

Network Working Group
Internet-Draft
Updates: [4361](#) (if approved)
Intended status: Informational
Expires: August 24, 2015

C. Huitema
Microsoft
February 20, 2015

Anonymity profile for DHCP clients
draft-huitema-dhc-anonymity-profile-00.txt

Abstract

Some DHCP options carry unique identifiers. These identifiers can enable device tracking even if the device administrator takes care of randomizing other potential identifications like link-layer addresses or IPv6 addresses. The anonymity profile is designed for clients that wish to remain anonymous to the visited network. The profile provides guidelines on the composition of DHCP or DHCPv6 requests, designed to minimize disclosure of identifying 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 August 24, 2015.

Copyright Notice

Copyright (c) 2015 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 (<http://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. Introduction](#) [2](#)
- [1.1. Requirements](#) [3](#)
- [2. Application domain](#) [3](#)
- [3. Anonymity profile for DHCPv4](#) [4](#)
- [3.1. Client IP address field](#) [5](#)
- [3.2. Requested IP address option](#) [6](#)
- [3.3. Client hardware address](#) [6](#)
- [3.4. Client Identifier Option](#) [6](#)
- [3.5. Host Name Option](#) [7](#)
- [3.6. Client FQDN Option](#) [7](#)
- [3.7. UUID/GUID-based Client Identifier Option](#) [8](#)
- [3.8. User and Vendor Class DHCP options](#) [8](#)
- [4. Anonymity profile for DHCPv6](#) [9](#)
- [4.1. Client Identifier DHCPv6 Option](#) [9](#)
- [4.2. Server Identifier Option](#) [9](#)
- [4.3. Address assignment options](#) [10](#)
- [4.4. Option Request Option](#) [10](#)
- [4.4.1. Previous option values](#) [10](#)
- [4.5. Authentication Option](#) [10](#)
- [4.6. User and Vendor Class DHCPv6 options](#) [11](#)
- [4.7. Client FQDN Option](#) [11](#)
- [5. Management considerations](#) [11](#)
- [6. Security Considerations](#) [11](#)
- [7. IANA Considerations](#) [11](#)
- [8. Acknowledgments](#) [11](#)
- [9. References](#) [11](#)
- [9.1. Normative References](#) [12](#)
- [9.2. Informative References](#) [12](#)
- Author's Address [13](#)

1. Introduction

Reports surfaced recently of systems that would monitor the wireless connections of passengers at Canadian airports [CNBC]. We can assume that these are either fragments or trial runs of a wider system that would attempt to monitor Internet users as they roam through wireless access points and other temporary network attachments. We can also assume that privacy conscious users will attempt to evade this monitoring, for example by ensuring that low level identifiers such as link-layer addresses are "randomized," so that the devices do not broadcast a unique identifier in every location that they visit.

Huitema

Expires August 24, 2015

[Page 2]

Of course, link layer "MAC" addresses are not the only way to identify a device. As soon as it connects to a remote network, the device may use DHCP and DHCPv6 to obtain network parameters. The analysis of DHCP and DHCPv6 options shows that parameters of these protocols can reveal identifiers of the device, negating the benefits of link-layer address randomization. The natural reaction is to restrict the number and values of such parameters in order to minimize disclosure.

In the absence of a common standard, different system developers are likely to implement this minimization of disclosure in different ways. Monitoring entities could then use the differences to identify the software version running on the device. The proposed anonymity profile provides a common standard that minimizes information disclosure, including the disclosure of implementation identifiers.

1.1. Requirements

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [[RFC2026](#)].

2. Application domain

Mobile nodes can be tracked using multiple identifiers, the most prominent being MAC addresses. For example, when devices use Wi-Fi connectivity, they place the MAC address in the header of all the packets that they transmit. Standard implementation of Wi-Fi use unique 48 bit MAC addresses, assigned to the devices according to procedures defined by IEEE 802. Even when the Wi-Fi packets are encrypted, the portion of the header containing the addresses will be sent in clear text. Tracking devices can "listen to the airwaves" to find out what devices are transmitting near them.

