Internet Engineering Task Force
INTERNET-DRAFT I-D

J. Henry
Cisco Systems
Y. Lee
Comcast
January 2021

Randomized and Changing MAC Address Framework

Abstract

To limit the association between a device traffic and its user, client vendors have started implementing MAC address rotation. When such rotation happens, sessions may break, which may affect network efficiency and the user experience. This document lists network services that may be affected by such rotation, and examines solutions to maintain user privacy while preserving user quality of experience and network operation efficiency.

Contents

1. Introduction

It has become easier for attackers to observe the activity of a personal device, particularly when traffic is sent over a wireless link. Once the association between a device and its user is made, identifying the device and its activity is sufficient to deduce information about what the user is doing, without the user consent.

To reduce the risks of correlation between a device activity and its owner, multiple vendors have started to implement Rotating and Changing Mac address (RCM). With this scheme, and end-device implements a different RCM over time when exchanging traffic over a wireless network. By randomizing the change, the association between a given traffic flow and a single device is made more difficult.

However, such address change may affect the user experience and the efficiency of network operations. For many decades, the unicity of the association between a device and a MAC address was assumed. When this association is broken, sessions may also break, packets in translation may find themselves without clear source or destination, network services may be over-solicited by a small number of stations that appear as many clients.

There is a need to assess how this association is made, enumerate services that may be affected by RCM, and evaluate possible solutions to maintain the quality of user experience and network efficiency while RCM happens and user privacy is reinforced. This document presents such assessment and recommendations.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [RFC2119].

3. MAC address as an identity: user vs device

Any device member of an IEEE 802 network includes several operating layers. Among them, the Media Access Control (MAC) layer defines rules to control how the device accesses the shared medium. In a network where a machine can communicate with one or more other machines, one such rule is that each machine needs to be identified, either as the target destination of a message, or as the source of a message (and thus the target destination of the answer). Initially intended as a 48-bit (6 octets) value, later versions of the Standard (802-2014) also allowed this address to take an extended format of 64 bits (8 octets), thus enabling a larger number of MAC addresses to coexist as the 802 technologies became widely adopted.

Regardless of the address length, different networks have different needs, and several bits of the first octet are reserved for specific purposes. In particular, the first bit is used to identify the destination address either as an individual (bit set to 0) or a group address (bit set to 1). The second bit, called the Universally or Locally Administered (U/L) Address Bit, indicates whether the address has been assigned by a local or universal administrator. Universally administered addresses have this bit set to 0. If this bit is set to 1, the entire address (i.e., 48 bits) has been locally administered (802-1990 5.2.1).

The intent of this provision is important for the present document. The 802 Standard recognized that some devices may never travel and thus, always attaching to the same network, would not need a globally unique MAC address. To accommodate for this relaxed requirement, the second bit of the MAC address first octet the MAC address format was designed to express whether the address was intended to be globally unique, or if significance was only local. The address allocation method was not defined in the Standard in this later case, but the mechanism was defined in the same clause that defined that an address should be unique so as to avoid collision.

It is also important to note that the purpose of the Universal version of the address was also to avoid collisions and confusion, as any machine could connect to any network, and each machine needs to determine if it is the intended destination of a message or its response. The same clause 5.2.1 reminds network designers and operators that \all potential members of a network need to have a unique identifier (if they are going to coexist in the network). The advantage of a universal address is that a node with such an address can be attached to any LAN in the world with an assurance that its address is unique.

With the rapid development of wireless technologies and mobile devices, this scenario became very common. With more than 70% of 802 networks on the planet implementing radio technologies at the access, the MAC address of a wireless device can appear anywhere on the planet and collisions should still be avoided. However, the same evolution brought the distinction between two types of devices that the 802 Standard generally referred to as ‘nodes in a network’. Their definition is found in the 802E Recommended Practice (clause 6.2). One type is a shared service device, which functions are used by a number of people large enough that the device itself, its functions or its traffic cannot be associated with a single or small group of people. Examples of such devices include switches in a dense network, 802.11 (Wi-Fi) access points in a crowded airport, task-specific (e.g. barcode scanners) devices, etc. Another type is a personal device, which is a machine, a node, primarily used by a single person or small group of people, and so that any identification of the device or its traffic can also be associated to the identification of the primary user or their traffic. Quite naturally, the unique identification of the device is trivial if the device expresses a universally unique MAC address. Then, the detection of elements directly or indirectly identifying the user of the device (Personally Identifiable Information, or PII) is sufficient to tie the universal MAC address to a user. Then, any detection of traffic that can be associated to the device becomes also associated with the known user of that device (Personally

Correlated Information, or PCI).

