

add
Internet-Draft
Intended status: Informational
Expires: January 29, 2021

D. Migault
Ericsson
July 28, 2020

DNS Resolver Discovery Protocol (DRDP)
draft-mglt-add-rdp-isp-00

Abstract

The DNS Resolving service Discovery Protocol (DRDP) enables to discover resolving services available and eventually upgrade to an encrypted resolving service.

DRDP requires a resolving domain or a pointer to a list of resolving domains. Currently ISP or CPEs do not advertise resolving domain or pointers to resolving domains which does not make possible for a DNS client to discover potential resolving services - such as encrypted DNS for example - made available by the ISP.

Instead, ISPs or CPE advertise via DHCP the IP address of the host with a IA Address Option [[RFC3315](#)] and the IP addresses of the resolver provided by the ISP with Recursive Name Server option [[RFC3646](#)].

This document describes a procedure for a DNS client to derive resolving domains from the legacy configuration of the host.

This is expected to ease the deployment of encrypted DNS from ISP as it will enable OS, applications to discover resolving service put in place by the ISP even though the CPE has not been upgraded.

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."

Internet-Draft

DRDP

July 2020

This Internet-Draft will expire on January 29, 2021.

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

1.	Requirements Notation	2
2.	Introduction	2
3.	IP to Pointers	5
3.1.	RD Pointer from Interface Address (IA)	5
3.2.	RD Pointer from Resolver IP address	5
3.3.	Cross Verification	6
3.4.	Configuration expected by the network operator	6
4.	Security Consideration	6
5.	References	6
5.1.	Normative References	6
5.2.	Informative References	7
	Author's Address	7

[1.](#) Requirements Notation

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.

[2.](#) Introduction

This document describes how a DNS client can discover resolving

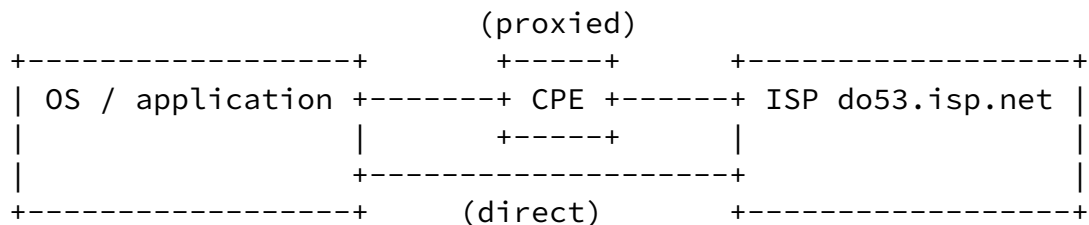
services made available by a network operator. The procedure requires minimal changes from the network operator and results in the encryption of a significant portion of the DNS traffic. The limitation relies on the CPE being upgraded to support encrypted DNS to resolve local scope names.

The considered architecture that is currently deployed is represented below.

In most architecture, the CPE co-hosts an authoritative server for the local zones (such as .home.arpa or .local) that are not represented in the global DNS architecture. The CPE in most common deployment works as a forwarder, that is, it responds to a query when it is either authoritative for the answer or the answer is in its cache. In any other case, the CPE resolves the query to the resolver of the ISP represented as (do53.isp.net).

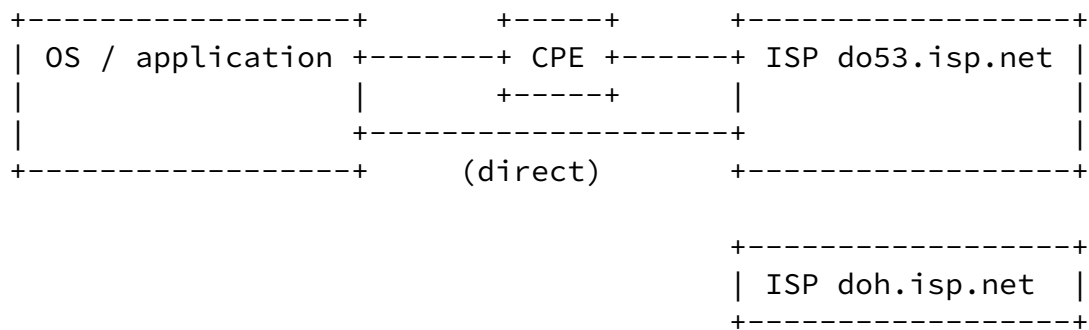
In most architecture, OS and CPE are provisioned IP addresses via DHCP IA Address Option [[RFC3315](#)]. This IP address is used for the connectivity purpose. Similarly, OS and CPE are provisioned IP addresses that are used to reach the resolving service provided by the network operator via the DHCP Recursive Name Server option [[RFC3646](#)]. These IP addresses may be local scope or global.

