IEEE STANDARDS ASSOCIATION

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

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 802.11aq™-2018
(Amendment to IEEE Std 802.11™-2016
as amended by IEEE Std 802.11ai™-2016,
IEEE Std 802.11ah™-2016,
IEEE Std 802.11aj™-2018,
and IEEE Std 802.11ak™-2018)

IEEE Std 802.11aq™-2018
(Amendment to IEEE Std 802.11™-2016
as amended by IEEE Std 802.11ai™-2016,
IEEE Std 802.11ah™-2016,
IEEE Std 802.11aj™-2018,
and IEEE Std 802.11ak™-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

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 14 June 2018

IEEE-SA Standards Board

Abstract: Modifications to IEEE Std 802.11™-2016, above the physical layer (PHY), to enable delivery of preassociation service discovery information to IEEE 802.11 stations (STAs) are defined in this amendment.

Keywords: amendment, bloom filter, hash function, IEEE 802.11™, IEEE 802.11aq™, preassociation, service discovery

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

PDF: ISBN 978-1-5044-5066-9 STD23224
Print: ISBN 978-1-5044-5067-6 STDPD23224

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents." They can also be obtained on request from IEEE or viewed at https://standards.ieee.org/IPR/disclaimers.html.

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

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association ("IEEE-SA") Standards Board. IEEE ("the Institute") develops its standards through a consensus development process, approved by the American National Standards Institute ("ANSI"), which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups are not necessarily members of the Institute 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 Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. 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.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. 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: PROCUREMENT OF 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 should be considered 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, or 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 his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide 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 revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854 USA

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 imply 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.

Copyrights

Photocopies

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. A current 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 ten years. When a document is more than ten 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 the IEEE-SA Website at https://ieeexplore.ieee.org or contact IEEE at the address listed previously. For more information about the IEEE SA or IEEE's standards development process, visit the IEEE-SA Website at https://standards.ieee.org.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE-SA Website at the following URL: https://standards.ieee.org/findstds/errata/index.html. Users are encouraged to check this URL for errata periodically.

Patents

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.

Participants

At the time this amendment was submitted to the IEEE-SA Standards Board for approval, the IEEE 802.11 Working Group had the following officers:

Dorothy V. Stanley, *Chair*
Jon W. Rosdahl, *Vice Chair*
Stephen McCann, *Secretary*
Robert Stacey and **Peter Ecclesine,** *Technical Editors*

At the time this amendment was submitted for balloting, the IEEE 802.11aq Task Group had the following membership:

Stephen McCann, *Chair*
Yunsong Yang, *Vice Chair*
Lee Armstrong, *Technical Editor*

Mohamed Abouelseoud
Osama Aboulmagd
Tomoko Adachi
Shubhodeep Adhikari
Jinsoo Ahn
Woojin Ahn
Kosuke Aio
Carlos Aldana
Yaron Alpert
Song-Haur An
Amelia Andersdotter
Carol Ansley
Yusuke Asai
Alfred Asterjadhi
Kwok Shum Au
Vijay Auluck
Geert Awater
Shahrnaz Azizi
Robert Baeten
Eugene Baik
Stephane Baron
Anuj Batra
Jianwei Bei
Friedbert Berens
Christian Berger
Nehru Bhandaru
Harry Bims
John Buffington
George Calcev
Rui Cao
Laurent Cariou
William Carney
Ricky Chair
Soo-Young Chang
Clint Chaplin
Cheng Chen
Jiamin Chen
Teyan Chen
Xiaogang Chen
George Cherian
Dmitry Cherniavsky
Rojan Chitrakar
Jinsoo Choi
Liwen Chu
Jinyoung Chun
Dana Ciochina
John Coffey
Carlos Cordeiro
Perry Correll
D. Nelson Costa
Claudio da Silva
Subir Das
Rolf de Vegt
Pierre Debergh
Thomas Derham
Donald Eastlake
Peter Ecclesine
Richard Edgar
Alecsander Eitan
Marc Emmelmann
Vinko Erceg
Andrew Estrada
Yonggang Fang
Xiang Feng
Norman Finn
Matthew Fischer
Michael Fischer
Jeremy Foland
Shunsuke Fujio
Sho Furuichi
Ming Gan
Eduard Garcia Villegas
Chittabrata Ghosh
James Gilb
Sachin Godbole
Tim Godfrey
Niranjan Grandhe
Michael Grigat
Qiang Guo
Yuchen Guo
Robert Hall
Mark Hamilton
Xiao Han
Thomas Handte
Christopher Hansen
Chris Hartman
Victor Hayes
Allen Heberling
Ahmadreza Hedayat
Robert Heile
Guido Hiertz
Duncan Ho
Jay Holcomb
Hanseul Hong
Chunyu Hu
Lei Huang
Po-Kai Huang
Zhiyong Huang
Sung Hyun Hwang
Yasuhiko Inoue
Timothy Jeffries
Chenlong Jia
Jia Jia
Feng Jiang
Jinjing Jiang
Liang Jin
Allan Jones
Jeffrum Jones
Vincent Knowles Jones
Volker Jungnickel
Christophe Jurczak
Carl Kain
Naveen Kakani
Teag Jin Kang
Dzevdan Kapetanovic
Assaf Kasher
Oren Kedem
Richard Kennedy
Stuart Kerry
Evgeny Khorov
Jeong Gon Kim
Jeongki Kim
Jin Min Kim
Sang Gook Kim
Suhwook Kim
Yongho Kim
Youhan Kim
Youn-Kwan Kim
Jarkko Kneckt
Geonjung Ko
Bruce Kraemer
Manish Kumar

Massinissa Lalam
Zhou Lan
Leonardo Lanante
James Lansford
Jae Seung Lee
Sungeun Lee
Wookbong Lee
Suzanne Leicht
James Lepp
Joseph Levy
Bo Li
Dejian Li
Guoqing Li
Huan-Bang Li
Qiang Li
Qinghua Li
Yanchun Li
Yunbo Li
Dandan Liang
Dong Guk Lim
Wei Lin
Yingpei Lin
Erik Lindskog
Chenchen Liu
Der-Zheng Liu
Jianhan Liu
Jinnan Liu
Yingzhuang Liu
Yong Liu
Yong Liu
Peter Loc
Hui-Ling Lou
Kaiying Lv
Lily Lv
Jing Ma
Mengyao Ma
Nitin Madan
Narendar Madhavan
Girish Madpuwar
Jouni Malinen
Alexander Maltsev
Hiroshi Mano
Roger Marks
Simone Merlin
Jianhua Mo
Apurva Mody
Bibhu Mohanty
Pooya Monajemi
Bruce Montag
Michael Montemurro
Hitoshi Morioka
Yuichi Morioka
Hiroyuki Motozuka
Robert Mueller
Yutaka Murakami
Andrew Myles
Sai Shankar Nandagopalan
Patrice Nezou
Paul Nikolich
Yujin Noh
John Notor
Minseok Oh
Oghenekome Oteri
Kazuyuki Ozaki
Stephen Palm
Eunsung Park
Minyoung Park
Sung-jin Park
Glenn Parsons
Abhishek Patil
Gaurav Patwardhan
James Petranovich
Albert Petrick
Brian Petry
Ambroise Popper
Ron Porat
Rethnakaran Pulikkoonattu
Emily Qi
Dengyu Qiao
Demir Rakanovic
Enrico-Henrik Rantala
Maximilian Riegel
Mark Rison
Zhigang Rong
Jon Rosdahl
Kiseon Ryu
Bahareh Sadeghi
Takenori Sakamoto
Kazuyuki Sakoda
Sam Sambasivan
Hemanth Sampath
Naotaka Sato
Sigurd Schelstraete
Andy Scott
Jonathan Segev
Yongho Seok
Julien Sevin
Stephen Shellhammer
Ian Sherlock
Shimi Shilo
Graham Smith
Ju-Hyung Son
Sudhir Srinivasa
Robert Stacey
Dorothy Stanley
Adrian Stephens
Noel Stott
Jung Hoon Suh
Takenori Sumi
Bo Sun
Li-Hsiang Sun
Sheng Sun
Yanjun Sun
Dennis Sundman
Mineo Takai
Yusuke Tanaka
Mukesh Taneja
Kentaro Taniguchi
Wu Tao
Bin Tian
Fei Tong
Payam Torab
Eric Torkildson
Solomon Trainin
Genadiy Tsodik
Yoshio Urabe
Richard Van Nee
Allert Van Zelst
Jerome Vanthournout
Prabodh Varshney
Ganesh Venkatesan
Lochan Verma
Sindhu Verma
Sameer Vermani
Pascal Viger
George Vlantis
Chao Chun Wang
Haiming Wang
Huizhao Wang
James June Wang
Lei Wang
Qian Wang
Xiaofei Wang
Xuehuan Wang
Lisa Ward
Julian Webber
Menzo Wentink
Leif Wilhelmsson
Jianbing Wu
Tianyu Wu
Kaifeng Xia
Yan Xin
Han Xu
Qi Xue
Min Yan
Zhongjiang Yan
Bo Yang
Mao Yang
Rui Yang
Xun Yang
Kazuto Yano
James Yee
Peter Yee
Su Khiong Yong
Christopher Young
Bo Yu
Jian Yu
Mao Yu
SunWoong Yun
Alan Zeleznikar
Hongyuan Zhang
Jiayin Zhang
Xingxin Zhang
Yan Zhang
Lei Zheng
Xiayu Zheng
Jun Zhu
Lan Zhuo
Xin Zuo

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

Santosh Abraham
Tomoko Adachi
Iwan Adhicandra
Thomas Alexander
Nobumitsu Amachi
Carol Ansley
Butch Anton
Lee Armstrong
Alfred Asterjadhi
Kwok Shum Au
Madhusudan Banavara
Harry Bims
Gennaro Boggia
Nancy Bravin
William Byrd
William Carney
Juan Carreon
Keith Chow
Charles Cook
Patrick Diamond
Yezid Donoso
Sourav Dutta
Richard Edgar
Marc Emmelmann
Michael Fischer
Avraham Freedman
Joel Goergen
David Goodall
Eric W. Gray
Randall Groves
Michael Gundlach
Mark Hamilton
Chris Hartman
Jerome Henry
Marco Hernandez
Guido Hiertz
Werner Hoelzl
David Hunter
Noriyuki Ikeuchi
Yasuhiko Inoue
Sergiu Iordanescu
Akio Iso
Atsushi Ito
Raj Jain
Sangkwon Jeong
Richard Kennedy
Jeritt Kent
Stuart Kerry
Yongbum Kim
Youhan Kim
Jarkko Kneckt
Bruce Kraemer
Yasushi Kudoh
Warren Kumari
George Kyle
Hyeong Ho Lee
Jae Seung Lee
James Lepp
Joseph Levy
Arthur H. Light
Elvis Maculuba
Jouni Malinen
Roger Marks
Jeffery Masters
Stephen McCann
Michael McInnis
Michael Montemurro
Matthew Mora
Ronald Murias
Rick Murphy
Michael Newman
Charles Ngethe
John Notor
Satoshi Obara
Robert O'Hara
Satoshi Oyama
Arumugam Paventhan
Clinton Powell
Venkatesha Prasad
Maximilian Riegel
Robert Robinson
Benjamin Rolfe
Jon W. Rosdahl
Naotaka Sato
Andy Scott
Michael Seaman
Yongho Seok
Ian Sherlock
Di Dieter Smely
Ju-Hyung Son
Kapil Sood
Dorothy V. Stanley
Thomas Starai
Adrian P. Stephens
Rene Struik
Walter Struppler
Mark Sturza
Bo Sun
Pedro Tonhozi de Oliveira
Payam Torab
Mark-Rene Uchida
Lorenzo Vangelista
Dmitri Varsanofiev
Prabodh Varshney
George Vlantis
Khurram Waheed
Lei Wang
Xiaofei Wang
Karl Weber
Hung-Yu Wei
Chun Yu Charles Wong
Yunsong Yang
Su Khiong Yong
Oren Yuen
Zhen Zhou

When the IEEE-SA Standards Board approved this amendment on 14 June 2018, it had the following membership:

Jean-Philippe Faure, *Chair*
Gary Hoffman, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Ted Burse
Guido R. Hiertz
Christel Hunter
Joseph L. Koepfinger*
Thomas Koshy
Hung Ling
Dong Liu
Xiaohui Liu
Kevin Lu
Daleep Mohla
Andrew Myles
Paul Nikolich
Ronald C. Petersen
Annette D. Reilly
Robby Robson
Dorothy Stanley
Mehmet Ulema
Phil Wennblom
Philip Winston
Howard Wolfman
Jingyi Zhou

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 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.

This amendment defines 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. It defines modifications to IEEE Std 802.11-2016, above the physical layer (PHY), to enable delivery of preassociation service discovery information to IEEE 802.11 stations (STAs).

Contents

Tables

Figures

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

This amendment is based on IEEE Std 802.11™-2016 as amended by IEEE Std 802.11ai™-2016, IEEE Std 802.11ah™-2016, IEEE Std 802.11aj™-2018, and IEEE Std 802.11ak™-2018.

NOTE—The editing instructions contained in this amendment define how to merge the material contained therein into the existing base standard and its amendments to form the comprehensive standard.

The editing instructions are shown in ***bold italic***. Four editing instructions are used: ***change, delete, insert, and replace***. Change is used to make corrections in existing text or tables. The editing instructions specifies the location of the change and describes what is being changed by using ~~strike through~~ (to remove old material) and underscore (to add new material). ***Delete*** removes existing material. ***Insert*** adds new material without disturbing the existing material. Insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. ***Replace*** is used to make changes in figures or equations by removing the existing figure or equation and replacing it with a new one. Editorial notes will not be carried over into future editions because the changes will be incorporated into the base standard.[1]

1. Overview

1.3 Supplementary information on purpose

Insert the following item at the end of the dashed list in 1.3:

— Defines mechanisms to enable delivery of preassociation service discovery information to IEEE 802.11 stations (STAs).

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

2. Normative references

Insert the following normative references into Clause 2 in alphanumeric order:

IEEE Std 802c™-2017, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture Amendment 2: Local Medium Access Control (MAC) Address Usage.[1,2]

IETF RFC 6335, Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry, August 2011.[3]

3. Definitions, acronyms, and abbreviations

3.1 Definitions

Insert the following definition into 3.1 in alphabetic order:

service hash: A value used for representing a service. This value is formed from a hash of the service name.

3.2 Definitions specific to IEEE Std 802.11

Insert the following definitions into 3.2 in alphabetic order:

service information client (SIC): A logical entity that initiates station (STA) service discovery.

service information registry (SIR): A logical entity that contains caches of information about services that are available via the basic service set (BSS).

3.4 Abbreviations and acronyms

Insert the following abbreviations into 3.4 in alphabetic order:

PAD	preassociation discovery
SIC	service information client
SIR	service information registry
SLAP	Structured Local Address Plan

[1] IEEE publications are available from The Institute of Electrical and Electronic Engineers (http://standards.ieee.org/).
[2] The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronic Engineers, Inc.
[3] IEFT documents (i.e., RFCs) are available from the Internet Engineering Task Force (http://tools.ieft.org/html/).