This possible identification or association presents a serious privacy issue, especially with wireless technologies. For most of them, and in particular for 802.11, the source and destination MAC addresses are not encrypted even in networks that implement encryption (so that each machine can easily detect if it is the intended target of the message before attempting to decrypt its content, and also identify the transmitter, so as to use the right key when multiple unicast keys are in effect).

This unique identification of the user associated to a node was clearly not the intent of the 802 MAC address. A logical solution to remove this association is to use a locally administered address instead, and change the address in a fashion that prevents a temporal association between one MAC address and some PII to be maintained fruitfully. However, other network devices on the same LAN implementing a MAC layer also expect the unicity of the MAC address. When a device changes its MAC address, other devices on the same LAN may fail to recognize that the same machine is attempting to communicate with them. Additionally, multiple layers implemented at upper OSI layers have been designed with the assumption that each node on the LAN, using these services, would have a unique MAC address. This assumption sometimes adds to the PII confusion, for example in the case of AAA services authenticating the user of a machine and associating the authenticated user to the device MAC address. Other services solely focus on the machine (e.g. DHCP), but still expect each device to use a single MAC address. Changing the MAC address may disrupt these services.

4. The actors: network functional entities and human entities

The risk of service disruption is therefore weighted against the privacy benefits. However, the plurality of actors involved in the exchanges tends to blurry the boundaries of what privacy should be protected against. It might therefore be useful to list the actors to the network exchanges. Some actors are functional entities, some others are humans (or related) entities.

4.1. Network functional entities:

- Wireless access network infrastructure devices (e.g. Wi-Fi access points or controllers): these devices participate in 802 LAN operations. As such, they need to uniquely identify machines as a source or destination so as to successfully continue exchanging frames. Part of the identification includes recording, and adapting to, devices communication capabilities (e.g. support for specific protocols). As a device changes its connection (roams) from one access point to another, the access points can exchange contextual information (e.g. device MAC, keying material) allowing the device session to continue seamlessly. These access points can also inform devices further in the wired network about the roam, to ensure that OSI model Layer 2 frames are redirected to the new device access point.

- Other network devices operating at the MAC layer: many wireless network access devices (e.g. 802.11 access points) are conceived as Layer 2 devices, and as such they bridge a frame from one medium (e.g. 802.11 or Wi-Fi) to another (e.g. 802.3 or Ethernet). This means that a wireless device MAC address often exists on the wire beyond the wireless access device. Devices connected to this wire also implement 802 technologies, and as such operate on the expectation that each device is associated to a unique MAC address for the duration of continuous exchanges. For example, switches and bridges associate MAC addresses to individual ports (so as to know which port to send a frame intended for a particular MAC address). Similarly, authentication, authorization and accounting

(AAA) services can validate the identity of a device and use the device MAC address as a first pointer to the device identity (before operating further verification). 802.1X-enabled devices may also selectively block the data portion of a port until a connecting device is authenticated. These services then use the MAC address as a first pointer to the device identity to allow or block data traffic. This list is not exhaustive. Multiple services are defined for 802.3 networks, and multiple services defined by the IEEE 802.1 working group are also applicable to 802.3 networks. Wireless access points may also connect to other mediums than 802.3, which also implements mechanism under the umbrella of the general 802 Standard, and therefore implement Layer 2 technologies and expect the unique association of a MAC address to a device.

- Network devices operating at upper layers: some network devices provide functions and services above the MAC layer. Some of them also operate a MAC layer function: for example, routers provide IP routing services, but rely on the device MAC address to create the appropriate frame structure. Other devices and services operate at upper layers, but also rely on the 802 MAC layer principle of MAC-to-device unique mapping. For example, DHCPv4 services commonly provide a single IP address per MAC address (do not assign more than one IPv4 address per MAC address, and assign a new IPv4 address to each new requesting MAC address). ARP and reverse-ARP services commonly expect that, once an IP-to-MAC mapping has been establish, this mapping is valid and unlikely to change for the cache lifetime. DHCPv6 services commonly do not assign the same IPv6 address to two different requesting MAC addresses. Hybrid services, such as EoIP, also assume stability of the device-to-MAC-and-IP mapping for the duration of a given session.

