

This pdf consolidates the proposed P802.11bh and 802.11bi PARs, CSDs, and their references.

The original 802.11 Random and Changing MAC Address study group can be found on mentor as listed further below, however these are in a variety application formats, and need to be downloaded with some of the hyperlink cross-references not appearing to work (at least for me) so I found organizing the documents to be quite a lot of work even before beginning to review process. This consolidate PDF is intended to make review easier, and thus feasible, for more 802.1 Working Group members.

The documents, with their (abbreviated) Mentor documents numbers (full originals and title on the pages of each document) are as follows (hyperlinked to their position in this document):

20-0854-07 P802.11bi PAR--Amendment: Enhanced service with Data Privacy Protection

20-1346-02 P802.11bi CSD

20-742-05 P802.11bh PAR--Amendment: Enhanced service with randomized MAC addresses

20-1117-03 P802.11bh CSD

Each of the CSDs has the same initial list of cross-references:

19-0588-02 ... summary of discussions on randomized and changing MAC addresses ...

19-0851-00 ... p802-1cq mac address assignment requirements ...

[Note statement on 802.1Q Scope here]

19-0884-00 ... temporary MAC addresses ...

19-1027-01 ...do not fear random macs ...

19-1313-02 ... pitfalls with address randomization ...

19-1314-02 ... privacy protection in wif-fi-analytics systems ...

19-1320-00 ... assignment of temporary addresses ...

together with general references to 802.11-2016 and 802.11aq. The P802.11bi CSD also references P802E.

The next page of this consolidated set gives a brief summary of the PARs.

P802.11bi--Amendment: Enhanced service with Data Privacy Protection

PAR (doc.:IEEE 802.11-20/0854r7): <https://mentor.ieee.org/802.11/dcn/20/11-20-0854-07-0rcm-par-proposal-for-privacy.docx>

PAR 5.2.b Scope of the project: : This amendment specifies modifications to the IEEE Std 802.11 medium access control (MAC) specification to specify new mechanisms that address and improve user privacy.

PAR 5.5 Need for the project: : Users and regulatory agencies are concerned about protecting personal information such as locations, movements, contacts and activities, etc. Devices incorporating IEEE Std 802.11 are ubiquitous, and being compliant with IEEE Std 802.11 does not sufficiently protect users from user tracking and user profiling attacks. Work has been done in this area in IEEE Std 802.11aq-2018. To ensure continued growth and support for IEEE Std 802.11, this project standardizes user privacy solutions applicable to IEEE Std 802.11.

CSD (doc.: IEEE 802.11-20/1346r1, apparently with duplicates in the filing system both as r1 and r2)

<https://mentor.ieee.org/802.11/dcn/20/11-20-1346-02-0rcm-csd-draft-for-privacy-amendment-of-rcm-project.docx>

[Note: It is unclear to which of the two proposed PARs this CSD refers. The title of the CSD is "CSD Draft for Privacy Amendment of RCM Study Group".]

P802.11bh--Amendment: Enhanced service with randomized MAC addresses

PAR (doc: 802.11-20-742-95-0rcm-RCM-final-draft)

<https://mentor.ieee.org/802.11/dcn/20/11-20-0742-05-0rcm-proposed-par-draft.docx>

5.2.b Scope of the project: This amendment specifies modifications to the IEEE Std 802.11 medium access control (MAC) specifications that preserve the existing IEEE Std 802.11 mechanisms that might otherwise be restricted in environments where STAs in an ESS use randomized or changing MAC addresses, without decreasing user privacy. User privacy concerns include exposure of trackable information to third parties or exposure of an individual's presence or behavior. This amendment introduces mechanisms to enable session continuity in the absence of unique MAC address-to-STA mapping. This amendment also aims at preserving the ability to provide customer support and troubleshooting, as well as arrival detection in a trusted environment, that might otherwise be restricted in environments where STAs in an ESS use randomized or changing MAC addresses.

5.5 Need for the Project: The number of mobile devices incorporating IEEE Std 802.11 is steadily increasing. Privacy concerns are pushing STA vendors to randomize the STAs' MAC addresses for a growing number of interactions with other IEEE Std 802.11 STAs. In turn, this randomization may affect the user

experience, for example by disrupting services that assume a unique MAC address per STA.

Additionally, many references in IEEE Std 802.11 to MAC address were made at times where the assumption of a unique association between a STA and a MAC address was strong.

There is a need to:

Ensure that IEEE Std 802.11 provisions that refer to a STA MAC address remain valid when that MAC address is random or changes.

Design mechanisms that enable an optimal user experience when the MAC address of a STA in an ESS is randomized or changes. These mechanisms should not decrease user privacy.

IEEE P802.11
Wireless LANs

RCM
A PAR Proposal**Date:** 09/25/2020**Author(s):**

Name	Affiliation	Address	Phone	Email
Rob Sun Edward Au Osama Abdoumagda	Huawei Technologies			Rob.sun@huawei.com
Carol Ansley				carol@ansley.com
Jerome Henry	Cisco Systems	124 Forest Ridge Lane, Pittsboro NC 27312	+1 919 392 2503	jerhenry@cisco.com

PAR

P802.11bi

Submitter Email:

Type of Project: Amendment to IEEE Standard 802.11-2016

Project Request Type: Initiation / Amendment

PAR Request Date:

PAR Approval Date:

PAR Expiration Date:

PAR Status: Draft

Root Project: 802.11-2016

1.1 Project Number: P802.11bi

1.2 Type of Document: Standard

1.3 Life Cycle: Full Use

2.1 Project Title: IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
Amendment: Enhanced service with Data Privacy Protection

3.1 Working Group: Wireless LAN Working Group(C/LM/802.11 WG)

3.1.1 Contact Information for Working Group Chair:

Name: Dorothy Stanley

Email Address: dstanley1389@gmail.com

3.1.2 Contact Information for Working Group Vice Chair:

Name: Jon Rosdahl

Email Address: jrosdahl@ieee.org

3.2 Society and Committee: IEEE Computer Society/LAN/MAN Standards Committee(C/LM)

3.2.1 Contact Information for Standards Committee Chair:

Name: Paul Nikolich

Email Address: p.nikolich@ieee.org

3.2.2 Contact Information for Standards Committee Vice Chair:

Name: James Gilb

Email Address: gilb@ieee.org

3.2.3 Contact Information for Standards Representative:

Name: James Gilb

Email Address: gilb@ieee.org

4.1 Type of Ballot: Individual

4.2 Expected Date of submission of draft to the IEEE SA for Initial Standards Committee Ballot:

Dec 2023

4.3 Projected Completion Date for Submittal to RevCom: Dec 2024

5.1 Approximate number of people expected to be actively involved in the development of this project: 50

5.2.a Scope of the complete standard: The scope of this standard is to define one medium access control (MAC) and several physical layer (PHY) specifications for wireless connectivity for fixed, portable, and moving stations (STAs) within a local area.

5.2.b Scope of the project: This amendment specifies modifications to the IEEE Std 802.11 medium access control (MAC) specification to specify new mechanisms that address and improve user privacy.

5.3 Is the completion of this standard contingent upon the completion of another standard? No

5.4 Purpose: The purpose of this standard is to provide wireless connectivity for fixed, portable, and moving stations within a local area. This standard also offers regulatory bodies a means of standardizing access to one or more frequency bands for the purpose of local area communication.

5.5 Need for the Project: Users and regulatory agencies are concerned about protecting personal information such as locations, movements, contacts and activities, etc. Devices incorporating IEEE Std 802.11 are ubiquitous, and being compliant with IEEE Std 802.11 does not sufficiently protect users from user tracking and user profiling attacks.

Work has been done in this area in IEEE Std 802.11aq-2018. To ensure continued growth and support for IEEE Std 802.11, this project standardizes user privacy solutions applicable to IEEE Std 802.11.

5.6 Stakeholders for the Standard: Manufacturers and users of semiconductors, personal computers, enterprise networking devices, consumer electronic devices, home networking equipment, and mobile devices; together with cellular operators, transportation industries, multiple system operators, and video content suppliers.

6.1 Intellectual Property

6.1.1 Is the Standards Committee aware of any copyright permissions needed for this project?

No

6.1.2 Is the Standards Committee aware of possible registration activity related to this project?

No

7.1 Are there other standards or projects with a similar scope? No

7.2 Is it the intent to develop this document jointly with another organization? No

8.1 Additional Explanatory Notes: 5.5: IEEE P802E - IEEE Draft Recommended Practice for Privacy Considerations for IEEE 802 Technologies, highlights techniques and concerns to improve privacy. IEEE Std 802.11aq™-2018: Preassociation Discovery (Amendment 5)

**IEEE P802.11
Wireless LANs**

**CSD Draft for Privacy Amendment of RCM Study
Group**

Date: 2020-08-31

Author(s):

Name	Affiliation	Address	Phone	email
Carol Ansley	self			carol@ansley.com

1. IEEE 802 criteria for standards development (CSD)

The CSD documents an agreement between the WG and the Sponsor that provides a description of the project and the Sponsor's requirements more detailed than required in the PAR. The CSD consists of the project process requirements, 1.1, and the 5C requirements, 1.2.

1.1 Project process requirements

1.1.1 Managed objects

Describe the plan for developing a definition of managed objects. The plan shall specify one of the following:

- a) The definitions will be part of this project.

Yes

- b) The definitions will be part of a different project and provide the plan for that project or anticipated future project.

- c) The definitions will not be developed and explain why such definitions are not needed.

1.1.2 Coexistence

A WG proposing a wireless project shall demonstrate coexistence through the preparation of a Coexistence Assurance (CA) document unless it is not applicable.

- a) Will the WG create a CA document as part of the WG balloting process as described in Clause 13?

Yes

- b) If not, explain why the CA document is not applicable.

1.2 5C requirements

1.2.1 Broad Market Potential

Each proposed IEEE 802 LMSC standard shall have broad market potential. At a minimum, address the following areas:

- a) Broad sets of applicability.

- User privacy is concerned with control of data that is or can be used to construct personally identifiable information (PII) and/or personally correlated information (PCI). A user of IEEE Std 802.11 compliant devices may generate PII and PCI. Retaining user control of the PII and PCI generated as a result of using such devices is a goal of this amendment.

- User privacy has also been an increasing area of focus in the wireless marketplace. Most smartphones, for example, have implemented at least randomly changing MAC addresses before associating with an access point. This trend is not confined to smartphones, other client devices such as laptops have also implemented this feature.
- The set of interested parties is not confined to client device manufacturers and users. At the same time, access points and the infrastructure that uses them have been increasing their capabilities to provide personalized services, as well as other tracking services, that are not necessarily compatible with privacy goals.

b) Multiple vendors and numerous users.

A wide variety of vendors currently build systems and products that impact privacy concerns for both the clients and access points. Based upon the variety of companies that participated in the RCM TIG and the RCM SG, it is anticipated that a substantial proportion of those vendors, and others, will participate in subsequent activities for improving privacy-related behaviors.

1.2.2 Compatibility

Each proposed IEEE 802 LMSC standard should be in conformance with IEEE Std 802, IEEE 802.1AC, and IEEE 802.1Q. If any variances in conformance emerge, they shall be thoroughly disclosed and reviewed with IEEE 802.1 WG prior to submitting a PAR to the Sponsor.

- a) Will the proposed standard comply with IEEE Std 802, IEEE Std 802.1AC and IEEE Std 802.1Q?

Yes

- b) If the answer to a) is no, supply the response from the IEEE 802.1 WG.

The review and response is not required if the proposed standard is an amendment or revision to an existing standard for which it has been previously determined that compliance with the above IEEE 802 standards is not possible. In this case, the CSD statement shall state that this is the case.

1.2.3 Distinct Identity

Each proposed IEEE 802 LMSC standard shall provide evidence of a distinct identity. Identify standards and standards projects with similar scopes and for each one, describe why the proposed project is substantially different.

This amendment defines modifications, additions and/or recommendations to the medium access control layer (MAC) to improve the privacy experienced by users in environments using IEEE Std 802.11 technology. These developments include a review of the recommendations of IEEE P802E.

There is no other WLAN standard focusing on enhancing the performance of IEEE Std 802.11 networks in regards to user privacy other than this amendment.

1.2.4 Technical Feasibility

Each proposed IEEE 802 LMSC standard shall provide evidence that the project is technically feasible within the time frame of the project. At a minimum, address the following items to demonstrate technical feasibility:

a) Demonstrated system feasibility.

There are already proprietary solutions available in the market to improve user privacy. However, there are a number of areas where standards support can enhance the overall performance of user privacy efforts.

The IEEE 802.11 Wireless Next Generation (WNG) Standing Committee (SC) and RCM Topic Interest Group (TIG)/Study Group (SG) have reviewed many presentations indicating that enhancements are technically feasible. These contributions outlined techniques related to privacy to enhance current use cases and enable new ones.

b) Proven similar technology via testing, modeling, simulation, etc.

IEEE Std. 802.11 technology is very mature and has a wide variety of legacy devices and a proven track record, with several billions of devices shipping each year. The principle of extending the IEEE 802.11 PHYs and MAC with new capabilities is also well established by previous amendments within IEEE 802.11.

The increased capabilities envisioned for the MAC necessary to implement the proposed amendment are in line with the current progress in technology and not expected to impinge testability.

1.2.5 Economic Feasibility

Each proposed IEEE 802 LMSC standard shall provide evidence of economic feasibility. Demonstrate, as far as can reasonably be estimated, the economic feasibility of the proposed project for its intended applications. Among the areas that may be addressed in the cost for performance analysis are the following:

a) Balanced costs (infrastructure versus attached stations).

WLAN equipment is accepted as having balanced costs. The development of features to support RCM features in WLAN network deployments will not disrupt the established balance.

b) Known cost factors.

Support of the proposed standard will likely require a manufacturer to develop modified firmware on AP STAs and non-AP STAs. The cost factors for these transitions are well known.

c) Consideration of installation costs.

The proposed amendment has no known impact on installation costs.

d) Consideration of operational costs (e.g., energy consumption).

This amendment is not expected to change today's operation costs.

e) Other areas, as appropriate.

None.

References:

- [1] [11-19-0588-02-0rcm-summary-of-discussions-on-randomized-and-changing-mac-addresses-2014-2019.odt](#)
- [2] [11-19-0851-00-0rcm-p802-1cq-mac-address-assignment-requirements.pptx](#)
- [3] [11-19-0884-00-0rcm-temporary-addresses.pptx](#)
- [4] [11-19-1027-01-0rcm-do-not-fear-random-macs.pptx](#)
- [5] [11-19-1313-02-0rcm-pitfalls-with-address-randomization.pptx](#)
- [6] [11-19-1314-02-0rcm-privacy-protection-in-wi-fi-analytics-systems.pptx](#)
- [7] [11-19-1320-00-0rcm-assignment-of-temporary-addresses.pptx](#)
- [8] 802.11-2016 - IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
- [9] 802.11aq-2018 - IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Preassociation Discovery.
- [10] IEEE P802E: Recommended Practice for Privacy Considerations for IEEE 802 Technologies highlights techniques and concerns to improve privacy.

IEEE P802.11
Wireless LANs

RCM
A PAR Proposal**Date:** 09/25/2020**Author(s):**

Name	Affiliation	Address	Phone	Email
Jerome Henry	Cisco	RTP 7, Research Triangle Park, NC 27560		jerhenry@cisco.com
Carol Ansley	Self			<u>carol@ansley.com</u>

PAR

P802.11bh

Submitter Email:**Type of Project:** Amendment to IEEE Standard 802.11-2016**Project Request Type:** Initiation / Amendment**PAR Request Date:****PAR Approval Date:****PAR Expiration Date:****PAR Status:** Draft**Root Project:** 802.11-2016

1.1 Project Number: P802.11bh**1.2 Type of Document:** Standard**1.3 Life Cycle:** Full Use

2.1 Project Title: IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
Amendment: Enhanced service with randomized MAC addresses**3.1 Working Group:** Wireless LAN Working Group(C/LM/802.11 WG)**3.1.1 Contact Information for Working Group Chair:****Name:** Dorothy Stanley**Email Address:** dstanley1389@gmail.com**3.1.2 Contact Information for Working Group Vice Chair:****Name:** Jon Rosdahl**Email Address:** jrosdahl@ieee.org**3.2 Society and Committee:** IEEE Computer Society/LAN/MAN Standards Committee(C/LM)**3.2.1 Contact Information for Standards Committee Chair:****Name:** Paul Nikolich**Email Address:** p.nikolich@ieee.org**3.2.2 Contact Information for Standards Committee Vice Chair:****Name:** James Gilb**Email Address:** gilb@ieee.org**3.2.3 Contact Information for Standards Representative:****Name:** James Gilb**Email Address:** gilb@ieee.org

4.1 Type of Ballot: Individual**4.2 Expected Date of submission of draft to the IEEE SA for Initial Standards Committee Ballot:**

Jun 2023

4.3 Projected Completion Date for Submittal to RevCom: Dec 2024

5.1 Approximate number of people expected to be actively involved in the development of this project: 50**5.2.a Scope of the complete standard:** The scope of this standard is to define one medium access control (MAC) and several physical layer (PHY) specifications for wireless connectivity for fixed, portable, and moving stations (STAs) within a local area.**5.2.b Scope of the project:** This amendment specifies modifications to the IEEE Std 802.11 medium access control (MAC) specifications that preserve the existing IEEE Std 802.11 mechanisms that might otherwise be restricted in environments where STAs in an ESS use randomized or changing MAC addresses, without decreasing user privacy. User privacy concerns include exposure of trackable information to third parties or exposure of an individual's presence or behavior.

