DNSOP Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 5, 2017

R. Licht
Charter Communications
D. Lawrence, Ed.
Akamai Technologies
January 2017

Client ID in Forwarded DNS Queries
draft-tale-dnsop-edns0-clientid-00

Abstract

This draft defines a DNS EDNS option to carry a client-specific identifier in DNS queries, with guidance for privacy protection of such information.

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 http://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 July 5, 2017.

Table of Contents

1. Introduction

Some DNS operators generate, or wish to generate, customized DNS responses based on the originator of a DNS query. For example, [RFC7871], "Client Subnet in DNS Queries", defines a method to convey partial IP network address information about the device that originated a DNS request, so that a response could be targeted to be topographically near the source.

Some specialized services, however, need more precise client identity information to function adequately. For example, a parental control service that restricts access to particular domains from particular devices needs to have a device-specific identifier.

This document defines an EDNS [RFC6891] option to convey client identification information that is relevant to the DNS query. It is added by software on the client's local area network, for transmission to the upstream DNS provider.

A similar EDNS option is already being used on the public Internet in two different implementations. One is between the [dnsmasq] resolver on the client side and Nominum's [Vantio_CacheServe] upstream. It uses EDNS option code 65073 from the "Reserved for Local/Experimental Use" range. The other implementation is for Cisco's [Umbrella], aka OpenDNS, which took option code 26946 from the middle of the "Unassigned" range. This document codifies a more extensible format than Nominum's but currently less so than Cisco's, and is intended to supersede those non-standard options. The authors recognize that Cisco's enhanced format is desired by at least a couple of

organizations but present this simplied version as a starting point for discussion.

This option is intended only for constrained environments where the use of the option can be carefully controlled. It is completely optional and should be ignored by most DNS software.

2. Privacy Considerations

The IETF is actively working on enhancing DNS privacy [DPRIVE_Working_Group], and the reinjection of personally identifiable information has been identified as a problematic design pattern [I-D.hardie-privsec-metadata-insertion].

Because this option trasmits information that is meant to identify specific clients, to be considered compliant with this draft implementations MUST NOT add the option without explicit opt-in by an administrator on the local area network. For example, agreeing to the terms of service for a device-specific DNS filtering product would allow the option to be enabled, and only for communication to the product's DNS server(s).

Implementers need to be aware of the various laws and regulations governing handling personal data, but they are out of scope of this document.

No explicit provision is made in the protocol to opt-out. For more discussion on this, see Section 7, "Security Considerations".

3. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]

For a comprehensive treatment of DNS terms, please see [RFC7719]. This document uses the following additional terms:

ECID EDNS Client Identification.

Client The user or device that originates a DNS lookup.

Nameserver A DNS server capable of resolving a DNS query and formulating a response.

Forwarding Resolver A nameserver that does not do iterative resolution itself, but instead passes that responsibility to another resolver, called a "Forwarder" in [RFC2308] section 1.

EUI-48 48 bit Extended Unique Identifier.

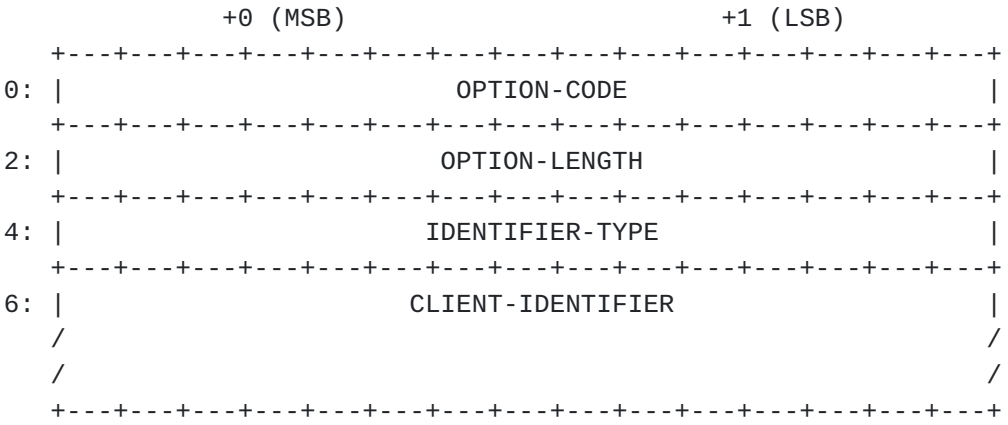
EUI-64 64 bit Extended Unique Identifier.

MAC Media Access Control.