4.2. Human-related entities:

- Over the air (OTA) observers: as the transmitting or receiving MAC address is usually not encrypted in wireless 802-technologies exchanges, and as any protocol-compatible device in range of the signal can read the frame header, OTA observers are able to read individual transmissions MAC addresses. Some wireless technologies also support techniques to establish distances or positions, allowing the observer, in some cases, to uniquely associate the MAC address to a physical device and it associated location. It can happen that an OTA observer has a legitimate reason to monitor a particular device, for example for IT support operations. However, it is difficult to control if another actor also monitors the same station with the goal of obtaining PII or PCI.

- Wireless access network operators: some wireless access networks are only offered to users or devices matching specific requirements, such as device type (e.g. IoT-only networks, factory operational networks, etc.) Therefore, operators can attempt to identify the devices (or the users) connecting to the networks under their care. They can use the MAC address to represent an identified device.

- Network access providers: wireless access networks are often considered beyond the first 2 Layers of the OSI model. For example, several regulatory or legislative bodies can group all OSI layers into their functional effect of allowing network communication between machines. In this context, entities operating access networks can see their liability associated to the activity of devices communicating through the networks that these entities operate. In other contexts, operators assign network resources based on contractual conditions (e.g. fee, bandwidth fair share, etc.) In these scenarios, these operators may attempt to identify the devices and the users of their networks. They can use the MAC address to represent an identified device.

- Over the wire internal (OTWi) observers: because the device wireless MAC address continues to be present over the wire if the infrastructure connection device

(e.g. access point) functions as a Layer 2 bridge, observers may be positioned over the wire and read transmission MAC addresses. Such capability supposes that the observer has access to the wired segment of the broadcast domain where the frames are exchanged. In most networks, such capability requires physical access to an infrastructure wired device in the broadcast domain (e.g. switch closet), and is therefore not accessible to all.

- Over the wired external (OTWe) observers: beyond the broadcast domain, frames headers are removed by a routing device, and a new Layer 2 header is added before the frame is transmitted to the next segment. The personal device MAC address is not visible anymore, unless a mechanism copies the MAC address into a field that can be read while the packet travels onto the next segment (e.g. pre-RFC4941 and pre-RFC 7217 IPv6 addresses built from the MAC address). Therefore, unless this last condition exists, OTWe observers are not able to see the device MAC address.

5. The environments

The surface of PII exposures that can drive MAC address randomization depends on the environment where the device operates. Therefore, a device can express an identity (such as a MAC address) that can be stable over time if trust is established, or that can be temporal if an identity is required for a service in an environment where trust has not been established:

1. There are environments where a device establishes a trust relationship and can share a stable device identity with the access network devices (access point and WLC), the services beyond the access point in the L2 broadcast domain (e.g. DHCP, AAA), and the device has confidence that its identity is not shared beyond the L2 broadcast domain boundary.

2. In other environments, the device may not be willing to share a stable identity with some elements of the Layer 2 broadcast domain, but may be willing to share a stable identity with other elements. For example, a device may want to change the MAC address it uses to communicate with the access point while maintaining the same IP address across the MAC address rotation (thus expressing a stable identity to the DHCP server). That stable identity may or may not be the same for different services.

3. In other environments, the device may not be willing to share any stable identity with any entity of the Layer 2 broadcast domain, and may express a temporal identity to each of them. That temporal identity may or not be the same for different services.