The application - such as a web browser - does not get provisioned via DHCP but is supposed to be able to access the IP addresses provisioned on the OS.



When the network operator introduces a new resolving service such as providing a DoH resolving service for example, the network operator would like to make that server available to the OS, application and the CPE. In the figure below, the new introduced service is designated as doh.isp.net and is expected to implement DoH.

(proxied)

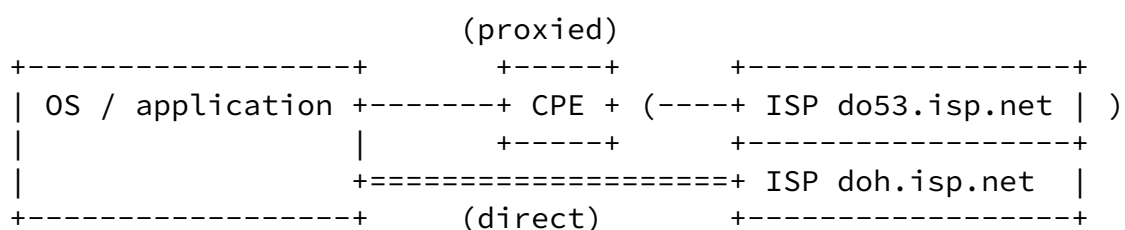


Because not all DNS clients will be upgraded at the same time and that DNS client, the network operator will need to support both do53.isp.net and doh.isp.net.

One possibility would be to co-host do53.isp.net and doh.isp.net with the same IP address. Such alternative is not considered in this document as in the long term it would require the network operator to co-host under the same IP address all different variant of the resolving services. This provides a to high contrail on the infrastructure.

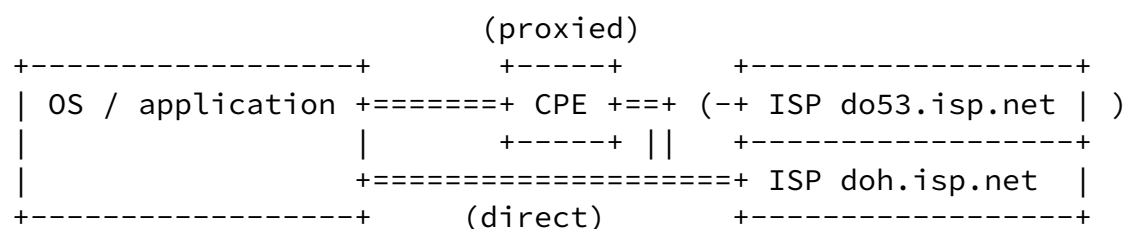
Having the DNS client try and test what is actually supported is also not considered in this document either.

When the CPE cannot be upgraded, only the OS or application can discover and upgrade to the doh.isp.net. Only application/OS that support the DRDP and this document will benefit from such upgrade. Maximization of encrypted DNS traffic is performed if the OS/application 1) sends the DNS queries that are resolved globally to doh.isp.net 2) limiting the DNS traffic to the CPE to the one associated to the local network.



When the CPE can be upgraded, it is expected that it implements a DoH resolver as well as a DNS client that implement this document. Since the DNS client of the CPE supports this specification, it is expected that the CPE will send its traffic only to doh.isp.net. Since the CPE is also being upgraded to provide a DoH resolving service, OS and application are expected to be connected to the CPE using the DoH resolving service using the mechanism described in this document or other appropriated mechanism. Note that such communication while encrypted MAY NOT be authenticated.

