DNS over HTTP resolver announcement Using DHCP or Router Advertisements
draft-peterson-doh-dhcp-00

Abstract

This specification describes a DHCP option and Router Advertisement (RA) extension to inform clients of the presents of a DNS over HTTP (DoH) service to be used for DNS queries.

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 October 27, 2019.

Copyright Notice

Copyright (c) 2019 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.
1. Introduction

DHCPv4 [RFC3132], DHCPv6 [RFC3646], and IPv6 Router Announcements [RFC8106] all provide means to inform clients of available resolvers using the incumbent DNS protocol for querying, however there is no means of specifying alternate protocols to perform DNS queries.

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. The DoH Option

The DoH DHCP/RA option informs the client that a DoH service is available for use for answering DNS queries. In order to support multiple "classes" of clients, the network operator can provide the URI template [RFC6570] which describes how a client can construct the URL to use for resolution. Whilst DoH servers may support multiple URI Templates, only one template MUST be transmitted.

URI Templates that contain a host name SHOULD only be sent where a DHCP server or Router provide name servers, as name resolution of any host name in the template will require clients to use the non-DoH servers provided or manual configuration.

The maximum length of the URI template that can be carried in IPv4 DHCP is 255 bytes, so URI templates longer than 255 bytes SHOULD NOT be used in IPv6 DHCP or IPv6 RA.
3.1. IPv4 DHCP Option

The format of the IPv4 DoH DHCP option is shown below.

```
+-------+-------+-------+-------+-------+-------+-------+-------+
|   Code   |  Length  | URI Template |
+-------+-------+-------+-------+-------+-------+-------+-------+
```

- Code: The DoH DHCPv4 option (one octet).
- Length: The length, in octets of the URI template.
- URI Template: The DoH server available, encoded following the rules of [RFC3986].

3.2. IPv6 DHCP Option

The format of the IPv6 Captive-Portal DHCP option is shown below.

```
+-------+-------+-------+-------+-------+-------+-------+-------+
| option-code | option-len | URI Template |
+-------+-------+-------+-------+-------+-------+-------+-------+
```

- option-code: TODO (two octets)
- option-len: The length, in octects of the URI Template.
- URI Template: The DoH server

3.3. The DoH IPv6 RA Option

The format of the DoH Router Advertisement option is shown below.
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Length    |      URI Template             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    o Type: TODO (one octet)
    o Length: 8-bit unsigned integer representing the entire length
      of all fields, in units of 8 bytes.
    o URI Template: The DoH server available for use. This should be
      padded with NULL (0x0) to make the total option length (including
      the Type and Length fields) a multiple of 8 bytes.

4. Security Considerations

An attacker with the ability to inject DHCP messages could include
this option and present a malicious resolver.

TODO: Further risk and threat assessments.

5. IANA Considerations

TODO: This section must be updated after assignments have been
issued.

This document requires the assignment of an option code assigned
under the "BOOTP Vendor Extensions and DHCP Options"
[bootp-registry], in addition to an option code assigned under the
"Option Codes" registry under DHCPv6 parameters [dhcpv6-registry].

Also, an assignment for an IPv6 RA Option Type from the "IPv6
Neighbor Discovery Option Formats" registry under ICMPv6 params
[icmpv6-registry].

6. References

6.1. 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,
6.2. Informative References

[bootp-registry]

[dhcpv6-registry]

[icmpv6-registry]


[RFC3646]

[RFC8106]
Acknowledgments

TODO

Author’s Address

Thomas Peterson

Email: nosretep.samoh@gmail.com