We can easily imagine that the MAC addresses can be correlated with other data, e.g., clear text names and cookies, to build a registry linking MAC addresses to the identity of devices' owners. Once that correlation is done, tracking the MAC address is sufficient to track individual people, even when all application data sent from the devices is encrypted. MAC addresses can also be correlated with IP addresses of devices, negating potential privacy benefits of IPv6 "privacy" addresses. Privacy advocates have some reason to be concerned.

The obvious solution is to "randomize" the MAC address. Before connecting to a particular network, the device replaces the MAC address with a randomly drawn 48 bit value. MAC address randomization was successfully tried at the IETF in Honolulu in

November 2014 [[IETFMACRandom](#)]. However, we have to consider the linkage between MAC addresses, DHCP identifiers and IP addresses.

From a privacy point of view, it is clear that MAC Addresses, IP addresses and DHCP identifiers shall evolve in synchrony. For example, if the MAC address changes and the DHCP identifier stays constant, then it is really easy to correlate old and new MAC addresses, either by listening to DHCP traffic or by observing that the IP address remains constant, since it is tied to the DHCP identifier. Conversely, if the DHCP identifier changes but the MAC address remains constant, the old and new identifiers and addresses can be correlated by listening to L2 traffic. The procedures documented in the following sections construct DHCP identifiers from the current MAC address, automatically providing for this synchronization.

Of course, there are downsides to randomizing MAC addresses and DHCP identifiers. By definition, randomization will break management procedures that rely on tracking MAC addresses. Even if this is not too much of a concern, we have to be worried about the frequency of MAC address randomization. Suppose for example that many devices would get new random MAC addresses at short intervals, maybe every few minutes. This would generate new DHCP requests in rapid succession, with a high risk of exhausting DHCPv4 address pools. Even with IPv6, there would still be a risk of increased neighbor discovery traffic, and bloating of various address tables. Implementers will have to be cautious when programming devices to use randomized MAC addresses. They will have to carefully choose the frequency with which such addresses will be renewed.

This document only provides guidelines for using DHCP when privacy is considered more important than network management. We assume that the request for anonymity is materialized by the assignment of a randomized MAC address to the network interface. Once that decision is made, the following guidelines will avoid leakage of identity in DHCP parameters or in assigned addresses.

There may be rare situations where the clients want anonymity to attackers but not to their DHCP server. These clients should still use MAC Address randomization to hide from observers, and some form of encrypted communication to the DHCP server. This document does not study this scenario.

3. Anonymity profile for DHCPv4

Clients using the DHCPv4 anonymity profile limit the disclosure of information by controlling the header parameters and by limiting the

number and values of options. The number of options depend on the specific DHCP message:

DISCOVER: The anonymized DISCOVER messages MUST contain the Message Type, Client Identifier, Host name, and Parameter Request List options. It SHOULD NOT contain any other option.

REQUEST: The anonymized REQUEST messages SHOULD contain the Message Type, Client Identifier, Host name, and Parameter Request List options. If the message is in response to an OFFER, it SHOULD contain the corresponding Server Identifier option. It SHOULD NOT contain any other option.

DECLINE: The anonymized DECLINE messages SHOULD contain the Message Type, Client Identifier and Server Identifier options.

RELEASE: The anonymized RELEASE messages SHOULD contain the Message Type, Client Identifier and Server Identifier options.

INFORM: The anonymized INFORM messages MUST contain the Message Type, Client Id, Host name, and Parameter Request List options. It SHOULD NOT contain any other option.

Header fields and option values SHOULD be set in accordance with the DHCP specification, but some header fields and option values SHOULD be constructed per the following guidelines.

3.1. Client IP address field

Four bytes in the header of the DHCP messages carry the "Client IP address" (ciaddr) as defined in [[RFC2131](#)]. In DHCP, this field is used by the clients to indicate the address that they used previously, so that as much as possible the server can allocate them the same address.

There is very little privacy implication of sending this address in the DHCP messages, except in one case, when connecting to a different network than the last network connected. If the DHCP client somehow repeated the address used in a previous network attachment, monitoring services might use the information to tie the two network locations. DHCP clients should ensure that the field is cleared when they know that the network attachment has changed, and in particular of the link layer address is reset by the device's administrator.

