Workgroup: Network Working Group
Internet-Draft:
draft-boucadair-add-deployment-considerations-02
Published: 18 October 2022
Intended Status: Informational
Expires: 21 April 2023
Authors: M. Boucadair, Ed. (Orange)
T. Reddy, Ed. (Nokia)
D. Wing (Citrix)
N. Cook (Open-Xchange)
T. Jensen (Microsoft)

# Discovery of Encrypted DNS Resolvers: Deployment Considerations

## Abstract

The document discusses some deployment considerations of the various options to discover encrypted DNS resolvers (e.g., DNS-over-HTTPS, DNS-over-TLS, or DNS-over-QUIC). In particular, the document describes how Discovery of Network-designated Resolvers (DNR) and Discovery of Designated Resolvers (DDR) can be used in typical deployment contexts.

This document does not intend to provide deployment recommendations, but is meant to exemplify how operators can enable the encrypted DNS discovery mechanisms. In addition, the document illustrates the feasibility of hosting encrypted DNS forwarders in Customer Premises Equipment (CPEs).

## 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 21 April 2023.

**Table of Contents**



## 1. Introduction

Discovery of Network-designated Resolvers (DNR) [I-D.ietf-add-dnr] specifies how a local encrypted DNS resolver 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. The ADN is used as a reference identifier for authentication purposes, while the list of IP addresses designate

where to locate the resolver without relying upon an external resolver. The service parameters provide additional information to characterize a DNS resolver (e.g., supported encrypted DNS, customized DNS port number, or URI Template for DNS-over-HTTPS (DoH)). Such an information is used by a DNS client for DNS resolver selection and session establishment.

This document discusses some considerations to make use of the discovery of encrypted DNS resolvers such as DoH [RFC8484], DNS-over-TLS (DoT) [RFC7858], or DNS-over-QUIC (DoQ) [RFC9250] in local networks.

Sample target deployment scenarios are discussed in Section 4; 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 5. In contexts where CPEs can't be upgraded to support DNR, Discovery of Designated Resolvers (DDR) [I-D.ietf-add-ddr] can be used. See Sections 5.1 and 6 for more details.

Techniques, such as the one defined in [I-D.ietf-opsawg-add-encrypted-dns], can be enabled together with [I-D.ietf-add-dnr] to feed the Encrypted DNS options. However, the document does not make any assumption about the internal behavior at the network side to feed the Encrypted DNS options that are supplied to requesting hosts; only the external observed behavior is detailed in the following sections.

Policies to guide the activation and selection of encrypted DNS can be configured by users using implementation specific means (e.g., CPE management interface).

## 2. Scope & Target Audience

This document is not setting deployment recommendations or claiming to share best current practices. It is purposely scoped to exemplify how encrypted DNS discovery mechanisms can be enabled in typical networks. A set of considerations are specifically drawn to assist Internet Service Providers (ISPs), CPE vendors, and home network security service providers.

Concretely, generalizing the use of encrypted DNS while preserving services that are offered to users (especially, those services that require a local DNS forwarder) depend on many actors:

**ISPs and home network security service providers:**

ISPs who need to investigate and elaborate plans about how their managed CPEs will be upgraded to support encrypted DNS forwarders and whether home network security mechanisms will still be required to enforce per-device policies.

Some ISPs may also need to investigate plans to offer encrypted DNS services even for CPE models whose firmware cannot be updated. For example, ISPs may consider updating the CPE configuration to point to the ISP's Do53 resolver for DDR to work.

ISPs will also need to assess the impacts of bypassing local DNS forwarders on their DNS infrastructure and the services they are offering to their subscribers.

**CPE vendors:** to help them assess the feasibly of CPEs to host an encrypted DNS forwarder. To that aim, the document sketches some realization approaches. For example, CPE vendors may learn from the effort that was conducted by some DNS providers to optimize the encrypted DNS forwarder to run in a container in home routers and how this may be integrated with home network security service agents.

**Users:** may want to avoid depending on the capabilities of their ISP-supplied CPE. They may consider deploying an unmanaged CPE that uses DNR to advertise the local encrypted DNS information to connected devices. Section 5.3 discusses how DNR can be used in such contexts.

**OS/Application clients:** which need to support the Discovery of Designated Resolvers (DDR) [I-D.ietf-add-ddr] or the Discovery of Network-designated Resolvers (DNR) [I-D.ietf-add-dnr] procedures.

This document is meant to assist future deployments and (hopefully) accelerate the network deployment of encrypted DNS servers.

## 3. Terminology

This document makes use of the terms defined in [RFC8499].

