

IEEE Recommended Practice for Privacy Considerations for IEEE 802[®] Technologies

IEEE Computer Society

Developed by the
LAN/MAN Standards Committee

IEEE Std 802E[™]-2020

IEEE Recommended Practice for Privacy Considerations for IEEE 802® Technologies

Developed by the

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 24 September 2020

IEEE SA Standards Board

Abstract: A privacy threat model for IEEE 802[®] technologies is specified by this recommended practice. The document also provides recommendations on how to protect against privacy threats and promotes a consistent approach to the mitigation of privacy threats by IEEE 802 protocol developers.

Keywords: bridging, confidentiality, fair use, IEEE 802.1[™], IEEE 802E[™], information model, LANs, Local Area Networks, metropolitan area networks, network management, personally identifiable information, personally correlated information, privacy, routing, security

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2020 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 13 November 2020. Printed in the United States of America.

IEEE and 802 are registered trademarks in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-1-5044-6976-0 STD24361
Print: ISBN 978-1-5044-6977-7 STDPD24361

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (<https://standards.ieee.org/ipr/disclaimers.html>), appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA, and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE Standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents.**

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and Standards Coordinating Committees are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the [IEEE SA myProject system](#). An IEEE Account is needed to access the application.

Comments on standards should be submitted using the [Contact Us](#) form.

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; <https://www.copyright.com/>. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit [IEEE Xplore](#) or [contact IEEE](#). For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the [IEEE SA Website](#). Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in [IEEE Xplore](#). Users are encouraged to periodically check for errata.

Patents

IEEE Standards are developed in compliance with the [IEEE SA Patent Policy](#).

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at <https://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

Participants

At the time this recommended practice was submitted to the IEEE SA Standards Board for approval, the IEEE 802.1 Working Group had the following membership:

Glenn Parsons, *Chair*
John Messenger, *Vice Chair*
Jessy V. Rouyer, *Secretary*
Mick Seaman, *Security Task Group Chair*
Karen Randall, *Security Task Group Vice Chair*
Jerome Henry, *Editor*

Astrit Ademaj
Ralf Assmann
Christian Boiger
Paul Bottorff
Radhakrishna Canchi
Feng Chen
Weiyang Cheng
Paul Congdon
Rodney Cummings
Josef Dorr
Hesham Elbakoury
Thomas Enzinger
János Farkas
Donald Fedyk
Norman Finn
Geoffrey Garner
Craig Gunther
Marina Gutierrez
Stephen Haddock
Mark Hantel
Marc Holness
Satoko Itaya

Yoshihiro Ito
Michael Karl
Stephan Kehrer
Randy Kelsey
Hajime Koto
James Lawlis
Christophe Mangin
Scott Mansfield
Kenichi Maruhashi
David McCall
Larry McMillan
Tero Mustala
Roy Myers
Hiroki Nakano
Bob Noseworthy
Tomoki Ohsawa
Hiroshi Ohue
Donald R. Pannell
Michael Potts
Dieter Proell
Wei Qiu

Maximilian Riegel
Atsushi Sato
Frank Schewe
Maik Seewald
Ramesh Sivakolundu
Johannes Specht
Marius Stanica
Guenter Steindl
Karim Traore
Balazs Varga
Hao Wang
Tongtong Wang
Xinyuan Wang
Karl Weber
Brian Weis
Ludwig Winkel
Jordon Woods
Takahiro Yamaura
Xiang Yu
Nader Zein
William Zhao
Helge Zinner

The following members of the individual balloting committee voted on this recommended practice. Balloters may have voted for approval, disapproval, or abstention.

Thomas Alexander	Raj Jain	Satoshi Obara
Johann Amsenga	SangKwon Jeong	Bansi Patel
Amelia Andersdotter	Pranav Jha	David Piehler
Butch Anton	Peter Jones	Clinton Powell
Harry Bims	Piotr Karocki	Karen Randall
Nancy Bravin	Randy Kelsey	R. K. Rannow
Vern Brethour	Stuart Kerry	Maximilian Riegel
Demetrio Bucaneg	Evgeny Khorov	Markus Rindchen
William Byrd	Yongbum Kim	Robert Robinson
Paul Cardinal	Tero Kivinen	Benjamin Rolfe
Pin Chang	Thomas Kurihara	Jessy V. Rouyer
Evelyn Chen	Chung-Yiu Lam	Frank Schewe
Charles Cook	Hyeong Ho Lee	James Schuessler
Rodney Cummings	James Lepp	Mick Seaman
Norman Finn	Jon Lewis	Manikantan Srinivasan
Avraham Freedman	Michael Lynch	Thomas Starai
Devon Gayle	John Mackay	Walter Struppler
Zhigang Gong	Jouni Malinen	David Tepen
David Goodall	Stephen McCann	Mark-Rene Uchida
Randall Groves	Brett McClellan	George Vlantis
Marek Hajduczenia	Larry McMillan	Khurram Waheed
Mark Hantel	Richard Mellitz	Karl Weber
Jerome Henry	John Messenger	Brian Weis
Marco Hernandez	Michael Montemurro	Scott Willy
Werner Hoelzl	Ronald Murias	Chun Yu Charles Wong
Oliver Holland	Rick Murphy	Yu Yuan
Russell Housley	Nick S. A. Nikjoo	Oren Yuen
Atsushi Ito	Paul Nikolich	Janusz Zalewski

When the IEEE SA Standards Board approved this recommended practice on 24 September 2020, it had the following membership:

Gary Hoffman, *Chair*
Jon Walter Rosdahl, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Ted Burse	David J. Law	Mehmet Ulema
Doug Edwards	Howard Li	Lei Wang
J. Travis Griffith	Dong Liu	Sha Wei
Grace Gu	Kevin Lu	Philip B. Winston
Guido R. Hiertz	Paul Nikolich	Daidi Zhong
Joseph L. Koepfinger*	Damir Novosel	Jingyi Zhou
	Dorothy Stanley	

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 802E™-2020, IEEE Recommended Practice for Privacy Considerations for IEEE 802® Technologies.

IEEE 802® technologies play a major role in Internet connectivity, but can disclose their users' private information. This recommended practice, IEEE Std 802E-2020, specifies a privacy threat model for IEEE 802 technologies and provides recommendations on how to protect against privacy threats.

Contents

1.	Overview.....	13
1.1	Scope.....	13
1.2	Purpose.....	13
1.3	Introduction.....	13
1.4	Applicability	14
1.5	Privacy definitions and the need for privacy	14
2.	Normative references	15
3.	Definitions	16
4.	Abbreviations and acronyms	18
5.	Recommendations.....	19
5.1	Recommendations terminology	19
5.2	General privacy principles	19
5.3	Documenting privacy considerations.....	19
6.	Rationale for privacy in IEEE 802.....	20
6.1	Personal information.....	20
6.2	Personal devices and shared service devices	21
6.3	Fingerprinting	21
6.4	Possible methods of adversaries	22
7.	Privacy threats.....	23
7.1	Source and Destination MAC addresses.....	23
7.2	MAC and physical layer operations.....	23
7.3	Flow identifiers	24
7.4	Optional fields.....	24
7.5	Network discovery	24
7.6	Wireless discovery and ranging.....	24
7.7	Authentication and access control	25
7.8	Directed queries	25
7.9	Frame timing.....	25
7.10	Frame sizes	25
8.	Designing for privacy	26
8.1	Limiting PII exposure	26
8.2	Privacy consideration checklist	26
8.3	Implementation considerations	28
	Annex A (informative) Bibliography	29
	Annex B (informative) Privacy threat examples	31
B.1	MAC address	31
B.2	Flow identifiers	31
B.3	Optional fields.....	32
B.4	Network discovery frames	33

B.5	Authentication and access control	37
B.6	Directed query or instruction frame.....	41

Figures

Figure B-1—IEEE 802.11 frame structure	33
Figure B-2—IEEE 802.11 Frame Control field.....	33

Tables

Table B-1—EAPOL Packet Types (from IEEE Std 802.1X-2010)	37
--	----

IEEE Recommended Practice for Privacy Considerations for IEEE 802[®] Technologies

1. Overview

1.1 Scope

This recommended practice specifies a privacy threat model for IEEE 802[®] technologies and provides recommendations on how to protect against privacy threats.

