Workgroup: ADD Working Group
Internet-Draft:
draft-stark-add-dns-forwarder-analysis-00
Published: 15 June 2021
Intended Status: Informational
Expires: 17 December 2021
Authors: B. Stark C. Box
AT&T BT

Analysis of DNS Forwarder Scenario Relative to DDR and DNR

Abstract

This draft analyzes the behaviors that residential end users and home network owners (e.g., parents of young children) might experience when operating systems and clients support [I-D.ietf-add-ddr] and/or [I-D.ietf-add-dnr] for discovery of encrypted DNS services and the CE router of the home network offers itself as the Do53 resolver. This use case is explicitly mentioned in [I-D.ietf-add-requirements] Section 3.2 and has several requirements related to it. This draft has two goals: determine if the analysis it provides is accurate and, if it is accurate, determine if the behavior is acceptable to the WG or if there should be changes to either of the discovery mechanisms.

Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the mailing list (add@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/add/.

Source for this draft and an issue tracker can be found at https://github.com/bhstark2/dns-forwarder-analysis.

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 17 December 2021.

Table of Contents

1. Introduction

This draft analyzes the behaviors that residential end users and home network owners (e.g., parents of young children) might experience when operating systems and clients support [I-D.ietf-add-ddr] and/or [I-D.ietf-add-dnr] for discovery of encrypted DNS services and the CE router of the home network offers itself as the Do53 resolver. This use case is explicitly mentioned in [I-D.ietf-add-requirements] Section 3.2 and has several requirements related to it.

This draft has two goals:

- determine if the analysis it provides is accurate

- if it is accurate, determine if the behavior is acceptable to the WG or if there should be changes to either of the discovery mechanisms.

Becoming a WG draft is *not* a goal of this draft. There is and will be no request for adoption by any WG.

While DNS forwarders / proxies may exist in environments other than home networks (e.g., hotspots, small businesses), this draft does not attempt to examine those usages. This draft is focused on home networks.

2. Conventions and Definitions

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.

3. Background

Having a DNS forwarder in the CE router that is advertised to the LAN using DHCP and RDNSS options is a common deployment model for many ISPs and is also the default in many retail consumer routers (e.g., Netgear).

[I-D.ietf-add-requirements] contains the following text related to this use case:

"Many networks offer a Do53 resolver on an address that is not globally meaningful, e.g. [RFC1918], link-local or unique local addresses. To support the discovery of encrypted DNS in these environments, a means is needed for the discovery process to work from a locally-addressed Do53 resolver to an encrypted DNS resolver that is accessible either at the same (local) address, or at a different global address. Both options need to be supported."

"R4.1 If the local network resolver is a forwarder that does not offer encrypted DNS service, an upstream encrypted resolver SHOULD be retrievable via queries sent to that forwarder."

"R4.2 Achieving requirement 4.1 SHOULD NOT require any changes to DNS forwarders hosted on non-upgradable legacy network devices."

In the context of a home network, there are several reasons why this deployment model is used. Some reasons are:

*Provide local name resolution

*Captive portal (Note that [RFC8952] defines an architecture that does not rely on "breaking" DNS; however, there exist many legacy devices with captive portals that do rely on "breaking" DNS.}

*Provide filtering (aka parental controls) and DNS-based vulnerability assessment in the CE router. Note that [I-D.ietf-add-requirements] describes this sort of filtering and monitoring behavior as an attack; nonetheless, this functionality is popular with many people -- especially parents.

*Caching responses to improve DNS performance

4. Scenario Analysis

The following sections will analyze what behavior a user is expected to see when certain conditions exist. In all cases, it's assumed the CE router is advertising itself as the Do53 server (using DHCP and/or RA). The clients and OSs that are of interest in these scenarios are using whatever Do53 server is advertised to them by DHCP/RA. There may be clients and devices that use other Do53 servers; those are out of scope of this analysis. Analyzing the behavior of clients that do not support either DoH or DoT, or do not support any mechanism to discover encrypted servers are also out of scope.

Assumptions common to all scenarios are:

*Common OSs support both DNR and DDR

*Some applications (e.g., browsers) support DDR

*No Certificate Authority will sign a certificate with a private IP address in a SAN

4.1. Scenario 1: No changes to CE router

Assumptions:

*The CE router (including its DNS forwarder and DHCP/RA capabilities) are not updated.

Expected behaviors:

*There will be no DHCP or RA advertisement of encrypted servers.

*The DNS forwarder will forward DDR queries (dns://resolver.arpa) to the DNS recursive resolver the CE router is configured to use.

*If that recursive resolver has the appropriate SVCB record, it will provide that in the response that is returned.