The following additional terms are used:

**DHCP:**
refers to both DHCPv4 and DHCPv6.

**Do53:** refers to unencrypted DNS.

**DNR:** refers to the Discovery of Network-designated Resolvers procedure defined in [I-D.ietf-add-dnr].

**DDR:** refers to the Discovery of Designated Resolvers procedure defined in [I-D.ietf-add-ddr].

**Encrypted DNS:** refers to a scheme where DNS exchanges are transported over an encrypted channel. Examples of encrypted DNS are DoT, DoH, or DoQ.

**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 ISP.

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

## 4. Sample Target Deployment Scenarios

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

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

* DHCPv4 [RFC2132] (Domain Name Server Option) or DHCPv6 [RFC8415] [RFC3646] (OPTION_DNS_SERVERS).

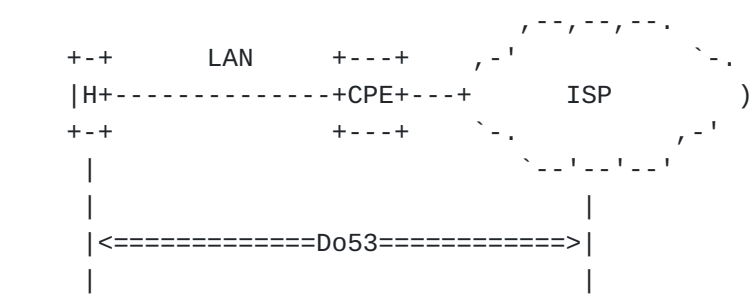
* IPv6 Router Advertisement [RFC4861][RFC8106] (Type 25 (Recursive DNS Server Option)).

The communication between a customer's device (possibly via a CPE) and an ISP-supplied DNS resolver takes place by using cleartext DNS messages (Do53). Some examples are depicted in cases (a) and (c) of 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.

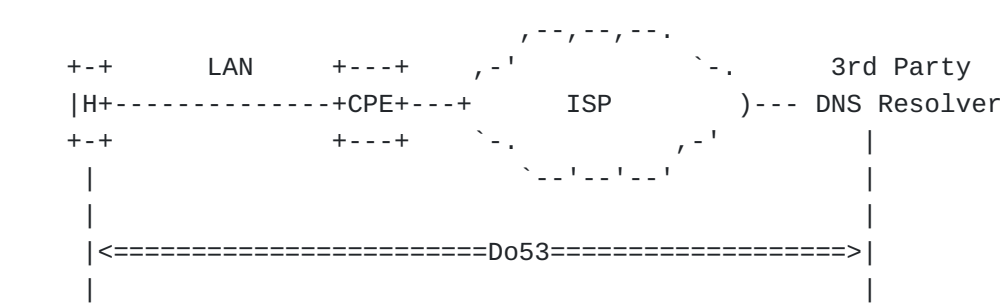
Some ISPs rely upon external resolvers (e.g., outsourced service or public resolvers); these ISPs provide their customers with the IP addresses of these external DNS resolvers. An example is depicted in cases (b) and (d) of Figure 1.

The IP addresses of the DNS resolver can also be configured on CPEs using dedicated management tools. As such, 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.

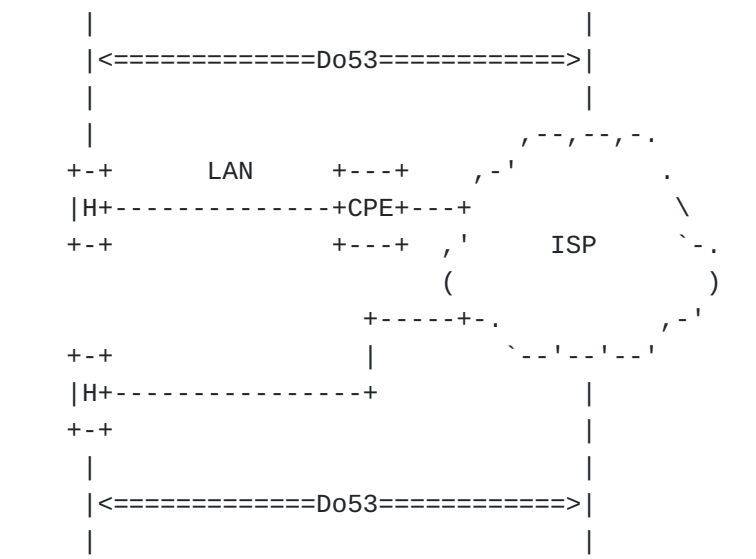
(a) Fixed networks with a local DNS resolver



