IETF 111 Virtual – MADINAS BoF

MAC Address Device Identification for Network and Application Services

WG Forming BoF

Chairs:
Juan Carlos Zúñiga - Sigfox
Carlos Bernardos – UC3M

July 2021

IETF 111 Virtual Meeting Tips + Etiquette

- Please join the queue before participating – Raise Hand in Meetecho ✋
- Mute your microphone unless you are speaking
- Preferably, turn your video off if you are not speaking

https://www.ietf.org/how/meetings/111

https://www.ietf.org/how/meetings/111/ietf111-meetecho/

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)

Reminders

- Minutes are taken
- This meeting is recorded
- Presence is logged (blue sheets) by logging into DataTracker
- Scribe(s): please contribute online to the minutes at https://codimd.ietf.org/notes-ietf-111-madinas
- Recordings and Minutes are public and may be subject to discovery in the event of litigation

Agenda

1. Welcome, Scope & Agenda Bashing – Chairs 15 minutes

2. Background + Clarification Q&A 30 minutes

   Background and status about MAC address randomization work at the IETF, Amelia Andersdotter (5 mins)

   Background and status about MAC address randomization work at the IEEE 802, Jerome Henry (CISCO) (10 mins)

   Background and status about MAC address randomization work at the Wireless Broadband Alliance, Tim Twell (10 mins)

3. Use cases and Problem statement + Clarification Q&A 25 minutes

   Randomized and Changing MAC Address Use Cases, Jerome Henry (CISCO) (15 mins)

4. Charter discussion – BoF Chairs w/AD Support 35 minutes

5. Next Steps – BoF Chairs w/AD Support 15 minutes

Purpose of MADINAS BoF

- Inform IETF community about latest MAC address randomization activities and purposes
- Present Network and Application Service-related issues related to MAC address randomization
- Identify whether any actions are required at the IETF, such as:
  - Coordination with other SDOs
  - Documentation of use cases
  - Identification of existing solutions/gaps

Purpose of a WG-forming BoF (RFC 5434)

Demonstrate that the community has agreement that:

- **there is a problem** that needs solving, and the IETF is the right group to attempt solving it.
- there is a **critical mass of participants willing to work** on the problem (e.g., write drafts, review drafts, etc.).
- **the scope of the problem is well defined** and understood, that is, people generally understand what the WG will work on (and what it won't) and what its actual deliverables will be.
- there is **agreement that the specific deliverables** (i.e., proposed documents) are the right set.
- it is believed that **the WG has a reasonable probability of having success** (i.e., in completing the deliverables in its charter in a timely fashion).

Background

MAC Address Randomization-related work at IETF

MAC Randomization at the IETF

(Andersdotter, Zúñiga, Bernardos)

- MAC-independent IPv6 address generation (SLAAC Privacy)
- Several initiatives in specialised protocols for networking in e.g. automobiles (ipwave, etc)
- Other privacy initiatives dealing with non-MAC and non-IP related identifiers (pearg, qname minimization, RFC7844 Anonymity profiles, …)
    - see also: draft-zuniga-mac-address-randomization
- RFC6973 Privacy Considerations for Protocol design sparked a number of RFC reviews that have also led to privacy-oriented changes, although not always identifier related.

Background

MAC Address Randomization work at IEEE 802

IEEE 802E

- Following IETF work in 2013-2015 on privacy, IEEE 802 (under the umbrella of the IEEE 802.1 Security Workgroup) published a *Recommended Practice for Privacy Considerations for IEEE 802 Technologies*
  - *https://standards.ieee.org/standard/802E-2020.html*
- *RCM is not directly recommended, however:*
- a) Temporary identifiers should be used or at least permitted, especially for the use of short-lived services such as network probes.
- b) Temporary identifiers should not persist across different stages of the communication process and should be restricted to specific protocol exchanges. (clause 8)

IEEE 802.11bh

- An RCM TIG/SG was formed in 2019 by IEEE 802.11 WG, concluded in 2020, and resulted in the formation of 2 groups:
- ***802.11bh: Enhanced service with randomized MAC addresses***
  - *The goal: given RCM, are there services that break with current 802.11?*
    - *Note that the goal is not to fix the entire world, not to ’encourage’ or ‘discourage’ RCM, not to address privacy aspects (although the proposed solution should not degrade privacy in 802.11)*
  - *The group is examining which services, which use cases may break*
  - *Once the relevant use cases/services will have been identified, remediations will be proposed (either recommendations or enhancements to the IEEE 802.11 Standard)*
  - *Group work is expected to be rather short (publication by mid-2023)*