4. General description

4.5 Overview of the services

4.5.4 Access control and data confidentiality services

Insert the following subclause (4.5.4.10) after 4.5.4.9:

4.5.4.10 MAC privacy enhancements

When a non-AP STA searches for, and connects to, an infrastructure BSS, IBSS, or PBSS or attempts to discover services on a network preassociation, it defines the addressing of its MAC layer for the particular connection. If the STA uses a fixed MAC address it is trivial to track the STA. An MSDU transmitted by a STA is assigned a sequence number that, if never reset, can also be used to track a device irrespective of the MAC address. If OFDM is used, the PHY DATA scrambler used can enable tracking of a device irrespective of the MAC address if it is not reseeded. The dynamic nature of BSS membership combined with this tracking information allows for construction of a network of connections, locations, and behavior. This network can be used to glean private and sensitive information regarding the individual behind the device.

Furthermore, even without establishing a connection, a mobile or portable STA that gratuitously transmits Probe Request frames containing SSIDs of favored infrastructure BSS networks, or announces the existence of IBSS networks, can reveal potentially sensitive information about its location and location history.

To mitigate this sort of traffic analysis a STA can support the ability to periodically and randomly change its MAC addresses and reset counters and seeds prior to association. While discovering networks, a STA can refrain from gratuitously transmitting Probe Request frames containing SSIDs of favored BSS networks.

4.5.9 Interworking with external networks

Insert the following subclause heading (4.5.9.1), and change the text (originating from the former 4.5.9) of the now 4.5.9.1 as shown:

4.5.9.1 General

The interworking service allows non-AP STAs to access services provided by an external network according to the subscription or other characteristics of that external network. An IEEE Std 802.11 non-AP STA might have a subscription relationship with an external network, e.g., with an SSPN.

An overview of the interworking functions addressed in this standard is provided below:

- Network discovery and selection
  - Discovery of suitable networks through the advertisement of access network type, roaming consortium and venue information, via Management frames
  - Selection of a suitable IEEE 802.11 infrastructure using advertisement services (e.g., access network query protocol (ANQP) or an IEEE 802.21™ Information Server) in the BSS or in an external network reachable via the BSS.
  - Selection of an SSPN or external network with its corresponding IEEE 802.11 Infrastructure
- Preassociation discovery (PAD)
  - Discovery of services offered by a BSS or an external network reachable via that BSS

- Emergency services
  - Emergency Call and Network Alert support at the link level
- QoS mapping distribution
- SSPN interface service between the AP and the SSPN

The generic advertisement service (GAS), described in 4.5.10, provides both support for a STA's network discovery and selection, and support for a conduit for communication by a non-AP STA with other information resources in a network before joining the wireless LAN.

The interworking service supports emergency services by providing methods for users to access emergency services via the IEEE 802.11 infrastructure, advertising that emergency services are supported (see 11.25.6) and identifying that a traffic stream is used for emergency services.

The interworking service provides QoS mapping for SSPNs and other external networks. Since each SSPN or other external network might have its own layer-3 end-to-end packet marking practice (e.g., differentiated services code point (DSCP) usage conventions), a means to remap the layer-3 service levels to a common over-the-air service level is necessary. The QoS Map service provides STAs a mapping of network-layer QoS packet marking to over-the-air QoS frame marking (i.e., user priority).

The SSPN Interface service supports service provisioning and transfer of user permissions from the SSPN to the AP. The method and protocol by which these permissions are transferred from the SSPN are outside the scope of this standard.

Insert the following subclause (4.5.9.2, including Figure 4-15a and Figure 4-15b) after 4.5.9.1:

4.5.9.2 Preassociation discovery (PAD)

4.5.9.2.1 Introduction

PAD is an interworking function provided by a BSS to allow a non-AP and non-PCP STA, prior to association, to discover information concerning services that might be available to the STA when it is associated with the BSS. PAD provides a method for the STA to gather information to aid in the decision to select a BSS with which to associate.

4.5.9.2.2 Architecture

Figure 4-15a and Figure 4-15b show the functional flow of MAC messaging and service information between a service information client (SIC) and a service information registry (SIR). These entities are described in 4.5.9.2.3, 4.5.9.2.4, and 4.5.9.2.5. The active components within the architecture differ depending upon whether unsolicited or solicited PAD is being used.

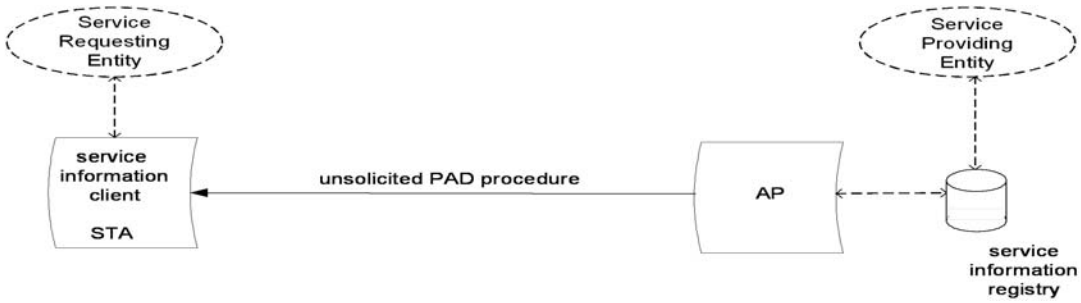

Figure 4-15a—Unsolicited PAD architecture

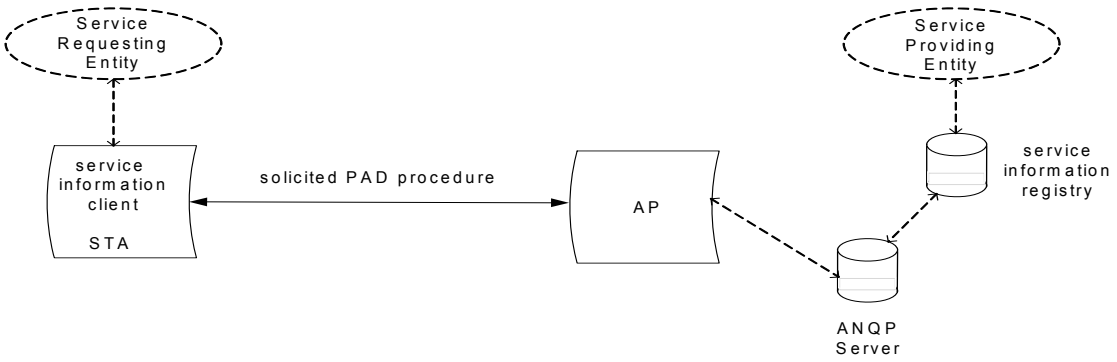

Figure 4-15b—Solicited PAD architecture

NOTE—A SIR can be either co-located with the AP or outside the AP. An SIR can only be co-located with a PCP. The communications between the SIR and the AP, together with the SIR and the ANQP server are out of the scope of this standard.

The unsolicited PAD procedure is described in11.25a.2 and solicited PAD procedure is described in 11.25a.3.

4.5.9.2.3 Service information entities

The SIC and SIR are used to exchange PAD service information. The PAD procedures operate between the SIC and SIR.

4.5.9.2.4 Service information registry (SIR)

The SIR caches information about services that might be reachable via the BSS and therefore might be available to the STA once the STA is associated with that BSS. How the SIR obtains the information about services is outside the scope of this standard.

There is typically one SIR assigned to each ESS. It can be addressed by each AP and each service within that ESS. It includes supporting service discovery requests and responses from the BSS.

The SIR communicates with the ANQP server to respond to ANQP requests.

4.5.9.2.5 Service information client (SIC)

The SIC initiates service discovery. The SIC exchanges service discovery requests and responses between the SME and applications.

The SME determines whether to use unsolicited PAD or solicited PAD procedures. The SME also composes ANQP requests for solicited PAD procedures.

6. Layer management

6.3 MLME SAP interface

6.3.3 Scan

6.3.3.3 MLME-SCAN.confirm

6.3.3.3.2 Semantics of the service primitive

Insert the following rows at the end of the untitled BSS Description parameter table in 6.3.3.3.2:

Name	Type	Valid range	Description	IBSS adoption
ServiceHint	Service Hint element	As defined in 9.4.2.233	Provides an indication of the services advertised in Beacon frames and Probe Response frames. The values from the Service Hint element, if such an element was present in the Beacon or Probe Response frame; else null.	Do not adopt
ServiceHash	Service Hash element	As defined in 9.4.2.234	Specifies services advertised in Beacon and Probe Response frames. The values from the Service Hash element, if such an element was present in the Beacon or Probe Response frame; else null.	Do not adopt

6.3.11 Start

6.3.11.2 MLME-START.request

6.3.11.2.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.11.2.2 as follows:

MLME-START.request(
SSID,
BSSType,
BeaconPeriod,
DTIMPeriod,
CF parameter set,
PHY parameter set,
IBSS parameter set,
NAVSyncDelay,
CapabilityInformation,
BSSBasicRateSet,
OperationalRateSet,
Country,
IBSS DFS Recovery Interval,
EDCAParameterSet,

DSERegisteredLocation,
HT Capabilities,
HT Operation,
BSSMembershipSelectorSet,
Extended Capabilities,
20/40 BSS Coexistence,
Overlapping BSS Scan Parameters,
MultipleBSSID,
InterworkingInfo,
AdvertisementProtocolInfo,
RoamingConsortiumInfo,
Mesh ID,
Mesh Configuration,
QMFPolicy,
DMG Capabilities,
Multi-band,
MMS,
DMG Operation,
Clustering Control,
CBAP Only,
PCP Association Ready,
VHT Capabilities,
VHT Operation,
Known OUIs,
S1G Capabilities,
S1GOperations,
ShortBeaconPeriod,
ShortBeaconDTIMPeriod,
CDMG Capabilities,
CMMG Capabilities,
CMMG Operation,
ServiceHint,
ServiceHash,
VendorSpecificInfo
)

Insert the following rows into the untitled parameter table in 6.3.11.2.2 before the "VendorSpecificInfo" row:

Name	Type	Valid range	Description
ServiceHint	Service Hint element	As defined in 9.4.2.233	Provides an indication of the services advertised in Beacon and Probe Response frames. The element is optionally present if dot11UnsolicitedPADActivated is true and absent otherwise.
ServiceHash	Service Hash element	As defined in 9.4.2.234	Specifies services advertised in Beacon and Probe Response frames. The element is optionally present if dot11UnsolicitedPADActivated is true and absent otherwise.

6.3.73 Network discovery and selection support

6.3.73.2 MLME-GAS.request

6.3.73.2.2 Semantics of the service primitive

Change 6.3.73.2.2 as follows:

The primitive parameters are as follows:

MLME-GAS.request(
~~Peer~~STAAddress,
DialogToken,
AdvertisementProtocolID,
Query,
QueryFailureTimeout,
Protected,
Multi-band,
GAMode,
GASExtension,
CAGNumber,
VendorSpecificInfo
)

Name	Type	Valid range	Description
~~Peer~~STAAddress	MacAddress	Any valid individual MacAddress. For a group address GAS frame, this is the broadcast address.	Specifies the address of the peer MAC entity or the broadcast address to which query is transmitted.
DialogToken	Integer	0–255	The dialog token to identify the GAS transaction.
AdvertisementProtocolID	Integer or Sequence of integers	As defined in Table 9-215	This contains an Advertisement Protocol ID (see 9.4.2.93), which might be IEEE Std 802.11 assigned or vendor specified.
Query	String	N/A	Query string formatted using protocol identified in AdvertisementProtocolID. E.g., if the AdvertisementProtocolID value is 1, then Query is formatted as defined in IEEE Std 802.21-2008.
QueryFailureTimeout	Integer	> 1	The time limit, in units of beacon intervals, after which the GAS Query procedure is terminated.
Protected	Boolean	true, false	Specifies whether the request is sent using a robust Management frame. If true, the request is sent using a Protected Dual of Public Action frame. Otherwise, the request is sent using a Public Action frame.
Multi-band	Multi-band element	As defined in 9.4.2.138	Specifies the frequency band and channel number to which the GAS transaction applies. The parameter is absent if the GAS transaction applies to the same frequency band and channel where the frame is transmitted.
GAMode	Boolean	true, false	If true, the request is sent using a group address GAS frame. Otherwise, the request is sent using a unicast GAS frame.

Name	Type	Valid range	Description
GASExtension	GAS Extension element	As defined in 9.4.2.235	Specifies GAS extensions information in the GAS frame to be transmitted. This parameter is optionally present if dot11GASExtensionImplemented is true; otherwise not present.
CAGNumber	CAG Number element	As defined in 9.4.2.177	One or more Common Advertisement Group (CAG) tuples. Each CAG Tuple specifies a pair of CAG Version and CAG Information Type cached by the transmitting STA. This parameter is optionally present when dot11FILSActivated is true or dot11SolicitedPADActivated is true; otherwise not present.
VendorSpecificInfo	A set of elements	As defined in 9.4.2.26	Zero or more elements.

6.3.73.2.4 Effect of receipt

Change 6.3.73.2.4 as follows:

The STA operates according to the procedures defined in 11.25.3 and 11.25a.

6.3.73.3 MLME-GAS.confirm

6.3.73.3.2 Semantics of the service primitive

Change 6.3.73.3.2 as follows:

The primitive parameters are as follows:

MLME-GAS.confirm(
~~Peer~~STAAddress,
DialogToken,
ResultCode,
ResponseInfo,
Protected,
Multi-band,
GASExtension,
VendorSpecificInfo
)

Name	Type	Valid range	Description
~~Peer~~STAAddress	Mac Address	Any valid individual MacAddress	Specifies the address of the peer MAC entity from ~~to~~ which Qquery Response is received~~transmitted~~.
DialogToken	Integer	0–255	The dialog token to identify the GAS transaction.

Name	Type	Valid range	Description
ResultCode	Enumeration	SUCCESS, NO_OUTSTANDING_GAS_REQUEST, GAS_ADVERTISEMENT_PROTOCOL_ NOT_SUPPORTED, GAS_QUERY_RESPONSE_ OUTSTANDING, GAS_QUERY_RESPONSE_TOO_LARGE, SERVER_UNREACHABLE, GAS_QUERY_TIMEOUT, GAS_RESPONSE_NOT_RECEIVED_ FROM_SERVER, SUCCESS_CAG_VERSIONS_MATCH	Indicates the result response to the GAS request from the peer MAC entity.
ResponseInfo	String	N/A	Query Response string formatted using protocol identified in AdvertisementProtocolID. E.g., if the AdvertisementProtocolID value is 1, then Query is formatted as defined in IEEE Std 802.21-2008.
Protected	Boolean	true, false	Specifies whether the response was received in a robust Management frame. If true, the response was received using a Protected Dual of Public Action frame. Otherwise, the response was received using a Public Action frame.
Multi-band	Multi-band element	As defined in 9.4.2.138	Specifies the frequency band and channel number to which the GAS transaction applies. The parameter is absent if the GAS transaction applies to the same frequency band and channel where the frame is transmitted.
GASExtension	GAS Extension element	As defined in 9.4.2.235	Specifies GAS extensions information in the GAS frame received. The values from the GAS Extension element in the GAS response received, if present; else null.
VendorSpecificInfo	A set of elements	As defined in 9.4.2.26	Zero or more elements.