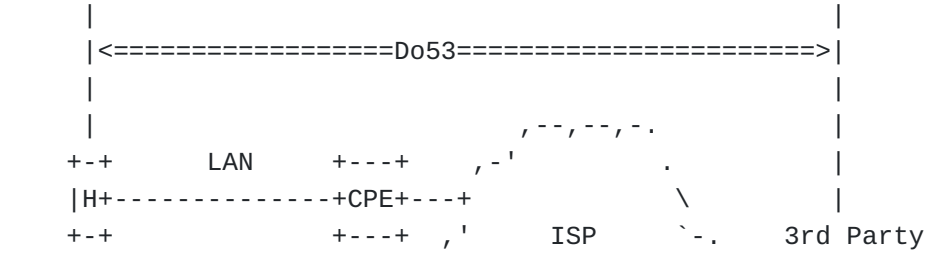

(b) Fixed networks with a 3rd party DNS resolver

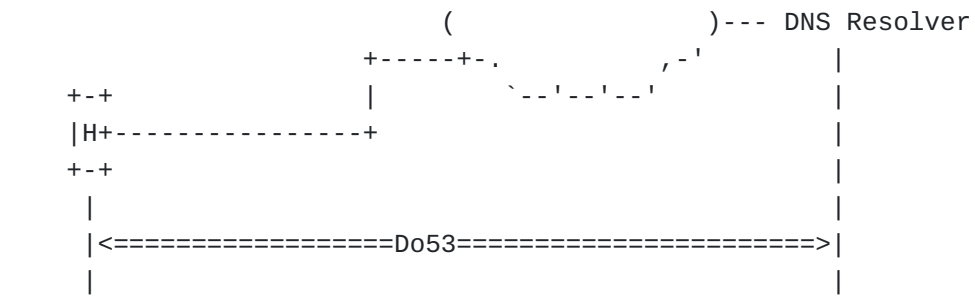



(c) Cellular networks with a local DNS resolver




(d) Cellular networks with a 3rd party DNS resolver






Legend:
 * H: refers to a host.

Figure 1: Sample Legacy Deployments

### 4.1. Managed CPEs

This section focuses on CPEs that are managed by ISPs.

#### 4.1.1. Direct DNS

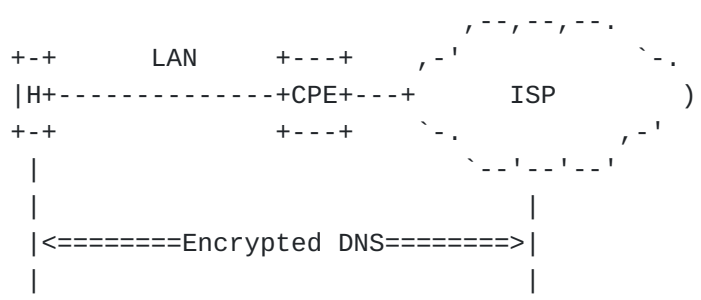
ISPs have developed an expertise in managing service-specific configuration information (e.g., CPE WAN Management Protocol [TR-069]). For example, these tools may be used to provision the DNS server's ADN and additional service parameters to managed CPEs if an encrypted DNS is supported by a network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

For example, DoH-capable DNS clients establish the DoH session with the discovered DoH server.

When the CPE supports DNR, the DNS client discovers whether the network-designated DNS resolver supports a given encrypted DNS scheme (e.g., DoT or DoH) by using the "alpn" service parameter (Section 3.1.5 of [I-D.ietf-add-dnr]). Otherwise, the DNS client uses DDR with the Do53 resolver advertised by the CPE and upgrades to encrypted DNS if that succeeds. Otherwise, the DNS client may fall back to using unencrypted DNS to the IP address advertised by the CPE or use some other configuration it has.

DNR is attempted first because it requires fewer round trips to any network peer because all of the necessary information to use encrypted DNS is presented directly by the CPE. DDR requires the DNS client to receive Do53 resolver configuration from the CPE and then further query for encrypted DNS support from the DNS resolver before any encrypted DNS can be attempted.