IEEE 802.11bi

- An RCM TIG/SG was formed in 2019 by IEEE 802.11 WG, concluded in 2020, and resulted in the formation of 2 groups:
- ***802.11bi: Enhanced service with Data Privacy Protection***
  - *The goal: can 802.11 be enhanced to offer better privacy?*
    - *Note that the goal is not to look at the consequences of RCM, although it is understood that RCM has a positive impact on privacy for personal devices*
  - *The group is examining which elements have an impact on privacy, which elements could improve privacy*
  - *The group will publish enhancements to the IEEE 802.11 Standard*
  - *Group work is expected to be longer than 802.11bh (publication by mid-2025)*

References

- https://www.ieee802.org/11/Reports/802.11_Timelines.htm
- https://mentor.ieee.org/802.11/documents
- https://www.ietf.org/archive/id/draft-zuniga-mac-address-randomization-01.txt

Background

MAC Address Randomization-related work at WBA

WIRELESS BROADBAND ALLIANCE

DRIVING NEXT WIRELESS EXPERIENCE

WBA WI-FI DEVICES IDENTIFICATION PROJECT

Presented by Tim Twell to IETF MADINAS 2021-07-28

Wi-Fi Device Identities Group - Objectives

- **Find alternative identities that will make the use of MAC address as a device identifier unnecessary**
  - beyond the legitimate per-session use.

- **Liaise with other Standards bodies working on the issue**
  - Provide and accept information from other organisations to ensure that standardised solutions are available.
  - Back in April we produced a Liaison Document to IETF, WFA etc which was very much a preview of the group's intended work, because that was the timely thing to do and 'incomplete' is better than 'too late'.

- **Analyse and document the problems and currently and available solutions**
  - There are existing technologies that can be used to identify devices instead of MAC addresses.
  - Systems may need adaptation to make use of these – e.g. tying ID to MAC every session

- **Recommend technologies and standards to suit various requirements**
  - There will not be a one-size-fits-all solution - e.g. Passpoint will be unlikely to work well in homes.

Wi-Fi Device Identities Group – Activities - updated

1. Problem Statement - Investigate the use of MAC addresses as device identifier

Beyond the legitimate per-session media access uses, the project has identified many use case where the use of the MAC address as a long term identifier may cause issues with the service. These were presented in the previous liaison documents.

2. Identify Wi-Fi Identification Requirements

By looking at the use cases, the project has identified the requirements that those cases have for identifying devices and/or users. Unfortunately, the summary of this is that identification of either the user or the device is required for most cases, and that the lifetime required of the identity can be anything from a few days to several years. This reinforces the view that different solutions may be required for different market segments

We have had a number of discussions on what level of identification is really required, rather than merely desired, and the principles of data protection and consent, where a user may decide to accept a lower level of service rather than consent to permanent identification.

3. Examine existing Solutions and Mitigations

At the moment we are examining existing technologies that include Wi-Fi identities and comparing those with the requirements that were identified in the previous stages of the project. We expect to complete that soon.

The idea is then to see whether there are any issues that cannot be solved by the existing solutions, the most obvious of which is making service levels associated to the identity available at the session level.

Wi-Fi Device Identities Group – Activities - updated

5. Recommendations for each Solution Category

The intention has changed a little at this point and we expect to start work on a high-level guide explaining how the solutions work and how one would go about deploying them as replacements in systems that have until now relied on MAC address. It is anticipated that that this may help to identify any further outstanding requirements, and that In-Home systems may be amongst the most troublesome due to the long legacy of equipment found in homes.

6. Outstanding Requirements

Having identified and outstanding requirements, we propose to again liaise with other standards bodies to see whether they already have or are developing anything that will resolve the issues.

We would, of course, also expect to provide assistance to develop solutions for any missing requirements if required.

7. White papers and recommendations

The final phase of the project will be to publish the whitepaper / papers and recommendation to the WBA membership. These are often accompanied by public summaries and may also be liaised to appropriate collaborating organisations.