3.2. Requested IP address option

The Requested IP address option (code 50) allows the client to request that a particular IP address be assigned. The option is mandatory in some protocol messages per [[RFC2131](#)], for example when a client selects to use an address offered by a server. However, this option is not mandatory in the DHCPDISCOVER message. It is simply a convenience, an attempt to regain the same IP address that was used in a previous connection. Doing so entails the risk of disclosing an IP address used by the client at a previous location, or with a different MAC Address.

When using the anonymity profile, clients SHOULD NOT use the Requested IP address option in DHCPDISCOVER Messages.

3.3. Client hardware address

Sixteen bytes in the header of the DHCP messages carry the "Client hardware address" (chaddr) as defined in [[RFC2131](#)]. The presence of this address is necessary for the proper operation of the DHCP service.

Hardware addresses, called "link layer address" in many RFCs, can be used to uniquely identify a device, especially if they follow the IEEE 802 recommendations. These unique identifiers can be used by monitoring services to track the location of the device and its user. The only plausible defense is to somehow reset the hardware address to a random value when visiting an untrusted location, before transmitting anything at that location with the hardware address. If the hardware address is reset to a new value, or randomized, the DHCP client SHOULD use the new randomized value in the DHCP messages.

3.4. Client Identifier Option

The client identifier option is defined in [[RFC2132](#)] with option code 61. It is discussed in details in [[RFC4361](#)]. The purpose of the client identifier option is to identify the client in a manner independent of the link layer address. This is particularly useful if the DHCP server is expected to assign the same address to the client after a network attachment is swapped and the link layer address changes. It is also useful when the same node issues requests through several interfaces, and expects the DHCP server to provide consistent configuration data over multiple interfaces.

The considerations for hardware independence and strong client identity have an adverse effect on the privacy of mobile clients, because the hardware-independent unique identifier obviously enables very efficient tracking of the client's movements.

The recommendations in [[RFC4361](#)] are very strong, stating for example that "DHCPv4 clients MUST NOT use client identifiers based solely on layer two addresses that are hard-wired to the layer two device (e.g., the Ethernet MAC address)." These strong recommendations are in fact a tradeoff between ease of management and privacy, and the tradeoff should depend on the circumstances.

In contradiction to [[RFC4361](#)], when privacy considerations trump management considerations, DHCP clients MUST use client identifiers based solely on the link layer address that will be used in the underlying connection. This will ensure that the DHCP client identifier does not leak any information that is not already available to entities monitoring the network connection. It will also ensure that a strategy of randomizing the link layer address will not be nullified by DHCP options.

[3.5.](#) Host Name Option

The Host Name option is defined in [[RFC2132](#)] with option code 12. Depending on implementations, the option value can carry either a fully qualified domain name such as "node1984.example.com," or a simple host name such as "node1984." The host name is commonly used by the DHCP server to identify the host, and also to automatically update the address of the host in local name services.

Fully qualified domain names are obviously unique identifiers, but even simple host names can provide a significant amount of information on the identity of the device. They are typically chosen to be unique in the context where the device is most often used. If that context is wide enough, in a large company or in a big university, the host name will be a pretty good identifier of the device. Monitoring services could use that information in conjunction with traffic analysis and quickly derive the identity of the device's owner.

When privacy considerations trump management considerations, DHCP clients MUST always send a non-qualified host name instead of a fully qualified domain name, and SHOULD obfuscate the host name value, so it could not be linked to anything other than the link layer address. A simple solution would be to set the host name value to a hexadecimal representation of the link layer address that will be used in the underlying connection.

[3.6.](#) Client FQDN Option

The Client FQDN option is defined in [[RFC4702](#)] with option code 81. The option allows the DHCP clients to advertise to the DHCP server their fully qualified domain name (FQDN) such as

"mobile.example.com." This would allow the DHCP server to update in the DNS the PTR record for the IP address allocated to the client. Depending on circumstances, either the DHCP client or the DHCP server could update in the DNS the A record for the FQDN of the client.

Obviously, this option uniquely identifies the client, exposing it to the DHCP server or to anyone listening to DHCP traffic. In fact, if the DNS record is updated, the location of the client becomes visible to anyone with DNS lookup capabilities.