(a) Fixed Networks




(b) Cellular Networks

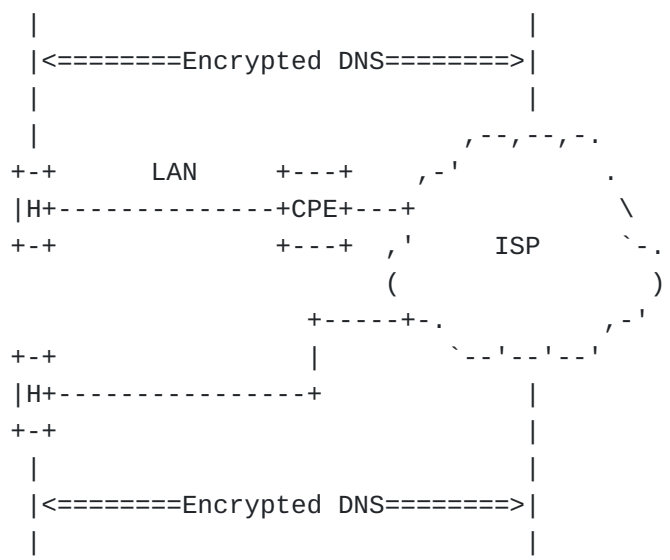



Figure 2: Encrypted DNS in the WAN

Figure 2 shows the scenario where the CPE relays the list of encrypted DNS resolvers that it learns from the network by using, e.g., DNR. Direct encrypted DNS sessions will be established between a host serviced by a CPE and an ISP-supplied encrypted DNS resolver. Figure 3 shows the example of exchanges that occur for an encrypted DNS capable host. The DNR exchanges that occur at the CPE WAN may be terminated by a centralized DHCP server or a router that is located at the edge of the ISP's network.

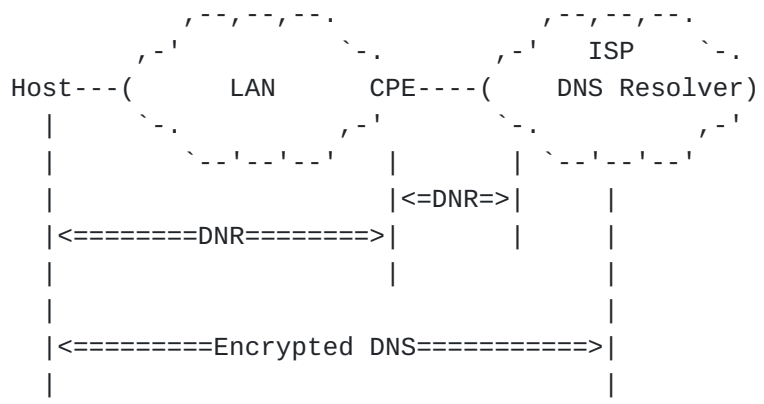
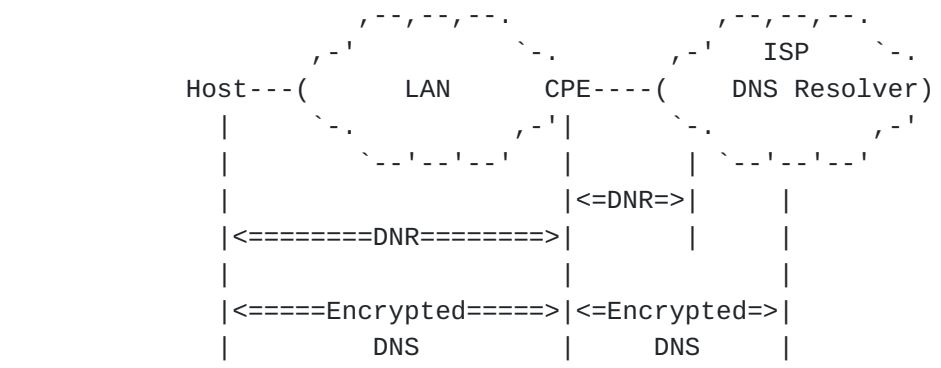



Figure 3: Direct Encrypted DNS Sessions

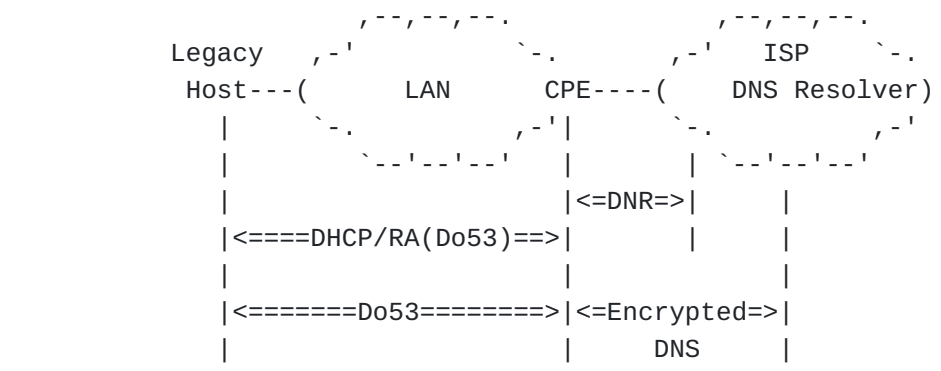
#### 4.1.2. Proxied DNS

Figure 4 shows various network setups where the CPE embeds a caching DNS forwarder. Cases (b) and (d) involves a host (called legacy host) that does not support DNR. Section 5.1 discusses the applicability of DDR as a function of the address used by the CPE for the verification of ownership.