1.2 Purpose

The purpose of this recommended practice is to promote a consistent approach by IEEE 802 protocol developers to mitigate privacy threats identified in the privacy threat model and provide a privacy guideline.

1.3 Introduction

A threat model facilitates methodical identification of threats to resources or activities, risks associated with those threats, and possible counter-measures. This recommended practice is concerned with privacy, and specifically with the unwanted disclosure of personal information (Clause 6) as a result of communication using procedures specified by IEEE 802 standards. Privacy definitions and the need for privacy are reviewed in 1.5, and possible goals of adversaries seeking access to, or making use of that personal information, are further described in 6.4.

The information conveyed in the user data frames that support the media access control (MAC) service (IEEE Std 802.1AC [B2]) provided by all IEEE 802 MAC technologies is typically specified by application or higher layer protocol standards and is outside the scope of this recommended practice. Unwanted disclosure of personal information in that user data is expected to be prevented by cryptographic confidentiality protection. All the user data may be protected, e.g., as specified in IEEE Std 802.11 [B8] or IEEE Std 802.1AE [B3]; or just the data conveyed by a higher layer protocol, e.g., by the Transport Layer Security Protocol (IETF RFC 8446 [B22]) may be protected.¹

IEEE 802 MAC technologies do not communicate explicit personal information other than in MAC Service user data frame fields. However, communication has observable properties, which include, but are not necessarily limited to, other frame fields, the sizes and transmission timing of both confidentiality protected and other frames, and physical layer signaling and power use and negotiation. An adversary can correlate these observable properties with the devices used by an individual or a small group of people (6.2) or with specific applications to fingerprint (6.3) those devices and applications.

¹ The numbers in brackets correspond to the numbers of the bibliography in Annex A.

Common ways in which IEEE 802 technologies contribute to fingerprinting and the resulting privacy threats are described in Clause 7. Specific questions designed to identify the presence of these and similar opportunities in specific technologies are posed in Clause 8. These questions are designed to prompt groups developing standards and individuals and organizations reviewing these standards to consider alternative designs to reduce privacy risks.

1.4 Applicability

The practices described in this recommended practice cannot be expected to protect privacy against determined efforts by adversaries who have pervasive access to the communication media that a person or an identifiable small group might use, or who can control or operate devices that allocate resources for network communication based on authentication or authorization of a person or a personal device. Such adversaries can include organizations that a person could reasonably expect to be trustworthy. This technical recommendation is therefore not a substitute for privacy regulation, nor should its existence be taken as reducing any independently determined need for regulation. There are potential adversaries whose span of control and ability to carry out correlation and fingerprinting as described in this recommended practice is more restricted. Helping to protect personal information against such less powerful adversaries remains an important goal.

An adversary cannot be expected to confine attacks to the threats exposed by any one specification, set of specifications, or layers in a network reference model. Measures developed in accordance with this recommended practice should be used in conjunction with others that specify design and implementation measures to protect communication and reduce disclosure of Personally Identifiable Information (PII) and Personally Correlated Information (PCI) by the network protocols and applications that make use of IEEE 802 Local Area Networks (LAN). Risk analysis should also take into account the ability of adversaries to combine network information with that discovered by other methods, e.g., the use of video surveillance to reduce the number of potential targets to be fingerprinted.

1.5 Privacy definitions and the need for privacy

The term *privacy* is used in many contexts and is defined in multiple ways. These definitions are sometimes specific to a domain (e.g., regulatory, social anthropology) or span across several domains. As a result, many organizations have defined privacy in a way specific to their needs. The work of these organizations can be based on IEEE 802 protocols. The use of the word *privacy* in this recommended practice does not preclude a broader understanding of the word *privacy* (e.g., as described in IETF RFC 6973 [B18]).

Historically, it has been argued that individuals who are law-abiding have no need for privacy protection: “nothing to hide, nothing to fear.” Experience has shown this judgment to be naive in a number of ways. There are three components to this: opportunity for attack, motivation of the adversary, and the consequence for the person whose privacy was compromised. Examples of these include the following:

- Social disapproval, even by a small minority, of purely legal activities or opinions can be exploited to an adversary’s financial gain or other advantage while inflicting considerable distress on the individuals whose privacy has been compromised.
- Individuals are often required to use personal information as a last resort or supplementary proof of identity when communicating with an organization. Possession of that personal information is often taken as authenticating organizational representatives; privacy breaches thus facilitate both “identity theft” and “phishing.”
- Data on personal preferences and associations can be used to manipulate the opinions and behavior of individuals who are unaware that the information delivered to them differs from that available to others.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used; therefore, each referenced document is cited in text, and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std 802®, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture.^{2,3}

² IEEE publications are available from The Institute of Electrical and Electronics Engineers (<https://standards.ieee.org>).

³ The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.

3. Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.⁴

attack: The actions taken by an adversary who accesses transmission media or network devices to obtain Personally Identifiable Information (PII) that its owner does not wish to be known by that adversary.

active adversary: An adversary who transmits frames as part of an attack.

adversary: A threat agent who is attempting to fingerprint one or more targets.

correlation: A statistical relationship.

NOTE—In the context of this recommended practice, an adversary can use correlations between frame fields and a particular personal device and take into account the time when these frames are observed to identify the user of that device.⁵

eavesdropping: Listening to communication without the consent from communicating parties.

NOTE—In the context of this recommended practice, eavesdropping involves observing communications supported by IEEE 802® media access control (MAC) procedures and can include observation of the details of MAC operation as well as those of addresses, protocol identifiers, data, and timing of transmitted frames.

fingerprinting: The process of uniquely identifying (with a sufficiently high probability) a person, a device, or an activity.

identifier: A name, address, label, distinguishing index, or attribute specified in an IEEE 802® standard.

information element: A field or set of fields defined in an IEEE 802® standard that is used to convey protocol information.

passive adversary: An adversary who observes frames but does not emit frames as part of an attack.

pattern: A combination of elements that form an identifiable sequence.

NOTE—In the context of this recommended practice, a sequence can extend to multiple frames and include timing information.

persistent identifier: An identifier that is reused by a device or by another device associated with the same person or group of persons for an indefinite period.

Personally Identifiable Information (PII): Any data that directly or indirectly identifies a person or from which the identity or the contact information of a person can be derived.

Personally Correlated Information (PCI): Data gathered about an identified person or small group of people by observing activities (e.g., communications) or events associated with those people.

personal device: A device associated with a user or a group of users, such that identification of the device also allows identification of its user or group of users.

respondent: A network device to which a target is intending to communicate.

⁴ *IEEE Standards Dictionary Online* is available at <https://dictionary.ieee.org>.

⁵ Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement the standard.

risk: The potential for loss or damage arising from a threat.

NOTE—In the context of this recommended practice, loss or damage affects a person's privacy. The assessment of risk takes into account the probability of threat exploitation, including costs that might deter an adversary, and the possible impact of exploitation.

shared service device: A device associated with a large enough group of users, such that identification of the device does not easily allow identification of individual users or groups of users.

target: The personal device from which the adversary wishes to obtain Personally Identifiable Information (PII). The PII may be obtained from frames emitted from the machine associated with the target.

temporary identifier: An identifier that takes on a fresh value, uncorrelatable to previously used values, whenever the operation of media access control (MAC) and higher layer protocols permit.

threat: A potential for violation of privacy; the unauthorized disclosure of Personally Identifiable Information (PII).

threat action: The unauthorized disclosure of Personally Identifiable Information (PII).

threat agent: An entity that performs a threat action.

tracking: The process of observing identifiers or information elements of personal devices repeatedly to perform fingerprinting.