Change 6.3.73.3.3 and 6.3.73.3.4 as follows:

6.3.73.3.3 When generated

This primitive is generated by the MLME as a response to the MLME-GAS.request primitive indicating the result of that request.

The primitive is generated when the requesting STA receives a query response in a (Protected) GAS Initial Response frame, or one or more (Protected) GAS Comeback Response frames, or a Group Addressed GAS Response frame.

6.3.73.3.4 Effect of receipt

The STA operates according to the procedures defined in 11.25.3 and 11.25a.

6.3.73.4 MLME-GAS.indication

6.3.73.4.2 Semantics of the service primitive

Change 6.3.73.4.2 as follows:

The primitive parameters are as follows:

MLME-GAS.indication(
PeerSTAAddress,
DialogToken,
AdvertisementProtocolID,
Query,
Protected,
Multi-band,
GAMode,
GASExtension,
CAGNumber,
VendorSpecificInfo
)

Name	Type	Valid range	Description
PeerSTAAddress	MacAddress	Any valid individual MAC address	Specifies the address of the peer MAC entity from which the query message was received.
DialogToken	Integer	0–255	The dialog token to identify the GAS transaction.
AdvertisementProtocolID	Integer or Sequence of integers	As defined in Table 9-215	This contains an Advertisement Protocol ID (see 9.4.2.93), which might be IEEE 802.11 assigned or vendor specified.
Query	String	N/A	Query string formatted using protocol identified in AdvertisementProtocolID. E.g., if the AdvertisementProtocolID value is 1, then Query is formatted as defined in IEEE Std 802.21-2008.
Protected	Boolean	true, false	Specifies whether the request was received in a robust Management frame. If true, the request was received in a Protected Dual of Public Action frame. Otherwise, the request was received in a Public Action frame.
Multi-band	Multi-band element	As defined in 9.4.2.138	Specifies the frequency band and channel number to which the GAS transaction applies. The parameter is absent if the GAS transaction applies to the same frequency band and channel where the frame is transmitted.
GAMode	Boolean	true, false	Set to true if the request is received in a Group Addressed GAS Request frame; otherwise set to false.

Name	Type	Valid range	Description
GASExtension	GAS Extension element	As defined in 9.4.2.235	Specifies GAS extensions information in the GAS frame received. The values from the GAS Extension element in the GAS request received, if present; else null.
CAGNumber	CAG Number element	As defined in 9.4.2.177	One or more Common Advertisement Group (CAG) tuples. Each CAG Tuple specifies a pair of CAG Version and CAG Information Type received from a requesting STA.
VendorSpecificInfo	A set of elements	As defined in 9.4.2.26	Zero or more elements.

6.3.73.4.4 Effect of receipt

Change 6.3.73.4.4 as follows:

The SME is notified of the request from the STA.

The SME operates according to the procedures defined in 11.25.3 and 11.25a.

The SME generates an MLME-GAS.response primitive within a dot11GASResponseTimeout.

6.3.73.5 MLME-GAS.response

6.3.73.5.2 Semantics of the service primitive

Change 6.3.73.5.2 as follows:

The primitive parameters are as follows:

MLME-GAS.response(
~~Peer~~STAAddress,
DialogToken,
ResultCode,
ResponseInfo,
Protected,
Multi-band,
GAMode,
GASExtension,
VendorSpecificInfo
)

Name	Type	Valid range	Description
~~Peer~~STAAddress	Mac Address	Any valid individual MAC address. For a group address GAS frame, this is the broadcast address.	Specifies the address of the ~~peer~~ MAC entity or the broadcast address to which the query response information is transmitted.
DialogToken	Integer	0–255	The dialog token to identify the GAS transaction.

Name	Type	Valid range	Description
ResultCode	Enumeration	SUCCESS, NO_OUTSTANDING_GAS_REQUEST, GAS_ADVERTISEMENT_PROTOCOL_ NOT_SUPPORTED, GAS_QUERY_RESPONSE_ OUTSTANDING, GAS_QUERY_RESPONSE_TOO_LARGE, SERVER_UNREACHABLE, GAS_QUERY_TIMEOUT, GAS_RESPONSE_NOT_RECEIVED_ FROM_SERVER, SUCCESS_CAG_VERSIONS_MATCH	Indicates the result response to the GAS-request from the peer MAC entity. See Table 9-46.
ResponseInfo	String	N/A	Query Response string formatted using protocol identified in AdvertisementProtocolID. E.g., if the AdvertisementProtocolID value is 1, then Query is formatted as defined in IEEE Std 802.21-2008.
Protected	Boolean	true, false	Specifies whether the response is sent using a robust Management frame. If true, the response is sent using a Protected Dual of Public Action frame. Otherwise, the response is sent using a Public Action frame.
Multi-band	Multi-band element	As defined in 9.4.2.138	Specifies the frequency band and channel number to which the GAS transaction applies. The parameter is absent if the GAS transaction applies to the same frequency band and channel where the frame is transmitted.
GAMode	Boolean	true, false	Specifies whether the response is sent using a group address GAS frame. If true, the response is sent using a group address GAS frame. Otherwise, the response is sent using a unicast GAS frame.

Name	Type	Valid range	Description
GASExtension	GAS Extension element	As defined in 9.4.2.235	Specifies GAS extensions information in the GAS frame to be transmitted. The parameter is present if GAMode is true, or if the STA is capable of retransmitting a GAS Query Response fragment upon request and the query response's length is larger than the maximum MMPDU size; else the parameter is null.
VendorSpecificInfo	A set of elements	As defined in 9.4.2.26	Zero or more elements.

6.3.73.5.4 Effect of receipt

Change 6.3.73.5.4 as follows:

This primitive causes the MAC entity at the STA to send a (Protected) GAS Initial Response frame to the requesting STA and optionally one or more (Protected) GAS Comeback Response frames or one Group Addressed GAS Response frame.

Insert the following subclause (6.3.119) after 6.3.118.9.4:

6.3.119 Update

6.3.119.1 Introduction

This mechanism supports the process of updating one or more parameters used in the BSS without restarting the BSS.

6.3.119.2 MLME-UPDATE.request

6.3.119.2.1 Function

This primitive requests that the MAC entity to initiate a BSS update procedure to update one or more parameters used in the BSS without restarting the BSS.

6.3.119.2.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-UPDATE.request(
                        ServiceHint,
                        ServiceHash,
                        VendorSpecificInfo
                        )
```

Name	Type	Valid range	Description
ServiceHint	Service Hint element	As defined in 9.4.2.233	If null, requests that Service Hint element be removed from Beacon and Probe Response frames. Otherwise, provides an indication of the services advertised in Beacon and Probe Response frames. The parameter is optionally present if dot11UnsolicitedPAD-Activated is true and absent otherwise.
ServiceHash	Service Hash element	As defined in 9.4.2.234	If null, requests that Service Hash element be removed from Beacon and Probe Response frames. Otherwise, specifies services advertised in Beacon and Probe Response frames. The parameter is optionally present if dot11UnsolicitedPAD-Activated is true and absent otherwise.
VendorSpecificInfo	A set of elements	As defined in 9.4.2.26	Zero or more elements.

6.3.119.2.3 When generated

This primitive is generated by the SME of an AP or PCP STA when one or more parameters used in the BSS are to be changed without restarting the BSS.

6.3.119.2.4 Effect of receipt

If the MLME of an AP or PCP STA receives an MLME-UPDATE.request primitive with ServiceHint and/or ServiceHash parameters, the AP or PCP STA shall use these parameters to update or remove the Service Hint element and/or Service Hash element in Beacon and Probe Response frames that the AP transmits or in DMG Beacon, Announce, and Probe Response frames that the PCP STA transmits.

6.3.119.3 MLME_UPDATE.confirm

6.3.119.3.1 Function

This primitive reports the results of a BSS update procedure.

6.3.119.3.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-UPDATE.confirm(
                        ResultCode
                        )
```

Name	Type	Valid range	Description
ResultCode	Enumeration	SUCCESS, BSS_NOT_STARTED, NOT_SUPPORTED, UPDATE_FAILED	Indicates the result of the MLME-UPDATE.request primitive.

6.3.119.3.3 When generated

This primitive is generated by the MLME as a result of an MLME-UPDATE.request primitive to update one or more parameters used in the BSS without restarting the BSS.

6.3.119.3.4 Effect of receipt

The SME is notified of the results of the BSS update procedure.

9. Frame formats

9.3 Format of individual frame types

9.3.3 Management frames

9.3.3.3 Beacon frame format

Insert the following rows into Table 9-27 in numeric order:

Table 9-27—Beacon frame body

Order	Information	Notes
72	Service Hint	The Service Hint element is optionally present if dot11UnsolicitedPADActivated is true.
73	Service Hash	The Service Hash element is optionally present if dot11UnsolicitedPADActivated is true.

9.3.3.11 Probe Response frame format

Insert the following rows into Table 9-34 in numeric order:

Table 9-34—Probe Response frame body

Order	Information	Notes
89	Service Hint	The Service Hint element is optionally present if dot11UnsolicitedPADActivated is true.
90	Service Hash	The Service Hash element is optionally present if dot11UnsolicitedPADActivated is true.

9.3.4.2 DMG Beacon

Insert the following rows into Table 9-41 in numeric order:

Table 9-41—DMG Beacon frame body

Order	Information	Notes
54	Service Hint	The Service Hint element is optionally present if dot11UnsolicitedPADActivated is true.
55	Service Hash	The Service Hash element is optionally present if dot11UnsolicitedPADActivated is true.

9.4 Management and Extension frame body components

9.4.1 Fields that are not elements

9.4.1.9 Status Code field

Insert the following rows into Table 9-46 in numeric order:

Table 9-46—Status codes

Status code	Name	Meaning
120	GAS_FRAGMENT_ NOT_AVAILABLE	The requested GAS fragment is not available.
121	SUCCESS_CAG_VERSIONS_MATCH	Success, the CAG Version provided by the requesting STA is the same as the latest CAG Version provided by the relevant server.

9.4.2 Elements

9.4.2.1 General

Insert the following rows into Table 9-77 in numeric order:

Table 9-77—Element IDs

Element	Element ID	Element ID Extension	Extensible	Fragmentable
Service Hint (see 9.4.2.233)	255	15	No	No
Service Hash (see 9.4.2.234)	255	16	No	No
GAS Extension (see 9.4.2.235)	255	40	Yes	Yes

9.4.2.27 Extended Capabilities element

Insert the following rows into Table 9-135 in numeric order:

Table 9-135—Extended Capabilities field

Bit	Information	Notes
75	PAD	Indicates support for PAD (see 11.25a).

9.4.2.177 CAG Number element

Change 9.4.2.177 as follows:

The Common Advertisement Group (CAG) is a group of elements that are defined by the same advertisement protocol and that do not change on a rapid basis within an AP. The CAG Number element provides one or more current version numbers of the CAG (CAG Version) associated with the AP, where each version number is associated with a specific advertisement protocol and server. The CAG Number element is optionally present in the Beacon or Probe Response frame to reduce GAS frame exchanges when dot11InterworkingServiceActivated is true. The CAG Number element is optionally present in the GAS Initial Request frame to indicate the CAG Version and the associated CAG Information Type cached by the non-AP STA when dot11SolicitedPADActivated is true.

The CAG Number element is shown in Figure 9-589b.

	Element ID	Length	CAG Tuple #1	CAG Tuple #2 (optional)	...	CAG Tuple #N (optional)
Octets:	1	1	2	0 or 2		0 or 2

Figure 9-589b—CAG Number element format

The Element ID and Length fields are defined in 9.4.2.1.

One or more 2-octet CAG Tuple fields are used. The format of a CAG Tuple field is shown in Figure 9-589c.

	B0 B7	B8 B15
	CAG Version	CAG Information Type ~~Advertisement Protocol ID~~
Bits:	8	8

Figure 9-589c—CAG Tuple field

The CAG Version subfield is an unsigned integer indicating the current version of the CAG of the associated advertisement protocol and server indicated by the CAG Information Type subfield in the same CAG Tuple field. The use of CAG Version is explained in 11.25.3.2.

The CAG Information Type ~~Advertisement Protocol ID~~ subfield indicates the type of information ~~is a 8-bit subfield and carries a value equal to the Advertisement Protocol ID of the advertisement protocol~~ associated with the CAG Version in the same CAG Tuple field. The CAG Information Type ~~Advertisement Protocol ID~~ is defined in ~~Table 9-215 in 9.4.2.93~~ Table 9-262a1.

Table 9-262a1—CAG Information Type definitions

Name	Value
Access network query protocol (ANQP)	0
MIH Information Service	1
MIH Command and Event Services Capability Discovery	2
Emergency Alert System (EAS)	3
Registered location query protocol (RLQP)	4
Reserved	5–127
ANQP with Service Information Registry	128
Reserved	129–220
Vendor Specific	221
Reserved	222–255

Insert the following subclauses (9.4.2.233, 9.4.2.234, and 9.4.2.235, including Table 9-262ah and Figure 9-589du to Figure 9-589dz) after 9.4.2.232:

9.4.2.233 Service Hint element

The Service Hint element provides a probabilistic representation of a set of services that are available to the BSS. The format of the Service Hint element is shown in Figure 9-589du.

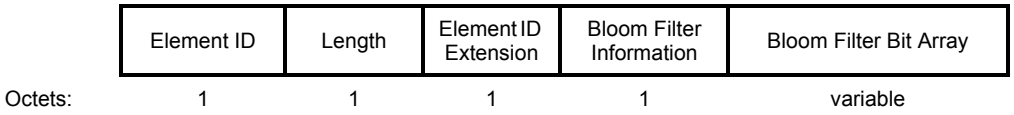

Figure 9-589du—Service Hint element format

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1.

The Bloom Filter Information field represents the stochastic characteristics of a Bloom filter that conveys the probabilistic data. The format of the Bloom Filter Information field is shown in Figure 9-589dv.

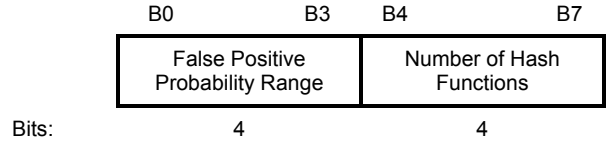

Figure 9-589dv—Bloom Filter Information field format

The False Positive Probability Range subfield represents the false positive probability range of the Bloom filter. The False Positive Probability Range subfield is shown in Table 9-262ah.