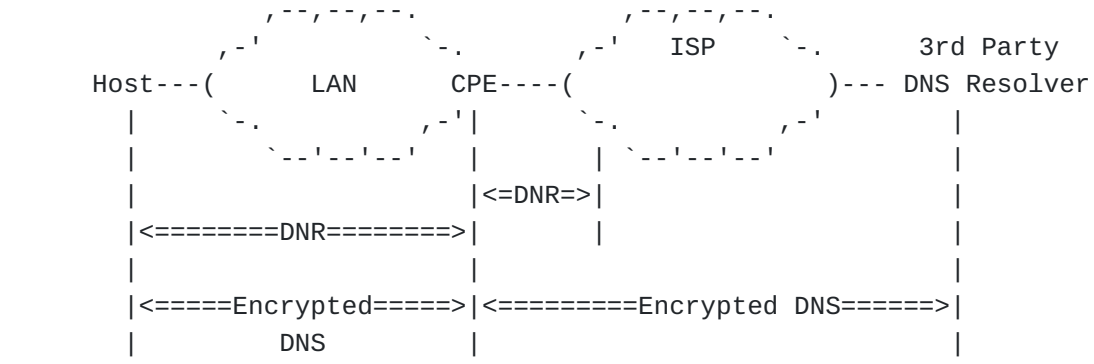
(a)


Host
LAN
CPE
ISP
DNS Resolver
<=DNR=>
<========DNR========>
<=====Encrypted=====>
<=Encrypted=>
DNS
DNS

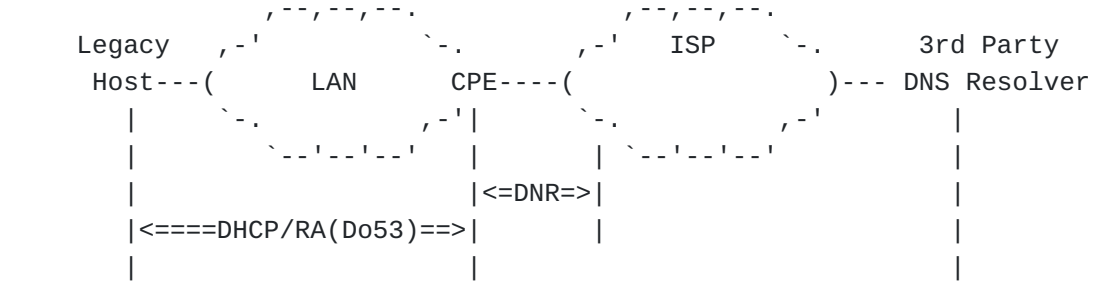
(b)


Legacy
Host
LAN
CPE
ISP
DNS Resolver
<=DNR=>
<====DHCP/RA(Do53)==>
<=======Do53========>
<=Encrypted=>
DNS

(c)


Host
LAN
CPE
ISP
3rd Party
DNS Resolver
<=DNR=>
<========DNR========>
<=====Encrypted=====>
<=========Encrypted DNS======>
DNS

(d)


Legacy
Host
LAN
CPE
ISP
3rd Party
DNS Resolver
<=DNR=>
<====DHCP/RA(Do53)==>

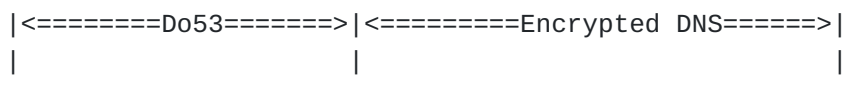

|<========Do53=======>|<==========Encrypted DNS======>|
|

Figure 4: Proxied Encrypted DNS Sessions

For all the cases shown in Figure 4, the CPE advertises itself as the default DNS server to the hosts it serves in the LAN. The CPE relies upon DHCP or RA to advertise itself to internal hosts as the default encrypted DNS (cases (a) and (c)) or Do53 resolver (cases (b) and (d)). When receiving a DNS request it cannot handle locally, the CPE forwards the request to an upstream encrypted DNS. The upstream encrypted DNS can be hosted by the ISP (cases (a) and (b)) or provided by a third party (cases (c) and (d)).

Such a forwarder presence is required for IPv4 service continuity purposes (e.g., Section 3.1 of [RFC8585]) or for supporting advanced services within a local network (e.g., malware filtering, parental control, Manufacturer Usage Description (MUD) [RFC8520] to only allow intended communications to and from an IoT device). When the CPE behaves as a DNS forwarder, DNS communications can be decomposed into two legs:

*The leg between an internal host and the CPE.

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

An ISP that offers encrypted DNS to its customers may enable encrypted DNS in one or both legs as shown in Figure 4. Additional considerations related to this setup are discussed in Section 5.