NOTE—Passive and active adversaries can track personal devices by fingerprinting their use of identifiers, information elements, or media access control (MAC) procedures. This action may result in the unique identification of a device and may also inform an adversary on the device location.

universal address: A globally unique media access control (MAC) address.

NOTE—See 8.2 of IEEE Std 802-2014.⁶

⁶ Information on references can be found in Clause 2.

4. Abbreviations and acronyms

The following abbreviations and acronyms are used in this recommended practice.

AP	access point
BSS	basic service set
DA	Destination MAC address
DMG	directional multi-gigabit
IP	Internet Protocol
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
MAC	media access control
PDU	protocol data unit
PCI	Personally Correlated Information
PII	Personally Identifiable Information
SA	Source MAC address
SSID	service set identifier
TIM	traffic indication map

5. Recommendations

This recommended practice makes recommendations for use by standards developers, implementers, network designers, network operators, and people who evaluate and use the results of their work and the services provided.

5.1 Recommendations terminology

For consistency with existing IEEE and IEEE 802.1 standards, recommendations are expressed using the following terminology:

- a) **May** is used to describe choices (*may* means permitted to; therefore, *may* and *may not* mean precisely the same thing);
- b) **Should** is used for recommended choices (the behaviors described by “should” and “should not” are both permissible but not equally desirable choices).

Needless repetition and apparent duplication of recommendations is avoided whenever the definite **is**, **is not**, **are**, and **are not** can be used in an appropriate context. Possible behaviors or conditions that do not always occur or are not directly controllable regardless of whether a recommendation has been adopted are described by **can**. Behaviors or conditions that never occur or never apply are described by **cannot**.

NOTE—Not all indicated possibilities are desirable. They include actions that an adversary **can** perform.

5.2 General privacy principles

IEEE 802 standards that define a service that can be used by a personal device should take into account the general privacy principles described in Clause 8.

5.3 Documenting privacy considerations

IEEE 802 standards that define a service or services that can be used by personal devices should include a clause or informative annex that aims at providing the following:

- a) Description of privacy exposures by answering the questions in Clause 8. These answers should be documented during the development of the standard for readers of the standard. Descriptive text for these answers should be provided in the published clause or an annex in the standard.
- b) Guidance on possible implications for implementers of the standard as described in 8.3.

6. Rationale for privacy in IEEE 802

This recommended practice provides a framework to assist the implementation of privacy by design in the context of developing and using IEEE 802 standards. This document

- Provides recommendations aimed at protecting privacy in IEEE 802 protocols and their implementations.
- Does not address how to balance privacy requirements with communication exchange requirements.
- Describes how elements used in IEEE 802 protocols may, directly or through correlation, contribute to exposure of potential Personally Identifiable Information (PII) and privacy elements.
- Provides recommendations on how protocols can limit this exposure.

This recommended practice, however,

- Does not address security specifically.
- Does not consider PII that transits as data payload through IEEE 802 technologies (except for identifying the need to support security with confidentiality so that data is not exposed).

It is understood that data communication can be integrity-protected and data payload can be encrypted for confidentiality. A security violation (e.g., weak key or compromised key) is likely to result in both security and privacy violations.

This recommended practice focuses on PII and elements in one or more of the following categories:

- a) Specified/defined/created and used within an IEEE 802 standard.
- b) Specified/defined/created and used within an IEEE 802 standard and used by other standards, protocols, or specifications.
- c) Specified/defined/created externally to IEEE 802 standards but used as part of the specified operation of an IEEE 802 standard.

6.1 Personal information

In this recommended practice, privacy is concerned with the information that relates to an individual (see 1.5). In particular, it concerns any data that directly or indirectly identifies an individual (PII) or from which identity or contact information of an individual can be derived, including data that allows the identification of an individual based on recognizing or analyzing correlations and patterns. This data can include information that can be used to identify where a person is or has been, or to associate certain traffic with the person and a particular time window, or to identify what the person is doing [Personally Correlated Information (PCI)] and when the person is performing a particular activity.

In all cases, there is an intrusion on a person's activity that correlates information collected through the usage of an IEEE 802 protocol and that person.

In IEEE 802 protocols, device identification or correlation is often necessary and sometimes needs to be explicitly stated. A typical case is where a device or a flow needs to receive a particular service: a device or flow might need to be clearly identified in order to receive the service, and the identifier might be local or might be propagated with the flow along the communication path. For example, a service accepting guaranteed bandwidth requests would need to retain the identity of devices that have reserved bandwidth.

The entity that provides the service is therefore expected to be authorized to observe or collect identifiers and any associated PII or PCI. This ability should be taken into consideration during standard and network

design to carefully choose the entity that controls the service and the location of that entity. In most designs, a single entity is not in charge of observing or collecting all identifiers (at multiple layers) for all provided services.

The collection of PII and PCI does not necessarily constitute a violation of privacy. Where information is provided voluntarily and freely by a person who has been given a reasonable opportunity to understand the implications of their choices, or when the information disclosure is necessary to provide the service requested by the user, collection of PII or PCI can imply big advantages for both the person and their service provider. A common example is the registration to a private network based on the user device's MAC address (e.g., in the IEEE 802.11 network of a hotel), or a heart rate sensor (constituting user PII) and its associated traffic (constituting PCI) that is voluntarily associated to the person wearing the sensor. Many other cases associate the voluntary association of a device and its associated traffic to a consenting person.

However, even if information was provided voluntarily, distributing the information or keeping the information beyond an expected duration (e.g., that of receiving the consented service) might constitute a violation of privacy.

6.2 Personal devices and shared service devices

A personal device is primarily used by a single person or a small group of people (e.g., members of a single household). As such, any IEEE 802 element that uniquely identifies this device also identifies the associated person or small group of people. This personal device may be a terminal equipment (e.g., a computer) or may provide infrastructure service to one or a small group of terminal equipment devices (e.g., a networking device connecting a single household to the Internet). The device does not need to be associated with a single person permanently. For correlation to occur, the device may just need to be associated to a person at the time of PII or PCI collection.

By contrast, a shared service device is used by a large enough number of people that IEEE 802 elements can identify the device without clearly identifying any person using the services provided by that device. An example of such shared service device includes a router, or a switch, in a medium to large network where multiple users exchange traffic.

6.3 Fingerprinting

A device can be identified by its use of observable IEEE 802 observable information and procedures. The correlation may be direct (i.e., a single IEEE 802 element identifies a single device) or indirect (i.e., several IEEE 802 elements observed and analyzed together imply the use of a particular device). The correlation can be strong enough for subsequent recognition based on a subset of its elements. PII can be exposed even if the correlation is imperfect, if the probability of correct identification is sufficient to be useful to an adversary. An adversary is assumed to have the capability to observe, manipulate, or inject frames from anywhere on the medium, on the full communication path, on the administrative network, etc.

The correlation between observable information elements and a device is called a *device fingerprint*, and its determination is called *device fingerprinting*. If the device is a personal device, successful device fingerprinting effectively labels a person or a small group of people. The fingerprint can be based on information that is ephemeral, e.g., use of successive values of a sequence number in a protocol, or can be persistent, e.g., using a permanently assigned MAC address or (for a wireless device) characteristics of the radio implementation. A persistent fingerprint can be used to track the location of a mobile personal device and hence the location of a person over a long period of time and can help an adversary establish the relationship between the fingerprint and a person's identity. Thus, in addition to the identification of persons, IEEE 802 information elements can be used to infer personal attributes of that person. For instance, IEEE 802.11 service set identifiers (SSIDs) can reveal employer's name, home location, and other visited

locations; likewise, the universal MAC address and vendor name can reveal the model of the device, which may be used to infer information on the person's wealth.