Thank you

WBA PMO
Bruno Tomas – bruno@wballiance.com
Pedro Mouta – pedro@wballiance.com

Engage on projects via WBA extranet | PMO contact: pmo@wballiance.com

Use Cases and Problem Statement

MADINAS

RCM Informational Problem Statement Framework

https://datatracker.ietf.org/doc/draft-henry-madinas-framework/

Jerome Henry

July 2021

Draft Scope

- Analyze Use Cases where RCM* affects Network Services
- Analyze Use Cases where RCM affects User Experiences
- List of Requirements

https://datatracker.ietf.org/doc/draft-henry-madinas-framework/

*RCM: Randomized and Changing MAC addresses

Draft Updates – Use Cases 1/2

Definition of use cases for RCM, by triaging contributing elements:

- User vs. devices, personal vs. shared service devices
- Who is “they”? actors involved in network operations
  - Network functional entities (802.11 entities [APs*, WLCs**], switches, routers, 802.1X/DHCP services and more)
  - Human-related entities (OTA observers, wireless network operators, network access providers, OTWi/OTWe observers)

*WiFi access points, ** Wireless LAN Controllers

OTA: over the air, OTW: over the wire (i=internal, e=external)

Draft Updates – Use Cases 2/2

Definition of use cases for RCM, by triaging contributing elements (cont.):

- “Trust” variable (full trust, vs. selective trust, vs. zero trust)
- Environments (individual residential settings, managed residential settings, public guest networks, enterprise, with BYOD or MDM)
- Network entities that track the MAC today (L2 infra, 802.1X/DHCP services, routers, policy engines)
- Current assumptions on RCM

Draft Updates – Requirements

- The network must not make any assumption about client MAC address persistence.
- MAC address change must happen while allowing for service continuity.
- If a service is interrupted during the RCM process, there must be a formal mechanism for the client and the network to exchange about the interruption.
- During duration of the services, the device should not change the identity (or interruptions would occur)

Draft Updates – Possible Steps

- Survey the current standards that use MAC address as a device identifier in the protocol. Make recommendation to the working groups to remove the dependency.
- Identify a secure mechanism to authenticate and exchange network identity to the device.
- Identify a secure mechanism to inform the device about the type of network the device is connecting to (e.g. public Wi-Fi, enterprise, home), allowing the user to select the device identity (or identities) accordingly.
- Identify a secure mechanism for the network to request device identity. Upon successful authentication, the network may provide the device a temporary network-based marker to use the network services.
- Identify a secure mechanism for the device to notify the network prior to updating the MAC address.

Draft History

- v00 in March 2021, v01 revision in April, v02 revision in May after MADINAS presentations and exchanges
- *feedback and additional input are welcome and encouraged*

Charter Discussion

MADINAS Draft Charter

The Medium Access Control (MAC) address is the Link Layer address used in IEEE 802 technologies. It was originally assigned statically for each physical network card by the Network Interface Card manufacturer, out of the space reserved by the IEEE Registration Authority Committee (RAC) for globally unique MAC addresses. The MAC address is used as source or destination target when sending and receiving frames. The default static assignment of the MAC address raises privacy concerns for personal devices, which have recently started to be mitigated by end-device vendors implementing and SDOs specifying the use of Randomized and Changing MAC addresses (RCM).

Device identity is important in scenarios where the network needs to know the device or user identity in order to offer, operate and maintain certain services. Currently, many use cases and applications make an implicit assumption about the unique association between the device identity and its MAC address. This assumption is being used in both control plane and data plane functions and protocols. RCM breaks this assumption. This requires update of the current applications to function across MAC address changes.

The MADINAS Working Group will examine the effect of RCM schemes on network and application services in several scenarios identified as relevant. The group will also evaluate various identifiers (beyond the MAC address) that can be used by the network to provide services, as well as scenarios where personal device identity is not required.

For scenarios where personal device identity stability is desirable, the Working Group will recommend protocols that can be used to protect the request and exchange of identifiers between the client and the service provider. For scenarios where privacy is paramount, the group will recommend best practices to ensure that the privacy achieved with RCM is not compromised by the communication of other identifiers. The MADINAS Working Group will examine other IETF work that may be applicable.