## 4.2. Unmanaged CPEs

### 4.2.1. 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 network-designated 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 4.1. A host can then establish encrypted DNS sessions with encrypted DNS resolvers similar to what is depicted in Figure 3 or Figure 4.

### 4.2.2. 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 resolvers that are supplied by the ISP (see Figure 5).

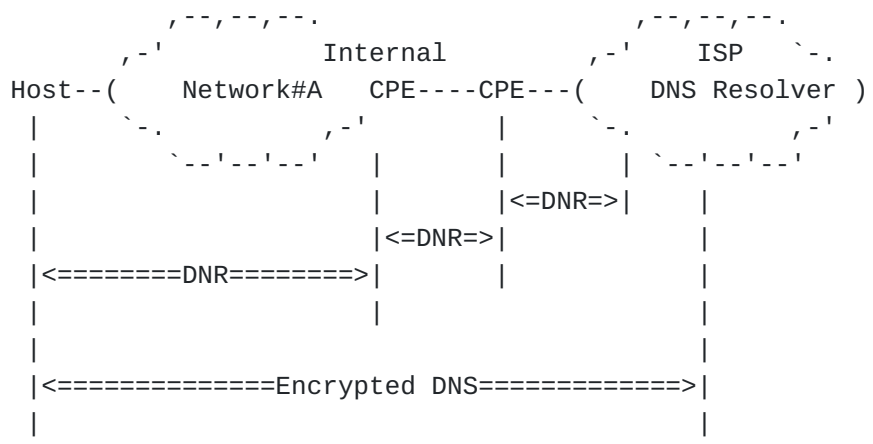



Figure 5: Direct Encrypted DNS Sessions with the ISP DNS Resolver (Internal CPE)

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

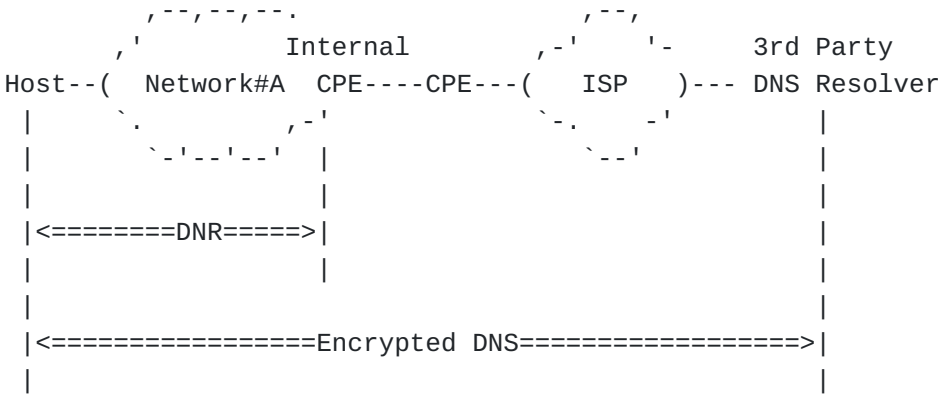



Figure 6: Direct Encrypted DNS Sessions with a Third Party DNS Resolver

Section 5.3 discusses considerations related to hosting a forwarder in the Internal CPE.

## 5. Hosting Encrypted DNS Forwarder in Local Networks

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

### 5.1. DDR/DNR Comparison and Naming Constraints

DDR requires proving possession of an IP address, as the DDR certificate contains the server's IPv4 and IPv6 addresses and is signed by a certificate authority. DDR is constrained to public IP addresses because WebPKI certificate authorities will not sign special-purpose IP addresses [RFC6890], most notably IPv4 private-use [RFC1918], IPv4 shared address [RFC6598], or IPv6 Unique-Local [RFC8190] address space. A tempting solution is to use the CPE's WAN IP address for DDR and prove possession of that IP address. However, the CPE's WAN IPv4 address will not be a public IPv4 address if the CPE is behind another layer of NAT (either Carrier Grade NAT (CGN) or another on-premise NAT), reducing the success of this mechanism to CPE's WAN IPv6 address. If the ISP renumbers the subscriber's network suddenly (rather than slow IPv6 renumbering described in [RFC4192]) encrypted DNS service will be delayed until that new certificate is acquired.