Additionally, network applications and activities supported by the device can result in a characteristic usage pattern of IEEE 802 protocol elements; such usage patterns may allow those applications to be fingerprinted with the additional possibility of exposing details of their use. For example, the sizes of successive packets sent by some financial websites can allow individual webpages to be identified and the size of account balances and transactions to be estimated, even if the data in the packets is unknown to an adversary. The repeated use of specific applications can help an adversary fingerprint a device.

This recommended practice does not determine a strict statistical threshold beyond which device or person identification would be established (and below which privacy would be maintained), but it considers that PII can be exposed as soon as a correlation can facilitate an association to a device or a person or his or her attributes or activities. As soon as this association is achieved, observation of the traffic can permit the acquisition of additional information (PCI) about the person. The threshold and the risk associated to such correlation are context-dependent.

6.4 Possible methods of adversaries

A number of actors are considered to be interested in exfiltrating (i.e., observing and capturing) PII from IEEE 802 frames with various goals. Possible methods used by these actors for gathering intelligence include the following:

- **Surveillance.** Passive fingerprinting by adversaries, where the goal is to observe where/when a target has connected to a network. For example, an adversary's collection of PII across many network links is referred to as *pervasive surveillance*. For a pervasive surveillance threat analysis, see IETF RFC 7624 [B20].
- **Probing.** Sourcing of packets sent to a target or its respondent in order to cause it to reveal PII.
- **Modification.** Changing frames sent to/from a target in order to cause it to reveal PII.

7. Privacy threats

IEEE 802 LAN standards specify the operation of media access control methods and protocols that support frame-based network communication. MAC procedures and various protocol frame formats and fields can be used to identify personal devices, their attributes, and their use to support specific networking applications and activities. As described in Clause 6, an adversary can use this information to obtain PII and PCI. The location of mobile personal devices and thus presumably the location of the person using that device can be tracked. The fact that users of personal devices are communicating with each other can be detected. A person's behavior can be monitored.

This clause describes some of the protocol elements and MAC characteristics that can be exploited by an adversary. It makes no claim to be an exhaustive list of privacy threats related to current IEEE 802 standards and standards under development. Annex B proposes detailed examples of such elements.

An adversary can require access to the medium supporting the MAC for an individual LAN (e.g., near enough to the target for adequate radio reception in the case of a wireless medium) to exploit some of the threats described. In other cases, the information sought by the adversary is potentially accessible from anywhere. Some threats are more effectively exploited by an active adversary if that adversary is willing to run the risk of detection.

7.1 Source and Destination MAC addresses

All IEEE 802 protocol frames begin with a Destination MAC address (DA) and a Source MAC address (SA). In order to simplify the analysis, these frame fields are considered independently, and their consideration applies to all use cases. The analysis is written as if a target is initiating frames, where the SA can be PII. (Of course, for frames directed to the target the DA would be considered PII.)

An SA is considered PII if it is associated with a target (i.e., is considered a "personal device" as defined by this recommended practice). Not every device emitting frames is considered a target. For example, a bridge within a network is not generally associated with a person and therefore would not be considered a target. However, the SA associated with a residential gateway network device is very much associated with its subscriber (i.e., a user or household of users) and thus would be considered a target.

Some IEEE standards further identify systems on the path of the frame, even if they are not directly SA or DA. For example, in addition to the SA and DA, IEEE Std 802.11 [B8] uses the transmitter address (TA) and the receiver address (RA) to allow relay of frames through an intermediate device. The TA can be considered a target when associated with a personal device. Similarly, the RA can be considered a target when associated with a personal device.

7.2 MAC and physical layer operations

All IEEE 802 transmitted protocol frames are subject to physical layer and MAC layer operations, which encode information that can be used to fingerprint each transmitting device. For example, frames can contain sequence numbers or seed values that may be sequential or predictable. Monitoring such values can be sufficient to fingerprint a device. Some IEEE 802 protocols include an encapsulated MAC address. Threats to MAC addresses identified in this clause apply to these MAC addresses. Additionally, a bridge identity can be considered to be PCI if the bridge is located at a network edge associated with people (e.g., a residential gateway). The Bridge Address associated with the bridge is required to be a universal address, and it can be used to locate host addresses (e.g., those embedded in a Stream Identifier).

Repeated use of a MAC address can result in an attacker's correlation of the use of that address across networks or over time (see 6.3). Correlation of a target MAC address is not always a threat to privacy. A

person can authorize the correlation for his or her own benefit by, for example, explicitly “opting in” to the correlation after having been offered special treatment by the network owner (e.g., a business). However, when the correlation is not authorized, it can be considered a threat to privacy.

7.3 Flow identifiers

IEEE 802 standards can include parameters that identify a particular frame, that distinguish the frame from other frames transiting through the network, and that distinguish the frame from other frames exchanged between the sender and the receiver. As such, an adversary may be able to observe these frames and, distinguishing them from other frames, acquire information about specific flows or segments. This information can be used directly or through correlation to identify a specific endpoint and expose PII (see Annex B for additional flow identifiers).

7.4 Optional fields

IEEE 802 standards may allow a transmitter to include optional elements in its frames. These elements can indicate support of specific capabilities described by the standard or support of vendor-specific capabilities. Support of these capabilities, or the way these capabilities should be supported, is sometimes left to vendor implementation. These elements can be used by an adversary to recognize the transmitter type or sometimes uniquely identify the transmitter.

7.5 Network discovery

IEEE 802 standards commonly include discovery mechanisms by which endpoints explore the network services available before connection or before data frame transmission. These mechanisms often use specific frames, which can specifically target a given service. Observing the occurrence of such frames and their specific characteristics can help an adversary uniquely identify the station requesting such service. These mechanisms can also require the infrastructure device to mention support for specific parameters through general announcements mentioning feature support or through specific responses to endpoint queries. These parameters can also be used to uniquely identify the infrastructure device and PII when the infrastructure device is a personal device.

7.6 Wireless discovery and ranging

IEEE 802 standards share privacy threats due to their capacity to provide communication for frame-based data networks. In addition, radio-based technologies in IEEE 802 standards have unique privacy threats due to their expansive discovery processes and the ability of an adversary to eavesdrop on those communications.

The process of network discovery by radio-based technologies in IEEE 802 standards can rely on transmission of probes that search for available and suitable networks in which to connect. This transmission exposes the DA/SA common fields threat vector (see 7.2) to anyone within range of the device’s radio.

Radio-based technologies use transactional exchanges to discover network services. These exchanges can be intended by both the network manager and device user, but are susceptible to eavesdropping, with searches for particular services contributing to correlation and fingerprinting. These exchanges are also open to forgery, e.g., faked discovery frames can be transmitted to elicit responses from (and thus identify) groups of devices or individual devices that would normally respond to an authentic discovery frame transmitted with the same or similar parameters in their home networks.

Wireless technologies can support ranging and location services that allow accurate determination of the location of target device. Ranging information can be used to determine the relative location of devices (e.g., to determine when a phone and smartwatch are close-by) with location information being disclosed without prior authentication of the device requesting that information. As such, ranging and location can provide an adversary with information useful to a correlation function, can be combined with other observations of a target (e.g., area video surveillance), and can be used to correlate the activities of, and relationships between, individuals.

7.7 Authentication and access control

Most IEEE 802 standards include mechanisms to control access to the network or its resources. In order to allow access, exchanges are required, during which frames are sent that can provide information to uniquely identify the end device. The end device may be mobile and fingerprinted through these exchanges. In some cases, the infrastructure device can be a personal device, and these exchanges can also uniquely identify the infrastructure device.