When privacy considerations trump management considerations, DHCP clients SHOULD NOT include the Client FQDN option in their DHCP requests. Alternatively, they MAY include a special purpose FQDN using the same hostname as in the Host Name Option, with a suffix matching the connection-specific DNS suffix being advertised by that DHCP server. Having a name in the DNS allows working with legacy systems that require one to be there, e.g., by verifying a forward and reverse lookup succeeds with the same result.

3.7. UUID/GUID-based Client Identifier Option

The UUID/GUID-based Client Machine Identifier option is defined in [[RFC4578](#)], with option code 97. The option is part of a set of options for Intel Preboot eXecution Environment (PXE). The purpose of the PXE system is to perform management functions on a device before its main OS is operational. The Client Machine Identifier carries a 16-octet Globally Unique Identifier (GUID), which uniquely identifies the device.

The PXE system is clearly designed for devices operating in a controlled environment, and its functions are not meant to be used by mobile nodes visiting untrusted networks. If only for privacy reasons, nodes visiting untrusted networks MUST disable the PXE functions, and MUST NOT send the corresponding options.

3.8. User and Vendor Class DHCP options

Vendor identifying options are defined in [[RFC2132](#)] and [[RFC3925](#)]. When using the anonymity profile, DHCP clients SHOULD NOT use the Vendor Specific Information option (code 43), the Vendor Class Identifier Option (60), the Vendor Class option (code 124), or the Vendor Specific Information option (code 125) as these options potentially reveal identifying information.

[4.](#) Anonymity profile for DHCPv6

DHCPv6 is typically used by clients in one of two scenarios: stateful and stateless configuration. In the stateful scenario, clients use a combination of SOLICIT, REQUEST, CONFIRM, RENEW, REBIND and RELEASE messages to obtain addresses, and manage these addresses.

In the stateless scenario, clients configure addresses using a combination of client managed identifiers and router-advertised prefixes, without involving the DHCPv6 services. Different ways of constructing these prefixes have different implications on privacy, which are discussed in [[I-D.ietf-6man-default-iids](#)] and [[I-D.ietf-6man-ipv6-address-generation-privacy](#)]. In the stateless scenario, clients use DHCPv6 to obtain network configuration parameters, through the INFORMATION-REQUEST message.

When using the anonymity profile, DHCPv6 clients carefully select DHCPv6 options used in the various messages that they sent. The list of options that are mandatory or optional for each message is specified in [[RFC3315](#)]. Some of these options have specific implications on anonymity. The following sections provide guidance on the choice of option values when using the anonymity profile.

[4.1.](#) Client Identifier DHCPv6 Option

The client identifier option is defined in [[RFC3315](#)] with option code 1. The purpose of the client identifier option is to identify the client to the server. The content of the option is a DHCP User ID (DUID) for which three formats are specified: Link-layer address plus time, Vendor-assigned unique ID based on Enterprise Number, Link-layer address.

When using the anonymity profile, DHCPv6 clients MUST use the DUID format number 3, Link-layer address. The value of the Link-layer address should be that currently assigned to the interface.

[4.2.](#) Server Identifier Option

When using the anonymity profile, DHCPv6 clients SHOULD use the Server Identifier Option (code 2) as specified in [[RFC3315](#)]. Clients MUST only include server identifier values that were received with the current MAC address, because reuse of old values discloses information that can be used to identify the client.

4.3. Address assignment options

When using the anonymity profile, DHCPv6 clients might have to use SOLICIT or REQUEST messages to obtain IPv6 addresses through the DHCP server. The clients SHOULD only use the options necessary to perform the requested DHCPv6 transactions, such as Identity Association for Non-temporary Addresses Option (code 3) or Identity Association for Temporary Addresses Option (code 4).

The clients MAY use the IA Address Option (code 5) but need to balance the potential advantage of "address continuity" versus the potential risk of "previous address disclosure." A potential solution is to remove all stored addresses when a MAC address changes, and to only use the IA Address option with addresses that have been explicitly assigned through the current MAC address.

4.4. Option Request Option

When using the anonymity profile, DHCPv6 clients SHOULD use the Option Request Option (code 6) as specified in [[RFC3315](#)].

