IEEE P802.11u™/D8.0

Draft 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 7: Interworking with External Networks

Prepared by the 802.11 Working Group of the 802 Committee

This document is an unapproved draft of a proposed IEEE Standard. As such, this document is subject to change. USE AT YOUR OWN RISK! Because this is an unapproved draft, this document must not be utilized for any conformance/compliance purposes. Permission is hereby granted for IEEE Standards committee participants to reproduce this document for purposes of international standardization consideration. Prior to adoption of this document, in whole or in part, by another standards development organization permission must first be obtained from the Manager, Standards Intellectual Property, IEEE Standards Activities Department. Other entities seeking permission to reproduce this document, in whole or in part, must obtain permission from the Manager, Standards Intellectual Property, IEEE Standards Activities Department.

IEEE Standards Activities Department
445 Hoes Lane, P.O. Box 1331
Piscataway, NJ 08854, USA

Abstract: This amendment specifies enhancements to the 802.11 MAC that support WLAN Interworking with External Networks. It enables higher layer functionalities to provide overall end-to-end solutions. The main goals of 802.11u are aiding network discovery and selection, enabling information transfer from external networks, enabling emergency services, and interfacing Subscription Service Provider Networks (SSPN) to 802.11 Networks that support Interworking with External Networks.

Keywords: wireless LAN, interworking, interworking with external networks, E911, emergency services, interface, QoS mapping, MIH, media independent handover, network advertisement, network discovery, network selection, emergency alert system, SSP, SSPN, subscriber service provider, generic advertisement service.

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

PDF: ISBN XXX-XXXXX-XXXX-XSTDXXXXX
Print: ISBN XXX-XXXXX-XXXX-X STDPDXXXXX

Introduction

This introduction is not part of IEEE 802.11u™/D8.0, IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems - LAN/MAN Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 7: Interworking with External Networks

The Interworking with External Networks is a key enabler to allow IEEE 802.11 devices to interwork with external networks, as typically found in hotspots or other public networks irrespective of whether the service is subscription based or free.

The Interworking Service aids network discovery and selection, enabling information transfer from external networks, and enabling emergency services. It provides information to the STAs about the networks prior to association. Interworking will not only help users within home, enterprise and public access markets, but also assist manufacturers and operators to provide common components and services for IEEE 802.11 customers.

The Interworking Service addresses MAC layer enhancements that allow higher layer functionality to provide the overall end-to-end interworking solution.

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard 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

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. 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 Standards Association website at http://ieeexplore.ieee.org/xpl/standards.jsp, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA website at http://standards.ieee.org.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: http://standards.ieee.org/reading/ieee/updates/errata/index.html. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: http://standards.ieee.org/reading/ieee/interp/index.html.

Patents

Attention is called to the possibility that implementation of this amendment may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence for validity of any patent rights in connection therewith. A patent holder or patent applicant has filed a statement of assurance that it will grant licenses under these 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. Other Essential Patent Claims may exist for which a statement 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 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 draft Standard was completed, the 802.11 Working Group had the following membership:

Bruce Kraemer, *Chair*
Adrian Stephens and Jon Rosdahl, *Vice-chairs*
Stephen McCann, *Secretary*

EDITORIAL NOTE—a three column list of voting members of 802.11 on the day the draft was sent for sponsor ballot will be inserted.

The following were officers of Task Group u:

Stephen McCann, *Chair*
Matthew S. Gast, Dave Stephenson, *Secretary*
Necati Canpolat, *Technical Editor*

Ccontributions to this amendment were received from the following individuals

:

Alex Ashley
Malik Audeh,
Gabor Bajko
Farooq Bari
Moussa Bavafa
Colin Blanchard
Daniel R. Borges
George Bumiller
Nancy Cam-Winget
Necati Canpolat
Angelo Centonza
Clint Chaplin
Hong Cheng
Liwen Chu
David Cypher
Sabine Demel
Roger Durand
Peter Ecclesine
Jon Edney
Mike Ellis
Stephen Emeott
Darwin Engwer
Stefano Faccin
Lars Falk
Matthew Fischer
Matthew Gast
Josh Graessley
Wolfgang Groeting
Shu Guiming
Vivek Gupta
Dongwoon Hahn
Brian Hart
Eleanor Hepworth
Frans Hermodsson
Ulises Olvera-Hernandez
Yasuhiko Inoue
Jari Jokela
Eunkyo Kim
Ronny Kim
Jouni Korhonen
Celine Liu
Osama Aboul-Magd
Alastair Malarky
Jouni Malinen
Bill Marshall
Stephen McCann
Andrew McDonald
Liangyao Mo
Patrick Mo
Michael Montemurro
Andrew Myers
Bob O Hara
Henry Ptasinski
Richard Roy
Marian Rudolf
Ajoy Singh
Srinivas Sreemanthula
Dorothy Stanley
Adrian Stephens
Dave Stephenson
Allan Thomson
Ganesh Venkatesan
Qi Wang
Michael Williams
Qiaobing Xie
Sihoon Yang
Zhonghui Yao
Amy Zhang
Ding Zhiming

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

EDITORIAL NOTE—a three-column list of responding sponsor ballot members will be inserted by IEEE staff.

Table of Contents

List of Figures

List of Tables

IEEE P802.11u™/D8.0

Draft 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 7: Interworking with External Networks

[This amendment is based on IEEE Std 802.11™-2007, as amended by IEEE Std P802.11k™ 2008, IEEE Std 802.11r™ 2008, IEEE Std P802.11y™, IEEE P802.11w D9.0, IEEE P802.11n D11.0, IEEE P802.11v D7.0, IEEE P802.11p D8.0 and IEEE P802.11z D5.0]

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.1

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 instruction specifies the location of the change and describes what is being changed by using ~~strikethrough~~ (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] Notes in text, tables, and figures are given for information only, and do not contain requirements needed to implement the standard.

1. Overview

1.2 Purpose

Change the text Inserting the following new item at end of the bulleted list as shown below:

— Defines functions and procedures aiding network discovery and selection by STAs, information transfer from external networks using QoS Mapping and a general mechanism for the provision of emergency services.

2. Normative references

Insert the following new references into 2 maintaining the ordering in the base spec:

3GPP TS 24.234 v8.1.0, 3GPP System to Wireless Local Area Network (WLAN) interworking; WLAN User Equipment (WLAN UE) to network protocols; Stage 3 (Release 8), September 2008.

IANA EAP Method Type Numbers, http://www.iana.org/assignments/eap-numbers.

IEEE Std 802.21-2008, IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services, January 2009.

IETF RFC 1034, Domain Names - Concept and Facilities, November 1987.

IETF RFC 3629, UTF-8, a transformation format of ISO 10646, F. Yergeau, November 2003.

IETF RFC 3748, Extensible Authentication Protocol (EAP), B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, June 2004.

IETF RFC 3986, Uniform Resource Identifier (URI): Generic Syntax, January 2005.

IETF RFC 4282, The Network Access Identifier, December 2005.

IETF RFC 5222, LoST: A Location-to-Service Translation Protocol, August 2008.

ISO 3166-1, Codes for the representation of names of countries and their subdivisions - Part 1: Country codes, November 2006.

OASIS Emergency Management Technical Committee, “Common Alerting Protocol Version 1.1” April 2005.

OASIS Emergency Management Technical Committee, “Emergency Data Exchange Language (EDXL) Distribution Element, v. 1.0”. OASIS Standard EDXL-DE v1.0, May-2006.

3. Definitions

Insert the following new definitions into 3 maintaining the ordering:

3.265 advertisement server: An entity that provides an interworking advertisement service to a non-AP STA. The server reports information related to an IEEE 802.11 ESS in response to queries from non-AP

STAs. Information may relate to authorization for use of an IEEE 802.11 infrastructure based on a roaming agreement. An example is a server which implements IEEE 802.21-IS.

3.266 authorization: The act of determining if a particular right, such as access to some resource, can be granted to an authenticated entity (see RFC 2903 [B48]).

3.267 infrastructure authorization information: The Information that specifies the access rights of the user of a non-AP STA in an IEEE 802.11 infrastructure. This may include the rules for routing the user traffic, a set of permissions about services that a user is allowed to access, QoS configuration information, or the accounting policy to be applied by the 802.11 infrastructure.

3.268 ESS link: In the context of an 802.11 medium access control (MAC) entity, a logical connection path through the wireless medium between a non-AP STA and only one set of AP STAs that are interconnected to form an extended service set (ESS).

3.269 homogenous ESS: A collection of BSSs, within the same extended service set (ESS), in which the SSPN or other external network reachable at one BSS, is reachable at all of them.

3.270 generic advertisement service (GAS): An IEEE 802.11 service that provides over-the-air transportation for frames of higher-layer advertisements between STAs or between a server in an external network and a non-AP STA. GAS supports higher-layer protocols that employ a query/response mechanism.

3.271 interworking service: A service that supports use of an IEEE 802.11 infrastructure with non-IEEE 802.11 networks. Functions of the interworking service assist non-AP STAs in discovering and selecting IEEE 802.11 networks, in using appropriate QoS settings for transmissions, in accessing emergency services, and in connecting to subscription service providers.

3.272 multi-level precedence and preemption (MLPP): A framework used with admission control for the treatment of traffic streams based on precedence, which supports the preemption of an active traffic stream by a higher-precedence traffic stream when resources are limited. Preemption is the act of forcibly removing a traffic stream in progress in order to free up facilities for another higher-precedence traffic stream.

3.273 native GAS: The Native Query protocol transported by GAS Public Action frames.

3.274 network access identifier (NAI): The user identity submitted by the client during IEEE 802.1X authentication (see RFC 4282).

3.275 network type: An identifier used to classify the conditions of network access. For example, an enterprise network has a condition of access of private network and users, which are employees of the enterprise, would expect to have user accounts to access the network and that other users will also be employed by the enterprise.

3.276 non-native GAS: Any advertisement protocol other than the Native Query protocol transported by GAS Public Action frames.

3.277 public safety answering point (PSAP): A physical location where emergency calls are received and routed to the proper emergency services such as police and ambulance etc., see NENA specification [B55].

3.278 roaming consortium: A roaming consortium is a group of SSPs having inter-SSP roaming agreements.

3.279 subscription service provider (SSP): An organization (operator) offering connection to network services, perhaps for a fee.

3.280 subscription service provider network (SSPN): The SSP controlled network. The network maintains user subscription information.

3.281 subscription service provider roaming: The act of a wireless terminal using a “visited” IEEE 802.11 infrastructure based on a subscription and formal agreement with its “home” SSP.

4. Abbreviations and acronyms

Insert the following new abbreviations and acronyms into clause 4 in alphabetical order:

3GPP	3rd generation partnership project
802.x LAN	IEEE 802 based local area networks such as 802.3 and 802.11
AAA	authentication, authorization, and accounting
ASRA	additional step required for access
DN	destination network
EAS	emergency alert system
EBR	expedited bandwidth request
ESC	emergency services capability
ES	emergency services
GAS	generic advertisement service
GPRS	general packet radio service
GRX	GPRS roaming exchange
HESSID	homogenous ESS identifier
LoST	location to service translation
MICS	media independent command service
MIES	media independent event service
MIH	media independent handover
MIIS	media independent information service
MLPP	multi-level precedence and preemption
MSFG	MAC State Generic Convergence Function
NAI	network access identifier
NQP	native query protocol
OI	organization identifier
PHB	per-hop behavior
PoS	point of service
PSAP	public safety answering point
SSP	subscription service provider
SSPN	subscription service provider network
UESA	un-authenticated emergency service accessible
URL	uniform resource locator
URI	uniform resource identifier
VLAN	virtual local area network

5. General description

5.2 Components of the IEEE 802.11 architecture

Insert the following new subclause after 5.2.11:

5.2.12 SSPN interface

An AP can interact with external networks using a logical SSPN interface for the purpose of authenticating users and provisioning services, as shown in Figure 5-6a. The exchange of authentication and provisioning information between the SSPN and the AP passes transparently through the Portal. The protocol used to exchange this information is out of scope of this standard. The logical SSPN interface provides the means for an AP to consult an SSPN for authenticating and authorizing a specific non-AP STA and to report statistics and status information to the SSPN. Authentication and provisioning information for non-AP STAs received from the SSPN are stored in the AP MIB and are used to limit layer-2 services provided to that non-AP STA. Detailed interactions describing the SSPN interface are provided in 11.23.4.

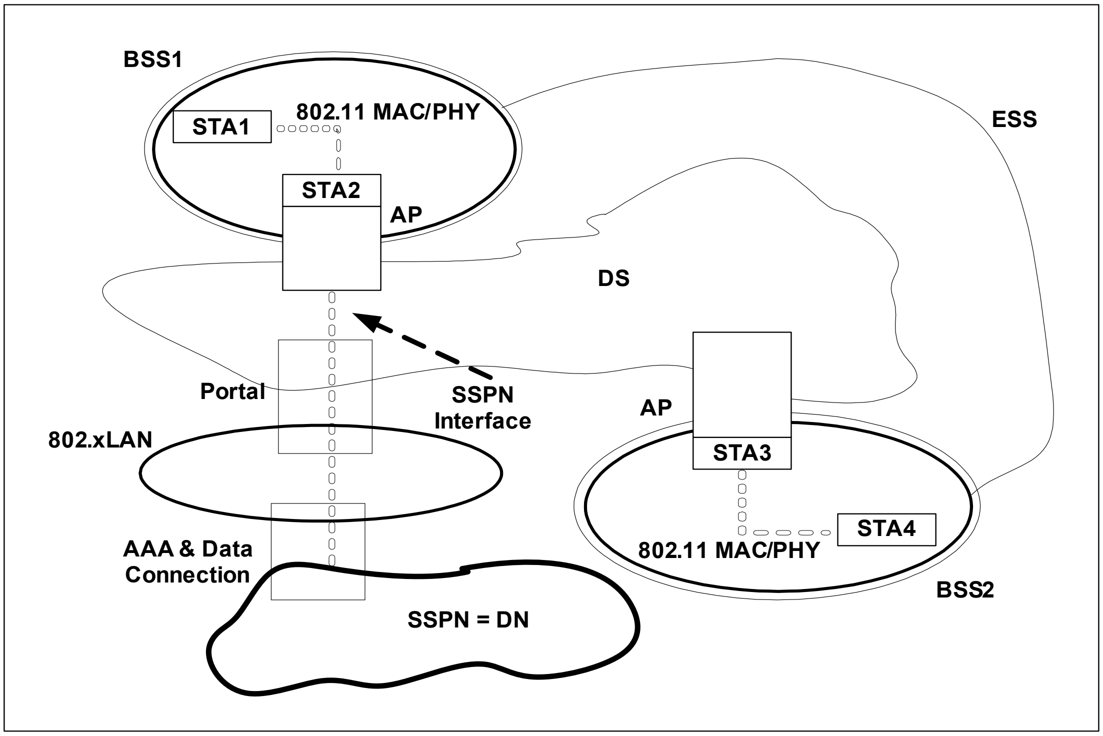

Figure 5-6a—SSPN interface service architecture

The SSPN interface provides the non-AP STA access to the services provisioned in the SSPN via the currently associated BSS. SSPN access may involve VLAN mapping or tunnel establishment that are transparent to the non-AP STA and out of scope of this standard. The SSPN interface also allows the non-AP STA to access services in DNs other than the SSPN. An example of a DN other than SSPN is the provision of Internet access via the IEEE 802 LAN, or an intermediary network that connects the IEEE 802.11 infrastructure and the SSPN.

NOTE—The SSPN Interface Service is not supported in an IBSS.

5.4 Overview of the services

Insert the following subclause 5.4.8 after 5.4.7

5.4.8 Interworking with External Networks

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 802.11 non-AP STA may 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 network type, roaming consortium and venue information
  - Selection of a suitable IEEE 802.11 infrastructure using advertisement services in the BSS or a server in an external network reachable via the BSS
  - Selection of an SSPN or External Network with its corresponding IEEE 802.11 infrastructure
- Emergency Services
  - Emergency Call and Network Alert support at the link level
- QoS Map distribution
- SSPN Interface service between the AP and the SSPN

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 out of scope of this standard.

The Generic Advertisement Service (GAS), described in 5.9, can be used by an AP to provide support for the network selection process and as a conduit for communication by a non-AP STA with other information resources in an external network before joining a network.

The Interworking Service supports Emergency Services (ES) by providing methods for un-authenticated users to access emergency services via the IEEE 802.11 infrastructure, advertising that emergency services are supported (see 11.23.5) and reachable 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 may have its own layer-3 end-to-end packet marking practice (e.g., DSCP usage conventions), a means to re-map 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).

5.7 Reference model

Insert the following subclause heading 5.7.1 after 5.7 and move the text in 5.7 to 5.7.1:

5.7.1 General

Change the first paragraph of 5.7.1 as follows:

This standard presents the architectural view, emphasizing the separation of the system into two major parts: the MAC of the data link layer (DLL) and the PHY. These layers are intended to correspond closely to the lowest layers of the ISO/IEC basic reference model of Open Systems Interconnection (OSI) (ISO/IEC 7498-

1: 1994). The MAC State Generic Convergence Function provides services to higher layer protocols based on MAC state machines and interactions between the layers. The layers and sublayers described in this standard are shown in Figure 5-10.

Insert the following subclause 5.7.2 after 5.7.1:

5.7.2 Interworking reference model

Interworking functions may require correlating information from multiple management entities. It is the function of the MAC State Generic Convergence Function (MSGCF) to correlate information for higher-layer entities. The MSGCF observes the interactions between the MLME and SME, and between the PLME and SME. After correlation of lower-layer MLME and PLME events, the MSGCF may synthesize indications to higher-layer entities.

Figure 5-10a shows an entity, the MAC State Generic Convergence Function (MSGCF), defined in clause 11B, that has access to all management information through exposure to the MAC and PHY Sublayer Management Entities, and provides management information to higher level entities, such as Mobility Managers, supporting heterogeneous medium mobility.

An example of how the MSGCF interfaces to these higher layer entities, is provided by the Media Independent Handover (MIH) interface, as defined in IEEE 802.21-2008.

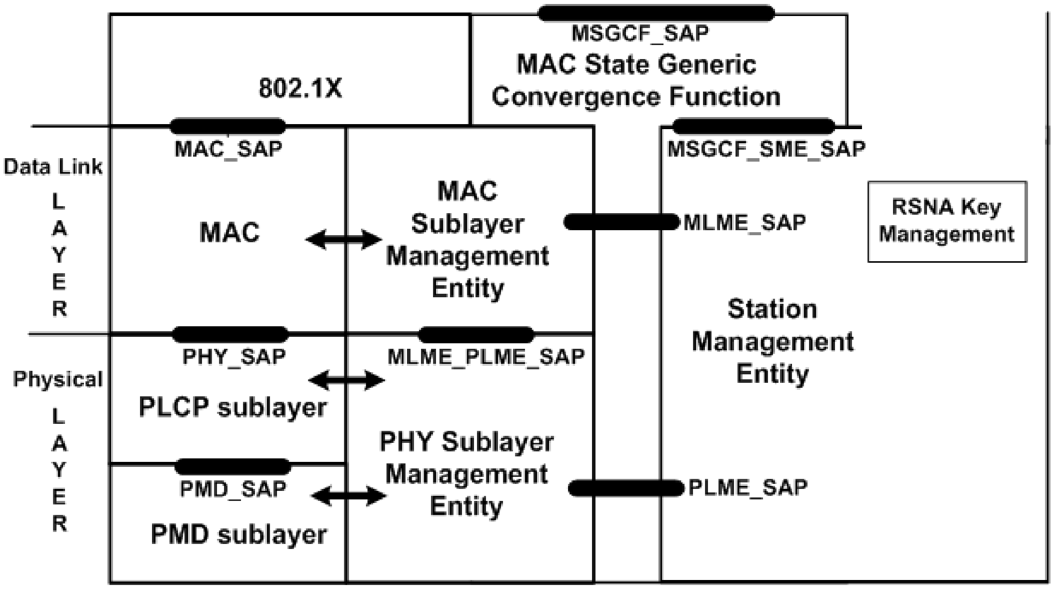

Figure 5-10a—Interworking Reference Model

The MSGCF is designed to provide the status of the connection of a non-AP STA to a set of BSSs comprising a single ESS. Figure 5-10b illustrates the concept of an ESS Link. This higher-layer concept is intended to reflect the state of a connection to an ESS independent of any particular access point. In Figure 5-10b, STA3 is associated with either AP1 or AP2. The state of the ESS Link is up when STA3 is associated with any of the APs comprising an ESS.

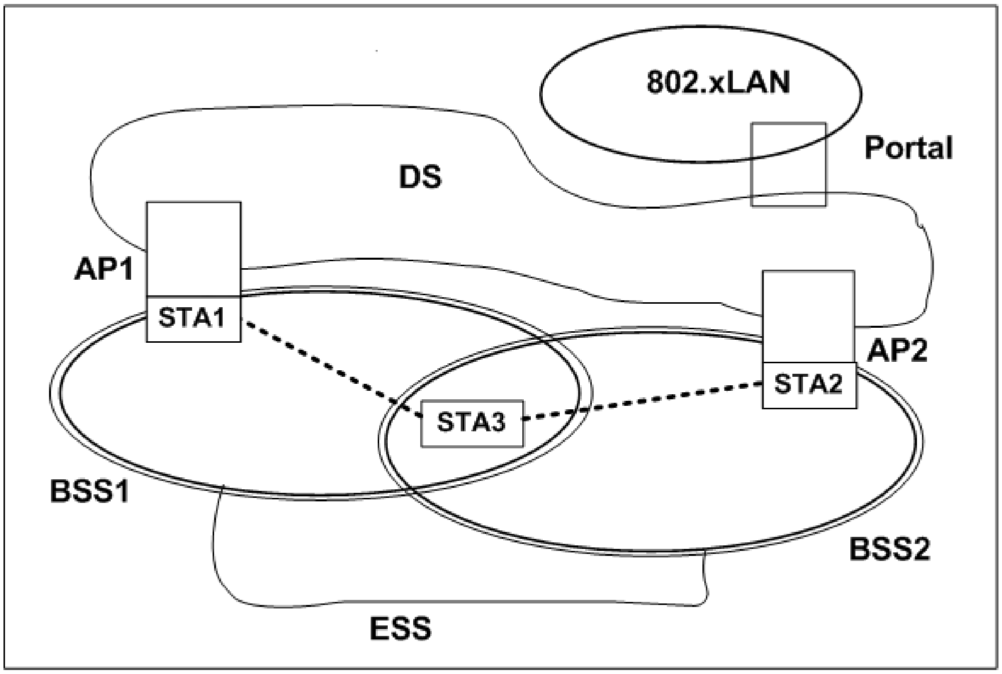

Figure 5-10b—ESS Link illustration

Insert the new subclause 5.9 below after 5.8

5.9 Generic Advertisement Service

In an infrastructure BSS the Generic Advertisement Service (GAS) provides functionality that enables non-AP STAs to discover the availability of information related to desired network services, e.g., information about local access services, available SSPs and/or SSPNs or other external networks.

While the specification of network services information is out of scope of IEEE 802.11, there is a need for non-AP STAs to query for information on network services provided by SSPNs or other external networks beyond an AP before they associate to the wireless LAN. GAS uses a generic container to advertise network services' information over an IEEE 802.11 network. Public Action frames are used to transport this information.

There are a number of reasons why providing information to a non-AP STA in a pre-associated state is beneficial:

— It supports more informed decision making about an IEEE 802.11 infrastructure with which to associate. This is generally more efficient than requiring a non-AP STA to associate with an AP before discovering the information and then deciding whether or not to stay associated.

— It is possible for the non-AP STA to query multiple networks in parallel.

— The non-AP STA can discover information about APs that are not part of the same administrative group as the AP with which it is associated, supporting the selection of an AP belonging to a different IEEE 802.11 infrastructure that has an appropriate SSP roaming agreement in place.

In an IBSS, GAS functionality enables a STA the availability and information related to desired services natively provided by another STA in the IBSS. Exchange of information using GAS may be performed either prior to joining an IBSS or after joining the IBSS.

6. MAC service definition

6.1 Overview of MAC services

6.1.5 MAC data service architecture

Change the first two paragraphs of 6.1.5 as follows:

The MAC data plane architecture (i.e., processes that involve transport of all or part of an MSDU) is shown in Figure 6-1. During transmission, an MSDU goes through some or all of the following processes: MSDU rate limiting. A-MSDU aggregation, frame delivery deferral during power save mode, sequence number assignment, fragmentation, encryption, integrity protection, and frame formatting and A-MPDU aggregation. IEEE Std 802.1X-2004 may block the MSDU at the Controlled Port. At some point, the data frames that contain all or part of the MSDU are queued per AC/TS. This queuing may be at any of the three points indicated in Figure 6-1.

During reception, a received data frame goes through processes of possible A-MPDU de-aggregation, MPDU header and cyclic redundancy code (CRC) validation, duplicate removal, possible reordering if the Block Ack mechanism is used, decryption, defragmentation, integrity checking, and replay detection. After replay detection (or defragmentation if security is used) ~~and~~ possible A-MSDU de-aggregation and possible MSDU rate limiting, the one or more MSDUs ~~is~~ are delivered to the MAC_SAP or to the DS. The IEEE 802.1X Controlled/Uncontrolled Ports discard ~~the~~ any received MSDU if the Controlled Port is not enabled and if the MSDU does not represent an IEEE 802.1X frame. TKIP and CCMP MPDU frame order enforcement occurs after decryption, but prior to MSDU defragmentation; therefore, defragmentation will fail if MPDUs arrive out of order.

Replace Figure 6-1—MAC data plane architecture with the following figure:

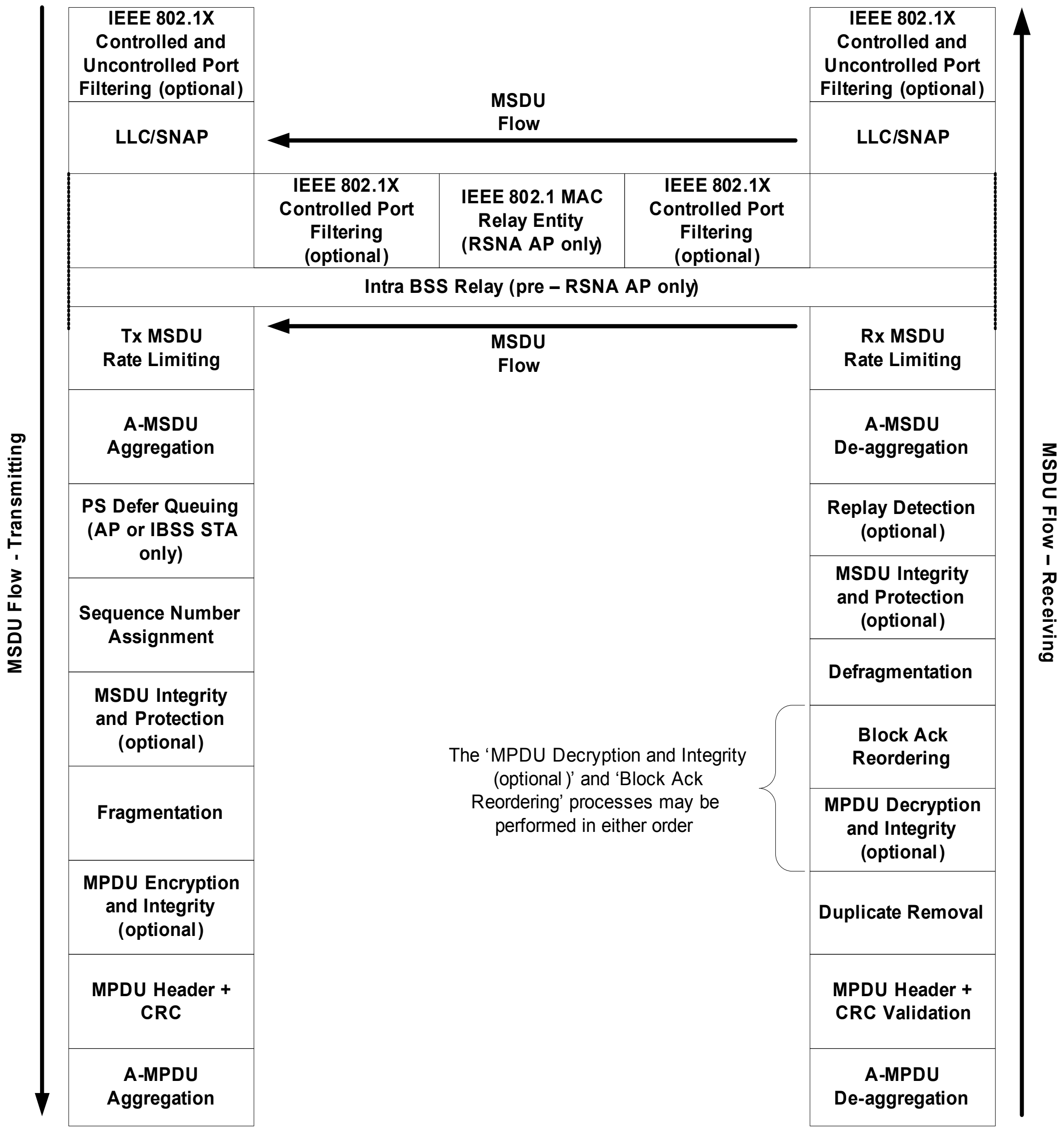
IEEE 802.1X Controlled and Uncontrolled Port Filtering (optional)
LLC/SNAP
MSDU Flow
IEEE 802.1X Controlled and Uncontrolled Port Filtering (optional)
LLC/SNAP
IEEE 802.1X Controlled Port Filtering (optional)
IEEE 802.1 MAC Relay Entity (RSNA AP only)
IEEE 802.1X Controlled Port Filtering (optional)
Intra BSS Relay (pre – RSNA AP only)
Tx MSDU Rate Limiting
MSDU Flow
Rx MSDU Rate Limiting
MSDU Flow - Transmitting
A-MSDU Aggregation
PS Defer Queuing (AP or IBSS STA only)
Sequence Number Assignment
MSDU Integrity and Protection (optional)
Fragmentation
MPDU Encryption and Integrity (optional)
MPDU Header + CRC
A-MPDU Aggregation
A-MSDU De-aggregation
Replay Detection (optional)
MSDU Integrity and Protection (optional)
Defragmentation
Block Ack Reordering
MPDU Decryption and Integrity (optional)
Duplicate Removal
MPDU Header + CRC Validation
A-MPDU De-aggregation
MSDU Flow – Receiving
The 'MPDU Decryption and Integrity (optional)' and 'Block Ack Reordering' processes may be performed in either order

Figure 6-1—MAC data plane architecture

6.2 Detailed service specification

6.2.1 MAC Data Services

6.2.1.1 MA-UNITDATA.request

6.2.1.1.4 Effect of receipt

Insert the following text after the first paragraph of 6.2.1.1.4.

At an AP for which dot11SSPNInterfaceEnabled is true, upon receipt of an MA-UNITDATA.request primitive having an individually addressed destination address and a priority of Contention or ContentionFree, the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationMaxAuthBestEffortRate in the dot11InterworkingEntry identified by the destination MAC address of the frame to be transmitted. The specific mechanism to perform rate limiting is outside the scope of this specification.

- If the rate limiting mechanism does not discard the frame, then dot11NonAPStationBestEffortMSDUCount shall be incremented by 1 and dot11NonAPStationBestEffortOctetCount shall be incremented by the number of octets in the MSDU.
- If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedBestEffortMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedBestEffortOctetCount shall be incremented by the number of octets in the MSDU.

At an AP for which dot11SSPNInterfaceEnabled is true, upon receipt of an MA-UNITDATA.request primitive having an individually addressed destination address for which the priority is an integer in the range of 0 to 7, inclusive, then the AP's MAC sublayer shall derive the access category from the priority using the mapping in Table 9-1. The AP's MAC sublayer shall retrieve the MIB variables listed below from the dot11InterworkingEntry identified by the destination MAC address of the frame to be transmitted and perform the following operations:

- If the access category is AC_VO, then the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationMaxAuthVoiceRate; the specific mechanism to perform rate limiting is outside the scope of this specification. If the rate limiting mechanism does not discard the frame, then dot11NonAPStationVoiceMSDUCount shall be incremented by 1 and dot11NonAPStationVoiceOctetCount shall be incremented by the number of octets in the MSDU. If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedVoiceMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedVoiceOctetCount shall be incremented by the number of octets in the MSDU.
- If the access category is AC_VI, then the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationMaxAuthVideoRate; the specific mechanism to perform rate limiting is outside the scope of this specification. If the rate-limiting mechanism does not discard the frame, then dot11NonAPStationVideoMSDUCount shall be incremented by 1 and dot11NonAPStationVideoOctetCount shall be incremented by the number of octets in the MSDU. If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedVideoMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedVideoOctetCount shall be incremented by the number of octets in the MSDU.
- If the access category is AC_BE, then the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationMaxAuthBestEffortRate; the specific mechanism to perform rate limiting is outside the scope of this specification. If the rate-limiting mechanism

does not discard the frame, then dot11NonAPStationBestEffortMSDUCount shall be incremented by 1 and dot11NonAPStationBestEffortOctetCount shall be incremented by the number of octets in the MSDU. If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedBestEffortMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedBestEffortOctetCount shall be incremented by the number of octets in the MSDU.

— If the access category is AC_BK, then the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationMaxAuthBackgroundRate; the specific mechanism to perform rate limiting is outside the scope of this specification. If the rate-limiting mechanism does not discard the frame, then dot11NonAPStationBackgroundMSDUCount shall be incremented by 1 and dot11NonAPStationBackgroundOctetCount shall be incremented by the number of octets in the MSDU. If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedBackgroundMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedBackgroundOctetCount shall be incremented by the number of octets in the MSDU.

At an AP for which dot11SSPNInterfaceEnabled is true, upon receipt of an MA-UNITDATA.request primitive having an individually addressed destination address whose priority is an integer in the range of 8 to 15, inclusive, then the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationAuthMaxHCCAHEMMRate; the specific mechanism to perform rate limiting is outside the scope of this specification.

— If the rate-limiting mechanism does not discard the frame, then dot11NonAPStationHCCAHEMMMSDUCount shall be incremented by 1, and dot11NonAPStationHCCAHEMMOctetCount shall be incremented by the number of octets in the MSDU.

— If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedHCCAHEMMMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedHCCAHEMMOctetCount shall be incremented by the number of octets in the MSDU.

6.2.1.2 MA-UNITDATA.indication

6.2.1.2.4 Effect of receipt

Insert the following text after the first paragraph of 6.2.1.2.4.

At an AP for which dot11SSPNInterfaceEnabled is true, upon receipt of a frame of type data with broadcast/ multicast DA, the AP's MAC sublayer shall discard the frame if dot11NonAPStationAuthSourceMulticast is false in the dot11InterworkingEntry identified by the source MAC address of the received frame. If dot11NonAPStationAuthSourceMulticast is true, the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationAuthMaxSourceMulticastRate in the dot11InterworkingEntry identified by the source MAC address of the received frame. The specific mechanism to perform rate limiting is outside the scope of this specification.

— If the rate limiting mechanism does not discard the frame, then dot11NonAPStationMulticastMSDUCount shall be incremented by 1 and dot11NonAPStationMulticastOctetCount shall be incremented by the number of octets in the MSDU.

— If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedMulticastMSDUCount. shall be incremented by 1 and dot11NonAPStationDroppedMulticastOctetCount. shall be incremented by the number of octets in the MSDU.

At an AP for which dot11SSPNInterfaceEnabled is true, upon receipt of an individually addressed frame of type data and a priority of Contention or ContentionFree, then the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationMaxAuthBestEffortRate in the dot11InterworkingEntry identified by the source MAC address of the received frame. The specific mechanism to perform rate limiting is outside the scope of this specification.

- If the rate limiting mechanism does not discard the frame, then dot11NonAPStationBestEffortMSDUCount shall be incremented by 1 and dot11NonAPStationBestEffortOctetCount shall be incremented by the number of octets in the MSDU.
- If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedBestEffortMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedBestEffortOctetCount shall be incremented by the number of octets in the MSDU.

At an AP for which dot11SSPNInterfaceEnabled is true, upon receipt of an individually addressed frame of type data, for which the priority is an integer in the range of 0 to 7, inclusive, then the AP's MAC sublayer shall derive the access category from the priority using the mapping in Table 9-1. The AP's MAC sublayer shall retrieve the MIB variables from the dot11InterworkingEntry identified by the source MAC address of the received frame and perform the following operations:

- If the access category is AC_VO, then the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationMaxAuthVoiceRate; the specific mechanism to perform rate limiting is outside the scope of this specification. If the rate-limiting mechanism does not discard the frame, then dot11NonAPStationVoiceMSDUCount shall be incremented by 1 and dot11NonAPStationVoiceOctetCount shall be incremented by the number of octets in the MSDU. If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedVoiceMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedVoiceOctetCount shall be incremented by the number of octets in the MSDU.
- If the access category is AC_VI, then the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationMaxAuthVideoRate; the specific mechanism to perform rate limiting is outside the scope of this specification. If the rate-limiting mechanism does not discard the frame, then dot11NonAPStationVideoMSDUCount shall be incremented by 1 and dot11NonAPStationVideoOctetCount shall be incremented by the number of octets in the MSDU. If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedVideoMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedVideoOctetCount shall be incremented by the number of octets in the MSDU.
- If the access category is AC_BE, then the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationMaxAuthBestEffortRate; the specific mechanism to perform rate limiting is outside the scope of this specification. If the rate-limiting mechanism does not discard the frame, then dot11NonAPStationBestEffortMSDUCount shall be incremented by 1 and dot11NonAPStationBestEffortOctetCount shall be incremented by the number of octets in the MSDU. If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedBestEffortMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedBestEffortOctetCount shall be incremented by the number of octets in the MSDU.
- If the access category is AC_BK, then the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationMaxAuthBackgroundRate; the specific mechanism to perform rate limiting is outside the scope of this specification. If the rate-limiting mechanism does not discard the frame, then dot11NonAPStationBackgroundMSDUCount shall be incremented by 1 and dot11NonAPStationBackgroundOctetCount shall be incremented by the number of octets in the MSDU. If the rate limiting mechanism discards the frame, then

dot11NonAPStationDroppedBackgroundMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedBackgroundOctetCount shall be incremented by the number of octets in the MSDU.