This amendment introduces mechanisms to enable session continuity in the absence of unique MAC

address-to-STA mapping. This amendment also aims at preserving the ability to provide customer support and troubleshooting, as well as arrival detection in a trusted environment, that might otherwise be restricted in environments where STAs in an ESS use randomized or changing MAC addresses.

5.3 Is the completion of this standard contingent upon the completion of another standard? No

5.4 Purpose: The purpose of this standard is to provide wireless connectivity for fixed, portable, and moving stations within a local area. This standard also offers regulatory bodies a means of standardizing access to one or more frequency bands for the purpose of local area communication.

5.5 Need for the Project: The number of mobile devices incorporating IEEE Std 802.11 is steadily increasing. Privacy concerns are pushing STA vendors to randomize the STAs' MAC addresses for a growing number of interactions with other IEEE Std 802.11 STAs. In turn, this randomization may affect the user experience, for example by disrupting services that assume a unique MAC address per STA. Additionally, many references in IEEE Std 802.11 to MAC address were made at times where the assumption of a unique association between a STA and a MAC address was strong.

There is a need to:

Ensure that IEEE Std 802.11 provisions that refer to a STA MAC address remain valid when that MAC address is random or changes.

Design mechanisms that enable an optimal user experience when the MAC address of a STA in an ESS is randomized or changes. These mechanisms should not decrease user privacy.

5.6 Stakeholders for the Standard: Manufacturers and users of semiconductors, personal computers, enterprise networking devices, consumer electronic devices, home networking equipment, and mobile devices; together with cellular operators, transportation industries, multiple system operators, and video content suppliers.

6.1 Intellectual Property

6.1.1 Is the Standards Committee aware of any copyright permissions needed for this project?

No

6.1.2 Is the Standards Committee aware of possible registration activity related to this project?

No

7.1 Are there other standards or projects with a similar scope? No

7.2 Is it the intent to develop this document jointly with another organization? No

8.1 Additional Explanatory Notes :

**IEEE P802.11
Wireless LANs**

**RCM SG Proposed CSD Draft for 802.11 RCM Pro-
ject**

Date: 2020-08-17

Author(s):

Name	Affiliation	Address	Phone	email
Carol Ansley	self			carol@ansley.com

Abstract

This document contains the IEEE 802.11 Random and Changing Mac Addresses (RCM) study group's (SG) proposed draft of Criteria for Standards Development (CSD) for the RCM project.

r0 – Initial presentation

r1 – Updated with comments from July 20 meeting

r2 - Updated after PAR discussion

r3 - Updated with comments from August 17 meeting

1. IEEE 802 criteria for standards development (CSD)

The CSD documents an agreement between the WG and the Sponsor that provides a description of the project and the Sponsor's requirements more detailed than required in the PAR. The CSD consists of the project process requirements, 1.1, and the 5C requirements, 1.2.

1.1 Project process requirements

1.1.1 Managed objects

Describe the plan for developing a definition of managed objects. The plan shall specify one of the following:

- a) The definitions will be part of this project.

Yes

- b) The definitions will be part of a different project and provide the plan for that project or anticipated future project.

- c) The definitions will not be developed and explain why such definitions are not needed.

1.1.2 Coexistence

A WG proposing a wireless project shall demonstrate coexistence through the preparation of a Coexistence Assurance (CA) document unless it is not applicable.

- a) Will the WG create a CA document as part of the WG balloting process as described in Clause 13?

Yes

- b) If not, explain why the CA document is not applicable.

1.2 5C requirements

1.2.1 Broad Market Potential

Each proposed IEEE 802 LMSC standard shall have broad market potential. At a minimum, address the following areas:

- a) Broad sets of applicability.

- User privacy has been an increasing area of focus in the wireless marketplace. Most smartphones, for example, have implemented at least randomly changing MAC addresses before associating with an access point. This trend is not confined to smartphones, other client devices such as laptops have also implemented this feature.

- The set of interested parties is not confined to client device manufacturers and users. At the same time, access points and the infrastructure that uses them have been increasing their capabilities to provide personalized services, as well as other tracking services, that are not necessarily compatible with privacy goals. Random and changing MAC addresses can impede the capabilities of access points and support infrastructure to provide services to the end users.
- b) Multiple vendors and numerous users.

A wide variety of vendors currently build systems and products that are affected by random and changing MAC addresses on both the client and access point sides. Based upon the variety of companies that participated in the RCM TIG it is anticipated that a substantial proportion of those vendors, and others, will participate in subsequent activities for improving RCM-related behaviors.

1.2.2 Compatibility

Each proposed IEEE 802 LMSC standard should be in conformance with IEEE Std 802, IEEE 802.1AC, and IEEE 802.1Q. If any variances in conformance emerge, they shall be thoroughly disclosed and reviewed with IEEE 802.1 WG prior to submitting a PAR to the Sponsor.

- a) Will the proposed standard comply with IEEE Std 802, IEEE Std 802.1AC and IEEE Std 802.1Q?

Yes

- b) If the answer to a) is no, supply the response from the IEEE 802.1 WG.

The review and response is not required if the proposed standard is an amendment or revision to an existing standard for which it has been previously determined that compliance with the above IEEE 802 standards is not possible. In this case, the CSD statement shall state that this is the case.

1.2.3 Distinct Identity

Each proposed IEEE 802 LMSC standard shall provide evidence of a distinct identity. Identify standards and standards projects with similar scopes and for each one, describe why the proposed project is substantially different.

This amendment defines modifications to the medium access control layer (MAC) to improve user or end device experiences in environments where IEEE 802.11 STAs (both AP and non-AP STAs) use random or changing MAC addresses. These modifications will address operational challenges resulting from the use of random or changing MAC addresses with at least three use cases.

The use cases to be addressed include at least initial infrastructure connection steering, customer support and troubleshooting and arrival detection in a home environment, or other trusted environments.

There is no other WLAN standard focusing on enhancing the performance of IEEE 802.11 networks in regards to random and changing MAC addresses other than this amendment.

This amendment will ensure coexistence and backward compatibility with legacy IEEE 802.11 devices and will not compromise current levels of privacy protection afforded by the IEEE 802.11 standard or the best understanding of current practices in RCM implementations.

1.2.4 Technical Feasibility

Each proposed IEEE 802 LMSC standard shall provide evidence that the project is technically feasible within the time frame of the project. At a minimum, address the following items to demonstrate technical feasibility:

a) Demonstrated system feasibility.

There are already proprietary solutions available in the market to handle random and changing MAC addresses. However, there are a number of areas where standards support can enhance the overall user experience when operating devices with RCM features.

The IEEE 802.11 Wireless Next Generation (WNG) Standing Committee (SC) and RCM Topic Interest Group (TIG)/Study Group (SG) have reviewed many presentations indicating that the proposed enhancements are technically feasible. These contributions outline techniques related RCM operation, privacy, and interoperability to enhance current use cases and enable new ones.

b) Proven similar technology via testing, modeling, simulation, etc.

IEEE Std. 802.11 technology is very mature and has a wide variety of legacy devices and a proven track record, with several billions of devices shipping each year. The principle of extending the IEEE 802.11 PHYs and MAC with new capabilities is also well established by previous amendments within IEEE 802.11.

The increased capabilities envisioned for the MAC necessary to implement the proposed amendment are in line with the current progress in technology and not expected to impinge testability.

1.2.5 Economic Feasibility

Each proposed IEEE 802 LMSC standard shall provide evidence of economic feasibility. Demonstrate, as far as can reasonably be estimated, the economic feasibility of the proposed project for its intended applications. Among the areas that may be addressed in the cost for performance analysis are the following:

a) Balanced costs (infrastructure versus attached stations).

WLAN equipment is accepted as having balanced costs. The development of features to support RCM features in WLAN network deployments will not disrupt the established balance.

b) Known cost factors.

Support of the proposed standard will likely require a manufacturer to develop modified firmware on AP STAs and non-AP STAs. The cost factors for these transitions are well known.

c) Consideration of installation costs.

The proposed amendment has no known impact on installation costs.

d) Consideration of operational costs (e.g., energy consumption).

This amendment is not expected to change today's operation costs.

e) Other areas, as appropriate.

None.

References:

- [1] [11-19-0588-02-0rcm-summary-of-discussions-on-randomized-and-changing-mac-addresses-2014-2019.odt](#)
- [2] [11-19-0851-00-0rcm-p802-1cq-mac-address-assignment-requirements.pptx](#)
- [3] [11-19-0884-00-0rcm-temporary-addresses.pptx](#)
- [4] [11-19-1027-01-0rcm-do-not-fear-random-macs.pptx](#)
- [5] [11-19-1313-02-0rcm-pitfalls-with-address-randomization.pptx](#)
- [6] [11-19-1314-02-0rcm-privacy-protection-in-wi-fi-analytics-systems.pptx](#)
- [7] [11-19-1320-00-0rcm-assignment-of-temporary-addresses.pptx](#)
- [8] 802.11-2016 - IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
- [9] 802.11aq-2018 - IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Pre-association Discovery.

**IEEE P802.11
Wireless LANs**

**Summary of discussions on randomized and changing MAC
addresses 2014-2019**

Date: 2019-05-13

Author(s):

Name	Affiliation	email
Amelia Andersdotter	ARTICLE19	amelia@article19.org

Abstract

This document summarizes the discussions on MAC randomization in IEEE P802.11 between 2017-2019, and presents a collection of academic research, as well as previous IEEE standardisation work relating to randomized and changing MAC addresses.

Rev. 2: added references in sections IETF and Deployment. Added links to all IEEE 802 presentations cited.

Background outside of IEEE 802.11

IEEE 1609 WAVE

The idea of randomizing a MAC address to enhance privacy protection is not new (Gruteser (2005)). IEEE 1609.4 WAVE introduced MAC "re-addressing" as a privacy enhancement measure as far back as 2012 following concerns relating to geolocation tracking of connected vehicles. There is a large body of research on the use of changing or randomized identifiers to mitigate privacy concerns in vehicular networks (Ch. 2.3.2, Förster, 2017).

IETF

Standards work external to the IEEE which takes into account randomized MAC addresses includes new methods for generating IPv6 addresses developed by the IETF. While previous versions of IPv6 have assumed the IPv6 can be generated from the MAC identifier, this is no longer required (RFC7721, c. 4, 2016). How to establish lasting connections over IPv6 in the absence of permanent layer-2 identifiers has been raised in the IPWAVE group.

Regulatory

Regulatory requirements on network operators motivate closer investigation of stronger protections against non-consensual geolocation tracking (Autoriteit Persoonegevens (2014), Bouchenard (2015), Datainspektionen (2015), FCC (2015)). As regulatory requirements stabilize in this field, it may be an advantage to be able to offer network operators a "clean default". Namely, a situation wherein which an operator does not need to worry that default analytics and trouble-shooting mechanisms risk conflicting with such requirements.

Deployment

Leading mobile OSs have already started introducing various software-based MAC randomization mechanisms. They have been studied with respect to their efficiency in protecting privacy of their users (Matte et al (2016), Martin et al (2017)). Work on and deployment of MAC randomization is continuing in this sector (see Android Open Source Project's Privacy: MAC Randomization).

Sufficiency

There is a lot of research on tracking of individual devices in wireless networks (f. ex. Cunche (2013), Sapiezynski (2015)). The IEEE 802 Privacy ECSG has further studied possibilities of profiling of individual devices in the absence of a permanent unique MAC address (privecsg-16-0003-00-0000, Vanhoef et al (2016)). It is clear that MAC randomization is not in itself a sufficient guarantee for privacy of individual users, but one partial solution among many.

The background in IEEE 802 LMSC

MAC randomization has been visible in IEEE 802 LMSC since 2014. The future expected prevalence of MAC randomization techniques was, for instance, raised by commenters in the draft 0.3 ballot of what is now IEEE 802C.

The privacy threat mitigation potential of MAC randomization was also studied by 802 LMSC members at the Privacy ECSG in 2014 (privecsg-14-0026-01-0000, privecsg-14-0025-01-0000) and 2015 (privecsg-15-0028-00-0000).

Together with the assessment of software-driven MAC randomization referenced above, this work led to the inclusion of MAC randomization as a privacy enhancing feature in the .11aq Pre-Association Service Discovery Task Group amendment to the 802.11-2016. This work can be revisited at the "TGaq (inactive)" repository of the 802.11 mentor website. The .11aq amendment was approved by the IEEE Standards Association Standards Board in June 2018.

In September 2018, three months after the publication of the official 802.11aq amendment, the IEEE 802.11 WG received a liaison statement from the Wireless Broadband Alliance (WBA) detailing network operator concerns with the disappearance of clear-text sufficiently-permanent unique device identifiers (11-18-1579-00-0000).

The ARC SC made efforts to address the concerns raised by the WBA in a response approved by the 802.11 Working Group in November 2018 (11-18-1988-02-0arc). In this response, the Working Group noted that some issues raised by WBA merit further consideration.

MAC randomization issues identified by ARC SG

1. The WBA had raised with IEEE 802.11 that "A single device using different MAC addresses in different bands and/or different SSIDs."

The IEEE 802.11 responses was: "[W]e agree that band steering in this scenario is likely an issue. 802.11 WG should look into this, perhaps providing recommendations about SSID assignment, depending on network deployment and goals. 802.11 should coordinate with Wi-Fi Alliance on this topic."

2. WBA expressed concern that "Even if the MAC address is "stable" for a given SSID, many clients will use the broadcast SSID in probe requests, and hence there is again no stability in MAC address."

The IEEE 802.11 response was: "[C]lient steering is likely an issue. 802.11 WG should look into this. 802.11 should coordinate with Wi-Fi Alliance on this topic, depending on our findings."

3. WBA raised that "Analytics may rely on MAC addresses for identification."

The IEEE 802.11 response was: "We realize that some types of network analytics and troubleshooting are done at the low layers of the network stack, and don't have access to high-level concepts for identification. 802.11 WG should look into this."

In relation to the last point, the IEEE 802.11 also observed that they agreed with WBA that "identification of manufacturer, based on OUI portion of the MAC address" would not be possible for devices with a randomized MAC address.

Work in other IEEE 802 LMSC Working Groups

The network analytics and device identification issue was discussed in the IEEE 802.1 OmniRAN Task Group in its F2F meeting on 15 January 2019 (The assertion was made that device manufacturer identification and network analytics and troubleshooting would be an issue in the absence of MAC identifiers (omniran-19-0002-00-CQ00)).

It has been agreed that OmniRAN should be presented with a "draft protocol proposal for secure signaling of a static device identifier to the access network" and "functional requirements describing the need to provide the possibility of fixed device identifiers" (omniran-19-0005-02-00TG).

Summary of work going ahead

Bearing this in mind, RCM TIG was created to investigate

- Current and planned implementations of random and changing MAC addresses in devices, and
- Current and planned 802.11/802 Standards treatment of randomized MAC addresses
- Impact on 802.11 features from randomized MAC addresses and/or changing addresses during:
 - Pre-association (stateless)
 - Preparing for (creating shared state) and during associations
- Potential mechanisms to address the above impacts, through:
 - Implementation options, or possible guidelines document
 - Modifications to the Standard, if any, and recommend continuing work (Study Group/PAR)

References:

Android Open Source Project, *Privacy: MAC Randomization*, August 2018.
<https://source.android.com/devices/tech/connect/wifi-mac-randomization>

Autoriteit Persoongegevens, z2014-00944, *Wifi-tracking van mobiele apparaten in en rond winkels door Bluetrace*.

C. Bouchenard, *JC Decaux's pedestrian tracking system blocked by french data regulator*, Marketinglaw, 2015. <http://marketinglaw.osborneclarke.com/advertisingregulation/jc-decauxs-pedestrian-tracking-system-blockedby-french-data-regulator/>

M. Cunche. *I know your MAC Address: Targeted tracking of individual using Wi-Fi*, International Symposium on Research in Grey-Hat Hacking - GreHack, Nov 2013, Grenoble, France. <hal-00858324>

Datainspektionen, 31702-2015, *Tillsyn enligt personuppgiftslagen (1998:204) av Västerås Citysamverkan AB*.

Federal Trade Commission, *Retail tracking firm settles FTC charges it misled consumers about opt out choices*, 2015. <https://www.ftc.gov/news-events/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-misled-consumers>

D. Förster, *Verifiable Privacy Protection for Vehicular Communication Systems*, Dissertation, Ulm University, Germany, 2017.

M. Gruteser, D. Grunwald, *Enhancing Location Privacy in Wireless LAN Through Disposable Interface Identifiers: A Quantitative Analysis*, Mobile Networks and Applications 10, 315–325, 2005.

J. Martin, T. Mayberry, C. Donahue, L. Foppe, L. Brown, C. Riggins, E. C. Rye, D. Brown, *A Study of MAC Address Randomization in Mobile Devices and When it Fails*, Proceedings on Privacy Enhancing Technologies ; 2017 (4):268–286

C. Matte, M. Cunche, F. Rousseau, M. Vanhoef, *Defeating MAC Address Randomization Through Timing Attacks*, in Proceedings of the 9th ACM Conference on Security; Privacy in Wireless and Mobile Networks, WiSec '16, pages 15–20. ACM, 2016.