4.4.1. Previous option values

According to [[RFC3315](#)], the client that includes an Option Request Option in a Solicit or Request message MAY additionally include instances of those options that are identified in the Option Request option, with data values as hints to the server about parameter values the client would like to have returned.

When using the anonymity profile, clients SHOULD NOT include such instances of options because old values might be used to identify the client.

4.5. Authentication Option

The purpose of the Authentication option (code 11) is to authenticate the identity of clients and servers and the contents of DHCP messages. As such, the option can be used to identify the client, and is incompatible with the stated goal of "client anonymity." DHCPv6 clients that use the anonymity profile SHOULD NOT use the authentication option. They MAY use it if they recognize that they are operating in a trusted environment, e.g., in a work place network.

4.6. User and Vendor Class DHCPv6 options

When using the anonymity profile, DHCPv6 clients SHOULD NOT use the User Class option (code 15) or the Vendor Class option (code 16), as these options potentially reveal identifying information.

4.7. Client FQDN Option

The Client FQDN option is defined in [[RFC4704](#)] with option code 29. The option allows the DHCP clients to advertise to the DHCP their fully qualified domain name (FQDN) such as "mobile.example.com." When using the anonymity profile, DHCPv6 clients SHOULD NOT include the Client FQDN option in their DHCPv6 messages because it identifies the client. As explained in [Section 3.6](#) they MAY use a local-only FQDN by combining a host name derived from the link layer address and a suffix advertised by the local DHCP server.

5. Management considerations

The anonymity profile has the effect of hiding the client identity from the DHCP server. This is not always desirable. Some DHCP servers provide facilities like publishing names and addresses in the DNS, or ensuring that returning clients get reassigned the same address. Implementers should be careful to only use the anonymity profile when privacy trumps management considerations.

6. Security Considerations

The use of the anonymity profile does not change the security considerations of the DHCPv4 or DHCPv6 protocols.

7. IANA Considerations

This draft does not require any IANA action.

8. Acknowledgments

The inspiration for this draft came from discussions in the Perpass mailing list. Several people provided feedback on early versions of this draft, notably Noel Anderson, Tushar Gupta, Gabriel Montenegro, Dave Thaler and Jun Wu.

9. References

9.1. Normative References

- [RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", [BCP 9](#), [RFC 2026](#), October 1996.
- [RFC2131] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), March 1997.
- [RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", [RFC 2132](#), March 1997.
- [RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [RFC 3315](#), July 2003.
- [RFC3925] Littlefield, J., "Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)", [RFC 3925](#), October 2004.
- [RFC4361] Lemon, T. and B. Sommerfeld, "Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)", [RFC 4361](#), February 2006.
- [RFC4578] Johnston, M. and S. Venaas, "Dynamic Host Configuration Protocol (DHCP) Options for the Intel Preboot eXecution Environment (PXE)", [RFC 4578](#), November 2006.
- [RFC4702] Stapp, M., Volz, B., and Y. Rekhter, "The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option", [RFC 4702](#), October 2006.
- [RFC4704] Volz, B., "The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client Fully Qualified Domain Name (FQDN) Option", [RFC 4704](#), October 2006.

9.2. Informative References

- [CNBC] Weston, G., Greenwald, G., and R. Gallagher, "CBC News: CSEC used airport Wi-Fi to track Canadian travellers", Jan 2014, <<http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881>>.
- [I-D.ietf-6man-default-iids] Gont, F., Cooper, A., Thaler, D., and W. Will, "Recommendation on Stable IPv6 Interface Identifiers", [draft-ietf-6man-default-iids-02](#) (work in progress), January 2015.

[I-D.ietf-6man-ipv6-address-generation-privacy]

Cooper, A., Gont, F., and D. Thaler, "Privacy Considerations for IPv6 Address Generation Mechanisms", [draft-ietf-6man-ipv6-address-generation-privacy-03](#) (work in progress), January 2015.

[IETFMACRandom]

Zuniga, J.C., "MAC Privacy", November 2014, <<http://www.ietf.org/blog/2014/11/mac-privacy/>>.

Author's Address

Christian Huitema
Microsoft
Redmond, WA 98052
U.S.A.

Email: huitema@microsoft.com