The Working Group will work together with other IETF WGs (e.g., DHC, IntArea), and will liaise with other relevant SDOs such as IEEE 802 and the Wireless Broadband Alliance (WBA). The Working Group will coordinate on the different recommendations, as well as potential follow-up activities within or outside the IETF.

MADINAS is expected to be a short timeframe (12-18 months) Working Group to quickly assess these needs. Additional solution space documents may be published after a rechartering process is identified as necessary and in coordination with other relevant SDOs.

MADINAS Draft Charter

Introductory part

The Medium Access Control (MAC) address is the Link Layer address used in IEEE 802 technologies. It was originally assigned statically for each physical network card by the Network Interface Card manufacturer, out of the space reserved by the IEEE Registration Authority Committee (RAC) for globally unique MAC addresses. The MAC address is used as source or destination target when sending and receiving frames. The default static assignment of the MAC address raises privacy concerns for personal devices, which have recently started to be mitigated by end-device vendors implementing and SDOs specifying the use of Randomized and Changing MAC addresses (RCM).

Device identity is important in scenarios where the network needs to know the device or user identity in order to offer, operate and maintain certain services. Currently, many use cases and applications make an implicit assumption about the unique association between the device identity and its MAC address. This assumption is being used in both control plane and data plane functions and protocols. RCM breaks this assumption. This requires update of the current applications to function across MAC address changes.

The MADINAS Working Group will examine the effect of RCM schemes on network and application services in several scenarios identified as relevant. The group will also evaluate various identifiers (beyond the MAC address) that can be used by the network to provide services, as well as scenarios where personal device identity is not required.
For scenarios where personal device identity stability is desirable, the Working Group will recommend protocols that can be used to protect the request and exchange of identifiers between the client and the service provider. For scenarios where privacy is paramount, the group will recommend best practices to ensure that the privacy achieved with RCM is not compromised by the communication of other identifiers. The MADINAS Working Group will examine other IETF work that may be applicable.

The Working Group will work together with other IETF WGs (e.g., DHC, IntArea), and will liaise with other relevant SDOs such as IEEE 802 and the Wireless Broadband Alliance (WBA). The Working Group will coordinate on the different recommendations, as well as potential follow-up activities within or outside the IETF.
MADINAS is expected to be a short timeframe (12-18 months) Working Group to quickly assess these needs. Additional solution space documents may be published after a rechartering process is identified as necessary and in coordination with other relevant SDOs.

MADINAS Draft Charter

The Medium Access Control (MAC) address is the Link Layer address used in IEEE 802 technologies. It was originally assigned statically for each physical network card by the Network Interface Card manufacturer, out of the space reserved by the IEEE Registration Authority Committee (RAC) for globally unique MAC addresses. The MAC address is used as source or destination target when sending and receiving frames. The default static assignment of the MAC address raises privacy concerns for personal devices, which have recently started to be mitigated by end-device vendors implementing and SDOs specifying the use of Randomized and Changing MAC addresses (RCM).

Device identity is important in scenarios where the network needs to know the device or user identity in order to offer, operate and maintain certain services. Currently, many use cases and applications make an implicit assumption about the unique association between the device identity and its MAC address. This assumption is being used in both control plane and data plane functions and protocols. RCM breaks this assumption. This requires update of the current applications to function across MAC address changes.

Scope

The MADINAS Working Group will examine the effect of RCM schemes on network and application services in several scenarios identified as relevant. The group will also evaluate various identifiers (beyond the MAC address) that can be used by the network to provide services, as well as scenarios where personal device identity is not required.

For scenarios where personal device identity stability is desirable, the Working Group will recommend protocols that can be used to protect the request and exchange of identifiers between the client and the service provider. For scenarios where privacy is paramount, the group will recommend best practices to ensure that the privacy achieved with RCM is not compromised by the communication of other identifiers. The MADINAS Working Group will examine other IETF work that may be applicable.

The Working Group will work together with other IETF WGs (e.g., DHC, IntArea), and will liaise with other relevant SDOs such as IEEE 802 and the Wireless Broadband Alliance (WBA). The Working Group will coordinate on the different recommendations, as well as potential follow-up activities within or outside the IETF.

MADINAS is expected to be a short timeframe (12-18 months) Working Group to quickly assess these needs. Additional solution space documents may be published after a rechartering process is identified as necessary and in coordination with other relevant SDOs.