At an AP for which dot11SSPNInterfaceEnabled is true, upon receipt of an individually addressed frame of type data for which the priority is an integer in the range of 8 to 15, inclusive, the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationAuthMaxHCCAHEMMRate; the specific mechanism to perform rate limiting is outside the scope of this specification.

- If the rate-limiting mechanism does not discard the frame, then dot11NonAPStationHCCAHEMMMSDUCount shall be incremented by 1, and dot11NonAPStationHCCAHEMMOctetCount shall be incremented by the number of octets in the MSDU.
- If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedHCCAHEMMMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedHCCAHEMMOctetCount shall be incremented by the number of octets in the MSDU.

6.2.1.3 MA-UNITDATA.confirm

6.2.1.3.1 Function

Insert the following items into the bulleted list after item i) as shown below:

j) For APs with dot11SSPNInterfaceEnabled set to TRUE, Undeliverable (violation of limit specified by dot11NonAPStationMaxAuthVoiceRate in the dot11InterworkingTable for the non-AP STA identified by the destination address of the MA-UNITDATA.request primitive).

k) For APs with dot11SSPNInterfaceEnabled set to TRUE, Undeliverable (violation of limit specified by dot11NonAPStationMaxAuthVideoRate in the dot11InterworkingTable for the non-AP STA identified by the destination address of the MA-UNITDATA.request primitive).

l) For APs with dot11SSPNInterfaceEnabled set to TRUE, Undeliverable (violation of limit specified by dot11NonAPStationMaxAuthBestEffortRate in the dot11InterworkingTable for the non-AP STA identified by the destination address of the MA-UNITDATA.request primitive).

m) For APs with dot11SSPNInterfaceEnabled set to TRUE, Undeliverable (violation of limit specified by dot11NonAPStationBackgroundRate in the dot11InterworkingTable for the non-AP STA identified by the destination address of the MA-UNITDATA.request primitive).

7. Frame formats

7.1 MAC frame formats

7.2 Format of individual frame types

7.2.3 Management frames

7.2.3.1 Beacon frame format

Change Table 7-8 by inserting text in the order 31 Multiple BSSID and adding order 45 through 48 information fields as shown below

Table 7-8—Beacon frame body

Order	Information	Notes
31	Multiple BSSID	One or more Multiple BSSID elements are present if dot11RRMMeasurementPilotCapability is a value between 2 and 7 and the AP is a member of a Multiple BSSID Set (see 11.10.11) with two or more members, or if dot11MgmtOptionMultiBSSIDEnabled is set to TRUE or if dot11InterworkingServiceEnabled is true and the AP is a member of a Multiple BSSID Set with two or more members and the value of at least one dot11GASAdvertisementID is not null.
45	Interworking	The Interworking element is present if dot11InterworkingServiceEnabled is true.
46	Advertisement Protocol	Advertisement Protocol element is present if dot11InterworkingServiceEnabled is true and the value of at least one dot11GASAdvertisementID is non null.
47	Roaming Consortium	The Roaming Consortium element is present if dot11InterworkingServiceEnabled is true and the dot11RoamingConsortiumTable has at least one non-null entry.
48	Emergency Alert	One or more Emergency Alert Identifier elements are present if dot11EASEnabled is true and there are one or more EAS message(s) active in the network.

7.2.3.4 Association Request frame format

Insert the order 18 information field into Table 7-11:

Table 7-11—Association Request frame body

Order	Information	Notes
18	Interworking	The Interworking element is present if dot11InterworkingServiceEnabled is true and the non-AP STA is requesting un-authenticated access to emergency services (see 11.3.2).

7.2.3.5 Association Response frame format

Insert the order 20 information field into Table 7-11:

Table 7-11—Association Response frame body

Order	Information	Notes
20	QoS Map	QoS Map is present if dot11QosMapEnabled is true and the QoS Map field in the Extended Capabilities element of the corresponding Association Request frame is set to 1.

7.2.3.6 Reassociation Request frame format

Insert the order 13 information field into Table 7-12

Table 7-12—Reassociation Request frame body

Order	Information	Notes
13	Interworking	The Interworking element is present if dot11InterworkingServiceEnabled is true and the non-AP STA is requesting un-authenticated access to emergency services (see 11.3.2).

7.2.3.7 Reassociation Response frame format

Insert the order 24 information field into Table 7-13:

Table 7-13—Reassociation Response frame body

Order	Information	Notes
24	QoS Map	QoS Map is present if dot11QosMapEnabled is true and the QoS Map field in the Extended Capabilities element of the corresponding Reassociation Request frame is set to 1.

7.2.3.8 Probe Request frame format

Insert order 12 information field into Table 7-14:

Table 7-14—Probe Request frame body

Order	Information	Notes
12	Interworking	The Interworking element is present if dot11InterworkingServiceEnabled is true.

7.2.3.9 Probe Response frame format

Change Table 7-15 by inserting text in order 24 Multiple BSSID and adding order 42 through 44 information fields as shown below:

Table 7-15—Probe Response frame body

Order	Information	Notes
24	Multiple BSSID	One or more Multiple BSSID elements are present if dot11RRMMeasurementPilotCapability is set to a value between 2 and 7 and the AP is a member of a Multiple BSSID Set (see 11.10.11) with two or more members, or if dot11MgmtOptionMultiBSSIDEnabled is set to true or if dot11InterworkingServiceEnabled is true and the AP is a member of a Multiple BSSID Set with two or more members and the value of at least one dot11GASAdvertisementID is not null.
44	Interworking	The Interworking element is present if dot11InterworkingServiceEnabled is true.
45	Advertisement Protocol	Advertisement Protocol element is present if dot11InterworkingServiceImplemented is true and at least one dot11GASAdvertisementID is not null.
46	Roaming Consortium	The Roaming Consortium element is present if dot11InterworkingServiceEnabled is true and the dot11RoamingConsortiumTable has at least one non-null entry.
47	Emergency Alert	One or more Emergency Alert Identifier elements are present if dot11EASEnabled is true and there are one or more EAS message(s) active in the network.

7.3 Management frame body components

7.3.1 Fields that are not information elements

7.3.1.7 Reason Code field

Insert the following items at the end of Table 7-22.

Table 7-22—Reason codes

Reason Code	Meaning
27	Disassociated because session terminated by SSP request
28	Disassociated because of lack of SSP roaming agreement
29	Requested service rejected because of SSP cipher suite or AKM requirement
30	Requested service not authorized in this location
46	Disassociated because authorized access limit reached
47	Disassociated due to external service requirements

7.3.1.9 Status Code field

Insert the following items to the end of Table 7-23 as shown below:

Table 7-23—Status Codes

Status Code	Meaning
59	GAS Advertisement Protocol not supported
60	No outstanding GAS request
61	GAS Response not received from the server in the external network
62	AP timed out waiting for GAS Query Response from the server in an external network
63	Partial GAS Query Response returned—MMPDU cannot hold all requested NQP elements
64	Advertisement server in the network is not currently reachable
65	Requested information is not configured for this BSSID
66	Request refused due to permissions received via SSPN interface
67	Request refused because AP does not support Emergency Services
68	Partial GAS Query Response returned - one or more of the requested NPQ elements is not configured for this BSSID

Insert the following new subclause after 7.3.1.30.

7.3.1.33 GAS Query Response Fragment ID

A GAS Query Fragment Response ID is used by the AP when a GAS Query Response spans multiple MMPDUs. APs use this field to inform the non-AP STA of the GAS fragment number (and thus if any fragments are missing) of the transmitted frames as well as identifying the last GAS fragment of the Query Response. The maximum value permitted in the GAS Query Response Fragment ID is 127. The More GAS Fragments field is set to 1 in GAS Query Response fragments of GAS Comeback Response Action frames that have another GAS fragment of the current query response to follow; otherwise, it is set to 0. The format of GAS Query Response Fragment ID is shown in Figure 7-36r.

	B0 B6	B7
	GAS Query Response Fragment ID	More GAS Fragments
Bits:	7	1

Figure 7-36r—GAS Query Response Fragment ID

7.3.2 Information elements

Insert the following to the contents of Table 7-26 as shown below:

Table 7-26—Element IDs

Information Element	**Element ID**	**Length (in octets)**	**Extensible**
Interworking (see 7.3.2.89)	107	3, 4, 5, 6, 9, 10, 11, 12	
Advertisement Protocol (see 7.3.2.90)	108	4 to 257	
Expedited bandwidth request (see 7.3.2.91)	109	3	
QoS Map Set (see 7.3.2.92)	110	18 to 60	Yes
Roaming Consortium (see 7.3.2.93)	111	variable	Yes
Emergency Alert (see 7.3.2.94)	112	variable	

7.3.2.27 Extended Capabilities information element

Insert the following additional rows at the end of Table 7-35a.

Table 7-35a—Capabilities field

Bit(s)	Information	Notes
28	Interworking	When dot11InterworkingServiceEnabled is set to TRUE, the Interworking field is set to 1 to indicate the STA supports Interworking Service as described in 11.23. When dot11InterworkingServiceEnabled is set to FALSE, the Interworking field is set to 0 to indicate the STA does not support this capability.
29	QoS Map	When dot11QosMapEnabled is set to TRUE, the QoS Map field is set to 1 to indicate the STA supports QoS Map service as described in 11.23.7. When dot11QosMapEnabled is set to FALSE, the QoS Map field is set to 0 to indicate the STA does not support this capability.
31	EBR	When dot11EBREnabled is set to TRUE, the EBR field is set to 1 to indicate the STA supports EBR as described in 7.3.2.91. When dot11EBREnabled is set to FALSE, the EBR field is set to 0 to indicate the STA does not support this capability.
32	SSPN Interface	When dot11SSPNInterfaceEnabled is set to TRUE, the SSPN Interface field is set to 1 to indicate the AP supports SSPN Interface service as described in 11.23.4. When dot11SSPNInterfaceEnabled is set to FALSE, the SSPN Interface is set to 0 to indicate the AP does not support this capability.
33	EAS	When dot11EASEnabled is set to TRUE, the EAS field is set to 1 to indicate the STA supports the EAS mechanism as described in 11.23.5. When dot11EASEnabled is set to FALSE, the EAS field is set to 0 to indicate the STA does not support this capability
34	MSGCF Capability	When dot11MSGCFEnabled is set to TRUE, the MSGCF Capability field is set to 1 to indicate the non-AP STA supports the MSGCF in 11B. When dot11MSGCFEnabled is set to FALSE, the MSGCF Capability is set to 0 to indicate the non-AP STA does not support this capability.

Insert the following new subclauses:

7.3.2.89 Interworking information element

The Interworking information element contains information about the Interworking Service capabilities of a STA as shown in Figure 7-95o113.

	Element ID	Length	Access Network Options	Venue Info (optional)	HESSID (optional)
Octets:	1	1	1	0 or 2	0 or 6

Figure 7-95o113—Interworking element format

The Length is a one-octet field whose value is 1 plus the length of each optional field present in the element.

The format of Access Network Options field is shown in Figure 7-95o114.

Bits:	B0 - B3	B4	B5	B6	B7
	Network Type	Internet	ASRA	ESC	UESA

Figure 7-95o114—Access Network Options format

A non-AP STA sets Internet, ASRA, ESC and UESA fields to 0 when including the Interworking element in the Probe Request frame. A non-AP STA sets the Internet, ASRA, and ESC bits to 0 when including the Interworking element in (Re)association request frames. In (Re)association request frames, a non-AP STA sets the UESA bit according to the procedures in 11.23.5. The Network Type Codes are shown in Table 7-43bb. The Network Type field is set by the AP to advertise its Network Type to non-AP STAs. A non-AP STA uses this field to indicate the desired Network Type in an active scan. See Annex W.1 for informative text on usage of fields contained within the Interworking element.

Table 7-43bb—Network Type codes

Network Type Codes	Meaning	Description
0	Private network	Non-authorized users are not permitted on this network. Examples of this network type are home networks and enterprise networks, which may employ user accounts. Private networks do not necessarily employ encryption.
1	Private network with guest access	Private network but guest accounts are available. Example of this network type is enterprise network offering access to guest users.
2	Chargeable public network	The network is accessible to anyone, however, access to the network requires payment. Further information on types of charges may be available through other methods (e.g., 802.21, http/https redirect or DNS redirection). Examples of this network type is a hotspot in a coffee shop offering internet access on a subscription basis or a hotel offering in-room internet access service for a fee.
3	Free public network	The network is accessible to anyone and no charges apply for the network use. An example of this network type is an airport hotspot or municipal network providing free service.
4	Personal Device Network	A network of personal devices. An example of this type of network is a camera attaching to a printer, thereby forming a network for the purpose of printing pictures.
5 to 13	Reserved	Reserved
14	Test or experimental	The network is used for test or experimental purposes only.
15	Wildcard	Wildcard network type

Bit 4 is the Internet field. The AP sets this field to 1 if the network provides connectivity to the Internet; otherwise it is set to 0 indicating that it is unspecified whether the network provides connectivity to the Internet.

Bit 5 is the Additional Step Required for Access (ASRA) field. It is set to 1 by the AP to indicate that the network requires a further step for access. It is set to 0 whenever dot11RSNAEnabled is true. For more information, refer to Network Authentication Type Information in 7.3.4.4. The non-AP STAs set this bit to 0 in Probe Request frames.

Bit 6 is the Emergency Services Capability (ESC) field. It is set to 1 by the AP to indicate that higher layer Emergency Services are available at the AP. When ESC field is set to 0, the Emergency Services are not supported, see 11.23.5. The non-AP STAs set this bit to 0 in Probe Request frames.

Bit 7 is the Unauthenticated Emergency Service Accessible (UESA) field. When the AP sets it to 0, this field indicates that no unauthenticated emergency services are reachable through a BSS using this SSID. When set to 1, this field indicates that higher layer unauthenticated emergency services are reachable through a BSS using this SSID. A STA uses the Interworking information element with the UESA bit set to 1 to gain unauthenticated access to a BSS to access emergency services. See 11.23.5 together with Annex W.4.2 and Annex W.4.4. A non-AP STA sets the UESA field to 0 in Probe Request frames.

The Venue Info field is a 2-octet field. It contains Venue Group and Venue Type fields. The format of Venue Info field is shown in Figure 7-95o115.

	Venue Group	Venue Type
Octets:	1	1

Figure 7-95o115—Venue Info format

The Venue Group and Venue Type fields are both one octet values selected from Table 7-43bc and Table 7-43bd respectively. The entries in Table 7-43bc and Table 7-43bd are drawn from the International Building Code's Use and Occupancy Classifications [B52].

Table 7-43bc—Venue Group codes and descriptions

Venue Group Code	Venue Group Description
0	Unspecified
1	Assembly
2	Business
3	Educational
4	Factory and Industrial
5	Institutional
6	Mercantile
7	Residential
8	Storage
9	Utility and Miscellaneous
10	Vehicular
11	Outdoor
12	Personal Network
13 – 255	Reserved

Table 7-43bd—Venue Type assignments

Venue Group	Venue Type Code	Venue Description
0	0	Unspecified
0	1 - 255	Reserved
1	0	Unspecified Assembly
1	1	Arena
1	2	Stadium

Table 7-43bd—Venue Type assignments *(continued)*

Venue Group	Venue Type Code	Venue Description
1	3	Passenger Terminal (e.g., airport, bus, ferry, train station)
1	4	Amphitheater
1	5	Amusement Park
1	6	Place of Worship
1	7	Convention Center
1	8	Library
1	9	Museum
1	10	Restaurant
1	11	Theater
1	12	Bar
1	13	Coffee Shop
1	14	Zoo or Aquarium
1	15	Emergency Coordination Center
1	16 - 255	Reserved
2	0	Unspecified Business
2	1	Doctor or Dentist office
2	2	Bank
2	3	Fire Station
2	4	Police Station
2	6	Post Office
2	7	Professional Office
2	8	Research and Development Facility
2	9	Attorney Office
2	10 – 255	Reserved
3	0	Unspecified Educational
3	1	School, Primary
3	2	School, Secondary
3	3	University or College
3	4-255	Reserved
4	0	Unspecified Factory and Industrial
4	1	Factory
4	2 – 255	Reserved
5	0	Unspecified Institutional
5	1	Hospital
5	2	Long-Term Care Facility (e.g., Nursing home, Hospice, etc.)
5	3	Alcohol and Drug Re-habilitation Center
5	4	Group Home

Table 7-43bd—Venue Type assignments *(continued)*

Venue Group	Venue Type Code	Venue Description
5	5	Prison or Jail
5	6 – 255	Reserved
6	0	Unspecified Mercantile
6	1	Retail Store
6	2	Grocery Market
6	3	Automotive Service Station
6	4	Shopping Mall
6	5	Gas Station
6	6 – 255	Reserved
7	0	Unspecified Residential
7	1	Hotel or Motel
7	2	Dormitory
7	3	Boarding House
7	4 – 255	Reserved
8	0 – 255	Reserved
9	0 – 255	Reserved
10	0	Unspecified Vehicular
10	1	Automobile or Truck
10	2	Airplane
10	3	Bus
10	4	Ferry
10	5	Ship or Boat
10	6	Train
10	7	Motor Bike
10	8 – 255	Reserved
11	0	Unspecified Outdoor
11	1	Muni-mesh Network
11	2	City Park
11	3	Rest Area
11	4	Traffic Control
11	5– 255	Reserved
12	0	Reserved

The HESSID field, which is the identifier for a homogeneous ESS, specifies the value of HESSID, see 11.23.1. A non-AP STA uses this field to indicate the desired HESSID in an active scan. The HESSID field for an AP is set to the value of dot11HESSID. Procedures for setting the proper HESSID value are defined in 11.1.3.

7.3.2.90 Advertisement Protocol element

The Advertisement Protocol element contains information that identifies a particular advertisement protocol and its corresponding Advertisement Control. The Advertisement Protocol information element format is shown in Figure 7-95o116.

	Element ID	Length	Advertisement Protocol Tuple # 1	Advertisement Protocol Tuple # 2 (optional)	...	Advertisement Protocol Tuple # n (optional)
Octets:	1	1	variable	variable		variable

Figure 7-95o116—Advertisement Protocol element format

The Length is a one-octet field whose value is equal to the sum of the lengths of the Advertisement Protocol Tuple fields.

The format of Advertisement Protocol Tuple is shown in Figure 7-95o117.

	B0 - B6	B7	
	Query Response Length Limit	PAME-BI	Advertisement Protocol ID
Octets:	◄—— 1	——►	variable

Figure 7-95o117—Advertisement Protocol Tuple format

The Advertisement Protocol Tuple field is defined as follows:

- The Query Response Length Limit indicates the maximum number of octets an AP will transmit in the Query Response field contained within one or more GAS Comeback Response Action frames. The Query Response Length Limit may be set to a value larger than the maximum MMPDU size in which case the Query Response spans multiple MMPDUs. The Query Response Length Limit is encoded as an integer number of 256 octet units. A value of zero is not permitted. A value of 0x7F means the maximum limit enforced is determined by the maximum allowable number of fragments in the GAS Query Response Fragment ID (see 7.3.1.33). The non-AP STA sets the Query Response Length Limit to zero on transmission and the AP ignores it upon reception.
- Bit 7, the Pre-Association Message Exchange BSSID Independent (PAME-BI) bit, is used by an AP to indicate whether the Advertisement server, which is the non-AP STA's peer for this advertisement protocol, will return a Query Response which is independent of the BSSID used for the GAS frame exchange. This bit is set to 1 to indicate the Query Response is independent of the BSSID; it is set to zero to indicate that the Query Response may be dependent on the BSSID. See 11.23.2.2.4 for further information. Bit 7 is reserved for non-AP STAs.
- The Advertisement Protocol ID is a variable length field. If the first octet of this field is the vendor specific Advertisement Protocol ID as provided in Table 7-43be, then this field will be structured per the Vendor Specific information defined in 7.3.2.26, where the Element ID of the Vendor Specific

element of 7.3.2.26 is the vendor specific Advertisement Protocol ID; otherwise its length is one octet and its value is one of the values in Table 7-43be. When one or more vendor-specific tuples are included in the Advertisement Protocol information element, their total length needs to be constrained such that the total length of all the Advertisement Protocol Tuple fields (both vendor specific and otherwise) is less than or equal to 255 octets.

Table 7-43be—Advertisement Protocol ID definitions

Name	Value
Native Query Protocol	0
MIH Information Service	1
MIH Command and Event Services Capability Discovery	2
Emergency Alert System (EAS)	3
Location-to-Service Translation Protocol	4
Reserved	5-220
Vendor Specific	221
Reserved	222-255

— Native Query Protocol (NQP) is a protocol used by a requesting STA to query another STA for locally configured data (i.e., the receiving STA can respond to queries without proxying the query to a server in an external network).

— MIH Information Service is a service defined in IEEE 802.21 (see IEEE P802.21-2008) to support information retrieval from an information repository in an external network.

— MIH Command and Event Services capability discovery is a mechanism defined in IEEE 802.21 (see IEEE P802.21-2008) to support discovering capabilities of command service and event service entities in an external network.

— The Emergency Alert System (EAS) service allows a network to disseminate emergency alert notifications from an external network to unauthenticated or unassociated or associated non-AP STAs. To provide a standardized alerting system, EAS uses the Common Alerting Protocol (CAP) (see OASIS CAP) carrying EDXL (see OASIS EDXL) formatted messages. Utilizing GAS and EAS Advertisement Protocol ID, CAP and EDXL can operate transparently over the air interface. The structure of the CAP Alert Message is defined in 1.3 of OASIS CAP. The message format itself is defined in 3.2 of OASIS EDXL, which is a special emergency type of XML message. The underlying transport mechanism in IEEE 802.11 networks for CAP is HTTP.

— Location-to-Service Translation Protocol (LoST) is used by a non-AP STA to access information from PSAP databases, for example a local emergency dial-string. It is also used to determine the location-appropriate PSAP URI for emergency services. The operation and message format is defined in RFC 5222. The underlying transport mechanism for LoST is HTTP.

— Advertisement Protocol ID 221 is reserved for Vendor Specific advertisement protocols. When the Advertisement Protocol ID is equal to 221, the format of the Advertisement Protocol element follows the format of the vendor specific information element in 7.3.2.26.

7.3.2.91 Expedited Bandwidth Request information element

The Expedited Bandwidth Request information element is transmitted from a non-AP STA to an AP in an ADDTS Request Action frame containing a TSPEC request and provides usage information for the bandwidth request. The expedited bandwidth request element format is shown in Figure 7-95o118.

	Element ID	Length	Precedence Level
Octets:	1	1	1

Figure 7-95o118—Expedited Bandwidth Request element format

The Length field is set to 1.

The precedence level field is provided in Table 7-43bf

Table 7-43bf—Precedence Level field description

Precedence Level Value	Description
0-15	Reserved
16	Emergency call, defined in [B55]
17	First responder (public)
18	First responder (private)
19	MLPP Level A
20	MLPP Level B
21	MLPP Level 0
22	MLPP Level 1
23	MLPP Level 2
24	MLPP Level 3
25	MLPP Level 4
26-255	Reserved

The precedence levels are derived from “3GPP TS 22.067” [B40].

The first responders (public) in Table 7-43bf are government agencies or entities acting on behalf of the government, and the first responders (private) are private entities, such as individuals or companies.

7.3.2.92 QoS Map Set information element

The QoS Map Set information element is transmitted from an AP to a non-AP STA and provides the mapping of higher-layer quality of service constructs to User Priorities defined by transmission of Data frames in this standard. This information element maps the higher-layer priority from the DSCP field used with the Internet Protocol to User Priority as defined by this standard. The QoS Map Set element is shown in Figure 7-95o119.

	Element ID	Length	DSCP Exception #1 (optional)	...	DSCP Exception #n (optional)	UP 0 DSCP Range	UP 1 DSCP Range	UP 2 DSCP Range	...	UP 7 DSCP Range
Octets:	1	1	2		2	2	2	2		2

Figure 7-95o119—QoS Map Set element description

The Length field is set to 16+2×n, where n is the number of Exception fields in the QoS Map set.

DSCP Exception fields are optionally included in the QoS Map Set. If included, the QoS Map Set has a maximum of 21 DSCP Exception fields. The format of the exception field is shown in Figure 7-95o120.

	DSCP Value	User Priority
Octets:	1	1

Figure 7-95o120—DSCP Exception format

The DSCP value in the DSCP Exception field is in the range 0 to 63 inclusive, or 255; the User Priority value is between 0 and 7, inclusive.

- When a non-AP STA begins transmission of a Data frame containing the Internet Protocol, it matches the DSCP field in the IP header to the corresponding DSCP value contained in this element. The non-AP STA will first attempt to match the DSCP value to a DSCP exception field and uses the UP from the corresponding UP in the same DSCP exception field if successful; if no match is found then the non-AP STA attempts to match the DSCP field to a UP n DSCP Range field, and uses the n as the UP if successful; and otherwise uses a UP of 0.
- Each DSCP Exception field has a different value of DSCP Value.

	DSCP Low Value	DSCP High Value
Octets:	1	1

Figure 7-95o121—DSCP Range description

The QoS Map Set has a DSCP Range field corresponding to each of the 8 user priorities. The format of the range field is shown in Figure 7-95o121. The DSCP Range value is between 0 and 63 inclusive, or 255.

- The DSCP range for each user priority is non-overlapping.
- The DSCP High Value is greater than or equal to the DSCP Low Value.

- — If the DSCP Range high value and low value are both equal to 255, then the corresponding UP is not used.

7.3.2.93 Roaming Consortium information element

The Roaming Consortium Information element contains information identifying the roaming consortium and/ or SSP whose security credentials can be used to authenticate with the AP transmitting this element. The element's format is shown in Figure 7-95o122.

	Element ID	Length	Number of Native-GAS OIs	OI #1 and #2 Lengths	OI #2 (optional)	OI #3 (optional)
Octets:	1	1	1	variable	variable	variable

Figure 7-95o122—Roaming Consortium element format

The Length is a one-octet field whose value is equal to 2 plus the sum of the number of octets in each OI field present.

The Number of Native-GAS OIs field's format is a one-octet unsigned integer whose value is the number of additional roaming consortium OIs obtainable via NQP. A value of zero means that no additional OIs will be returned in response to a Native GAS query for the Roaming Consortium List. A value of 255 means that 255 or more additional OIs are obtainable via NQP.

The OI #1 and #2 Lengths field format is shown in Figure 7-95o123.

- — The value of the OI #1 Length subfield is the length in octets of the OI #1 field.
- — The value of the OI #2 Length subfield is the length in octets of the OI #2 field. If the OI #2 field is not present, the value of the OI #2 Length subfield is set to zero.

Note—When there are three OIs, the OI #3 Length is calculated by subtracting the value of the OI #1 and #2 Lengths field from the value of the Length field.

Bits:	B0 - B3	B4 - B7
	OI #1 Length	OI #2 Length

Figure 7-95o123—OI Lengths field format

The OI field is defined in 7.3.1.21. Each OI identifies a roaming consortium (group of SSPs with inter-SSP roaming agreement) or a single SSP. A non-AP STA in possession of security credentials for the SSPN(s) identified by the OI should be able to successfully authenticate to this AP. The value of the OI(s) in this table are equal to the value of the first 3 OIs in the dot11RoamingConsortiumTable. If fewer than 3 values are defined in the dot11RoamingConsortiumTable, then only as many OIs as defined in the table are populated in this element.

7.3.2.94 Emergency Alert information element

The Emergency Alert information element provides a hash to identify instances of the active EAS messages which are currently available from the network. The hash allows the non-AP STA to assess whether an EAS message advertised by an AP has been previously received and therefore whether it is necessary to download from the network. The format of the Emergency Alert information element is provided in Figure 7-95o124.

	Element ID	Length	Alert Identifier Hash
Octets:	1	1	8

Figure 7-95o124—Emergency Alert Identifier element format

The Length is a 1-octet field whose value is equal to 8.

The Alert Identifier Hash (AIH) is a 8-octet field. It is a unique value used to indicate an instance of an EAS message. The value of this field is the hash produced by the HMAC-SHA1-64 hash algorithm operating on the EAS message.

AIH =HMAC-SHA1-64(“ES_ALERT”, Emergency_Alert_Message)

Where AIH is then truncated to the first 64 bits of this function.

Emergency_Alert_Message is the EAS message itself.

Insert the following new subclauses after 7.3.3:

7.3.4 Native Query Protocol elements

Native Query Protocol elements are defined to have a common format consisting of a 2-octet Info ID field, a 2-octet length field, and a variable-length element-specific information field. Each element is assigned a unique Info ID as defined in this standard. The Native Query Protocol query element format is shown in Figure 7-95o125. See Annex W.1 for informative text on NQP usage.

	Info ID	Length	Information
Octets:	2	2	variable

Figure 7-95o125—Native Query Protocol query element format

Each Native Query Protocol element in 7.3.4 is assigned a unique 2-octet Info ID. The set of valid Info IDs are defined in Table 7-43bg. The 2-octet Info ID is encoded following the conventions given in 7.1.1.

The Length field specifies the number of octets in the Information field and is encoded following the conventions given in 7.1.1.

7.3.4.1 Capability List

The Capability List provides a list of information/capabilities that has been configured on a STA. The Native

Query Protocol elements that may be configured are shown in Table 7-43bg. The Capability List element is returned in response to a Native GAS Query Request.

Table 7-43bg—Native Query Protocol info ID definitions

Info Name	Info ID	Native Info Element (clause)
Reserved	0-255	n/a
Capability List	256	7.3.4.1
Venue Name information	257	7.3.4.2
Emergency Call Number information	258	7.3.4.3
Network Authentication Type information	259	7.3.4.4
Roaming Consortium List	260	7.3.4.5
IP Address Type Availability information	261	7.3.4.7
NAI Realm List	262	7.3.4.8
3GPP Cellular Network information	263	7.3.4.9
AP Geospatial Location	264	7.3.4.10
AP Civic Location	265	7.3.4.11
Domain Name List	266	7.3.4.12
Emergency Alert URI	267	7.3.4.13
Reserved	268–56796	n/a
Native Query Protocol vendor-specific list	56797	7.3.4.6
Reserved	56798 – 65535	n/a

The format of the Capability List is provided in Figure 7-95o126.

	Info ID	Length	Info ID #1	Info ID #2 (optional)	…	Info ID #n (optional)	NQP Vendor-Specific List #1 (optional)	…	NQP Vendor-Specific List #n (optional)
Octets:	2	2	2	0 or 2	…	0 or 2	variable	…	variable

Figure 7-95o126—Capability List format

The Info ID is a 2-octet field whose value is drawn from Table 7-43bg corresponding to the Capability List.

The Length is a 2-octet field whose value is equal to 2 times the number of Info IDs present plus the number of octets in each NQP Vendor-Specific list.

Each Info ID included in the Capability List declares that a subsequent query for that Info ID will return the requested NQP element and will not return a response with status code indicating Requested information is not configured for this BSSID. Each Info ID returned is one of the Info IDs in Table 7-43bg. The Info ID for Capability list is always included in the Capability List returned in a Native-GAS Query Response. The list does not include any duplicate Info IDs, except possibly the Info ID for the NQP (Native Query Protocol) Vendor-specific list. The Info IDs returned in the Capability List are ordered by increasing Info ID value except for NQP Vendor-specific lists which are always ordered to be at the end.

The NQP Vendor-specific list is defined in 7.3.4.6. The Capability list is structured such that when an Info ID equal to the value of the NQP Vendor-specific list from Table 7-43bg is present, that Info ID is the Info ID of the NQP Vendor-specific list (i.e., it is the first 2 octets of the list). When a NQP Vendor-specific list is present in the Capability List, the Capability List element contains the capabilities of that vendor-specific query protocol.

7.3.4.2 Venue Name information

The Venue Name information provides one or more venue names associated with the BSS. The format of the Venue Name information is shown in Figure 7-95o127. The Venue Name information may be used to provide additional metadata on the BSS. For example, this information may be used to assist a user in selecting the appropriate BSS with which to associate. One or more Venue Name fields may be included in the same or different languages.

	Info ID	Length	Venue Name information (optional)	…	Venue Name information (optional)
Octets:	2	2	variable	…	variable

Figure 7-95o127—Venue Name information format

The Info ID field is equal to the value in Table 7-43bg corresponding to the Venue Name information as defined in Figure 7-95o127.

The Length is a 2-octet field whose value is equal to the number of octets in Venue Name information fields.

The format of the Venue Name information field is shown in Figure 7-95o128.

	Length	Language Code	Venue Name
Octets:	1	3	variable

Figure 7-95o128—Venue Name information field

- The Length is a one octet field whose value is equal to 3 plus the number of octets in the Venue Name field.
- The Language Code field is an ISO-14962-1997 [B54] encoded string that defines the language used in the Venue Name field. The Language Code field is a two or three character language code selected from ISO-639 [B53]. A two character language code has a zero (“null” in ISO-14962-1997) appended to make it 3 octets in length.
- The Venue Name field is a UTF-8 formatted field containing the venue’s name. The maximum length of this field is 252 octets. UTF-8 format is defined in RFC 3629.

7.3.4.3 Emergency Call Number information

The Emergency Call Number information provides a list of emergency phone numbers to call a PSAP that is used in a specific geographical area. The format of the Emergency Call Number information is provided in Figure 7-95o129.

	Info ID	Length	Emergency Call Number Unit #1	Emergency Call Number Unit #2 (optional)	…	Emergency Call Number Unit #N (optional)
Octets:	2	2	variable	variable	…	variable

Figure 7-95o129—Emergency Call Number information format

The Info ID field is equal to the value in Table 7-43bg corresponding to the Emergency Call Number information.

The Length is a 2-octet field whose value is determined by the number and size of the Emergency Call Number Units.

Each Emergency Call Number Unit has the structure shown in Figure 7-95o130.

	Length of Emergency Call Number	Emergency Call Number
Octets:	1	variable

Figure 7-95o130—Emergency Call Number Unit format

The Length of Emergency Call Number is a one octet field whose value is determined by the size of the Emergency Call Number field.

The Emergency Call Number field indicates the dialing digits used to obtain emergency services from the network. This field is encoded using the UTF-8 character set, defined in RFC 3629.

7.3.4.4 Network Authentication Type information

The Network Authentication Type information provides a list of authentication types when ASRA is set to 1 in 7.3.2.89. The format of the Network Authentication Type information is shown in Figure 7-95o131.

	Info ID	Length	Network Authentication Type Unit #1	Network Authentication Type Unit #2 (optional)	…	Network Authentication Type Unit #N (optional)
Octets:	2	2	variable	variable	…	variable

Figure 7-95o131—Network Authentication Type information format

The Info ID field is equal to the value in Table 7-43bg corresponding to the Network Authentication Type information.

The Length is a 2-octet field whose value is determined by the number and size of the Network Authentication Type Units.

Each Network Authentication Type Unit has the structure shown in Figure 7-95o132.

	Network Authentication Type Indicator	Re-direct URL Length	Re-direct URL (optional)
Octets:	1	2	variable

Figure 7-95o132—Network Authentication Type Unit

The Network Authentication Type Indicator has one of the values shown in Table 7-43bh.

Each Network Authentication Type Indicator defines additional information that may be communicated.

Table 7-43bh—Network Authentication Type Indicator

Value	Meaning
0	Acceptance of terms and conditions
1	On-line enrollment supported
2	http/https redirection
3	DNS redirection
4-255	Reserved

If the Network Authentication Type Indicator is zero, the network requires the user to accept terms and conditions, the Re-direct URL Length will be set to 0 and the Re-direct URL will not be present.

If the Network Authentication Type Indicator is 1, the network supports on-line enrollment. Higher-layer protocols on the non-AP STA may indicate to the user that accounts may be created. When the Network Authentication Type Indicator is 1, the Re-direct URL Length will be set to 0 and the Re-direct URL will not be present.

If the Network Authentication Type Indicator is 2 the network infrastructure performs http/https redirect.

If the Network Authentication Type Indicator is 3, the network supports DNS redirection. Higher layer software on the non-AP STA will exchange credentials with the network, the Re-direct URL Length will be set to 0 and the Re-direct URL will not be present.

The Re-direct URL Length field is a 2-octet field whose value is the length in octets of the Re-direct URL. The value of the Re-direct URL length field is set to 0 whenever the Re-direct URL is not present.

If the Network Authentication Type Indicator is 2, a re-direct URL may optionally be included. If the Network Authentication Type Indicator is other than 2, a re-direct URL is not included. The URL is formatted in accordance with RFC 3986.

7.3.4.5 Roaming Consortium List

The Roaming Consortium List provides a list of information about the Roaming Consortium and/or SSPs whose networks are accessible via this AP. This list may be returned in response to a Native GAS Query Request. The format of the Roaming Consortium List is provided in 7-95o133.

	Info ID	Length	OI Duple #1 (optional)	OI Duple #2 (optional)	…	OI Duple #N (optional)
Octets:	2	2	variable	variable		variable

Figure 7-95o133—Roaming Consortium List format

The Info ID field is equal to the value in Table 7-43bg corresponding to the Roaming Consortium List.

The Length is a 2-octet field whose value is dependent on the number and size of OIs present in the element.

The format of the OI Duple field is provided in Figure 7-95o126a. There are zero or more OI Duples in this list. OIs contained within the Roaming Consortium element (see 7.3.2.87) are also included in this list. The value of the OI subfield(s) in this list are equal to the values of the OI(s) in the dot11RoamingConsortiumTable.