Table 9-262ah—False Positive Probability Range subfield values

Value	False positive probability range, *p*
0	$p > 25\%$
1	$20\% < p \leq 25\%$
2	$15\% < p \leq 20\%$
3	$10\% < p \leq 15\%$
4	$5\% < p \leq 10\%$
5	$1\% < p \leq 5\%$
6	$0.5\% < p \leq 1\%$
7	$0.1\% < p \leq 0.5\%$
8	$0.05\% < p \leq 0.1\%$
9	$0.01\% < p \leq 0.05\%$
10	$p \leq 0.01\%$
11–15	Reserved

The Number of Hash Functions subfield is set to a value equal to k–1, where k is the number of hash functions used by the Bloom filter as described in 11.25a.5.

The Bloom Filter Bit Array field provides an indication of the services offered by or through the AP or PCP with a target probability of false positive p. The length of the Bloom Filter Bit Array field in octets is Ceil(m/8) where m is the size of the Bloom filter in bits. How the size of the Bloom filter is determined is out of the scope of this standard. The maximum length of the Bloom Filter Bit Array field is 128 octets.

9.4.2.234 Service Hash element

The Service Hash element contains one or more service hashes. The format of the Service Hash element is shown in Figure 9-589dw.

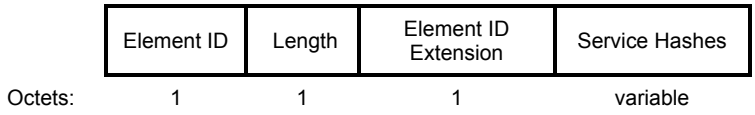

Figure 9-589dw—Service Hash element format

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1.

The Service Hashes field contains one or more 6-octet service hash values. See 11.25a.4 for procedures for generating a service hash used in the Service Hash element.

9.4.2.235 GAS Extension element

The GAS Extension element is defined in Figure 9-589dx. When present in the GAS Initial Request frame, the GAS Extension element indicates whether the STA is capable of receiving a Group Addressed GAS Response frame.

	Element ID	Length	Element ID Extension	GAS Flags	Maximum Channel Time	Fragment ID	Number of Response Map Duples	Response Map Duples
Octets:	1	1	1	1	0 or 1	0 or 1	0 or 1	Variable

Figure 9-589dx—GAS Extension element format

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1.

The GAS Flags field is defined in Figure 9-589dy.

	B0	B1	B2	B3	B4	B5 B7
	Group-addressed GAS	Fragment Retransmission	Maximum Channel Time Flag	Fragment ID Flag	Response Map Flag	Reserved
Bits:	1	1	1	1	1	3

Figure 9-589dy—GAS Flags field

The Group-addressed GAS subfield is set to 1 to indicate that the STA is capable of receiving Group Addressed GAS Request and Group Addressed GAS Response frames and is set to 0 otherwise.

The Fragment Retransmission subfield, when present in a GAS Initial Response frame, is set to 1 to indicate that the responding STA is capable of retransmitting a GAS Query Response fragment upon request and is set to 0 otherwise.

The Maximum Channel Time Flag subfield is set to 1 to indicate that the Maximum Channel Time field is present in the element and is set to 0 otherwise.

The Fragment ID Flag subfield is set to 1 to indicate that Fragment ID field is present in the element and is set to 0 otherwise.

The Response Map Flag subfield is set to 1 to indicate that the Number of Response Map Duples field and the Response Map Duples field are present in the element and is set to 0 otherwise.

The Maximum Channel Time field indicates the maximum duration the STA will, or needs to, remain on the channel to receive a GAS Initial Response, a GAS Comeback Response, or Group Addressed GAS Response, expressed as a multiple of 10 TUs beginning from the end of the PPDU carrying this element. The field has a valid range of 1–255.

The Fragment ID field, when present in the GAS Comeback Request, indicates which fragment the STA is requesting. It is present only when the Fragment ID Flag subfield is set to 1 in the GAS Flags field.

The Number of Response Map Duples field indicates the number of Response Map Duple subfields contained in the Response Map Duples field. It is present only when the Response Map Flag subfield is set to 1 in the GAS Flags field. When present, the Number of Response Map Duples field is set to a nonzero value and the value of zero is reserved.

The Response Map Duples field is present only when the Number of Response Map Duples field is present and contains a nonzero value. The Response Map Duples field, when present, contains one or more Response Map Duple subfields as indicated by the Number of Response Map Duples field. The format of the Response Map Duple subfield is shown in Figure 9-589dz. The Response Map Duples field is included in a Group Addressed GAS Response frame.

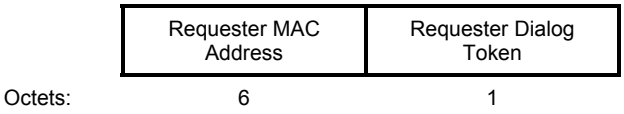

Figure 9-589dz—Response Map Duple subfield format

The Response Map Duple subfield contains a Requester MAC Address subfield and a Requester Dialog Token subfield. An AP or PCP includes one or more Response Map Duple subfields in a Group Addressed GAS Response frame.

9.4.5 Access Network Query Protocol (ANQP) elements

9.4.5.1 General

Insert the following rows into Table 9-271 in numeric order, and change the Reserved row accordingly:

Table 9-271—ANQP-element definitions

ANQP-element name	Info ID	ANQP-element (subclause)
Service Information Request	281	9.4.5.28
Service Information Response	282	9.4.5.29

9.4.5.27 CAG ANQP-element

Change 9.4.5.27 as follows:

The CAG ANQP-element provides the info IDs for the ANQP-elements contained within a CAG associated with ANQP, or ANQP with Service Information Registry, and the current value of the ANQP CAG version, indicating the version of information within the CAG associated with ANQP, or ANQP with Service Information Registry. The selection of the specific number of info IDs and the specific values of info IDs in a CAG associated with ANQP is left to the implementation and is beyond the scope of this document.

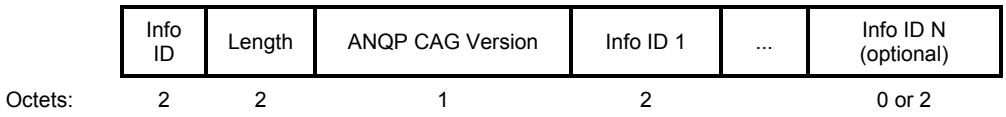

Figure 9-628e—CAG ANQP-element format

The Info ID and Length fields are defined in 9.4.5.1.

The ANQP CAG Version field indicates the current version of the CAG associated with ANQP, or ANQP with Service Information Registry.

The Info ID field represents the info ID of an ANQP-element Info ID specified in Table 9-271.

Insert the following subclauses (9.4.5.28 and 9.4.5.29, including Figure 9-628f to Figure 9-628i) after 9.4.5.27:

9.4.5.28 Service Information Request ANQP-element

The Service Information Request ANQP-element contains a generic request for service information associated with the service hash(es) provided.

The format of the Service Information Request ANQP-element is shown in Figure 9-628f.

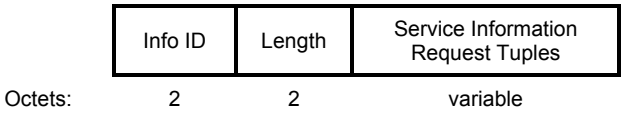

Figure 9-628f—Service Information Request ANQP-element format

The Info ID and Length fields are defined in 9.4.5.1.

The Service Information Request Tuples field contains one or more Service Information Request Tuple subfields. The format of the Service Information Request Tuple subfield is shown in Figure 9-628g.

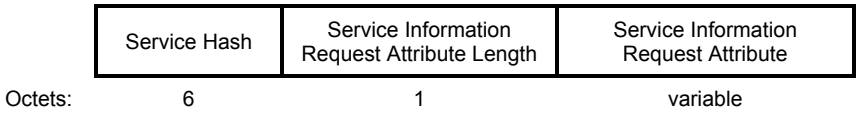

Figure 9-628g—Service Information Request Tuple subfield format

The Service Hash field contains a 6-octet service hash value. See 11.25a.4 for procedures for generating a service hash.

The Service Information Request Attribute Length subfield indicates the length of the Service Information Request Attribute subfield.

The Service Information Request Attribute subfield contains a service-specific query. The value of this subfield is out of the scope of this standard.

9.4.5.29 Service Information Response ANQP-element

The Service Information Response ANQP-element contains the detailed service information in response to a Service Information Request ANQP-element.

The format of the Service Information Response ANQP-element is shown in Figure 9-628h.

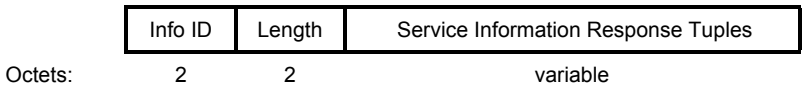

Figure 9-628h—Service Information Response ANQP-element format

The Info ID and Length fields are defined in 9.4.5.1.

The Service Information Response Tuples field contains zero or more Service Information Response Tuple subfields.

The format of the Service Information Response Tuple subfield is shown in Figure 9-628i.

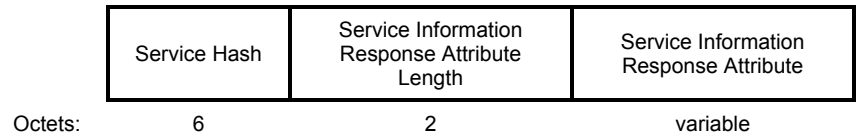

Figure 9-628i—Service Information Response Tuple subfield format

The Service Hash field contains a 6-octet service hash value. See 11.25a.4 for procedures for generating a service hash.

The Service Information Response Attribute Length subfield indicates the length of the Service Information Response Attribute subfield.

The content of the Service Information Response Attribute subfield is service specific based on the corresponding Service Information Request Attribute subfield in the Service Information Request Tuples of the Service Information Request ANQP-element as described in 9.4.5.28.

9.6.8 Public Action details

9.6.8.1 Public Action frames

Insert the following rows into Table 9-307 in numeric order, and change the Reserved row accordingly:

Table 9-307—Public Action field values

Public Action field value	Description
43	Group Addressed GAS Request
44	Group Addressed GAS Response

9.6.8.12 GAS Initial Request frame format

Insert the following rows into Table 9-313 in numeric order:

Table 9-313—GAS Initial Request Action field format

Order	Information
7	CAG Number (optional)
8	GAS Extension (optional)

Insert the following paragraphs at the end of 9.6.8.12:

When present in a GAS Initial Request frame, the CAG Number element includes one or more Common Advertisement Group (CAG) tuples. Each CAG tuple specifies a pair of CAG Version and CAG Information Type cached by the requesting STA and associated with the query request contained in the Query Request field.

The GAS Extension element indicating the STA support for GAS extension in GAS frame exchanges is optionally present if dot11GASExtensionImplemented is true.

9.6.8.13 GAS Initial Response frame format

Change the first paragraph of 9.6.8.13 as follows:

The GAS Initial Response frame is a Public Action frame. It is transmitted in response ~~responding~~ to a GAS Initial Request frame or a Group Addressed GAS Request frame. The format of the GAS Initial Response Action field is shown in Table 9-314.

Insert the following row into Table 9-314 in numeric order:

Table 9-314—GAS Initial Response Action field format

Order	Information
9	GAS Extension (optional)

Change the fourth paragraph of 9.6.8.13 as follows:

The Dialog Token field is copied from the corresponding GAS Initial Request frame or Group Addressed GAS Request frame.

Insert the following paragraph at the end of 9.6.8.13:

The GAS Extension element indicating the STA support for GAS extension in GAS frame exchanges is optionally present if dot11GASExtensionImplemented is true. It is included as a response to a GAS Initial Request frame containing a GAS Extension element.

9.6.8.14 GAS Comeback Request frame format

Insert the following row into Table 9-315 in numeric order:

Table 9-315—GAS Comeback Request Action field format

Order	Information
4	GAS Extension (optional)

Insert the following paragraph at the end of 9.6.8.14:

When present in a GAS Comeback Request frame, the GAS Extension element indicates a request to retransmit a GAS Query Response fragment.

Insert the following subclauses (9.6.8.45 and 9.6.8.46, including Table 9-325n and Table 9-325o) after 9.6.8.44:

9.6.8.45 Group Addressed GAS Request frame format

The Group Addressed GAS Request frame is a Public Action frame. It is transmitted by a requesting STA to request information from another STA. The format of the GAS Initial Request Action field is shown in Table 9-325n.

Table 9-325n—Group Addressed GAS Request Action field format

Order	Information
0	Category
1	Public Action
2	Dialog Token
3	Advertisement Protocol element
4	Query Request Length
5	Query Request
6	Multi-band (optional)
7	GAS Extension

The Category field is defined in 9.4.1.11.

The Public Action field is defined in 9.6.8.1.

The Dialog Token field is defined in 9.4.1.12 and set by the requesting STA.

The Advertisement Protocol element is defined in 9.4.2.93. The Advertisement Protocol element includes exactly one Advertisement Protocol ID.

The Query Request Length field format is provided in Figure 9-666. The value of the Query Request Length field is set to the total number of octets in the Query Request field.

The Query Request field format is provided in Figure 9-667. The Query Request field is a generic container whose value is a GAS Query that is formatted in accordance with the protocol identified in the Advertisement Protocol element.

When present in a Group Addressed GAS Request frame, the Multi-band element indicates the frequency band, operating class, and channel number to which the Group Addressed GAS Request frame applies.

The GAS Extension element indicates parameters that the AP or PCP may use to transmit a response back to the requesting STA.

9.6.8.46 Group Addressed GAS Response frame format

The Group Addressed GAS Response frame is a Public Action frame. It is transmitted in response to a GAS Initial Request frame or Group Addressed GAS Request frame. The format of the Group Addressed GAS Response Action field is shown in Table 9-325o.

Table 9-325o—Group Addressed GAS Response Action field format

Order	Information
0	Category
1	Public Action
2	Dialog Token
3	Status Code
4	Advertisement Protocol element
5	Query Response Length
6	Query Response
7	Multi-band (optional)
8	GAS Extension

The Category field is defined in 9.4.1.11.

The Public Action field is defined in 9.6.8.1.

The Dialog Token field is copied from the corresponding GAS Initial Request frame or Group Addressed GAS Request frame.

The Status Code values are defined in Table 9-46.

The Advertisement Protocol element is defined in 9.4.2.93. The Advertisement Protocol element includes exactly one Advertisement Protocol ID.

The Query Response Length field format is provided in Figure 9-669. The value of the Query Response Length field is set to the total number of octets in the Query Response field.

The Query Response field format is provided in Figure 9-670. The Query Response field is a generic container whose value is the response to a GAS Query and is formatted in accordance with the protocol specified in the Advertisement Protocol element.

When present in a Group Addressed GAS Response frame, the Multi-band element indicates the frequency band, operating class, and channel number to which the GAS Initial Response frame applies.

When present in a Group Addressed GAS Response frame, the GAS Extension element indicates parameters to which STA and which Query Request of the STA the response is responding.