RFC 7721, A. Cooper, F. Gont, D. Thaler, *Security and Privacy Considerations for IPv6 Address Generation Mechanisms*, Internet Engineering Task Force (IETF), March 2016.
<https://tools.ietf.org/html/rfc7721>

P. Sapiezynski, A. Stopczynski, R. Gatej, S. Lehmann, *Tracking Human Mobility Using WiFi Signals*, PLoS ONE 10(7): e0130824, 2015, doi:10.1371/journal.pone.0130824

M. Vanhoef, C. Matte, M. Cunche, L. Cardoso, F. Piessens. *Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms*, in ACM AsiaCCS, 2016.

IEEE 802 LMSC references:

OmniRAN, *F2F meeting minutes* (omniran-19-0005-02-00TG), Hao Wang, January 2019. <https://mentor.ieee.org/omniran/dcn/19/omniran-19-0005-02-00TG-jan-2019-f2f-meeting-minutes.docx>

OmniRAN, *Random MAC impact* (omniran-19-0002-00-CQ00), Max Riegel, January 2019. <https://mentor.ieee.org/omniran/dcn/19/omniran-19-0002-00-CQ00-random-mac-impact.pptx>

Privacy ECSG, *Secure Moderated Random MAC Addresses* (privecsg-14-0026-01-0000), Robert Moskowitz, January 2015. <https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0026-01-0000-secure-moderated-random-mac-addresses.ppt>

Privacy ECSG, *WiFi Privacy network experiment at #IETF91* (privecsg-14-0025-01-0000), C. J. Bernardos, F. Giust, A. de la Oliva, J.C. Zuniga, January 2015. <https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0025-01-0000-wifi-privacy-network-experiment-at-ietf91.pptx>

Privacy ECSG, *WiFi Privacy network experiment at IEEE 802 May plenary and IETF91 meetings* (privecsg-15-0028-00-0000), C. J. Bernardos, A. de la Oliva, J.C. Zuniga, July 2015. <https://mentor.ieee.org/privecsg/dcn/15/privecsg-15-0028-00-0000-wifi-privacy-network-experiment-at-ieee-802-may-plenary-and-ietf91-meetings.pptx>

Privacy ECSG, *Tracking 802.11 stations without relying on the link layer identifier* (privecsg-16-0003-00-0000), Mathieu Cunche, April 2016. <https://mentor.ieee.org/privecsg/dcn/16/privecsg-16-0003-00-0000-tracking-802-11-stations-without-relying-on-the-link-layer-identifier.pdf>

IEEE 802.11 WG, *2018-09- Liaison from WBA re: MAC randomization impacts* (11-18-1579-00-0000), September 2018. <https://mentor.ieee.org/802.11/dcn/18/11-18-1579-01-0000-2018-09-liaison-from-wba-re-mac-randomization-impacts.docx>

IEEE 802.11 ARC SC, *Proposed response to liaison from WBA on MAC Address randomization impacts* [sic!] (11-18-1988-02-0arc), November 2018. <https://mentor.ieee.org/802.11/dcn/18/11-18-1988-02-0arc-proposed-response-to-liaison-from-wba-on-mac-address-randomization-impacts.docx>

P802.1CQ MAC Address Assignment Requirements

Date: 2019-05-12

Authors:

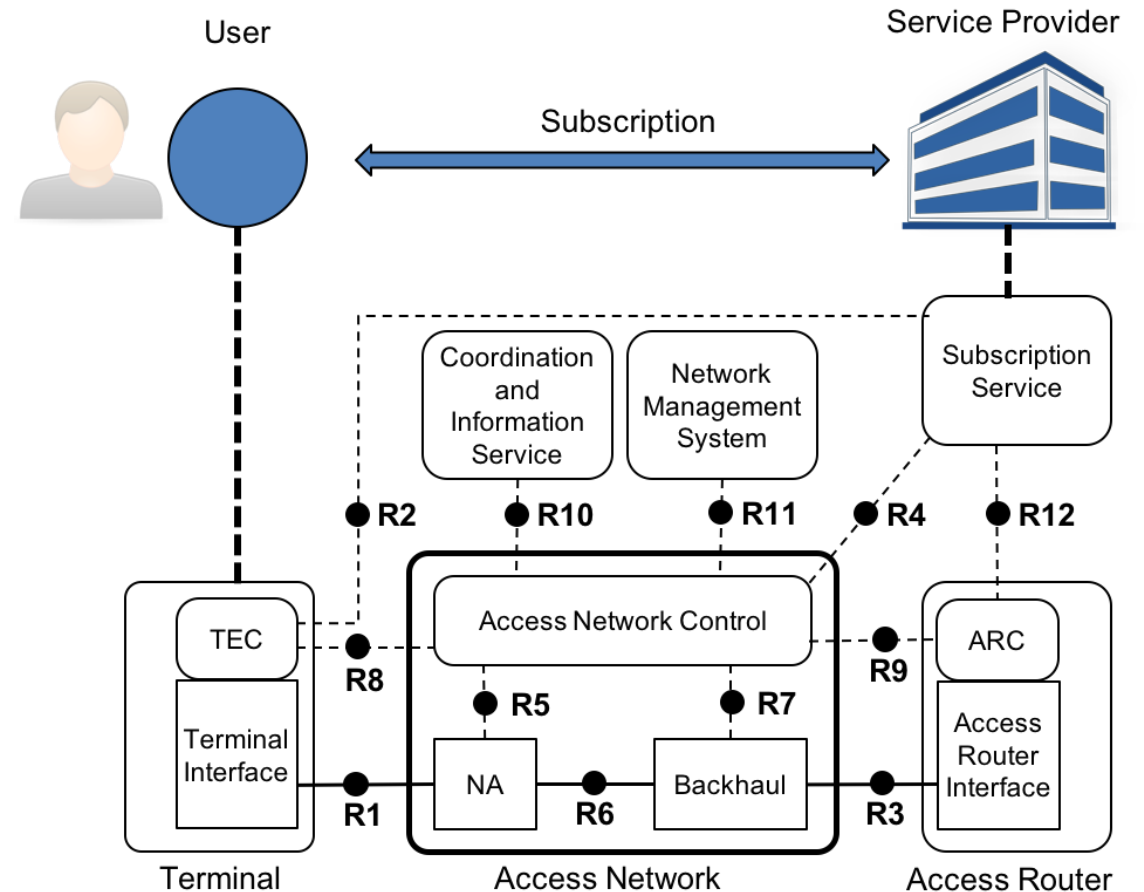
Name	Affiliations	Phone	email
Max Riegel	Nokia		maximilian.riegel@nokia.com

Abstract

- **This presentation provides a brief summary of the conclusions for P802.1CQ out of the discussions on impact of randomized MAC addresses at the 802.1 OmniRAN TG Jan 2019 interim meeting.**
- **P802.1CQ: Standard for Local and Metropolitan Area Networks: Multicast and Local Address Assignment**
 - This standard specifies protocols, procedures, and management objects for locally-unique assignment of 48-bit and 64-bit addresses in IEEE 802 networks. Peer-to-peer address claiming and address server capabilities are specified.

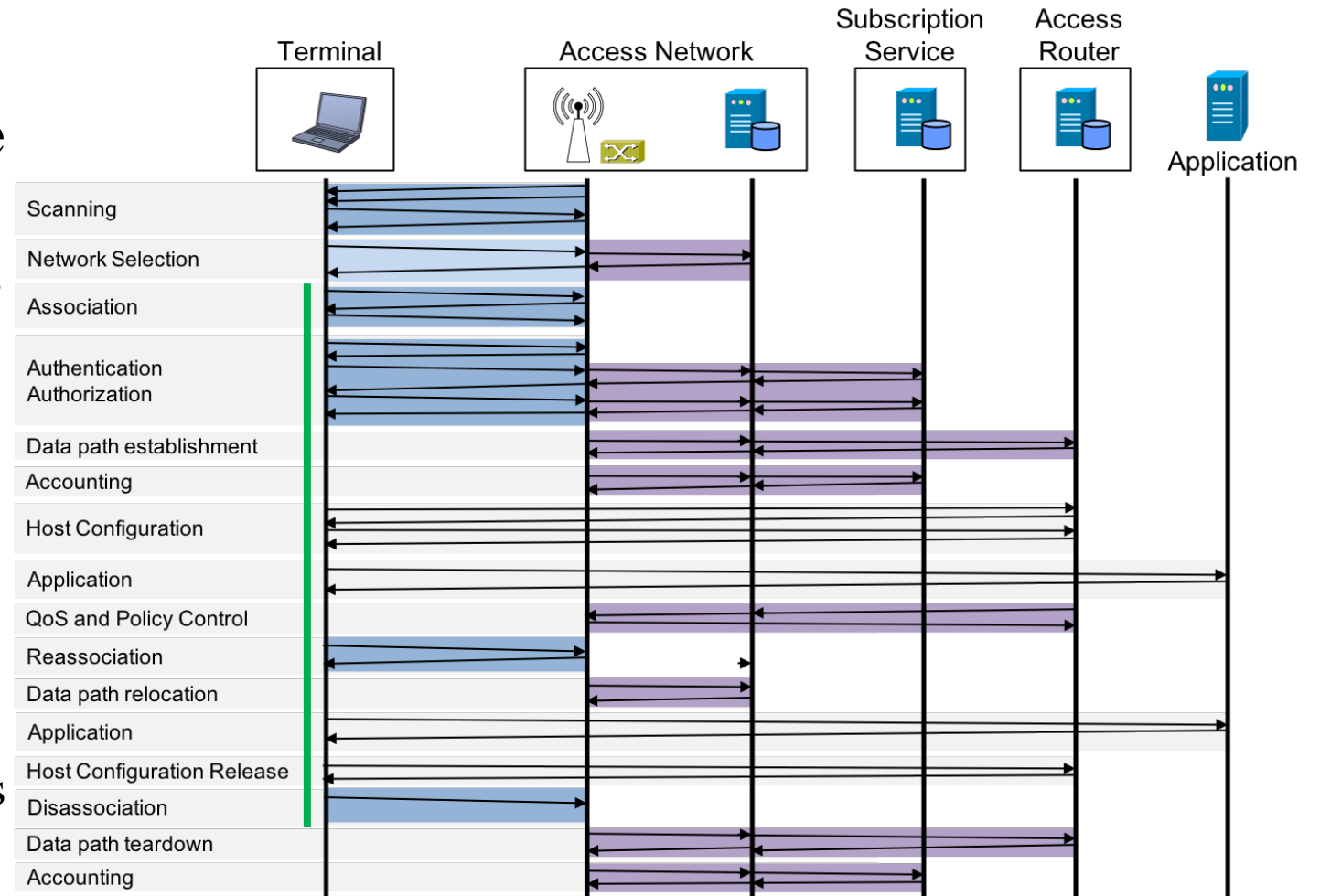
Random address discussions in OmniRAN TG

- **Triggered by WBA liaison to IEEE 802.11 and Wi-Fi Alliance**
 - <https://mentor.ieee.org/802.11/dcn/18/11-18-1579-01-0000-2018-09-liaison-from-wba-re-mac-randomization-impacts.docx>
- **Issue arises through binding of a human user with the terminal interface identifier (MAC address)**
 - No major issue when user isn't related to a human, e.g. if user is a control unit of a robot in a factory.



IEEE 802.1 Assumptions

- **Bridging protocols (main scope of IEEE 802.1) assume that MAC addresses of end-stations do not change while being connected to a bridge.**
 - From Association to Disassociation
- **P802.1CQ is currently the only 802.1 project dealing with end-station behavior**
 - Formerly, protocols for end-stations were out of scope for 802.1



P802.1Q position on MAC randomization

- **Discussion slides:**
 - <https://mentor.ieee.org/omniran/dcn/19/omniran-19-0002-00-CQ00-random-mac-impact.pptx>
- **Agreement reached that WBA use cases are legitimate reasons to provide the possibility to assign static device identifier to stations for initiating the dynamic MAC address assignment**
 - Static device identifier allows LAAP to assign fixed MAC addresses to devices.
- **Conclusions:**
 - Protocol proposal will allow for secure signaling of a static device identifier to the access network
 - Functional requirements section will describe the need to provide the possibility of fixed device identifiers

Temporary Addresses

Date: 2019-05-13

Authors:

Name	Affiliations	Address	Phone	email
Roger Marks	EthAirNet Associates	Denver, CO, USA	1-802-capable	roger@ethair.net

Abstract

This contribution provides background information on the use of temporary addresses in IEEE 802, IEEE 802.11, and other standards. It is intended for the information and consideration of the IEEE 802 RCM TIG.

Note: Much of this information was presented to IEEE 802.11 Plenary in September 2017 [1]. Additional background information on the topic is found in [5].

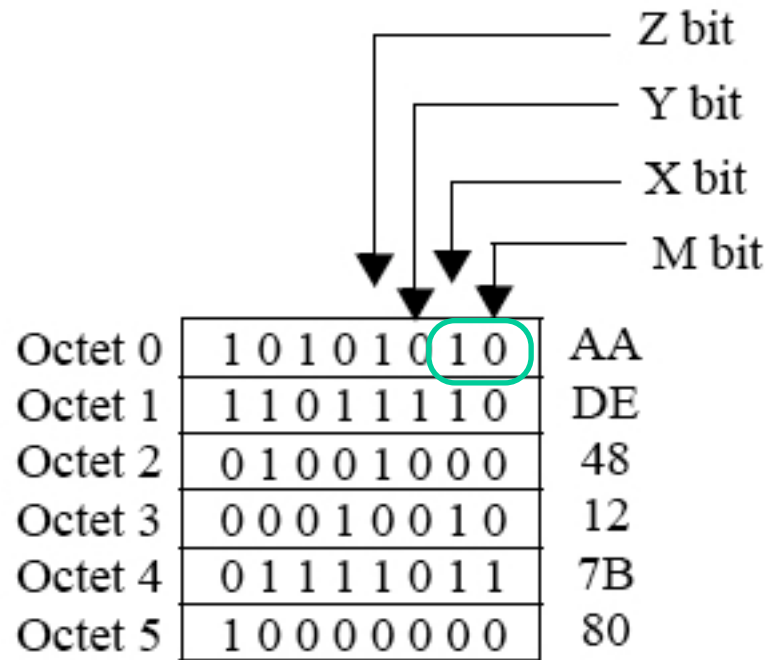
Temporary Addresses in IEEE 802

- IEEE 802 MAC address space is half global, half local
 - Global: EUI-48 based on OUI-48; typically permanent
 - Local: typically temporary
- Temporary addresses can serve many different purposes
 - Examples from other technologies are included herein
- Temporary addresses may be useful in 802.11
- Vital to ensure that the address types are distinguishable
- Foundation of distinguishable local addresses is established in IEEE Std 802 (per 802c-2017 amendment)

IEEE Std 802c: Key Facts

- IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture – Amendment 2: Local Medium Access Control (MAC) Address Usage [2]
- Standard approved: 2017-06-15; published 2017-08-25
 - 802.1 [Local Address Study Group](#), Nov 2014 - July 2015
 - PAR Authorized: 2015-06-11
- Scope in brief:
 - *provide an optional local MAC address space structure to allow multiple administrations to coexist*
 - *designate a range of local MAC addresses for protocols using a Company ID (CID) assigned by the IEEE Registration Authority*
 - *range of local MAC addresses will be designated for assignment by local administrators*
 - *range of local MAC addresses for use by IEEE 802 protocols*

Local Address: Example



- M bit (I/G bit): as before, 1 for multicast
- X bit (U/L) bit: as before, 1 for local
 - Y and Z bits: new designations

SLAP

- *Structured Local Address Plan (SLAP): An optional standardized specification for the use of local medium access control (MAC) address space entailing the use of*
 - *Extended Local Identifier (ELI),*
 - *Standard Assigned Identifier (SAI), and*
 - *Administratively Assigned Identifier (AAI)**addresses in specific disjoint ranges.*

Assignment Protocols

- *An address assignment protocol assigning local MAC addresses to devices on a LAN should ensure uniqueness of those addresses.*
- *When multiple address assignment protocols operate on a LAN without centralized administration, address duplication is possible, even if each protocol alone is designed to avoid duplication, unless such protocols assign addresses from disjoint address pools.*
- *Administrators who deploy multiple protocols on a LAN in accordance with the SLAP will enable the unique assignment of local MAC addresses within the LAN as long as each protocol maintains unique assignments within its own address subspace.*

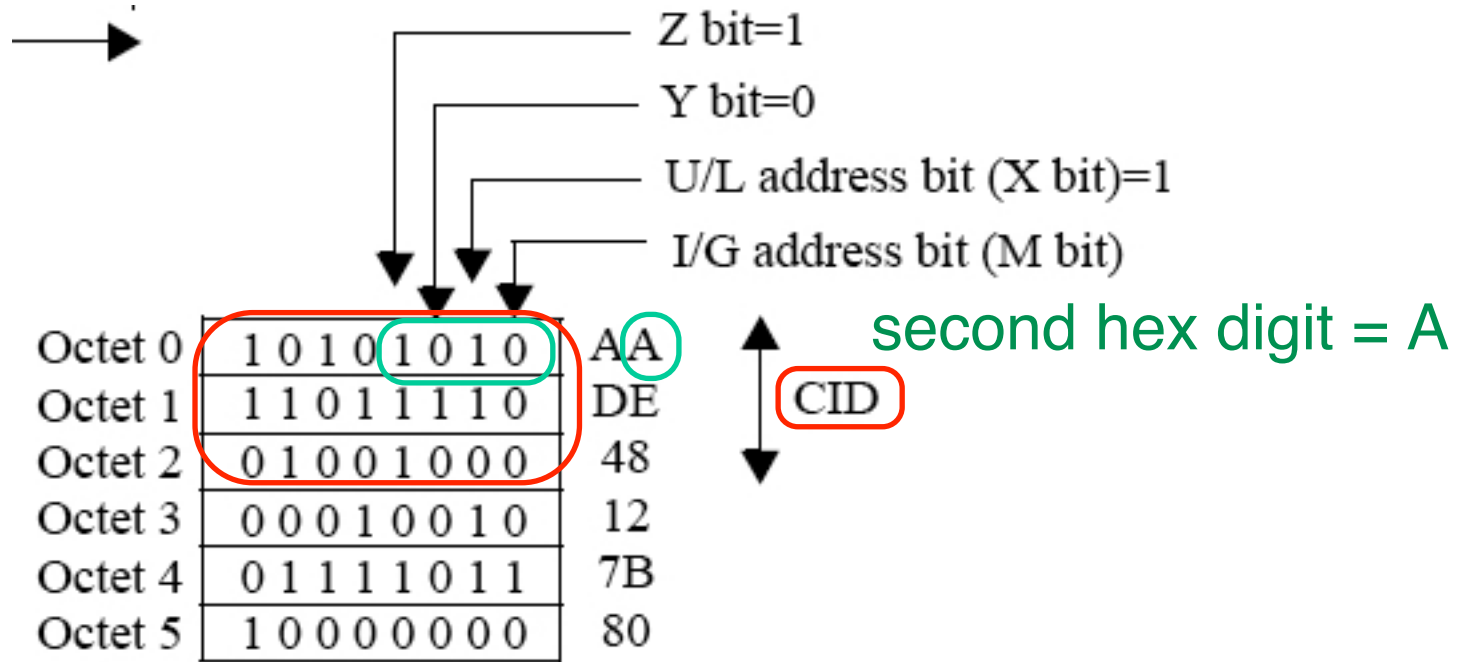
SLAP Quadrants

SLAP quadrant	Y bit	Z bit	ZYXM	second hex digit	SLAP local identifier type	SLAP local identifier
01	0	1	1010	A	Extended Local	ELI
11	1	1	1110	E	Standard Assigned	SAI
00	0	0	0010	2	Administratively Assigned	AAI
10	1	0	0110	6	<i>Reserved</i>	<i>Reserved</i>

“A” for AAI and “E” for ELI would have been nice, but prior IEEE RA assignments put ELI in the “A” quadrant.

