Wi-Fi Identification Scope for Liasing.

In a post MAC Randomization Era

Source: Wireless Broadband Alliance
Author(s): Testing & Interoperability Work Group
Issue date: March 2021
Version: 1.0
Document status: Final

ABOUT THE WIRELESS BROADBAND ALLIANCE

Founded in 2003, the vision of the Wireless Broadband Alliance (WBA) is to drive seamless, interoperable service experiences via Wi-Fi within the global wireless ecosystem. WBA's mission is to enable collaboration between service providers, technology companies and organizations to achieve that vision. WBA undertakes programs and activities to address business and technical issues, as well as opportunities, for member companies.

WBA work areas include industry guidelines, standards development, trials certification and advocacy. Its key programs include NextGen Wi-Fi, 5G, IoT, Testing & Interoperability, Roaming and Policy & Regulatory Affairs, with member-led Work Groups dedicated to enable interoperability, resolving standards and technical issues to promote end-to-end services and accelerate business opportunities. WBA's membership is comprised of major operators, identity providers and leading technology companies, including, Commscope, Facebook, HPE Aruba, Nokia, Orange, Qualcomm, Rogers, Samsung, Shaw, Swisscom, Softbank, Telstra, Telus and T-Mobile US.

For a complete list of current WBA **Board** and WBA members, **click here**.

Follow Wireless Broadband Alliance:

www.twitter.com/wballiance

http://www.facebook.com/WirelessBroadbandAlliance

https://www.linkedin.com/company/wireless-broadband-alliance

UNDERTAKINGS AND LIMITATION OF LIABILITY

This Document and all the information contained in this Document is provided on an 'as is' basis without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for particular purpose, or non-infringement.

In addition, the WBA (and all other organizations who may have contributed to this document) makes no representations or warranties about the accuracy, completeness, or suitability for any purpose of the information. The information may contain technical inaccuracies or typographical errors. All liabilities of the WBA (and all other organizations who may have contributed to this document) howsoever arising for any such inaccuracies, errors, incompleteness, suitability, merchantability, fitness and non-infringement are expressly excluded to the fullest extent permitted by law. None of the contributors make any representation or offer to license any of their intellectual property rights to the other, or to any third party. Nothing in this information or communication shall be relied on by any recipient.

The WBA also disclaims any responsibility for identifying the existence of or for evaluating the applicability of any claimed copyrights, patents, patent applications, or other intellectual property rights, and will take no position on the validity or scope of any such rights. The WBA takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any effort to identify any such rights.

Neither the WBA nor any of the other organizations who may have contributed to this document will be liable for loss or damage arising out of or in connection with the use of this information. This is a comprehensive limitation of liability that applies to all damages of any kind, including (without limitation) compensatory, direct, indirect or consequential damages, loss of data, income or profit, loss of or damage to property and claims of third parties.

CONTENTS

1 Executive Summary

Since the early days of networking, the device MAC (Media Access Control) address was a fixed unique hardware address that uniquely identified the device on a network. Times and technology changed. Wi-Fi came along and MAC addresses moved into firmware and then into software. Having the MAC address broadcast over the Wi-Fi airwaves meant that 3rd parties could observe it and track the behavior of the devices, and having it set by software meant that devices could be configured to masquerade as others.

Together these introduced issues on both privacy and authenticity. To address the privacy issue, Operating Systems such as iOS, Android, and Windows have been introducing anonymization of Wi-Fi client device MAC addresses over the last couple of years to improve users' privacy. This is typically happening in an incremental way and started with probe requests whilst still using the true MAC address when connecting to the network.

The WBA community has been looking at the issues of MAC address anonymization for quite some time and has identified a list of potential impacts of these changes to existing systems and solutions. The WBA hopes this can help towards defining a mitigation path and steps required to update the Wi-Fi network ecosystem.

Subsequently, the WBA community agreed on a priority set of use cases that a Wi-Fi Identification Standard should address and performed the market requirements analysis and matching technologies able to scale and achieve longer term sustainability of deployed services.

2 MAC Randomization Problem Statement

Currently most OSs are anonymizing the MAC address differently for each network SSID and for probing so that users cannot easily be tracked between networks. A further feature of this per-SSID randomization is that it may change to a new value if the user forgets the network and then rejoins it, and the same thing may also happen if the device is reset.

Forthcoming versions of the OSs will not only randomize this MAC address differently for each SSID but will have the ability to change it approximately every 24 hours, preventing an eavesdropper from tracking user behavior on an individual network over time, and that will eventually become the default behavior for all operating systems. In all cases, these randomized MAC addresses are generated within the locally managed address space and so are local to the layer 2 network.