This trust relationship naturally depends on the relationship between the user of the personal device and the operator of the service. Thus, it is useful to distinguish several types of environments:

a) Residential settings under the control of the user: this is typical of a home with Wi-Fi and Internet connection. In this environment, the MAC address activity may be detectable beyond the home walls. However, if traffic is encrypted (e.g. WPA3), some protection for OTA eavesdropping can be assumed. The wire segment within the broadcast domain is under the control of the user, and is therefore usually not at risk of hosting an eavesdropper. Trust is typically established at this level. Traffic over the Internet does not expose the MAC address if it is not copied to another field before routing happens.

b) Managed residential setting: examples of this type of environment include shared living facilities and other collective environments where an operator manages the network for the residents. The OTA exposure is similar to that of a home. A number

of devices larger than in a standard home may be present, and the operator may be requested to provide IT support to the residents. Therefore, the operator may need to identify a device activity in real time, but may also need to analyze logs so as to understand a past reported issue. For both activities, a device identification associated to the session is needed. Trust is often established in this environment, at the scale of a series of a few sessions.

c) Public guest networks: public hotspots, such as in shopping malls, hotels, stores, trains stations and airports are typical of this environment. The guest network operator may be legally mandated to identify devices or users or may have the option to leave all devices and users untracked. In this environment, trust is commonly not established with any element of the L2 broadcast domain.

d) Enterprises (with BYOD): in this environment, users may be provided corporate devices or may bring their own devices. The devices are not directly under the control of a corporate IT team. Trust may be established as the device joins the network.

e) Managed enterprises: in this environment, users are typically provided with corporate devices, and all connected devices are managed, for example through a Mobile Device Management (MDM) profile installed on the device. Trust is created as the MDM profile is installed.

6. The purpose of identification and associated problems

Most network functional devices offering a service to a personal device use the device MAC address to maintain continuity of service.

Wireless access points and controllers use the MAC address to validate the device connection context, including protocol capabilities, confirmation that authentication was completed, QoS or security profiles, encryption key material. Some advanced access points and controllers also include upper layer functions which purpose is covered below. A device changing its MAC address, without another recorded device identity, would cause the access point and the controller to lose these parameters. As such, the L2 infrastructure does not know that the device (with its new MAC address) is authorized to communicate through the network. The encryption keying material is not identified anymore (causing the access point to fail decrypting the device traffic, and fail selecting the right key to send encrypted traffic to the device). In short, the entire context needs to be rebuilt, and a new session restarted. The time consumed by this procedure breaks any flow that needs continuity or short delay between packets on the device (e.g. real-time audio, video, AR/VR etc.) The 802.11i Standard recognizes that a device may leave the network and come back after a short time window. As such, the standard suggest that the infrastructure should keep the context for a device up to one hour after the device was last seen. MAC address rotation in this context can cause resource exhaustion on the wireless infrastructure and the flush of contexts, including for devices that are simply in temporal sleep mode.

Other devices in the Layer 2 broadcast domain also use the MAC address to know when and where to forward frames. MAC rotation can cause these devices to exhaust their resources, holding in memory traffic for a device which port location can no longer be found. As these infrastructure devices also implement a cache (to remember the port position of each known device), frequent MAC rotation can cause resources exhaustion and the flush of older MAC addresses, including for devices that did not rotate their MAC. For the MAC rotating device, these effects translate into session continuity and return traffic losses.

In wireless contexts, 802.1X authenticators rely on the device and user identity validation provided by a AAA server to open their port to data transmission. The

MAC address is used to verify that the device is in the authorized list, and the associated key used to decrypt the device traffic. A change in MAC address causes the port to be closed to the device data traffic until the AAA server confirms the validity of the new MAC address. Therefore, MAC rotation can interrupt the device traffic, and cause a strain on the AAA server.

DHCP servers, without a unique identification of the device, lose track of which IP address is validly assigned. Unless the device that rotates the MAC releases the IP address before the rotation occurs, DHCP servers are at risk of scope exhaustion, causing new devices (or MAC rotating devices) to fail obtaining a new IP address. Even if the that rotates the MAC releases the IP address before the rotation occurs, the DHCP server typically holds the releases IP address for a certain duration, in case the leaving MAC would return. As the DHCP server cannot know if the release is due to a temporal disconnection or a MAC rotation, the risk of scope address exhaustion exists even in cases where the IP address is released.

Routers keep track of which MAC address is on which interface. MAC rotation can cause MAC address cache exhaustion, but also the need for frequent ARP and inverse ARP exchanges.

In residential settings (environments type A), policies may be in place to control the traffic of some devices (e.g. parental control). These policies are often based on the device MAC address. Rotation removes the ability for this control.