Authentication MAY be provided is the homenetwork enables DNSSEC (and the distribution of the Trust Anchor) or the certificate.



[3.](#) IP to Pointers

This document describe how to generate a pointer to resolving domains (Pointer) from the Interface address (IA) ([Section 3.1](#)) as well as from the IP address of the resolvers [Section 3.2](#) when these IP addresses are global.

[3.1.](#) RD Pointer from Interface Address (IA)

This section describes the procedure to derive resolving domains (RD) or RD Pointers from an Interface Address (IA), that is the IP or network assigned by the network operator to provide connectivity to the host.

1. Get a global IA: If the IA IP address is an IPv4 address of local scope, the DNS client establish the public IP address used by the network operator using appropriated mechanisms such as STUN [[RFC3489](#)] for example. The exchange SHOULD be protected by (D)TLS and the DNS client considers the mapped IP address as it global IA IP address. In any other case, the IA IP address is global.

2. Proceed to a reverse resolution and consider the resulting domain (IA Pointer) as a Pointer
3. DRDP [[I-D.mglt-add-rdp](#)] MAY be started from the resulting pointer. Optionally the DNS client MAY retrieve the RD to proceed to additional verifications - see [Section 3.3](#). Note that such conversion places a lot of trust into the STUN resolution when such resolution is required.

[3.2](#). RD Pointer from Resolver IP address

This section describes the procedure to derive RD from the IP address of the resolving service. The procedure only works when the resolver is provisioned with a global IP address and MAY not be applicable for some DNS client.

1. Proceed to a reverse resolution and consider the resulting domain (Resolver Pointer) as a Pointer.
2. DRDP [[I-D.mglt-add-rdp](#)] MAY be started from the resulting pointer, however, it is recommended to retrieve the RD and proceed to additional steps described in [Section 3.3](#). Note that such conversion places a lot of trust into the DHCP provisioning.

[3.3](#). Cross Verification

When the discovery of the public IA involves a third party (or is not sufficiently protected), it is RECOMMENDED to derive the Pointer from Resolvers IP as described in [Section 3.2](#) - when that is possible.

In that case, the following steps SHOULD be performed:

1. Retrieve RD (RD_IA) from the IA Pointer.
2. Retrieve RD (RD_Resolver) from the Resolver Pointer.
3. Consider the resolving domains shared by the two Pointers as provided by your network operator and other as independent resolving domains.

3.4. Configuration expected by the network operator

The network operator is expected to update the forward zone of the CPE as follows:

```
b._dns.cpe_isp_fqdn.isp.net PTR resolver.isp.net
b._dns.cpe_isp_fqdn.isp.net PTR third_party_delegated_resolver.isp.net
```

The network operator is expected to update the zone that corresponds to the resolving domains as follows:

```
b._dns.resolver.isp.net PTR resolver.isp.net
b._dns.resolver.isp.net PTR third_party_delegated_resolver.isp.net
```

4. Security Consideration

Rough STUN server

Rough DHCP

5. References

5.1. 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>>.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [RFC 3315](#), DOI 10.17487/RFC3315, July 2003, <<https://www.rfc-editor.org/info/rfc3315>>.

[RFC3489] Rosenberg, J., Weinberger, J., Huitema, C., and R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", [RFC 3489](#),

DOI 10.17487/RFC3489, March 2003,
<<https://www.rfc-editor.org/info/rfc3489>>.

[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>>.

[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>>.

[5.2](#). Informative References

[I-D.mglt-add-rdp]
Migault, D., "DNS Resolver Discovery Protocol (DRDP)",
[draft-mglt-add-rdp-02](#) (work in progress), May 2020.

Author's Address

Daniel Migault
Ericsson
8275 Trans Canada Route
Saint Laurent, QC 4S 0B6
Canada

EMail: daniel.migault@ericsson.com