In summary, the MAC address will no longer be a persistent identifier for a device either across SSIDs or even within a single SSID and unfortunately it has been widely used in this manner for a wide variety of purposes (for example for Access Control on Wi-Fi networks) often intended to improve the user experience, which will cease to function as intended at the expense of the user experience.

The scale of the changes required to remove dependence on MAC address as a long-term identifier from all affected Wi-Fi networks will be significant and expensive. When the MAC address is no longer used as a device identifier, this will also go some way towards addressing the issue of other devices using a MAC address for impersonation.

2.1 MAC Randomization Impacts

WBA community identified a list of potential impacts of these changes to existing systems and solutions:

MAC-based access control:

With per-session MAC randomization, listing devices to deny access based on MAC Address becomes completely ineffective. This might be used for example, where a user account has been invalidated but the profile remans on the device and repeatedly challenges the AAA only to receive authentication failures. Conversely, having a list of permitted devices would quickly result in complete denial of access as the MAC addresses changed.

MAC is recorded on first time usage and identifies the device on subsequent logins. e.g. MAC Authentication, rules for connection management that are configured by MAC, certain widely deployed captive portal configurations. In these cases, the customer would have to re- sign-in and register the device each time the MAC changes and may exceed any operator-imposed limits on permitted number of devices.

On the service side, it would result in a long list of MAC address per device, and on those networks with limits on the number of devices per customer, the customer would find it difficult to manage the permitted devices list as the device identities change.

Certain widely used Pay Per Use (PPU) customers have their pass associated with a MAC, so if the MAC Address changes there is no way to transfer that pass to that changed MAC.

Certain widely used term-limited complimentary services could be accessed by customers repeatedly upon getting a new MAC Address. This would allow customers to get another free session / allowance, simply by forgetting the SSID.

This may impair the ability of the Wi-Fi service to enforce policies tied to specific devices, such as parental controls. The user can easily get a new MAC address, and network-based parental controls would no longer be applied appropriately.

Passpoint profiles are not SSID-based:

When a device connects to an SSID with a particular profile, using a particular MAC address there is no guarantee that the same MAC address will be used for the same profile on a different SSID. Likewise, if one device connects to a particular SSID using two or more different Passpoint profiles, we will be guaranteed not to have the same randomized MAC address will be used for different profiles on the same SSID.

However, there are User-experience issue regarding Passpoint profile deployment - the limited proportion of in-use devices supporting Passpoint Release 2 (Online Sign-Up), and the all too often daunting experience when installing a profile.

There are also aspects of Passpoint where the recommendations may be reliant upon MAC address as an identifier persisting beyond the session for the feature to function. In these cases, we need to liaise with the WFA to clarify or change the recommendations.

The ones identified so far are:

- The acceptance of terms & conditions in Section 10.1 indicates that the AAA server saves the timestamp associates with the STA MAC address.
- Certificate Enrollment in Section 7.6.1/7.6.4, the STA MAC address is one of the options to identify a Wi-Fi client device and bind a certificate to.
- DevDetail MO vendor specific extension Section 9.2, the DevDetail MO contains a *Wi-FiMACAddress* node which the STA fills with its currently set MAC address.

Wi-Fi Client steering:

Different bands with different SSIDs (split-SSID on 2.4GHz and 5GHz), will see different MAC addresses on the different SSIDs, which breaks (band-) steering between the SSIDs. Any network supporting more than one SSID will suffer similar Wi-Fi client steering issues.

In some implementations, client devices may use a different randomized MAC address for probing and for association, even when probing for the specific SSID. Pre-emptive Wi-Fi Client steering depends on probes having the same MAC address as the one the Wi-Fi Client will use when associated. In cases where this is not within the same ESS (e.g. with Public and private SSIDs) it will be for ESSs from the same service provider.

Certain steering applications are QoE (quality of experience) oriented. As such, they try to self-improve and deliver a higher QoE over time by learning a Wi-Fi client's steering related behavior. For example, successes and failures to comply with the steering action or the disconnection time in a network caused by a steering action. In In-Home Wi-Fi networks, a client device's MAC address is the key to relate all the learned parameters. Note that not all In-Home Wi-Fi networks are accompanied by a cloud system hence they keep all optimizations organized per MAC address as this was considered the reliable identifier of a device.

When different MAC addresses are used, Wi-Fi client steering cannot determine that the observed devices are the same Wi-Fi client.