In residential settings (environments type A) and in enterprises (environments types D and E), device recognition and ranging may be used for IoT-related functionalities (door unlock, preferred light and temperature configuration, etc.) These functions often rely on the detection of the device wireless MAC address. MAC address rotation breaks those services.

In managed residential settings (environments types B) and in enterprises (environments types D and E), the network operator is often requested to provide IT support. With MAC address rotation, real time support is only possible if the user is able to provide the current MAC address. Service improvement support is not possible if the MAC address that the device had at the (past) time of the reported issue is not known at the time the issue is reported.

7. Possible solutions

In environments of type 1 (settings of type a, b, d and/or e), the device or its user may have confidence that over the air eavesdropping does not present a threat. In that case, usage of a fixed MAC address per SSID is a possibility.

In other cases in the same environments, over the air eavesdropping may be a concern. In that case, the device may be able to express, in a protected frame, a stable identity to the wireless infrastructure. The format of the container of this identity, encapsulated into a Layer 2 element, is protocol-specific and can be defined by the associated protocol standard designers. In that case, the device expresses a randomized and changing MAC address (RCM) over the air, but a stable identity to the wireless infrastructure.

In networks implementing 802.1X/EAP, a AAA server may be informed that a device presenting a new MAC address expresses the same device identity as the same device with a previous MAC address. That AAA server may then inform the access network, for example with a RADIUS RFC 5176 CoA message, of the unique identity of the device across RCMs.

In the cases where the unicity of the station identity is expressed through a protected mean to the trusted access infrastructure, we recommend that the infrastructure expresses a single MAC address for the device toward the wired part of the network. In such setting, the device first connects to the wireless infrastructure and expresses a stable identity. The wireless infrastructure, acting as a proxy, generates a locally-administered MAC address for the device. That MAC

address is used to represent the device toward services in the other elements of the wired network. Next, when the device rotates its over-the-air MAC address and informs the wireless infrastructure of its stable identity, the wireless infrastructure identifies that the new MAC address matches the same device as the previous MAC address, and continues using the previously generated locally-administered MAC address to represent the device to wired infrastructure services.

In environments of type 2, the device may share different identities with different services. For example, the device may express an over-the-air RCM, a stable encapsulated identity to the wireless infrastructure, a device identity to a AAA server, and a different client identity to a DHCP server. In a multi-link scenario, it may also happen that the device expresses more than one identity to the DHCP server, with connections going through the same wireless infrastructure. Because the device may express a stable identity to one or more network services, because this identity may be shareable with the wireless infrastructure, we recommend that the wireless infrastructure uses to represent the device, one of the stable identities expressed by that device. Because different identities can be expressed, and because the role of the wireless infrastructure is not to monitor closely all activities from the device, we recommend that the wireless infrastructure uses as the device stable identity, the stable identity expressed to the wireless infrastructure, if it is available. If such identity is not available, we recommend that the infrastructure uses the stable identity expressed to the AAA server, if it is available and shared back with the wireless infrastructure. If such identity is not available, we recommend that the wireless infrastructure uses a stable identity expressed to the DHCP server, if such identity is available and visible to the wireless infrastructure. These recommendations recognize the fact that the wireless infrastructure has visibility into all traversing non-protected traffic. As such, the wireless infrastructure may be able to read identifiers sent in unprotected DHCP requests. Additionally, the wireless infrastructure would also see, for example, a device with a new MAC address expressing the same DHCP identity, or requesting the same IP address, as another device previously connected through the same wireless system. Therefore, the device may not be able to obfuscate its DHCP identity from the wireless infrastructure if DHCP exchanges are not encrypted. Additionally, and because the wireless infrastructure may not be able to distinguish a device rotating its MAC and attempting to obtain the same DHCP address as with its previous MAC address, from a malicious device attempting to steal the DHCP identity from another device, mechanisms on the infrastructure may prevent such requests for already assigned resources from being forwarded successfully.

Thus, in all environments where a device uses a rotating and changing locally-administered MAC address, we recommend that rotation from one address to the next is preceded by a release of network resources, such as open connections closure and DHCP address releases.

8. IANA Consideration

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.

9. Security Considerations

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

10. Normative References

11. Informative References