9.6.22.2 Announce frame format

Insert the following rows into Table 9-416 in numeric order:

Table 9-416—Announce frame Action field format

Order	Information	Notes
26	Service Hash	The Service Hash element is optionally present if dot11UnsolicitedPADActivated is true; otherwise not present.
27	Service Hint	The Service Hint element is optionally present if dot11UnsolicitedPADActivated is true; otherwise not present.

10. MAC sublayer functional description

10.3 DCF

10.3.2 Procedures common to DCF and EDCAF

10.3.2.11 Duplicate detection and recovery

10.3.2.11.2 Transmitter requirements

Change the first paragraph of 10.3.2.11.2 as follows:

A STA maintains one or more sequence number spaces that are used when transmitting a frame to determine the sequence number for the frame. When multiple sequence number spaces are supported, the appropriate sequence number space is determined by information from the MAC control fields of the frame to be transmitted. Except as noted below, each sequence number space is represented by a modulo 4096 counter, starting at 0 and incrementing by 1, for each MSDU or MMPDU transmitted using that sequence number space. If dot11MACPrivacyActivated is true, the counter in each sequence number space shall be set to a random number modulo 4096 when the STA's MAC address is changed.

11. MLME

11.25 WLAN interworking with external networks procedures

11.25.3 Interworking procedures: generic advertisement service (GAS)

11.25.3.1 Introduction

Change the first paragraph of 11.25.3.1 as follows:

This subclause describes the actions and procedures that are used to invoke GAS. GAS may be used to enable network selection or service discovery for STAs when dot11InterworkingServiceActivated is true. GAS provides transport mechanisms for advertisement services while STAs are in the unassociated state as well as the associated state. This is accomplished via the use of Public Action frames, which are Class-1 frames. GAS information shall be transmitted using ~~individually addressed~~ Public Action frames. When management frame protection is negotiated, stations shall use individually addressed Protected Dual of Public Action frames instead of ~~individually addressed~~ Public Action frames.

Insert the following paragraphs after the second paragraph ("A GAS frame exchange ....") of 11.25.3.1:

A STA may transmit group addressed GAS Query Request. Multiple STAs that receive a group addressed GAS Query Request may send a unicast or group addressed GAS Query Response.

A STA that receives multiple, similar GAS Query Requests from multiple STAs that require the same GAS Query Response may aggregate the response and transmit a group addressed GAS Query Response.

A STA that receives a group addressed GAS Query Response may process the GAS Response information without transmitting a GAS Query Request frame.

11.25.3.2 GAS Protocol

11.25.3.2.1 General

Change the first paragraph of 11.25.3.2.1 as follows:

The presence of the Interworking element in Beacon or Probe Response frames indicates support for the GAS protocol. The additional presence of the GAS Extension element with the Group-addressed GAS subfield in the GAS Extension element set to true in a GAS Initial Request frame or group addressed GAS frames indicates support for the use of group addressed GAS frames. The presence of the Advertisement Protocol element in Beacon or Probe Response frames indicates the Advertisement Protocol IDs supported in the BSS or IBSS. A STA transmits a GAS Query Request in either a GAS Initial Request frame or a Group Addressed GAS Request frame, and the responding STA provides the GAS Query Response or information on how to receive the GAS Query Response in a GAS Initial Response frame or Group Addressed GAS Response frame. The GAS Query Response shall be delivered in a single GAS Initial Response frame, in a Group Addressed GAS Response frame, or in one or more GAS Comeback Response frames. The GAS Query Response shall not be split between a GAS Initial Response frame and one or more GAS Comeback Response frames or between a Group Addressed GAS Response frame and one or more GAS Comeback Response frames. The GAS message sequence diagrams are shown in Figure 11-38, Figure 11-39, ~~and~~ Figure 11-40, and Figure 11-40a.

Insert the following paragraph after the first paragraph of 11.25.3.2.1:

If a GAS Initial Request frame or a Group Addressed GAS Request frame contains a Maximum Channel Time field in the GAS Extension Element and if the conditions for replying as described in 11.25.3.2.3 and 11.25.3.2.4 are met, the responding STA shall queue for transmission a GAS Initial Response frame or a Group Addressed GAS Response frame within the indicated Maximum Channel Time.

Insert the following paragraphs (including Figure 11-40a to Figure 11-40d) at the end of 11.25.3.2.1:

Figure 11-40a describes the GAS frame exchange sequence when a STA sends a Group Addressed GAS Request frame to a group of STAs. The receiving STA may or may not respond to the GAS Query Request. If the receiving STA responds, it may respond with either a GAS Initial Response frame or a Group Addressed GAS Response frame.

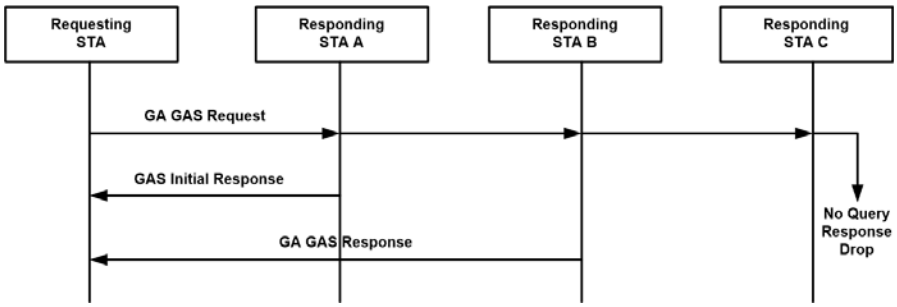

Figure 11-40a—Group addressed GAS Query Request exchange sequence

Figure 11-40b describes a GAS frame exchange sequence when multiple STAs send a GAS Initial Request frame that would result in the same GAS Query Response. The receiving STA responds with a Group Addressed GAS Response frame.

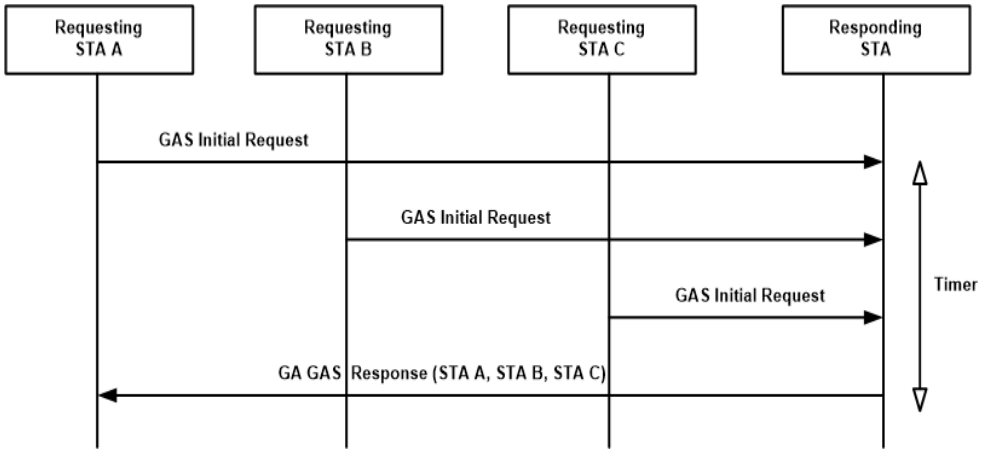

Figure 11-40b—Group addressed GAS Query Response exchange sequence

Figure 11-40c describes the GAS frame exchange sequence when a STA issues a GAS Initial Request frame and, during the course of receiving a fragmented GAS Comeback Response frame, requests a specific fragment for retransmission from the transmitting STA.

Figure 11-40d describes a GAS frame exchange sequence using CAG Version when a requesting STA requests information that the requesting STA has a cached version of a previous query response and the associated Common Advertisement Group (CAG) Version. The requesting STA provides its cached CAG Version in a GAS Initial Request frame along with the query request. When the responding STA determines that the CAG Version cached by the requesting STA matches a valid CAG Version that the responding STA receives from a relevant Advertisement Server as indicated by the CAG Information Type, which is provided by the requesting STA in the same CAG Tuple field that contains the cached CAG Version, then the responding STA provides a GAS response indicating that the information cached by the requesting STA is still valid. When the responding STA determines that the CAG Version cached by the requesting STA does not match any valid CAG Version that the responding STA receives from a relevant Advertisement Server as indicated by the CAG Information Type, which is provided by the requesting STA in the same CAG Tuple field that contains the cached CAG Version, then the responding STA posts the query request to the relevant Advertisement Server as specified in 11.25.3.2.3, receives a query response from the Advertisement Server, and transmits the query response to the requesting STA as specified in 11.25.3.2.4.

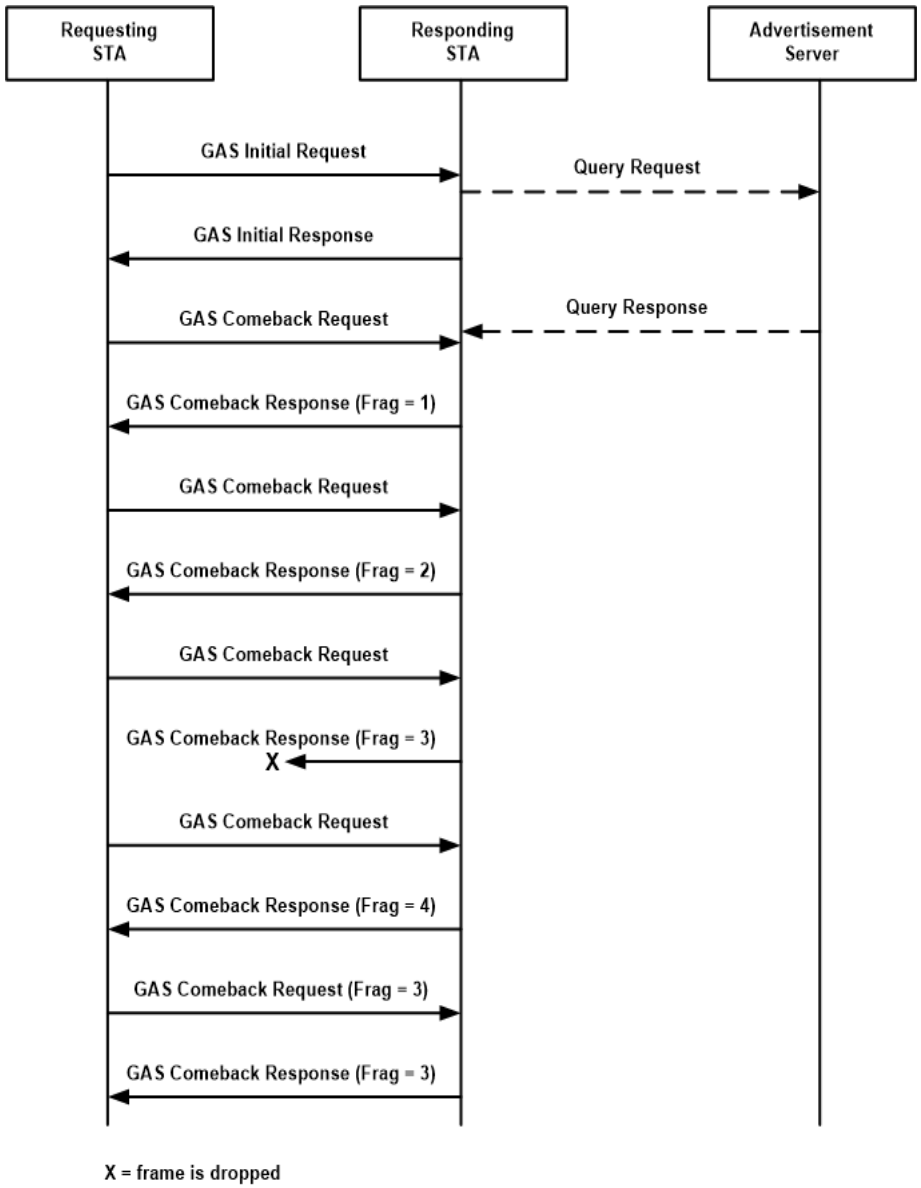

Figure 11-40c—Group addressed GAS Query for a specific fragment exchange sequence

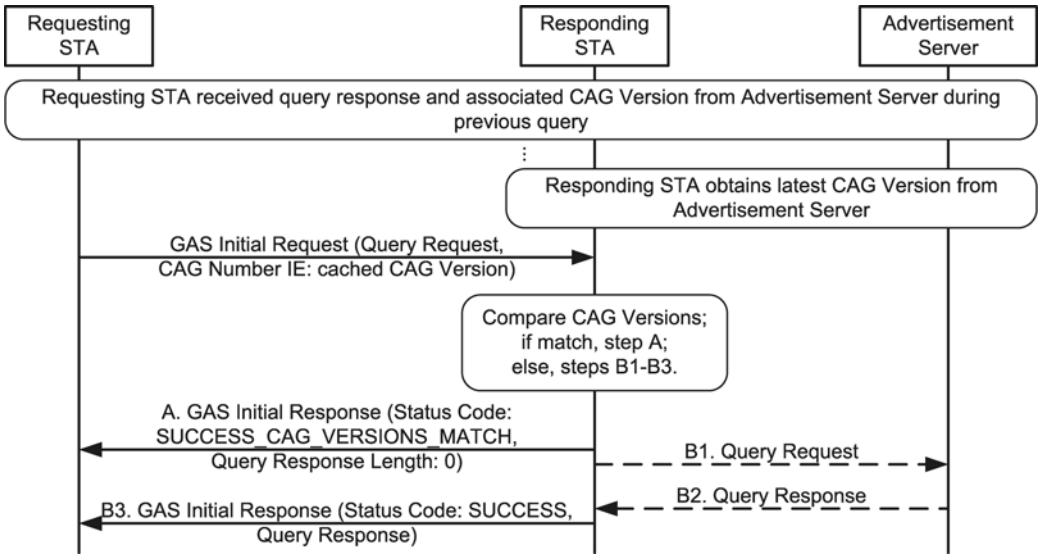

Figure 11-40d—GAS frame exchange sequence using CAG Version

Change 11.25.3.2.2 and 11.25.3.2.3 as follows:

11.25.3.2.2 STA procedures to transmit a GAS Query

Upon receipt of an MLME-GAS.request primitive, the requesting STA shall engage in the following procedure to transmit a query:

a) If GAMode in the primitive is null or set to false, t~~T~~he requesting STA sends a GAS Query by transmitting a GAS Initial Request frame containing a Dialog Token, an Advertisement Protocol element containing an Advertisement Protocol ID, and the GAS Query in the Query Request field. If the GAS Initial Request frame requests information relating to a frequency band different from the frequency band in which the frame is transmitted, the STA shall include a Multi-band element in the GAS Initial Request frame with the Band ID, Operating Class, and Channel Number fields set to indicate to which frequency band the GAS Initial Request frame applies, with other fields in the Multi-band element being reserved. If the frame requests information relating to the frequency band in which the frame is transmitted, a Multi-band element shall not be included in the frame. If the GAS Initial Request frame requests information that the requesting STA has a cached version of a previous query response and the associated CAG Version, the requesting STA may include the cached CAG Version and the associated CAG Information Type in a CAG Number element in the GAS Initial Request frame. If GAMode in the primitive is set to true, the requesting STA transmits a Group Addressed GAS Request frame including a GAS Extensions element with the Maximum Channel Time field set to the value of the dot11GASResponseTimeout divided by 10, rounded to the nearest integer, and limited to a value of 255.

b) Upon transmission of the GAS Initial Request frame or Group Addressed GAS Request frame, the STA shall set a timer, referred to as the *dot11GASResponseTimer*, equal to dot11GASResponseTimeout or the QueryFailureTimeout parameter provided in the MLME-GAS.request primitive. If both values are present, the timer shall be set to the lesser of the two values.

c) If the requesting STA is not in the associated state, it shall remain in active mode until the receipt of a GAS Initial Response frame or Group Addressed GAS Response frame with the same value of the Dialog Token field as in the GAS Initial Request frame or until the expiration of the timer, whichever occurs first. If the requesting STA is in the associated state, it may go into power save

state until the GAS Initial Response frame or Group Addressed GAS Response frame is available for receipt or the timer expiration, whichever occurs first.

d) If the dot11GASResponseTimer expires before a GAS Initial Response frame or Group Addressed GAS Response frame is received, the GAS Query was not successful and the MLME shall issue an MLME-GAS.confirm primitive with ResultCode equal to GAS_QUERY_TIMEOUT and shall set the Query Response Length field to 0.