DNR requires proving possession of an FQDN as the encrypted resolver's certificate contains the FQDN. The entity (e.g., ISP, network administrator) managing the CPE would assign a unique FQDN to the CPE. There are two mechanisms for the CPE to obtain the certificate for the FQDN: using one of its WAN IP addresses or requesting its signed certificate from an Internet-facing server used for remote CPE management (e.g., the Auto Configuration Server (ACS) in the CPE WAN Management Protocol [TR-069]). If using a CPE's WAN IP address, the CPE needs a public IPv4 or a global unicast IPv6 address together with DNS A or AAAA records pointing to that CPE's WAN address to prove possession of the DNS name to obtain a WebPKI CA-signed certificate (that is, the CPE fulfills the DNS or HTTP challenge discussed in ACME [RFC8555]). However, a CPE's WAN address will not be a public IPv4 address if the CPE is behind another layer of NAT (either a CGN or another on-premise NAT), reducing the success of this mechanism to a CPE's WAN IPv6 address. If the subscribers IPv4 or IPv6 address is included in the certificate name (e.g., "dyn-192-0-2-1.example.net") then DNR will experience IP renumbering complications identical to DDR, described above. The former mechanism has the following limitations when ACME protocol is used for certificate issuance:

* Each CPE would have to create a different account for ordering a certificate. When a large scale of CPEs request certificate issuance for a large number of subdomains, it could be treated as an attacker by the certificate authorities to overwhelm it.

* The CPE would have to host an Internet-facing HTTP server or a DNS authoritative server to complete the HTTP or DNS challenge.

### 5.2. Managed CPEs

The section discusses mechanisms that can be used to host an encrypted DNS forwarder in a managed CPE (Section 4.1).

#### 5.2.1. DNS Forwarders

The managed CPE should support a configuration parameter to instruct the CPE whether it has to relay the encrypted DNS resolver 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 resolver received from the ISP's network.

#### 5.2.2. 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.

### 5.3. Unmanaged CPEs

The approach specified in Section 5.2 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 resolver certificate is managed by the entity in-charge of hosting the encrypted DNS forwarder.

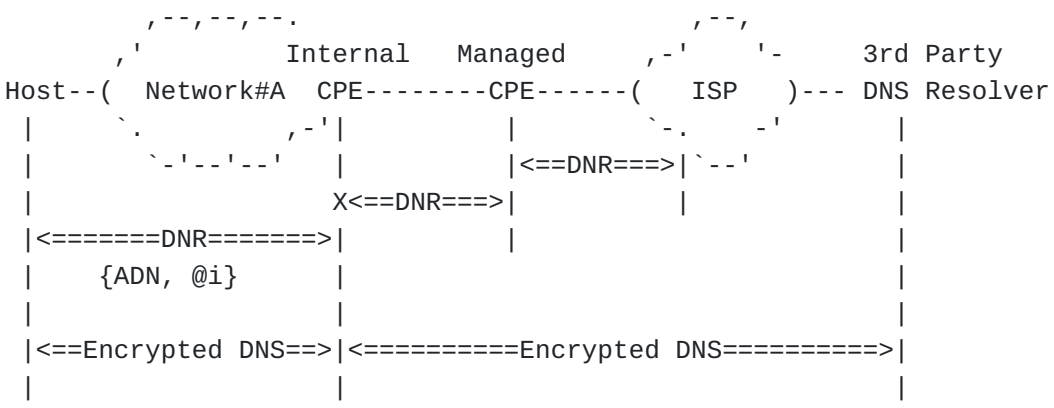
  Alternatively, a security service provider can assign a unique FQDN to the CPE. The encrypted DNS forwarder will act like a private encrypted DNS resolver only be accessible from within the local network.

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

* The unmanaged CPE will advertise the encrypted DNS forwarder ADN using DHCP/RA to internal hosts as per [I-D.ietf-add-dnr].

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

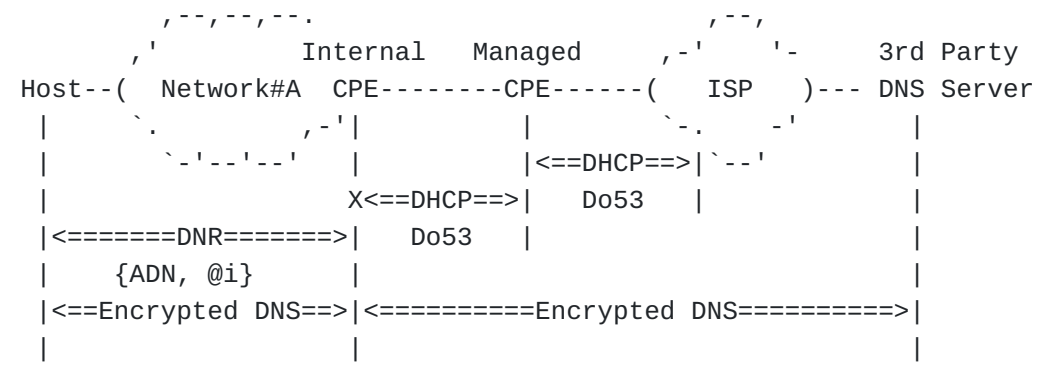
forwarder. The internal CPE may support a mechanism (e.g., [I-D.ietf-add-split-horizon-authority]) to resolve split-horizon domains (e.g., provider's private name discussed in Section 2 of [RFC6731]).