— The value of the OI Length field is equal to the number of octets in the OI field.

- The OI field is a defined in 7.3.1.21. Each OI identifies a roaming consortium (group of SSPs with inter-SSP roaming agreement) or a single SSP. A non-AP STA in possession of security credentials for the SSPN(s) identified by the OI should be able to authenticate with this AP.

	OI Length	OI
Octets:	1	variable

Figure 7-95o134—OI Duple format

7.3.4.6 Native Query Protocol vendor specific list

The Native Query Protocol vendor-specific list is used to query for information not defined in this standard within a single defined format, so that reserved Info IDs are not usurped for nonstandard purposes and inter operability is more easily achieved in the presence of nonstandard information. The element is in the format shown in Figure 7-95o135.

	Info ID	Length	OI	Vendor Specific Content
Octets:	2	2	variable	variable

Figure 7-95o135—Native Query Protocol vendor specific query format

The Info ID field is equal to the value in Table 7-43bg corresponding to the Native Query Protocol vendor specific list.

The Length is a 2-octet field whose value is equal to the number of octets in the OI field plus the number of octets in the Vendor-Specific Content field.

The OI field is defined in 7.3.1.21.

The Vendor-Specific Content field is content that has been defined by the entity defined by the OI field.

7.3.4.7 IP Address Type Availability Information

The IP Address Type Availability information provides non-AP STA with the information about the availability of IP address version and type which could be allocated to the non-AP STA after successful association. This information may be returned in response to a Native GAS Query Request. The format of the IP

Address Type Availability information is shown in Figure 7-95o136.

	Info ID	Length	IP Address
Octets:	2	2	1

Figure 7-95o136—IP Address Type Availability information

The Info ID field is equal to the value in Table 7-43bg corresponding to the IP Address Type Availability information.

The Length is a 2-octet field whose value is 1.

The format of the IP Address field shown in Figure 7-95o137.

Bits:	B0 - B1	B2 - B7
	IPv6 Address	IPv4 Address

Figure 7-95o137—IP Address field format

The IPv6 address field format is shown in Table 7-43bi.

Table 7-43bi—IPv6 address field values

Address Value	Meaning
0	Address type not available
1	Address type available
2	Availability of the address type not known
3	Reserved

The IPv4 address field format is shown in Table 7-43bj.

.

Table 7-43bj— IPv4 address field values

Address Value	Meaning
0	Address type not available
1	Public IPv4 address available
2	Port-restricted IPv4 address available
3	Single NATed private IPv4 address available
4	Double NATed private IPv4 address available
5	Port-restricted IPv4 address and single NATed IPv4 address available
6	Port-restricted IPv4 address and double NATed IPv4 address available
7	Availability of the address type is not known
8 - 63	Reserved

7.3.4.8 NAI Realm List

The NAI Realm List provides a list of NAI Realms corresponding to SSPs or other entries whose networks or services are accessible via this AP; optionally included with each NAI Realm is a list of one or more EAP Method sub-fields, which that NAI Realm uses for authentication. The NAI Realm list may be returned in response to a Native GAS Query Request. The format of the NAI Realm List is provided in Figure 7-95o138.

	Info ID	Length	NAI Realm Count	NAI Realm Data #1 (optional)	NAI Realm Data #2 (optional)	. . .	NAI Realm Data #n (optional)
Octets:	2	2	1	variable	variable		variable

Figure 7-95o138—NAI Realm List format

The Info ID field is equal to the value in Table 7-43bg corresponding to the NAI Realm List.

The Length field is a 2-octet field whose value is determined by the number and size of the NAI Realm Data fields.

The NAI Realm count is a one-octet field which specifies the number of NAI Realms included in the NAI Realm list.

The format of the NAI Realm Data field is shown in Figure 7-95o139.

	NAI Realm Data Field Length	NAI Realm Encoding	NAI Realm Length	NAI Realm	EAP Method Count	EAP Method #1 (optional)	EAP Method #2 (optional)	. . .	EAP Method #n (optional)
Octets:	2	1	1	variable	1	variable	variable		variable

Figure 7-95o139—NAI Realm Data field format

NAI Realm Data Field Length is a 2-octet sub-field whose value is equal to 3 plus the length of the NAI Realm sub-field plus the sum of the lengths of the EAP Method List subfields.

The NAI Realm Encoding is a 1-octet sub-field whose format is shown in Figure 7-95o140.

The NAI Realm Encoding Type sub-field is a 1-bit sub-field. It is set to 0 to indicate that the NAI Realm in the NAI Realm sub-field is formatted in accordance with RFC-4282. It is set to 1 to indicate it is a UTF-8 formatted character string which is not formatted in accordance with RFC-4282.
Note—this encoding is to facilitate roaming consortium or other entities that use non-standard NAI realm formats.

Bits:	B0	B1 - B7
	NAI Realm Encoding Type	Reserved

Figure 7-95o140—NAI Realm Encoding sub-field format

NAI Realm Length sub-field is a 1-octet sub-field whose value is the length of the NAI Realm sub-field.

The NAI Realm sub-field is an NAI Realm formatted as defined in the NAI Realm Encoding Type bit of the NAI Realm Encoding subfield. The maximum length of this sub-field is 255 octets.

The EAP Method Count specifies the number of EAP methods sub-fields for the NAI Realm. If the count is zero, there is no EAP method information provided for the NAI realm.

The format of the optional EAP Method sub-field is shown in Figure 7-95o141. Each EAP Method sub-field contains a set of Authentication Parameters associated with the EAP-Method.

	Length	EAP Method	Authentication Parameter Count	Authentication Parameter #1 (optional)	Authentication Parameter #2 (optional)	. . .	Authentication Parameter #n (optional)
Octets:	1	1	1	variable	variable		variable

Figure 7-95o141—EAP Method sub-field format

The length of the EAP Method sub-field is a 1-octet sub-field whose value is equal to 2 plus the length of the Authentication Parameter sub-fields.

The EAP method sub-field is a 1-octet sub-field which is set to the EAP Type value as given in IANA EAP Method Type Numbers.

If the value of the EAP Method field is 254 indicating an Expanded EAP Type, then the Expanded EAP Method Authentication Parameter is included.The Authentication Parameter count indicates how many additional Authentication Parameter sub-fields are specified for the supported EAP Method. If the Authentication Parameters sub-field is zero, there are no sub-fields present, meaning no additional Authentication Parameters are specified for the EAP Method.

The format of the Authentication Parameter sub-field is shown in Figure 7-95o142.

	ID	Length	Authentication Parameter Value
Octets:	1	1	variable

Figure 7-95o142—Authentication Parameter sub-field format

The ID is a 1-octet field which indicates the type of authentication information provided.

The length of the Authentication Parameter sub-field is a 1-octet sub-field whose value is equal to the length in octets of the Authentication Parameter Value field.

The Authentication Parameter Value is a variable length field containing the value of the parameter indicated by the ID.

The ID and its associated formats are specified in Table 7-43bk. Each ID indicates a different type of information. Use of multiple Authentication Parameter sub-fields allows all the required authentication parameter requirements to be provided.

Table 7-43bk—Authentication Parameter types

Authentication Information	ID	Description	Length (octets)
Reserved	0		
Expanded EAP Method	1	Expanded EAP Method Subfield	7
Non-EAP Inner Authentication Type	2	Enum (0 - Reserved, 1 - PAP, 2 – CHAP, 3 - MSCHAP, 4 - MSCHAPV2)	1
Inner Authentication EAP Method Type	3	Value drawn from IANA EAP Method Type Numbers	1
Expanded Inner EAP Method	4	Expanded EAP Method Subfield	7
Credential Type	5	Enum (1-SIM, 2-USIM, 3-NFC Secure Element, 4-Hardware Token, 5-Softoken, 6 - Certificate, 7 – username/password, 8-Vendor Specific)	1
Tunneled EAP Method Credential Type	6	Enum (1-SIM, 2-USIM, 3-NFC Secure Element, 4-Hardware Token, 5-Softoken, 6 - Certificate, 7 – username/password, 8-Vendor Specific)	1
Reserved	7 - 220		
Vendor Specific	221	variable	variable
Reserved	222 - 255		

If the EAP Method type is an Expanded EAP type (the EAP Method value is 254), the Expanded EAP Method Authentication Parameter is used to specify additional information on the EAP method. Table 7-43bl describes the Authentication Parameter format for the Expanded EAP method; values for the Vendor ID and Vendor Type are specified in RFC 3748. The Vendor ID and Vendor Type fields are expressed in big endian byte order.

Table 7-43bl—Authentication Parameter format for the Expanded EAP Method

Parameters	Length (octets)
ID	1
Length	1
Vendor ID	3
Vendor Type	4

The Non-EAP Inner Authentication Type is specified as single enumerated value given in Table 7-43bk. This Authentication Information type is used for non-EAP Inner Authentication methods. The possible values are

PAP (as specified in RFC 1334), CHAP (as specified in RFC 1994), MSCHAP (as specified in RFC 2433), and MSCHAPv2 (as specified in RFC 2759).

The Inner Authentication EAP Method Type is specified as the EAP number as defined in IANA EAP Method Type Numbers. This Authentication Information type is used when the Inner Authentication method is an EAP method. If the Inner Authentication EAP Method Type is equal to 254 indicating an Expanded EAP Type, then the Expanded EAP Method Authentication Parameter is included.

If Credential Type is required by the STA (or required by the user), this is selected by a single enumerated value as shown in Table 7-43bk. If the value is equal to the “Vendor Specific” value, then a Vendor-Specific Authentication Parameter is included.

Vendor specific parameters are specified as shown in Table 7-43bm.

Table 7-43bm—Vendor-Specific Authentication Parameters

Parameters	Length (octets)
ID	1
Length	variable
OI	variable
Authentication Parameter Value	Vendor-specific Content

7.3.4.9 3GPP Cellular Network information

The 3GPP Cellular Network information contains cellular information such as network advertisement information e.g. network codes and country codes to assist a 3GPP non-AP STA in selecting an AP to access 3GPP networks. The format of the 3GPP Cellular Network information is shown in Figure 7-95o143.

	Info ID	Length	Payload
Octets:	2	2	variable

Figure 7-95o143—3GPP Cellular Network information format

The Info ID field is equal to the value in Table 7-43bg corresponding to the 3GPP Cellular Network information.

The Length field is a 2-octet field and is equal to the length of the Payload field.

The Payload field is a generic container whose content is defined in Annex A of 3GPP TS 24.234 v8.1.0.

7.3.4.10 AP Geospatial Location

The AP Geospatial Location element provides the AP's location in LCI format, see 7.3.2.22.9. This list element may be returned in response to a Native GAS Query Request. The format of the AP Geospatial Location element is provided in Figure 7-95o144.

	Info ID	Length	Location Configuration Report
Octets:	2	2	18

Figure 7-95o144—AP Geospatial Location format

The Length field is a 2-octet field and is equal to 18.

The format of the Location Configuration Report is provided in 7.3.2.22.9. There is no Optional Subelements field present in the Location Configuration Report when it is used in the AP Geospatial Location element. This information is taken from the dot11APLCITable MIB object.

7.3.4.11 AP Civic Location

The AP Civic Location element provides the AP's location in civic format. This list element may be returned in response to a Native GAS Query Request. The format of the AP Civic Location element is provided in Figure 7-95o145.

	Info ID	Length	Location Civic Report
Octets:	2	2	variable

Figure 7-95o145—AP Civic Location format

The Length field is a 2-octet field and is equal to the length of the Location Civic Report.

The format of the Location Civic Report is provided in 7.3.2.21.13. This information is taken from the dot11ApCivicLocation MIB object.

7.3.4.12 Domain Name List

The Domain Name List element provides a list of domain names corresponding to SSPs whose networks are accessible via the AP. Domain Names in this element are taken from dot11DomainNameTable. This list element may be returned in response to a Native GAS Query Request. The format of the Domain Name List element is provided in Figure 7-95o146.

	Info ID	Length	Domain Name field #1	Domain Name field #2 (optional)	. . .	Domain Name field #N (optional)
Octets:	2	2	variable	variable		variable

Figure 7-95o146—Domain Name List format

The Length is a 2-octet field whose value is equal to the number and size of the Domain Name Fields

The Domain Name field is shown in Figure 7-95o147.

	Length	Domain Name
Octets:	1	variable

Figure 7-95o147—Domain Name field format

The Length subfield is the length in octets of the Domain Name subfield.

The Domain Name subfield is a domain name compliant with the “Preferred Name Syntax” as defined in RFC 1034. The maximum length of this field is 255 octets.

7.3.4.13 Emergency Alert URI Information

The Emergency Alert URI information provides a URI for EAS message retrieval. The format of the Emergency Alert URI information is provided in Figure 7-95o148.

	Info ID	Length	Emergency Alert URI
Octets:	2	2	variable

Figure 7-95o148—Emergency Alert URI format

The Length is a 2 - octet field whose value is equal to the length of the Emergency Alert URI field.

The Emergency Alert URI is a variable length field used to indicate the URI at which an EAS message may be retrieved. See 11.23.6. The Emergency Alert URI is formatted in accordance with RFC 3986.

7.4 Action frame format details

7.4.1 Spectrum management action details

7.4.2 QoS Action frame details

Change Table 7-45 by inserting the Action field value 4 row and changing the Reserved row as shown:

Table 7-45—QoS Action field values

Action field value	Meaning
0	ADDTS request
1	ADDTS response
2	DELTS
3	Schedule
4	QoS Map Configure
5-255	Reserved

7.4.2.1 ADDTS Request frame format

Change Table 7-46 by inserting new row as shown below.

Table 7-46—ADDTS Request frame body

Order	Information
1	Category
2	Action
3	Dialog token
4	TSPEC
5 – n	TCLAS (optional)
n + 1	TCLAS processing (optional)
n + 2	Expedited bandwidth request element (optional)

Change the last paragraph in 7.4.2.1 with the following text.

The TSPEC element, defined in 7.3.2.30, and the optional TCLAS element, defined in 7.3.2.31, contain the QoS parameters that define the TS. The TS is identified by the TSID and Direction fields within the TSPEC element. The TCLAS element is optional at the discretion of the non-AP STA that sends the ADDTS Request frame, regardless of the setting of the access policy (EDCA or HCCA). *n* is the number of optional TCLAS elements. There may be one or more TCLAS elements in the ADDTS frame. The TCLAS Processing element is present when there are more than one TCLAS element and is defined in 7.3.2.33. There may be one Expedited bandwidth request element, which is defined in 7.3.2.91.

Insert the following new subclause after 7.4.2.4

7.4.2.5 QoS Map Configure frame format

The QoS Map Configure frame is used by an AP to provide the QoS Map Set to a non-AP STA using the procedures defined in 11.23.7.

The frame body of the QoS Map Configure frame contains the information shown in Table 7-49a.

Table 7-49a—QoS Map configure frame body

Order	Information
0	Category
1	Action
2	QoS Map Set

The Category field is set to the value in Table 7-24 (representing QoS).

The Action field is set to the value in Table 7-45 (representing QoS Map Configure).

The QoS Map Set element is defined in 7.3.2.92.

7.4.7 Public Action details

7.4.7.1 Public Action frames

Change the first paragraph of 7.4.7.1 as follows.

The Public Action frame is defined to allow inter-BSS and AP to un-associated-STA communications and Generic Advertisement Services. The defined Public Action frames are listed in Table 7-57e.

Change Table 7-57e by inserting new 4 rows and change Reserved row Action field value as shown below.

Table 7-57e—Public Action field values

Action field value	Description
10	GAS Initial Request, see 7.4.7.14
11	GAS Initial Response, see 7.4.7.15
12	GAS Comeback Request, see 7.4.7.16
13	GAS Comeback Response, see 7.4.7.17
~~9~~14-255	Reserved

Insert the following new subclauses after 7.4.7.14:

7.4.7.14 GAS Initial Request frame format

The GAS Initial Request Action frame is transmitted by a STA to request information from another STA. The format of the GAS Initial Request Action frame body is shown in Table 7-57aj.

Table 7-57aj—GAS Initial Request frame body format

Order	Information
0	Category
1	Action
2	Dialog Token
3	Advertisement Protocol information element
4	Query Request length
5	Query Request

The Category field is set to the value indicating a Public Action frame, as specified in Table 7-24.

The Action field is set to the value specified in Table 7-57e for a GAS Initial Request Action frame.

The Dialog Token field is defined in 7.3.1.12 and set by the requesting STA.

The Advertisement Protocol information element is defined in 7.3.2.90. The Advertisement Protocol element includes exactly one Advertisement Protocol ID or one vendor-specific element, see 7.3.2.26.

The Query Request length field is defined in Figure 7-101bc. The value of the Query Request length field is set to the total number of octets in the Query Request field.

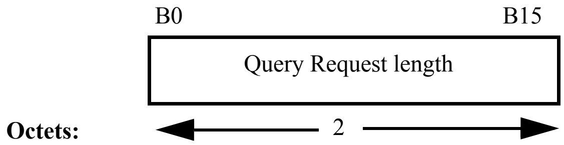

Figure 7-101bc—Query Request length field

The Query Request field is defined in Figure 7-101bd. The Query Request field is a generic container whose value is a GAS query which is formatted in accordance with the protocol specified in the Advertisement protocol information element.

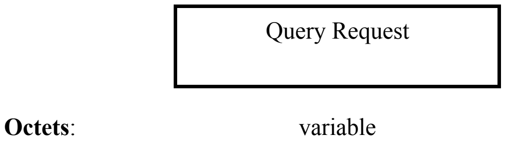

Figure 7-101bd—Query Request field

7.4.7.15 GAS Initial Response frame format

The GAS Initial Response Action frame is transmitted by an STA responding to a request from another STA. The format of the GAS Initial Response Action frame body is shown in Table 7-57ak.

Table 7-57ak—GAS Initial Response frame body format

Order	Information
0	Category
1	Action
2	Dialog Token
3	Status Code
4	GAS Comeback Delay
5	Advertisement protocol information element
6	Query Response Length
7	Query Response (optional)

The Category field is set to the value indicating a Public Action frame, as specified in Table 7-24.

The Action field is set to the value specified in Table 7-57e for a GAS Initial Response Action frame.

The Dialog Token field is copied from the corresponding GAS Initial Request Action frame.

The Status Code values are defined in Table 7-23.

The GAS Comeback Delay field specifies the delay time value in TUs. Upon expiry of this delay, the non-AP STA should attempt to retrieve the Query Response using a Comeback Request Action frame. The GAS Comeback Delay field format is provided in Figure 7-101be.

— A zero value will be returned by the STA when a Query Response is provided in this frame.

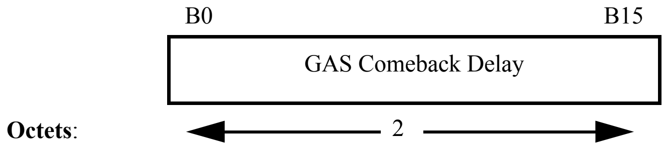

Figure 7-101be—GAS Comeback Delay field

The Advertisement Protocol information element is defined in 7.3.2.90. The Advertisement Protocol element includes exactly one Advertisement Protocol ID or one vendor-specific element, see 7.3.2.26.

The Query Response Length field is defined in Figure 7-101bf. The value of the Query Response Length field is set to the total number of octets in the Query Response field. If the Query Response Length field is set to 0, then there is no Query Response included in this Action frame.

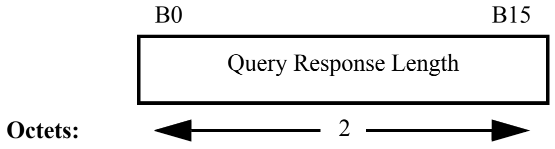

Figure 7-101bf—Query Response length field

The Query Response field is defined in Figure 7-101bg. 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 information element.

.

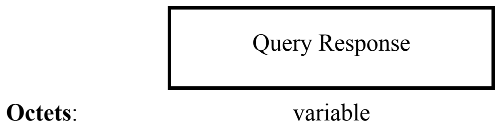

Figure 7-101bg—Query Response field

7.4.7.16 GAS Comeback Request frame format

The GAS Comeback Request Action frame is transmitted by a non-AP STA to an AP. The format of the GAS Comeback Request Action frame body is shown in Table 7-57al.

Table 7-57al—GAS Comeback Request Action frame body format

Order	Information
0	Category
1	Action
2	Dialog Token

The Category field is set to the value indicating a Public Action frame, as specified in Table 7-24.

The Action field is set to the value specified in Table 7-57e for a GAS Comeback Request Action frame.

The Dialog Token field is copied from the corresponding GAS Initial Request Action frame.

7.4.7.17 GAS Comeback Response frame format

The GAS Comeback Response Action frame is transmitted by an AP to a non-AP STA. The format of the GAS Comeback Response Action frame body is shown in Table 7-57am.

Table 7-57am—GAS Comeback Response Action frame body format

Order	Information
0	Category
1	Action
2	Dialog Token
3	Status Code
4	GAS Query Response Fragment ID
5	GAS Comeback Delay
6	Advertisement Protocol information element
7	Query Response Length
8	Query Response (optional)

The Category field is set to the value indicating a Public Action frame, as specified in Table 7-24.

The Action field is set to the value specified in Table 7-57e for a GAS Comeback Response Action frame.

The Dialog Token field is copied from the Dialog Token field of the corresponding GAS Initial Response Action frame.

The Status Code values are defined in Table 7-23. The same status code value will be present in all fragments of a multi-fragment query response.

The GAS Query Response Fragment ID is defined in 7.3.1.33. If the AP has not received a response to the query that it posted on behalf of a non-AP STA, then the AP sets the GAS Query Response Fragment ID to 0. When there is more than one query response fragment, the AP sets the GAS Query Response Fragment ID to 1 for the initial fragment and increments it by 1 for each subsequent fragment in a multi-fragment Query Response. The More GAS Fragments field is set to 0 whenever the final fragment of a query response is being transmitted. A GAS Query Response Fragment ID field having a non-zero Fragment ID and the More GAS Fragments field set to 1 indicates to the non-AP STA that another GAS Comeback Action frame exchange should be performed to continue the retrieval of the query response.

The GAS Comeback Delay field format is provided in Figure 7-101be. A non-zero GAS Comeback Delay value is returned by the AP in this frame to indicate that the Non-Native GAS query being carried out on behalf of the non-AP STA is still in progress.

- A non-zero value indicates to the non-AP STA that another GAS Comeback Action frame exchange should be performed after expiry of the GAS Comeback Delay timer in order to retrieve the query response.
- This field is set to 0 for all GAS Comeback Response Action frames containing a query response or a fragment of a multi-fragment query response.

The Advertisement Protocol information element is defined in 7.3.2.90. The Advertisement Protocol element includes exactly one Advertisement Protocol ID or one vendor-specific element, see 7.3.2.26.

The Query Response Length field is defined in Figure 7-101bf. The value of the Query Response Length field is set to the total number of octets in the Query Response field. If the Query Response Length field is set to 0, then there is no Query Response included in this Action frame.

The Query Response field is defined in Figure 7-101bg. The value of the Query Response field is a generic container dependent on the Advertisement Protocol specified in the Advertisement protocol information element and the query itself. In a multi-fragment query response, the response to the query posted on behalf of a non-AP STA is fragmented such that each fragment to be transmitted fits within the MMPDU size limitation.

7.4.9 SA Query Action frame details

7.4.9a Protected Dual of Public Action details

7.4.9a.1 Protected Dual of Public Action frames

Change Table 7-57m by inserting the following items 9 thru 12 and re-numbering the Action field value for the "Reserved" row accordingly as shown below:

Table 7-57m—Protected Dual of Public Action field values

Action Field Value	Description
9	GAS Initial Request
10	GAS Initial Response
11	GAS Comeback Request
12	GAS Comeback Response
~~8~~13-255	Reserved

8. Security

Insert the following clause after the RSNA assumptions and constraints sub-clause

8.1.6 Emergency Service establishment in an RSN

An AP that supports RSNAs and supports interworking Emergency Services supports both RSNAs and Emergency Services associations simultaneously.

NOTE—For emergency services operations in a RSN BSS, it is recommended to use a separate VLAN on the network side of the AP, so that the layer 2 broadcast domains for the emergency services VLAN is separate from the layer 2 broadcast domain used for non emergency service traffic. This ensures that no group addressed frames destined to non emergency non-AP STAs will be replicated in unprotected frames transmitted to the emergency services STA.

9. MAC sublayer functional description

9.2 DCF

9.2.7 Broadcast and multicast MPDU transfer procedure

Change the first paragraph of 9.2.7 as follows:

In the absence of a PCF, when broadcast or group addressed MPDUs are transferred from a STA with the To DS field clear, only the basic access procedure shall be used. Regardless of the length of the frame, no RTS/CTS exchange shall be used. In addition, no ACK shall be transmitted by any of the recipients of the frame. Any broadcast or group addressed MPDUs transferred from a STA with a To DS field set shall, in addition to conforming to the basic access procedure of CSMA/CA, obey the rules for RTS/CTS exchange and the ACK procedure because the MPDU is directed to the AP. When dot11SSPNInterfaceEnabled is true, an AP shall distribute the broadcast/multicast message into the BSS only if dot11NonAPStationAuthSourceMulticast in the dot11InterworkingEntry identified by the source MAC address in the received message is set to TRUE. When dot11SSPNInterfaceEnabled is false, t~~T~~he broadcast/multicast message shall be distributed into the BSS. The STA originating the message shall receive the message as a broadcast/multicast message. Therefore, all STAs shall filter out broadcast/multicast messages that contain their address as the source address. When dot11SSPNInterfaceEnabled is false, ~~B~~broadcast and multicast MSDUs shall be propagated throughout the ESS. When dot11SSPNInterfaceEnabled is set to TRUE, broadcast and multicast MSDUs shall be propagated throughout the ESS only if dot11NonAPStationAuthSourceMulticast in the dot11InterworkingEntry identified by the source MAC address in the received message is set to TRUE.

9.9 HCF

9.9.3.1 Contention-based admission control procedures

Change the second paragraph of 9.9.3.1 as follows:

The AP uses the ACM (admission control mandatory) subfields advertised in the EDCA Parameter Set element to indicate whether admission control is required for each of the ACs. While the CWmin, CWmax, AIFS, TXOP limit parameters may be adjusted over time by the AP, the ACM field shall be static for the duration of the lifetime of the BSS. An ADDTS Request frame shall be transmitted by a non-AP STA to the HC in order to request admission of traffic in any direction (i.e., uplink, downlink, direct, or bidirectional) employing an AC that requires admission control. The ADDTS Request frame shall contain the UP associated with the traffic and shall indicate EDCA as the access policy. The AP shall associate the received UP of the ADDTS Request frame with the appropriate AC as per the UP-to-AC mappings described in 9.1.3.1. The non-AP STA may transmit un-admitted traffic for the ACs for which the AP does not require admission control. If a STA desires to send data without admission control using an AC that mandates admission control, the STA shall use EDCA parameters that correspond to a lower priority and do not require admission control. All ACs with priority higher than that of an AC with an ACM flag equal to 1 should have the ACM flag set to 1. The HC contained within an AP having dot11SSPNInterfaceEnabled set to TRUE shall admit a non-AP STA's request based on the value of dot11NonAPStationAuthAccessCategories stored in that non-AP STA's dot11InterworkingEntry, which is part of the dot11InterworkingTable. The dot11InterworkingEntry specifies the EDCA access classes and throughput limitations on each access class for which a non-AP STA is permitted to transmit.

9.9.3.1.1 Procedures at the AP

Change the second paragraph of 9.9.3.1.1 as follows:

The algorithm used by the AP to make this determination is an AP local matter. An AP having dot11SSPNInterfaceEnabled set to TRUE shall use the policies delivered by the SSPN which are stored in the dot11InterworkingEntry which is part of the dot11InterworkingTable. If the AP decides to accept the request, the AP shall also derive the medium time from the information conveyed in the TSPEC element in the ADDTS Request frame. The AP may use any algorithm in deriving the medium time, but K.2.2 provides a procedure that may be used. Having made such a determination, the AP shall transmit a TSPEC element to the requesting non-AP STA contained in an ADDTS Response frame. If the AP is accepting the request, the Medium Time field shall be specified.

9.9.3.2 Controlled-access admission control

Insert the following list item at the end of second paragraph (the bulleted list) of 9.9.3.2:

- The HC shall admit its request based on Infrastructure Authorization Information in dot11InterworkingEntry which is part of the dot11InterworkingTable. The dot11InterworkingEntry specifies whether a non-AP STA is permitted to use HCCA, its throughput limitation and its minimum delay bound.

10. Layer management

10.3 MLME SAP Interface

10.3.2 Scan

10.3.2.1 MLME-SCAN.request

10.3.2.1.2 Semantics of the service primitive

Change the primitive parameter list in 10.3.2.1.2 as shown:

```
MLME-SCAN.request
                    BSSType,
                    BSSID,
                    SSID,
                    ScanType,
                    ProbeDelay,
                    ChannelList,
                    MinChannelTime,
                    MaxChannelTime,
                    NetworkType,
                    HESSID,
                    VendorSpecificInfo
                    )
```

Insert the following rows before the VendorSpecificInfo row of the untitled table defining the primitive parameters in 10.3.2.1.2:

Name	Type	Valid Range	Description
NetworkType	As defined in Table 7-43bb.	0 to 15	Specifies a desired specific Network Type or the wildcard network type. This field is present when dot11InterworkServiceEnabled is set to TRUE.
HESSID	MAC Address	Any valid individual MAC address or the broadcast MAC address	Specifies the desired specific HESSID network identifier or the wildcard network identifier. This field is present when dot11InterworkServiceEnabled is set to TRUE.

10.3.6 Associate

10.3.6.1 MLME-ASSOCIATE.request

10.3.6.1.2 Semantics of the service primitive

Change the primitive parameter list in 10.3.6.1.2 as shown:

```
MLME-ASSOCIATE.request (
            PeerSTAAddress,
            AssociateFailureTimeout,
            CapabilityInformation,
            ListenInterval,
```

Supported Channels,
RSN,
QoSCapability,
EmergencyServices,
VendorSpecificInfo
)

Insert the following row before the VendorSpecificInfo row of the untitled table defining the primitive parameters in 10.3.6.1.2:

Name	Type	Valid Range	Description
EmergencyServices	Boolean	True, False	Specifies that the non-AP STA intends to associate for the purpose of un-authenticated access to emergency services. The parameter shall only be present if dot11InterworkingServiceEnabled is set to TRUE.

10.3.6.2 MLME-ASSOCIATE.confirm

10.3.6.2.2 Semantics of the service primitive

Change the primitive parameter list in 10.3.6.2.2 as shown:

MLME-ASSOCIATE.confirm (
ResultCode,
CapabilityInformation,
AssociationID,
SupportedRates,
EDCAParameterSet,
RCPI.request,
RSNI.request,
RCPI.response,
RSNI.response,
RRMEnabledCapabilities
Content of FT Authentication Information Elements,
SupportedRegulatoryClasses,
HT Capabilities,
Extended Capabilities,
20/40 BSS Coexistence,
BSSMaxIdlePeriod,
TIMBroadcastResponse,
TimeStamp,
QosMapSet,
VendorSpecificInfo
)

Insert the following rows before the VendorSpecificInfo row of the untitled table defining the primitive parameters in 10.3.6.2.2:

Name	Type	Valid Range	Description
TimeStamp	Integer	N/A	The timestamp of the event, measured as the number of TUs since the 802.11 interface was powered on. This field is present when dot11InterworkingServiceEnabled is set to TRUE.
QoSMapSet	As defined in frame format	As defined in 7.3.2.92	Specifies the QoS Map Set the non-AP STA should use.

10.3.6.4 MLME-ASSOCIATE.response

10.3.6.4.2 Semantics of the service primitive

Change the primitive parameter list in 10.3.6.4.2 as shown:

```
MLME-ASSOCIATE.response
                PeerSTAAddress
                ResultCode,
                CapabilityInformation,
                AssociationID,
                Content of FT Authentication Information Elements
                SupportedRegulatoryClasses,
                HT Capabilities,
                Extended Capabilities,
                20/40 BSS Coexistence,
                BSSMaxIdlePeriod,
                TIMBroadcastResponse,
                QoSMapSet,
                VendorSpecificInfo
                )
```

Insert the following row before the VendorSpecificInfo row of the untitled table defining the primitive parameters in 10.3.6.4.2:

Name	Type	Valid Range	Description
QoSMapSet	As defined in frame format	As defined in 7.3.2.92	Specifies the QoS Map Set the non-AP STA should use.

10.3.7 Reassociate

10.3.7.1 MLME-REASSOCIATE.request

10.3.7.1.2 Semantics of the service primitive

Change the primitive parameter list in 10.3.7.1.2 as shown:

```
MLME-ASSOCIATE.request (
                PeerSTAAddress,
                AssociateFailureTimeout,
                CapabilityInformation,
                ListenInterval,
                Supported Channels,
                RSN,
                QoSCapability,
                EmergencyServices,
                VendorSpecificInfo
                )
```

Insert the following row before the VendorSpecificInfo row of the untitled table defining the primitive parameters in 10.3.7.1.2:

Name	Type	Valid Range	Description
EmergencyServices	Boolean	True, False	Specifies that the non-AP STA intends to associate for the purpose of un-authenticated access to emergency services. The parameter shall only be present if dot11InterworkingServiceEnabled is set to TRUE.

10.3.7.2 MLME-REASSOCIATE.confirm

10.3.7.2.2 Semantics of the service primitive

Change the primitive parameter list in 10.3.7.2.2 as shown:

```
      MLME-REASSOCIATE.confirm (
                  ResultCode,
                  CapabilityInformation,
                  AssociationID,
                  SupportedRates,
                  EDCAParameterSet,
                  Content of FT Authentication Information Elements,
                  SupportedRegulatoryClasses,
                  HT Capabilities,
                  Extended Capabilities,
                  20/40 BSS Coexistence,
                  BSSMaxIdlePeriod,
                  TIMBroadcastResponse,
                  QoSMapSet,
                  VendorSpecificInfo
                  )
```

Insert the following row before the VendorSpecificInfo row of the untitled table defining the primitive parameters in 10.3.7.2.2:

Name	Type	Valid Range	Description
QoSMapSet	As defined in frame format	As defined in 7.3.2.92	Specifies the QoS Map Set the non-AP STA should use.

10.3.7.4 MLME-REASSOCIATE.response

10.3.7.4.2 Semantics of the service primitive

Change the primitive parameter list in 10.3.7.2.2 as shown:

```
      MLME-REASSOCIATE.response (
                  PeerSTAAddress,
                  ResultCode,
                  CapabilityInformation,
```

AssociationID,
Content of FT Authentication Information Elements
SupportedRegulatoryClasses,
HT Capabilities,
Extended Capabilities,
20/40 BSS Coexistence,
BSSMaxIdlePeriod,
TIMBroadcastResponse,
QoSMapSet,
VendorSpecificInfo
)

Insert the following row before the VendorSpecificInfo row of the untitled table defining the primitive parameters in 10.3.7.2.2:

Name	Type	Valid Range	Description
QoSMapSet	As defined in frame format	As defined in 7.3.2.92	Specifies the QoS Map Set the non-AP STA should use.

10.3.10 Start

10.3.10.1 MLME-START.request

10.3.10.1.2 Semantics of the service primitive

Change the primitive parameter list in 10.3.10.1.2 as shown:

MLME-START.request(
SSID,
BSSType,
BeaconPeriod,
DTIMPeriod,
CF parameter set,
PHY parameter set,
IBSS parameter set,
ProbeDelay,
CapabilityInformation,
BSSBasicRateSet,
OperationalRateSet,
Country,
IBSS DFS Recovery Interval,
EDCAParameterSet,
DSERegisteredLocation,
HT Capabilities,
HT Operation,
BSSMembershipSelectorSet,
BSSBasicMCSSet,
HTOperationalMCSSet,
Extended Capabilities,
20/40 BSS Coexistence,
Overlapping BSS Scan Parameters,
InterworkingInfo,
AdvertismentProtocolInfo,
RoamingConsortiumInfo,
VendorSpecificInfo
)

Insert the following rows before the VendorSpecificInfo row of the untitled table defining the primitive parameters in 10.3.10.1.2:

Name	Type	Valid Range	Description
InterworkingInfo	As defined in frame format	As defined in Interworking element in 7.3.2.89	Specifies the Interworking capabilities of STA. This field is present when dot11InterworkServiceEnabled is set to TRUE.
AdvertisementProtocolInfo	Integer or Sequence of Integers	As defined in Advertisement Protocol element in Table 7-43be	Identifies zero or more advertisement protocols and advertisement control to be used in the BSSs. This field is present when dot11InterworkServiceEnabled is set to TRUE.
RoamingConsortiumInfo	As defined in frame format	As defined in roaming consortium element in 7.3.2.93	Specifies identifying information for SSPs whose security credentials can be used to authenticate with the AP

10.3.24 TS management interface

10.3.24.1 MLME- ADDTS.request

10.3.24.1.2 Semantics of the service primitive

Change the primitive parameter list in 10.3.24.1.2 as shown:

```
MLME-ADDTS.request(
                    DialogToken,
                    TSPEC,
                    TCLAS,
                    TCLASProcessing,
                    ADDTSFailureTimeout,
                    EBR,
                    VendorSpecificInfo
                    )
```

Insert the following row before the VendorSpecificInfo row of the untitled table defining the primitive parameters in 10.3.24.1.2:

Name	Type	Valid Range	Description
EBR	As defined in frame format	As defined in 7.3.2.91	Specifies the precedence level of the TS request. This element may be present when dot11EBREnabled is true.