*The querying OS/app will determine that the IP address of its Unencrypted Resolver (the CE router) and the IP address of the Unencrypted Resolver in the supplied certificate do not match and will not do "authenticated discovery".

*The querying OS/app will determine that the IP address of its Unencrypted Resolver (the CE router) does not match the IP address of the Encrypted Resolver and will not do "opportunistic discovery".

*The OS/app will not discover a local Encrypted Resolver.

The end result is that no Encrypted Resolver will be used by an OS or app that uses DDR or DNR to discover an Encrypted Resolver, unless the OS or app subsequently uses some non-standard mechanism to select an Encrypted Resolver. Note that this suggests that the DDR and DNR proposals in their current form do not satisfy the requirement "R4.2 Achieving requirement 4.1 SHOULD NOT require any changes to DNS forwarders hosted on non-upgradable legacy network devices."

Also note that non-upgraded legacy routers will not satisfy the [I-D.ietf-add-ddr] requirement that a "DNS forwarder SHOULD NOT forward queries for "resolver.arpa" upstream." If the CE router were updated to not forward queries for "resolver.arpa" upstream, the end result would not change. Since this scenario provides the same end result, it isn't broken out separately.

4.2. Scenario 2: CE router updated to provide DNR in DHCP/RA

Assumptions:

*The CE router is updated to provide Encrypted Resolver info in DHCP/RA

*The CE router gets its Encrypted Resolver info from DHCP; getting that was part of the update

*The upstream ISP has updated its core network resolver to support encryption, and announces this resolver in DHCP

Expected behaviors:

*OSs will use the Encrypted Resolver

*Applications that try "resolver.arpa" will not do their own upgrade, because that will fail

Additional results:

*Local name resolution is broken?

*Legacy captive portal is now broken?

*Filtering in the CE router (parental controls and other security mechanisms enabled by the home network owner) is now broken

*Any filtering deployed in the core network resolver continues to operate

*No local caching

4.3. Scenario 3: CE router updated to support opportunistic encryption to its DNS forwarder

Assumptions:

*The CE router supports encrypted connectivity to its DNS forwarder

*The CE router is updated to provide Encrypted Resolver info in DHCP/RA

*The CE router is updated to reply to dns://resolver.arpa; SVCB record points to the CE router with a self-signed certificate

Note that the effort do do these upgrades is considered to be rather large.

Expected behaviors:

*Some OSs and applications accept DDR Opportunistic Discovery, resulting in use of the CE router's Encrypted Resolver.

*Some OSs and applications do not.

*Across a range of households, and even within a single household, there is inconsistent behavior.

5. Conclusions

Since Scenario 3 is considered a large effort and the resulting behavior is unpredictable, it is unlikely to be pursued.

Since Scenario 2 will break some of the functionality that a significant number of home network owners have purposefully enabled (e.g., router-based DNS-based parental controls), will break existing captive portal implementations used to simplify setup of broadband connections, and may break local name resolution (?) it is unlikely to be pursued.

This leaves Scenario 1 (do nothing in routers that provide DNS forwarder).

6. Questions for the WG

Are these the results we want to achieve with Encrypted Resolver discovery mechanisms?

7. Security Considerations

Breaking the security mechanisms that many users currently have enabled in their home network routers (e.g., DNS filtering) will worsen the security of those users. While these mehanisms are not perfect, and can easily be bypassed by client applications that run DoH, this does not make them completely useless.

8. IANA Considerations

This document has no IANA actions.

9. References

9.1. 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/rfc/rfc2119>.

[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/rfc/rfc8174>.

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", Work in Progress, Internet-Draft, draft-ietf-add-ddr-01, 14 June 2021, <https://tools.ietf.org/html/draft-ietf-add-ddr-01>.

[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-02, 17 May 2021, <https://tools.ietf.org/html/draft-ietf-add-dnr-02>.

[I-D.ietf-add-requirements] Box, C., Pauly, T., Wood, C. A., Reddy, T., and D. Migault, "Requirements for Discovering Designated Resolvers", Work in Progress, Internet-Draft, draft-ietf-add-requirements-00, 8 March 2021, <https://tools.ietf.org/html/draft-ietf-add-requirements-00>.

[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/rfc/rfc1918>.

[RFC8952] Larose, K., Dolson, D., and H. Liu, "Captive Portal Architecture", RFC 8952, DOI 10.17487/RFC8952, November 2020, <https://www.rfc-editor.org/rfc/rfc8952>.

Acknowledgments

Thanks to ...

Authors' Addresses

Barbara Stark
AT&T
Austin, TX,
United States of America

Email: barbara.stark@att.com

Chris Box
BT
Bristol
United Kingdom

Email: chris.box@bt.com