MAC Collisions:

MAC randomization could result in duplication of another randomized MAC address, creating a duplicate MAC scenario (collision). Collision of MAC addresses under the same DHCP server would cause issues with the users accessing the network.

Physical Layer Analytics:

Wi-Fi analytics rely on the ability to identify a unique device consistently over time. Not only from the point of view of collecting the data to perform an analysis, but to take remedial action towards a specific Wi-Fi client via the service network.

Helpdesks need to be able to identify specific devices that the customer is calling about and understand how they have behaved over time. If a user forgets the SSID because they are having connectivity problems or if the target Wi-Fi client randomizes its MAC address due to a time-gating rule, the service provider will lose traceability of the issue. This will also make it more difficult for the user to identify their device to the helpdesk advisor.

If a device has an association failure on first attempting to connect, there is no guarantee the same MAC Address will be used subsequently. The failure cannot be reliably traced and attributed to a specific troublesome device.

Access points / Service providers which track the history of devices that have connected will end up with bloated records which contain additional entries for devices where the MAC address has changed.

Locally managed MACs mean that it will no longer be possible to identify manufacturer from OUIs or CIDs in the IEEE registry for the purposes of troubleshooting, diagnostics, and analytics.

Accounting and billing issues:

MAC Address is tied to this in use cases where rates rely on a unique device identifier. This could be accomplished instead with proper support for Chargeable-User-Identity (CUI).

Without MAC there may be diminished ability to handle Legal requirements for providing the type of information required for device traceability, device ownership, and legal intercept; but MAC was increasingly unreliable anyway.

Quality of Service (QoS) and Quality of Experience (QoE)

QoS and QoE are popular features on which a lot of effort is being spent by Wi-Fi equipment vendors and Telecommunication equipment vendors in general.

QoS for example is important to allow prioritization for both services and devices in a network. It should be noted that a lot of the services and data connections consumed in residential networks are not properly QoS - tagged nor is it sometimes even possible to do so. For example, if a QoS rule would have to link with a device rather than an IP-based service.

Access points are as such configured with QoS/QoE rules to force Wi-Fi clients in a specific priority scheme such as a Wi-Fi Alliance® WMM access class or an AP’s airtime scheduling queue.

In In-Home Wi-Fi networks, Wi-Fi clients are identified by means of their unique MAC address, as such, the access points (APs) that form the network hold a synchronized list of MAC address to QoS/QoE mapping to ensure that Wi-Fi clients receive a uniform QoS/QoE treatment throughout the full network.

If Wi-Fi clients randomize their MAC address, they effectively remove themselves from the current QoS/QoE ruleset that has been put in place to improve their operation in the network.

Lawful intercept

Lawful interception (LI) is the legally sanctioned official access to private communications. In general, LI is a security process in which a network operator or service provider gives law enforcement officials access to the communications of private individuals.

LI may use the uniqueness of a Wi-Fi device's MAC address to facilitate identification of a particular user's devices behind a network gateway that implements network address translation (NAT) for example.

For public hotspots, but also In-Home networks, the unique MAC address is used to help link IP sessions to particular users' devices.

If Wi-Fi clients implement randomized MAC addresses, including full randomization even at OUI level, MAC addresses can no longer be used as a persistent client device identification technique. Identification of users is of course by association.

For other publications please visit:
wballiance.com/resources/wba-white-papers

To participate in future projects, please contact:
pmo@wballiance.com

READ MORE

3 Wi-Fi Identification Standards

3.1 Market Requirements – by network type

Most use-cases are trying to provide a service that is specific to either a user or a specific device previously identified by MAC, and these will have to identify the device or user by some more private means. (Note: some of these may use IP address as the identifier, but the allocation of an IP address is typically dependent on MAC.)

All Networks

- Wi-Fi Client steering within an ESS is a MAC-based phy-layer feature. (The MAC persists across the ESS for the entire session so this should not be affected.)

Home Networks

- Steering across ESSs - e.g. for split SSIDs or to ensure devices use the private home network on APs that also support a community network (Maybe a MAC plus network-provider specific UID/DID required).
- Access time, content filtering, QoS and QoE controls are ESS MAC-based so will need to be tied to a UID/DID every session.
- L2 analytics for troubleshooting are MAC-based so may need to be tied to a DID every session if we are to get longer term analysis (e.g. for intermittent connectivity issues).
- Support for IoT and legacy items - Maintaining both device-specific authentication and a legacy PSK/MAC-based network is likely to be necessary but will place an added burden on low-resource APs and will probably be confusing to users.
- Restricted access for guests is similar to parental controls and may also be a problem!