7.8 Directed queries

Once network discovery is completed, some IEEE 802 standards implement a mechanism by which an endpoint can query an infrastructure device, or an infrastructure device can query an endpoint, to enable a particular service or perform a specific function. In many cases, the query and its response are optional in the standard, but may be accompanied by specific IEEE 802 frames or exchange sequences. The ability to perform such a query, the service queried, and/or the reply can be used by an adversary to uniquely identify the endpoint or the infrastructure device.

7.9 Frame timing

Some IEEE standards rely on timing synchronization between device communication functions, for example, to ensure the proper allocation of resources at the time of a particular device transmission. The resulting transmission timing can facilitate the association of frames with a particular device and thus support device identification for a period of time.

7.10 Frame sizes

Many of the exchanges described in this clause may rely on the use of frames with specific characteristics of format. Other frames (e.g., carrying data) may also be drawn to carry a specific amount of payload (e.g., driven by the application exchange characteristics or function of the device communication driver). Such characteristics can be used to fingerprint a device exchanging flows for a specific application. Avoidance of such fingerprinting possibilities is commonly the task of the application designer.

8. Designing for privacy

Each standard should contain an informative clause or annex (as detailed in 5.3) describing to users of the standard what privacy exposures are envisaged in the standard. Development and updating of this informative clause or annex, at the time of the development of the standard or the addition of new capabilities, can help prevent or limit privacy exposures by inviting reflection on protocol features, their design, their implementation, and their use in particular contexts or applications.

8.1 Limiting PII exposure

A standard should not require communications with a personal device that allow for correlation and fingerprinting across different stages of the communication process (typically, service discovery, authentication, and subsequent communication) or different services. Where identifiers are required to support a service provided by the standard, it is suggested that, in accordance with the principle of data minimization, these guidelines be followed:

- a) Temporary identifiers should be used or at least permitted, especially for the use of short-lived services such as network probes.
- b) Temporary identifiers should not persist across different stages of the communication process and should be restricted to specific protocol exchanges.
- c) When switching to a new temporary identifier, variable fields such as sequence numbers should be reset to their default value or to a non-deterministic value. Where multiple temporary identifiers are used concurrently, their replacement should be synchronized to avoid correlation between sets of old and new identifiers.
- d) A personal device persistent or temporary identifier should not be stored by any device specified by the standard other than the devices using those identifiers to provide or support the service.
- e) Persistent and temporary identifiers should not be stored by any device for longer than is required to provide or support the service.
- f) Periodic communications or transmissions of deterministic values or identifiers should occur at non-correlatable intervals.
- g) Temporary identifiers should not be shared across services.
- h) The use, persistence, and storage of identifiers by devices specified in the standard, and their configurability, should be described in the standard.

A standard's specification of parameter selection, configuration, or settings that can expose PII or PCI associated with a target should

- i) Allow for such selection, configuration, or setting to be done by the target.
- j) Have as the default a configuration that provides the highest level of privacy protections, while still allowing for an acceptable level of service operation.

8.2 Privacy consideration checklist

This subclause poses questions that can be used to prompt and assist in the development of a privacy considerations clause or annex within each IEEE 802 standard. They are not exhaustive and should be supplemented by considerations specific to a particular standard. Development of methodical approaches to privacy is encouraged. The following questions may also be answered by standard developers to assist network designers in their work to interpret a standard's specification with respect to its privacy impacts. These questions may also serve as a guideline for individuals or organizations reviewing the specification.

The answers to the questions that follow can serve both to highlight privacy exposures for personal devices and to explain why further steps to reduce apparent exposure were not taken. Such answers can help to guard against implementation and deployment optimizations that can have unwanted consequences.

8.2.1 Identifiers

- a) Is this standard focused on shared service devices?
- b) What identifiers are required by the service to operate?
- c) In which places in the network are these identifiers foreseen to be stored, and for how long might they be stored (as storage location and duration may have consequences for long-time exposure)?
- d) Are there any information elements containing predictable values or parameters that can be used as identifiers?
- e) Would exposure of PII or PCI (such that it allows correlation or fingerprinting) be continuous, or can it be made temporary in duration?
- f) Are the identifiers persistent, and can they be constructed so that they are not persistent?
- g) Can the goals of the feature be achieved with fewer identifiers or linkages between parameters and identifiers, or by making exposures of identifiers or linkages temporary rather than continuous, or by not exposing identifiers or linkages?

8.2.2 Observers

- a) Are exchanges between respondents and personal devices protected so that PII and PCI exposure is limited?
- b) Is the respondent device the final recipient of any particular identifier or parameter used to carry the feature, or does the respondent device need to expose the identifier(s) or parameter(s) to other nodes?
- c) What protection mechanisms are foreseen to block adversaries from having direct or indirect access to the identifiers or parameters while in transmission from personal device to respondent and vice versa?
- d) What mechanisms does the standard allow that enable an observer to become an active adversary and obtain additional PII or PCI?

8.2.3 Parameters selection

- a) In which way does the selection of parameters related to the feature (or a set of features) contribute to the fingerprinting through correlation, for instance, by creating a set of parameters so unique that a node is effectively exposed through fingerprinting?
- b) Are there identifiers or exposed parameters that can be configured by the respondent device?
- c) Are these identifiers or exposed parameters persistent or temporary? (The analysis may be different for each.)
- d) Can the identifiers or exposed parameters be configured by a personal device? Are there foreseen trajectories between nodes for these identifiers and parameters?
- e) Which set of combined parameters would be most conducive to mitigate correlation, continuity, or transmission of identifiers?
- f) Is this set of parameters the minimum needed to advance to the next step in the communications protocol, or are some parameters not needed at this stage?
- g) Does the length of parameters vary depending on the transmitted value?

8.3 Implementation considerations

To assist standards implementers in their work to interpret a standard's specification with respect to its privacy impacts, 8.2 may be used by the standards developers to answer the questions in this subclause. Answers to these questions may be detailed within the specification or provided as in a specific clause or annex:

- a) If a feature requires configuration, is there an indication to implementers about how to configure a device using the minimal set of identifiers, regardless of whether the identifiers are temporary or persistent, so that the exposure of PII or correlation elements to a personal device is minimized?
- b) Is there a similar indication for parameter selections, the order of their transmission, and the order of their inclusion in a frame?
- c) Is it possible to provide an indication about how different options in items a) and b) of this list can contribute to tracking or correlation?

Annex A

(informative)

Bibliography

[B1] IEEE Std 802.1AB™, IEEE Standard for local and metropolitan area networks—Station and Media Access Control Connectivity and Discovery.^{7,8}

[B2] IEEE Std 802.1AC™, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Service Definition.

[B3] IEEE Std 802.1AE™, IEEE Standard for local and metropolitan area networks—Media Access Control (MAC) Security.

[B4] IEEE Std 802.1AR™, IEEE Standard for Local and Metropolitan Area Networks—Secure Device Identifier.

[B5] IEEE Std 802.1Q™, IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks.

[B6] IEEE Std 802.1X™, IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control.

[B7] IEEE Std 802.3™, IEEE Standard for Ethernet.

[B8] IEEE Std 802.11™, 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.

[B9] IEEE Std 802.15.1™, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs).

[B10] IEEE Std 802.15.3™, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs).

[B11] IEEE Std 802.15.4™, IEEE Standard for Local and metropolitan area networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs).

[B12] IETF RFC 2863, The Interfaces Group MIB using SMIV2, K. McCloghrie and F. Kastenholz, June 2000.⁹

[B13] IETF RFC 3394, Advanced Encryption Standard (AES) Key Wrap Algorithm, J. Schaad and R. Housley, Sept. 2002.

⁷ IEEE publications are available from The Institute of Electrical and Electronics Engineers (<https://standards.ieee.org>).

⁸ The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.

⁹ IETF Requests for Comments (RFCs) are available from the Internet Engineering Task Force (<https://tools.ietf.org/>).