	Y = 0	Y = 1
Z = 0	AAI	<i>Reserved</i>
Z = 1	ELI	SAI

ELI: Extended Local Identifier



- like an EUI, but with a Company ID (CID) instead of an OUI
 - CID has X = 1 (local space).
- IEEE Registration Authority (RA) assigns CIDs, all in SLAP 01
 - CID predates 802c
- 802c reserves 4 CIDs for the local administrator

AAI: Administratively Assigned Identifier

- AAI: Administratively Assigned Identifier
 - second hex digit = 2
 - *Administrators who wish to assign local MAC addresses in an arbitrary fashion (for example, randomly) and yet maintain compatibility with other assignment protocols operating under the SLAP on the same LAN may assign a local MAC address as AAI.*
- Reserved quadrant can be used like AAI, with reservations:
 - second hex digit = 6
 - *may be administratively used and assigned in accordance with the considerations specified for AAI usage, without effect on SLAP assignments. However, administrators should be cognizant of possible future specifications... that would render administrative assignment incompatible with the SLAP.*

SAI: Standard Assigned Identifier

- second hex digit = E
- *Specification of the use of the SAI quadrant for SLAP address assignments is reserved for the standard forthcoming from IEEE P802.1CQ.*
- *An SAI is assigned by a protocol specified in an IEEE 802 standard.*
- *Multiple protocols for assigning SAI may be specified within various IEEE 802 standards. Coexistence of such protocols may be supported by restricting each to assignments within a subspace of SAI space.*
- *In some cases, an SAI assignment protocol may assign the SAI to convey specific information. Such information may be interpreted by receivers and bridges that recognize the specific SAI assignment protocol, as identified by the subspace of the SAI. The functionality of receivers and bridges that do not recognize the protocol is not affected.*

P802.1CQ

- IEEE (Draft) Standard for Local and Metropolitan Area Networks: Multicast and Local Address Assignment
- PAR authorized: 2016-02-05
- *Scope: This standard specifies protocols, procedures, and management objects for locally-unique assignment of 48-bit and 64-bit addresses in IEEE 802 networks. Peer-to-peer address claiming and address server capabilities are specified.*
- *Need: Currently, global addresses are assigned to most IEEE 802 end station and bridge ports. Increasing use of virtual machines and Internet of Things (IoT) devices could exhaust the global address space. To provide a usable alternative to global addresses for such devices, this project will define a set of protocols that will allow ports to automatically obtain a locally-unique address in a range from a portion of the local address space. Multicast flows also need addresses to identify the flows. They will benefit from a set of protocols to distribute multicast addresses. Peer-to-peer address claiming and address server capabilities will be included to serve the needs of smaller (e.g. home) and larger (e.g. industrial plants and building control) networks.*
- See update [3]

Address Block Sizes (48-bit addresses)

second hex digit	address type	Admin	Block Size	Subdivision	Subdivision Block Size
..00 (0,4,8,C)	EUI-48	IEEE RA	$2^{46} \approx 7.0 \cdot 10^{13}$	MA-L (OUI)	$2^{24} \approx 1.7 \cdot 10^7$
				MA-M	$2^{20} \approx 1.0 \cdot 10^6$
				MA-S	$2^{12} \approx 4.1 \cdot 10^3$
..01 (2,6,A,E)	all local unicast		$2^{46} \approx 7.0 \cdot 10^{13}$		
1010 (A)	ELI	IEEE RA	$2^{44} \approx 1.8 \cdot 10^{13}$	CID	$2^{24} \approx 1.7 \cdot 10^7$
1110 (E)	SAI	IEEE 802	$2^{44} \approx 1.8 \cdot 10^{13}$		
0010 (2)	AAI		$2^{44} \approx 1.8 \cdot 10^{13}$		
0110 (6)	<i>Reserved</i>		$2^{44} \approx 1.8 \cdot 10^{13}$		

- How many is 2^{46} ?
 - IEEE manages EUI-48 space to support unique identification of hardware anywhere in the world for 100 years.
 - The SLAP gives IEEE 802 a space one quarter of that size to exploit for a LAN!

SLAP Happy

- The SLAP offers:
 - organizations a block of $\sim 17\text{M}$ addresses for innovative ELI uses
 - IEEE 802 a block of $\sim 1.8 * 10^{13}$ addresses for innovative SAI uses
 - administrators a block of $\sim 1.8 * 10^{13}$ addresses to do what they want while avoiding collision with ELI and SAI users
- The SAI block is a huge opportunity for IEEE 802!
- Let's use it!

IEEE RA Tutorial – Guidelines for Use of EUI, OUI, CID

- IEEE Registration Authority assigns OUIs, CIDs, etc.
- Provides tutorials on identifiers and policies:
 - <http://standards.ieee.org/develop/regauth/tut>
- Tutorial on EUI (referenced in IEEE Std 802) [4]:
- *Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI), and Company ID (CID)*
 - Published August 2017, in coordination with 802c

Temporary Addresses in 802.11

- Temporary addresses were introduced with 802.11aq (Pre-Association Discovery)
 - **12.2.10 Requirements for support of MAC privacy enhancements**
 - *MAC privacy enhancements are enabled on a non-AP STA when dot11MACPrivacyActivated is set to true. The STA shall periodically change its MAC address to a random value while not associated to a BSS. The STA shall construct the randomized MAC address from the locally administered address space as defined in IEEE Std 802[®]-2014 and IEEE Std 802c[™]-2017...*
- Many comments were received on limiting randomization to less than the entire local address space, to leave room for other address types and algorithms.
- 802.11 RCM TIG is considering the limitations of purely random addresses, including needs to identify sender identity from source addresses [5].
- Currently, in P802.11REVmd ballot, comment resolution has led to a proposal to allow a network to advertise its address policy [6].
 - Network can restrict self-selected addresses to a subset of address space based on a specified address prefix.
 - Provides for future support of addresses allocated per P802.1CQ

Proposed MAC Address Policy ANQP [6]

Table 9-820a – MAC Address Policy field bits

Bitmap value	Description
Bit 0 (MSB)	EUI-48 supported
Bit 1	ELI-48 supported
Bit 2	SAI-48 supported
Bit 3	Address server assignment supported
Bit 4	Self-assignment using specified MAC address prefix supported
Bit 5	Preconfigured administered address supported
Bit 6	Reserved
Bit 7	Reserved

Some Address Features

- Uniqueness
 - most fundamental property
 - local (on the LAN), or universal
 - relevant to identity
- Permanence/Longevity
 - relevant to trackability
 - relevant to management
- Structure and Information content
 - Does the address convey information beyond identity?
 - Can address convey location (e.g., IP)
 - other possibilities

Some Address Assignment Protocols

- Stateful (per IETF)
 - typically server-based (e.g. DHCP)
 - Stateless (per IETF)
 - IPv6 “Stateless Address Autoconfiguration” (SLAAC)
 - could be based on IEEE EUI
 - requires Duplicate Address Detection (DAD)
 - claiming
 - device claims an address by announcement, but:
 - may probe first for addresses in use
 - may check afterwards for collisions
- P802.1CQ PAR mentions “peer-to-peer address claiming and address server capabilities”

Example: Bluetooth Link-Layer Privacy [7]

- Public Device Address (PDA) is a permanent (global) EUI-48
- Identity Resolving Key (IRK): shared secret (exchanged during pairing)
 - bound to a fixed identifier (e.g, PDA) by both devices
 - can be specific to the pair
- sender chooses a random 22-bit prand
 - sender calculates a hash based on prand and IRK
 - Source Address is Resolvable Private Address (RPA) of prand and hash
 - receiver calculates hash from prand for each stored IRK
 - receiver finds a match and caches result
 - receiver can identify the source; those without IRK cannot
- prerequisite: receiver can distinguish RPA from PDA

local bit \Leftrightarrow RPA



Example: IPv4

- IPv4 address can be globally routable
- IPv4 address can be local
- IPv4 address is hierarchical, with two components:
 - prefix: identifies network or subnet
 - host identifier: identifies interface
 - hierarchy provides for routing by network, not by address
 - 802.11 local addressing could support this approach
 - e.g. prefix could identify the associated AP

View from IETF: IPv6

- IPv6 unicast address (128 bits) includes:
 - subnet prefix (n bits, typically 64)
 - interface ID (IID) (128- n bits, typically 64)
 - used to identify interfaces on a link
 - formerly encouraged creation from IEEE EUI (e.g. RFC 4291)
 - RFC 7136: *various new forms of IIDs have been defined: including temporary addresses [RFC4941], Cryptographically Generated Addresses (CGAs) [RFC3972] [RFC4982], Hash-Based Addresses (HBAs) [RFC5535] ...*

IETF: Temporary Addresses

- SLAAC = “Stateless Address Autoconfiguration”
- RFC 4941: Privacy Extensions for SLAAC in IPv6
 - Sept. 2007
 - *...for interfaces whose interface identifier is derived from an IEEE identifier. Use of the extension causes nodes to generate global scope addresses from interface identifiers that change over time, even in cases where the interface contains an embedded IEEE identifier. Changing the interface identifier (and the global scope addresses generated from it) over time makes it more difficult for eavesdroppers and other information collectors to identify when different addresses used in different transactions actually correspond to the same node.*

Semantically Opaque Interface Identifiers

- RFC 7217
 - Apr. 2014
 - *temporary addresses can be challenging.... from a network-management point of view, they tend to increase the complexity of event logging, troubleshooting, enforcement of access controls, and quality of service.... some organizations disable the use of temporary addresses even at the expense of reduced privacy... may also result in increased implementation complexity*
 - *...Interface Identifier changes when the host moves from one network to another. This method is meant to be an alternative to generating Interface Identifiers based on hardware addresses (e.g., IEEE LAN Media Access Control (MAC) addresses), such that the benefits of stable addresses can be achieved without sacrificing the security and privacy of users.*

IETF CGA

- CGA = “Cryptographically Generated Address”
- RFC 3972
 - March 2005
 - *interface identifier is generated by computing a cryptographic one-way hash function from a public key and auxiliary parameters. The binding between the public key and the address can be verified by re-computing the hash value and by comparing the hash with the interface identifier. Messages sent from an IPv6 address can be protected by attaching the public key and auxiliary parameters and by signing the message with the corresponding private key. The protection works without a certification authority or any security infrastructure.*
 - includes collision count field based on duplicate address detection

Example: Authentication and Privacy can coexist

- On a LAN, some devices strive for privacy
 - may use a randomized address
- On a LAN, some devices may not value privacy but put value on other features, such as verification
 - example: access points should be easily found
 - address may be structured
- Both types of devices should be able to coexist
 - random addresses should stay out of assigned space
 - receiver can then determine the type of address and respond accordingly

Summary

- The local address space is huge and valuable.
- The IEEE RA's CID give companies a chance to innovate
 - SLAP supports ELIs based on CID
 - 802 standards should not step on any company's ELIs
- SLAP specifies an AAI quadrant
 - Good place for randomization
- SLAP specifies a reserved quadrant
 - 802 standards should not step on it
- SLAP offers a 44 bit SAI quadrant to IEEE 802 to exploit.
 - 802 standards should put SAI to use in an orderly fashion.
 - Can implement versions of ideas from other technologies.
- Let's ensure protocol coexistence for best success!

References (1/2)

- [1] R. Marks, “Local MAC Addresses in the Overview and Architecture based on IEEE Std 802c,” 2017-09-13 (IEEE 802.11-17/1466r01)
- [2] IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture – Amendment 2: Local Medium Access Control (MAC) Address Usage (2017-06-15)
- [3] M. Riegel, “P802.1CQ MAC Address Assignment Requirements,” 2019-05-12 (IEEE 802.11-19/0851r00)
- [4] “Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI), and Company ID (CID),” IEEE Registration Authority (2017-08)
<http://standards.ieee.org/develop/regauth/tut>

References (2/2)

- [5] A. Andersdotter, “Summary of discussions on randomized and changing MAC addresses 2014-2019,” 2019-05-13 (IEEE 802.11-19/0623r3)
- [6] R. Marks, A. de la Oliva, S. McCann, and M. Hamilton, “MAC Address Policy ANQP,” 2019-05-13 (IEEE 802.11-19/0286r6)
- [7] S. Gupta and R. Kumar, “BLE v4.2: Creating Faster, More Secure, Power-Efficient Designs—Part 2,” 2016-09-27
 - <https://www.electronicdesign.com/communications/ble-v42-creating-faster-more-secure-power-efficient-designs-part-2>

Do Not Fear Random MAC Addresses!

Date: 2019-07-04

Authors:

Name	Affiliations	Address	Phone	email
Dan Harkins	HPE	3333 Scott Boulevard Santa Clara, California, United States of America	+1 408 555 1212	

Abstract

The rise of MAC randomization has been treated as if it is an outbreak of an infectious disease and discussion around it has been “*how do we respond?*”

This submission discusses the motivations of MAC randomization, why it’s a good thing, 802c applicability, and the concerns raised over MAC randomization.

Motivation For 802.11 MAC Randomization

pri·va·cy

/ˈprɪvəsē/

noun

1. the state or condition of being free from being observed or disturbed by other people.
"she returned to the privacy of her own home"
synonyms: [seclusion](#), [solitude](#), [isolation](#), freedom from disturbance, freedom from interference [More](#)



Concerns of Communications Privacy are Not New

**Use the Automatic
During the Convention**



Make the Automatic Telephone Station at the Coliseum *your* headquarters. A reception room, booths and uniformed pages at your service on the main floor of the Annex.

Let us facilitate your work—and let us demonstrate to you the *wonderful efficiency* of the Automatic telephone—

**The ONE Phone
That Gives
SECRET SERVICE**

Automatic Telephone Service is pulling the biggest popular vote in history! Local Chicago traffic has more than doubled, and long distance increased 89% since January 1, 1912.

Because of its very low cost, its instantaneous connections, its secrecy, its splendid carrying powers, the Automatic is the *only logical telephone*. By all means take advantage of this special convention service.

Local Calls 5c
Long distance calls at remarkably low rates

Illinois Telephone & Telegraph Co.
(Successor to Illinois Tunnel Co. Telephone Department)
162 W. Monroe St.

