Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: 26 March 2021

Y. Lee
J. Livingood
Comcast
J. Weil
Charter Communications

22 September 2020

Problem Statements for MAC Address Randomization
draft-lee-randomized-macaddr-ps-01

Abstract

MAC Addresses are Link Layer addresses used in IEEE Ethernet, WiFi, and other link layer protocols. A MAC Address is a fixed locally unique address assigned by the Network Interface Card (NIC) manufacturer, though they may be modified by an operating system, and they enable a device to connect to a network. Due to the static nature of a MAC Address, it raises some privacy concerns that have led to randomization of MAC Addresses by operating systems. This draft documents the impacts of MAC Address randomization to existing use cases of network and application services and proposes few next steps IETF may consider working on.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction 2
1.1. Requirements Language 3
2. Problem Statement 4
3. IANA Considerations 5
4. Security Considerations 5
5. Normative References 5
6. Informative References 5
Appendix A. Additional Stuff 6
Authors' Addresses 6

1. Introduction

A Network Interface Card (NIC) needs a locally unique address in order to connect to a network. The IEEE [IEEE.802-1D.1993] created the Media Access Control (MAC) Address for use by any IEEE 802 link layer standard protocols (e.g. Ethernet & WiFi). A MAC Address is 48 bits long and is usually defined in the hardware by the NIC manufacturer. A device can have one or more MAC addresses; for example an IoT device may have a single WiFi interface and one MAC Address but a laptop may have three interfaces that encompass two wired Ethernet ports and a WiFi interface, and therefore will have three MAC addresses. MAC Addresses must be locally unique in order for communications to be sent and received by the correct devices.

The device manufacturer typically assigns the MAC address to an interface. Unless the user or operating system modifies the MAC address, which is sometimes the case. Because of the static nature of the manufacturer's MAC addresses, a MAC address is used for device identification for a variety of operational and troubleshooting reasons in the LAN (e.g., home network). For example, a MAC address can be used to determine to which device on a LAN to permit or deny access at a particular time of day (e.g. child's tablet may not access Internet after 22:00 hrs until 06:00 hrs).

Privacy concerns have led some operating systems developers to implement MAC Address randomization [IEEE.802.11AQ]. However, this can pose problems for network and application services that rely upon

the manufacturer's MAC Addresses or assumed that MAC Addresses would not be limitlessly randomized. Many network and application services today rely upon a persistent MAC Address to uniquely identify a device. For example: "Sticky" DHCP assignment can enable a device to retain the same IP address for an extended time and this often maps IP to MAC address. Broken sticky MAC address to IP assignment will break some local network policies such as persistent network address port translation (NAPT) port-forwarding, demilitarized zone setup (DMZ, or safe zone) and LAN Quality of Service (QoS), application of security policies (i.e. IoT devices have one firewall policy while tablets have another), parental controls (e.g. device X belongs to child 1 & access to the network is not permitted between 22:00-06:00 hours) are all typically based on persistent MAC Address for device identification. There are also business policies that have depended upon persistent MAC address such as hospitality Internet service used in hotels, airplanes, and community WiFi often uses MAC address to tie to Internet subscription (e.g. after initial authorization the MAC Address is added to the allow list & subsequent authorization on every new connection is unnecessary).

Thus, many network and application services have developed over many years that are dependent upon persistent MAC Addresses. This could be in tension with the move of major operating systems to deploy MAC Address randomization. As a result, network and application services on which end users have grown to depend upon will break. We are interested in determining if there is sufficient interest in the IETF community to define best practices and potentially a new protocol or methods for service continuity in the presence of MAC Address randomization and/or recommendations for how to implement that randomization while not negatively impacting network and application services desired by end users.

1.1. Requirements Language

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 RFC 2119 [RFC2119].

2. Problem Statement

Recently, privacy concerns have been raised related to persistent (static) MAC Addresses. In particular, the privacy security communities worry about the risks associated with being able to associate a MAC Address to a particular device and/or person (refs needed). While networks and application have long used MAC Addresses to enable end user services, the concern that this may be abused such as for data monetization purposed led to the development of techniques to randomize MAC Addresses (though some research disputes the efficacy of that, ref needed).

MAC Address randomization is a technique similar to IPv6 temporary IIDs defined in [RFC7217]. Devices will auto-generate the MAC Address based on the device policy and use the random generated MAC Address instead of the hardware based MAC Address assigned by the manufacturer when they connect to the network. Many modern Operation Systems such as Apple iOS (https://support.apple.com/en-us/HT211227), Google Android (https://source.android.com/devices/tech/connect/wifi-mac-randomization) and Microsoft Windows 10 (https://support.microsoft.com/en-us/help/4027925/windows-how-and-why-to-use-random-hardware-addresses) are experimenting with MAC Address randomization. The randomization policy could be time based, network based, a combination of both or involve other factors. MAC Address randomization may be one of many tactics to protect end user privacy but it can also break some network and application services that make assumptions about the persistence of MAC Address when they were designed and developed.

There are perhaps some use cases in which a balance between persistence and randomization may be found. In some circumstances, users may want to give a trusted network (e.g., home network) some predictability of the MAC Address in order to enable some important and valuable to end user services. This document defines a set of problem statements to continue the existing network and application services when MAC Addresses are randomized. These are defined by "PS" for Problem Statement below:

[PS-01] An Internet Service Provider (ISP) or other network operator must not make any assumption about the persistence of MAC Addresses.

[PS-02] An ISP or other network operator must not make any assumption of the Randomization Policy for MAC Addresses.

[PS-03] LAN policies must not depend upon a fixed, persistent MAC Address.

[PS-04] A mechanism must be defined to securely identify a device. The mechanism can leverage existing protocols (e.g., EAP) or a newly defined protocol.

[PS-05] ISP or other network operators, device manufacturers, and operating system developers may leverage existing protocols or define a new mechanism to exchange information about MAC Address randomization.

3. IANA Considerations

This memo includes no request to IANA.

All drafts are required to have an IANA considerations section (see Guidelines for Writing an IANA Considerations Section in RFCs [RFC5226] for a guide). If the draft does not require IANA to do anything, the section contains an explicit statement that this is the case (as above). If there are no requirements for IANA, the section will be removed during conversion into an RFC by the RFC Editor.

4. Security Considerations

All drafts are required to have a security considerations section. See RFC 3552 [RFC3552] for a guide.

5. 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>.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <https://www.rfc-editor.org/info/rfc3552>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 5226, DOI 10.17487/RFC5226, May 2008, <https://www.rfc-editor.org/info/rfc5226>.

6. Informative References

[IEEE.802-1D.1993]
Institute of Electrical and Electronics Engineers, "Information technology - Telecommunications and information exchange between systems - Local area networks - Media access control (MAC) bridges", IEEE Standard 802.1D, July 1993.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <https://www.rfc-editor.org/info/rfc7217>.

Appendix A. Additional Stuff

This becomes an Appendix.

Authors' Addresses

Yiu L. Lee
Comcast
1800 Arch Street
Philadelphia, PA 19103
United States of America

Email: yiu_lee@comcast.com

Jason Livingood
Comcast
1800 Arch Street
Philadelphia, PA 19103
United States of America

Email: jason_livingood@comcast.com

Jason Weil
Charter Communications
Orlando, FL
United States of America

Email: Jason.Weil@charter.com