Community Networks

- Access control is often MAC based and may end up with daily authentication (or should move to Passpoint or 802.1X).
- Any QoS that may be used is MAC- or IP- based, but where specific users or devices get a privileged service, those at least need to be tied to a UID/DID every session.

Enterprise/Corporate Networks.

- Networks are largely 802.1X based but may need MAC for L2 QoS and/or analytic purposes.

For other publications please visit:
wballiance.com/resources/wba-white-papers

To participate in future projects, please contact:
pmo@wballiance.com

READ MORE

- Network analytics for service planning, management, and security auditing may or may not need Device IDs.

Hospitality Networks

- If MAC-based, you may have to accept that the guest may need to reauthenticate daily, or otherwise will require some means to tie the device to a UID/DID every session e.g. through a portal page, a barcode on a receipt, or a branded App. (Consider changing to a more secure mechanism such as Passpoint.)

Public Networks

- Networks may choose to accept per-session authentication and loss of control over access restrictions.
- Authentication of the user is managed by the Home SP AAA. Visited networks often do not need to know who the user is.
- Need some guidelines for CUIs that protect privacy, and the mechanisms needed to obtain lawful access to identities when actually required from the HSP – MAC addr' was never really reliable anyway.
- Passpoint networks requiring Ts & Cs acceptance – need to investigate this and other Passpoint features and any dependence they may have on MAC.
- MACs can no longer be used to block devices that make repeated retries of invalid credentials, the AAA must communicate to the device that the credentials are not valid, and the device must honor that and seek remediation or stop trying to use them.

3.2 Implementation Options

A) MAC addresses will remain the identifier for the physical layer network within each session and will continue to be used to control physical-layer aspects of the network.
The control mechanism for purposes such as QoS and Wi-Fi diagnostics will still need a mapping from the authorization service to the session MAC and/or IP being used by the device and; particularly for in-home wi-fi; the system must be able to continue functioning when internet connectivity is lost (e.g. for access to the AP management page, or in-home streaming).
For many older or less capable devices, an AP may also still need to support WPA-PSK and MAC access controls as it always has done.

For other publications please visit:
wballiance.com/resources/wba-white-papers

To participate in future projects, please contact:
pmo@wballiance.com

READ MORE

B) For access control and identification on Public, Community and Enterprise networks, switch to technologies such as OpenRoaming, Passpoint and use AAA/WRIX for roaming and billing.

C) For Operator-provided/-managed home networks, whilst the basic network should continue to function normally any functions that are based on MAC address (e.g. parental controls, traffic limiting, per-device services) will either cease to work or start to affect the user experience. Wi-Fi layer 2 diagnostics will be seriously impacted.
These networks may not be suitable for implementing Passpoint and an alternative device identification standard that is appropriate to the needs will be required. As a result, diagnostic and policy enforcement functionality will have to be re-implemented and updated across all affected APs.

D) For consumer self-installed home networks that use any MAC features, firmware or equipment updates may be the only option.

4 Items for Future Investigation

The suitability of the following for alleviating MAC rand issues:

- Passpoint and WRIX/AAA
- OpenRoaming
- Captive Portal/Capport

Security/Trust:

- OSU, Capport, and Apps as mechanisms for installation of credentials and profiles
- Sharing/leaking of ‘identity’/credentials to other devices to allow them to use a network (common practice for PSKs) where these may previously have been anchored to a MAC.
- Certificates and their acceptance for specific Wi-Fi uses (e.g. Private CA for device auth)
- Private DNS (privacy impacts of DoH and DoT)
- Identifying Wi-Fi networks without revealing user location.
- Services sending or receiving identities when they have no need to know/reveal them.

Legal obligations - User Identification and ‘Lawful Intercept’ - on public and home network operators.

5 Industry Next Steps

WBA would like to recommend that the operator and vendor community join forces to identify further mitigations for the effects of MAC randomization, and alternative secure identifiers that are not publicly observable, nor shared outside of a network.

This Wi-Fi Identification standard document collates the latest WBA members' identified paths towards achieving broad adoption whilst maintaining user privacy.

WBA has recently started a new project within Testing & Interoperability to identify and promote broad adoption of secure Wi-Fi Identity standards that support the provision of Wi-Fi networks and services whilst limiting the identification of users.

WBA plans to host regular discussions under its Testing & Interoperability group and would welcome participation from the various players in the ecosystem.

For more information and to participate please contact: **pmo@wballiance.com**

For other publications please visit:
wballiance.com/resources/wba-white-papers

To participate in future projects, please contact:
pmo@wballiance.com

READ MORE