Tailored Response A response from a nameserver that is customized based on a policy defined for the client requesting the query.

4. Option Format

This protocol uses an EDNS [RFC6891] option to include client identification information in DNS messages. The option is structured as follows:



OPTION-CODE 2 octets per [RFC6891]. For ECID the code is TBD by IANA.

OPTION-LENGTH: 2 octets per [RFC6891]. Contains the length of the payload following OPTION-LENGTH, in octets.

IDENTIFIER-TYPE 2 octets, indicates the format of the CLIENT-IDENTIFIER contained in the option. This document only defines the format for 3 different types of CLIENT-IDENTIFIER; namely, a 48-bit MAC address, an IPv4 address, or an IPv6 address. Including the IDENTIFIER-TYPE indicator as part of the option allows for easy evolution of ECID to include other types of identifying addresses, such as EUI-48 or EUI-64 [RFC7042] or a DHCP Unique Identifier [RFC3315] and [RFC6355], as devices and needs change. The IDENTIFIER-TYPE could even indicate that the CLIENT-IDENTIFIER is a specially encrypted identifier that only the DNS Nameserver can decrypt. The following IDENTIFIER-TYPE values are defined. The values chosen correspond to the address family codes as assigned by IANA in [Address Family Numbers].

IDENTIFIER-TYPE 16389 (0x40 0x05), 48 octet MAC address
IDENTIFIER-TYPE 1 (0x00 0x01), 32 octet IP version 4 address
IDENTIFIER-TYPE 2 (0x00 0x02), 128 octet IP version 6 address Note that some initial implementations MAY limit support to the IDENTIFIER-TYPE 16389 (48-bit MAC), with other defined IDENTIFIER-TYPE values simply reserved as described above.

CLIENT-IDENTIFIER variable number of octets, depending on the value of IDENTIFIER-TYPE. The IDENTIFIER-TYPE, and its corresponding CLIENT-IDENTIFIER, fields may be repeated in a single ECID option, increasing OPTION-LENGTH correspondingly. However, the same IDENTIFIER-TYPE may not appear more than once. (This should be reflected in the packet diagram but I still have to hunt down whether there's a convention for that.

All fields are in network byte order ("big-endian", per [RFC1700], Data Notation).

5. Protocol Description

5.1. DNS Query

Any client that originates a DNS query message MAY include the ECID option in the DNS Query message. It is normally expected that the client itself would not do this, but rather that it will be added by the local forwarding resolver.

When a DNS forwarding resolver, provided as part of a router for example, receives a DNS query message from the originating client it adds any ECID IDENTIFIER-TYPE / CLIENT-IDENTIFIER pairs for IDENTIFIER-TYPEs that it supports but which are not present in the existing client request. It then sends the request to the upstream full-service resolver.

Because the option contains personally identifiable information, it should be protected by either only being used within Autonomous Systems [RFC1930] controlled by the same provider, or by going over an opaque channel such as DNS over TLS [RFC7858]. It MUST NOT be sent in clear-text across the Internet.

5.2. DNS Response

The logic used by a full-service resolver to customize a response based on ECID is out of scope for this document. The resolver MUST NOT include the ECID option in any queries that it makes to external authoritative DNS servers.

For possible caching purposes, the forwarding resolver needs to know whether filtering affected the response. If the name resolution involved any names for which customization was possible, even if such filtering resulted in delivering the original data, the response SHOULD include an ECID option which contains the IDENTIFIER-TYPE and CLIENT-IDENTIFIER that were considered for filtering.

For example, if a filter is set such that only names in the example.com domain are possibly restricted to some devices, then a request for foo.example.com would have the ECID in the response even when the request came from a device which was not restricted. Requests for any other names would not include ECID in the response.

So that the caching forwarding resolver does not need to have any knowledge about what filters are in place, it is the full-service resolver's responsibility to adjust any TTLs in the response as might be dictated by the filter policy it has configured. That is, if some name is filtered only between the hours of 09:00 and 17:00 and a request is received for that name at 16:59:59, the TTL on a positive response or the SOA ncache field on a negative response should be set to just one second and the ECID option included as described above.

If the request contains a malformed ECID option, such as CLIENT-IDENTIFIER not correctly matching the length of described by OPTION-LENGTH and IDENTIFIER-TYPE, the resolver SHOULD reply with DNS rcode FORMERR.

If the resolver by policy does not respond to requests that are lacking ECID of the appropriate IDENTIFIER-TYPE, it SHOULD reply with DNS rcode REFUSED.