Commercial Dept. 33-111
Information 892
Long Distance Call (O) on the Dial



Privacy was an important selling point for dial phones in 1912 since they did not require the use of an operator to make the call



Privacy Concerns with 802.11

- **Passive observation of 802.11 bands reveals MAC addresses and more!**
 - STAs active probing when not connected to a network
 - Communication to connected network
 - STAs frantically searching for particular SSIDs
- **Location plus time plus frequency plus MAC address allows sensitive information to be gleaned**
 - This MAC address pops up at the AIDs clinic twice a week
 - This MAC address is near the liquor store at 8am every day
 - This MAC address leaves a certain apartment building in the early morning almost every weekend
- **Straightforward to create Personally Identifiable Information (PII) from this data**

802.11 Privacy is Not Theoretical

- **London Trashcans Silently Track Smartphones**
 - The company boasted that the cans, which included LCD advertising screens, "*provide an unparalleled insight into the past behavior of unique devices*"—and hence of the people who carry them around
- **Seattle Police Deactivate Wi-Fi Spy Grid After Outcry**
 - A DHS and Seattle police network collecting location information of Wi-Fi devices
- **Transport for London to track all Wi-Fi devices in 2019**
 - Month-long trial collected 509M pieces of information from 5.6M unique devices on 42M journeys
 - Marketed as a service to users— map delays and congestion, notify where queues are forming— but commercial applications are obvious. So are nefarious ones
 - Claim that scheme will eventually *tokenize* MAC address for privacy

Privacy and MAC Randomization

- **MAC randomization**
 - Choose a random 48-bit number, interpret it as a MAC address
 - Set the local bit, clear the broadcast bit, assign it
 - Periodically change this value
- **Simple and effective**
 - Opt-in/out schemes presume that all parties are trustworthy
 - *Garbage in, garbage out* more effective: if the data is garbage then the result of Big Data Analytics will be garbage– there will be no PII
 - Control is in the hands of the user, where it should be

How is “Client Privacy” Addressed in 802.11?

IEEE 802.11aq added a MIB variable for “privacy”

When that MIB variable is set, a STA will:

- Periodically randomize its MAC address pre-association by selecting an address out of the local address space
- Not probe for specific SSIDs
- Reset the sequence number counter used to identify MSDUs and MMPDUs when the MAC address changes
- Reseed the OFDM scrambler when the MAC address changes
- Choose a random MAC address to associate to an AP and retain that MAC address during the STA’s connection to the ESS
- Set its MAC address to a previously used (random) MAC address when it attempts to use some state on the AP bound to the previous MAC address

Some vendors are already randomizing MAC addresses

- Whether they are doing in per-802.11aq remains to be seen

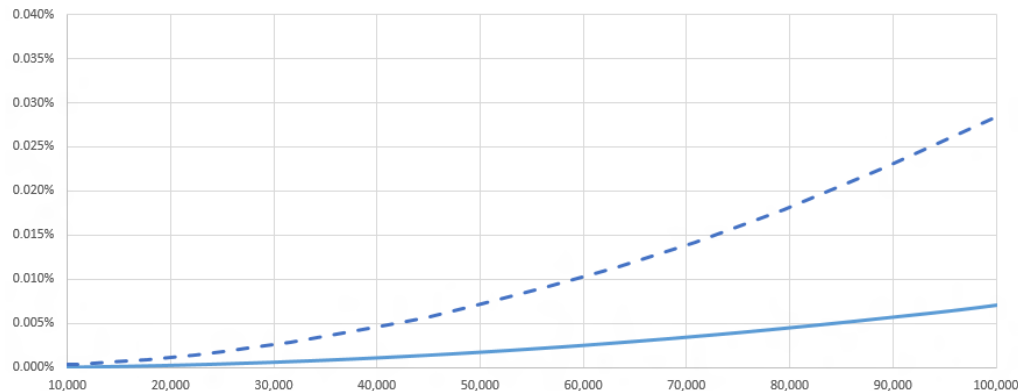
802c and MAC Randomization

802c partitioned the local address space into quadrants

- ELI– prefix is a CID, remaining octets are assigned per policy
- SAI– for use with 802.1CQ
- AAI– administrator has some arbitrary local policy and wishes to not conflict with ELI– or SAI–style addresses that may also be on his network
- Reserved

802c consumes 2 of the 46 available bits of a 48-bit MAC

- This vastly increases likelihood of MAC address collision



802c and MAC Randomization

802c does not assign local address space

- The SLAP is optional
- 802c provides a way to support multiple administrative policies in the same local address space *if the administrator so desires*, but it's still local
- Using any CID, or no CID, to construct a local address is not prohibited

802c does not restrict random MACs to a quadrant

- Randomness in the AAI is an example of a possible local policy but is clearly not the only local policy for the AAI quadrant

Randomizing with all available (46) bits of a MAC...

- ...has always been possible, is still possible, will be possible in the future
- ...is the wise thing to do in order to avoid collision

802c is a LAN administrator issue, not a user/STA issue

- Policy enforcement does not scale for 802.11 STAs in access network

802c is Not Useful for an 802.11 Network

802c motivation was data centers and non-access networks

- Handle networking of a large number of VMs
- Identification of weirdo L2 protocols on a data center network

Privacy Issues of 802.11 are aimed at network connectivity

- Planes, trains, automobiles...shopping malls, bars, restaurants...
enterprise, home, office... it's all the same: *get on the 'net*
- A network that accepts all comers cannot presume to have instilled sufficient local address policy knowledge on each and every client
- Privacy concerns are lessened if local policy has been provisioned already
- No historical concerns about local address usage in these sorts of access networks, no reason to believe that would change going forward
- MAC address is only significant on local LAN segment, once it gets to a router the MAC address of the STA is irrelevant

802c is unlikely to ever be used in an 802.11 network

WBA Liasion

Raised issues that were perceived to be problems associated with randomization of 802.11 MAC addresses

- Some were unserious or overblown: different MAC address used with same Passpoint Profile, Pay-per-use services are associated with MAC addresses, complimentary service offerings can be abused by changing MAC addresses, blacklisting by MAC address will no longer be effective, lawful intercept issues, etc
- Some point to changes that will be necessary: band-steering will be difficult if different MACs are used on different bands, helpdesks that have come to rely on fixed MAC addresses will have issues

None of the issues raised compel a loss of privacy by users

MAC addresses are being randomized, that trend will grow

- Important to ensure they do it the 11aq way

Summary

- **802.11 MAC randomization is not the networking equivalent of Ebola**
- **There are valid reasons to for users to randomize their 802.11 MAC address**
- **Randomization is not illegal, nor is it prevented or limited by any other 802 standards**
- **Randomization will not create chaos in networks**
 - It is a disruptive technology, but disruption can be good
 - Better ways of tracking and accounting for users will be employed– e.g. authenticated identities
 - Better security will be provided for network service offerings by not assuming a fixed global MAC address

References

- **IEEE 802.11-13/1448r1**
 - Paul Lambert’s original proposal on MAC randomization for privacy
- **IEEE 802.11-14/0430r2**
- **IEEE 802c**
- **Draft P802.11REVmd_D2.0**
- **IEEE 802.11-18/1579r1**

The pitfalls of address randomization in wireless networks

Date: 2019-07-17

Authors:

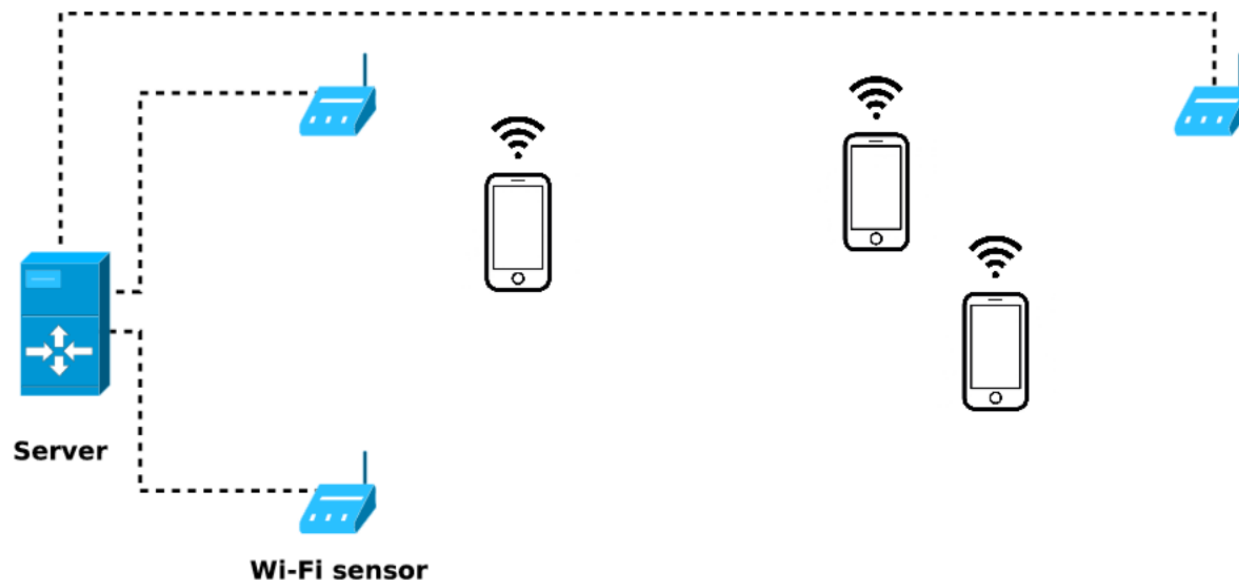
Name	Affiliation	Contact
Mathieu Cunche	Univ. Lyon, INSA Lyon, Inria, CITI	mathieu.cunche@insa-lyon.fr

Abstract

Address randomization has been adopted by vendors as a technique to protect users against passive tracking. This anti-tracking mechanism can be undermined by some elements of transmitted frames. Those issues should be carefully considered by developers.

Tracking people using radio signals

- Set of sensors capturing identifiers found in frames
- User detection and tracking



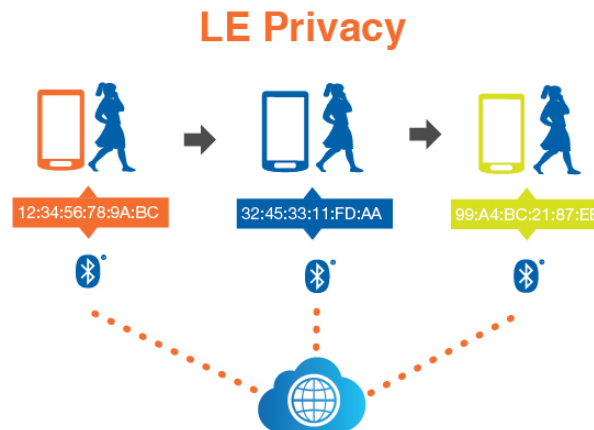
Discovery protocols in wireless networks

Discovery frames: probe requests / advertising packets



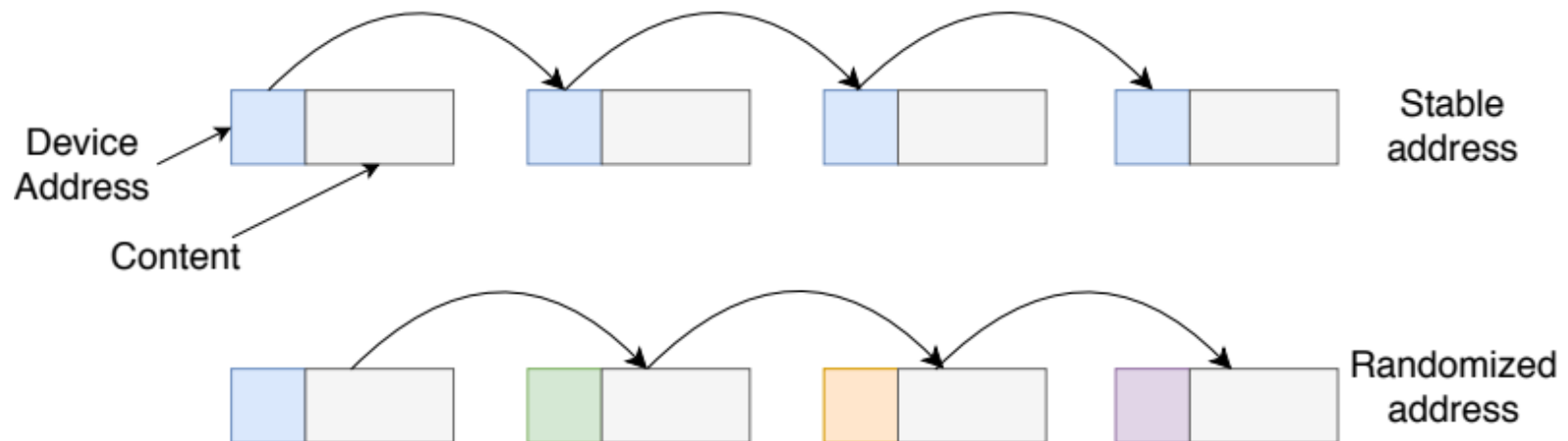
Address randomization

- **Adoption of address randomization**
 - **Random WiFi addresses implemented in major systems (iOS, Android, Windows, GNU/Linux)**
 - **Random BLE addresses since version 4.2 of Bluetooth**



Model

- **Attacker model:**
 - **Capabilities: Monitor the wireless channel(s)**
 - **Objective: track a device over time by linking frames**



Secondary Stable Identifiers

- **Secondary stable identifiers: several byte-long fields whose value is constant across frames**



Secondary Stable Identifiers

- **WPS UUID in Wi-Fi frames**
 - **A 128 bits UUID derived from the MAC address**

- Wifi Protected Setup State: Configured (0x02)
- Response Type: AP (0x03)
- ▾ UUID E

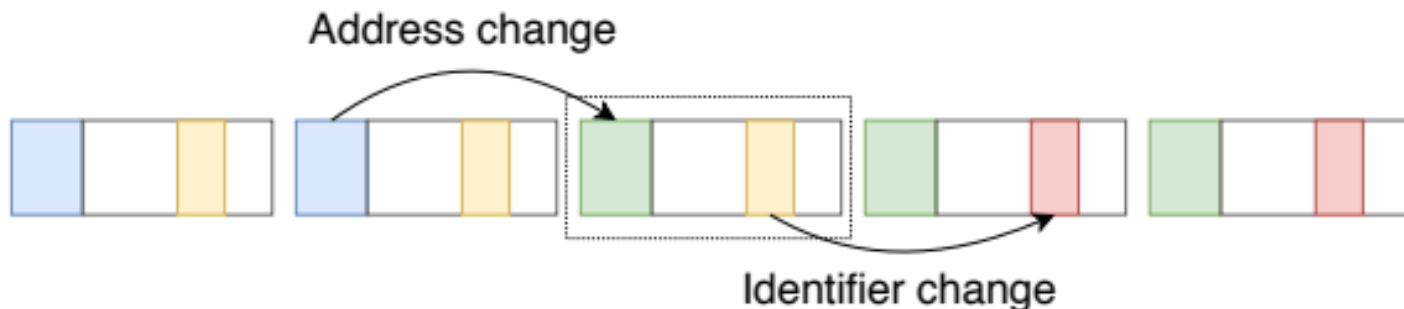
Data Element Type: UUID E (0x1047)

Data Element Length: 16

UUID Enrollee: 63041ba

Synchronization issues

- **All identifiers must be rotated together with the device address**
 - **Those change must be synchronized ...**
 - **Otherwise the identifier can be used to trivially link two consecutive addresses**



Synchronization issues

- **Ex.: Bad synchronization of *Nearby Id* in Apple Handoff (BLE)**

Time (s)	BD_ADDR	Apple Handoff Data		
		Cnt	Data	Nearby Id
899.885	43:26:33:d5:78:61	-	-	10050b1060c708
899.990	43:26:33:d5:78:61	-	-	10050b1060c708
900.091	6d:01:ff:0a:52:84	-	-	10050b1060c708
900.203	6d:01:ff:0a:52:84	-	-	10050b109d88fb
900.354	6d:01:ff:0a:52:84	-	-	10050b109d88fb

Predictable fields

- **Predictable field: a fields whose value can be computed from the previous occurrences(s)**



Predictable fields

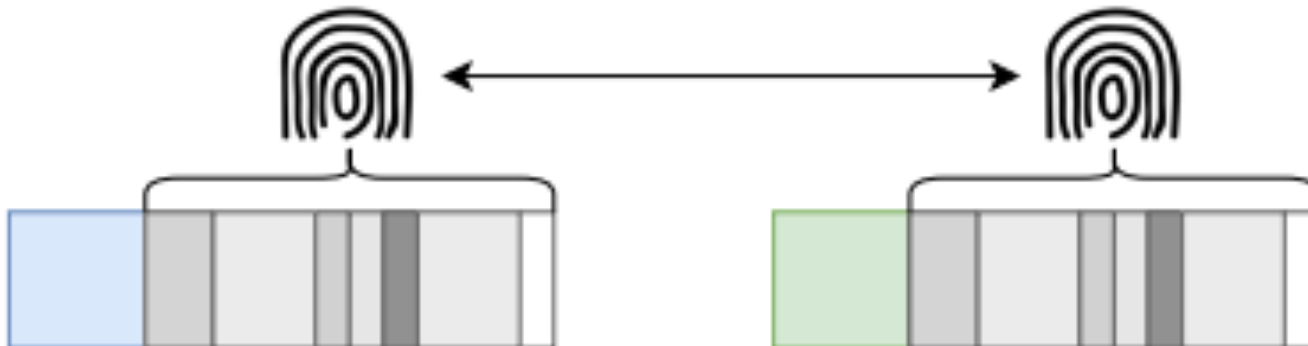
- **Ex.: sequence number field in early implementations of address randomization**

324	2.922240000	2a:21:fd:74:38:aa	Broadcast	Probe Request, SN=1035	SSID=Broadcast
328	2.923264000	2a:21:fd:74:38:aa	Broadcast	Probe Request, SN=1034	SSID=Broadcast
331	2.923264000	2a:21:fd:74:38:aa	Broadcast	Probe Request, SN=1035	SSID=Broadcast
338	2.995396000	2a:21:fd:74:38:aa	Broadcast	Probe Request, SN=1039	SSID=Broadcast
538	4.896581000	Apple_74:16:d4	Broadcast	Probe Request, SN=1040	SSID=Broadcast
539	4.896585000	Apple_74:16:d4	Broadcast	Probe Request, SN=1042	SSID=Broadcast
541	4.915017000	Apple_74:16:d4	Broadcast	Probe Request, SN=1043	SSID=Broadcast

Figure 7: Illustration of randomized iOS 8.1.3 MAC addresses.