- [B14] IETF RFC 3748, Extensible Authentication Protocol (EAP), B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, ed., June 2004.
- [B15] IETF RFC 4493, The AES-CMAC Algorithm, J. H. Song, J. Lee, and T. Iwata, June 2006.
- [B16] IETF RFC 5216, The EAP-TLS Authentication Protocol, D. Simon, B. Aboba, and R. Hurst, Mar. 2008.
- [B17] IETF RFC 5247, Extensible Authentication Protocol (EAP) Key Management Framework, B. Aboba, D. Simon, and P. Eronen, Oct. 2007.
- [B18] IETF RFC 6973, Privacy Considerations for Internet Protocols, A. Cooper, H. Tschofenig, B. Aboba, J. Peterson, J. Morris, M. Hansen, and R. Smith, July 2013.
- [B19] IETF RFC 7170, Tunnel Extensible Authentication Protocol (TEAP) Version 1, H. Zhou, N. Cam-Winget, J. Salowey, and S. Hanna, May 2014.
- [B20] IETF RFC 7624, Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement, R. Barnes, B. Schneier, C. Jennings, T. Hardie, B. Trammé, C. Huiteman, and D. Borkmann, Aug. 2015.
- [B21] IETF RFC 7642, System for Cross-domain Identity Management: Definitions, Overview, Concepts, and Requirements, K. Li, P. Hunt, B. Khasnabish, A. Nadalin, and Z. Zeltsan, Sept. 2015.
- [B22] IETF RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3, E. Rescorla, Aug. 2018.
- [B23] NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions, Lily Chen, Nov. 2008.¹⁰

¹⁰ NIST publications are available from the National Institute of Standards and Technology (<https://www.nist.gov/>).

Annex B

(informative)

Privacy threat examples

B.1 MAC address

Some IEEE 802 protocols include an encapsulated MAC address. Examples of such protocols include

- IEEE 802.1Q Congestion Notification Message protocol data unit (PDU).
- IEEE 802.1Q Stream Reservation Protocol (SRP) StreamID.
- IEEE 802.1Q Virtual Station Interface Instance Identifier (VSIID).
- IEEE 802.1AB Chassis ID.
- IEEE 802.1AB Port ID.
- IEEE 802.1X Extensible Authentication Protocol over LANs MACsec Key Agreement protocol (EAPOL-MKA) Secure Channel Identifier (SCI).
- IEEE 802.1AE MAC Security Tag (SecTAG).

Additionally,

- a) When the target MAC address is a universal address, correlation of the target MAC address across multiple networks in time and space is possible. Such correlation includes cases where the MAC address is used as an SA or DA on the frame or is included in a well-known network header (e.g., an encapsulated Ethernet header, IEEE 802.1Q I-TAG, or IPv6 header).
- b) Correlation of any target MAC address can be used as an aid to the following:
 - 1) Tracking location of the target MAC address when it is mobile.
 - 2) Collecting frames to and from the target MAC address, to be used for further analysis. Further analysis can include the identification of MAC addresses that appear to be associated with a person or, once it is associated with a person, to evaluate it to determine which person.

B.2 Flow identifiers

IEEE 802 standards can include parameters that identify a particular frame, that distinguish the frame from other frames transiting through the network, and that distinguish the frame from other frames exchanged between the sender and the receiver. This subclause provides examples of such marking and highlights why such marking can be a threat.

B.2.1 Priority Code Point

A Priority Code Point (PCP) is found in several IEEE 802.1Q protocol elements: VLAN tag, Congestion Notification Message PDU, and the Multiple Stream Reservation Protocol (MSRP) structure. The PCP typically marks frames that should be prioritized because they have particular latency requirements (such as voice or video frames). In some cases, an adversary is looking for certain classes of traffic or endpoints that emit those classes of traffic.

Threats:

- a) Classes of targets can be identified based on the PCP if the adversary is aware of the PCP mappings. Some mappings are de facto or actual standards. Identification of voice and video traffic are well known and can aid in the identification of classes of targets.

B.2.2 VLAN Identifier (IEEE Std 802.1Q [B5])

A VLAN tag is used within networks to mark a frame for a particular priority and/or provide an identifier used to classify the frame. A VLAN Identifier (VID) is often used to separate different types of traffic, such as traffic from different organizations or people with different roles in the organization. The VID may be generic (default) or specific.

Threat:

- a) Classes of targets (e.g., Organization, Role) can be identified based on the VID value if the adversary is aware of the VID mappings. Such mappings are likely to be network specific and less likely to be obvious to the adversary unless correlated with other traffic analysis. However, the adversary can ascertain the mappings with enough correlation analysis.

B.2.3 Congestion Notification Tag (IEEE Std 802.1Q [B5])

An end station can add a Congestion Notification Tag (CN-TAG) to every frame it transmits from a congestion-controlled flow, which contains Flow Identifier (see 33.2.1 of IEEE Std 802.1Q-2018). The format of the Flow Identifier is not specified, but in order to be useful is likely to be persistent for a flow.

Threats:

- a) A particular flow between a target and respondent can be identified based on a Flow Identifier without the adversary interpreting the value of the tag.
- b) An adversary with knowledge of how to interpret the tag may be able to correlate flows between a target and one or more respondents.

B.2.4 StreamID (IEEE Std 802.1Q [B5])

In IEEE Std 802.1Q, StreamID is a 64-bit field that uniquely identifies a time-sensitive stream (i.e., a stream of data frames that are required to be delivered with a bounded latency). Various encodings of these eight octets are possible to identify a Talker (i.e., sender of a stream) and to differentiate different streams sourced by the same Talker. An adversary with an understanding of these StreamIDs can correlate and interpret flows between end stations in the network in terms of grouping, dependencies, and relationships.

In various IEEE standards related to time-sensitive networking, StreamID identifiers are used to separate, filter, and process streams based on rules and schedules. An adversary can derive relevant information from these identifiers and interpret relationships between stations and application flows.

B.3 Optional fields

IEEE 802 standards may allow a transmitter to include optional elements in its frames. The following subclauses provide examples of such elements.

B.3.1 IEEE 802.11 optional fields in all frames

All IEEE 802.11 frames include a common header as displayed in Figure B-1.

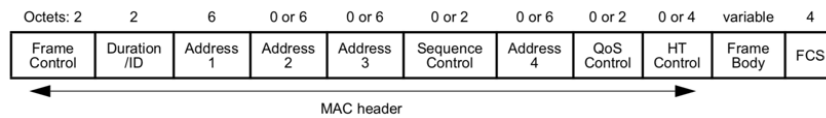


Figure B-1—IEEE 802.11 frame structure

Most fields are mandatory. Some fields, like quality of service (QoS) control and high-throughput (HT) control, are optional and present only if the transmitter supports the relevant IEEE 802.11 clauses. As such, these optional fields can be used to identify a specific device.

The Frame Control field (see Figure B-2) is present in all IEEE 802.11 frames. Its structure is specific for IEEE 802.11 operations in 60 GHz and is as follows for all other frequency bands:

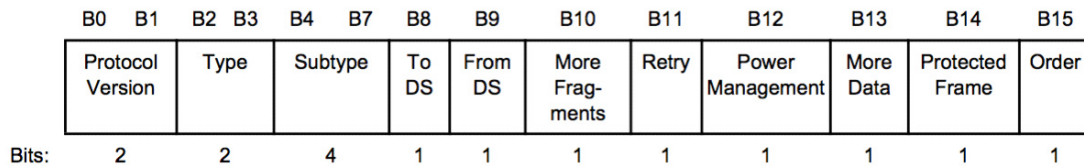


Figure B-2—IEEE 802.11 Frame Control field

Several subfields can be used to identify a transmitter:

- More Fragments: fragmenting is optional. Some driver implementations never use fragments; some others commonly do. This field can be used to fingerprint a transmitter.
- Power Management: IEEE 802.11 wireless access points (APs) usually do not sleep. Some client stations always implement power management; some others implement power management based on mode (regardless of whether connected to power source); and some client stations never implement power management. Observing this bit and its pattern for a given source can be used to fingerprint a transmitter.