11.25.3.2.3 STA procedures to post a GAS Query to an Advertisement Server

Upon receipt of a GAS Initial Request or a Group Addressed GAS Request frame, an MLME-GAS.indication primitive shall be issued to the STA's SME. Upon receipt of an MLME-GAS.indication~~response~~ primitive indicating the receipt of a GAS Initial Request frame, the STA shall transmit a GAS Initial Response or Group Addressed GAS Response frame to the requesting STA according to the following procedures. Upon receipt of an MLME-GAS.indication primitive indicating the receipt of a Group Addressed GAS Request frame, the STA may transmit a GAS Initial Response frame to the requesting STA or transmit a Group Addressed GAS Response frame according to the following procedures. If the requesting STA is in the associated state and in the power save mode, the responding STA shall buffer the MMPDU for transmission according to the procedures in 11.2.3; otherwise the STA shall queue the MMPDU for transmission as follows:

a) If the Advertisement Protocol ID in the Advertisement Protocol element does not equal the value contained in any dot11GASAdvertisementID, then the STA shall not post the query to an Advertisement Server. The STA shall transmit an individually addressed GAS Initial Response frame to the requesting STA containing a dialog token whose value is identical to the dialog token in the GAS Initial Request frame, a Status Code equal to GAS_ADVERTISEMENT_PROTOCOL_NOT_SUPPORTED (see Table 9-46), an Advertisement Protocol element containing the Advertisement Protocol ID used in the GAS Initial Request frame and a Comeback Delay and Query Response Length both set to 0.

b) If the query request corresponds to an Advertisement Protocol whose server is currently unreachable, the responding STA shall transmit an individually addressed GAS Initial Response frame to the requesting STA containing a dialog token whose value is identical to the dialog token in the GAS Initial Request frame, a Status Code equal to SERVER_UNREACHABLE, an Advertisement Protocol element containing an Advertisement Protocol ID equal to the Advertisement Protocol ID contained in the GAS Initial Request frame, and a GAS Comeback Delay and Query Response Length both set to 0. The method used by the AP to determine the server is unreachable is out of the scope of this standard. A STA receiving a status code indicating SERVER_UNREACHABLE should wait at least 1 min before transmitting any further queries using the same Advertisement Protocol ID to the responding STA.

c) If the GAS Initial Request frame includes a CAG Number element and all the CAG Versions in the CAG Number element match a valid CAG Version that the STA receives from the associated Advertisement Server, which is identified by the CAG Information Type subfield within the same CAG Tuple field as the CAG Version subfield, then the STA may transmit an individually addressed GAS Initial Response frame to the requesting STA containing a dialog token whose value is identical to the dialog token in the GAS Initial Request frame, a Status Code equal to SUCCESS_CAG_VERSIONS_MATCH, an Advertisement Protocol element containing the Advertisement Protocol ID used in the GAS Initial Request frame, and a GAS Comeback Delay and Query Response Length both set to 0, without posting the query to an Advertisement Server. This completes the GAS Query and GAS Query Response exchange.

d) ~~c)~~ If the Advertisement Protocol ID in the Advertisement Protocol element equals the value contained in any dot11GASAdvertisementID, then the STA shall initialize a timer, referred to as the *PostReplyTimer*, to the value of the Maximum Channel Time field times 10, if received in the GAS Initial Request or Group Addressed GAS Request frame, or otherwise, to the value in dot11GASResponseTimeout. ~~and~~ The STA posts the query to the Advertisement Server identified

by the Advertisement Protocol ID. If the GAMode associated with the Query Request is true, the STA includes the GAMode parameter, the GAS extension information, the MAC Address, and the Dialog token when it posts the query to the Advertisement Server for processing. The methods and protocols the STA uses to post the query are outside the scope of this standard.

1) If the GAMode associated with the Query Request is true and the Advertisement Server has no response to the Query Request, the Advertisement Server may drop the request.

2) If the Advertisement Server receives multiple GAS Query Requests resulting in the same response, the Advertisement Server may aggregate these responses into a single GAS Query Response. The Advertisement Server responds to the STA including the aggregated responses as described in 11.25.3.2.4a.

e) ~~d)~~ If dot11GASPauseForServerResponse is false, the responding STA shall transmit an individually addressed GAS Initial Response frame to the requesting STA containing a dialog token whose value is identical to the dialog token in the GAS Initial Request frame, a Status Code set to SUCCESS, an Advertisement Protocol element containing the Advertisement Protocol ID used in the GAS Initial Request frame, a GAS Comeback Delay set to the value in dot11GASComebackDelay for this Advertisement Protocol, and a Query Response Length set to 0.

f) ~~e)~~ If dot11GASPauseForServerResponse is true, the GAS Query Response is delivered as defined in 11.25.3.2.4.

11.25.3.2.4 STA procedures for transmitting the GAS Query Response

Change the fourth paragraph in 11.25.3.2.4 as follows:

The following procedures shall be used by the responding STA to deliver the query response to the requesting STA:

a) If dot11GASPauseForServerResponse is true:

1) If the query response is received from the Advertisement Server before the PostReplyTimer expires, and if the query response's length is less than or equal to the maximum MMPDU size and the query response is not an aggregated response, the STA shall transmit an individually addressed GAS Initial Response frame to the requesting STA containing a dialog token whose value is identical to the dialog token in the GAS Initial Request frame, a Status Code set to SUCCESS, an Advertisement Protocol element containing the Advertisement Protocol ID used in the GAS Initial Request frame or the Group Addressed Request frame, a GAS Comeback Delay set to 0, the Query Response and a Query Response Length set to the query response length. This completes the GAS request and response exchange.

2) If the query response is received from the Advertisement Server before the PostReplyTimer expires, and if the query response's length is less than or equal to the maximum MMPDU size and the query response is an aggregated response, the STA shall transmit a Group Addressed GAS Response frame containing a dialog token set to 0, a Status Code set to SUCCESS, an Advertisement Protocol element containing the Advertisement Protocol ID used in the GAS Initial Request frame or the Group Addressed Request frame, a GAS Comeback Delay set to 0, the Query Response and a Query Response Length set to the query response length, and a GAS Extension element containing a list of MAC Address/Dialog Token pairs in the Response Map Duples subfield of the GAS Extension element, identifying the requesting STAs and their Query Requests to which the Group Addressed GAS Response frame responds. This completes the GAS request/response exchange.

3) ~~1)~~ If the PostReplyTimer expires before the ~~GAS Q~~query ~~R~~response is received from the Advertisement Server for responding to a GAS Initial Request frame, then the responding STA shall transmit an individually addressed GAS Initial Response frame to the requesting STA containing a dialog token whose value is identical to the dialog token in the GAS Initial Request frame, a Status Code set to GAS_QUERY_TIMEOUT (see Table 9-46), an

Advertisement Protocol element containing the Advertisement Protocol ID used in the GAS Initial Request frame, a GAS Comeback Delay set to 0 and a Query Response Length set to 0. If the query response is subsequently received from the Advertisement Server, it shall be dropped by the responding STA.

4) If the PostReplyTimer expires before the query response is received from the Advertisement Server for responding to a Group Addressed GAS Request frame, then the responding STA shall not transmit an individually addressed GAS Initial Response frame or a Group Addressed GAS Response frame to the requesting STA. Note: If there is no response to the Query Request, the Advertisement Server may drop the request.

5) ~~2)~~ If the Query Response received from the Advertisement Server is larger than dot11GASQueryResponseLengthLimit or requires more than 128 fragments for transmission to the requesting STA, it shall be dropped by the responding STA. Then the responding STA shall transmit an individually addressed GAS Initial Response frame to the requesting STA containing a dialog token whose value is identical to the dialog token in the GAS Initial Request frame, a Status Code set to GAS_QUERY_RESPONSE_TOO_ LARGE (see Table 9-46), an Advertisement Protocol element containing the Advertisement Protocol ID used in the GAS Initial Request frame, a GAS Comeback Delay set to 0 and a Query Response Length set to 0.

~~3) If the query response's length is less than or equal to the maximum MMPDU size, the STA shall transmit an individually addressed GAS Initial Response frame to the requesting STA containing a dialog token whose value is identical to the dialog token in the GAS Initial Request frame, a Status Code set to SUCCESS, an Advertisement Protocol element containing the Advertisement Protocol ID used in the GAS Initial Request frame or the Group addressed Request frame, a GAS Comeback Delay set to 0, the Query Response and a Query Response Length set to the query response length. This completes the GAS Query and GAS Query Response exchange.~~

6) ~~4)~~ If the query response's length is larger than the maximum MMPDU size, the responding STA shall transmit an individually addressed GAS Initial Response frame to the requesting STA containing a dialog token whose value is identical to the dialog token in the GAS Initial Request frame, a Status Code set to SUCCESS, an Advertisement Protocol element containing the Advertisement Protocol ID used in the GAS Initial Request frame, a GAS Comeback Delay set to 1 TU, and a Query Response Length set to 0; this indicates the query response will be transmitted using GAS Comeback Request and Response frames that support GAS fragmentation as follows. If the responding STA is capable of retransmitting a Query Response fragment upon request, the responding STA shall include, in the GAS Initial Response frame, a GAS Extension element with the Fragment Retransmission subfield of the GAS Flags field set to 1.

b) If dot11GASPauseForServerResponse is false:

1) If the PostReplyTimer expires before the GAS Query Response is received from the Advertisement Server then the responding STA shall buffer for transmission a GAS Comeback Response frame with a status code equal to GAS_QUERY_TIMEOUT (see Table 9-46). If the query response is subsequently received from the Advertisement Server, it shall be dropped by the STA.

2) If the Query Response received from the Advertisement Server is larger than dot11GASQueryResponseLengthLimit, it shall be dropped by the responding STA. Then the STA shall buffer for transmission a GAS Comeback Response frame with status code set to GAS_QUERY_RESPONSE_TOO_ LARGE.

c) If the Query Response is received before the expiration of the PostReplyTimer and its length is less than dot11GASQueryResponseLengthLimit, then the Query Response shall be buffered in one or more GAS Comeback Response frames with status code set to SUCCESS. The responding STA transmits one GAS Comeback Response frame in response to each GAS Comeback Request frame. If the Query Response received from the Advertisement Server is less than or equal to the maximum

MMPDU size, then the GAS Query Response Fragment ID shall be set to 0 and the More GAS Fragments field in the GAS Query Response Fragment ID shall be set to 0. If the Query Response received from the Advertisement Server is greater than the maximum MMPDU size, then the GAS Query Response Fragment ID shall be set to 0 if this is the first fragment of the Query Response transmitted; otherwise it shall be incremented by 1; the More GAS Fragments field in the GAS Query Response Fragment ID shall be set to 1 if there are more fragments of the Query Response to be transmitted; otherwise it shall be set to 0 (i.e., this fragment is the last fragment of the Query Response). If a responding STA receives a GAS Comeback Request that includes the GAS Extension element with the Fragment ID field set to a valid Fragment ID the responding STA shall respond with a GAS Comeback Response frame that includes the fragment corresponding to the received Fragment ID.

d) If a responding STA receives a GAS Comeback Request frame whose source MAC address and dialog token match the destination MAC address and value of the Dialog Token field respectively of an outstanding GAS Initial Response frame and the query response has not been received from the Advertisement Server and the PostReplyTimer has not expired, the responding STA shall transmit a GAS Comeback Response frame with status code equal to GAS_RESPONSE_NOT_RECEIVED_FROM _SERVER (see Table 9-46) and GAS Comeback Delay set to the value in dot11GASComebackDelay for this Advertisement Protocol to indicate when the requesting STA should come back to obtain its Query Response.

e) If a responding STA receives a GAS Comeback Request frame whose source MAC address and Dialog Token do not match the destination MAC address and value of the Dialog Token field respectively of an outstanding GAS Initial Response frame, the STA should transmit a GAS Comeback Response frame with a status code equal to NO_OUTSTANDING_GAS_REQUEST.

Insert the following paragraph after the fifth paragraph ("A requesting STA ....") in 11.25.3.2.4:

If the requesting STA supports GAS extension, and the requesting STA is unable to receive a GAS Query Response fragment, then the following procedures apply:

a) If the Fragment Retransmission subfield in the GAS Extension element in the corresponding GAS Initial Response frame is equal to 1, the requesting STA may transmit a GAS Comeback Request frame, including the GAS Extension element with the Fragment ID subfield of the GAS Flags field set to the fragment ID of the Query Response to be retransmitted. Upon successfully receiving the GAS Comeback Request, the responding STA shall transmit a GAS Comeback Response frame that includes the Query Response fragment corresponding to the value received in the Fragment ID field and with the GAS Query Response Fragment ID subfield in GAS Query Response Fragment field set to the value received in the Fragment ID field. If the Query Response fragment is not available, the responding SA shall respond with a GAS Comeback Response frame with a status code set to GAS_FRAGMENT_NOT_AVAILABLE.

b) If the corresponding GAS Initial Response frame does not contain a GAS Extension element or the value of the Fragment Retransmission subfield in the GAS Extension element is equal to 0, the requesting STA shall not request the retransmission of a GAS Query Response fragment using a GAS Comeback Request frame.

Insert the following subclause (11.25.3.2.4a) after 11.25.3.2.4:

11.25.3.2.4a Group addressed GAS procedures

Upon receipt of an MLME-GAS.request primitive with the GAMode parameter set to 1 (true), the requesting STA shall follow procedures defined in 11.25.3.2.2 to transmit a Group Addressed GAS Request frame instead of a GAS Initial Request frame.