10.3.24.2 MLME- ADDTS.confirm

10.3.24.2.2 Semantics of the service primitive

Change the primitive parameter list in 10.3.24.2.2 as shown:

```
MLME-ADDTS.confirm(
                    ResultCode,
                    DialogToken,
                    TSDelay,
                    TSPEC,
                    Schedule,
                    TCLAS,
                    TCLASProcessing,
                    EBR,
                    VendorSpecificInfo
                    )
```

Change ResultCode row in the following table in 10.3.24.2.2 as shown below and insert EBR row at the end of the table, before VendorSpecificInfo:

Name	Type	Valid Range	Description
ResultCode	Enumeration	SUCCESS, INVALID_PARAMETERS, REJECTED_WITH_SUGGESTED_CHANGES, REJECTED_HOME_WITH_SUGGESTED_CHANGES, REJECTED_FOR_DELAY_PERIOD, TIMEOUT, TRANSMISSION_FAILURE	Indicates the results of the corresponding MLME-ADDTS.request primitive.
EBR	As defined in frame format	As defined in 7.3.2.91	Specifies the precedence level of the TS request. This element may be present when dot11EBREnabled is true.

Change the second paragraph of 10.3.24.2.2 as follows:

For other values of ResultCode, no new TS has been created. In the case of REJECTED_WITH_SUGGESTED_CHANGES, the TSPEC represents an alternative proposal by the HC based on information about the current status of the MAC entity. In the case of REJECTED_HOME_WITH_SUGGESTED_CHANGES, the TSPEC represents an alternative proposal by the HC based on information received from the SSPN interface. A TS is not created with this definition. If the suggested changes are acceptable to the non-AP STA, it is the responsibility of the non-AP STA to set up the TS with the suggested changes.

10.3.24.3 MLME- ADDTS.indication

10.3.24.3.2 Semantics of the service primitive

Change the primitive parameter list in 10.3.24.3.2 as shown:

```
MLME-ADDTS.indication(
                    DialogToken,
                    DialogToken,
                    Non-APSTAAddress
                    TSPEC,
                    TCLAS,
                    TCLASProcessing,
                    EBR,
                    VendorSpecificInfo
                    )
```

Insert the following EBR row before the VendorSpecificInfo row of the untitled table defining the primitive parameters in 10.3.24.3.2:

Name	Type	Valid Range	Description
EBR	As defined in frame format	As defined in 7.3.2.91	Specifies the precedence level of the TS request. This element may be present when dot11EBREnabled is true.

10.3.24.4 MLME-ADDTS.response

10.3.24.4.2 Semantics of the service primitive

Change the primitive parameter list in 10.3.24.4.2 as follows:

```
MLME-ADDTS.response (
                    ResultCode,
                    DialogToken,
                    Non-APSTAAddress,
                    TSDelay,
                    TSPEC,
                    Schedule,
                    TCLAS,
                    TCLASProcessing,
                    EBR,
                    VendorSpecificInfo
                    )
```

Change ResultCode row in the following table in 10.3.24.4.2 as shown below and insert EBR row at the end of the table, before VendorSpecificInfo:

Name	Type	Valid Range	Description
ResultCode	Enumeration	SUCCESS, INVALID_PARAMETERS, REJECTED__WITH_SUGGESTED_ CHANGES, REJECTED_HOME_WITH_SUGGESTED_ CHANGES, REJECTED_FOR_DELAY_PERIOD, TIMEOUT, TRANSMISSION_FAILURE	Indicates the results of the corresponding MLMEADDTS.request primitive.
EBR	As defined in frame format	As defined in 7.3.2.91	Specifies the precedence level of the TS request. This element may be present when dot11EBREnabled is true.

Change the third paragraph in 10.3.24.4.2 as follows:

If the result code is REJECTED_WITH_SUGGESTED_CHANGES or

REJECTED_HOME_WITH_SUGGESTED_CHANGES, the TSPEC and TCLAS parameters represent an alternative proposed TS either based on information local to the MAC entity, or using additional information received across the SSPN interface. The TS, however, is not created. The TSID and direction values within the TSPEC are as in the matching MLME-ADDTS.indication primitive. The difference may lie in the QoS (e.g., minimum data rate, mean data rate, and delay bound) values, as a result of admission control performed at the SME of the HC on the TS requested to be added (or modified) by the non-AP STA. If sufficient bandwidth is not available, the QoS values may be reduced. In one extreme, the minimum data rate, mean data rate, and delay bound may be all set to 0, indicating that no QoS is to be provided to this TS.

Insert the following subclauses (10.3.70 through 10.3.72.1.4) after 10.3.69.4.4

10.3.70 Network Discovery and Selection Support

This set of primitives supports the process of Generic Advertisement Services.

10.3.70.1 MLME-GAS.request

10.3.70.1.1 Function

This primitive requests the information of a specific advertisement service from another STA and requests the STA to provide the Generic Advertisement Service.

10.3.70.1.2 Semantics of the service primitive

The primitive parameters are as follows:

```
        MLME-GAS.request (
                                  PeerSTAAddress,
                                  AdvertisementProtocolID,
                                  Query,
                                  QueryFailureTimeout
                                  )
```

Name	Type	Valid Range	Description
PeerSTAAddress	MacAddress	Any valid individual MacAddress	Specifies the address of the peer MAC entity to which query is transmitted.
AdvertisementProtocolID	Integer or Sequence of Integers	As defined in Table 7-43be	Identifies which protocol is used to format Query. This is either an 802.11 assigned Advertisement Protocol ID or a vendor-specific information element containing a vendor-specific advertisement protocol ID.
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 will be terminated.

10.3.70.1.3 When generated

This primitive is generated by the SME at a STA to request a specific advertisement service from another STA, which, for non-native advertisement protocols, may relay the query to a server in an external network.

10.3.70.1.4 Effect of receipt

The STA operates according to the procedures defined in 11.23.2.

10.3.70.2 MLME-GAS.confirm

10.3.70.2.1 Function

This primitive reports the status code and Query Response to a GAS query of a specific advertisement service from an STA, which, for non-native advertisement protocols, may be relaying the query response from a server in an external network.

10.3.70.2.2 Semantics of the service primitive

The primitive parameters are as follows:

```
        MLME-GAS.confirm (
                            PeerSTAAddress,
                            ResultCode,
                            ResponseInfo
                            )
```

Name	Type	Valid Range	Description
PeerSTAAddress	MacAddress	Any valid individual MacAddress	Specifies the address of the peer MAC entity to which query is transmitted.
ResultCode	Enumeration	SUCCESS, TIMEOUT, UNSPECIFIED_FAILURE, ADVERTISEMENT_PROTOCOL_NOT_SUPPORTED, QUERY_RESPONSE_TOO_LARGE, PARTIAL_QUERY_RESPONSE_CONFIG, PARTIAL_QUERY_RESPONSE_SIZE, SERVER_UNREACHABLE, REQUEST_INFO_NOT_CONFIGURED, TRANSMISSION_FAILURE	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.

The mapping of Status Code received in the GAS Response frame is mapped to the corresponding Result Code in Table 11-4.

10.3.70.2.3 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 STA receives a query response in a GAS Initial Response Action frame or a non-AP STA receives a query response in a GAS Comeback Response Action frame from the AP.

10.3.70.2.4 Effect of receipt

The STA operates according to the procedures defined in 11.23.2.

10.3.70.3 MLME-GAS.indication

10.3.70.3.1 Function

This primitive reports to the STA's SME about the GAS Request.

10.3.70.3.2 Semantics of the service primitive

The primitive parameters are as follows:

```
        MLME-GAS.indication (
                              PeerSTAAddress,
                              AdvertisementProtocolID,
                              Query
                              )
```

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.
AdvertisementProtocolID	Integer or Sequence of Integers	As defined in Table 7-43be	Identifies which protocol is used to format Query. This is either an 802.11 assigned Advertisement Protocol ID or a vendor-specific information element containing a vendor-specific advertisement protocol ID.
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.

10.3.70.3.3 When generated

This primitive is generated by the MLME as a result of receipt of a GAS request from STA.

10.3.70.3.4 Effect of receipt

The SME is notified of the request from the STA.

The SME operates according to the procedures defined in 11.23.2.

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

10.3.70.4 MLME-GAS.response

10.3.70.4.1 Function

This primitive responds to the request for an advertisement service by a specified STA MAC entity.

10.3.70.4.2 Semantics of the service primitive

The primitive parameters are as follows:

```
            MLME-GAS.response (
                              PeerSTAAddress,
                              ResultCode,
                              ResponseInfo
                              )
```

Name	Type	Valid Range	Description
PeerSTAAddress	MacAddress	Any valid individual MAC address	Specifies the address of the peer MAC entity to which query response information is transmitted.
ResultCode	Enumeration	SUCCESS, NO_REQUEST_OUTSTANDING, ADVERTISEMENT_PROTOCOL_NOT_SUPPORTED, QUERY_RESPONSE_OUTSTANDING, QUERY_RESPONSE_TOO_LARGE, PARTIAL_QUERY_RESPONSE_CONFIG, PARTIAL_QUERY_RESPONSE_SIZE, SERVER_UNREACHABLE, REQUEST_INFO_NOT_CONFIGURED, TIMEOUT	Indicates the result response to the GAS-request from the peer MAC entity. See Table 11-4.
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.

10.3.70.4.3 When generated

This primitive is generated by the MLME at a STA as a result of an MLME-GAS.indication primitive.

10.3.70.4.4 Effect of receipt

This primitive causes the MAC entity at the STA to send a GAS Initial Response frame to the requesting STA. The primitive could also cause the MAC entity to transmit a GAS Comeback Response Action frame.

10.3.71 Protected Dual of Network Discovery and Selection Support

This set of primitives supports the process of Generic Advertisement Services using Protected Dual of Public Action frames.

10.3.71.1 MLME-PDGAS.request

10.3.71.1.1 Function

This primitive requests the information of a specific advertisement service from another STA and requests the STA to provide the Generic Advertisement Service.

10.3.71.1.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-PDGAS.request (
                    PeerSTAAddress,
                    AdvertisementProtocolID,
                    Query,
                    QueryFailureTimeout
                    )
```

Name	Type	Valid Range	Description
PeerSTAAddress	MacAddress	Any valid individual MacAddress	Specifies the address of the peer MAC entity to which query is transmitted.
AdvertisementProtocolID	Integer or Sequence of Integers	As defined in Table 7-43be	Identifies which protocol is used to format Query. This is either an 802.11 assigned Advertisement Protocol ID or a vendor-specific information element containing a vendor-specific advertisement protocol ID.
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 will be terminated.

10.3.71.1.3 When generated

This primitive is generated by the SME at a STA to request a specific advertisement service from another STA, which, for non-native advertisement protocols, may relay the query to a server in an external network. This primitive is used when Management Frame Protection is negotiated.

10.3.71.1.4 Effect of receipt

The STA operates according to the procedures defined in 11.23.2

10.3.71.2 MLME-PDGAS.confirm

10.3.71.2.1 Function

This primitive reports the status code and query response to a GAS query of a specific advertisement service from an STA, which, for non-native advertisement protocols, may be relaying the query response from a server in an external network.

10.3.71.2.2 Semantics of the service primitive

The primitive parameters are as follows:

```
        MLME-PDGAS.confirm (
                                PeerSTAAddress,
                                ResultCode,
                                ResponseInfo
                                )
```

Name	Type	Valid Range	Description
PeerSTAAddress	MacAddress	Any valid individual MacAddress	Specifies the address of the peer MAC entity to which query is transmitted.
ResultCode	Enumeration	SUCCESS, TIMEOUT, UNSPECIFIED_FAILURE, ADVERTISEMENT_PROTOCOL_NOT_SUPPORTED, QUERY_RESPONSE_TOO_LARGE, PARTIAL_QUERY_RESPONSE, SERVER_UNREACHABLE, REQUEST_INFO_NOT_CONFIGURED, TRANSMISSION_FAILURE	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.

The mapping of Status Code received in the GAS Response frame is mapped to the corresponding Result Code in Table 7-15.

10.3.71.2.3 When generated

This primitive is generated by the MLME as a response to the MLME-GAS.request primitive indicating the result of that request. This primitive is used when Management Frame Protection is negotiated.

The primitive is generated when the STA receives a query response in a GAS Initial Response Action frame or a non-AP STA receives a query response in a GAS Comeback Response Action frame from the AP.

10.3.71.2.4 Effect of receipt

The STA operates according to the procedures defined in 11.23.2.

10.3.71.3 MLME-PDGAS.indication

10.3.71.3.1 Function

This primitive reports to the STA's SME about the GAS Request.

10.3.71.3.2 Semantics of the service primitive

The primitive parameters are as follows:

```
        MLME-PDGAS.indication (
                                        PeerSTAAddress,
                                        AdvertisementProtocolID,
                                        Query
                                        )
```

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.
AdvertisementProtocolID	Integer or Sequence of Integers	As defined in Table 7-43be	Identifies which protocol is used to format Query. This is either an 802.11 assigned Advertisement Protocol ID or a vendor-specific information element containing a vendor-specific advertisement protocol ID.
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.

10.3.71.3.3 When generated

This primitive is generated by the MLME as a result of receipt of a GAS request from STA. This primitive is used when Management Frame Protection is negotiated.

10.3.71.3.4 Effect of receipt

The SME is notified of the request from the STA.

The SME operates according to the procedures defined in 11.23.2.

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

10.3.71.4 MLME-PDGAS.response

10.3.71.4.1 Function

This primitive responds to the request for an advertisement service by a specified STA MAC entity.

10.3.71.4.2 Semantics of the service primitive

The primitive parameters are as follows:

```
        MLME-PDGAS.response (
                                    PeerSTAAddress,
                                    ResultCode,
                                    ResponseInfo
                                    )
```

Name	Type	Valid Range	Description
PeerSTAAddress	MacAddress	Any valid individual MAC address	Specifies the address of the peer MAC entity to which query response information is transmitted.
ResultCode	Enumeration	SUCCESS, NO_REQUEST_OUTSTANDING, ADVERTISEMENT_PROTOCOL_NOT_SUPPORTED, QUERY_RESPONSE_OUTSTANDING, QUERY_RESPONSE_TOO_LARGE, PARTIAL_QUERY_RESPONSE_CONFIG, PARTIAL_QUERY_RESPONSE_SIZE, SERVER_UNREACHABLE, REQUEST_INFO_NOT_CONFIGURED, TIMEOUT	Indicates the result response to the GAS-request from the peer MAC entity. See Table 7-15
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.

10.3.71.4.3 When generated

This primitive is generated by the MLME at a STA as a result of an MLME-GAS.indication primitive. This primitive is used when Management Frame Protection is negotiated.

10.3.71.4.4 Effect of receipt

This primitive causes the MAC entity at the STA to send a GAS Initial Response frame to the requesting STA. The primitive could also cause the MAC entity to transmit a GAS Comeback Response Action frame.

10.3.72 QoS Map Set element management

The QoS Map Set element is provided to non-AP STAs in (Re)-association response frames. However, if the SME of an AP detects a change of the QoS Map information while one or more non-AP STAs are associated to the BSS, then the AP may transmit an un-solicited QoS Map Set element to associated STAs. The AP's SME invokes the MLME-QoSMap.request primitive to cause individually-addressed frames containing a QoS Map Set element to be transmitted to associated STAs. The AP's SME invokes the MLME-QoSMap.request primitive to transmit individually-addressed frames containing a QoS Map Set element to associated STAs. When a non-AP STA receives such unsolicited QoS Map information, its MLME generates a MLME-QoSMap.indication to the STA's SME. In turn, the SME should take appropriate action, e.g., initiate an ADDTS or DELTS if admission control changes are necessary.

10.3.72.1 MLME-QoSMap.request

10.3.72.1.1 Function

This primitive is used by an AP to transmit an un-solicited QoS Map Set to a specified non-AP STA MAC entity. The specified non-AP STA MAC address is an individual MAC address.

10.3.72.1.2 Semantics of the service primitive

The primitive parameters are as follows:

```
        MLME-QoSMap.request        (
                                   Non-APSTAAddress,
                                   QoSMapSet
                                   )
```

Name	Type	Valid Range	Description
Non-APSTAAddress	MacAddress	Any valid individual MAC address	Specifies the address of the peer MAC entity from which query message is received.
QoSMapSet	As defined in frame format	As defined in 7.3.2.92	Specifies the QoS Map Set the non-AP STA should use.

10.3.72.1.3 When generated

This primitive is generated by the MLME at the AP as a result of any change in the AP QoS Map configurations.

10.3.72.1.4 Effect of receipt

This primitive causes the MAC entity at the AP to send a QoS MAP Set element in a QoS MAP Configure Action frame to the non-AP STA.

10.3.72.2 MLME-QoSMap.indication

10.3.72.2.1 Function

This primitive reports the QoS Mapping information sent from the AP to the non-AP STA.

10.3.72.2.2 Semantics of the service primitive

The primitive parameters are as follows:

```
          MLME-QoSMap.indication  (
                                  QoSMapSet
                                  )
```

Name	Type	Valid Range	Description
QoSMapSet	As defined in frame format	As defined in 7.3.2.92	Specifies the QoS Map Set to be used by the non-AP STA.

10.3.72.2.3 When generated

This primitive is generated when the non-AP STA receives a QoS Map Set element in an un-solicited QoS Map Configure Action frame from the AP.

The SME of the non-AP STA should use the information to decide proper actions. For example, an ADDTS or DELTS procedure should be activated if the QoS Map information indicates a change in the admission control.

10.3.72.2.4 Effect of receipt

The non-AP STA operates according to the procedures defined in 11.23.7.

11. MLME

11.1 Synchronization

11.1.1 Basic approach

11.1.2 Maintaining synchronization

11.1.3 Acquiring synchronization, scanning

Change the second paragraph of 11.1.3 as shown below:

Active scanning is prohibited in some frequency bands and regulatory domains. The MAC of a STA receiving an MLME-SCAN.request shall use the regulatory domain information it has to process the request and shall return a result code of NOT_SUPPORTED to a request for an active scan if regulatory domain information indicates ~~an~~ any active scan is illegal. Where regulations permit active scanning after certain conditions are met, the active scan shall proceed after those conditions are met.

11.1.3.1 Passive Scanning

11.1.3.2 Active Scanning

11.1.3.2.1 Sending a Probe Response

Change the first paragraph of 11.1.3.2.1 as follows:

STAs, subject to criteria below, receiving Probe Request frames not containing an Interworking field in the Extended capabilities element set to 1, shall respond with a Probe Response only if

Insert the following text after the first paragraph (bulleted list) of 11.1.3.2.1 as shown below:

STAs having dot11InterworkingServiceEnabled set to TRUE, subject to criteria below, receiving Probe Request frames containing an Interworking field in the Extended capabilities element set to 1 shall respond with a Probe Response only if:

a) The SSID in the Probe Request is the wildcard SSID, the SSID in the Probe Request is the specific-SSID of the STA, or the specific SSID of the STA is included in the SSID List element,

b) The BSSID field in the Probe Request is the wildcard BSSID or the BSSID of the STA, ~~and~~

c) The DA field in the Probe Request is the broadcast address or the specific MAC address of the STA.~~,~~

d) the HESSID field, if present in the Interworking element, is the wildcard HESSID or the HESSID of the STA, and

e) the Network Type field in the Interworking element is the wildcard Network Type or the Network Type of the STA.

11.3 STA authentication and association

11.3.2 Association, reassociation, and disassociation

11.3.2.1 STA association procedures

Change the text as follows:

a) The STA shall transmit an Association Request frame to an AP with which that STA is authenticated. If the MLME-ASSOCIATE.request primitive contained an RSN information element with only one pairwise cipher suite and only one authenticated key suite, this RSN information element shall be included in the Association Request frame. If dot11InterworkingServiceEnabled is true and the STA does not have credentials for the AP, and the STA is initiating an Unauthenticated Emergency Service Accessible connection, it includes the Interworking element with the Unauthenticated Emergency Service Accessible bit set to 1.

11.3.2.2 AP association procedures

Change the text as follows:

When an Association Request frame is received from a STA, the AP shall associate with the STA using the following procedure:

a) If the STA is not authenticated, the AP shall transmit a Deauthentication frame to the STA and terminate the association procedure.

a1 If the Association Request frame includes the Interworking element with Unauthenticated Emergency Service Accessible field set to 1 and does not include an RSN element, then the AP shall accept the association request even if dot11RSNAEnabled is set to TRUE and dot11PrivacyInvoked is set to TRUE thereby granting unsecured access to Emergency Services only when UESA is set to 1.

11.3.2.3 STA reassociation procedures

Change the text as follows:

Upon receipt of an MLME-REASSOCIATE.request primitive, a STA shall reassociate with an AP via the following procedure:

b) The STA shall transmit a Reassociation Request frame to the new AP. If the MLME-REASSOCIATE.request primitive contained an RSN information element with only one pairwise cipher suite and only one authenticated key suite, this RSN information element shall be included in the Reassociation Request frame.

b1) If dot11InterworkingServiceEnabled is true and the STA was associated to the ESS for Unauthenticated Emergency Service Accessible, it includes the Interworking element with the Unauthenticated Emergency Service Accessible bit set to 1 in the MLME-REASSOCIATE.request primitive.

11.3.2.4 AP reassociation procedures

Change the text as follows:

Whenever a Reassociation Request frame is received from a STA, the AP uses the following procedure to support reassociation:

a) a) If the STA is not authenticated, the AP shall transmit a Deauthentication frame to the STA and terminate the reassociation procedure.

a1) If the Reassociation Request frame includes the Interworking element with Unauthenticated Emergency Service Accessible field set to 1 and does not include an RSN element, then the AP shall accept the association request even if dot11RSNAEnabled is set to TRUE and dot11PrivacyInvoked is set to TRUE thereby granting unsecured access to Emergency Services only when UESA is set to 1.

11.4 TS Operation

11.4.1 Introduction

Insert the following text after the second paragraph of 11.4.1 as shown below:

TS may have zero or one Expedited Bandwidth Request (EBR) element associated with it. An AP uses the parameters in the EBR to understand the precedence level requested by a non-AP STA (see Annex W.4.3). For example, the precedence level may be used to convey to the AP that the requested TS is for the purposes of placing an emergency call. Support for precedence levels greater than 18 is optional for STAs.

Change the third paragraph of 11.4.1 as shown below:

Traffic specification (TSPEC), ~~and~~ the optional traffic classification (TCLAS) elements, and the optional EBR element are transported on the air by the ADDTS, in the corresponding QoS Action frame and across the MLME SAP by the MLME-ADDTS primitives. In addition, a TS could be created if a STA sends a resource request to an AP prior to initiating a transition to that AP or in the Reassociation Request frame to that AP.

Insert the following text as the last paragraph at the end of 11.4.1:

When dot11SSPNInterfaceEnabled is set to TRUE, TSPEC processing by the HC may be subject to limitations received from the SSPN interface. The SSPN may limit access to certain QoS priorities, and further restrict the data rate and delay used with any priority.

11.4.2 TSPEC construction

11.4.3 TS lifecycle

Change the fifth paragraph of 11.4.3 as follows:

An active TS becomes inactive following a TS deletion process initiated at either non-AP STA or HC. It also becomes inactive following a TS timeout detected at the HC, or if the HC within an AP having dot11SSPNInterfaceEnabled set to TRUE determines as defined in 11.23.4 that the non-AP STA’s TS has exceeded the transmitted MSDU limit for the access category in which the TS was admitted. When an active TS becomes inactive, all the resources allocated for the TS are released.

11.4.4 TS setup

Change the fifth paragraph of 11.4.4 as follows:

The SME in the HC decides whether to admit the TSPEC as specified, refuse the TSPEC, or not admit but suggest an alternative TSPEC. If the TSPEC is received from a non-AP STA by an AP having dot11SSPNInterfaceEnabled set to TRUE, the HC shall use the permissions stored in the dot11InterworkingEntry for that STA in the decision to admit or deny the request. The SME then generates an MLME-ADDTS.response primitive containing the TSPEC and a ResultCode value. The contents of the TSPEC and Status fields contain values specified in 10.3.24.4.2.

Insert the following text after the fifth paragraph of 11.4.4 as follows:

When the HC in an AP having dot11SSPNInterfaceEnabled set to TRUE receives a TSPEC, the AP shall inspect it to determine the requested access policy, user priority and mean datarate.

a) The access category shall be determined from the user priority according to Table 9-1. For a TS to be admitted when the requested access policy is set to EDCA, both of the following shall be true:
   - i) The field corresponding to this access category in dot11NonAPStationAuthAccessCategories from the non-AP STA's dot11InterworkingEntry is equal to 1.
   - ii) The sum of the mean data rate of all the requesting STA's active TSs in this access category plus the mean data rate in the TSPEC is less than or equal to the non-AP STA's dot11InterworkingEntry for dot11NonAPStationAuthMaxVoiceRate, dot11NonAPStationAuthMaxVideoRate, dot11NonAPStationAuthMaxBestEffortRate, or dot11NonAPStationAuthMaxBackgroundRate depending on whether the derived access category is AC_VO, AC_VI, AC_BE or AC_BK, respectively.

b) For a TS to be admitted when the requested access policy is set to HCCA, all of the following shall be true:
   - i) The dot11NonAPStationAuthHCCAHEMM value is set to TRUE.
   - ii) The sum of the mean data rate of all the requesting STA's active TSs having access policy set to HCCA plus the mean data rate in the TSPEC is less than or equal to dot11NonAPStationAuthMaxHCCAHEMMRate in the non-AP STA's dot11InterworkingEntry.
   - iii) The delay bound which will be provided by the HC in the TSPEC response is less than or equal to dot11NonAPStationAuthHCCAHEMMDelay in the non-AP STA's dot11InterworkingEntry.

Change the sixth paragraph of 11.4.4 as follows:

The HC MAC transmits an ADDTS Response frame containing this TSPEC and status. The encoding of the ResultCode values to Status Code field values is defined in Table 11-2. In an AP having dot11SSPNInterfaceEnabled set to TRUE, the HC shall set the dot11NonAPStationAddtsResultCode in the non-AP STA's dot11InterworkingEntry equal to the ResultCode.

Change the Table 11-2 by inserting a new code into the ResultCode list as shown below.

Table 11-2—Encoding of ResultCode to Status Code field value

ResultCode	Status code
SUCCESS	0
INVALID_PARAMETERS	38
REJECTED_WITH_SUGGESTED_CHANGES	39
REJECTED_HOME_WITH_SUGGESTED_CHANGES	43
REJECTED_FOR_DELAY_PERIOD	47

Insert the following text as the last paragraph of 11.4.4 as shown below:

When a STA requests service at a higher priority than authorized by its dot11InterworkingTableEntry, the HC may optionally provide a suggested TSPEC with a data rate and lower priority that would be authorized. Usage of the TSPEC in an Interworking environment is described in Annex K (Admission Control).

11.7 DLS operation

11.7.1.2 Setup procedure at the AP

Change the second paragraphs of 11.7.1.2 as indicated:

Upon receipt of the DLS Request frame (step 1a in Figure 11-15), the AP shall

- Send DLS Response frame to the STA that sent the DLS Request frame with a result code of Not Allowed in the BSS, if direct links are not allowed in the BSS, or for the AP with dot11SSPNInterfaceEnabled set to TRUE with a result code of Not Allowed by SSP if the dot11NonAPStationAuthDls MIB variable in either of the non-AP STA's dot11InterworkingTable.

Insert the following subclause after 11.22

11.23 WLAN Interworking with External Networks Procedures

This subclause describes the actions and the procedures that provide interworking capabilities between 802.11 infrastructure and external networks.

11.23.1 Interworking capabilities and information

STAs indicate their support for Interworking Service by setting the dot11InterworkingServiceEnabled MIB variable to true. When dot11InterworkingServiceEnabled is true, APs include the Interworking element in Beacon and Probe Response frames and non-AP STAs include the Interworking element in Probe Request frames.

When dot11InterworkingServiceEnabled. and dot11ExtendedChannelSwitchEnabled are both set to TRUE, the AP may provide its operating channel and regulatory class to an Interworked SSPN using the dot11RegulatoryClassesTable MIB entry.

The Interworking information element contains signaling for Homogeneous ESSs. The HESSID is a 6 octet MAC address which identifies the homogeneous ESS. The HESSID value shall be identical to one of the BSSIDs in the homogeneous ESS. Thus, it is a globally unique identifier, which in conjunction with the SSID, may be used to provide network identification for an SSPN.

NOTE—It is required by this standard that the HESSID field in the Interworking element is administered consistently across all BSSs in a homogeneous ESS.

The Interworking information element also provides a Network Type value in Beacon and Probe Response frames to assist the non-AP STA with network discovery and selection.

11.23.2 Interworking Procedures: Generic Advertisement Services

This subclause describes the actions and procedures that are used to invoke Generic Advertisement Services (GAS). GAS may be used to enable network selection for STAs having dot11InterworkingServiceEnabled set to TRUE. GAS provides transport mechanisms for advertisement services while STAs are in un-associated state as well as the associated state, as defined in 11.3. This is accomplished via the use of Public Action management frames which are class 1 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.

There are two forms for GAS: Native GAS and Non-Native GAS. Native GAS is used with NQP (see Table 7-43bg) and Non-Native GAS is used for all other advertisement protocols. A native-GAS message exchange may take place between two STAs; one STA transmits a GAS query and the receiving STA transmits the GAS Query Response as described in 11.23.2.1. However, as described in 11.23.2.2 for non-native GAS, a non-AP STA shall transmit the GAS query and an AP shall transmit the GAS response.

Native GAS uses GAS Public Action frames for transport of NQP. NQP supports the query request and response mechanism for information defined in 7.3.4. It is referred to as “native” since this information is available at STA and there is no need to query a server in an external network for the requested information.

Non-Native GAS uses GAS Public Action frames for transport of a query request and response using one of the query protocols in Table 7-43be. Non-Native GAS shall be supported by a STA when dot11InterworkingServiceEnabled is true and one or more dot11GASAdvertisementID are not null. Support for Non-Native GAS advertisement protocols on a STA is optional when dot11InterworkingServiceEnabled is true and all dot11GASAdvertisementID are null. Non-AP STAs shall not use Non Native GAS advertisement protocols unless the advertisement protocol ID is included in the advertisement protocol element in a beacon or Probe Response frame. The Advertisement Protocol information element specifies the Advertisement Protocols that a non-AP STA may use to communicate with advertisement servers, which may be located in an external network. The Advertisement Protocol identifies the query language used by the advertisement server.

The GAS protocol, which is used to transport Queries and Query Responses, is transparent to the Advertisement Protocol. GAS information delivery is supported only using individually addressed action frames.

11.23.2.1 Native GAS Protocol

11.23.2.1.1 Native Query protocol procedures

Native GAS shall be supported by a STA whenever dot11InterworkingServiceEnabled is true. A STA may use Native GAS protocol to discover supported services.

A STA accomplishes this by transmitting one or more Info IDs or NQP vendor-specific query elements in the Query Request field in a GAS Initial Request Action frame. The receiving STA responds to the query using a GAS Initial Response Action frame. GAS Comeback Request and GAS Comeback Response Action frames are not used for Native GAS.

Native Query Protocol (NQP) frame usage for Infrastructure BSSs and IBSSs shall be in accordance with Table 11-3. Frame usage defines the entities permitted to transmit and received particular NQP elements. STAs with dot11InterworkingServiceEnabled set to TRUE which are capable of operating in an IBSS shall be capable of requesting a Capability List and returning the Capability List in a native-GAS message exchange; STA support for all other NQP elements is optional. APs with dot11InterworkingServiceEnabled set to TRUE which are capable of operating in an Infrastructure BSS shall be capable of returning the Capability List in a native-GAS message exchange; AP support for all other NQP elements is optional. Non-AP STAs with dot11InterworkingServiceEnabled set to TRUE which are capable of operating in an Infrastructure BSS shall be capable of requesting the Capability List in a native-GAS message exchange; non-AP STA support for all other NQP elements is optional.

Table 11-3—Native Query Protocol usage

		BSS		IBSS
Info Name	**Native Info Element (clause)**	**AP**	**Non-AP STA**	**STA**
Capability List	7.3.4.1	T, R	T, R	T, R
Venue Name information	7.3.4.2	T	R	----
Emergency Call Number information	7.3.4.3	T	R	----
Network Authentication Type information	7.3.4.4	T	R	----
Roaming Consortium List	7.3.4.5	T	R	----
Native Query Protocol vendor-specific list	7.3.4.6	T, R	T, R	T, R
IP Address Type Availability information	7.3.4.7	T, R	T, R	T, R
NAI Realm List	7.3.4.8	T	R	T, R
3GPP Cellular Network information	7.3.4.9	T	R	----
AP Geospatial Location	7.3.4.10	T	R	T, R

Table 11-3—Native Query Protocol usage *(continued)*

		BSS		IBSS
Info Name	**Native Info Element (clause)**	**AP**	**Non-AP STA**	**STA**
AP Civic Location	7.3.4.11	T	R	T, R
Domain Name List	7.3.4.12	T	R	----
Emergency Alert URI	7.3.4.13	T	R	T, R

Symbols

T	NQP element may be transmitted by MAC entity
R	NQP element may be received by MAC entity
---	NQP element is neither transmitted nor received by MAC entity

A STA that encounters an unknown or reserved NQP Info ID value in a GAS frame (see Table 7-57aj) received without error shall ignore that NQP Info ID and shall parse any remaining NQP Info IDs.

A STA that encounters an unknown vendor-specific OI field or subfield in a GAS frame (see Table 7-57aj) received without error shall ignore that field or subfield respectively, and shall parse any remaining fields or subfields for additional information with recognizable field or subfield values.

11.23.2.1.1.1 AP Geospatial Location procedures

A STA having dot11InterworkingServiceEnabled set to true, may retrieve an AP's Geospatial location using Native-GAS procedures in 11.23.2.1. A STA in the associated state should retrieve geospatial location information from the AP using the procedures in 11.10.8 or 11.22.4.

11.23.2.1.1.2 AP Civic Location procedures

A STA having dot11InterworkingServiceEnabled set to true, may retrieve an AP's Civic location using Native-GAS procedures in 11.23.2.1. A STA in the associated state should retrieve Civic location information from the AP using the procedures in 11.10.8 or 11.23.4.

11.23.2.1.1.3 AP Procedures for advertising EAP Method associated with an NAI Realm

When dot11RSNAEnabled is true, NAI Realms along with their supported authentication methods may be advertised using the NAI Realm List (see 7.3.4.8). Each realm may be optionally associated with a set of EAP methods. Each EAP method may be optionally associated with a set of Authentication Parameters. The NAI realm information provides a hint on the methods a STA can establish an association in an RSN IEEE 802.1X environment. If the non-AP STA recognizes the NAI Realm, it may attempt authentication even if it believes the EAP methods are incorrect.

A non-AP STA where dot11InterworkingServiceEnabled is true, may process the NAI realm list. The selection of the NAI realm the non-AP STA uses for authentication is out of scope of this standard.

A non-AP STA having dot11InterworkingServiceEnabled may optionally process the EAP Method list as follows:

- The EAP Method list provided by the AP shall be in priority order (the most preferred EAP Method is listed first).
- The credential types help the STA to determine what credentials to use for authentication
- The STA should confirm the GAS advertisement after an RSNA is established by performing a native-GAS query for the NAI Realm List using Protected Dual of Public Action frames.

Note—The advertisements should be confirmed after the RSNA is established to avoid downgrade attacks.

The policy which determines whether or not a non-AP STA should attempt authentication and/or association with any particular IEEE 802.11 Access Network is outside the scope of this standard.

11.23.2.1.2 Native GAS Procedures at the Requesting STA

Upon receipt of an MLME-GAS.request primitive with Advertisement Protocol ID set to NQP, the requesting STA shall engage in a Native GAS message exchange according to the following procedure:

a) The STA sends a Native GAS query by transmitting a GAS Initial Request Action frame containing a Dialog Token, an Advertisement Protocol information element containing an Advertisement Protocol ID set to NQP, one or more Native Query Info ID values drawn from Table 7-43bg that are not equal to the vendor-specific value, followed by zero or more NQP vendor-specific query elements in the Query Request field.

   Alternatively, the STA may send a Native GAS query by transmitting a GAS Initial Request Action frame containing a Dialog Token, an Advertisement Protocol information element containing an Advertisement Protocol ID set to NQP, zero or more Native Query Info ID values drawn from Table 7-43bg that are not equal to the vendor-specific value, followed by one or more NQP vendor-specific query elements in the Query Request field.

b) Upon transmission of the GAS Initial Request Action frame, the non-AP STA shall set a timer equal to the dot11GASResponseTimeout MIB object 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 STA is not associated to an AP, it shall remain in active mode until the receipt of a GAS Initial Response Action frame with the same Dialog Token as in the GAS Initial Request Action frame or until the expiry of the timer, whichever occurs first. If the requesting STA is a non-AP STA and is in the associated state, it may go into power save mode until the GAS Initial Response Action frame is available for receipt or the timer expiry, whichever occurs first.

d) If a GAS Initial Response Action frame is received with a status value of “successful”, the Native query was successful and the MLME shall issue an MLME-GAS.confirm primitive indicating successful completion of the query along with the query response.

e) If the timer expires before a GAS Initial Response Action frame is received, the Native query was not successful and the MLME shall issue an MLME-GAS.confirm primitive indicating timeout and shall set the Query Response Length to 0.

f) If a GAS Initial Response Action frame is received with a status value indicating “Request Info Not Configured” (Table 11-4), the Native query was not successful because the information corresponding to the query was not configured on the STA. The MLME shall issue an MLME-GAS.confirm primitive so indicating and shall set the Query Response Length to 0.

g) If a GAS Initial Response Action frame is received with a status value indicating “Partial Query Response” (Table 11-4), only part of the Native Query Response would fit within the maximum MMPDU size. The MLME shall issue an MLME-GAS.confirm primitive so indicating and shall include the Query Response provided in the GAS Initial Response Action frame. Upon receiving this response, the SME may compare it with the Query request to determine the Native Query protocol elements which were not included and transmit a subsequent query for those elements.

Table 11-4—GAS MLME Primitive's Encoding of Result Code to Status Code field

StatusCode	ResultCode
59	ADVERTISEMENT_PROTOCOL_NOT_SUPPORTED
60	NO_REQUEST_OUTSTANDING
61	QUERY_RESPONSE_OUTSTANDING
62	TIMEOUT
63	QUERY_RESPONSE_TOO_LARGE
64	PARTIAL_QUERY_RESPONSE_CONFIG
65	SERVER_UNREACHABLE
66	REQUEST_INFO_NOT_CONFIGURED
67	TRANSMISSION_FAILURE
68	PARTIAL_QUERY_RESPONSE_SIZE

11.23.2.1.3 Native GAS Procedures at the Responding STA

Upon receipt of a GAS Initial Request Action frame with Advertisement Protocol ID set to NQP, an MLME-GAS.indication primitive shall be issued to the STA's SME. Upon receipt of an MLME-GAS.response primitive, the STA shall transmit a GAS Initial Response Action frame to the requesting STA according to the following procedures. If the requesting STA is a non-AP STA, is in the associated state and in the power-save mode, the AP shall buffer the frame for transmission according to the procedures in 11.2.1; otherwise the AP shall queue the frame for transmission. If the requesting STA is a member of an IBSS in which PS mode is permitted, the STA shall buffer the frame for transmission according to the procedures in 11.2.2; otherwise the STA shall queue the frame for transmission. The Comeback Delay shall be set to 0 in GAS Initial Response Action frames.

a) If the query request corresponds to information that has been configured on the STA, the STA shall transmit a directed GAS Initial Response Action frame to the requesting STA containing a dialog token whose value is identical to the dialog token in the GAS Initial Request Action frame, a Status Code set to "success", an Advertisement Protocol information element containing an Advertisement Protocol ID set to NQP and a query response containing one or more Native Info elements corresponding to the query (Table 7-43bg). If the query request Info ID contained a value equal to the Native Query protocol Vendor Specific List value, then one or more Native Query protocol Vendor Specific List elements (see 7.3.4.6) shall be returned in the Query Response field.

b) If all of the InfoIDs in the query requests corresponds to information that is not available on the STA, the STA shall transmit a directed GAS Initial Response Action frame to the requesting STA containing a dialog token whose value is identical to the dialog token in the GAS Initial Request Action frame, a Status Code equal to "Request Info Not Configured", an Advertisement Protocol information element containing an Advertisement Protocol ID set to NQP and a Query Response Length set to 0.

c) If one or more of the Info IDs in the query request corresponds to information that has been configured on the STA and one or more of the Info IDs in the query request corresponds to information that is not available on the STA, the STA shall transmit a directed GAS Initial Response Action frame to the requesting STA containing a dialog token whose value is identical to the dialog token in the GAS Initial Request Action frame, a Status Code equal to "Partial Query Response returned—one or more of the requested NPQ elements is not configured for this BSSID", an Advertisement

Protocol information element containing an Advertisement Protocol ID set to NQP and a Query Response containing the available NQP response elements.

Note—this behavior facilitates a requesting STA to combine a query for the Capabilities List with a query for other NQP elements into a single query request before it's known to the requesting STA whether or not they can be provided in a query response. This may lead to a more efficient query and response message exchange.

d) If the query response is larger than the MMPDU maximum payload size, the STA shall transmit a directed GAS Initial Response Action frame to the requesting STA containing a dialog token whose value is identical to the dialog token in the GAS Initial Request Action frame, a Status Code equal to "Partial Query Response returned—MMPDU cannot hold all requested NQP elements", an Advertisement Protocol information element containing an Advertisement Protocol ID set to NQP and a Query Response containing as many query response elements as will fit within an MMPDU. The STA shall only include complete NQP elements in the query response.

11.23.2.2 Non-Native GAS Protocol

A non-AP STA obtains GAS advertisement capability information from Beacon or Probe Response frames. The Advertisement Protocol information element indicates the Advertisement Protocol IDs supported in the BSS. A non-AP STA transmits a Non-Native GAS query using GAS Initial Request Action frames and the AP provides information on how to receive the query response via a GAS Initial Response Action frame.

11.23.2.2.1 Non-AP STA Procedures to Transmit a Non-Native GAS Query

Upon receipt of an MLME-GAS.request primitive with Advertisement Protocol ID not set to NQP, the non-AP STA shall engage in the following procedure to transmit a query:

a) The non-AP STA sends a Non-Native GAS query by transmitting a GAS Initial Request Action frame containing a Dialog Token, an Advertisement Protocol information element containing an Advertisement Protocol ID not set to NQP and the Query Request field.

b) Upon transmission of the GAS Initial Request Action frame, the STA shall set a timer, referred to as the dot11GASResponseTimer, equal to the dot11GASResponseTimeout MIB object 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 non-AP STA is not in the associated state, it shall remain in active mode until the receipt of a GAS Initial Response Action frame with the same Dialog Token as in the GAS Initial Request Action frame or until the expiry of the timer, whichever occurs first. If the non-AP STA is in the associated state, it may go into power save state until the GAS Initial Response Action frame is available for receipt or the timer expiry, whichever occurs first.

d) If a GAS Initial Response Action frame is received with a status value equal to "successful", the Non-Native query was successfully sent and the non-AP STA shall use the procedures outlined in 11.23.2.2.3 to retrieve the query response. Upon reception of the GAS Initial Response Action frame with a status value equal to "successful", the non-AP STA shall reset the dot11GASResponseTimer to the value in the dot11GASResponseTimeout MIB object.

e) If a GAS Initial Response Action frame is received with a status value equal to "Advertisement Protocol Not Supported", the Non-Native GAS query was not successful and the MLME shall issue an MLME-GAS.confirm primitive with status so indicating and shall set the Query Response Length field to 0.

f) If a GAS Initial Response Action frame is received with a status value equal to "Server unreachable", the Non-Native GAS query was not successful and the MLME shall issue an MLME-GAS.confirm primitive with status so indicating and shall set the Query Response Length field to 0.

g) If the dot11GASResponseTimer expires before a GAS Initial Response Action frame is received, the Non-Native GAS query was not successful and the MLME shall issue an MLME-GAS.confirm primitive indicating "timeout" and shall set the Query Response Length field to 0.

11.23.2.2.2 AP procedures to respond to a Non-Native GAS query

Upon receipt of a GAS Initial Request Action frame with Advertisement Protocol ID not set to NQP, an MLME-GAS.indication primitive shall be issued to the AP's SME. Upon receipt of an MLME-GAS.response primitive, the AP shall transmit a GAS Initial Response Action frame to the requesting non-AP STA according to the following procedures. If the requesting non-AP STA is in the associated state and in the power-save mode, the AP shall buffer the frame for transmission according to the procedures in 11.2.1; otherwise the AP shall queue the frame for transmission.

a) If the Advertisement Protocol ID in the Advertisement Protocol information element does not equal the value contained in any dot11GASAdvertisementID MIB object, then the AP shall not post the query to an Advertisement server in an external network. The AP shall transmit a directed GAS Initial Response Action frame to the requesting non-AP STA containing a dialog token whose value is identical to the dialog token in the GAS Initial Request Action frame, a Status Code equal to "Advertisement Protocol Not Supported" (see Table 11-4), an Advertisement Protocol information element corresponding to the Advertisement Protocol ID contained in the GAS Initial Request Action 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 in an external network is currently unreachable, the AP shall transmit a directed GAS Initial Response Action frame to the requesting non-AP STA containing a dialog token whose value is identical to the dialog token in the GAS Initial Request Action frame, a Status Code equal to "Server Unreachable", an Advertisement Protocol information element containing an Advertisement Protocol ID corresponding to the Advertisement Protocol ID contained in the GAS Initial Request Action frame and a 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 scope of this specification. A non-AP STA receiving a status code indicating the server is unreachable should wait at least 1 minute before transmitting any further queries using the same Advertisement Protocol ID to any AP in the homogeneous ESS.

c) If the Advertisement Protocol ID in the Advertisement Protocol information element equals the value contained in any dot11GASAdvertisementID MIB object, then the AP shall post the query to the Advertisement server in an external network. The methods and protocols the AP uses to post the query are outside the scope of this specification.

d) Upon posting the query to the server in an external network the AP initializes a timer, referred to as the PostReplyTimer, to the value in dot11GASResponseTimeout MIB object.

e) The AP shall then transmit an individually addressed GAS Initial Response Action frame to the requesting non-AP STA containing a dialog token whose value is identical to the dialog token in the GAS Initial Request Action frame, a Status Code set to "success", an Advertisement Protocol information element corresponding to the Advertisement Protocol ID contained in the GAS Initial Request Action frame, a GAS Comeback Delay set to the value in dot11GASComebackDelay for this Advertisement Protocol and a Query Response Length set to 0.

11.23.2.2.3 AP Procedures for delivering a non-Native GAS Query Response

After receiving a query response from a server in an external network, an AP shall buffer the query response for a minimum of dot11GASResponseBufferingTime after the expiry of the GAS Comeback Delay. If the AP does not receive a GAS Comeback Request frame whose source MAC address and Dialog Token match the source MAC address and Dialog Token respectively of the corresponding GAS Initial Response Action frame within this time, it may drop the query response.

If an AP receives a Query Response from a server in an external network which is larger than the configured Query Response Length Limit, it shall discard the response and instead return a status code of "GAS Query Response larger than permitted per configured AP policy" in the GAS Comeback Response Action frame. This behavior helps to prevent abuses of the medium which may be caused by overly general queries, which evoke a very large query response.

The GAS protocol supports Query Responses whose length is greater than the 802.11 maximum MMPDU size by the AP's use of the GAS Query Response Fragment ID field in the GAS Comeback Response Action frame; the Query Response Fragment ID shall be set to 1 for the initial fragment and incremented by 1 for each subsequent fragment in a multi-fragment query response. If the Query Response is a multi-fragment response (i.e., contains more than 1 fragment), the AP shall transmit all fragments that belong to the same Query Response until all fragments are exhausted. The AP shall set the More GAS Fragments field of the GAS Query Response Fragment ID to 0 when the transmitted fragment is the final fragment.

An AP shall use the following procedures to deliver a Non-Native GAS Query Response. Upon receipt of a GAS Comeback Request Action frame with Advertisement Protocol ID not set to NQP, an MLME-GAS.indication primitive shall be issued to the AP's SME. Upon receipt of an MLME-GAS.response primitive, the AP shall transmit a GAS Comeback Response Action frame to the requesting STA according to the following procedures. If the requesting non-AP STA, is in the associated state and in the power-save mode, the AP shall buffer the frame for transmission according to the procedures in 11.2.1; otherwise the AP shall queue the frame for transmission.

a) If the PostReplyTimer expires before the GAS Query Response is received from the advertisement server in an external network then the AP shall buffer for transmission a GAS Comeback Response Action frame with a status code equal to "Timeout" (see Table 11-4). If the query response is subsequently received from the server in an external network, it shall be dropped by the AP.

b) If the Query Response received from the server is larger than dot11GASQueryResponseLengthLimit, it shall be dropped by the AP. Then the AP shall buffer for transmission a GAS Comeback Response Action frame with status code set to "Query Response too large".

c) If the Query Response is received from the external network before the expiry of the PostReplyTimer and its length is less than dot11GASQueryResponseLengthLimit, then the Query Response shall be buffered in one or more GAS Comeback Response Action frames with a status code set to "success". The AP transmits one GAS Comeback Response Action frame in response to each GAS Comeback Request Action frame. If the Query Response received from the external network is less than or equal to the maximum MMPDU payload size, then the GAS Query Response Fragment ID shall be set to zero and the More GAS Fragments field in the GAS Query Response Fragment ID shall be set to zero. If the Query Response received from the external network is greater than the maximum MMPDU payload size, then the GAS Query Response Fragment ID shall be set to zero 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 one if there are more fragments of the Query Response to be transmitted, otherwise it shall be set to zero (i.e., this fragment is the last fragment of the Query Response).

d) If a query response has not been received from the external network and the PostReplyTimer has not expired, the AP shall transmit a GAS Comeback Response Action frame with status equal to "Query response outstanding" (see Table 11-4) and GAS Comeback Delay set to the value in dot11GasComebackDelay for this Advertisement Protocol to indicate when the non-AP STA should comeback to obtain its Query Response.

e) If an AP receives a GAS Comeback Request Action frame whose source MAC address and Dialog Token do not match the destination MAC address and Dialog Token respectively of an outstanding GAS Initial Response Action frame, the AP should transmit a GAS Comeback Response action frame with a status code equal to "No request outstanding".

11.23.2.2.4 Non-AP STA Procedures to retrieve a non-Native Query Response

A non-AP STA shall transmit a GAS Comeback Request Action frame including the Dialog Token (drawn from the corresponding GAS Initial Response Action frame) immediately after the expiry of the GAS Comeback Delay. In response, the AP provides the Query Response in one or more GAS Comeback Response Action frames with the corresponding Dialog Token.

If a non-AP STA receives a GAS Comeback Response Action frame with status set to “Query response outstanding”, the non-AP STA shall wait for the GAS Comeback Delay from that frame and upon expiry of the GAS Comeback Delay, transmit another GAS Comeback Request Action frame. If the non-AP STA’s dot11GASResponseTimer (set in 11.23.2.2.1 step b) expires prior to receiving a GAS Comeback Response Action frame whose source MAC address and Dialog Token match those in the corresponding GAS Initial Response Action frame, the STA shall issue an MLME-GAS.confirm primitive with result code set to “timeout” and shall set the Query Response Length to 0.

If a non-AP STA receives a GAS Comeback Response Action frame with status set to “success” and the More GAS Fragments field in the GAS Query Response Fragment ID set to one, it shall transmit another GAS Comeback Request Action frame in order to retrieve the next GAS fragment of a multi-fragment query response.

If a non-AP STA receives a GAS Comeback Response Action frame with status set to “success” and the More GAS Fragments field in the GAS Query Response Fragment ID set to zero, the non-AP STA’s MLME shall determine that all fragments have been received by confirming that all fragment IDs from 0 to the value in the GAS Query Response Fragment ID when the More GAS Fragments field was set to 0 have been received. Upon receipt of the first GAS Comeback Response frame and every GAS Comeback Response Action frame thereafter, the dot11GASResponseTimer shall be reset. If all of the query response fragments were received before the expiry of the dot11GASResponseTimer, then the MLME shall issue an MLME-GAS.confirm with result code set to “success” along with the query response. If all of the query response fragments were not received before the expiry of the dot11GASResponseTimer, then the MLME shall issue an MLME-GAS.confirm with result code set to “transmission failure” and shall set the Query Response Length to 0.

After a non-AP STA receives the first GAS fragment of a multi-fragment query response, it shall continue retrieving the query response until all GAS fragments are received or until a transmission failure is detected; the non-AP STA shall not commence the retrieval of a another non-native GAS Query Response from the same AP until all GAS fragments are received or until a transmission failure is detected on the first GAS Query Response.

If a non-AP STA receives a GAS Comeback Response with status set to “Timeout” or “Query Response too large”, then the MLME shall issue an MLME-GAS.confirm with result code so indicating and shall set the Query Response Length to 0.

If a non-AP STA receives a GAS Comeback Response with status set to “No request outstanding”, then the MLME shall issue an MLME-GAS.confirm with result code set to “unspecified failure” and shall set the Query Response Length to 0.

11.23.2.2.5 Non-Native GAS procedures interaction with Multiple BSSID Set

Non-AP STAs in the un-associated state may use non-native GAS procedures to query servers in an external network for information. As described in 11.23.2.2, APs indicate their support for a particular Non-Native GAS advertisement protocol by including an Advertisement protocol element with that Advertisement protocol ID in Beacon and Probe Response frames as described in 7.2.3.1 and 7.2.3.9 respectively. Non-AP STAs receiving Beacon or Probe Response frames from different APs may choose to engage in GAS frame exchange sequences with one or more of these APs. In some deployment scenarios, these APs may be operating as a Multiple BSSID set (as defined in 11.10.11) and may relay the GAS queries to the same logical advertisement server. Depending on the configuration of the IEEE 802.11 access network, the external network and the advertisement server, a query response from the advertisement server may or may not be dependent on the BSSID used in the GAS frame exchange sequence and thus the AP from which the query was relayed. If the GAS Query Response is dependent on the BSSID, a non-AP STA may choose to post queries using GAS procedures to more than one AP and expect possibly different Query Responses. If the Query Response is not dependent on the BSSID, then a non-AP STA may choose to post queries using GAS procedures to only one AP in the Multiple BSSID set (i.e., posting the same query to another member of the Multiple BSSID set would yield the same response).

When a Multiple BSSID (as defined in 11.10.11) set contains two or more members and dot11InterworkingServiceEnabled is set to TRUE and dot11GASAdvertisementID is not null and a query to the advertisement server corresponding to the value of dot11GASAdvertisementID is not dependent on the BSSID value used in the GAS frame exchange sequence to post the query, then the PAME-BI bit in the Advertisement protocol tuple of the Advertisement protocol element corresponding to the value of dot11GASAdvertisementID shall be set to 1; otherwise this bit shall be set to zero.

11.23.3 Interworking Procedures: IEEE 802.21 MIH Support

The IEEE 802.21 MIH (Media Independent Handover) standard supports handovers across heterogeneous networks. APs with dot11InterworkingServiceEnabled set to TRUE and having the dot11GasAdvertisementId MIB object set to MIH Information Service (see Table 7-43be) shall support the transmission and reception of MIIS queries for non-AP STAs in all states. APs with dot11InterworkingServiceEnabled set to TRUE and having a dot11GasAdvertisementId MIB object set to MIH Command and Event Services Capability Discovery (see Table 7-43be) provide support for MICS/MIES capability discovery for non-AP STAs in all states.

Additionally, support for MIIS query and MICS/MIES capability discovery to non-AP STA's in the associated state is provided by the AP moving IP datagrams destined for the MIH PoS to the DS.

A non-AP STA discovers support for these services by receiving Beacon or Probe Response frames with an Advertisement Protocol information element having Advertisement Protocol ID(s) for MIH Information Service and/or MIES/MICS capability discovery.

Non-AP STAs in the un-authenticated or un-associated or associated states can use Non-Native GAS procedures to discover MIH Command and Event Services Capability as specified in Table 7-43be.

11.23.4 Interworking Procedures: Interactions with SSPN

11.23.4.1 General Operation

To provide SSPN Interface services, the IEEE 802.11 network interacts with the SSPN corresponding to the user of the non-AP STA either directly or via a roaming relationship. As part of setting up the RSN security association, user policies are communicated to the AP. If dot11SSPNInterfaceEnabled is true, these permissions shall be stored in the AP's dot11InterworkingTableEntry for that STA. Thereafter, the AP shall use the dot11InterworkingTableEntry for controlling the service provision to that non-AP STA. User policies from the SSPN affect authentication, authorization, and admission control decisions at the AP. In addition, the AP collects statistics about the non-AP STA and reports the statistics to the SSPN when requested. The SSPN may also send service provision instructions to the AP, e.g., to terminate the connection to a non-AP STA. Non-AP STAs do not support the SSPN Interface.

Network deployments typically provide that the AP and the server in the SSPN have a trustworthy channel that can be used to exchange information, without exposure to or influence by any intermediate parties. The establishment of this secure connection between the IEEE 802.11 infrastructure and the SSPN is out of scope of this standard.

11.23.4.2 Authentication and cipher suites selection with SSPN

When the non-AP STA initiates IEEE 802.1X authentication, in the Interworking case, the EAP messages are forwarded to the SSPN based on the home realm information provided by the non-AP STA. If the IEEE 802.11 infrastructure is unable to forward the EAP message, the AP having dot11SSPNInterfaceEnabled set to TRUE shall disassociate the non-AP STA with Reason Code “Disassociated because lack of SSP roaming agreement to SSPN”.

In addition to the EAP messages, the IEEE 802.11 infrastructure also provides extra information regarding the non-AP STA to the SSPN as defined in Annex W.3.1, e.g., the Cipher Suite supported by non-AP STA, the location of the AP to which the non-AP STA is associated, etc. Such information may be used by the SSPN to make authentication and service provisioning decisions.

In the SSPN Interface Service, the SSPN uses more information than is carried over EAP to decide on the authentication result. The SSPN can reject a connection request if the cipher suites supported by non-AP STA does not meet its security requirements. In this situation, the SME of the AP having dot11SSPNInterfaceEnabled set to TRUE shall invoke a disassociation procedure as defined in 11.3.2.7 by issuing the MLME-DISASSOCIATE.request primitive. The AP disassociates the corresponding non-AP STA with Reason Code “Requested service rejected because of SSPN cipher suite requirement”.

The SSPN can reject the association request based on the location of the non-AP STA, e.g., if the non-AP STA is requesting association to an AP or associated to an AP located in a forbidden zone. In this situation, the SME of the AP having dot11SSPNInterfaceEnabled set to TRUE shall invoke a disassociation procedure as defined in 11.3.2.7 by issuing the MLME-DISASSOCIATE.request primitive. The AP disassociates the corresponding non-AP STA with Reason Code “Requested service not authorized in this location”.

11.23.4.3 Reporting and Session Control with SSPN

An AP with dot11SSPNInterfaceEnabled set to TRUE shall create a dot11InterworkingEntry in its dot11InterworkingTable for each STA that successfully associates. Permissions received from the SSPN for each associated STA shall be populated into the table; if no permissions are received from the SSPN for a particular non-AP STA, then the default permissions or an AP’s locally defined policy may be used for that STA’s dot11InterworkingEntry. If the AP’s local policy is more restrictive than an object’s permission value received from the SSPN Interface, then the AP’s local policy may be enforced instead.

An AP having dot11SSPNInterfaceEnabled set to TRUE, the following procedure occurs:

- The non-AP STA's state contained within the dot11InterworkingEntry shall be transmitted to the new AP after a successful transition. The state definition and the protocol used to transfer the state are beyond the scope of this standard.
- After the state is successfully transmitted to the new AP, the dot11InterworkingEntry for that non-AP STA shall be deleted from the AP's dot11InterworkingTable.

An AP with dot11SSPNInterfaceEnabled set to TRUE shall delete the dot11InterworkingEntry for a non-AP STA when it disassociates from the BSS.

An AP with dot11SSPNInterfaceEnabled set to TRUE shall enforce the dot11InterworkingEntry limits for a particular non-AP STA by comparing the values of octet counters to authorized access limits:

- dot11NonAPStationVoiceOctetCount is compared to dot11NonAPStationAuthMaxVoiceOctets. When the value of the authorized maximum octet count is exceeded, if the ACM field for AC_VO is set to 1 then the HC shall delete all admitted TSs on this access category and deny all subsequent ADDTS request frames with TID set 6 or 7, or if the ACM field for AC_VO is set to 0 then the non-AP STA shall be disassociated.
- dot11NonAPStationVideoOctetCount is compared to dot11NonAPStationAuthMaxVideoOctets. When the value of the authorized maximum octet count is exceeded, if the ACM field for AC_VI is set to 1 then the HC shall delete all admitted TSs on this access category and deny all subsequent ADDTS request frames with TID set 4 or 5, or if the ACM field for AC_VI is set to 0 then the non-AP STA shall be disassociated.

- dot11NonAPStationBestEffortOctetCount is compared to dot11NonAPStationAuthMaxBestEffortOctets. When the value of the authorized maximum octet count is exceeded, if the ACM field for AC_BE is set to 1 then the HC shall delete all admitted TSs on this access category and deny all subsequent ADDTS request frames with TID set 0 or 3, or if the ACM field for AC_BE is set to 0 then the non-AP STA shall be disassociated.
- dot11NonAPStationBackgroundOctetCount is compared to dot11NonAPStationAuthMaxBackgroundOctets. When the value of the authorized maximum octet count is exceeded, if the ACM field for AC_BK is set to 1 then the HC shall delete all admitted TSs on this access category and deny all subsequent ADDTS request frames with TID set 1 or 2, or if the ACM field for AC_BK is set to 0 then the non-AP STA shall be disassociated.
- dot11NonAPStationHCCAHEMMOctetCount is compared to dot11NonAPStationAuthMaxHCCAHEMMOctets. When the value of the authorized maximum octet count is exceeded, then the HC shall delete all admitted TSs with access policy of HCCA or HEMM and deny all subsequent ADDTS request frames with access policy set to HCCA or HEMM.
- The sum of dot11NonAPStationVoiceOctetCount, dot11NonAPStationVideoOctetCount, dot11NonAPStationBestEffortOctetCount, dot11NonAPStationAuthMaxBackgroundOctets, and dot11NonAPStationHCCAHEMMOctetCount is compared to dot11NonAPStationAuthMaxTotalOctets. When the value of the authorized maximum octet count is exceeded, the non-AP STA shall be disassociated.

11.23.5 Interworking Procedures: Emergency Services Support

Emergency Service support provides STAs with the ability to contact authorities, in an emergency situation. The following procedures allow the STA to determine whether emergency services are supported by the AP, and whether un-authenticated emergency service access is allowed.

In an AP, when dot11ESNetwork is set to TRUE, emergency service operation shall be supported. When emergency operation is not supported, dot11ESNetwork shall be set to FALSE.

When the AP is located in a regulatory domain that requires location capabilities, the ESC field shall only be set to 1 if location capability is enabled on the AP. Location capability is enabled when the Civic Location or Geo Location field in the Extended Capabilities Element is set to 1 in a Beacon or probe response frame.

The ESC and UESA fields shall be set as shown in Table 11-5.

Table 11-5—ESC and UESA fields settings

Description	ESC	UESA
Emergency Services are not supported	0	0
Emergency Services are only supported for authenticated STAs	1	0
Not Allowed	0	1
Emergency Services are supported for STAs. For open SSID networks (non-RSN), which support emergency services this option shall be used.	1	1

In addition, the ESC field shall only be set to 1 if both of the following are true (see Annex W.4.2 for further information):

— dot11QosOptionImplemented is true

— dot11EBREnabled is true.

11.23.6 Interworking Procedures: Emergency Alert System (EAS) Support

The Emergency Alert System (EAS) provides alerts, typically issued by authorities. The Interworking Procedures EAS support enables the alerts to be transmitted upon request from APs to non-AP STAs. Subsequent to advertisement in Beacon and Probe Response frames, a non-AP STA uses Native and non-Native GAS queries to retrieve an EAS message from the network according to the following procedures.

When dot11EASEnabled is set to TRUE, EAS operation shall be supported. When EAS operation is not supported, dot11EASEnabled shall be set to FALSE.

When the IEEE 802.11 infrastructure is informed of the availability of an EAS message (the mechanism by which is out of scope of this standard), an AP with dot11EASEnabled set to TRUE shall advertise the availability of the EAS message by including an Emergency Alert Identifier element (see 7.3.2.94) for that message in its Beacon and Probe Response frames. The AP shall include one instance of an Emergency Alert Identifier element in its Beacon and Probe Response frames for each active EAS Message. The Emergency Alert Identifier element provides an Alert Identifier Hash value, a unique indicator of the EAS Message of the alert to the non-AP STA. The Alert Identifier Hash value allows the non-AP STA to determine whether this is a new alert.

NOTE—The same value of hash will be computed by each AP in an ESS and by each AP in different ESSs. Thus a non-AP STA, which can download emergency alert messages when in a pre-associated state, can unambiguously determine that it has already downloaded the message, avoiding unnecessary duplicates.

When an EAS Message has expired (the mechanism by which is out of scope of this standard), an AP with dot11EASEnabled set to TRUE shall remove the corresponding instance of an Emergency Alert Identifier element from its Beacon and Probe Response frames.

The Alert Identifier Hash in the Emergency Alert Identifier element shall be computed using HMAC-SHA1-64 hash algorithm as shown in 7.3.2.94.

Upon receiving an Emergency Alert Identifier element for an EAS Message which has not already been retrieved from the network, a non-AP STA having dot11EASEnabled set to TRUE shall retrieve the Emergency Alert Server URI (see 7.3.4.13) using a Native GAS query according to the procedures in 11.23.2.1. Then the STA shall form the EAS Message URI by concatenating the Emergency Alert Server URI with the hexadecimal numerals of the Alert Identifier Hash converted to UTF-8 encoded characters and the ".xml" file extension.

Example: If the Emergency Alert Server URI is http://eas.server.org, the Alert Identifier Hash is 0x1234567890abcdef, then the EAS Message URI is http://eas.server.org/1234567890abcdef.xml.

A non-AP STA in the un-associated state having dot11EASEnabled set to TRUE shall retrieve the EAS message using non-native GAS procedures defined in 11.23.2.2 with Advertisement Protocol ID set to the value for EAS (see Table 7-43be). A non-AP STA in the associated state having dot11EASEnabled set to TRUE shall retrieve the EAS message using either non-native GAS procedures defined in 11.23.2.2 with Advertisement Protocol ID set to the value for EAS (see Table 7-43be) or HTTP using Internet Protocols (the latter being preferred).

11.23.7 Support for QoS Mapping from External Networks

Maintaining proper end-to-end QoS is an important factor when providing Interworking Service. This is because the external networks may employ different network-layer (Layer 3) QoS practices. For example, the use of a particular differentiated services code point (DSCP) for a given service may be different between different networks. To ensure the proper QoS over-the-air in the IEEE 802.11 infrastructure, the mapping from DSCP to UP for the corresponding network needs to be identified and made known to the STAs. If an inconsistent mapping is used then:

— Admission control at the AP may incorrectly reject a service request, because the non-AP STA used the incorrect UP.

— Non-AP STAs may use the incorrect value for User Priority in TSPEC and TCLAS elements.

— The user may be given a different QoS over the IEEE 802.11 network than expected, e.g., a lower QoS may be provided than the STA expected.

Therefore, APs with dot11QosmapEnabled set to TRUE shall set the QoSMap field in the Extended capabilities element to 1; APs with dot11QoSmapEnabled set to FALSE shall set the QoSMap field in the Extended capabilities element to 0. The AP's SME causes the QoS Map Set to be available to higher layer protocols or applications so they will be able to set the correct priority in an MA-UNITDATA.request primitive.

For frames transmitted by an AP belonging to an admitted TS, the UP obtained from the TS's TCLAS element shall be used instead of the UP derived from the QoS Map Set. For frames transmitted by an AP belonging to an admitted TS not having a TCLAS element, the UP shall be derived from the QoS Map Set.

Non-AP STAs with dot11QosmapEnabled set to TRUE shall set the QoSMap field in the Extended capabilities element to 1. An AP receiving an Association request frame or Reassociation request frame having the QoS Map field in the Extended Capabilities element set to 1 shall include the QoS Map Set element in the corresponding Association response frame or Reassociation response frame as defined in 7.2.3.5 or 7.2.3.7 respectively. Upon receiving the QoS Map Set element, the non-AP STA's SME causes the QoS Map Set to be available to higher layer protocols or applications so they will be able to set the correct priority in an MA-UNITDATA.request primitive.

When the AP's SME detects a change in the QoS mapping information, it shall update the non-AP STA with the new QoS Map Set element. It accomplishes this update by invoking the MLME-QoSMap.response primitive.

When the MAC entity at the non-AP STA receives a QoS Map Configure Action frame from the AP, the MLME shall issue an MLME-QoSMap.confirm primitive to its SME.

When the non-AP STA's SME receives the QoS Map response, it shall make the QoS Map available to higher layers so that in turn, they can invoke the MA-UNITDATA.request with the correct priority.

11A Fast Transition

11A.11 Resource request procedures

11A.11.1 General

11A.11.2 Resource Information Container

Change the seventh paragraph of 11A.11.2 as follows:

For example, when the resource being requested is QoS for downstream traffic, a TSPEC information element~~s~~ may be followed by one or more TCLAS information elements and, when multiple TCLAS information elements are present, a TCLAS Processing element and an Expedited Bandwidth Request (EBR) element. Such an example Resource Request with two alternative TSPECs, the second of which has an EBR, is shown in Figure 11A-24.

Change Table 11A-2 in 11A.11.2 as follows:

Table 11A-2—Resource Types and Resource Descriptor definitions

Resource Type	Resource Description Definition	Notes
802.11 QoS	In a request: TSPEC (see 7.3.2.30), followed by zero or more TCLAS (see 7.3.2.31), followed by zero or one TCLAS Processing (See 7.3.2.33). followed by zero or one Expedited Bandwidth Request elements (see 7.3.2.91). In a response: TSPEC (see 7.3.2.30), followed by zero or one Schedule (See 7.3.2.34)	May be sent by a QoS non-AP STA to a QoS AP. Definition of TSPEC information elements shall be as given in 11.4. Definition of TCLAS, TCLAS Processing, Expedited Bandwidth Request and Schedule information elements, and the rules for including them in requests and responses, shall be as given in 11.4. Resource request procedures shall be as given in 11.4.

Replace Figure 11A-24 in 11A.11.2 with the following figure.

RDIE	TSPEC	TCLAS	TCLAS	TCLAS Processing	TSPEC	TCLAS	TCLAS	TCLAS Processing	EBR

Figure 11A-24—Resource Request example #2

11A.11.3 Creation and handling of a resource request

11A.11.3.1 STA procedures

Change the fifth paragraph of 11A.11.3.1 as follows:

In generating the RDIE for QoS resources for a TS, the procedures of 11.4 shall be followed for the generation of TSPECs and inclusion of TCLAS, ~~and~~ TCLAS Processing, and Expedited Bandwidth Request elements. If the TS is a downstream flow, then the RDIE may also include one or more TCLAS element(s) (defined in 7.3.2.31) ~~and (if multiple TCLAS elements are included)~~ a TCLAS Processing element (defined in 7.3.2.33) if multiple TCLAS elements are included, and an optional Expedited Bandwidth Request (EBR) element, defined in 7.3.2.91. If present, the TCLAS shall appear after the corresponding TSPEC. If present, an EBR element shall appear after the corresponding TSPEC, TCLAS, and TCLAS Processing elements of the TSPEC.

11A.11.3.2 AP procedures

Change the sixth paragraph of 11A.11.3.2 as follows:

If the resource request included QoS resources and is successful, then the procedures for handling of TSPEC, TCLAS, ~~and~~ TCLAS Processing, ~~elements~~ and Expedited Bandwidth Request elements shall be as specified in 11.4, and the AP shall place the Traffic Streams into the “Accepted” state. The RIC-response shall contain the updated accepted TSPEC. Each RDIE may also include a Schedule information element (as defined in

7.3.2.34) after the accepted TSPEC. Upon reassociation, AP shall move all of the Traffic Streams from the "Accepted" state into the "Active" state.

Insert the new clause 11B after 11A as follows:

11B MAC State Generic Convergence Function.

11B.1 Overview of the convergence function

This clause defines the MAC State Generic Convergence Function (MSGCF) and its interaction with other management entities. The MSGCF correlates information exchanged between the MAC management entities regarding the state of an 802.11 interface and converges this information into events and status for consumption by higher layer protocols. Non-AP STAs having dot11MSGCFEnabled set to TRUE shall support the MSGCF procedures in this clause; APs do not support the MSGCF.

This clause defines interactions between the MSGCF and MLME and PLME through the MLME_SAP and PLME_SAP respectively, as well as with the SME via the MSGCF-SME_SAP. The detailed manner in which the SAPs are implemented is not specified within this standard.

The MSGCF operates at the level of an 802.11 ESS, and generates events based on the state of the link between a non-AP STA and an ESS. A non-AP STA that transitions between two APs in the same ESS can operate transparently to the LLC sublayer, and will not change state in the state machine defined within this clause.

11B.2 Convergence function state machine

11B.3.1 Overview of state machine

The convergence function maintains information on the state of the ESS, using the state machine shown in Figure 11B-1. Because Figure 11B-1 is defined in terms of ESS connectivity, it is not affected by changes in association provided that the transition was an intra-ESS transition.

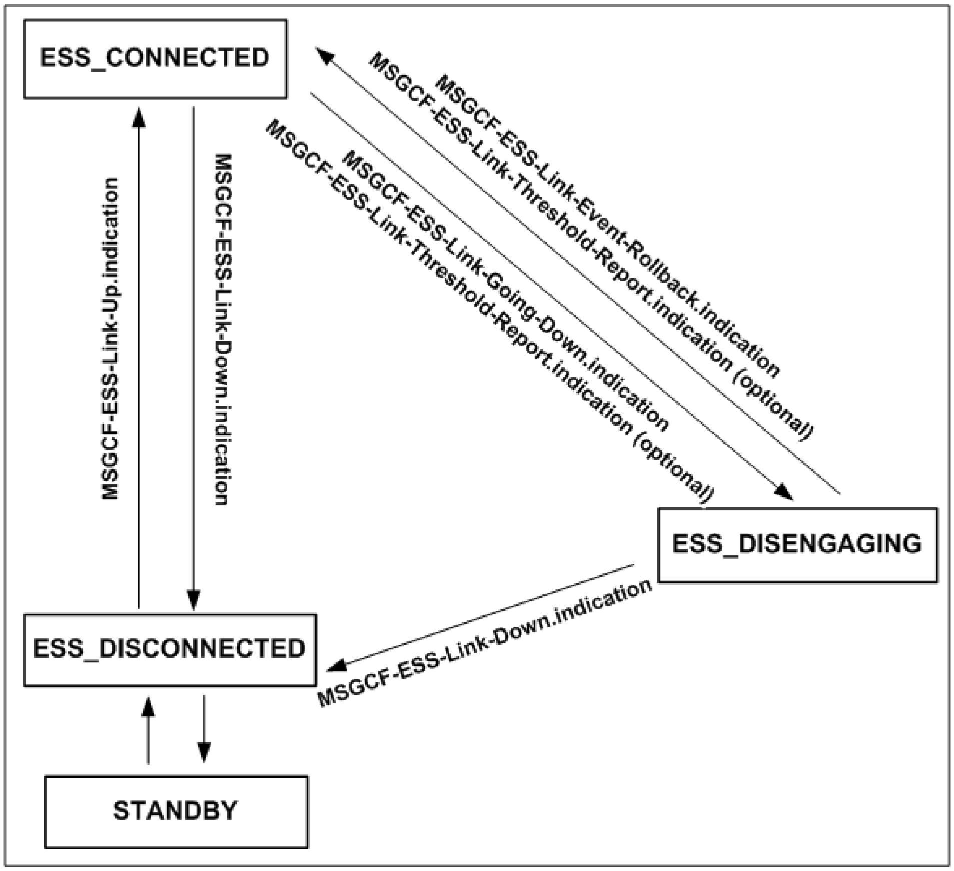
ESS_CONNECTED
MSGCF-ESS-Link-Up.indication
MSGCF-ESS-Link-Down.indication
MSGCF-ESS-Link-Event-Rollback.indication
MSGCF-ESS-Link-Threshold-Report.indication (optional)
MSGCF-ESS-Link-Going-Down.indication
MSGCF-ESS-Link-Threshold-Report.indication (optional)
ESS_DISENGAGING
MSGCF-ESS-Link-Down.indication
ESS_DISCONNECTED
STANDBY

Figure 11B-1—MAC State Generic Convergence Function state machine

11B.3.2 State list

11B.3.2.1 ESS_CONNECTED

In the ESS_CONNECTED state, a non-AP STA has completed all layer 2 setup activities and is able to send Class 3 frames to peer LLC entities. A non-AP STA will be in this state as long as it is possible to send Class 3 frames through any AP within an ESS. A non-AP STA does not leave this state upon successful intra-ESS transitions.

11B.3.2.2 ESS_DISCONNECTED

In the ESS_DISCONNECTED state, a non-AP STA is unable to send Class 3 frames to peer LLC entities. Higher-layer network protocols are unavailable. In this state, a non-AP STA may use the Generic Advertisement Service and Public Action frames to perform network discovery and selection.

11B.3.2.3 ESS_DISENGAGING

In the ESS_DISENGAGING state, the non-AP STA's SME anticipates that links to all APs within the ESS will be lost in a defined time interval, but the non-AP STA is still able to send Class 3 frames to peer LLC entities. The predictive failure of the link may be due to explicit disassociation by the peer, the imminent invalidation of cryptographic keys because of usage limits (such as sequence counter exhaustion), or predictive signal strength algorithms. In this state, it is recommended that a non-AP STA also initiate a search to find a new ESS.

11B.3.2.4 STANDBY

In the STANDBY state, the non-AP STA is powered down and unable to communicate with any other 802.11 STAs.

11B.3.3 State transitions

11B.3.3.1 Transitions to ESS_CONNECTED

11B.3.3.1.1 From ESS_DISCONNECTED

To make this transition, a non-AP STA will have completed the network selection process and the relevant procedures to attach to the ESS, including 802.11 authentication, 802.11 association, and, if required, 802.11 RSN procedures. When this transition is completed, the MSGCF sends an MSGCF-ESS-Link-Up.indication primitive to higher layers.

11B.3.3.1.2 From ESS_DISENGAGING

To make this transition, the SME will cancel a previous event that predicted an ESS link failure. This may be due to network parameters indicating renewed link strength or a successful renewal of an expiring RSN SA. When this transition is complete, the MSGCF sends an MSGCF-ESS-Link-Event-Rollback.indication event to indicate that a prior link failure predictive event is no longer valid. If the transition was due to network parameters crossing a threshold, the MSGCF also issues an MSGCF-ESS-Link-Threshold-Report.indication to higher layers.

11B.3.3.2 Transitions to ESS_ DISCONNECTED

11B.3.3.2.1 From ESS_CONNECTED

This transition indicates that administrative action was taken to shut down the link, a sudden loss of signal strength or that RSN keys expired and could not be renewed. At the conclusion of this transition, the MSGCF issues an MSGCF-ESS-Link-Down.indication event to higher layer protocols.

11B.3.3.2.2 From ESS_DISENGAGING

This transition indicates that the predictive link failure event has occurred. At the conclusion of this transition, the MSGCF issues an MSGCF-ESS-Link-Down.indication event to higher layer protocols.

11B.3.3.2.3 From STANDBY

This transition occurs when the non-AP STA is powered on and initialized. No events are issued by the MSGCF.

11B.3.3.3 Transitions to ESS_DISENGAGING

11B.3.3.3.1 From ESS_CONNECTED

When the network quality parameters degrade or imminent action is taken to bring down the link, the SME may predict an imminent link failure. Upon completion of this transition, the MSGCF issues an MSGCF-ESS-Link-Going-Down event. If the cause of the transition was the degradation of network parameters beyond the thresholds stored in the MIB, an MSGCF-ESS-Link-Threshold-Report.indication is also issued to higher layers.

11B.3.3.4 Transitions to STANDBY

11B.3.3.4.1 From ESS_DISCONNECTED

When the non-AP STA has disconnected from an ESS, it may be administratively powered off to extend battery life. No events are issued by the MSGCF upon completion of this transition.

11B.4 Informational events

Informational events may occur in any state. When they occur, the SME updates the convergence function MIB with new parameters. Informational events do not cause state changes in Figure 11B-1. Informational events are generated when new potential ESS links are discovered, when the network parameter thresholds are set or read, and when higher layer protocols issue commands to the non-AP STA through the MSGCF-ESS-Link-Command.request primitive.

11B.5 MAC state generic convergence SAP

The MAC state generic convergence SAP is the interface between the convergence function and higher layer protocols. It presents a standardized interface for higher layer protocols to access the state of the MAC, whether that state information is available in the MLME, PLME, or SME.

Some events on the MAC state generic convergence SAP require event identifiers for use as a dialog token in event sequencing and rollback. The EventID is an unsigned integer that is initialized to one when the non-AP STA leaves the STANDBY state.

11B.5.1 ESS status reporting

11B.5.1.1 MSGCF-ESS-Link-Up

11B.5.1.1.1 Function

This event is triggered when a new ESS has been made available for sending frames.

11B.5.1.1.2 Semantics of the service primitive

The primitive parameters are as follows:

```
        MSGCF-ESS-Link-Up.indication(
                                        NonAPSTAMacAddress,
                                        ESSIdentifier
                                        )
```

Name	Type	Valid Range	Description
NonAPSTAMacAddress	MAC Address	Any valid individual MAC Address	The MAC address of the non-AP STA that is reporting that an 802.11 ESS has become available.
ESSIdentifier	String	N/A	An identifier for the network, composed of the string value of the SSID information element used to identify the network, concatenated with the value of the HESSID if it is in use. The HESSID is encoded in upper-case ASCII characters with the octet values separated by dash characters, as described in IETF RFC 3580 [B49].

11B.5.1.1.3 When generated

This primitive is generated when the ESS link to a network of APs is available to exchange data frames. The generation of this primitive may vary depending on the contents of dot11WEPDefaultKeysTable and dot11WEPKeyMappingsTable and the setting of dot11RSNAOptionImplemented.

If there are no entries in the dot11WEPDefaultKeysTable, no entry for the current AP in dot11WEPKeyMappingsTable, and dot11RSNAOptionImplemented is set to FALSE, then the network does not use encryption. This event is generated upon receipt of an MLME-Associate.confirm message with a result code of success.

If there are entries in the dot11WEPDefaultKeysTable, or an entry for the current AP in dot11WEPKeyMappingsTable, or dot11RSNAOptionImplemented is set to TRUE, then the network requires the use of encryption on the link. Before declaring that the link is ready to exchange data frames, the convergence function will receive an MLME-Associate.confirm primitive along with an MLME-SetKeys.confirm, both with result codes of success. The latter primitive is used to ensure that a WEP key is available, or that the RSN 4-Way Handshake has completed.

This event is not triggered by MLME-Reassociate.confirm messages because MLME-Reassociate.confirm messages are defined as transitions within the same ESS.

The MLME-Associate.confirm primitive may be issued upon AP transitions. It is the objective of the MAC State Generic Convergence Function to generate this event only upon the initial connection to an 802.11 network, when the MSGCF state machine moves into the ESS_CONNECTED state.

11B.5.1.1.4 Effect of receipt

This event is made available to higher-layer protocols by the convergence function. Actions taken by higher layers are out of the scope of this standard, but may include router discovery, IP configuration, and other higher layer protocol operations.

11B.5.1.2 SGCF-ESS-Link-Down.indication

11B.5.1.2.1 Function

This event is triggered to indicate that an 802.11 ESS is no longer available for sending frames.

11B.5.1.2.2 Semantics of the service primitive

The event's parameters are as follows:

```
MSGCF-ESS-Link-Down.indication (
                    NonAPSTAMacAddress,
                    ESSIdentifier,
                    ReasonCode
                    )
```

Name	Type	Valid Range	Description
NonAPS-TAMacAddress	MAC Address	Any valid individual MAC Address	The MAC address of the non-AP STA that is reporting that an 802.11 ESS is no longer available.
ESSIdentifier	String	N/A	An identifier for the network, composed of the string value of the SSID used to identify the network, concatenated with the value of the HESSID if it is in use.
ReasonCode	Enumerated	EXPLICT_DISCONNECT, KEY_EXPIRATION, LOW_POWER, VENDOR_SPECIFIC	Reason code, drawn from Table 11B.1.

Table 11B.1—Reason codes for Network Down

Name	Description
EXPLICIT_DISCONNECT	An explicit disconnection operation (Disassociation or Deauthentication) was initiated by the non-AP STA or the non-AP STA's current serving AP and the non-AP STA was unable to Reassociate to an alternate AP in the same ESS.
KEY_EXPIRATION	Keys used by an RSN SA have expired due to time or traffic limitations, or TKIP countermeasures have invalidated the key hierarchy.
LOW_POWER	If the SME reports that the 802.11 interface was shut down to conserve power, that event may be reported to higher level protocols.
VENDOR_SPECIFIC	Vendor specific usage.

11B.5.1.2.3 When generated

This event is generated when the SME declares that connectivity to an ESS is lost. It may be generated in the case of an explicit disconnection from the link peer, received as an MLME-Deauthenticate.indication or an MLME-Diassociate.indication primitive message. When dot11RSNAProtectedManagementFramesEnabled is set to TRUE, this event is only generated if the disconnect messages successfully pass IGTK authentication. The SME should wait for a period of dot11ESSDisconnectFilterInterval before declaring connectivity lost to ensure that a non-AP STA is unable to reassociate to any alternate AP within the ESS.

11B.5.1.2.4 Effect of receipt

This event is made available to higher-layer protocols by the convergence function. Actions taken by those higher layers are out of the scope of this standard, but may include removing entries from routing and forwarding, and attempting to initiate handover of open application connections to network interfaces which are still active.

11B.5.1.3 MSGCF-ESS-Link-Going-Down

11B.5.1.3.1 Function

This event is triggered to indicate the expectation that 802.11 ESS will no longer be available for sending frames in the near future.

11B.5.1.3.2 Semantics of the service primitive

The event parameters are as follows:

```
        MSGCF-ESS-Link-Going-Down.indication (
                                NonAPSTAMacAddress,
                                ESSIdentifier,
                                EventID,
                                TimeInterval,
                                ReasonCode
                                )
```

Name	Type	Valid Range	Description
NonAPSTAMac-Address	MacAddress	Any valid individual MAC Address	The MAC address of the non-AP STA that is reporting that an 802.11 ESS is expected to go down.
ESSIdentifier	String	N/A	An identifier for the network, composed of the string value of the SSID information element used to identify the network, concatenated with the value of the HESSID if it is in use.
EventID	Integer	N/A	A string used to identify the event that is used in the case of event rollback.
TimeInterval	Integer	N/A	Time Interval in time units which the link is expected to go down. Connectivity is expected to be available at least for time specified by TimeInterval.
Reason Code	Enumerated	EXPLICT_DISCONNECT, KEY_EXPIRATION, LOW_POWER, VENDOR_SPECIFIC	Indicates the reason the link is expected to go down, drawn from Table 11B.1.

11B.5.1.3.3 When generated

This notification is generated by the MSGCF when the 802.11 ESS link is currently established and is expected to go down within the specified time interval. The network may be expected to go down because of an event whose timing is well understood, such as an explicit disconnection event observed on the MLME_SAP.

Table 11B-1—Reason codes for ESS Link Going-Down

Name	Description
EXPLICIT_DISCONNECT	An explicit disconnection operation (Disassociation or Deauthentication) was initiated by the non-AP STA or the non-AP STA's current serving AP.
KEY_EXPIRATION	Keys used by an RSN SA have expired due to time or traffic limitations, or TKIP countermeasures have invalidated the key hierarchy.
LOW_POWER	If the SME reports that the 802.11 interface will be shut down to conserve power, that event may be reported to higher level protocols.
VENDOR_SPECIFIC	Vendor specific usage.

It may also be expected as the result of a predictive algorithm that monitors link quality. The details of such a predictive algorithm used are beyond the scope of this standard.

The convergence function should attempt to deliver this event at least dot11ESSLinkDownTimeInterval time units before the link is predicted to go down. Different higher layer network protocols may require different levels of advance notice, and may configure the dot11ESSLinkDownTimeInterval attribute accordingly.

Not all thresholds in the dot11MACStateParameterTable are supported by every PHY. In the case where a threshold parameter is not supported (e.g., RSSI in clause 16), it is not applied.

11B.5.1.3.4 Effect of receipt

This event is made available to higher-layer protocols by the convergence function. Actions taken by those higher layers are out of the scope of this standard, but may include beginning preparations for handover.

11B.5.1.4 MSGCF-ESS-Link-Event-Rollback.indication

11B.5.1.4.1 Function

This event is used to indicate that specific previous reports or events are no longer valid and should be disregarded.

11B.5.1.4.2 Semantics of the service primitive

The event parameters are as follows:

```
        MSGCF-ESS-Link-Event-Rollback.indication (
                         NonAPSTAMacAddress,
                         ESSIdentifier,
                         EventID
                         )
```

Name	Type	Valid Range	Description
NonAPSTAMacAddress	MacAddress	Any valid individual MAC Address	The MAC address of the non-AP STA that is reporting that a previous event relating to an 802.11 ESS is no longer valid.
ESSIdentifier	String	N/A	An identifier for the network, composed of the string value of the SSID information element used to identify the network, concatenated with the value of the HESSID if it is in use.
EventID	Integer	N/A	A string used to identify the event that is used in the case of event rollback.

11B.5.1.4.3 When generated

This event is generated when a previous predictive event is no longer valid within its expiration time.

MSGCF-ESS-Link-Event-Rollback.indication is used in conjunction with MSGCF-ESS-Link-Going-Down. MSGCF-ESS-Link-Event-Rollback.indication events are issued when the prediction of link failure is no longer valid. Algorithms used to determine that link failure predictions are beyond the scope of this standard.

11B.5.1.4.4 Effect of receipt

This event is made available to higher-layer protocols by the convergence function to cancel any actions begun by the previous event. Actions taken by those higher layers are out of the scope of this standard, but may include cancelling any handover procedures started by the MSGCF-ESS-Link-Going-Down event.

11B.5.1.5 MSGCF-ESS-Link-Detected.indication

11B.5.1.5.1 Function

This event reports on the presence of a new 802.11 ESS.

11B.5.1.5.2 Semantics of the service primitive

The primitive parameters are as follows:

```
        MSGCF-ESS-Link-Detected.indication (
                                        NonAPSTAMacAddress,
                                        ESSIdentifier,
                                        ESSDescription
                                        )
```

Name	Type	Valid Range	Description
NonAPSTAMacAddress	MacAddress	Any valid individual MAC Address	The MAC address of the non-AP STA that is reporting the new network.
ESSIdentifier	String	N/A	An identifier for the network, composed of the string value of the SSID used to identify the network, concatenated with the value of the HESSID if it is in use.
ESSDescription	As defined in Table 11B-2	N/A	A set of information about the ESS.

Table 11B-2—ESS Description

Name	Syntax	Description
SSID	String	The SSID used by the ESS.
InformationServiceSupport	As described in Table 11B-3	A set of values indicating the type of information services supported on this network.
TriggerSupport	As described in Table 11B-3	A set of values indicating the support for the types of triggers that can be used to propose that the station take action.
RSN	As defined in 7.3.2.25	The RSN configuration of the ESS.
Interworking	As defined in 7.3.2.89	Interworking configuration of the ESS.

Table 11B-3—Trigger Support Values

Name	Description
MIH_CS_ES_Support	This network supports the 802.21 MIH Command Service (CS) and Event Service (ES).
Vendor_Specific_Trigger_Support	This network supports a vendor-specific trigger service.

11B.5.1.5.3 When generated

To maintain the list of detected networks, the SME issues recurring MLME-SCAN.request primitives to the MLME. The SME may schedule these requests to avoid interruption of user traffic. Responses to these requests, received in the MLME-SCAN.confirm primitives, contain a list of detected networks. Each network is stored in the MIB in the dot11MACStateESSLinkDetectedTable. This table holds a list of networks, organized by Network Identifier. Each entry in the table contains a list of BSSIDs within the network, as well as indications of support for media independent handover. Support for media independent handover is indicated by the presence or absence of the relevant GAS Advertisement Protocol IDs in the Interworking information element. Each entry in the table will be held for at least dot11ESSLinkDetectionHoldInterval time units. When a non-AP STA has not observed an ESS for longer than dot11ESSLinkDetectionHoldInterval, it may be removed from the table.

This event is generated when a new entry is made into the dot11MACStateESSLinkDetectedTable. Modifications to existing entries in the list, such as an update to the BSSID list, do not trigger this event.

11B.5.1.5.4 Effect of receipt

This event is made available to higher-layer protocols by the convergence function. Actions taken by those higher layers are out of the scope of this standard.

11B.5.1.6 MSGCF-ESS-Link-Scan.request

11B.5.1.6.1 Function

This function is used by higher layer protocols to request that the SME perform a scan operation for available ESSs.

11B.5.1.6.2 Semantics of the service primitive

The primitive parameters are as follows:

```
          MSGCF-ESS-Link-Scan.request (
                                        SSID,
                                        HESSID,
                                        NetworkType
                                        )
```

Name	Type	Valid Range	Description
SSID	Octet string	0-32 octets	Specific or wildcard.
HESSID	As defined in 7.3.2.89	As defined in 7.3.2.89	The HESSID to search for. It can be set to all 1's for use as a wildcard to match all available HESSID values.
NetworkType	As defined in 7.3.2.89	As defined in 7.3.2.89	This may be a specific value to match one type of networks, or all 1's to match all network types.

11B.5.1.6.3 When generated

This request is generated when higher protocol layers request a list of available ESSs.

11B.5.1.6.4 Effect of receipt

The SME will generate a corresponding MLME-SCAN.request primitive to find available networks.

11B.5.1.7 MSGCF-ESS-Link-Scan.confirm

11B.5.1.7.1 Function

This function reports information on available ESSs to higher protocol layers.

11B.5.1.7.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MSGCF-ESS-Link-Scan.confirm (
                              NonAPSTAMacAddress,
                              ESSIdentifiers,
                              ESSDescriptions
                              )
```

Name	Type	Valid Range	Description
NonAPSTAMacAddress	MacAddress	Any valid individual MAC Address	The MAC address of the non-AP STA that is reporting the new network.
ESSIdentifiers	Set of Strings	N/A	An identifier for the network composed of the string value of the SSID used to identify the network, concatenated with the value of the HESSID if it is in use.
ESSDescriptions	Set of ESSDescriptions, as defined in Table 11B-2	N/A	A set of information about each discovered ESS.

11B.5.1.7.3 When generated

This primitive is generated when scan results are available for reporting to higher protocol layers, in response to an MSGCF-ESS-Link-Scan.request primitive.

11B.5.1.7.4 Effect of receipt

This event is made available to higher-layer protocols by the convergence function. Actions taken by those higher layers are out of the scope of this standard.

11B.5.2 Network configuration

11B.5.2.1 MSGCF-ESS-Link-Capability.request

11B.5.2.1.1 Function

This primitive requests a list of the capabilities supported by a network.

11B.5.2.1.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MSGCF-ESS-Link-Capability.request (
                              NonAPSTAMacAddress,
                              ESSIdentifier
                              )
```

Name	Type	Valid Range	Description
NonAPSTAMac-Address	MacAddress	Any valid individual MAC Address	The MAC address of the non-AP STA that is reporting the new network.
ESSIdentifier	String	N/A	An identifier for the network, composed of the string value of the SSID information element used to identify the network, concatenated with the value of the HESSID if it is in use.

11B.5.2.1.3 When generated

This primitive is issued to service higher layer protocols by reporting on the capabilities of a particular network.

11B.5.2.1.4 Effect of receipt

The convergence function retrieves the capabilities and reports them via the MSGCF-ESS-Link-Capability.confirm primitive.

11B.5.2.2 MSGCF-ESS-Link-Capability.confirm

11B.5.2.2.1 Function

This primitive reports the convergence function capabilities of the network to higher layer protocols.

11B.5.2.2.2 Semantics of the service primitive

The primitive parameters are as follows:

```
        MSGCF-ESS-Link-Capability.confirm (
                                          NonAPSTAMacAddress,
                                          ESSIdentifier,
                                          EssLinkParameterSet,
                                          ReasonCode
                                          )
```

Name	Type	Valid Range	Description
NonAPSTAMac-Address	MacAddress	Any valid individual MAC Address	The MAC address of the non-AP STA that is reporting the new network.
ESSIdentifier	String	N/A	An identifier for the network, composed of the string value of the SSID information element used to identify the network, concatenated with the value of the HESSID if it is in use.
EventCapability-Set	As defined in Table 11B-4	N/A	List of supported events.
ReasonCode	Enumerated	SUCCESS, UNKNOWN_NETWORK, UNKNOWN_CAPABILITIES	An error code, if applicable.

Table 11B-4—Event Capability Set

Name	Type	Valid Range	Description
NonAPSTAMacAddress	MacAddress	Any valid individual MAC Address	The MAC address of the non-AP STA that is reporting the new network.
ESSIdentifier	String	N/A	An identifier for the network, composed of the string value of the SSID information element used to identify the network, concatenated with the value of the HESSID if it is in use.
ESS-Link-Up	Boolean	true, false	indicates whether the MSGCF-ESS-Link-Up.indication event as defined in 11B.5.1.1 is supported.
ESS-Link-Down	Boolean	true, false	Indicates whether the MSGCF-ESS-Link-Down.indication event as defined in 11B.5.1.2 is supported.
ESS-Link-Going-Down	Boolean	true, false	Indicates whether the MSGCF-ESS-Link-Going-Down event as defined in 11B.5.1.3 is supported.
ESS-Link-Event-Rollback	Boolean	true, false	Indicates whether the MSGCF-ESS-Link-Event-Rollback.indication event as defined in 11B.5.1.4 is supported.
ESS-Link-Detected	Boolean	true, false	Indicates whether the MSGCF-ESS-Link-Detected.indication event as defined in 11B.5.1.5 is supported.
ESS-Link-Threshold-Report	Boolean	true, false	Indicates whether the MSGCF-ESS-Link-Threshold-Report.indication event as defined in 11B.5.3.1 is supported.
ESS-Link-Command	Boolean	true, false	Indicates whether the MSGCF-ESS-Link-Command.request primitive as defined in 11B.5.4.1 is supported.

11B.5.2.2.3 When generated

This primitive is generated in response to the MSGCF-ESS-Link-Capability.request primitive to report whether or not specific events are supported.

11B.5.2.2.4 Effect of receipt

This event is made available to higher-layer protocols by the convergence function.

11B.5.2.3 MSGCF-Set-ESS-Link-Parameters.request

11B.5.2.3.1 Function

This primitive sets thresholds for reporting of network events.

11B.5.2.3.2 Semantics of the service primitive

The primitive parameters are as follows:

```
        MSGCF-Set-ESS-Link-Parameters.request (
                                              NonAPSTAMacAddress,
                                              ESSIdentifier,
                                              EssLinkParameterSet
                                              )
```

Name	Type	Valid Range	Description
NonAPSTAMacAddress	MacAddress	Any valid individual MAC Address	The MAC address of the non-AP STA that is reporting the new network.
ESSIdentifier	String	N/A	An identifier for the network, composed of the string value of the SSID information element used to identify the network, concatenated with the value of the HESSID if it is in use.
ESSLinkParameterSet	As defined in Table 11B-5	N/A	The EssLinkParameterSet is used to configure when event reports will be sent to higher protocol layers.

The ESSLinkParameterSet is defined in Table 11B-5. It may include any or all of the elements in Table 11B-5.

Table 11B-5—ESS Link Parameter Set

Name	Type	Valid Range	Description
PeakOperational-Rate	Integer	As defined in 7.3.2.2	The integer representing the desired peak modulation data rate used for data frame transmission.
MinimumOpera-tionalRate	Integer	As defined in 7.3.2.2	The integer encoding of the desired minimum modulation data rate used in data frame transmission
NetworkDown-timeInterval	Integer	N/A	Desired advance warning time interval for MSGCF-ESS-Link-Going-Down events.
DataFrameRSSI	Integer	-100 to 40	The received signal strength in dBm of received Data frames from the network. This may be time-averaged over recent history by a vendor-specific smoothing function.
BeaconRSSI	Integer	-100 to 40	The received signal strength in dBm of Beacon frames received on the channel. This may be time-averaged over recent history by a vendor-specific smoothing function.
BeaconSNR	Integer	0-100	The signal to noise ratio of the received data frames, in dB. This may be time-averaged over recent history by a vendor-specific smoothing function.
DataFrameSNR	Integer	0-100	The signal to noise ratio of the received Beacon frames, in dB. This may be time-averaged over recent history by a vendor-specific smoothing function.
DataThroughput	Real	N/A	The data throughput in megabits per second, rounded to the nearest megabit. This may be time-averaged over recent history by a vendor-specific smoothing function.
FrameErrorRate	Real	N/A	The frame error rate of the network. This may be time-averaged over recent history by a vendor-specific smoothing function.
VendorSpecifc	Vendor Specific	As defined by 7.3.2.26	Additional vendor-specific parameters may be included in this event.

11B.5.2.3.3 When Generated

This event is generated when higher protocol layers wish to set the performance parameters for a network. Higher protocol layers are responsible for ensuring that the set of configured network parameters is consistent with all subscribers to those higher layer protocols.

11B.5.2.3.4 Effect of receipt

Parameters supplied in the event are stored in the MIB, either in the dot11MACStateConfigTable or the dot11MACStateParameterTable.

11B.5.2.4 MSGCF-Set-ESS-Link-Parameters.confirm

11B.5.2.4.1 Function

This primitive indicates whether network parameters were accepted.

11B.5.2.4.2 Semantics of the service primitive

The primitive parameters are as follows:

```
        MSGCF-Set-ESS-Link-Parameters.confirm (
                                  NonAPStaMacAddress,
                                  ESSIdentifier,
                                  EssLinkParameterSet,
                                  ResultCode
                                  )
```

Name	Type	Valid Range	Description
NonAPSTAMacAddress	MacAddress	Any valid individual MAC Address	The MAC address of the non-AP STA that is reporting the new network.
ESSIdentifier	String	N/A	An identifier for the network, composed of the string value of the SSID information element used to identify the network, concatenated with the value of the HESSID if it is in use.
EssLinkParameterSet	As defined in Table 11B-5	N/A	The EssLinkParameterSet is used to configure when event reports will be sent to higher protocol layers.
ResultCode	Enumeration	SUCCESS, INVALID_PARAMETERS	The result code of the parameter set operation.

11B.5.2.4.3 When generated

This primitive is generated in response to the MSGCF-Set-ESS-Link-Parameters.request primitive and is used to indicate whether the parameter set was accepted.

11B.5.2.4.4 Effect of receipt

The SME is notified of the new parameter set.

11B.5.2.5 MSGCF-Get-ESS-Link-Parameters.request

11B.5.2.5.1 Function

This primitive retrieves the current network parameters for a specific network

11B.5.2.5.2 Semantics of the service primitive

The primitive parameters are as follows:

```
        MSGCF-Get-ESS-Link-Parameters.request (
                                  ESSIdentifier
                                  )
```

Name	Type	Valid Range	Description
ESSIdentifier	String	N/A	An identifier for the network, composed of the string value of the SSID information element used to identify the network, concatenated with the value of the HESSID if it is in use.

11B.5.2.5.3 When generated

This primitive is used by higher layers to retrieve the currently stored parameters for a network.

11B.5.2.5.4 Effect of receipt

The SME retrieves the network parameters and makes them available through the MSGCF-Get-ESS-Link-Parameters.confirm primitive.

11B.5.2.6 MSGCF-Get-ESS-Link-Parameters.confirm

11B.5.2.6.1 Function

This primitive reports the current network parameters.

11B.5.2.6.2 Semantics of the service primitive

The primitive parameters are as follows:

```
        MSGCF-Set-ESS-Link-Parameters.confirm (
                                    ESSIdentifier,
                                    EssLinkParameterSet,
                                    ResultCode
                                    )
```

Name	Type	Valid Range	Description
ESSIdentifier	String	N/A	An identifier for the network, composed of the string value of the SSID information element used to identify the network, concatenated with the value of the HESSID if it is in use.
EssLinkParameterSet	As defined 11B.5.2.3	N/A	The EssLinkParameterSet is used to configure when event reports will be sent to higher protocol layers.
ResultCode	Enumeration	SUCCESS, INVALID_PARAMETERS	The result code of the parameter set operation.

11B.5.2.6.3 When generated

This primitive is generated by the MSGCF as a result of the MSGCF-Get-ESS-Link-Parameters.request primitive.

11B.5.2.6.4 Effect of receipt

The higher layer protocols are notified of the current network parameters.

11B.5.3 Network events

11B.5.3.1 to MSGCF-ESS-Link-Threshold-Report.indication

11B.5.3.1.1 Function

This event reports that the layer 2 network performance has crossed a threshold set by the operations described in Table 11B-3.

11B.5.3.1.2 Semantics of the service primitive

The primitive parameters are as follows:

```
        MSGCF-ESS-Link-Threshold-Report.indication (
                                        NonAPSTAMacAddress,
                                        ESSIdentifier,
                                        EssLinkParameterSet,
                                        ThresholdCrossingDirectionSet
                                        )
```

Name	Type	Valid Range	Description
NonAPSTAMacAddress	MacAddress	Any valid individual MAC Address	The MAC address of the non-AP STA that is reporting the threshold crossing.
ESSIdentifier	String	N/A	An identifier for the network, composed of the string value of the SSID information element used to identify the network, concatenated with the value of the HESSID if it is in use.
EssLinkParameterSet	As defined in Table 11B-4	N/A	List of EssLinkParameterSets and their current values that have crossed pre-set thresholds for alerts.
ThresholdCrossingDirectionSet	Set of ThresholdCrossingDirections, one for each value in the EssLinkParameterSet	UPWARD, DOWNWARD	Whether the parameter has crossed the threshold while rising or falling.

11B.5.3.1.3 When generated

The convergence function is responsible for monitoring network performance. If the monitored parameters cross the configured threshold, this event is generated to inform higher-layer protocols.

11B.5.3.1.4 Effect of receipt

This event is made available to higher-layer protocols by the convergence function. Actions taken by those higher layers are out of the scope of this standard, but may include preparations for handover or assessing whether handover should be imminent.

11B.5.4 Network command interface

11B.5.4.1 MSGCF-ESS-Link-Command.request

11B.5.4.1.1 Function

This primitive requests that a STA take action for a network.

11B.5.4.1.2 Semantics of the service primitive

```
MSGCF-ESS-Link-Command.request (
                                NonAPSTAMacAddress,
                                ESSIdentifier,
                                CommandType
                                )
```

Name	Type	Valid Range	Description
NonAPSTAMacAddress	MacAddress	Any valid individual MAC Address	The MAC address of the non-AP STA that is reporting the threshold crossing.
ESSIdentifier	String	N/A	An identifier for the network, composed of the string value of the SSID information element used to identify the network, concatenated with the value of the HESSID if it is in use.
CommandType	Enumerated	DISCONNECT, LOW_POWER, POWER_UP, POWER_DOWN, SCAN	Type of command to perform on the link as described in the following subclauses.

11B.5.4.1.3 When generated

This primitive is generated by a higher layer protocol.

11B.5.4.1.4 Effect of receipt

The convergence function will issue commands to the SME to implement the requested action on behalf of higher layers.

When the DISCONNECT command type is specified, the higher layer is requesting that the STA disconnect from its peer. When the SME on a non-AP STA receives this command, the SME issues an MLME-Deauthenticate.request to disconnect from the network, and the SME refrains from reconnecting to that network. When this command is issued on an AP, the AP issues an MLME-Disassociate.request to disconnect the specified non-AP STA from the specified ESS.

When the POWER_DOWN command type is specified, the SME will power down the non-AP STA. Before doing so, it may choose to notify the AP. This command is not valid on an AP STA.

When the POWER_UP command type is specified, the SME will start the non-AP STA.

When the LOW_POWER command type is specified, the higher layer is requesting that the 802.11 interface be placed in a low power mode. This action is accomplished by issuing an MLME-POWERMGT.request primitive with the PowerManagementMode parameter set to POWER_SAVE.

When the SCAN command type is specified, the higher layer is requesting that the STA search for 802.11 networks. This action is accomplished by issuing an MLME-SCAN.request primitive. Detected networks will be made available in the dot11MACStateESSLinkDetectedTable, as well as through the MSGCF-ESS-Link-Detected.indication event.

11B.6 MAC State SME ME SAP

11B.6.1 Mobility Management

11B.6.1.1 MSSME-ESS-Link-Down-Predicted.indication

11B.6.1.1.1 Function

This primitive indicates that the SME is predicting a link failure.

11B.6.1.1.2 Semantics of the service primitive

The primitive parameters are as follows:

```
      MSSME-ESS-Link-Going-Down.indication (
                                    NonAPSTAMacAddress,
                                    ESSIdentifier,
                                    TimeInterval,
                                    ReasonCode
                                    )
```

Name	Type	Valid Range	Description
NonAPSTAMacAddress	MacAddress	Any valid individual MAC Address	The MAC address of the non-AP STA that is reporting that an 802.11 ESS is expected to go down.
ESSIdentifier	String	N/A	An identifier for the network, composed of the string value of the SSID information element used to identify the network, concatenated with the value of the HESSID if it is in use.
TimeInterval	Integer	N/A	Time Interval in time units which the link is expected to go down. Connectivity is expected to be available at least for time specified by *TimeInterval*.
Reason Code	Enumerated	EXPLICIT_DISCONNECT, LINK_PARAMETER_DEGRADATION, KEY_EXPIRATION, LOW_POWER, QOS_UNAVAILABLE, VENDOR_SPECIFIC	Indicates the reason the link is expected to go down.

11B.6.1.1.3 When generated

This notification is generated by the SME when the 802.11 network connection is currently established and is expected to go down. The details of the predictive algorithm used are beyond the scope of this standard. One method of implementing this function would be to generate this indication when link quality is fading and no better AP can be found.

11B.6.1.1.4 Effect of receipt

This indication is received by the MAC State Generic Convergence function and is used to generate the MS-GCF-ESS-Link-Down.indication event due to link parameter degradation.

Annex A

(normative)

Protocol Implementation Conformance Statement (PICS) Proforma

A.2.1 Abbreviations and special symbols

A.2.2 General abbreviations for Item and Support columns

Insert a new item at the end of A.2.2 list.

IW	Interworking with External Networks

A.4 PICS proforma–IEEE Std. 802.11, 2007

A.4.3 IUT configuration

Insert the following entry to the end of the IUT configuration table:

Item	IUT configuration	References	Status	Support
*CF18	Is Interworking with External Networks Service supported?	Extended Capabilities 7.3.2.27	(CF 15, CF8 & CF11):O	Yes, No

Insert A.4.21 after A.4.21 as following:

A.4.22 Interworking (IW) with External Networks extensions

Item	Protocol Capability	References	Status	Support
	Are the following Interworking with External Networks capabilities supported?			
IW1	Interworking capabilities and Information	7.3.2.89, 11.23.1	CF18:M	Yes, No, N/A
IW1.1	Interworking information element	7.3.2.89	CF18:M	Yes, No, N/A
IW1.2	Network Type	7.3.2.89	CF18:M	Yes, No, N/A
IW1.3	802.11 Venue Type	7.3.2.90	CF18:M	Yes, No, N/A
IW1.4	HESSID	7.3.2.89	CF18:M	Yes, No, N/A
IW1.5	Interworking Action frame	7.4.7a	CF18:M	Yes, No, N/A
IW2	Generic Advertisement Services	11.23.2	CF18:M	Yes, No, N/A
IW2.1	Advertisement Protocol element	7.3.2.90	CF18:M	Yes, No, N/A
IW2.2	Native GAS Protocol	11.23.2.1	CF18:M	Yes, No, N/A
IW2.3	Non-Native GAS Protocol	11.23.2.2	CF18:O	Yes, No, N/A
IW2.3.1	MIH IS	7.3.2.90	CF18:O	Yes, No, N/A
IW2.3.2	MIH ES & CS Discovery	7.3.2.90	CF18:O	Yes, No, N/A
IW2.3.3	EAS	7.3.2.90, 7.3.2.94	CF18:O	Yes, No, N/A
IW2.3.4	Native GAS Vendor Specific	7.3.2.90	CF18:O	Yes, No, N/A
IW2.4	Native Query Protocol	7.3.4, 7.3.4.6	CF18:M	Yes, No, N/A
IW2.5	GAS Initial Request Action frame	7.4.7.14	CF18:M	Yes, No, N/A
IW2.6	GAS Initial Response Action frame	7.4.7.15	CF18:M	Yes, No, N/A
IW2.7	GAS Comeback Request Action frame	7.4.7.16	CF18:M	Yes, No, N/A
IW2.8	GAS Comeback Response Action frame	7.4.7.17	CF18:M	Yes, No, N/A
IW3	QoS Mapping from External Networks	11.23.7 9.9.3.1, 9.9.3.2	CF18:O	Yes, No, N/A
IW3.1	QoS Map Set element	7.3.2.92	CF18:M	Yes, No, N/A
IW3.2	Transport of QoS Map Set	11.23.7	CF18:M	Yes, No, N/A
IW3.3	QoS Map Configure	7.4.2.5	CF18:M	Yes, No, N/A
IW4	MIH Support	11B, 11.23.4	CF18:O	Yes, No, N/A
IW4.1	MAC State Generic Convergence Function Support	11B	CF18:M	Yes, No, N/A
IW4.2	Informational events	11B.4	CF18:M	Yes, No, N/A

Item	Protocol Capability	References	Status	Support
IW4.3	ESS status reporting	11B.5.1	CF18:M	Yes, No, N/A
IW4.4	Network configuration	11B.5.2	CF18:M	Yes, No, N/A
IW4.5	Network events	11B.5.3	CF18:M	Yes, No, N/A
IW4.6	Network command interface	11B.5.4	CF18:M	Yes, No, N/A
IW4.7	Mobility management	11B.6.1	CF18:M	Yes, No, N/A
IW4.8	Network configuration	11B.5.2	CF18:M	Yes, No, N/A
IW5	Extended channel switch enabled	7.3.2.58, 11.1.3	(CF15 AND DSE9):M	Yes, No, N/A
IW6	Expedited Bandwidth Request	7.3.2.91	CF18:O	Yes, No, N/A
IW7	SSPN Interface	11.23.4	CF18:O	Yes, No, N/A

Annex D

Change the dot11StationConfigEntry list in Annex D by inserting the shown entries:

```
Dot11StationConfigEntry::=
          SEQUENCE {
          dot11StationID                            MacAddress,
          dot11MediumOccupancyLimit                 INTEGER,
          dot11CFPollable                           TruthValue,
          dot11CFPPeriod                            INTEGER,
          dot11CFPMaxDuration                       INTEGER,
          dot11AuthenticationResponseTimeOut        Unsigned32,
          dot11PrivacyOptionImplemented             TruthValue,
          dot11PowerManagementMode                  INTEGER,
          dot11DesiredSSID                          OCTET STRING,
          dot11DesiredBSSType                       INTEGER,
          dot11OperationalRateSet                   OCTET STRING,
          dot11BeaconPeriod                         INTEGER,
          dot11DTIMPeriod                           INTEGER,
          dot11AssociationResponseTimeOut           Unsigned32,
          dot11DisassociateReason                   INTEGER,
          dot11DisassociateStation                  MacAddress,
          dot11DeauthenticateReason                 INTEGER,
          dot11DeauthenticateStation                MacAddress,
          dot11AuthenticateFailStatus               INTEGER,
          dot11AuthenticateFailStation              MacAddress,
          dot11MultiDomainCapabilityImplemented     TruthValue,
          dot11MultiDomainCapabilityEnabled         TruthValue,
          dot11CountryString                        OCTET STRING,
          dot11SpectrumManagementImplemented        TruthValue,
          dot11SpectrumManagementRequired           TruthValue,
          dot11RSNAOptionImplemented                TruthValue,
          dot11RSNAPreauthenticationImplemented     TruthValue,
          dot11RegulatoryClassesImplemented         TruthValue,
          dot11RegulatoryClassesRequired            TruthValue,
          dot11QosOptionImplemented                 TruthValue,
          dot11ImmediateBlockAckOptionImplemented   TruthValue,
          dot11DelayedBlockAckOptionImplemented     TruthValue,
          dot11DirectOptionImplemented              TruthValue,
          dot11APSDOptionImplemented                TruthValue,
          dot11QAckOptionImplemented                TruthValue,
          dot11QBSSLoadOptionImplemented            TruthValue,
          dot11QueueRequestOptionImplemented        TruthValue,
          dot11TXOPRequestOptionImplemented         TruthValue,
          dot11MoreDataAckOptionImplemented         TruthValue,
          dot11AssociateinNQBSS                     TruthValue,
          dot11DLSAllowedInQBSS                     TruthValue,
          dot11DLSAllowed                           TruthValue,
          dot11AssociateStation                     MacAddress,
          dot11AssociateID                          INTEGER,
          dot11AssociateFailStation                 MacAddress,
          dot11AssociateFailStatus                  INTEGER,
          dot11ReassociateStation                   MacAddress,
          dot11ReassociateID                        INTEGER,
          dot11ReassociateFailStation               MacAddress,
          dot11ReassociateFailStatus                INTEGER,
          dot11RadioMeasurementCapable              TruthValue,
          dot11RadioMeasurementEnabled              TruthValue,
          dot11RadioMeasurementProbeDelay           INTEGER,
          dot11MeasurementPilotReceptionEnabled     TruthValue,
          dot11MeasurementPilotTransmissionEnabled  TruthValue,
          dot11MeasurementPilotTransmissionVirtualApSetEnabled TruthValue,
          dot11MeasurementPilotPeriod               INTEGER,
          dot11LinkMeasurementEnabled               TruthValue,
          dot11NeighborReportEnabled                TruthValue,
          dot11ParallelMeasurementsEnabled          TruthValue,
          dot11TriggeredMeasurementsEnabled         TruthValue,
          dot11RepeatedMeasurementsEnabled          TruthValue,
          dot11MeasurementPauseEnabled              TruthValue,
          dot11QuietIntervalEnabled                 TruthValue,
          dot11PassiveBeaconMeasurementEnabled      TruthValue,
          dot11ActiveBeaconMeasurementEnabled       TruthValue,
          dot11TableBeaconMeasurementEnabled        TruthValue,
          dot11ReportingConditionsEnabled           TruthValue,
          dot11FrameMeasurementEnabled              TruthValue,
          dot11ChannelLoadEnabled                   TruthValue,
          dot11NoiseHistogramEnabled                TruthValue,
          dot11StatisticsReportEnabled              TruthValue,
          dot11LCIReportEnabled                     TruthValue,
          dot11TransmitStreamMeasurementEnabled     TruthValue,
          dot11APChannelReportEnabled               TruthValue,
          dot11AnnexQMIBSupportEnabled              TruthValue,
          dot11NonOperatingChannelMeasurementsEnabled TruthValue,
          dot11MaximumMeasurementDuration           Unsigned32,
          dot11MeasurementPilotSupport              Unsigned32,
          dot11FastBSSTransitionImplemented         TruthValue,
          dot11LCIDSEImplemented                    TruthValue,
          dot11LCIDSERequired                       TruthValue,
          dot11DSERequired                          TruthValue,
          dot11ExtendedChannelSwitchEnabled         TruthValue,
          dot11HighThroughputOptionImplemented      TruthValue,
          dot11WirelessManagementImplemented        TruthValue,
          dot11MaxIdlePeriod                        INTEGER,
          dot11TIMBroadcastInterval                 INTEGER,
          dot11TIMBroadcastOffset                   INTEGER,
          dot11MinTriggerTimeout                    INTEGER,
          dot11RRMCivicMeasurementEnabled           TruthValue,
          dot11RRMIdentifierMeasurementEnabled      TruthValue,
          dot11DMSMAXSTAS                           INTEGER,
          dot11DMSMAXCHANNELLOADFORNEWSERVICE       INTEGER,
          dot11DMSMAXCHANNELLOAD                    INTEGER,
          dot11UTCTSFDTIMInterval                   INTEGER,
          dot11UTCTSFOffsetAccuracy                 INTEGER,
          dot11UTCTSFOffsetValue                    INTEGER,
          dot11UTCTSFOffsetTimeError                INTEGER,
          dot11UTCTSFOffsetTimeValue                INTEGER,
          dot11InterworkingServiceImplemented       TruthValue,
          dot11InterworkingServiceEnabled           TruthValue,
          dot11QosmapImplemented                    TruthValue,
          dot11QosMapEnabled                        TruthValue,
          dot11EBRImplemented                       TruthValue,
          dot11EBREnabled                           TruthValue,
          dot11ESNetwork                            TruthValue,
          dot11SSPNInterfaceImplemented             TruthValue,
          dot11SSPNInterfaceEnabled                 TruthValue,
          dot11GASResponseBufferingTime             INTEGER,
          dot11HESSID                               MacAddress,
          dot11EASImplemented                       TruthValue,
          dot11EASEnabled                           TruthValue,
          dot11MSGCFImplemented                     TruthValue,
          dot11MSGCFEnabled                         TruthValue
          }
```

Insert the following elements to the dot11StationConfigTable definitions in Annex D.

```
dot11InterworkingServiceImplemented OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "This attribute when true, indicates the STA is capable of
                interworking with external networks. A STA setting this to
                TRUE implements Interworking Service. When this is set to
                FALSE, the STA does not implement Interworking Service."
        DEFVAL {false}
        ::= {dot11StationConfigEntry 116}


dot11InterworkingServiceEnabled OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "This attribute when true, indicates the capability of the
                STA to interwork with external networks is enabled. The
                capability is disabled otherwise."
        DEFVAL {false}
        ::= {dot11StationConfigEntry 117}


dot11QosmapImplemented OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "This attribute available at STAs, when true, indicates the
                STA is capable of supporting the QoS Map procedures. When
                this is set to FALSE, the STA does not implement QoS Map
                procedures."
        DEFVAL {false}
        ::= {dot11StationConfigEntry 118}


dot11QosMapEnabled OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "This attribute, when true, indicates the capability of the
                STA to support QoS Map procedures is enabled. The capability
                is disabled otherwise."
        DEFVAL {false}
        ::= {dot11StationConfigEntry 119}


dot11EBRImplemented OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "This attribute available at STAs, when true, indicates the
                STA is capable of supporting Expedited Bandwidth Request
                procedures. When this is set to FALSE, the STA does not
                implement Expedited Bandwidth Request procedures.”
        DEFVAL {false}
        ::= {dot11StationConfigEntry 120}


dot11EBREnabled OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                “This attribute, when true, indicates the capability of the
                STA to support Expedited Bandwidth Request procedures is
                enabled. The capability is disabled otherwise.”
        DEFVAL {false}
        ::= {dot11StationConfigEntry 121}


dot11ESNetwork OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
                “The Emergency Services Network Type set to TRUE for this
                HESSID set Indicates that higher layer emergency call
                services are reachable via this SSID.“
        ::= {dot11StationConfigEntry 122}


dot11SSPNInterfaceImplemented OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
             “This attribute when true, indicates the AP is capable of SSPN
             Interface service. When this is set to FALSE, the STA does not
             implement SSPN Interface Service. This object is not used by
             non-AP STAs. The default value of this attribute is false.”
        DEFVAL {false}
        ::= {dot11StationConfigEntry 123}


dot11SSPNInterfaceEnabled OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
             “This attribute, when true, indicates the capability of the AP
             to provide SSPN Interface service is enabled. The capability is
             disabled, otherwise. The default value of this attribute is
             false.”
        DEFVAL {false}
        ::= {dot11StationConfigEntry 124}


dot11GASResponseBufferingTime OBJECT-TYPE
        SYNTAX INTEGER (0..65535)
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
```

```
                "This object defines the time duration after the expiry of
                the GAS Comeback Delay that an STA will buffer a Query
                Response. The units of this MIB object are TUs. Upon expiry
                of this time, the STA may discard the Query Response."
        DEFVAL {1000}
        ::= { dot11StationConfigEntry 125}


dot11HESSID OBJECT-TYPE
        SYNTAX MacAddress
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "This attribute is used by an AP and is the 6-octet
                homogeneous ESS identifier field, whose value is set to one
                of the BSSIDs in the ESS. It is required that the same value
                of HESSID be used for all BSSs in the homogeneous ESS."
        ::= {dot11StationConfigEntry 126}


dot11EASImplemented OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
             "This attribute when true, indicates the STA is capable of
             emergency alert system notification with external networks. A
             STA setting this to TRUE implements emergency alert system
             notification. When this is set to FALSE, the STA does not
             implement emergency alert system notification."
        DEFVAL {false}
        ::= {dot11StationConfigEntry 127}


dot11EASEnabled OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
             "This attribute when true, indicates the capability of the STA
             to support emergency alert system when interwork with external
             networks is enabled. The capability is disabled otherwise."
        DEFVAL {false}
        ::= {dot11StationConfigEntry 128}


dot11MSGCFImplemented OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
             "This attribute when true, indicates the non-AP STA is capable
             of supporting the MSGCF procedures defined in 11B. When false,
             the non-AP STA does not implement MSGCF procedures. This object
             is not used by APs. The default value of this attribute is
             false."
        DEFVAL (FALSE)
        ::= {dot11StationConfigEntry 129}
```

```
dot11MSGCFEnabled OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
             "This attribute, when true, indicates the capability of the
             non-AP STA to provide the MSGCF is enabled. The capability is
             disabled, otherwise. The default value of this attribute is
             false."
        DEFVAL (FALSE)
        ::= {dot11StationConfigEntry 130}
```

Insert the following elements just before PHY attributes in Annex D:

```
        -- Interworking Management (IMT) Attributes
        -- DEFINED AS "The Interworking management object class provides
        -- the necessary support for an SSPN Interface function to manage
        -- interworking with external systems. IMT objects are conceptual
        -- objects for Interworking Service and are defined only for the
        -- AP."

dot11imt OBJECT IDENTIFIER ::= {ieee802dot11 4}

        -- IMT GROUPS
          -- dot11BSSIdTable               ::= { dot11imt 1 }
          -- dot11InterworkingTable        ::= { dot11imt 2 }
          -- dot11APLCI                    ::= { dot11imt 3 }
          -- dot11APCivicLocation          ::= { dot11imt 4 }
          -- dot11RoamingConsortiumTable   ::= { dot11imt 5 }
          -- dot11NAIRealmTable            ::= { dot11imt 6 }
          -- dot11DomainNameTable          ::= { dot11imt 7 }

-- Generic Advertisement Service (GAS) Attributes
-- DEFINED AS "The Generic Advertisement Service management
-- object class provides the necessary support for an Advertisement
-- service to interwork with external systems."

         -- GAS GROUPS
         -- dot11GASAdvertisementTable     ::= { dot11imt 8 }
```

Insert the following dot11BSSIdTable elements in Annex D:

```
--**********************************************************************
-- * dot11BSSId TABLE
--**********************************************************************

dot11BSSIdTable OBJECT-TYPE
        SYNTAX         SEQUENCE OF Dot11BSSIdEntry
        MAX-ACCESS     not-accessible
        STATUS         current
        DESCRIPTION
               "This object is a table of BSSIDs contained within an Access
               Point (AP)."
        ::= { dot11imt 1 }
```

```
dot11BSSIdEntry OBJECT-TYPE
        SYNTAX     Dot11BSSIdEntry
        MAX-ACCESS not-accessible
        STATUS     current
        DESCRIPTION
                “This object provides the attributes identifying a particular
                BSSID within an AP.”
        INDEX { dot11APMacAddress }
        ::= { dot11BSSIdTable 1 }


Dot11BSSIdEntry ::=
        SEQUENCE {
                dot11APMacAddress       MacAddress
               }


 dot11APMacAddress OBJECT-TYPE
        SYNTAX     MacAddress
        MAX-ACCESS read only
        STATUS     current
        DESCRIPTION
                “This object specifies the MAC address of the BSSID
                represented on a particular BSSID interface and uniquely
                identifies this entry.”
        ::= { dot11BSSIdEntry 1 }

--**********************************************************************
-- * End of dot11BSSId TABLE
--**********************************************************************



--**********************************************************************
-- * dot11Interworking TABLE
--**********************************************************************


dot11InterworkingTable OBJECT-TYPE
        SYNTAX SEQUENCE OF Dot11InterworkingEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
             "This table represents the non-AP STAs associated to the AP. An
             entry is created automatically by the AP when the STA becomes
             associated to the AP. The corresponding entry is deleted when
             the STA disassociates. Each STA added to this table is uniquely
             identified by its MAC address."
        ::= { dot11imt 2 }


dot11InterworkingEntry OBJECT-TYPE
        SYNTAX Dot11InterworkingEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
             "Each entry represents a conceptual row in the
             dot11InterworkingTable and provides information about
             permissions received from an SSPN Interface. If a non-AP STA
             does not receive permissions for one or more of these objects,
             then the object's default values or AP's locally defined
             configuration may be used instead. If the AP's local policy(s)
             is more restrictive than an object's value received from the
             SSPN Interface, then the AP's local policy shall be enforced.
             An entry is identified by the AP's MAC address to which the STA
             is associated and the STA's MAC address."
        INDEX { dot11APMacAddress, dot11NonAPStationMacAddress }
        ::= { dot11InterworkingTable 1 }


Dot11InterworkingEntry ::=
        SEQUENCE {
             dot11NonAPStationMacAddress               MacAddress,
             dot11NonAPStationUserIdentity             DisplayString,
             dot11NonAPStationInterworkingCapability   BITS,
             dot11NonAPStationAssociatedSSID           OCTET STRING,
             dot11NonAPStationUnicastCipherSuite       OCTET STRING,
             dot11NonAPStationBroadcastCipherSuite     OCTET STRING,
             dot11NonAPStationAuthAccessCategories     BITS,
             dot11NonAPStationAuthMaxVoiceRate         Unsigned32,
             dot11NonAPStationAuthMaxVideoRate         Unsigned32,
             dot11NonAPStationAuthMaxBestEffortRate    Unsigned32,
             dot11NonAPStationAuthMaxBackgroundRate    Unsigned32,
             dot11NonAPStationAuthMaxVoiceOctets        Unsigned32,
             dot11NonAPStationAuthMaxVideoOctets       Unsigned32,
             dot11NonAPStationAuthMaxBestEffortOctets   Unsigned32,
             dot11NonAPStationAuthMaxBackgroundOctets   Unsigned32,
             dot11NonAPStationAuthMaxHCCAHEMMOctets    Unsigned32,
             dot11NonAPStationAuthMaxTotalOctets       Unsigned32,
             dot11NonAPStationAuthHCCAHEMM             TruthValue,
             dot11NonAPStationAuthMaxHCCAHEMMRate      Unsigned32,
             dot11NonAPStationAuthHCCAHEMMDelay        Unsigned32,
             dot11NonAPStationAuthSourceMulticast      TruthValue,
             dot11NonAPStationAuthMaxSourceMulticastRate Unsigned32,
             dot11NonAPStationVoiceMSDUCount           Counter32,
             dot11NonAPStationDroppedVoiceMSDUCount    Counter32,
             dot11NonAPStationVoiceOctetCount          Counter32,
             dot11NonAPStationDroppedVoiceOctetCount   Counter32,
             dot11NonAPStationVideoMSDUCount           Counter32,
             dot11NonAPStationDroppedVideoMSDUCount    Counter32,
             dot11NonAPStationVideoOctetCount          Counter32,
             dot11NonAPStationDroppedVideoOctetCount   Counter32,
             dot11NonAPStationBestEffortMSDUCount      Counter32,
             dot11NonAPStationDroppedBestEffortMSDUCount Counter32,
             dot11NonAPStationBestEffortOctetCount     Counter32,
             dot11NonAPStationDroppedBestEffortOctetCount Counter32,
             dot11NonAPStationBackgroundMSDUCount      Counter32,
             dot11NonAPStationDroppedBackgroundMSDUCount Counter32,
             dot11NonAPStationBackgroundOctetCount     Counter32,
             dot11NonAPStationDroppedBackgroundOctetCount Counter32,
             dot11NonAPStationHCCAHEMMMSDUCount        Counter32,
             dot11NonAPStationDroppedHCCAHEMMMSDUCount Counter32,
             dot11NonAPStationHCCAHEMMOctetCount       Counter32,
             dot11NonAPStationDroppedHCCAHEMMOctetCount Counter32,
             dot11NonAPStationMulticastMSDUCount       Counter32,
             dot11NonAPStationDroppedMulticastMSDUCount Counter32,
             dot11NonAPStationMulticastOctetCount      Counter32
             dot11NonAPStationDroppedMulticastOctetCount Counter32
             dot11NonAPStationPowerManagementMode      INTEGER,
             dot11NonAPStationAuthDls                  TruthValue,
             dot11NonAPStationVLANId                   INTEGER,
            dot11NonAPStationVLANName                 OCTET STRING,
            dot11NonAPStationAddtsResultCode          INTEGER}


dot11NonAPStationMacAddress OBJECT-TYPE
        SYNTAX     MacAddress
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "This object specifies the MAC address of the client for this
                entry and uniquely identifies
        this entry."
        ::= { dot11InterworkingEntry 1 }


dot11NonAPStationUserIdentity OBJECT-TYPE
        SYNTAX DisplayString (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
                "This attribute reflects the user identity for the subscriber
                operating this non-AP STA"
        ::= { dot11InterworkingEntry 2 }


dot11NonAPStationInterworkingCapability OBJECT-TYPE
        SYNTAX BITS {
                    interworkingCapability(0)
                    qosMapCapability(1)
                    expeditedBwReqCapability(2)}
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
                "This attribute defines the Interworking capabilities
                possessed by a non-AP STA. Interworking Capability is set to
                1 when the STA includes the Interworking Capability
                information element in its (Re)Association request. The
                QosMapCapability and ExpeditedBwReqCapability bits reflect
                the same values and meanings as those defined in 7.3.2."
        ::= { dot11InterworkingEntry 3 }


dot11NonAPStationAssociatedSSID OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..32))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
                "This attribute reflects the SSID to which the non-AP STA is
                associated"
        ::= { dot11InterworkingEntry 4 }


dot11NonAPStationUnicastCipherSuite OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(4))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
```

```
               "The selector of the AKM cipher suite that is currently in
               use by the non-AP STA. It consists of an OUI (the first 3
               octets) and a cipher suite identifier (the last octet)."
        ::= { dot11InterworkingEntry 5 }


dot11NonAPStationBroadcastCipherSuite OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(4))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
               "The selector of an AKM suite for broadcast and group
               addressed frame transmissions. It consists of an OUI (the
               first 3 octets) and a cipher suite identifier the last
               octet)."
        ::= { dot11InterworkingEntry 6 }


dot11NonAPStationAuthAccessCategories OBJECT-TYPE
        SYNTAX     BITS {
                      bestEffort(0),
                      background(1),
                      video(2),
                      voice(3
                      }
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
               "The object that represents the access categories which the
               non-AP STA is permitted to use regardless of whether
               admission control is configured on that AC. Frames received
               on an AC which the non-AP STA is not permitted to use should
               be downgraded to best effort. An AC is permitted to be used
               if its corresponding bit is set to 1; otherwise it is not
               permitted to be used."
        DEFVAL {15}
        ::= { dot11InterworkingEntry 7}


dot11NonAPStationAuthMaxVoiceRate OBJECT-TYPE
        SYNTAX      Unsigned32 (1..4294967295)
        UNITS       "kbps"
        MAX-ACCESS read-only
        STATUS      current
        DESCRIPTION
               "This attribute indicates the maximum authorized data rate in
               kbps the non-AP STA may use, either transmitting to an AP or
               receiving from an AP on the voice access category. If this
               rate is exceeded, the AP should police the flows traversing
               this AC. The value '4294967295', which is the default value,
               means that the SSP is not requesting the AP to limit the data
               rate used by the non-AP STA. Local configuration of the AP,
               however, may cause the rate to be limited, especially when
               the AC is configured for mandatory admission control."
        DEFVAL {4294967295}
        ::= { dot11InterworkingEntry 8}


dot11NonAPStationAuthMaxVideoRate OBJECT-TYPE
        SYNTAX      Unsigned32 (1..4294967295)
        UNITS       "kbps"
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                “This attribute indicates the maximum authorized data rate in
                kbps the non-AP STA may use, either transmitting to an AP or
                receiving from an AP on the video access category. If this
                rate is exceeded, the AP should police the flows traversing
                this AC. The value '4294967295', which is the default value,
                means that the SSP is not requesting the AP to limit the data
                rate used by the non-AP STA. Local configuration of the AP,
                however, may cause the rate to be limited, especially when
                the AC is configured for mandatory admission control.”
        DEFVAL {4294967295}
        ::= { dot11InterworkingEntry 9}


dot11NonAPStationAuthMaxBestEffortRate OBJECT-TYPE
        SYNTAX     Unsigned32 (1..4294967295)
        UNITS      “kbps”
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                “This attribute indicates the maximum authorized data rate in
                kbps the non-AP STA may use, either transmitting to an AP or
                receiving from an AP on the best effort access category. If
                this rate is exceeded, the AP should  police the flows
                traversing this AC. The value '4294967295', which is the
                default value, means that the SSP is not requesting the AP to
                limit the data rate used by the non-AP STA. Local
                configuration of the AP, however, may cause the rate to be
                limited, especially when the AC is configured for mandatory
                admission control.”
        DEFVAL {4294967295}
        ::= { dot11InterworkingEntry 10}


dot11NonAPStationAuthMaxBackgroundRate OBJECT-TYPE
        SYNTAX     Unsigned32 (1..4294967295)
        UNITS      “kbps”
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                “This attribute indicates the maximum authorized data rate in
                kbps the non-AP STA may use, either transmitting to an AP or
                receiving from an AP on the background access category. If
                this rate is exceeded, the AP should  police the flows
                traversing this AC. The value '4294967295', which is the
                default value, means that the SSP is not requesting the AP to
                limit the data rate used by the non-AP STA. Local
                configuration of the AP, however, may cause the rate to be
                limited, especially when the AC is configured for mandatory
                admission control.”
        DEFVAL {4294967295}
        ::= { dot11InterworkingEntry 11 }


dot11NonAPStationAuthMaxVoiceOctets OBJECT-TYPE
        SYNTAX     Unsigned32 (0..4294967295)
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
```

```
               "This attribute indicates the maximum authorized total octet
               count that a STA may use on the voice access category. If
               this octet count is exceeded, the AP should disassociate the
               non-AP STA. A value of zero indicates that there is no octet
               limit."
        DEFVAL {0}
        ::= { dot11InterworkingEntry 12 }


dot11NonAPStationAuthMaxVideoOctets OBJECT-TYPE
        SYNTAX     Unsigned32 (0..4294967295)
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
             "This attribute indicates the maximum authorized total octet
             count that a STA may use on the video access category. If this
             octet count is exceeded, the AP should disassociate the non-AP
             STA. A value of zero indicates that there is no octet limit."
        DEFVAL {0}
        ::= { dot11InterworkingEntry 13 }


dot11NonAPStationAuthMaxBestEffortOctets OBJECT-TYPE
        SYNTAX     Unsigned32 (0..4294967295)
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
             "This attribute indicates the maximum authorized total octet
             count that a STA may use on the best effort access category. If
             this octet count is exceeded, the AP should disassociate the
             non-AP STA. A value of zero indicates that there is no octet
             limit."
        DEFVAL {0}
        ::= { dot11InterworkingEntry 14 }


dot11NonAPStationAuthMaxBackgroundOctets OBJECT-TYPE
        SYNTAX     Unsigned32 (0..4294967295)
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
             "This attribute indicates the maximum authorized total octet
             count that a STA may use on the background access category. If
             this octet count is exceeded, the AP should disassociate the
             non-AP STA. A value of zero indicates that there is no octet
             limit."
        DEFVAL {0}
        ::= { dot11InterworkingEntry 15 }


dot11NonAPStationAuthMaxHCCAHEMMOctets OBJECT-TYPE
        SYNTAX     Unsigned32 (0..4294967295)
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
             "This attribute indicates the maximum authorized total octet
             count that a STA may use with HCCA or HEMM access. If this
             octet count is exceeded, the AP should disassociate the non-AP
             STA. A value of zero indicates that there is no octet limit."
        DEFVAL {0}
        ::= { dot11InterworkingEntry 16 }
```

```
dot11NonAPStationAuthMaxTotalOctets OBJECT-TYPE
        SYNTAX     Unsigned32 (0..4294967295)
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
             "This attribute indicates the maximum authorized total octet
             count that a STA may use on all access categories combined. If
             this octet count is exceeded, the AP should disassociate the
             non-AP STA. A value of zero indicates that there is no octet
             limit.”
        DEFVAL {0}
        ::= { dot11InterworkingEntry 17 }


dot11NonAPStationAuthHCCAHEMM OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “This attribute, when true, indicates that the non-AP STA is
             permitted by the SSP to request HCCA or HEMM service via ADDTS
             management frames. If this attribute is false, then HCCA or
             HEMM service is not permitted by the SSP.”
        DEFVAL {true}
        ::= { dot11InterworkingEntry 18 }


dot11NonAPStationAuthMaxHCCAHEMMRate OBJECT-TYPE
        SYNTAX     Unsigned32 (1..4294967295)
        UNITS      “kbps”
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
             “This attribute indicates the maximum authorized data rate in
             kbps the non-AP STA may use, either transmitting to an AP or
             receiving from an AP via HCCA or HEMM. The value '4294967295',
             which is the default value, means that the SSP is not
             requesting the AP to limit the data rate used by the non-AP
             STA. Local configuration of the AP, however, may cause the rate
             to be otherwise limited.”
        DEFVAL {4294967295}
        ::= { dot11InterworkingEntry 19 }


dot11NonAPStationAuthHCCAHEMMDelay OBJECT-TYPE
        SYNTAX     Unsigned32 (1..4294967295)
        UNITS      “microseconds”
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
             “This attribute indicates the delay bound for frames queued at
             an AP to a non-AP STA in the HCCA or HEMM queue. An AP should
             deliver frames to the non-AP STA within the time period
             specified in this attribute. When a non- AP STA requests
             admission control to the HCCA or HEMM queue, the requested
             delay will be equal to or higher than this value. The value
             '4294967295', which is the default value, means that the SSP is
             not requesting the AP limit the delay bound in this queue for
             transmissions to the non-AP STA.”
        DEFVAL {4294967295}
        ::= { dot11InterworkingEntry 20 }
```

```
dot11NonAPStationAuthSourceMulticast OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "This attribute, when true, indicates that the AP’s MAC
             sublayer shall perform rate limiting to enforce the resource
             utilization limit in
             dot11NonAPStationAuthMaxSourceMulticastRate in the
             dot11InterworkingEntry identified by the source MAC address of
             the received frame.  If this attribute is false, at an AP for
             which dot11SSPNInterfaceEnabled is true, upon receipt of a
             frame of type data with broadcast/multicast DA, then the AP’s
             MAC sublayer shall discard the frame."
        DEFVAL{true)
        ::= { dot11InterworkingEntry 21}


dot11NonAPStationAuthMaxSourceMulticastRate OBJECT-TYPE
        SYNTAX     Unsigned32 (1..4294967295)
        UNITS      “kbps”
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
             “This attribute indicates the maximum authorized data rate in
             kbps which the non-AP STA may transmit group addressed frames
             to an AP. If this rate is exceeded, the AP should police the
             flows. The value '4294967295', which is the default value,
             means that the SSP is not requesting the AP to limit the
             multicast data rate used by the non-AP STA.”
        DEFVAL {4294967295}
        ::= { dot11InterworkingEntry 22}


dot11NonAPStationVoiceMSDUCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “For EDCA operation, this counter shall be incremented for each
             MSDU successfully transmitted by the AP on the voice access
             category and for each MSDU successfully received on either user
             priority 6 or 7."
        ::= { dot11InterworkingEntry 23 }


dot11NonAPStationDroppedVoiceMSDUCount Counter32
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “For EDCA operation, this counter shall be incremented for each
             MSDU dropped by the AP on the voice access category.”
        ::= { dot11InterworkingEntry 24}


dot11NonAPStationVoiceOctetCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "For EDCA operation, this counter shall be incremented by the
             octet length of each MSDU successfully transmitted by the AP on
             the voice access category and by the octet length of each MSDU
             successfully received on either user priority 6 or 7."
        ::= { dot11InterworkingEntry 25 }


dot11NonAPStationDroppedVoiceOctetCount OBJECT-TYPE
       SYNTAX Counter32
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
             “For EDCA operation, this counter shall be incremented for each
             octet dropped by the AP on the voice access category."
       ::= { dot11InterworkingEntry 26 }


dot11NonAPStationVideoMSDUCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “For EDCA operation, this counter shall be incremented for each
             MSDU successfully transmitted by the AP on the video access
             category and for each MSDU successfully received on either user
             priority 4 or 5."
        ::= { dot11InterworkingEntry 27 }


dot11NonAPStationDroppedVideoMSDUCount Counter32
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “For EDCA operation, this counter shall be incremented for each
             MSDU dropped by the AP on the video access category.”
        ::= { dot11InterworkingEntry 28}


dot11NonAPStationVideoOctetCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
               "For EDCA operation, this counter shall be incremented by the
               octet length of each MSDU successfully transmitted by the AP
               on the voice access category and by the octet length of each
               MSDU successfully received on either user priority 4 or 5."
        ::= { dot11InterworkingEntry 29 }


dot11NonAPStationDroppedVideoOctetCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “For EDCA operation, this counter shall be incremented for each
             octet dropped by the AP on the video access category."
```

```
      ::= { dot11InterworkingEntry 30 }


dot11NonAPStationBestEffortMSDUCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
                “For EDCA operation, this counter shall be incremented for
                each MSDU successfully transmitted by the AP on the best
                effort access category and for each MSDU successfully
                received on either user priority 0 or 3. For DCF or PCF
                operation, this counter shall be incremented for each MSDU
                successfully transmitted or received by the AP.”
        ::= { dot11InterworkingEntry 31 }


dot11NonAPStationDroppedBestEffortMSDUCount Counter32
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “For EDCA operation, this counter shall be incremented for each
             MSDU dropped by the AP on the best effort access category and
             for each MSDU dropped by the AP on either user priority 0 or 3.
             For DCF or PCF operation, this counter shall be incremented for
             each MSDU dropped by the AP.”
        ::= { dot11InterworkingEntry 32}


dot11NonAPStationBestEffortOctetCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "For EDCA operation, this counter shall be incremented by the
             octet length of each MSDU successfully transmitted by the AP on
             the best effort access category and by the octet length of each
             MSDU successfully received on either user priority 0 or 3. For
             DCF or PCF operation, this counter shall be incremented the
             octet length of each MSDU successfully transmitted or received
             by the AP."
        ::= { dot11InterworkingEntry 33 }


dot11NonAPStationDroppedBestEffortOctetCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “For EDCA operation, this counter shall be incremented for the
             octet length of each MSDU dropped by the AP on the best effort
             access category and by the octet length of each MSDU dropped by
             the AP for either user priority 0 or 3. For DCF or PCF
             operation, this counter shall be incremented for the octet
             length of each MSDU dropped by the AP.”
      ::= { dot11InterworkingEntry 34 }
```

```
dot11NonAPStationBackgroundMSDUCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “For EDCA operation, this counter shall be incremented for each
             MSDU successfully transmitted by the AP on the background
             access category and for each MSDU successfully received on
             either user priority 1 or 2."
        ::= { dot11InterworkingEntry 35}


dot11NonAPStationDroppedBackgroundMSDUCount Counter32
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “For EDCA operation, this counter shall be incremented for each
             MSDU dropped by the AP on the background access category”
        ::= { dot11InterworkingEntry 36}


dot11NonAPStationBackgroundOctetCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "For EDCA operation, this counter shall be incremented by the
             octet length of each MSDU successfully transmitted by the AP on
             the background access category and by the octet length of each
             MSDU successfully received on either user priority 1 or 2."
        ::= { dot11InterworkingEntry 37 }


dot11NonAPStationDroppedBackgroundOctetCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “For EDCA operation, this counter shall be incremented by the
             octet length of each MSDU dropped by the AP on the background
             access category”
       ::= { dot11InterworkingEntry 38 }


dot11NonAPStationHCCAHEMMMSDUCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “For HCCA or HEMM operation, this counter shall be incremented
             for each MSDU successfully transmitted by the AP and for each
             MSDU successfully received on either.”
        ::= { dot11InterworkingEntry 39}


dot11NonAPStationDroppedHCCAHEMMMSDUCount Counter32
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
                “For HCCA or HEMM operation, this counter shall be
                incremented for each MSDU dropped by the AP.”
        ::= { dot11InterworkingEntry 40}


dot11NonAPStationHCCAHEMMOctetCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “For HCCA or HEMM operation, this counter shall be incremented
             by the octet length of each MSDU successfully transmitted by
             the AP and by the octet length of each MSDU successfully
             received.”
        ::= { dot11InterworkingEntry 41 }


dot11NonAPStationDroppedHCCAHEMMMSDUCount Counter32
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “For HCCA or HEMM operation, this counter shall be incremented
             by the octet length of each MSDU dropped by the AP.”
        ::= { dot11InterworkingEntry 42}


dot11NonAPStationMulticastMSDUCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “For Multicast operation, this counter shall be incremented for
             each Multicast MSDU successfully transmitted by the AP and for
             each Multicast MSDU successfully received at the AP.”
        ::= { dot11InterworkingEntry 43}


dot11NonAPStationDroppedMulticastMSDUCount Counter32
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
                “For Multicast operation, this counter shall be incremented
                for each Multicast MSDU dropped by the AP.”
        ::= { dot11InterworkingEntry 44}


dot11NonAPStationMulticastOctetCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “For Multicast operation, this counter shall be incremented by
             the octet length of each MSDU successfully transmitted by the
             AP and by the octet length of each Multicast MSDU successfully
             received.”
        ::= { dot11InterworkingEntry 45 }
```