B.4 Network discovery frames

IEEE 802 standards commonly include discovery mechanisms by which endpoints use specific frames to explore the network services available before connection or before data frame transmission. These mechanisms and associated frames sent by the endpoint, or the general announcements or responses sent by the infrastructure, can be used to fingerprint the transmitter. The following subclauses provide examples of such mechanisms.

B.4.1 LLDP (IEEE Std 802.1AB [B1])

Link Layer Discovery Protocol (LLDP) frames deliver information about a station as type/length/value tuples (TLVs), which can be valuable to other peers on a network segment. LLDP frames are typically emitted by network infrastructure components, but can also be emitted from other non-consumer types of endpoint devices [e.g., Power over Ethernet (PoE) connected luminaires] and from consumer devices.

Threats:

- a) A network address (MAC address or IP address) in a network address TLV can be used to identify a target.
- b) A system name subTLV can be used to identify a target by domain name.
- c) A System Capabilities TLV can identify the class of a target [e.g., telephone, Data Over Cable Service Interface Specification (DOCSIS) cable device] and can be PCI.

Organizationally Specific TLVs can be defined to contain PII or PCI.

B.4.2 IEEE 802.11 Probe Request frames

The IEEE 802.11 Probe Request contains some elements that identify the requesting station capabilities. These elements are identical to those found in the Association Request frame later sent by the same station. Their characteristics are identical for the Association Request and the Probe Request and can be used to uniquely identify the requesting station and its characteristics.

Elements present in the Association Request and similarly present in the Probe Request frames include the following:

- Supported Rates and BSS Membership Selectors element
- Extended Supported Rates and BSS Membership Selectors element
- Supported Operating Classes element
- HT Capabilities element
- 20/40 BSS Coexistence element
- Extended Capabilities element
- Multi-band element
- DMG Capabilities element
- Multiple MAC Sublayers element
- VHT Capabilities element
- Vendor Specific element

The Probe Request also includes the following elements that can contain further information to uniquely fingerprint the requesting station:

- SSID element
- DSSS Parameter Set element
- SSID List element
- Channel Usage element
- Mesh ID element
- Interworking element
- Estimated Service Parameter element
- Extended Request element

B.4.3 IEEE 802.11 Beacon frames

The Beacon is sent by the AP to inform about the network characteristics. In many networks, information contained in the Beacon only identifies the wireless infrastructure and does not contain useful PII. However, beacon information can be correlated to PII when the AP is associated to a person, for example, when implemented in a home or small store, a mobile Wi-Fi hotspot, or in a peer-to-peer [e.g., independent basic service set (IBSS)] topology. Beacon frames advertise information about the network. Multiple fields are optional or contain optional elements to specify what features are supported. An adversary can observe the beacons and use the observed fields to fingerprint the transmitter.

In particular, an adversary can use the Beacon Timestamp, Beacon interval, and Capability field as well as the following elements to fingerprint the transmitter:

- SSID element
- Supported Rates and BSS Membership Selectors element
- DSSS Parameter Set element
- IBSS Parameter Set element
- TIM element
- Power Constraint element
- Channel Switch element
- Quiet element
- IBSS DFS element
- TPC Report element
- ERP element
- Extended Supported Rates and BSS Membership Selectors element
- RSN element
- BSS Load element
- EDCA Parameter Set element
- QoS Capability element
- AP Channel Report element
- BSS Average Access Delay element
- Antenna element
- BSS Available Admission Capacity element
- BSS AC Access Delay element
- Measurement Pilot Transmission element
- Multiple BSSID element
- RM Enabled Capabilities element
- Mobility Domain element
- DSE Registered Location element
- Extended Channel Switch Announcement element
- Supported Operating Classes element
- HT Capabilities element
- HT Operations element
- 20/40 BSS Coexistence element
- Overlapping BSS Scan Parameters element
- Extended Capabilities element

- FMS Descriptor element
- QoS Traffic Capability element
- Time Advertisement element
- Interworking element
- Advertisement Protocol element
- Roaming Consortium element
- Emergency Alert Identifier element
- Mesh ID element
- Mesh Configuration element
- Mesh Awake Window element
- Beacon Timing element
- MCCAOP Advertisement Overview element
- MCCAOP Advertisement element
- Mesh Channel Switch Parameters element

An adversary can also emit a Transmit Power Control (TPC) request, observe the TPC response from the AP in the subsequent beacon, and use this information to fingerprint the transmitter and its location. Additionally, an adversary can emit a Beacon containing an SSID string identical to that of another system and thus attract targets to the adversary's device rather than the legitimate AP.

B.4.4 IEEE 802.11 DMG Beacon frames

The directional multi-gigabit (DMG) Beacon frame presents a structure similar to that of the Beacon frame, many of the same fields and therefore the same threats. The DMG Beacon frame also contains fields specific to the 60 GHz operations that can be used fingerprint the emitting AP.

In particular, the following fields and elements can be used to fingerprint the emitting AP:

- Sector Sweep field
- Clustering Control field
- DMG Capabilities element
- Extended Schedule element
- DMG Operation element
- Next DMG ATI element
- DMG BSS Parameter Change element
- Multi-band element
- Awake Window element
- DMG Wakeup Schedule element
- UPSIM element
- Nontransmitted BSSID Capability element
- SSID List element
- PCP Handover element
- Next PCP List element
- Antenna Sector ID Pattern element

B.4.5 IEEE 802.11 Probe Response frames

The Probe Response frame structure is very similar to that of the Beacon frame, and the same elements can be used to fingerprint the transmitter.

However, Probe Responses do not contain TIM fields, QoS capability, the FMS descriptor, the HCCA TXOP Update Count element, and the Future Channel Guidance element.

B.5 Authentication and access control

Most IEEE 802 standards include mechanisms to control access to the network or its resources. The exchanges associated to these mechanisms can contain elements that may allow an adversary to uniquely identify the endpoint or infrastructure device. The following subclauses provide examples of such cases.

B.5.1 Port-Based Network Access Control (IEEE Std 802.1X [B6])

Several types of management frames can be represented as Extensible Authentication Protocol (EAP) over LAN (EAPOL) frames. Table B-1 lists EAPOL Packet Types detailed in Table 11-3 of IEEE Std 802.1X-2010.

Table B-1—EAPOL Packet Types (from IEEE Std 802.1X-2010)

Packet Type
EAPOL-EAP
EAPOL-Start
EAPOL-Logoff
EAPOL-Key
EAPOL-Encapsulated-ASF-Alert
EAPOL-MKA
EAPOL-Announcement (Generic)
EAPOL-Announcement (Specific)
EAPOL-Announcement-Req

Message types that can contain PII include the following:

- EAPOL-EAP. This type provides an IEEE 802 framing around EAP (IETF RFC 3748 [B14]) frames, which allow a station to authenticate itself to the network and gain access to the network. Credentials can be user credentials, host credentials, or both.
- EAPOL-MKA. MACsec Key Agreement (MKA) determines session keys for IEEE 802.1AE MAC Security (MACsec). MKA identities (“Member Identifier”) are not persistent. They also carry a MACsec Secure Channel Identifier (SCI) associated with the member.
- EAPOL Announcements. Announcements include capabilities for the station, including information describing a cached, secure Connectivity Association Key (CAK).

Threats:

- a) A passive adversary between the target and EAP authenticator can observe any information that an EAP method passes without confidentiality protection. This threat can be mitigated by using a “tunneled EAP” method [e.g., Tunnel Extensible Authentication Protocol (TEAP) (IETF RFC 7170 [B19])].
- b) An active adversary between the target and EAP authenticator can be able to spoof a legitimate respondent in an EAP method to the point where the target presents its identity (e.g., the subject name in a client certificate).
- c) A passive adversary in the broadcast domain of the target can observe Announcement data and identify or deduce the class of target. The Key Management Domain (KMD) or Network Identity (NID) can identify the organization; the set of announcement data presented can indicate the type of device.