Content based fingerprinting

- **Fingerprint: set of stable fields that can be used to identify a device**



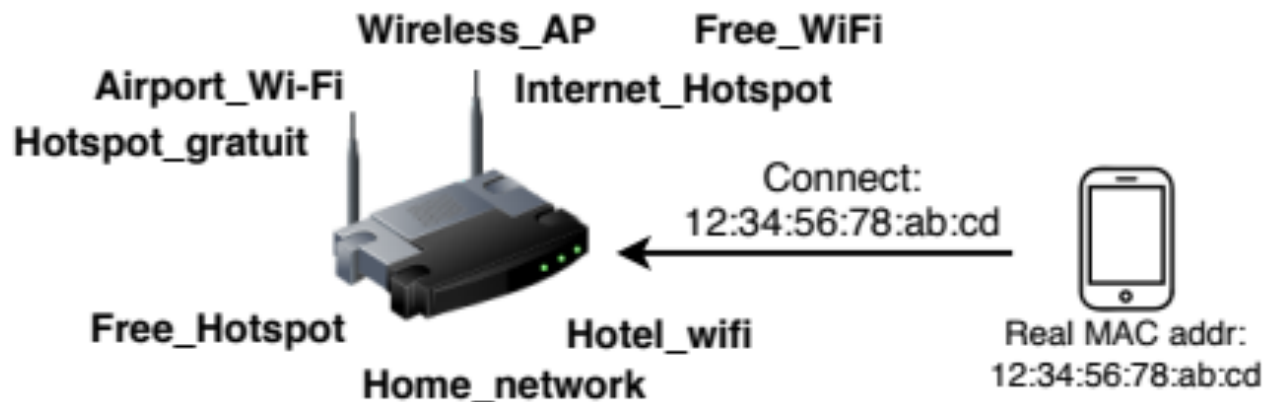
Content based fingerprinting

- **Ex.: Wi-Fi information elements in probe requests**

```
▼Tag: HT Capabilities (802.11n D1.10)
  Tag Number: HT Capabilities (802.11n D1.10) (45)
  Tag length: 26
  ▼HT Capabilities Info: 0x100c
    .... ..0 = HT LDPC coding capability: Transmitter does not support receiving LDPC coded packets
    .... ..0. = HT Support channel width: Transmitter only supports 20MHz operation
    .... ..11.. = HT SM Power Save: SM Power Save disabled (0x0003)
    .... ..0 .... = HT Green Field: Transmitter is not able to receive PPDU with Green Field (GF) preamble
    .... ..0. .... = HT Short GI for 20MHz: Not supported
    .... ..0.. .... = HT Short GI for 40MHz: Not supported
    .... ..0... .... = HT Tx STBC: Not supported
    .... ..00 .... = HT Rx STBC: No Rx STBC support (0x0000)
    .... ..0.. .... = HT Delayed Block ACK: Transmitter does not support HT-Delayed BlockAck
    .... ..0... .... = HT Max A-MSDU length: 3839 bytes
    .... ..1 .... = HT DSSS/CCK mode in 40MHz: Will/Can use DSSS/CCK in 40 MHz
    .... ..0. .... = HT PSMP Support: Won't/Can't support PSMP operation
    .... ..0.. .... = HT Forty MHz Intolerant: Use of 40 MHz transmissions unrestricted/allowed
    .... ..0... .... = HT L-SIG TXOP Protection support: Not supported
  ▼A-MPDU Parameters: 0x19
    .... ..01 = Maximum Rx A-MPDU Length: 0x01 (16383[Bytes])
    .... ..1 10.. = MPDU Density: 8 [usec] (0x06)
    .... ..000. .... = Reserved: 0x00
  ▶Rx Supported Modulation and Coding Scheme Set: MCS Set
  ▶HT Extended Capabilities: 0x0000
  ▶Transmit Beam Forming (TxBF) Capabilities: 0x0000
  ▶Antenna Selection (ASEL) Capabilities: 0x00
```

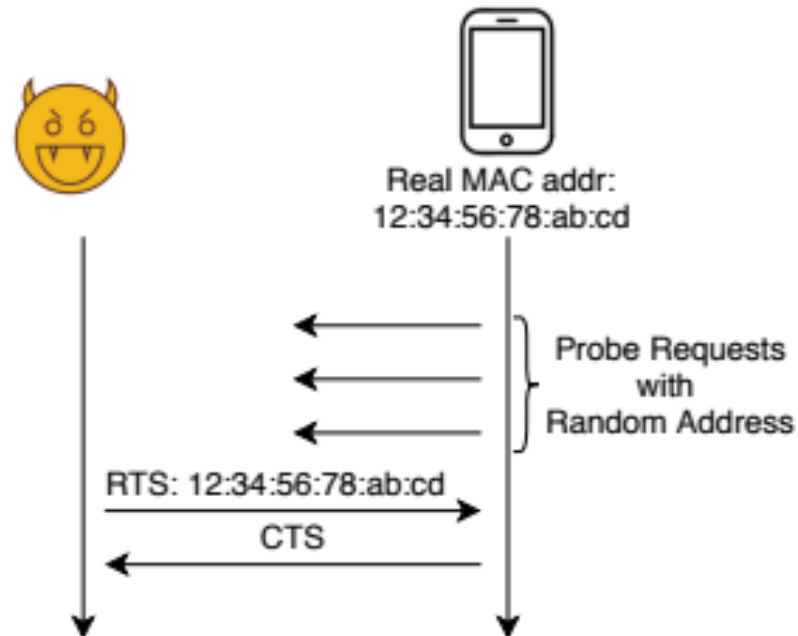

Active attacks

- **Attacker allowed to capture, replay, forge frames**
- **Ex.: Revisited Karma Attack**
 - **Attack: set up Karma AP and wait for devices to reveal their MAC addr**



Active attacks

- **Ex.: Send control frame attacks**
 - **Send RTS frame to the target real MAC addr; it will respond if in range**



Technical countermeasures

- **Identifiers**
 - **Remove them or rotate them with device address**
- **Predictable fields**
 - **Reset to random value when rotating device address**
- **Content-based fingerprinting**
 - **Reduce content to bare minimum**
- **Timing-based fingerprinting**
 - **Introduce randomness in timings**
- **Replay attacks**
 - **Timestamps and authentication**

Lessons learned

- **Bugs: new mechanisms integrated in already complex systems**
- **Lack of specifications: no specification for address randomization in Wi-Fi**
- **Specifications:**
 - **Too much freedom given to vendors ? (Vendor specific fields)**
 - **Privacy is not always considered**
 - **Interactions with privacy and security researchers could be improved**

Manufacturer specific data

- **Manufacturer/Vendor Specific Data: fields dedicated to carry custom data**
 - Available in BLE and Wi-Fi
 - Up to 32 bytes of data for custom applications
- **Used to implement Proximity Protocols**
 - Custom protocols for close range applications
 - Google Nearby, Apple Continuity, Microsoft CDP ...
 - Activity transfer, pairing, Instant Hotspot
- **No specification/restriction on their content**
 - Source of major privacy and security issues in BLE

Conclusion

- **Address Randomization is hard**
 - **Complex protocols and a lot of freedom left to vendors**
- **Wireless networks are affected by other privacy issues**
 - **Activity inference, inventory attacks, leaks of private data ...**
- **Issues that are likely to grow ...**
 - **Growing number of connected objects using wireless communications (IoT, wearables ...)**
 - **Growing number of the applications and use cases (smarthome, health, V2X, ...)**
 - **Growing number of number of standards and protocols (LPWAN, 802.11p, Z-Wave, Zigbee, LPD433 ...)**

References

- **Julien Freudiger. “How talkative is your mobile device?: an experimental study of Wi-Fi probe requests”. In: Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks. ACM, 2015, p. 8**
- **Mathy Vanhoef et al. “Why MAC Address Randomization is Not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms”. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ASIA CCS '16. New York, NY, USA: ACM, 2016, pp. 413–424. isbn: 978-1-4503-4233-9.**
- **Jeremy Martin, Travis Mayberry, et al. “A Study of MAC Address Randomization in Mobile Devices and When it Fails”. In: Proceedings on Privacy Enhancing Technologies (Mar. 2017), pp. 268–286. (Visited on 03/10/2017)**
- **“Saving Private Addresses: An Analysis of Privacy Issues in the Bluetooth-Low-Energy Advertising Mechanism”. In: (2019). Under review and embargo due to responsible disclosure**
- **Jeremy Martin, Douglas Alpuche, et al. “Handoff All Your Privacy: A Review of Apple’s Bluetooth Low Energy Implementation”. In: arXiv:1904.10600 [cs] (Apr. 2019). arXiv: 1904.10600. url: <http://arxiv.org/abs/1904.10600>**

Privacy protection in Wi-Fi analytics systems

Date: 2019-07-17

Authors:

Name	Affiliation	Contact
Mathieu Cunche	Univ. Lyon, INSA Lyon, Inria, CITI	mathieu.cunche@insa- lyon.fr

Abstract

Systems collecting network information for analytics and tracking purposes have been used for some time. Data collected by those systems can result in privacy threats and may be conflicting with data protection regulations.

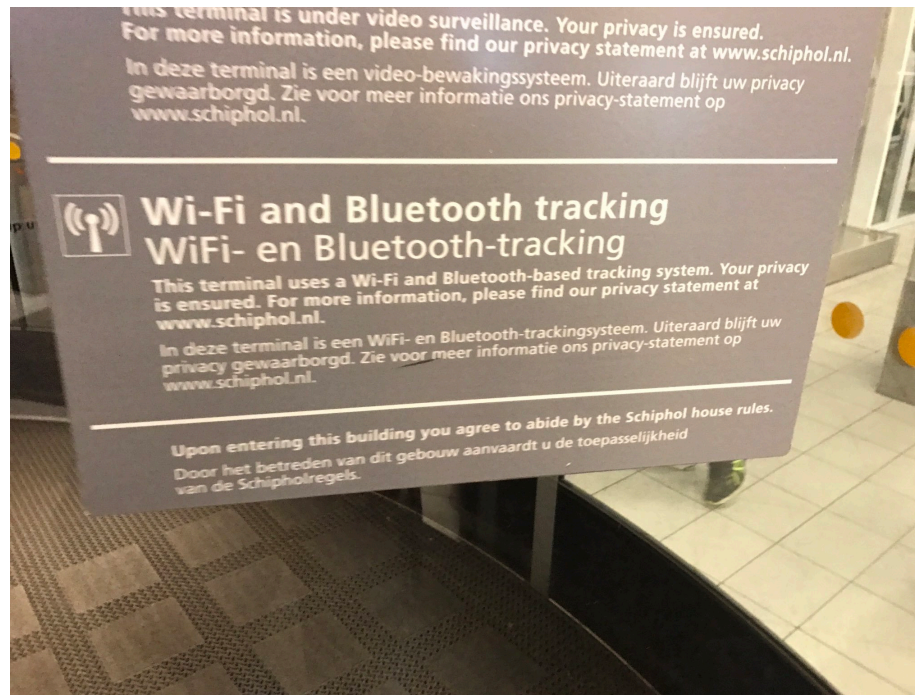
Privacy protection principles

Desirable privacy enhancing features in any data collection system

- **User information**
- **Consent & Opt-out**
- **Data anonymization**

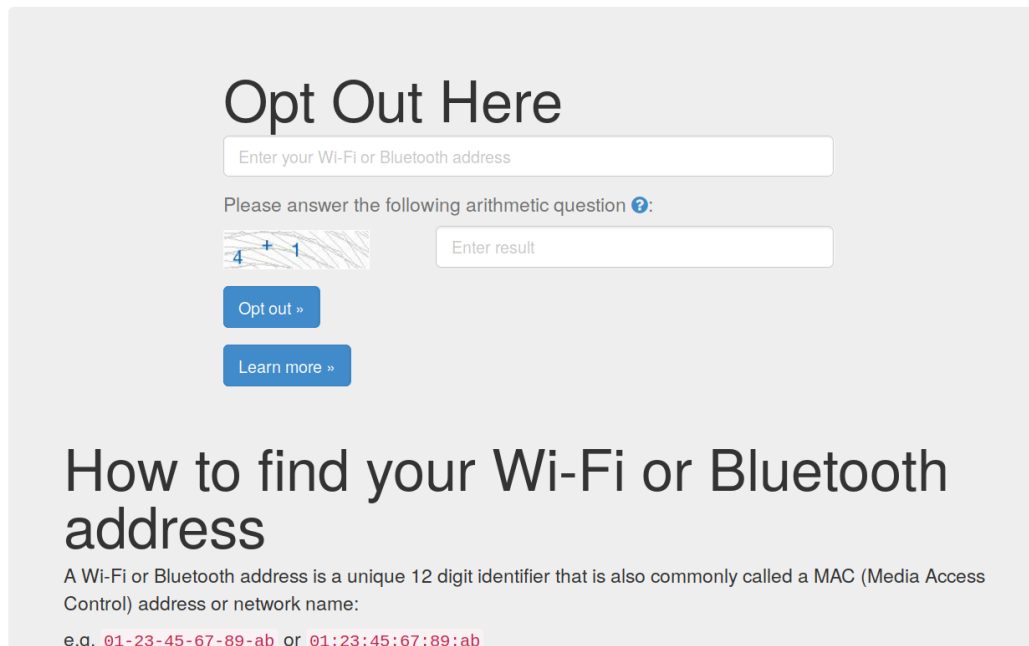
Subject Information

State of the art subject information in Wi-Fi tracking




Consent & Opt-out


- **Consent is never asked**
- **Opt-out solution may be offered (e.g. <https://optout.smart-places.org>)**



Opt Out Here

Enter your Wi-Fi or Bluetooth address

Please answer the following arithmetic question :

 Enter result

Opt out »

Learn more »

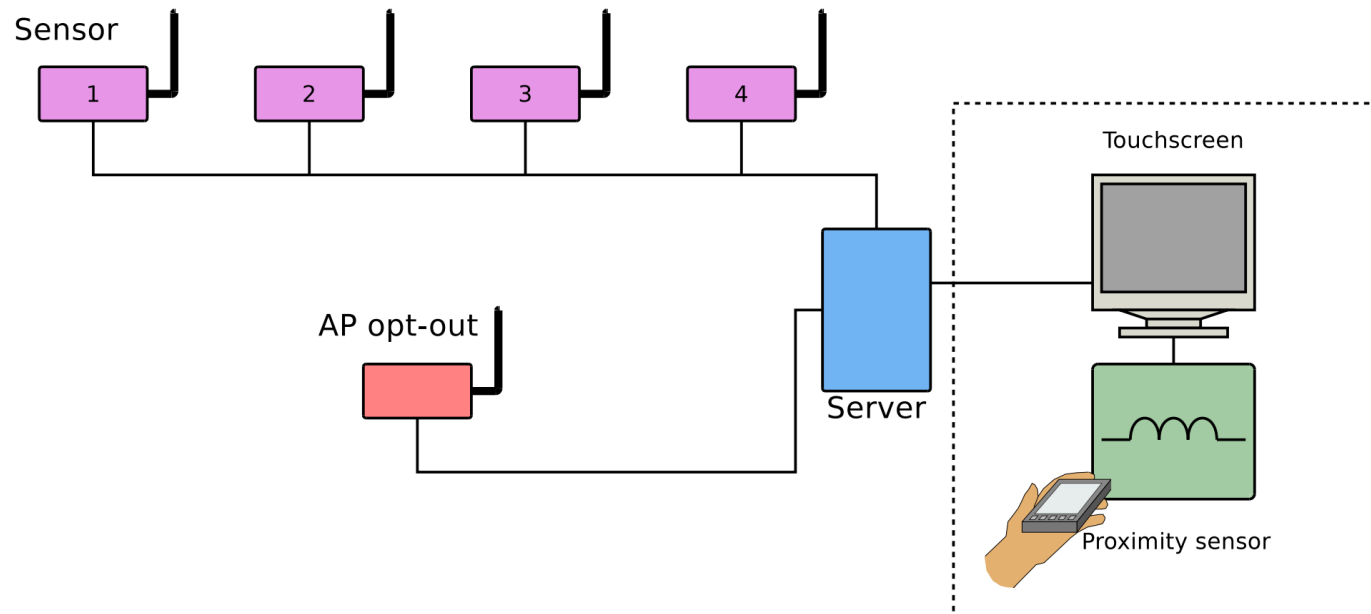
How to find your Wi-Fi or Bluetooth address

A Wi-Fi or Bluetooth address is a unique 12 digit identifier that is also commonly called a MAC (Media Access Control) address or network name:

e.g. 01-23-45-67-89-ab or 01:23:45:67:89:ab

Wombat: An experimental Wi-Fi tracking system


- **Detects Wi-Fi devices and collect mobility data**
- **Deployed as demonstrator at Cité Des Sciences et de l'Industrie (Paris) for 1 year**



Wombat: Wi-Fi based opt-out mechanism

- **Dummy AP with explicit SSID, e.g. "Wi-Fi Do not track"**
 - 1) User connect to AP to opt-out**
 - 2) MAC address of STA collected during Association process**
 - 3) MAC address added to a black-list**
 - 4) Data coming from black-listed devices is dropped**

Wombat: Wi-Fi based opt-out mechanism

ATTENTION! 