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

Figure 7: Example of an Internal CPE Hosting a Forwarder

An unmanaged CPE can be used to host an encrypted DNS forwarder even if the managed CPE does not support DNR. In the example depicted in Figure 8, the ISP uses DHCP to provision Do53 resolvers to managed CPEs, while DNR is enabled between the internal CPE and the hosts it services. The internal CPE ignores the DNS configuration that it receives from the managed CPE.




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

Figure 8: Example of an Internal CPE Hosting a Forwarder (2)

## 6. 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 resolver hosted by the ISP, in particular. If the ADN is not discovered using DHCP/RA, such hosts will have to fall back 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 a case.

## 7. Security Considerations

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

## 8. IANA Considerations

This document does not require any IANA action.

## 9. Acknowledgements

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

Thanks to Eliot Lear for the ISE review.

## 10. References

### 10.1. Normative References

**[I-D.ietf-add-ddr]** Pauly, T., Kinnear, E., Wood, C. A., McManus, P., and T. Jensen, "Discovery of Designated Resolvers", Work in Progress, Internet-Draft, draft-ietf-add-ddr-10, 5 August 2022, <https://www.ietf.org/archive/id/draft-ietf-add-ddr-10.txt>.

**[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)", Work in Progress, Internet-Draft, draft-ietf-add-dnr-13, 13 August 2022, <https://www.ietf.org/archive/id/draft-ietf-add-dnr-13.txt>.

### 10.2. Informative References

**[I-D.ietf-add-split-horizon-authority]**

Reddy.K, T., Wing, D., Smith, K., and B. M. Schwartz, "Establishing Local DNS Authority in Split-Horizon Environments", Work in Progress, Internet-Draft, draft-ietf-add-split-horizon-authority-02, 20 September 2022, <https://www.ietf.org/archive/id/draft-ietf-add-split-horizon-authority-02.txt>.

**[I-D.ietf-opsawg-add-encrypted-dns]** Boucadair, M. and T. Reddy.K, "RADIUS Extensions for Encrypted DNS", Work in Progress, Internet-Draft, draft-ietf-opsawg-add-encrypted-dns-03, 6 October 2022, <https://www.ietf.org/archive/id/draft-ietf-opsawg-add-encrypted-dns-03.txt>.

**[RFC1918]** Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <https://www.rfc-editor.org/info/rfc1918>.

**[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>.

**[RFC4192]** Baker, F., Lear, E., and R. Droms, "Procedures for Renumbering an IPv6 Network without a Flag Day", RFC 4192, DOI 10.17487/RFC4192, September 2005, <https://www.rfc-editor.org/info/rfc4192>.

**[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>.

**[RFC6598]** Weil, J., Kuarsingh, V., Donley, C., Liljenstolpe, C., and M. Azinger, "IANA-Reserved IPv4 Prefix for Shared Address Space", BCP 153, RFC 6598, DOI 10.17487/RFC6598, April 2012, <https://www.rfc-editor.org/info/rfc6598>.

**[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>.

**[RFC6890]** Cotton, M., Vegoda, L., Bonica, R., Ed., and B. Haberman, "Special-Purpose IP Address Registries", BCP 153, RFC

6890, DOI 10.17487/RFC6890, April 2013, <https://www.rfc-editor.org/info/rfc6890>.

[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>.

[RFC8190] Bonica, R., Cotton, M., Haberman, B., and L. Vegoda, "Updates to the Special-Purpose IP Address Registries", BCP 153, RFC 8190, DOI 10.17487/RFC8190, June 2017, <https://www.rfc-editor.org/info/rfc8190>.

[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>.

[RFC8585] Palet Martinez, J., Liu, H. M.-H., and M. Kawashima, "Requirements for IPv6 Customer Edge Routers to Support IPv4-as-a-Service", RFC 8585, DOI 10.17487/RFC8585, May 2019, <https://www.rfc-editor.org/info/rfc8585>.

[RFC9250] Huitema, C., Dickinson, S., and A. Mankin, "DNS over Dedicated QUIC Connections", RFC 9250, DOI 10.17487/

RFC9250, May 2022, <https://www.rfc-editor.org/info/rfc9250>.

**[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
35000 Rennes
France

Email: mohamed.boucadair@orange.com

Tirumaleswar Reddy (editor)
Nokia
India

Email: kondtir@gmail.com

Dan Wing
Citrix Systems, Inc.
United States of America

Email: dwing-ietf@fuggles.com

Neil Cook
Open-Xchange
United Kingdom

Email: neil.cook@noware.co.uk

Tommy Jensen
Microsoft
United States of America

Email: tojens@microsoft.com