DNS over Transport Layer Security announcements using DHCP or Router Advertisement
draft-peterson-dot-dhcp-01

Abstract

This specification describes a DHCP option and Router Advertisement (RA) extension to inform clients of the presence of DNS resolvers with Transport Layer Security (TLS).

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 January 23, 2020.

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 [RFC2131], 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.

"DoT", "Do53" and other related abbreviations follow the definitions as defined in [I-D.draft-hoffman-dns-terminology-ter-01].

3. The DNS over TLS Option

The DoT DHCP/RA option informs the client that a DoT service is available for use for answering DNS queries using the same IP address(es) returned in Do53 DNS Server DHCP/RA options. Thus networks which announce DoT services MUST announce DNS resolver availability via their respective options, and provide a TLS certificate on the DoT service which passes verification ([RFC6125]) against the DNS Host Name provided in the DoT DHCP/RA option.

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

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

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Code     |      Len      |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                          DNS Host Name                        |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code: The DoT DHCPv4 option (one octet)
Len: Length of the DNS Host Name
DNS Host Name: The DNS Host Name

3.2. IPv6 DHCP Option

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

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          option-code          |           option-len           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                           DNS Host Name                        |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

option-code: TODO (two octets)
option-len: Length of the DNS Host Name, in octects
DNS Servers: The DNS Host Name

3.3. The DoT IPv6 RA Option

The format of the DoT Router Advertisement option is shown below.
3.4. Trust Anchoring

TODO: Put in considerations for using DANE and/or existing certificate authorities for trust anchoring.

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 parameters [icmpv6-registry].

6. References
6.1. Normative References

[I-D.draft-hoffman-dns-terminology-ter-01]


6.2. Informative References

[bootp-registry]

[ dhcpv6-registry]
Acknowledgments

The author would like to acknowledge the extensive feedback from Martin Thomson.

Author’s Address

Thomas Peterson

Email: nosretep.samoh@gmail.com