Upon receipt of an aggregated Query Response from the Advertisement Server, the responding STA may transmit the aggregated Query responses using Group Addressed GAS Response frame to the receiving STAs. The length of the Group Addressed GAS Response frame shall not exceed the IEEE 802.11 maximum MMPDU size. The STA shall include a list of MAC Address/Dialog Token pairs in the Response Map duples subfield of the GAS Extension element included in the Group Addressed GAS Response frame.

11.25.3.3 ANQP procedures

11.25.3.3.1 General

Change the ninth paragraph in 11.25.3.3.1 as follows:

A ~~FILS~~ STA that makes use of the CAG Version is subject to the following:

- The STA may obtain the CAG Version from the CAG Number element received in Beacon or Probe Response frames.
- The STA searches its cached information using ~~either~~ the BSSID, HESSID, or SSID of the AP as an index to obtain the correct cached ANQP CAG Version entry.
- If the cached ANQP CAG Version does not match the CAG version received in Beacon or Probe Response frames, the STA should transmit an ANQP request for any of the ANQP-elements contained within the CAG. If the CAG Versions do match, the STA should use the stored ANQP attributes and information of the CAG for network discovery.

Change the column heading in Table 11-15, insert the following rows at the end of the table, and change the Symbols list as shown:

Table 11-15—ANQP usage

ANQP-element name	ANQP-element (subclause)	ANQP-element type	BSS		IBSS
			AP	Non-AP and non-PCP STA	STA
Service Information Request	9.4.5.28	Q	R, G	T, G	—
Service Information Response	9.4.5.29	S	T, G	R, G	—

Symbols
Q element is an ANQP request
S element is an ANQP response
T ANQP-element may be transmitted by MAC entity
R ANQP-element may be received by MAC entity
G Group addressed ANQP request/response may be transmitted and received by a MAC entity
— ANQP-element is neither transmitted nor received by MAC entity

11.25.3.3.15 CAG procedure

Change 11.25.3.3.15 as follows:

The CAG ANQP-element is used by a requesting STA to perform an ANQP query to retrieve the Info IDs contained within the CAG associated with ANQP, or ANQP with Service Information Registry, and the current ANQP CAG Version associated with these Info IDs. If the requesting STA to perform an ANQP

query to retrieve the Info IDs related both to ANQP and to ANQP with Service Information Registry, the requesting STA shall use separate CAG ANQP-elements. For this purpose, a requesting STA shall use the procedures defined in 11.25.3.2.1 and 11.25.3.2.2 and shall include in the ANQP query the Info ID of the CAG ANQP-element as shown in Table 11-15. When a responding AP receives a Query List ANQP-element that contains the Info ID of CAG ANQP-element, the responding STA shall include in the ANQP Query Response frame a CAG ANQP-element containing the ANQP CAG Version and the Info IDs of the ANQP-elements that are in the CAG associated with ANQP, or ANQP with Service Information Registry, in the increasing order of the Info ID values. If the responding STA receives Info IDs related both to ANQP and to ANQP with Service Information Registry, the responding STA shall include separate CAG ANQP-elements in the ANQP response. The ANQP response also includes the (other) ANQP-elements that a STA requested in the ANQP query list in the increasing order of the Info ID values.

The ANQP CAG Version is an unsigned number, and it is incremented when there is any change in the CAG associated with ANQP, or ANQP with Service Information Registry, including a change of the Info ID of the ANQP-elements of the CAG or a change in the values of the ANQP-elements included in the CAG. If the ANQP CAG Version exceeds 255, it is reset to 0.

Insert the following subclause (11.25a) after 11.25:

11.25a Preassociation discovery (PAD) procedures

11.25a.1 General

There are two types of PAD procedures: unsolicited and solicited. The unsolicited PAD procedure is described in 11.25a.2, and the solicited PAD procedure is described in 11.25a.3.

When dot11UnsolicitedPADActivated or dot11SolicitedPADActivated is true, a non-AP and non-PCP STA may use PAD procedures to allow the SIC to discover the availability of services that the same non-AP and non-PCP STA may access when associated. While the specification of service-specific information is outside the scope of this standard, the service-specific information in the BSS is proxied by a SIR (see 4.5.9.2.4), which might be collocated with the AP or PCP.

A non-AP STA with dot11SolicitedPADActivated set to true shall invoke MAC privacy procedures by setting dot11MACPrivacyActivated to true (see 12.2.10).

An AP advertises support for PAD by setting the PAD field of the Extended Capabilities element to 1 in its Beacon and Probe Response frames.

A PCP advertises support for PAD by setting the PAD field of the Extended Capabilities element to 1 in its DMG Beacon, Announce, and Probe Response frames.

11.25a.2 Unsolicited PAD procedure

When dot11UnsolicitedPADActivated is true, an AP shall advertise services from an SIR using a Service Hint element or a Service Hash element, or both, in Beacon and Probe Response frames. Each service may be advertised using either a Service Hint element or a Service Hash element, but not both, in a Beacon or Probe Response frames.

When dot11UnsolicitedPADActivated is true, a PCP shall advertise services from an SIR using a Service Hint element or a Service Hash element, or both, in DMG Beacon, Announce, or Probe Response frames. Each service may be advertised using either a Service Hint element or a Service Hash element, but not both, in DMG Beacon, Announce, or Probe Response frames.

A Service Hint element is used to advertise the presence of one or more services reachable via a BSS with a probability of matching a wrong service as indicated in the False Positive Probability Range subfield of the Service Hint element. A Service Hash element is used to advertise the presence of one or more services reachable via a BSS with a negligible probability of matching a wrong service. The mechanism for selecting which of a Service Hash or Service Hint element to use to advertise a particular service is beyond the scope of this standard.

When dot11UnsolicitedPADActivated is true, a non-AP and non-PCP STA searching for a service shall perform the following steps for each BSS:

a) From the received Beacon, DMG Beacon, Announce, or Probe Response frames, process the Service Hash elements to generate a list of services reachable via the BSS, and process the Service Hint elements to determine the parameters of the bloom filter.
b) Construct a list comprising service hash values for each service being searched. Then determine the bit positions in the Bloom Filter Array field that will be set to 1 for each service in the list.
c) For each service being searched, determine whether there is a matched service within the list of services, based on either of the following:
    1) The service hash value in the list of services matches the corresponding service hash value constructed in step b).
    2) The values of the bit positions of the Bloom Filter Bit Array field of the Service Hint element, as determined in step b), are all equal to 1.

The non-AP and non-PCP STA may use the resulting information about which services are reachable as input to network discovery and selection procedures. The non-AP and non-PCP STA might proceed with the solicited PAD procedure (see 11.25a.3) or authentication and association procedure (see 11.3) based on the indicated false positive probability and the requirements of the service or the SIC (see the examples in Annex Y).

11.25a.3 Solicited PAD procedure

When dot11SolicitedPADActivated is true, a non-AP and non-PCP STA may transmit to an AP or PCP a Service Information Request ANQP-element to request information from the SIR about services reachable via the BSS. A non-AP and non-PCP STA may use the Interworking and PAD fields of the Extended Capabilities element received from the AP or PCP to determine whether that AP or PCP supports Solicited PAD.

NOTE—An Interworking field value of 1 implies support for ANQP.

The Service Information Request ANQP-element is used by a non-AP and non-PCP STA to request detailed information about services reachable via the BSS; see examples illustrated in Annex Y.

When dot11SolicitedPADActivated is true, a non-AP and non-PCP STA may send a Service Information Request ANQP-element (see 9.4.5.28) to obtain information about a matching service. The Service Information Request ANQP-element shall include one or more Service Information Request Tuple subfields. Each Service Information Request Tuple subfield shall include a service hash within the Service Hash subfield and a Service Information Request Attribute subfield that is a service-specific request.

When dot11SolicitedPADActivated is true, an SIR shall use the information from the Service Information Request ANQP-element to determine whether the requested service(s) are reachable via the BSS. If matching services are found, corresponding to the Service Hash subfield, the SIR shall respond by requesting the AP or PCP to transmit a Service Information Response ANQP-element that contains a Service Information Response Tuple subfield for each service that satisfies the request. The Service Information Response ANQP-element contains detailed information about the services. When there is no

matching service corresponding to the Service Hash subfield in an individually addressed GAS Initial Request frame, the SIR shall respond by requesting the AP or PCP to transmit a Service Information Response ANQP-element containing zero Service Information Response Tuple subfields.

The SIC receives service information from the contents of the Service Information Response ANQP-element. The non-AP and non-PCP STA may use the service information regarding which services are reachable as input to network discovery and selection procedures. The non-AP and non-PCP STA might proceed with the authentication and association procedure (see 11.3) (see examples illustrated in Annex Y).

11.25a.4 Service hash procedures

A service hash is generated from a service name after all single octet uppercase alphabetic characters in the service name are converted into corresponding lowercase characters. A service name is defined in IETF RFC 6335.[4]

A service hash contained in the Service Hash subfield of the Service Hash element, or in the Service Information Request ANQP-element, or in the Service Information Response ANQP-element, or a service hash used to map into the Bloom Filter Bit Array is generated as follows:

service hash = L(SHA-256(service name), 0, 48).

For example, a service hash for the service name of "_ipp._tcp" is created as follows: The service hash contained in the Service Hash subfield of the Service Hash element, the Service Information Request ANQP-element, and the Service Information Response ANQP-element is "bfd39037d25c," and the service hash used as input to compute the Bloom Filter Bit Array field is "0xbfd39037d25c."

11.25a.5 Bloom filter hash function operation

The Bloom filter for a set of service hashes is created as described below.

Let m denote the number of bits in the Bloom filter, and let k–1 be the setting of the Number of Hash Functions field in the Bloom Filter information field (see 9.4.2.233), i.e., k is the number of Bloom filter hash functions (out of a maximum of 16) used by the Bloom filter. For example, when the Number of Hash Functions field is equal to 1, the first two hash functions are used (j =0x00,0x01).

Create the Bloom filter as follows:

a) Set all bits in the Bloom filter to zero.
b) For each service hash in the set of service hashes, compute the k bit positions by setting j = 0,….k–1, in the function H(j,X,m) shown below. Set the bits at the k computed bit positions to 1. Note that, in some cases, different values of j may return the same bit position.

Let H(j,X,m) denote the Bloom filter hash function,

where

j is the Bloom filter hash function prepend parameter used in the computation; j is a single octet and ranges from 0x00 to 0x0F, in hexadecimal notation
X is the service hash that is mapped into the Bloom Filter Bit Array field (see 11.25a.4 for procedures for generating a service hash used to map into the Bloom Filter Bit Array field)

[4]Information on normative references can be found in Clause 2.

m is the size, in number of bits, of the Bloom filter; how the size of the Bloom filter is determined is out of the scope of this standard

The $H(j,X,m)$ is computed as follows:

Step 1: Compute $A(j,X) = [j \,||\, X]$, where || denotes an append operation.
Step 2: Compute $B(j,X) = CRC32(A(j,X))$ & 0x0000FFFF. In other words, obtain the least significant 2 octets of the 32-bit CRC of $A(j,X)$, where CRC32() is the same 32-bit CRC as defined in 9.2.4.8.
Step 3: $H(j,X,m) = B(j,X) \bmod m$.

12. Security

12.2 Framework

Insert the following subclause (12.2.10) after 12.2.9:

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. However, the non-AP STA shall not change its MAC address during a transactional exchange, for example, transmitting Public Action frames for preassociation discovery, or during the creation of state on an AP using preassociation capabilities, for example, RSN preauthentication or FT over-the-DS. The smaller the period of MAC address change, down to a single transmitted frame per MAC address, the greater the privacy these enhancements afford. The actual period used when changing a MAC address is implementation dependent and outside the scope of this standard..

If such a non-AP STA starts any transaction that establishes state bound to a MAC address and might elect to establish an association or establish transaction state with a discovered BSS, it shall check the value of dot11LocallyAdministeredMACConfig and shall configure its MAC address according to the rules of the local address space prior to the start of the transaction. State created with an AP using a prior MAC address, for instance, RSN preauthentication state or FT state established over-the-DS, is bound to the MAC address used when that state was created. Prior to establishing an association to the AP, the non-AP STA shall change its MAC address to the MAC address used when the state was created.

Every time a MAC address is changed to a new random value, counters in all sequence number spaces used to identify each MSDU or MMPDU shall be reset (see 10.3.2.11.2), and the OFDM data scrambler shall be reseeded per the procedure described in 17.3.5.5, if applicable.

The non-AP STA connecting to an infrastructure BSS shall retain a single MAC address for the duration of its connection across an ESS. A PMKSA created as part of an RSNA will contain the MAC address used to create the PMKSA. The non-AP STA that supports PMKSA caching shall, if necessary, change its MAC address back to that value when attempting a subsequent association to the ESS using PMKSA caching.

To construct a random MAC address, the STA shall select a randomized MAC address according to IEEE Std 802-2014 and IEEE Std 802c-2017.

To avoid leakage of possibly sensitive network-identifying information, STAs should refrain from transmitting Probe Request frames containing preferred SSID values and, instead, use passive scanning or transmit Probe Request frames containing the wildcard SSID.

17. Orthogonal frequency division multiplexing (OFDM) PHY specification

17.3 OFDM PHY

17.3.5 DATA field

17.3.5.5 PHY DATA scrambler and descrambler

Change 17.3.5.5 by inserting a new paragraph after the second paragraph as follows:

The 127-bit sequence generated repeatedly by the scrambler shall be (leftmost used first), 00001110 11110010 11001001 00000010 00100110 00101110 10110110 00001100 11010100 11100111 10110100 00101010 11111010 01010001 10111000 1111111, when the all 1s initial state is used. The same scrambler is used to scramble transmit data and to descramble receive data. If the TXVECTOR parameter CH_BANDWIDTH_IN_NON_HT is not present, when transmitting, the initial state of the scrambler shall be set to a pseudorandom nonzero state. If the TXVECTOR parameter CH_BANDWIDTH_IN_NON_HT is present,

— The first 7 bits of the scrambling sequence shall be set as shown in Table 17-7 (with field values defined in Table 17-8 and Table 17-10) and shall be also used to initialize the state of the scrambler.
— The scrambler with this initialization shall generate the remainder (i.e., after the first 7 bits) of the scrambling sequence as shown in Figure 17-7.
— CH_BANDWIDTH_IN_NON_HT is transmitted LSB first. For example, if CBW80 has a value of 2, which is '10' in binary representation, then B5=0 and B6=1.

<u>If dot11MACPrivacyActivated is true, the initial state of the scrambler shall be reset when the STA's MAC address is changed.</u>

Annex A

(informative)

Bibliography

Insert the following bibliographic entry into Annex A in numeric order:

[B58] Tarkoma, S., Rothenberg, C. E., and Lagerspetz, E., "Theory and Practice of Bloom Filters for Distributed Systems," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 1, pp. 131–155, Feb. 2011.