B.5.2 IEEE 802.11 Authentication frames

The Authentication Frame can be used as a request or a response. An adversary can observe specific elements to uniquely identify the sender. An adversary can also generate authentication messages and observe the AP response. From the AP response, the adversary can deduce information about the AP feature support or uniquely fingerprint the AP.

In particular, an adversary can observe the following elements:

- In both the station and AP messages: Mobility Domain element (MDE), Fast BSS Transition element (FTE), RIC element, Multi-band element, and Vendor Specific element.
- Also, in the AP messages: Timeout Interval element, Send Confirm element, Confirm element, and Neighbor Report element.
- Also, in the station messages: Finite Cyclic Group element, Finite Field element, Anti-Clogging Token element, or Scalar element.

B.5.3 IEEE 802.11 Deauthentication frames

Deauthentication frames include reason codes values. Reason codes have been examined in B.5.4 and can be used to fingerprint the AP by listing AP supported features (or unsupported features). Deauthentication frames also include specific elements that can be further used to fingerprint the AP, such as the Management MIC element (MME) or Vendor Specific element.

B.5.4 IEEE 802.11 Disassociation frames

Disassociation frames contain a reason code, one or several Vendor Specific elements, and optionally a Management MIC element when Management Frame Protection is enabled and the frame is addressed to a group. All these elements can be used to uniquely identify the sender and its position in the infrastructure.

In particular, several reason codes can be used to uniquely identify an AP, such as the following:

- Reason code 1 (unspecified) in response to targeted messages
- Reason code 4 (inactivity)
- Reason code 5 (no more STAs)
- Reason code 10 (unacceptable power capabilities)
- Reason code 11 (unacceptable supported channels)

- Reason code 13 (invalid element)
- Reason code 28 (lack of roaming agreement to service provider)
- Reason code 30 (requested service not authorized in this location)
- Reason code 32 (unspecified QoS reason)
- Reason code 33 (not enough bandwidth)
- Reason code 34 (missing acks, too many frames to ack but AP RF conditions prevent sending them)
- Reason code 46 (peer initiated, authorized access limit reached)
- Reason code 47 (AP initiated, due to external service requirements)
- Reason code 53 (mesh max peers STA reached)
- Reason code 56 (mesh max retries)
- Reason code 57 (mesh confirm timeout)
- Reason code 61 (mesh path error, no proxy information for target destination)
- Reason code 62 (mesh path error, no forwarding information for target destination)
- Reason code 63 (mesh path error, destination unreachable)
- Reason code 66 (mesh channel switch for unspecified reason)

The presence or absence of the Management MIC element can also be used to uniquely identify an AP.

B.5.5 IEEE 802.11 Association Request frames

Association Request frames are typically sent by a STA attempting to join a basic service set (BSS). As such, they describe in detail the capabilities of the requesting station. These elements, individually and in combinations, provide multiple ways of uniquely identifying the requesting station.

In particular, the adversary can observe the presence (or absence) and content of the following fields and elements:

- Capability Information field
- Listen Interval field
- Supported Rates and BSS Membership Selectors element
- Extended Supported Rates and BSS Membership Selectors element
- Power Capability element
- Supported Channels element
- QoS Capability element
- RM Enabled Capabilities element
- Mobility Domain element
- Supported Operating Classes element
- HT Capabilities element
- 20/40 BSS Coexistence element
- Extended Capabilities element
- QoS Traffic Capability element
- TIM Broadcast Request element
- Interworking element
- Multi-band element
- DMG Capabilities element

- Multiple MAC Sublayers element
- VHT Capabilities element
- Operating Mode Notification element
- Vendor Specific element

B.5.6 IEEE 802.11 Association Response frames

The Association Response is typically sent in response to the Association Request. As such it contains the capability of the BSS provider (typically an AP). Elements of the response can contain, individually or in combination, enough unique information for an adversary to uniquely identify the sender and its capabilities. Additionally, an adversary can generate Association Request frames that announce various capabilities and observe the response, including the status code, of the AP. With this process, the adversary can trigger the AP to provide extended information about the supported parameters and, in this way, uniquely identify the AP.

In particular, the adversary can observe the following field and elements:

- Capabilities Information field
- Supported Rates and BSS Membership Selectors element
- Extended Supported Rates and BSS Membership Selectors element
- EDCA Parameter Set element
- RCPI element
- RSNI element
- RM Enabled Capabilities element
- Mobility Domain element
- Fast BSS Transition element
- DSE Registered Location element
- Timeout Interval element
- HT Capabilities element
- HT Operation element
- 20/40 BSS Coexistence element
- Overlapping BSS Scan Parameters element
- Extended Capabilities element
- BSS Max Idle Period element
- TIM Broadcast Response element
- QoS Map element
- QMF Policy element
- Multi-band element
- DMG Capabilities element
- DMG Operation element
- Multiple MAC Sublayers element
- Neighbor Report element
- VHT Capabilities element
- VHT Operation element
- Operating Mode Notification element

- Future Channel Guidance element
- Vendor Specific element

B.5.7 IEEE 802.11 Reassociation Request frames

The structure of the Reassociation Request frame is similar to that of the Association Request frame. The Reassociation Request frame contains all the elements that can be found in the Association Request frame.

The Reassociation Request frame also contains the following additional elements that can be used to further uniquely fingerprint the requesting station:

- Current AP Address element
- Fast BSS Transition element
- RIC element
- FMS Request element
- DMS Request element

B.5.8 IEEE 802.11 Reassociation Response frames

The Reassociation Response frame is similar in structure to the Association Response frame. All the elements of the Association Response frame are present in the Reassociation Response frame.

The Reassociation Response frame also contains the following additional elements that can be used to further uniquely fingerprint the responding AP:

- RIC element
- FMS Request element
- DMS Request element

B.6 Directed query or instruction frame

Some protocols implement a mechanism by which an endpoint can query an infrastructure device, or an infrastructure device can query an endpoint, to enable a particular service or perform a specific function. In many cases, the query and its response are optional in the standard. The ability to perform such query, the service queried and/or the reply can be used by an adversary to uniquely identify the endpoint or the infrastructure device. The following subclauses provide examples of such behaviors.

B.6.1 IEEE 802.11 Action frames






Action frames form a large family of management frames that aim to convey specific information or instructions, in specific contexts or for specific capability information exchange. Besides containing information elements that can be used to identify the sender (such as the Vendor Specific element), they are by nature indicative of specific capabilities or specific context mandating a particular action and, as such, can be used to uniquely identify the sender of a frame and the responder. IEEE Std 802.11-2016 describes 162 types of individual action frames, among which 6 were found to be neutral (i.e., not providing unique information about the sender of the destination). All the others can be used by an adversary to uniquely identify the sender or receiver. In some cases, frames can be generated by an adversary to trigger a response and fingerprint the responder.

B.6.2 IEEE 802.11 Action No ACK frames

The structure of the Action No ACK frame is similar to that of the Action frame, with the exception that Action No Ack cannot contain the Mesh Peering Exchange Element or the Management MIC element. However, Action No Ack frames can also contain the Vendor Specific element and can be used to uniquely identify the emitter.

RAISING THE WORLD'S STANDARDS

Connect with us on:

-  **Twitter:** twitter.com/ieeesa
-  **Facebook:** facebook.com/ieeesa
-  **LinkedIn:** linkedin.com/groups/1791118
-  **Beyond Standards blog:** beyondstandards.ieee.org
-  **YouTube:** youtube.com/ieeesa

standards.ieee.org
Phone: +1 732 981 0060