MADINAS Draft Charter

The Medium Access Control (MAC) address is the Link Layer address used in IEEE 802 technologies. It was originally assigned statically for each physical network card by the Network Interface Card manufacturer, out of the space reserved by the IEEE Registration Authority Committee (RAC) for globally unique MAC addresses. The MAC address is used as source or destination target when sending and receiving frames. The default static assignment of the MAC address raises privacy concerns for personal devices, which have recently started to be mitigated by end-device vendors implementing and SDOs specifying the use of Randomized and Changing MAC addresses (RCM).

Device identity is important in scenarios where the network needs to know the device or user identity in order to offer, operate and maintain certain services. Currently, many use cases and applications make an implicit assumption about the unique association between the device identity and its MAC address. This assumption is being used in both control plane and data plane functions and protocols. RCM breaks this assumption. This requires update of the current applications to function across MAC address changes.

The MADINAS Working Group will examine the effect of RCM schemes on network and application services in several scenarios identified as relevant. The group will also evaluate various identifiers (beyond the MAC address) that can be used by the network to provide services, as well as scenarios where personal device identity is not required.
For scenarios where personal device identity stability is desirable, the Working Group will recommend protocols that can be used to protect the request and exchange of identifiers between the client and the service provider. For scenarios where privacy is paramount, the group will recommend best practices to ensure that the privacy achieved with RCM is not compromised by the communication of other identifiers. The MADINAS Working Group will examine other IETF work that may be applicable.

Timeframe and inter-SDO coordination

The Working Group will work together with other IETF WGs (e.g., DHC, IntArea), and will liaise with other relevant SDOs such as IEEE 802 and the Wireless Broadband Alliance (WBA). The Working Group will coordinate on the different recommendations, as well as potential follow-up activities within or outside the IETF.
MADINAS is expected to be a short timeframe (12-18 months) Working Group to quickly assess these needs. Additional solution space documents may be published after a rechartering process is identified as necessary and in coordination with other relevant SDOs.

MADINAS Draft Charter

The Medium Access Control (MAC) address is the Link Layer address used in IEEE 802 technologies. It was originally assigned statically for each physical network card by the Network Interface Card manufacturer, out of the space reserved by the IEEE Registration Authority Committee (RAC) for globally unique MAC addresses. The MAC address is used as source or destination target when sending and receiving frames. The default static assignment of the MAC address raises privacy concerns for personal devices, which have recently started to be mitigated by end-device vendors implementing and SDOs specifying the use of Randomized and Changing MAC addresses (RCM).

Device identity is important in scenarios where the network needs to know the device or user identity in order to offer, operate and maintain certain services. Currently, many use cases and applications make an implicit assumption about the unique association between the device identity and its MAC address. This assumption is being used in both control plane and data plane functions and protocols. RCM breaks this assumption. This requires update of the current applications to function across MAC address changes.

The MADINAS Working Group will examine the effect of RCM schemes on network and application services in several scenarios identified as relevant. The group will also evaluate various identifiers (beyond the MAC address) that can be used by the network to provide services, as well as scenarios where personal device identity is not required.
For scenarios where personal device identity stability is desirable, the Working Group will recommend protocols that can be used to protect the request and exchange of identifiers between the client and the service provider. For scenarios where privacy is paramount, the group will recommend best practices to ensure that the privacy achieved with RCM is not compromised by the communication of other identifiers. The MADINAS Working Group will examine other IETF work that may be applicable.

The Working Group will work together with other IETF WGs (e.g., DHC, IntArea), and will liaise with other relevant SDOs such as IEEE 802 and the Wireless Broadband Alliance (WBA). The Working Group will coordinate on the different recommendations, as well as potential follow-up activities within or outside the IETF.
MADINAS is expected to be a short timeframe (12-18 months) Working Group to quickly assess these needs. Additional solution space documents may be published after a rechartering process is identified as necessary and in coordination with other relevant SDOs.

Deliverables

The group will produce the following deliverables:
- An Informational Problem Statement document, including use cases analysis and requirements.
- An Informational MAC Address Randomization analysis document.
- A Best Common Practices document.

Questions

- Does the community think that the problem statement is clear, well-scoped, solvable, and useful to solve?

- Who is willing to review documents (or comment on the mailing list)?

- Is there support to form a WG with the following charter?