Si vous disposez d'un appareil dont le wi-fi est activé, votre parcours dans l'exposition va être automatiquement enregistré. Vous pourrez le découvrir à la table n° 24 dans l'expérience multimédia « Le wi-fi ».

Votre suivi wi-fi sera automatiquement supprimé de la base de données au bout de trois heures.

Si vous ne souhaitez pas être suivi, il vous suffit:

- de désactiver le wi-fi de votre appareil
- ou de vous connecter via le wi-fi au point d'accès « Pas de suivi wi-fi. Do not track. ».

Welcome to the exhibition
Terra Data – Our lives in the digital era.

CAUTION!

If you have equipment on which the Wi-Fi is activated, your path through the exhibition is going to be automatically recorded. You can discover it on Table No. 24 in the multimedia experiment entitled "Wi-Fi".

Your Wi-Fi track will be automatically deleted from the database after 3 hours.

If you do not wish to be tracked, you merely need to:

- deactivate the Wi-Fi on your equipment
- or log on to the "Pas de suivi wi-fi. Do not track." access point via Wi-Fi.

Benvenuto nella mostra Terra Data –
Le nostre vite nell'era del digitale.

ATTENZIONE!

Se dispone di un apparecchio con Wi-Fi attivato, il suo percorso all'interno della mostra verrà automaticamente registrato. Potrai scoprirlo al tavolo n° 24, nell'esperienza multimediale "Il Wi-Fi".

Il controllo Wi-Fi verrà automaticamente eliminato dal database dopo 3 ore.

Se non desidera essere seguito, è sufficiente:

- disattivare il Wi-Fi dell'apparecchio
- o connetterti al punto di accesso "Pas de suivi wi-fi. Do not track." via il Wi-Fi.

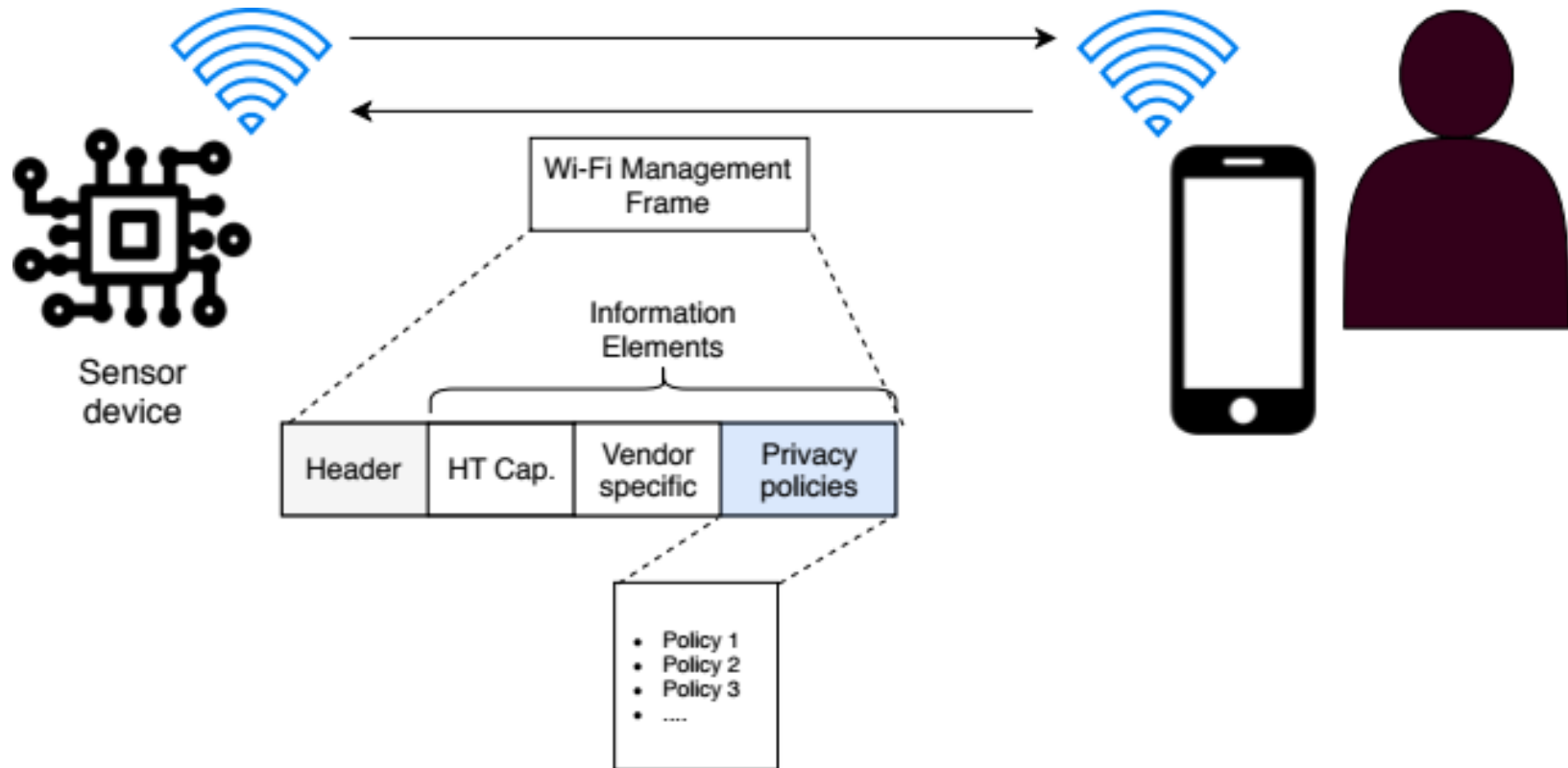
Consent in new regulations

- **Opt-out is not a valid solution under GDPR: prior consent is required**
 - **e-Privacy directive may relax this requirement**
 - 2. **The collection of information emitted by terminal equipment** to enable it to connect to another device and, or to network equipment **shall be prohibited, except if:**
 - (a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or
 - (b) **a clear and prominent notice is displayed** informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.
 - **How to to collect consent in Wi-Fi tracking context**
?

Framework for information and consent

- **Leverage discovery mechanism of wireless technologies (802.11, BLE)**
- **Tracking system broadcast information**
 - **Data collected, privacy policies, data controller coordinates ...**
 - **Data carried in Vendor/Manufacturer specific fields**
- **Subject connect to communicate consent**

Framework for information and consent

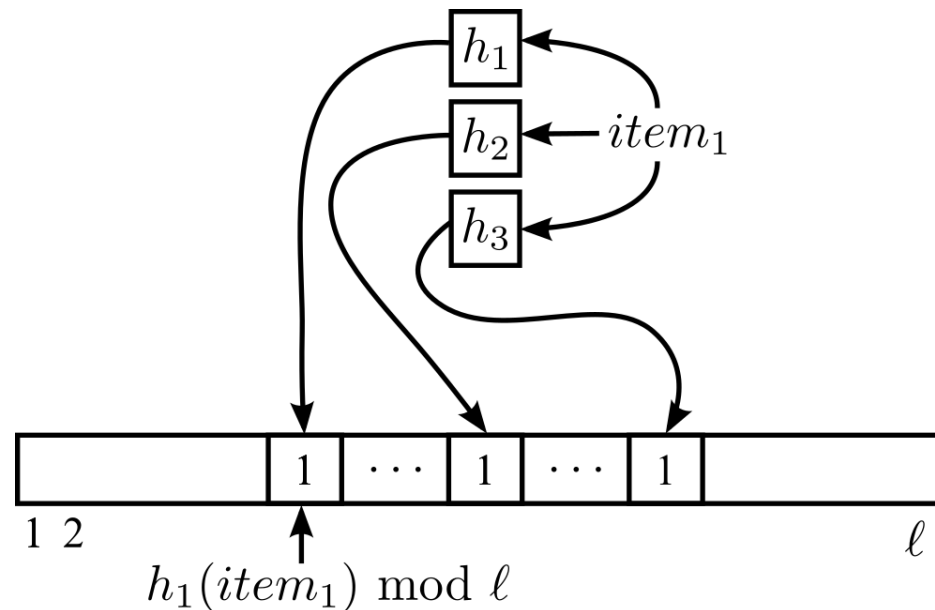


Data anonymization

- **Wi-Fi presence data ~~should~~ must be anonymized**
- **Hashing the identifiers (MAC addr.) do not work**
 - **Simple hashing can be reversed**
 - **Still considered by some as sufficient**

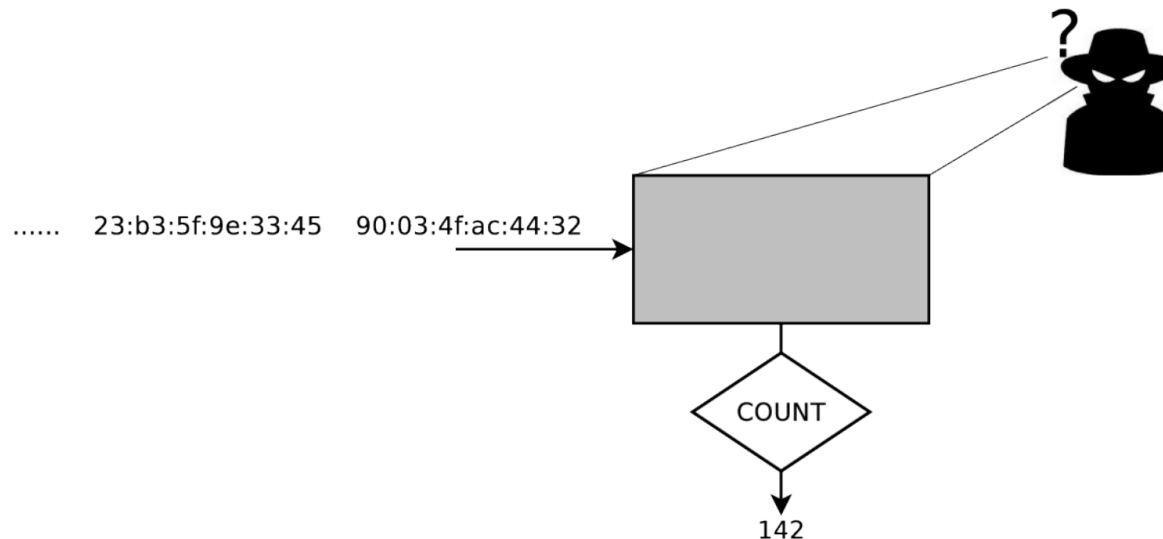
Datastructures with Differential Privacy

- **Bloom-Filter supporting cardinal estimation**
- **Perturbation to enforce Differential Privacy**



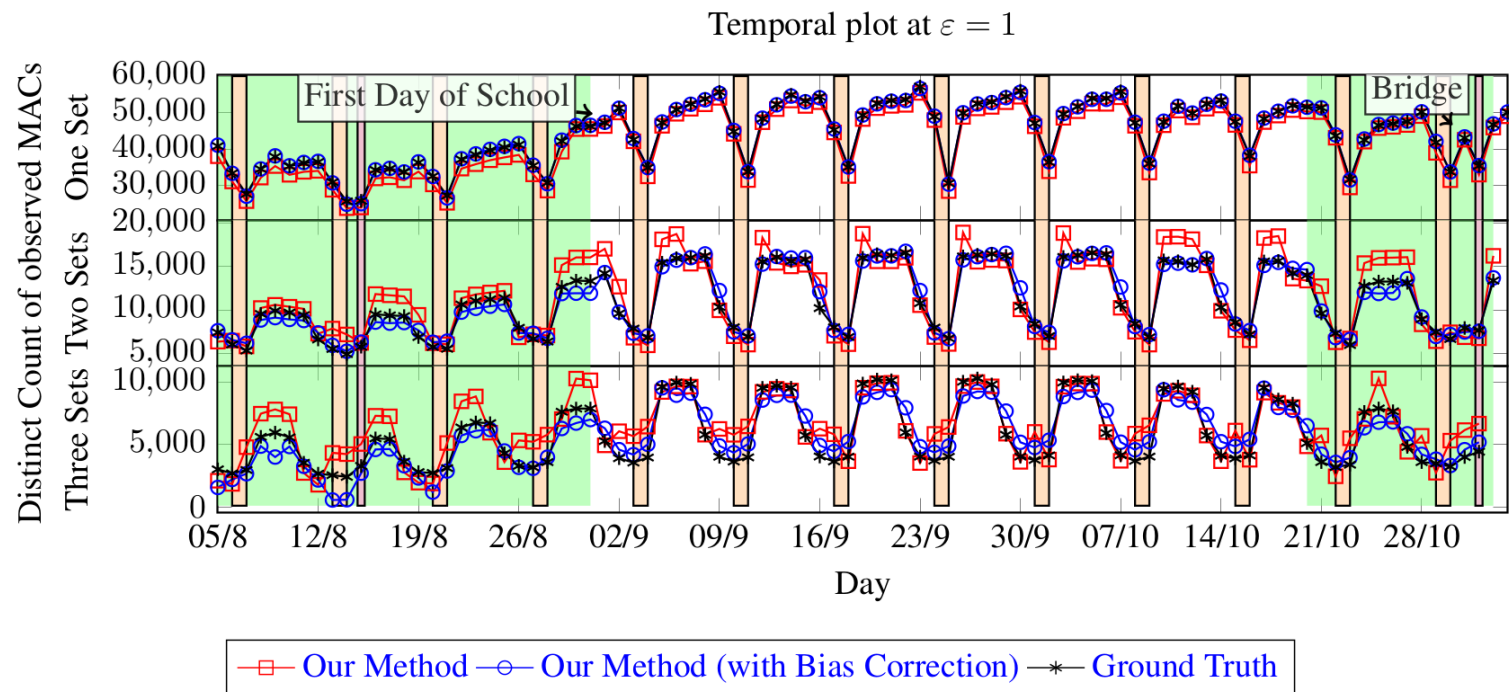
Datastructures with Differential Privacy

- **No information about single identifiers can be learned from the datastructure**
- **Estimation of the number of stored identifier is possible**



Datastructures with Differential Privacy

- Evaluation on a real world data set of MAC addr.



Datastructures with Differential Privacy

- **Strong privacy requirements (GDPR ...)**
- **May seem difficult or impossible to implement**
- **But technical solutions may be possible ...**
- **Some are currently being developed**
 - **Exception in regulations are not necessarily required (e.g. ePrivacy 8-b)**

References

- **Levent Demir, Mathieu Cunche, and Cédric Lauradoux. “Analysing the privacy policies of Wi-Fi trackers”. In: Workshop on Physical Analytics. Bretton Woods, United States: ACM, June 2014. doi: 10.1145/2611264.2611266**
- **Célestin Matte and Mathieu Cunche. “Wombat: An experimental Wi-Fi tracking system”. In: 8e édition de l’Atelier sur la Protection de la Vie Privée (APVP). Correncon, France, July 2017. url: <https://hal.inria.fr/hal-01679007>**
- **Mathieu Cunche, Daniel Le Métayer, and Victor Morel. “A Generic Information and Consent Framework for the IoT”. In: TRUSTCOM 2019 - 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. 2019. url: <https://hal.inria.fr/hal-02166181>**
- **Mohammad Alaggan, Mathieu Cunche, and Sébastien Gambs. “Privacy-preserving Wi-Fi Analytics”. en. In: Proceedings on Privacy Enhancing Technologies 2018.2 (Apr. 2018), pp. 4–26. doi: 10.1515/popets-2018-0010.**

Assignment of Temporary Addresses

Date: 2019-07-17

Authors:

Name	Affiliations	Address	Phone	email
Roger Marks	EthAirNet Associates	Denver, CO, USA	1-802-capable	roger@ethair.net

Abstract

This contribution provides views on the assignment of temporary addresses in IEEE 802.11. It is intended for the information and consideration of the IEEE 802 RCM TIG. This contribution is a followup to “Temporary Addresses” 2019-05-13 (IEEE 802.11-19-0884r00)

Temporary Addresses in IEEE 802

- IEEE 802 MAC address space is half global, half local
 - Global: EUI-48 based on OUI-48; typically permanent
 - Local: typically temporary
- Temporary addresses can serve many different purposes
- Temporary addresses may be useful in 802.11
- Vital to ensure that the address types are distinguishable
- Foundation of distinguishable local addresses is established in IEEE Std 802 (per 802c-2017 amendment)

Assignment Protocols, per IEEE Std 802

- *An address assignment protocol assigning local MAC addresses to devices on a LAN should ensure uniqueness of those addresses.*
- *When multiple address assignment protocols operate on a LAN without centralized administration, address duplication is possible, even if each protocol alone is designed to avoid duplication, unless such protocols assign addresses from disjoint address pools.*
- *Administrators who deploy multiple protocols on a LAN in accordance with the SLAP will enable the unique assignment of local MAC addresses within the LAN as long as each protocol maintains unique assignments within its own address subspace.*

