--------------+CPE+---+      ISP        )
              +-+              +---+    `-.           ,-'
               |                           `--'--'--'
               |                               |
               |<========Encrypted DNS========>|
               |                               |

          (b) Cellular Networks

               |                               |
               |<========Encrypted DNS========>|
               |                               |
               |                           ,--,--,-.
              +-+      LAN     +---+    ,-'         .
              |H+--------------+CPE+---+             \
              +-+              +---+  ,'     ISP     `-.
                                      (                )
                                 +-----+-.          ,-'
              +-+                |        `--'--'--'
              |H+----------------+             |
              +-+                              |
               |                               |
               |<========Encrypted DNS========>|
               |                               |
```

Figure 2: Encrypted DNS in the WAN

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

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

Figure 3: Direct Encrypted DNS Sessions

3.1.2. **Proxied DNS**

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., Section 5.4.1 of [I-D.ietf-v6ops-rfc7084-bis]) or for supporting advanced services within a local network (e.g., malware filtering, parental control, Manufacturer Usage Description (MUD) [RFC8520] to only allow intended communications to and from an IoT device). When the CPE behaves as a DNS forwarder, DNS communications can be decomposed into two legs:

- 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 encrypted DNS to its customers may enable encrypted DNS in one or both legs as shown in Figure 4. Additional considerations related to this deployment are discussed in Section 4.

```
   (a)
                         ,--,--,--.             ,--,--,--.
                      ,-'          `-.       ,-'   ISP    `-.
              Host---(      LAN      CPE----(    DNS Server  )
                |     `-.          ,-'|      `-.          ,-'
                |        `--'--'--'   |         `--'--'--'
                |                     |             |
                |<=====Encrypted=====>|<=Encrypted=>|
                |         DNS         |     DNS     |

   (b)
                         ,--,--,--.             ,--,--,--.
             Legacy   ,-'          `-.       ,-'   ISP    `-.
              Host---(      LAN      CPE----(    DNS Server  )
                |     `-.          ,-'|      `-.          ,-'
                |        `--'--'--'   |         `--'--'--'
                |                     |             |
                |<=======Do53========>|<=Encrypted=>|
                |                     |     DNS     |
```

Figure 4: Proxied Encrypted DNS Sessions

3.2. Unmanaged CPEs

3.2.1. ISP-facing Unmanaged CPEs

Customers may decide to deploy unmanaged CPEs (assuming the CPE is compliant with the network access technical specification that is usually published by ISPs). Upon attachment to the network, an unmanaged CPE receives from the network its service configuration (including the DNS information) by means of, e.g., DHCP. That DNS information is shared within the LAN following the same mechanisms as those discussed in Section 3.1. A host can thus establish DoH/DoT session with a DoH/DoT server similar to what is depicted in Figure 3 or Figure 4.

3.2.2. Internal Unmanaged CPEs

Customers may also decide to deploy internal routers (called hereafter, Internal CPEs) for a variety of reasons that are not detailed here. Absent any explicit configuration on the internal CPE to override the DNS configuration it receives from the ISP-supplied CPE, an Internal CPE relays the DNS information it receives via DHCP/RA from the ISP-supplied CPE to connected hosts. Encrypted DNS sessions can be established by a host with the DNS servers of the ISP (see Figure 5).

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

Figure 5: Direct Encrypted DNS Sessions with the ISP DNS Resolver (Internal CPE)

Similar to managed CPEs, a user may modify the default DNS configuration of an unmanaged CPE to use his/her favorite DNS servers instead. Encrypted DNS sessions can be established directly between a host and a 3rd Party DNS server (see Figure 6).

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

Figure 6: Direct Encrypted DNS Sessions with a Third Party DNS Resolver

Section 4.2 discusses considerations related to hosting a forwarder in the Internal CPE.

4. Hosting Encrypted DNS Forwarder in Local Networks

This section discusses some deployment considerations to host an encrypted DNS forwarder within a local network.

4.1. Managed CPEs

The section discusses mechanisms that can be used to host an encrypted DNS forwarder in a managed CPE (Section 3.1).

4.1.1. DNS Forwarders

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

4.1.2. ACME

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

4.2. Unmanaged CPEs

The approach specified in Section 4.1 does not apply for hosting a DNS forwarder in an unmanaged CPE.

The unmanaged CPE administrator can host an encrypted DNS forwarder on the unmanaged CPE. This assumes the following:

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

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

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

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

Figure 7 illustrates an example of an unmanaged CPE hosting a forwarder which connects to a 3rd party encrypted DNS server. In this example, the DNS information received from the managed CPE (and therefore from the ISP) is ignored by the Internal CPE hosting the forwarder.

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

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

Figure 7: Example of an Internal CPE Hosting a Forwarder

5. Legacy CPEs

Hosts serviced by legacy CPEs that can't be upgraded to support the options defined in Sections 4, 5, and 6 of [I-D.ietf-add-dnr] won't be able to learn the encrypted DNS server hosted by the ISP, in particular. If the ADN is not discovered using DHCP/RA, such hosts will have to fallback to use discovery using the resolver IP address as defined in Section 4 of [I-D.ietf-add-ddr] to discover the designated resolvers.

The guidance in Sections 4.1 and 4.2 of [I-D.ietf-add-ddr] related to the designated resolver verification has to be followed in such case.

6. Security Considerations

DNR-related security considerations are discussed in Section 7 of [I-D.ietf-add-dnr].

7. IANA Considerations

This document does not require any IANA action.

8. Acknowledgements

This text was initially part of [I-D.ietf-add-dnr].

9. References

9.1. Normative References

[I-D.ietf-add-dnr]
Boucadair, M., Reddy, T., Wing, D., Cook, N., and T. Jensen, "DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)", draft-ietf-add-dnr-00 (work in progress), February 2021.

9.2. Informative References

[I-D.ietf-add-ddr]
Pauly, T., Kinnear, E., Wood, C. A., McManus, P., and T. Jensen, "Discovery of Designated Resolvers", draft-ietf-add-ddr-00 (work in progress), February 2021.

[I-D.ietf-dprive-dnsoquic]
Huitema, C., Mankin, A., and S. Dickinson, "Specification of DNS over Dedicated QUIC Connections", draft-ietf-dprive-dnsoquic-02 (work in progress), February 2021.

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

[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>.

[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>.

[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>.

[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>.

[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 (editor)
Orange
Rennes 35000
France

Email: mohamed.boucadair@orange.com

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

Email: TirumaleswarReddy_Konda@McAfee.com

Dan Wing
Citrix Systems, Inc.
USA

Email: dwing-ietf@fuggles.com

Neil Cook
Open-Xchange
UK

Email: neil.cook@noware.co.uk

Tommy Jensen
Microsoft
USA

Email: tojens@microsoft.com