Annex B

(normative)

Protocol Implementation Conformance Statement (PICS) proforma

B.2 Abbreviations and special symbols

B.2.2 General abbreviations for Item and Support columns

Insert the following abbreviation into B.2.2 in alphabetic order:

PAD preassociation discovery

B.4 PICS proforma—IEEE Std 802.11-2016[5]

B.4.3 IUT configuration

Insert the following row at the end of the table in B.4.3:

Item	IUT configuration	References	Status	Support
* CFPAD	preassociation discovery	11.25a	O	Yes ☐ No ☐ N/A ☐

B.4.20 Interworking (IW) with external networks extensions

Insert the following rows after IW2.6 in the table in B.4.20:

Item	Protocol capability	References	Status	Support
IW2.7	Group Addressed GAS Request frame	9.6.8.16	O	Yes ☐ No ☐ N/A ☐
IW2.8	Group Addressed GAS Response frame	9.6.8.17	O	Yes ☐ No ☐ N/A ☐
IW2.9	Re-transmission of a query response fragment	11.25.3.2.1	O	Yes ☐ No ☐ N/A ☐

[5]*Copyright release for PICS proforma:* Users of this standard may freely reproduce the PICS proforma in this annex so that it can be used for its intended purpose and may further publish the completed PICS.

Insert the following subclause (B.4.32) after B.4.31 in Annex B:

B.4.32 Preassociation discovery extensions

Item	Protocol Capability	References	Status	Support
*PAD1	Unsolicited PAD procedure	11.25a.2	CFPAD:M	Yes ☐ No ☐ N/A ☐
PAD1.1	Service Hint element	9.4.2.233	PAD1:M	Yes ☐ No ☐ N/A ☐
PAD1.2	Service Hash element	9.4.2.234	PAD1:M	Yes ☐ No ☐ N/A ☐
*PAD2	Solicited PAD procedure	11.25a.3	(CFPAD AND IW2.2.2):M	Yes ☐ No ☐ N/A ☐
PAD2.1	Service Information Request	9.4.5.28	PAD2:M	Yes ☐ No ☐ N/A ☐
PAD2.2	Service Information Response	9.4.5.29	PAD2:M	Yes ☐ No ☐ N/A ☐

Annex C

(normative)

ASN.1 encoding of the MAC and PHY MIB

C.3 MIB detail

Insert the following entries at the end of the "Dot11StatonConfigEntry ::= SEQUENCE" list in the "dot11StationConfig TABLE" in C.3:

```
      dot11SolicitedPADActivated                    TruthValue,
      dot11UnsolicitedPADActivated                  TruthValue,
      dot11MACPrivacyActivated                      TruthValue,
      dot11GASExtensionImplemented                  TruthValue,
      dot11LocallyAdministeredMACConfig             Unsigned32
```

Insert the following OBJECT-TYPE definitions in the "dot11StationConfig TABLE" after "dot11StationConfigEntry 166" in C.3:

```
dot11SolicitedPADActivated OBJECT-TYPE
   SYNTAX TruthValue
   MAX-ACCESS read-write
   STATUS current
   DESCRIPTION
   "This is a control variable.
   It is written by an external management entity or the SME. Changes take effect
      as soon as practical in the implementation.
   This attribute when true, indicates that the capability of the STA to operate
      solicited PAD with external networks is enabled. The capability is
      disabled otherwise."
   DEFVAL {false}
::= { dot11StationConfigEntry 167 }

dot11UnsolicitedPADActivated OBJECT-TYPE
   SYNTAX TruthValue
   MAX-ACCESS read-write
   STATUS current
   DESCRIPTION
   "This is a control variable.
   It is written by an external management entity or the SME. Changes take effect
      as soon as practical in the implementation.
   This attribute when true, indicates that the capability of the STA to operate
      unsolicited PAD with external networks is enabled. The capability is
      disabled otherwise."
   DEFVAL {false}
::= { dot11StationConfigEntry 168 }

dot11GASExtensionImplemented OBJECT-TYPE
   SYNTAX TruthValue
   MAX-ACCESS read-only
   STATUS current
   DESCRIPTION
   "This is a capability variable. Its value is determined by device
      capabilities. This attribute, when true, indicates that the STA is capable
      of operating in GAS extension in GAS frame exchanges. Otherwise, it is
      false. The default value of this attribute is false."
```

```
    DEFVAL {false}
::= { dot11StationConfigEntry 183 }

dot11MACPrivacyActivated OBJECT-TYPE
    SYNTAX TruthValue
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
    "This is a control variable.
    It is written by an external management entity or the SME. Changes take effect
       as soon as practical in the implementation. This attribute when true,
       indicates that the STA enables MAC privacy considerations. The capability
       is disabled otherwise."
    DEFVAL {false}
::= { dot11StationConfigEntry 184 }

dot11LocallyAdministeredMACConfig OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
    "This is a control variable.
    It is written by an external management entity or the SME. Changes take effect
       as soon as practical in the implementation. This attribute identifies an
       addressing plan to use for when associating with the BSS.

       0: local addresses comply with the Structured Local Address Plan (SLAP) as
       defined in IEEE Std 802c-2017
       1: local addresses are constructed according to vendor-specific local
       address plan.
    DEFVAL {0}
::= { dot11StationConfigEntry 185 }
```

Change "dot11GASResponseTimeout OBJECT-TYPE" in "dot11GASAdvertisement TABLE" in C.3 as follows:

```
dot11GASResponseTimeout OBJECT-TYPE
    SYNTAX Unsigned32 (10~~00~~..65535)
    UNITS "TUs"
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
       "This is a control variable.

       It is written by an external management entity or the SME.
       Changes take effect as soon as practical in the implementation.

       This parameter shall indicate the GAS response timeout value."
    DEFVAL {50~~00~~}
    ::= { dot11GASAdvertisementEntry 3 }
```

Insert the following OBJECT-GROUP after the "dot11FineTimingMeasurement OBJECT-GROUP" { dot11Groups 93 } in "Groups - units of compliance" in C.3:

```
dot11PADComplianceGroup OBJECT-GROUP
    OBJECTS {
       dot11SolicitedPADActivated,
       dot11UnsolicitedPADActivated,
    }
    STATUS current
    DESCRIPTION
```

```
      "This object group provides the objects from the IEEE 802.11
      MIB required to manage preassociation discovery functionality."
   ::= { dot11Groups 94 }
```

Change OPTIONAL-GROUPS in Compliance Statements (dot11Compliances 1) in C.3 as follows:

```
-- OPTIONAL-GROUPS {
   -- ...,
   -- dot11FILSComplianceGroup,
   -- dot11PADComplianceGroup }
```

Insert the following compliance statement at the end of the "Compliance Statements" part in C.3:

```
-- ********************************************************************
-- * Compliance Statements- PAD
-- ********************************************************************

dot11PADCompliance MODULE-COMPLIANCE
   STATUS current
   DESCRIPTION
      "This object class provides the objects from the IEEE 802.11
      MIB required to manage preassociation discovery functionality."
   MODULE -- this module
   MANDATORY-GROUPS { dot11PADComplianceGroup }
::= { dot11Compliances 20 }
```

Insert the following text (Annex Y) after Annex X:

Annex Y

(informative)

Preassociation discovery (PAD) additional information

Y.1 Preassociation discovery usage models

The preassociation discovery (PAD) and service information procedures (see 11.25a) support several ways of obtaining service information. The following subclauses describe two methods: background search and immediate search.

Y.2 Background search

Applications that run in the background on the STA (e.g., automatically receiving sales coupons within messages transmitted from a BSS for which a user has previously signed up) might not require immediate discovery results to be presented to the user. It may be appropriate to prevent non-AP and non-PCP STAs, running such background applications, from performing a solicited PAD procedure.

Solicited PAD has the potential to introduce network congestion, and it is recommended that STAs limit the use of solicited PAD to cases requiring an active search for services. In those cases, it is more effective to perform an unsolicited PAD search, in which an AP or PCP advertises multiple services known to the SIR, while non-AP and non-PCP STAs need respond only if there is a matched service.

The SIR can advertise services through an AP or PCP, using the Service Hash element, and advertise remaining services, using the Service Hint element, in the Beacon or DMG Beacon frame. Alternatively, the SIR can advertise all of the services through an AP or PCP, using either the Service Hash or Service Hint element, in the Beacon or DMG Beacon. Upon receiving a Beacon or DMG Beacon frame, the SIC in a non-AP and non-PCP STA processes the Service Hash and Service Hint elements to verify if there are any potential matching services. Figure Y-1 and Figure Y-2 show two cases where there is a matching service hint.

If the probability of false positives as indicated in the False Positive Probability Range field of the Service Hint element is considered relatively high by the SIC in the non-AP and non-PCP STA (see Figure Y-1), the SIC can send, through the non-AP and non-PCP STA, a Service Information Request ANQP-element containing Service Information. The SIR then responds, through an AP or PCP, with a Service Information Response ANQP-element containing the Service Information Response Attribute subfield. This subfield contains information about the service(s) that was requested. Following these service information exchanges, the non-AP and non-PCP STA might associate to the AP or PCP.

If the probability of false positive as indicated in False Positive Probability Range field of the Service Hint element is considered relatively low by the SIC in the non-AP and non-PCP STA, the SIC might choose the AP or PCP as a candidate BSS. The SIC might send a Service Information Request ANQP-element to confirm if a service is reachable through the AP or PCP as shown in Figure Y-1. Based on the results of either of these steps, the SIC in the non-AP and non-PCP STA might request association with the BSS.

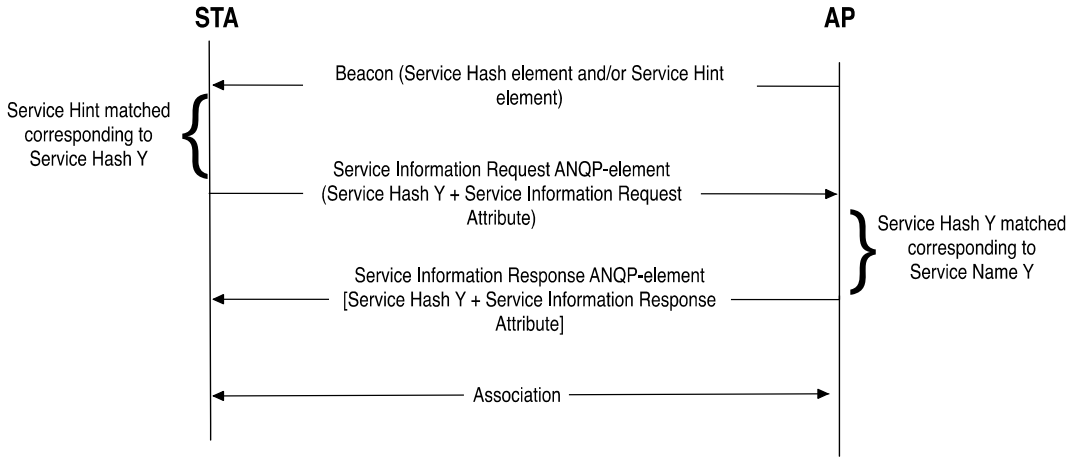

Figure Y-1—Example of a frame exchange for background search with Service Hint matching

In a scenario where there is a matching service hash, the non-AP and non-PCP STA can send a Service Information Request ANQP-element containing a Service Information Request Attribute to the AP or PCP to obtain more information about the service from the SIR as shown in Figure Y-2. The SIR responds to the ANQP request, through the AP or PCP, with a Service Information Response ANQP-element containing the Service Information Response Attribute subfield. Following these service message exchanges, the non-AP and non-PCP STA might associate with the AP or PCP. Alternatively, the non-AP and non-PCP STA might choose to associate based on the matching Service Hash element.

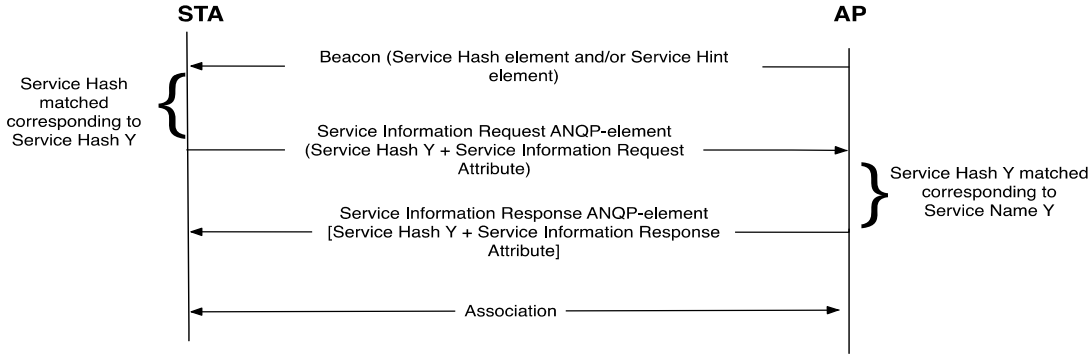

Figure Y-2—Example of frame exchange for background search with matching Service Hash element

Y.3 Immediate search

Applications that are initiated by users on the STA (e.g., a user is looking for a fast movie download service provided by a BSS) require immediate discovery results to be presented to the STA or a user so that network selection can be performed by either a STA or the user to obtain the desired service.

Figure Y-3 shows a non-AP and non-PCP STA performing a solicited PAD procedure, whereby the non-AP and non-PCP STA sends a Service Information Request ANQP-element to query specific services

immediately after user initiation of the service/application. The SIR responds through an AP or PCP with a Service Information Response ANQP-element accordingly if there is a matched service.

Following these service message exchanges, the SIC in the non-AP and non-PCP STA can make an informed decision about choosing to associate to the AP or PCP.

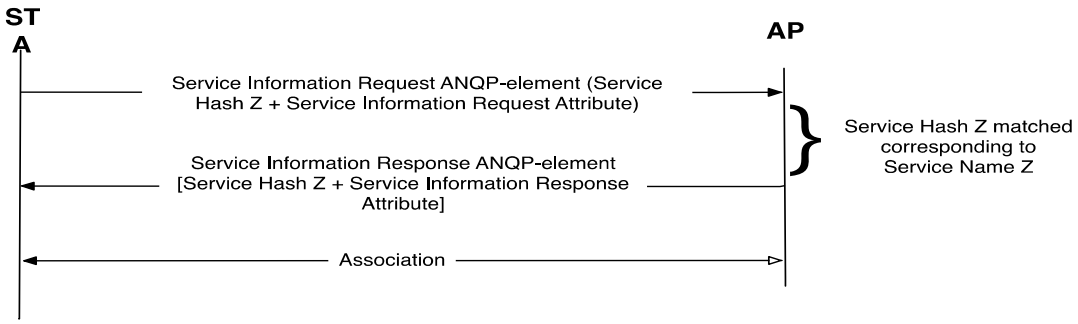

Figure Y-3—Example of frame exchange for immediate search

Consensus

WE BUILD IT.

Connect with us on:

Facebook: https://www.facebook.com/ieeesa

Twitter: @ieeesa

LinkedIn: http://www.linkedin.com/groups/IEEESA-Official-IEEE-Standards-Association-1791118

IEEE-SA Standards Insight blog: http://standardsinsight.com

YouTube: IEEE-SA Channel

IEEE
standards.ieee.org
Phone: +1 732 981 0060 Fax: +1 732 562 1571