Address Assignment Protocols

- See IEEE Project P802.1CQ (“Multicast and Local Address Assignment”) in IEEE 802.1 TSN Task Group
 - <https://1.ieee802.org/tsn/802-1cq/>
- Pure random – no duplicate detection
 - Create an address and go
 - Simple
 - Requires huge address space to avoid collisions
- Client/server
 - Address assignment upon request
 - Avoids collisions; operates in a small address space
- Peer-to-peer claiming
 - Propose an address and check for duplication

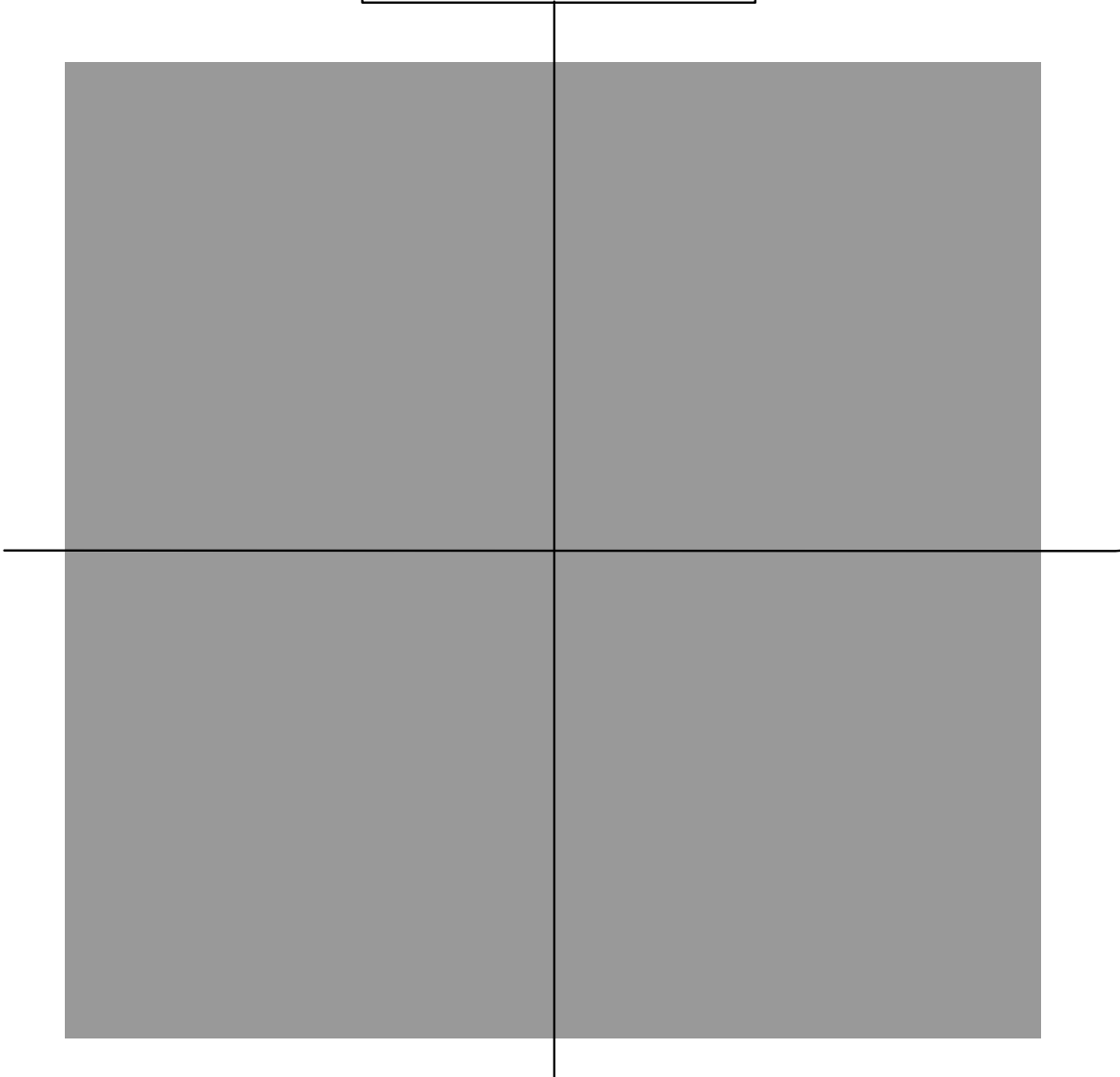
Privacy

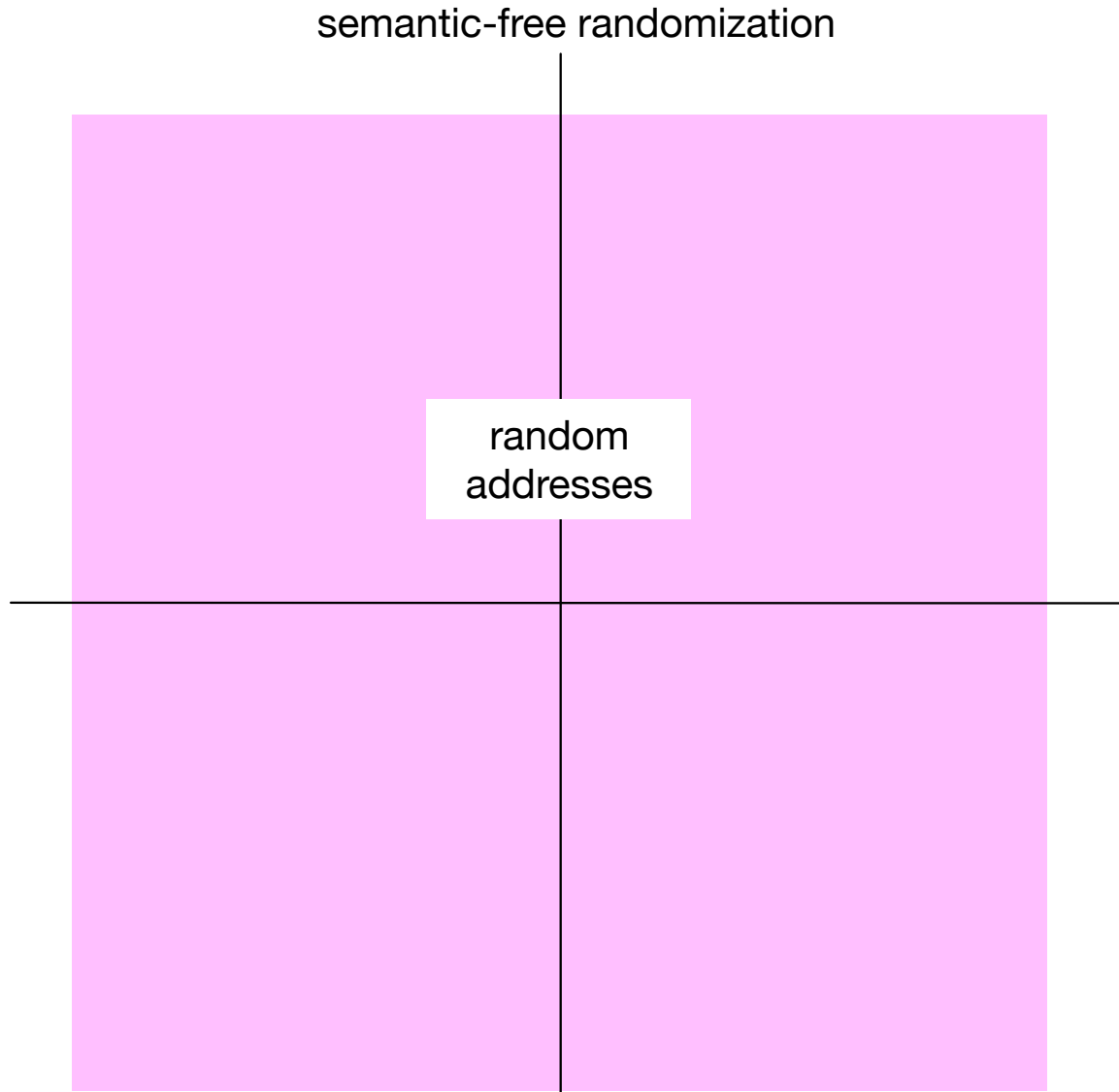
- Permanent addresses can limit privacy
- Privacy is enhanced by use of temporary addresses
 - True for random addresses
 - True also for assigned addresses (e.g. DHCP)
- Not all devices have privacy requirements
 - e.g. infrastructure

A Shared Space

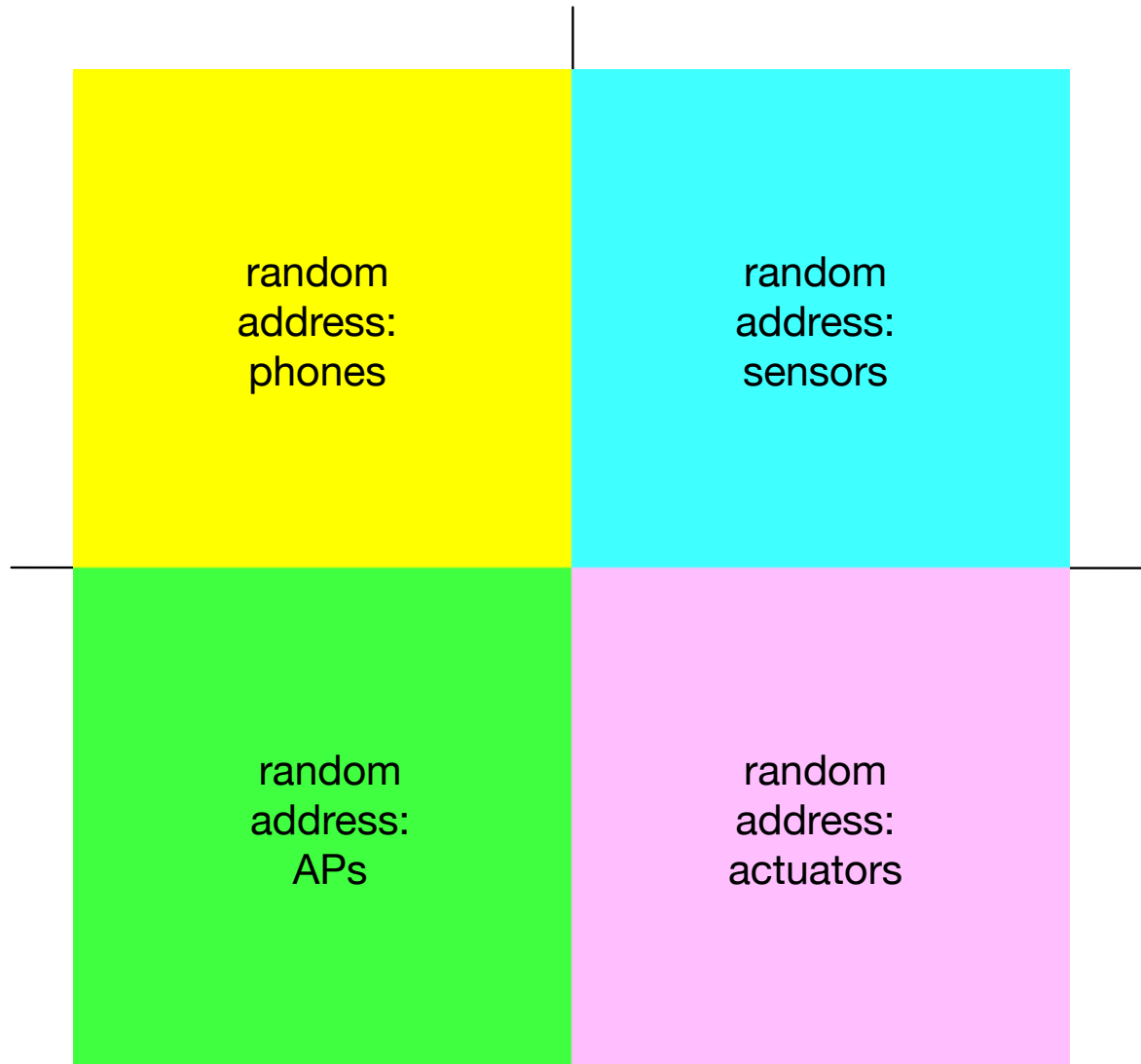
- The IEEE 802 address space is a shared one
- In 802.11, the address space is shared by, e.g.
 - APs
 - Mobile phones
 - Desktop computers
 - Industrial equipment
 - Televisions
 - Printers....
- The addressing requirements may vary.
 - e.g. varying privacy requirements
- Some address protocols support privacy, authentication, etc. [6]

46 bit local address space



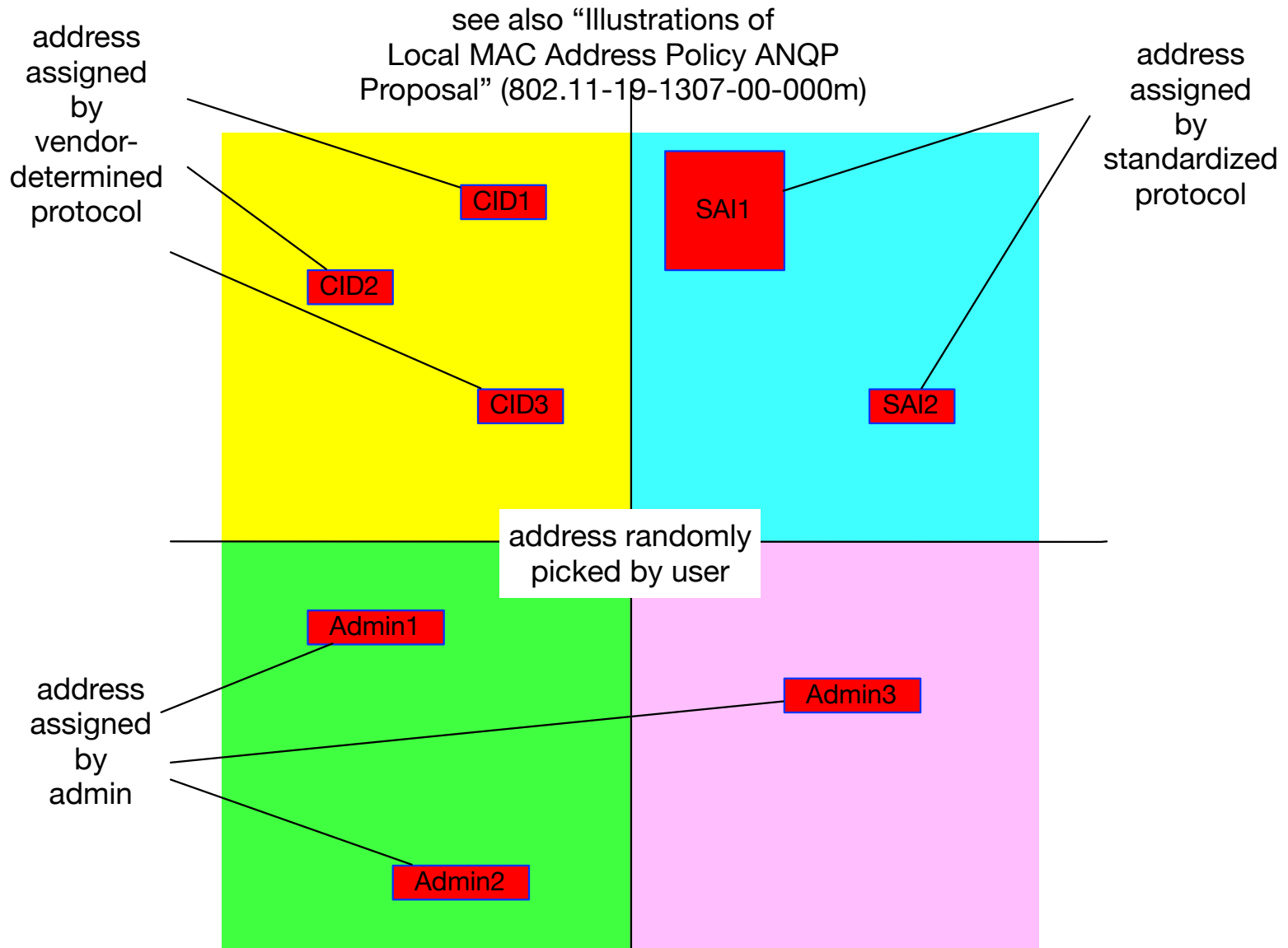


simple structured randomization



structured address space and protocols





Summary

- The local address space is huge and valuable.
- Wireless LANs serve many purposes.
- In a single wireless LAN, the address space is shared by many types of devices with different needs.
- Let's make room for multiple schemes to flourish and serve multiple purposes.

References

- [1] R. Marks, “Local MAC Addresses in the Overview and Architecture based on IEEE Std 802c,” 2017-09-13 (IEEE 802.11-17/1466r01)
- [2] IEEE Std 802c: IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture – Amendment 2: Local Medium Access Control (MAC) Address Usage (2017-06-15)
- [3] IEEE Project P802.1CQ, Multicast and Local Address Assignment <<https://1.ieee802.org/tsn/802-1cq>>
- [4] R. Marks, A. de la Oliva, S. McCann, and M. Hamilton, “MAC Address Policy ANQP,” 2019-07-08 (IEEE 802.11-19/0286r7)
- [5] R. Marks, “Illustrations of Local MAC Address Policy ANQP Proposal,” 2019-07-16 (IEEE 802.11-19-1307r00)
- [6] R. Marks, “Temporary Addresses,” 2019-05-13 (IEEE 802.11-19-0884r00)