6. NAT Considerations

Devices that perform Network Address Translation (NAT) need not give special consideration for ECID. NAT translates between a layer 3 private IP address assigned to a client device on the Local Area Network and a layer 3 public IP address for use within the Wide Area Network.

ECID information identifies a client device by a different means, e.g. its layer 2 address. A device's identifier is NOT impacted by NAT. Therefore, DNS queries may be passed without modification of any ECID information.

7. Security Considerations

The identifier of the client that initiated the request will be visible to all servers that are passed the ECID option, and the various devices on the path between the local network and the full-service resolver being used by the forwarding resolver.

DNS filtering products are easy circumvented and should not be considered real security measures. With commonly available tools it is trivial to discover the non-filtered DNS responses and use them in place of the filtered responses.

Along those lines, opting out of this specific protocol is as simple as using a different resolver, such as a full-service resolver on the device itself or one of the well-known public resolvers. Of course, other devices on the local network will still be able to see unencrypted DNS requests from the device, and the only way to really protect against such monitoring is to use an opaque tunnel to a trusted resolver.

8. IANA Considerations

IANA is requested to assign a new value in the DNS EDNS Option Codes registry for the Device ID option.

9. Acknowledgements

The authors wish to thank the Barry Greene, Martin Deen and Benjamin Petrin for their feedback and review during the initial development of this document.

10. References

10.1. Normative References

[Address_Family_Numbers]
"Address Family Numbers", n.d., <http://www.iana.org/assignments/address-family-numbers/>.

[RFC1700] Reynolds, J. and J. Postel, "Assigned Numbers", RFC 1700, DOI 10.17487/RFC1700, October 1994, <http://www.rfc-editor.org/info/rfc1700>.

[RFC1930] Hawkinson, J. and T. Bates, "Guidelines for creation, selection, and registration of an Autonomous System (AS)", BCP 6, RFC 1930, DOI 10.17487/RFC1930, March 1996, <http://www.rfc-editor.org/info/rfc1930>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2308] Andrews, M., "Negative Caching of DNS Queries (DNS NCACHE)", RFC 2308, DOI 10.17487/RFC2308, March 1998, <http://www.rfc-editor.org/info/rfc2308>.

[RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, DOI 10.17487/RFC6891, April 2013, <http://www.rfc-editor.org/info/rfc6891>.

[RFC7719] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", RFC 7719, DOI 10.17487/RFC7719, December 2015, <http://www.rfc-editor.org/info/rfc7719>.

[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, <http://www.rfc-editor.org/info/rfc7858>.

[RFC7871] Contavalli, C., van der Gaast, W., Lawrence, D., and W. Kumari, "Client Subnet in DNS Queries", RFC 7871, DOI 10.17487/RFC7871, May 2016, <http://www.rfc-editor.org/info/rfc7871>.

10.2. Informative References

[dnsmasq] "dnsmasq", n.d., <http://www.thekelleys.org.uk/dnsmasq/doc.html>.

[DPRIVE_Working_Group] "DPRIVE Working Group", n.d., <https://datatracker.ietf.org/wg/dprive/charter/>.

[I-D.hardie-privsec-metadata-insertion] Hardie, T., "Design considerations for Metadata Insertion", draft-hardie-privsec-metadata-insertion-05 (work in progress), January 2017.

[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, <http://www.rfc-editor.org/info/rfc3315>.

[RFC6355] Narten, T. and J. Johnson, "Definition of the UUID-Based DHCPv6 Unique Identifier (DUID-UUID)", RFC 6355, DOI 10.17487/RFC6355, August 2011, <http://www.rfc-editor.org/info/rfc6355>.

[RFC7042] Eastlake 3rd, D. and J. Abley, "IANA Considerations and IETF Protocol and Documentation Usage for IEEE 802 Parameters", BCP 141, RFC 7042, DOI 10.17487/RFC7042, October 2013, <http://www.rfc-editor.org/info/rfc7042>.

[Umbrella] "Umbrella", n.d., <https://docs.umbrella.com/developer/networkdevices-api/identifying-dns-traffic2>.

[Vantio_CacheServe] "Vantio CacheServe", n.d., <http://www.nominum.com/product/caching-dns/>.

Authors' Addresses

Robert Licht
Charter Communications
13820 Sunrise Valley Dr
Herndon VA 20171
USA

Email: robert.licht@charter.com

David C Lawrence (editor)
Akamai Technologies
150 Broadway
Cambridge MA 02142-1054
USA

Email: tale@akamai.com