```
dot11NonAPStationDroppedMulticastOctetCount Counter32
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “For Multicast operation, this counter shall be incremented by
             the octet length of each Multicast MSDU dropped by the AP.”
        ::= { dot11InterworkingEntry 46}


dot11NonAPStationPowerManagementMode OBJECT-TYPE
        SYNTAX INTEGER { active(1), powersave(2) }
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “This attribute indicates the power management mode of the non-
             AP STA.”
        ::= { dot11InterworkingEntry 47}


dot11NonAPStationAuthDls OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “This attribute, when true, indicates that the non-AP STA is
             permitted by the SSPN Interface to use direct link service
             (DLS). This object does not mean the AP is capable of providing
             DLS service. This service is disabled otherwise.”
        DEFVAL {true}
        ::= { dot11InterworkingEntry 48}


dot11NonAPStationVLANId OBJECT-TYPE
        SYNTAX     INTEGER (0..4095)
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
             “This attribute indicates the VLAN ID on the an external
             network to which frames from the non-AP STA are bridged.”
        ::= { dot11InterworkingEntry 49}


dot11NonAPStationVLANName OBJECT-TYPE
        SYNTAX DisplayString (SIZE(0..64))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “This attribute indicates the VLAN name corresponding to the
             VLAN ID on the external network to which frames from the non-AP
             STA are bridged.”
        ::= { dot11InterworkingEntry 50}


dot11NonAPStationAddtsResultCode OBJECT-TYPE
        SYNTAX INTEGER {
                   success(1),
                   invalid_parameters(2),
                   rejected_with_suggested_changes(3),
                   rejected_for_delay_period(4)}
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “This attribute indicates the most recent result code returned
             by the AP in an ADDTS Response.”
        ::= { dot11InterworkingEntry 51}

-- **********************************************************************
-- * End of dot11Interworking TABLE
-- **********************************************************************
```

Insert the following entries in dot11APLCI in Annex D:

```
-- **********************************************************************
-- * dot11APLCI TABLE
-- **********************************************************************


dot11APLCITable OBJECT-TYPE
        SYNTAX         SEQUENCE OF Dot11APLCIEntry
        MAX-ACCESS     read-write
        STATUS         current
        DESCRIPTION
             “This table represents the geospatial location of the AP as
             specified in clause 7.3.2.22.9.”
        ::= { dot11imt 3 }


dot11APLCIEntry OBJECT-TYPE
        SYNTAX Dot11APLCIEntry
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
             “AP location in geospatial coordinates”
        INDEX { dot11APLCIDIndex }
        ::= { dot11APLCITable 1 }


Dot11APLCIEntry ::=
        SEQUENCE {
             dot11APLCIIndex                           Unsigned32,
             dot11APLCILatitudeResolution              INTEGER,
             dot11APLCILatitudeInteger                 Integer32,
             dot11APLCILatitudeFraction                Integer32,
             dot11APLCILongitudeResolution             INTEGER,
             dot11APLCILongitudeInteger                Integer32,
             dot11APLCILongitudeFraction               Integer32,
             dot11APLCIAltitudeType                    INTEGER,
             dot11APLCIAltitudeResolution              INTEGER,
             dot11APLCIAltitudeInteger                 Integer32,
             dot11APLCIAltitudeFraction                Integer32,
             dot11APLCIDatum                           INTEGER,
             dot11APLCIAzimuthType                     INTEGER,
             dot11APLCIAzimuthResolution               INTEGER,
             dot11APLCIAzimuth                         Integer32
             }
```

```
dot11APLCIIndex OBJECT-TYPE
        SYNTAX Unsigned32
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
             "Index for AP LCI elements in dot11APLCITable, greater than 0."
        ::= { dot11APLCIEntry 1 }


dot11APLCILatitudeResolution OBJECT-TYPE
        SYNTAX INTEGER (0..63)
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “Latitude resolution is 6 bits indicating the number of valid
             bits in the fixed-point value of Latitude. This field is
             derived from IETF RFC 3825, and is accessed big-endian.”
        ::= { dot11APLCIEntry 2 }


dot11APLCILatitudeInteger OBJECT-TYPE
        SYNTAX Integer32 (-90..90)
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “Latitude is a 34 bit fixed point value consisting of 9 bits of
             integer and 25 bits of fraction. This field contains the 9 bits
             of integer portion of Latitude. This field is derived from RFC-
             3825, and is accessed big-endian.”
        ::= { dot11APLCIEntry 3}


dot11APLCILatitudeFraction OBJECT-TYPE
        SYNTAX Integer32 (-16777215..16777215)
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “Latitude is a 34 bit fixed point value consisting of 9 bits of
             integer and 25 bits of fraction. This field contains the 25
             bits of fraction portion of Latitude. This field is derived
             from RFC-3825, and is accessed big-endian.”
        ::= { dot11APLCIEntry 4}


dot11APLCILongitudeResolution OBJECT-TYPE
        SYNTAX INTEGER (0..63)
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “Longitude resolution is 6 bits indicating the number of valid
             bits in the fixed-point value of Longitude. This field is
             derived from RFC-3825, and is accessed big-endian.”
        ::= { dot11APLCIEntry 5}


dot11APLCILongitudeInteger OBJECT-TYPE
        SYNTAX Integer32 (-180..180)
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
```

```
             "Longitude is a 34 bit fixed point value consisting of 9 bits
             of integer and 25 bits of fraction. This field contains the 9
             bits of integer portion of Longitude. This field is derived
             from RFC-3825, and is accessed big-endian."
        ::= { dot11APLCIEntry 6}


dot11APLCILongitudeFraction OBJECT-TYPE
        SYNTAX Integer32 (-16777215..16777215)
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "Longitude is a 2's complement 34 bit fixed point value
             consisting of 9 bits of integer and 25 bits of fraction. This
             field contains the 25 bits of fraction portion of Longitude.
             This field is derived from IETF RFC 3825, and is accessed big-
             endian."
        ::= { dot11APLCIEntry 7}


dot11APLCIAltitudeType OBJECT-TYPE
        SYNTAX INTEGER {
                   meters(1),
                   floors(2),
                   hagm (3) }
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "Altitude Type is four bits encoding the type of altitude.
             Codes defined are: meters in 2s-complement fixed-point 22-bit
             integer part with 8-bit fraction floors in 2s-complement fixed-
             point 22-bit integer part with 8-bit fraction hagm: Height
             Above Ground in meters, in 2s-complement fixed-point 22-bit
             integer part with 8-bit fraction. This field is derived from
             IETF RFC 3825, and is accessed big-endian."
        ::= { dot11APLCIEntry 8}


dot11APLCIAltitudeResolution OBJECT-TYPE
        SYNTAX INTEGER (0..63)
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "Altitude resolution is 6 bits indicating the number of valid
             bits in the altitude. This field is derived from IETF RFC 3825,
             and is accessed big-endian."
        ::= { dot11APLCIEntry 9}



dot11APLCIAltitudeInteger OBJECT-TYPE
        SYNTAX Integer32 (-2097151..2097151)
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "Altitude is a 30 bit value defined by the Altitude type field.
             The field is encoded as a 2s-complement fixed-point 22-bit
             integer Part with 8-bit fraction. This field contains the
             fixed-point Part of Altitude. This field is derived from IETF
             RFC 3825, and is accessed big-endian."
        ::= { dot11APLCIEntry 10}
```

```
dot11APLCIAltitudeFraction OBJECT-TYPE
        SYNTAX Integer32 (-127..127)
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “Altitude is a 30 bit value defined by the Altitude type field.
             The field is encoded as a 2s-complement fixed-point 22-bit
             integer Part with 8-bit fraction. This field is derived from
             IETF RFC 3825, and is accessed big-endian.”
        ::= { dot11APLCIEntry 11 }


dot11APLCIDatum OBJECT-TYPE
        SYNTAX INTEGER (0..255)
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “Datum is an 8-bit value encoding the horizontal and vertical
             references used for the coordinates given in this LCI. IETF RFC
             3825 defines the values of Datum. Type 1 is WGS-84, the
             coordinate system used by GPS. Type 2 is NAD83 with NAVD88
             vertical reference. Type 3 is NAD83 with Mean Lower Low Water
             vertical datum. All other types are reserved. This field is
             derived from IETF RFC 3825, and is accessed big-endian.”
        ::= { dot11APLCIEntry 12 }


dot11APLCIAzimuthType OBJECT-TYPE
        SYNTAX INTEGER {
        frontSurfaceOfSTA(0),
        radioBeam(1) }
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “Azimuth Type is a one bit attribute encoding the type of
             Azimuth. Codes defined are: front surface of STA: in 2s-
             complement fixed-point 9-bit integer radio beam: in 2s-
             complement fixed-point 9-bit integer.”
        ::= { dot11APLCIEntry 13 }


dot11APLCIAzimuthResolution OBJECT-TYPE
        SYNTAX INTEGER (0..15)
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “Azimuth Resolution is 4 bits indicating the number of valid
             bits in the azimuth.”
        ::= { dot11APLCIEntry 14 }


dot11APLCIAzimuth OBJECT-TYPE
        SYNTAX Integer32 (-511...511)
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “Azimuth is a 9 bit value defined by the Azimuth Type
             field.The field is encoded as a 2s-complement fixed-point 9-bit
             integer horizontal angle in degrees from True North.”
        ::= { dot11APLCIEntry 15 }
```

```
-- **********************************************************************
-- * End of dot11APLCI TABLE
-- **********************************************************************
```

Insert the following entries in dot11APCiviLocation in Annex D:

```
-- **********************************************************************
-- * dot11APCivicLocation TABLE
-- **********************************************************************


dot11APCivicLocationTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF Dot11ApCivicLocationEntry
        MAX-ACCESS     read-write
        STATUS         current
        DESCRIPTION
             “This table represents the location of the AP in civic format
             using the Civic Address Type elements defined in IETF RFC-477
             [B50].”
        ::= { dot11imt 4 }


dot11APCivicLocationEntry OBJECT-TYPE
        SYNTAX Dot11ApCivicLocationEntry
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
             “Civic Address location of the AP described with Civic Address
             Type elements defined in IETF RFC-4776 [B50].”
        INDEX {dot11APCivicLocationIndex} ::= {dot11APCivicLocationTable 1}


Dot11ApCivicLocationEntry ::=
        SEQUENCE {
             dot11APCivicLocationIndex                 Unsigned32,
             dot11APCivicLocationCountry               OCTET STRING,
             dot11APCivicLocationA1                    OCTET STRING,
             dot11APCivicLocationA2                    OCTET STRING,
             dot11APCivicLocationA3                    OCTET STRING,
             dot11APCivicLocationA4                    OCTET STRING,
             dot11APCivicLocationA5                    OCTET STRING,
             dot11APCivicLocationA6                    OCTET STRING,
             dot11APCivicLocationPrd                   OCTET STRING,
             dot11APCivicLocationPod                   OCTET STRING,
             dot11APCivicLocationSts                   OCTET STRING,
             dot11APCivicLocationHno                   OCTET STRING,
             dot11APCivicLocationHns                   OCTET STRING,
             dot11APCivicLocationLmk                   OCTET STRING,
             dot11APCivicLocationLoc                   OCTET STRING,
             dot11APCivicLocationNam                   OCTET STRING,
             dot11APCivicLocationPc                    OCTET STRING,
             dot11APCivicLocationBld                   OCTET STRING,
             dot11APCivicLocationUnit                  OCTET STRING,
             dot11APCivicLocationFlr                   OCTET STRING,
             dot11APCivicLocationRoom                  OCTET STRING,
             dot11APCivicLocationPlc                   OCTET STRING,
             dot11APCivicLocationPcn                   OCTET STRING,
              dot11APCivicLocationPobox                 OCTET STRING,
              dot11APCivicLocationAddcode               OCTET STRING,
              dot11APCivicLocationSeat                  OCTET STRING,
              dot11APCivicLocationRd                    OCTET STRING,
              dot11APCivicLocationRdsec                 OCTET STRING,
              dot11APCivicLocationRdbr                  OCTET STRING,
              dot11APCivicLocationRdsubbr               OCTET STRING,
              dot11APCivicLocationPrm                   OCTET STRING,
              dot11APCivicLocationPom                   OCTET STRING
              }


dot11APCivicLocationIndex OBJECT-TYPE
        SYNTAX Unsigned32
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
             "Index for APCivicLocation elements in
             dot11APCivicLocationTable, greater than 0."
        ::= { dot11APCivicLocationEntry 1 }


dot11APCivicLocationCountry OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “This attribute contains the two uppercase characters which
             correspond to the alpha-2 codes in ISO 3166-1. Example: US.”
        ::= { dot11APCivicLocationEntry 2 }


dot11APCivicLocationA1 OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “This attribute contains the national subdivisions (state,
             Region, province, prefecture). Example: California. The A1
             element is used for the top level subdivision within a country.
             In the absence of a country-specific guide on how to use the A-
             series of elements, the second part of the ISO 3166-2 code
             [ISO.3166-2] for a country subdivision SHOULD be used. The ISO
             3166-2 code is a formed of a country code and hyphen plus a
             code of one, two or three characters or numerals. For the A1
             element, the leading country code and hyphen are omitted and
             only the subdivision code is included.

             For example, the codes for Canada include CA-BC, CA-ON, CA-
             QC;Luxembourg has just three single character codes: LU-D, LU-G
             And LU-L; Australia uses both two and three character codes:
             AU-ACT, AU-NSW, AU-NT; France uses numerical codes for mainland
             France and letters for territories: FR-75, FR-NC.”
        ::= { dot11APCivicLocationEntry 3 }


dot11APCivicLocationA2 OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
```

```
             "This attribute contains the county, parish, gun (JP), District
             (IN). Example: King's County."
        ::= { dot11APCivicLocationEntry 4}


dot11APCivicLocationA3 OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "This attribute contains the city, township, shi (JP). Example:
             San Francisco."
        ::= { dot11APCivicLocationEntry 5}


dot11APCivicLocationA4 OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "This attribute contains the city division, borough, city
             District, ward, chou (JP). Example: Manhattan."
        ::= { dot11APCivicLocation 6}


dot11APCivicLocationA5 OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "This attribute contains the neighborhood, block. Example:
             Morningside Heights."
        ::= { dot11APCivicLocationEntry 7}


dot11APCivicLocationA6 OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "This attribute contains the street. Example: Broadway. The A6
             element is retained for use in those countries that require
             this level of detail. Where A6 was previously used for street
             names in IETF RFC 5139 [B51], it will not be used, the RD
             element will be used for thorough fare data. However, without
             additional information these fields will not be interchanged
             when converting between different civic formats. Where civic
             address information is obtained from another format, such as
             the DHCP form IETF RFC 4776 [B50], the A6 element will be
             copied directly from the source format."
        ::= { dot11APCivicLocationEntry 8}


dot11APCivicLocationPrd OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "This attribute contains the leading street direction. Example:
             NW."
        ::= { dot11APCivicLocationEntry 9}


dot11APCivicLocationPod OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "This attribute contains the trailing street suffix. Example:
             SW."
        ::= { dot11APCivicLocationEntry 10}


dot11APCivicLocationSts OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "This attribute contains the street suffix. Example: Avenue,
             "Platz, Street"."
        ::= { dot11APCivicLocationEntry 11}


dot11APCivicLocationHno OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
        "This attribute contains the numeric part only of the
        House number. Example: 123."
        ::= { dot11APCivicLocationEntry 12 }


dot11APCivicLocationHns OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "This attribute contains the house number suffix. Example: A,
             ½."
        ::= { dot11APCivicLocationEntry 13 }


dot11APCivicLocationLmk OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "This attribute contains the landmark or vanity address.
             Example: Low Library."
        ::= { dot11APCivicLocationEntry 14 }


dot11APCivicLocationLoc OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
```

```
              “This attribute contains additional location information.
              Example: Room 543."
         ::= { dot11APCivicLocationEntry 15 }


dot11APCivicLocationNam OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
              “This attribute contains the Name (residence, business, or
              office occupant. Example: Joe’s Barbershop.”
         ::= { dot11APCivicLocation 16 }


dot11APCivicLocationPc OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
              “This attribute contains the postal code. Example: 10027-0401.”
         ::= { dot11APCivicLocationEntry 17 }


dot11APCivicLocationBld OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
              “This attribute contains the building (structure). Example:
              Hope Theater.”
         ::= { dot11APCivicLocationEntry 18 }


dot11APCivicLocationUnit OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255)
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
              “This attribute contains the unit (apartment, suite). Example:
              12a.”
         ::= { dot11APCivicLocationEntry 19 }


dot11APCivicLocationFlr OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
              “This attribute contains the floor number. Example: 5."
         ::= { dot11APCivicLocation 20}


dot11APCivicLocationRoom OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255)
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
              “This attribute contains the room. Example: 450F.”
         ::= { dot11APCivicLocationEntry 21 }
```

```
dot11APCivicLocationPlc OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “This attribute contains the place type. Example: office.”
        ::= { dot11APCivicLocationEntry 22 }


dot11APCivicLocationPcn OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “This attribute contains the postal community name. Example:
             Leonia.”
        ::= { dot11APCivicLocationEntry 23 }


dot11APCivicLocationPobox OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “This attribute contains the post office box (P.O. Box).
             Example: U40.”
        ::= { dot11APCivicLocationEntry 24 }


dot11APCivicLocationAddcode OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “This attribute contains the additional code. Example:
             13203000003."
        ::= { dot11APCivicLocationEntry 25 }


dot11APCivicLocationSeat OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “This attribute contains the seat (desk, cubicle, Workstation).
             Example: WS 181”.
        ::= { dot11APCivicLocationEntry 26 }


dot11APCivicLocationRd OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “This attribute contains the primary road or street. Example:
             Broadway.”
        ::= { dot11APCivicLocationEntry 27 }
```

```
dot11APCivicLocationRdsec OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
                "This attribute contains the road section. Example: 14.In
                some countries a thoroughfare can be broken up into sections,
                and it is not uncommon for street numbers to be repeated
                between sections. A road section identifier is required to
                ensure that an address is unique. For example, West Alice
                Parade has 5 sections, each numbered from 1; unless the
                section is specified 7 West Alice Parade could exist in 5
                different places."
        ::= { dot11APCivicLocationEntry 28 }


dot11APCivicLocationRdbr OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "This attribute contains the road branch. Example: Lane 7."
             Minor streets can share the same name, so that they can only Be
             distinguished by the major thoroughfare with which they
             intersect. For example, both West Alice Parade, Section 3 and
             Bob Street could both be interested by a Carol Lane. This
             element is used to specify a road branch where the name of the
             branch does not uniquely identify the road. Road branches MAY
             also be used where a major thoroughfare is split into
             sections."
        ::= { dot11APCivicLocationEntry 29 }


dot11APCivicLocationRdsubbr OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "This attribute contains the road sub-branch. Example: Alley
             8."
        ::= { dot11APCivicLocationEntry 30}


dot11APCivicLocationPrm OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "This attribute contains the road pre-modifier. Example: Old."
        ::= { dot11APCivicLocationEntry 31 }


dot11APCivicLocationPom OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(0..255))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "This attribute contains the road post-modifier. Example:
             Extended."
        ::= { dot11APCivicLocationEntry 32 }
```

```
-- **********************************************************************
-- * End of dot11APCivicLocation TABLE
-- **********************************************************************
```

Insert the following entries in Annex D:

```
-- **********************************************************************
-- * dot11RoamingConsortium TABLE
-- **********************************************************************


dot11RoamingConsortiumTable OBJECT-TYPE
       SYNTAX SEQUENCE OF Dot11RoamingConsortiumEntry
       MAX-ACCESS not-accessible
       STATUS current
       DESCRIPTION
             "This is a Table of OIs which are to be transmitted in an NQP
             Roaming Consortium List. Each table entry corresponds to a
             roaming consortium or single SSP. The first 3 entries in this
             table are transmitted in Beacon and Probe Response frames."
        ::= { dot11imt 5 }


dot11RoamingConsortiumEntry OBJECT-TYPE
        SYNTAX Dot11RoamingConsortiumEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
               "Each OI identifies a roaming consortium (group of SSPs with
               inter-SSP roaming agreement) or a single SSP. A non-AP STA in
               possession of security credentials for the SSPN(s) identified
               by the OI, should be able to successfully authenticate to
               this AP."
        INDEX { dot11RoamingConsortiumOI }
        ::= { dot11RoamingConsortiumTable 1 }


Dot11RoamingConsortiumEntry ::=
        SEQUENCE {
              dot11RoamingConsortiumOI OCTET STRING,
              dot11RoamingConsortiumRowStatus RowStatus
              }


dot11RoamingConsortiumOI OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(16))
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
             "This attribute contains the IEEE defined OI as defined in
             7.3.1.21."
        ::= { dot11RoamingConsortiumEntry 1 }


dot11RoamingConsortiumRowStatus OBJECT-TYPE
        SYNTAX RowStatus
        MAX-ACCESS read-create
        STATUS current
        DESCRIPTION
             “This object represents the status column for a conceptual row
             in this table.”
        ::= { dot11RoamingConsortiumEntry 2 }

-- **********************************************************************
-- * End of dot11RoamingConsortium TABLE
-- **********************************************************************

-- **********************************************************************
-- * dot11NAIRealm TABLE
-- **********************************************************************


dot11NAIRealmTable   OBJECT-TYPE
        SYNTAX                SEQUENCE OF Dot11NAIRealmEntry
        MAX-ACCESS            not-accessible
        STATUS                current
        DESCRIPTION
             “This is a table of NAI Realms which form the NAI Realm List in
             Native Query Protocol. The NAI Realm List may be transmitted to
             a non-AP STA in a Native-GAS Response. Each table entry
             corresponds to a single NAI Realm.”
        ::= { dot11imt 6 }


dot11NAIRealmEntry OBJECT-TYPE
        SYNTAX Dot11NAIRealmEntry
        MAX-ACCESS not-accessible
        STATUS     current
        DESCRIPTION
               “Each NAI Realm identifies an NAI Realm as specified in
               RFC4282 corresponding to an SSP whose network is accessible
               via this AP. A non-AP STA in possession of security
               credentials for the SSPN or network identified by the NAI
               Realm Name should be able to successfully authenticate with
               this AP.”
        INDEX { dot11NAIRealmOui }
        ::= { dot11NAIRealmTable 1 }


Dot11NAIRealmEntry ::=
        SEQUENCE {
             dot11NAIRealm           DisplayString,
             dot11NAIRealmRowStatus  RowStatus
             }


dot11NAIRealm OBJECT-TYPE
        SYNTAX DisplayString(SIZE(0...255))
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
             “This attribute contains an NAI Realm of up to 255 octets
             formatted in accordance with RFC4282.”
        ::= { dot11NAIRealmEntry 1 }
```

```
dot11NAIRealmRowStatus OBJECT-TYPE
        SYNTAX RowStatus
        MAX-ACCESS read-create
        STATUS current
        DESCRIPTION
             “This object represents the status column for a conceptual row
             in this table.”
        ::= { dot11NAIRealmEntry 2 }


-- **********************************************************************
-- *  End of dot11NAIRealm TABLETable
-- **********************************************************************



-- **********************************************************************
-- * dot11DomainName TABLE
-- **********************************************************************


dot11DomainNameTable   OBJECT-TYPE
        SYNTAX                SEQUENCE OF Dot11DomainNameEntry
        MAX-ACCESS            not-accessible
        STATUS                current
        DESCRIPTION
             This is a table of Domain Names which form the Domain Name List
             in Native Query Protocol. The Domain Name List may be
             transmitted to a non-AP STA in a Native-GAS Response. Each
             table entry corresponds to a single Domain Name.
        ::= { dot11imt 6 }


dot11DomainNameEntry OBJECT-TYPE
        SYNTAX     Dot11DomainNameEntry
        MAX-ACCESS not-accessible
        STATUS     current
        DESCRIPTION
             “Each Domain Name identifies a SSP or other provider of a
             network service. A non-AP STA in possession of security
             credentials for the SSPN or network identified by the Domain,
             Name should be able to successfully authenticate with this AP.”
        INDEX { dot11DomainNameOui }
        ::= { dot11DomainNameTable 1 }


Dot11DomainNameEntry ::=
        SEQUENCE {
             dot11DomainName           OCTET STRING
             dot11DomainNameRowStatus  RowStatus
           }


dot11DomainName OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(255))
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
```

```
                “This attribute contains a Domain Name of up to 255 octets
                formatted in accordance with the “Preferred Name Syntax” as
                defined in RFC 1034.”
        ::= { dot11DomainNameEntry 1 }


dot11DomainNameRowStatus OBJECT-TYPE
        SYNTAX RowStatus
        MAX-ACCESS read-create
        STATUS current
        DESCRIPTION
                “This object represents the status column for a conceptual row
                in this table.”
        ::= { dot11DomainNameEntry 2 }

-- **********************************************************************
-- * dot11NAIRealmTable
-- **********************************************************************
```

Insert the following dot11GASAdvertisement table entries in Annex D: This insertion spans through dot11DetectedNetworkMIHCapabilities at the end of this annex.

```
-- **********************************************************************
-- * dot11GASAdvertisement TABLE
-- **********************************************************************


dot11GASAdvertisementTable OBJECT-TYPE
        SYNTAX          SEQUENCE OF Dot11GASAdvertisementEntry
        MAX-ACCESS      not-accessible
        STATUS          current
        DESCRIPTION
                  “This object is a table of GAS counters that allows for
                  multiple instantiations of those counters on an STA.”
        ::= { dot11imt 7}


dot11GASAdvertisementEntry OBJECT-TYPE
        SYNTAX      Dot11GASAdvertisementEntry
        MAX-ACCESS  not-accessible
        STATUS     current
        DESCRIPTION
                “This object provides the attributes identifying a GAS counter
                within an STA.”
        INDEX { dot11GASAdvertisementId }
        ::= { dot11GASAdvertisementTable 1 }


Dot11GASAdvertisementEntry ::=
        SEQUENCE {
                dot11GASAdvertisementId                 INTEGER,
                dot11GASQueries                         Counter32,
                dot11GASQueryRate                       Gauge,
                dot11GASResponses                       Counter32,
                dot11GASResponseRate                    INTEGER,
                dot11GASResponseTimeout                 INTEGER,
                dot11GASTransmittedFragmentCount        Counter32,
                dot11GASFailedCount                     Counter32,
                dot11GASRetryCount                      Counter32,
                dot11GASMultipleRetryCount                Counter32,
                dot11GASFrameDuplicateCount               Counter32,
                dot11GASACKFailureCount                   Counter32,
                dot11GASReceivedFragmentCount             Counter32,
                dot11GASTransmittedMSDUCount              Counter32,
                dot11GASDiscardedMSDUCount                Counter32,
                dot11GASRetriesReceivedCount              Counter32,
                dot11GASComebackDelay                     INTEGER,
                dot11GASQueryResponseLengthLimit          INTEGER
                }


dot11GASAdvertisementId OBJECT-TYPE
        SYNTAX INTEGER (0..255)
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
                "The one octet identification number for the GAS
                Advertisement protocol, as defined in Table 7-43be, for which
                statistics are stored the logical row of the GASAdvertisement
                table."
        ::= { dot11GASAdvertisementEntry 1}


dot11GASQueries OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "The number of GAS queries sent or received for the protocol
             identified by dot11GASAdvertisementId."
        ::= { dot11GASAdvertisementEntry 2 }


dot11GASQueryRate OBJECT-TYPE
        SYNTAX Gauge
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "The number of GAS queries per minute received for the protocol
             identified by dot11GASAdvertisementId, averaged over the
             previous ten minutes."
        ::= { dot11GASAdvertisementEntry 3}


dot11GASResponses OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "The number of GAS responses sent or received for the protocol
             identified by dot11GASAdvertisementId."
        ::= { dot11GASAdvertisementEntry 4}


dot11GASResponseRate OBJECT-TYPE
        SYNTAX INTEGER
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
```

```
             “The number of responses to GAS queries per minute received for
             the protocol identified by
             dot11GASAdvertisementIddot11GASAdvertisementId, averaged over
             the previous ten minutes.”
        ::= { dot11GASAdvertisementEntry 5}


dot11GASTransmittedFragmentCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “This counter shall be incremented for an acknowledged MMPDU,
             with an individual address in the address 1 field.”
        ::= { dot11GASAdvertisementEntry 6}


dot11GASFailedCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “This counter shall be incremented when an MMPDU is not
             transmitted successfully due to the number of transmit attempts
             exceeding either the dot11ShortRetryLimit or
             dot11LongRetryLimit.”
        ::= { dot11GASAdvertisementEntry 7}


dot11GASRetryCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “This counter shall be incremented when an MMPDU is
             successfully transmitted after one or more retransmissions.”
        ::= { dot11GASAdvertisementEntry 8}


dot11GASMultipleRetryCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “This counter shall be incremented when an MMPDU is
             successfully transmitted after more than one retransmissions.”
      ::= { dot11GASAdvertisementEntry 9}


dot11GASFrameDuplicateCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             “This counter shall be incremented when a n MMPDU is received
             that the Sequence Control field indicates is a duplicate.”
      ::= { dot11GASAdvertisementEntry 10}
```

```
dot11GASACKFailureCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
              "This counter shall increment when an ACK is not received in
              response to an MMPDU."
      ::= { dot11GASAdvertisementEntry 11}


dot11GASReceivedFragmentCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "This counter shall be incremented for each successfully
             received MMPDU of type Data"
        ::= { dot11GASAdvertisementEntry 12 }


dot11GASTransmittedMSDUCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
              "This counter shall be incremented for each successfully
              transmitted MMPDU."
      ::= { dot11GASAdvertisementEntry 13 }


dot11GASDiscardedMSDUCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
              "This counter shall be incremented for each Discarded MMPDU."
      ::= { dot11GASAdvertisementEntry 14 }


dot11GASRetriesReceivedCount OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "This counter shall increment for each received MMPDU."
        ::= { dot11GASAdvertisementEntry 15 }


dot11GASResponseTimeout OBJECT-TYPE
        SYNTAX INTEGER (1000..65535)
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
              "This parameter shall indicate the GAS response timeout value
              in TUs."
        DEFVAL {5000)
      ::= { dot11GASAdvertisementEntry 16 }
```

```
dot11GASComebackDelay OBJECT-TYPE
        SYNTAX INTEGER (0..65535)
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "This object identifies the GAS Comeback Delay (in TUs) to be
                used for this Advertisement Protocol"
        DEFVAL {1000}
        ::= { dot11GASAdvertisementEntry 17 }


dot11GASQueryResponseLengthLimit OBJECT-TYPE
        SYNTAX INTEGER (1..127)
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "This object indicates the maximum number of octets an AP
                will transmit in one or more Query Response fields contained
                within GAS Comeback Response  Action frame(s). A value of 127
                means the maximum limit enforced is  contained by the maximum
                allowable number of fragments in the GAS Query  Fragment
                Response ID"
        ::= { dot11GASAdvertisementEntry 18}



-- **********************************************************************
-- * End of dot11GASAdvertisement TABLE
-- **********************************************************************

-- **********************************************************************
-- * MAC State Generic Convergence
-- **********************************************************************

-- MAC State Generic Convergence Function attributes
   -- DEFINED AS "The MAC state generic convergence function object
   -- class provides the necessary support for support of event-driven
   -- triggers to higher-layer protocols and the capabilities to
   -- support those triggers."



dot11MSGCF OBJECT IDENTIFIER ::= { ieee802dot11 7}

      -- MAC State GROUPS
      -- dot11MACStateConfigTable ::= { dot11MSGCF 1 }
      -- dot11MACStateParameterTable ::= { dot11MSGCF 2 }
      -- dot11MACStateESSLinkTable ::= { dot11MSGCF 3 }

-- *********************************************************************
-- * dot11ESSLinkIdentifier type definition
-- *********************************************************************


Dot11ESSLinkIdentifier ::== OCTET STRING (SIZE(0..38))
   -- This object type holds the identifier for an 802.11
   -- network. It is composed of the SSID string concatenated
   -- with the HESSID, if present.
-- **********************************************************************
-- * dot11MACStateConfig TABLE
-- **********************************************************************


dot11MACStateConfigTable OBJECT-TYPE
        SYNTAX SEQUENCE OF Dot11MACStateConfigEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
             “This table holds configuration parameters for the 802.11 MAC
             State Convergence Function.”
        ::= { dot11MSGCF 1 }


dot11MACStateConfigEntry OBJECT-TYPE
        SYNTAX Dot11MACStateConfigEntry
        MAX-ACCESS not-accessible
        STATUS     current
        DESCRIPTION
             “Each entry represents a conceptual row in the
             dot11MACStateConfigTable and provides information about network
             configuration parameters used in the MAC State Generic
             Convergence Function.”
        INDEX { dot11ESSLinkIdentifier, dot11NonAPStationMacAddress }
        ::= { dot11MACStateConfigTable 1 }


Dot11MACStateConfigEntry ::=
        SEQUENCE {
             dot11ESSDisconnectFilterInterval INTEGER,
             dot11ESSLinkDetectionHoldInterval INTEGER
             }


dot11ESSDisconnectFilterInterval OBJECT-TYPE
        SYNTAX INTEGER
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
             “This attribute is set to the number of time units (TUs) that
             will elapse after an MLME-Disassociate.confirm or MLME-
             Deauthentication.confirm primitive without a subsequent
             association before the link is declared down. This interval is
             intended to allow a non-AP STA time to transition to another AP
             within the same ESS before declaring that the link to the ESS
             is lost.”
        ::= { dot11MACStateConfigEntry 1}


dot11ESSLinkDetectionHoldInterval OBJECT-TYPE
        SYNTAX INTEGER
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
             “This attribute is set to the number of time units (TUs) that
             an ESS is held in the dot11MACStateESSLink table after its last
             observation before purging the entry from the table.”
        ::= { dot11MACStateConfigEntry 2}
```

```
-- **********************************************************************
-- * End of dot11MACStateConfig TABLE
-- **********************************************************************



-- **********************************************************************
-- * dot11MACStateParameter TABLE
-- **********************************************************************


dot11MACStateParameterEntry OBJECT-TYPE
        SYNTAX          SEQUENCE OF Dot11MACStateParameterEntry
        MAX-ACCESS      not-accessible
        STATUS          current
        DESCRIPTION
              "This table holds the current parameters used for each 802.11
              network for 802.11 MAC convergence functions."
        ::= { dot11MSGCF 2 }


dot11MACStateParameterTable OBJECT-TYPE
        SYNTAX Dot11MACStateParameterEntry
        MAX-ACCESS not-accessible
        STATUS     current
        DESCRIPTION
              "Each entry represents a conceptual row in the
              dot11MACStateParameterTable and provides information about link
              configuration parameters used in the MAC State Generic
              Convergence Function."
        INDEX { dot11ESSLinkIdentifier, dot11NonAPStationMacAddress }
        ::= { dot11MACStateParameterTable 1 }



Dot11MACStateParameterEntry ::=
        SEQUENCE {
              dot11ESSLinkIndex Unsigned32,
              dot11ESSLinkDownTimeInterval Unsigned32,
              dot11ESSLinkRssiDataThreshold Unsigned32,
              dot11ESSLinkRssiBeaconThreshold Unsigned32,
              dot11ESSLinkDataSnrThreshold Unsigned32,
              dot11ESSLinkBeaconSnrThreshold Unsigned32,
              dot11ESSLinkBeaconFrameErrorRateThreshold Unsigned32,
              dot11ESSLinkBeaconFrameErrorRateThresholdFraction Unsigned32,
              dot11ESSLinkBeaconFrameErrorRateThresholdExponent Unsigned32,
              dot11ESSLinkBitErrorRateThresholdUnsigned32 Unsigned32,
              dot11ESSLinkBitErrorRateThresholdFraction Unsigned32,
              dot11ESSLinkBitErrorRateThresholdExponent Unsigned32,
              dot11PeakOperationalRate Unsigned32,
              dot11MinimumOperationalRate Unsigned32,
              dot11ESSLinkDataThroughputInteger Unsigned32,
              dot11ESSLinkDataThroughputFraction Unsigned32,
              dot11ESSLinkDataThroughputExponent Unsigned32
              }


dot11ESSLinkIndex OBJECT-TYPE
        SYNTAX Unsigned32
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
             “Index for ESS Link elements in dot11ESSLinkTable, greater than
             0."
        ::= { dot11MACStateParameterEntry 1 }


dot11ESSLinkDownTimeInterval OBJECT-TYPE
        SYNTAX Unsigned32
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
             “This attribute defines the desired time interval that the MAC
             State Generic convergence function will attempt to predict the
             failure of an 802.11 network in time units (TUs). The
             convergence function should issue predicted network failure
             events at least this time interval before the network failure
             is detected.”
        ::= { dot11MACStateParameterEntry 2}


dot11ESSLinkRssiDataThreshold OBJECT-TYPE
        SYNTAX Unsigned32
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
             “This attribute defines the threshold value for RSSI on Data
             frames. When the RSSI drops below this threshold, a report is
             issued.”
        ::= { dot11MACStateParameterEntry 3}


dot11ESSLinkRssiBeaconThreshold OBJECT-TYPE
        SYNTAX Unsigned32
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
             “This attribute defines the threshold value for RSSI on Beacon
             frames. When the RSSI drops below this threshold, a report is
             issued.”
        ::= { dot11MACStateParameterEntry 4}


dot11ESSLinkBeaconSnrThreshold OBJECT-TYPE
        SYNTAX Unsigned32
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
             “This attribute defines the threshold value for SNR on received
             Beacon frames. When the SNR drops below this threshold, a
             report is issued”
        ::= { dot11MACStateParameterEntry 5}


dot11ESSLinkDataSnrThreshold OBJECT-TYPE
        SYNTAX Unsigned32
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
```

```
          "This attribute defines the threshold value for SNR on received
          Data frames. When the SNR drops below this threshold, a report
          is issued."
     ::= { dot11MACStateParameterEntry 6}


dot11ESSLinkBeaconFrameErrorRateThresholdInteger OBJECT-TYPE
     SYNTAX Unsigned32
     MAX-ACCESS read-write
     STATUS current
     DESCRIPTION
          "The Beacon frame error rate is stored in scientific notation
          as a significant and exponent. This attribute contains the
          integer value of the significand."
     ::= { dot11MACStateParameterEntry 7}


dot11ESSLinkBeaconFrameErrorRateThresholdFraction OBJECT-TYPE
     SYNTAX Unsigned32
     MAX-ACCESS read-write
     STATUS current
     DESCRIPTION
          "The Beacon frame error rate is stored in scientific notation
          as a significant and exponent. This attribute contains the
          fractional value of the significand."
     ::= { dot11MACStateParameterEntry 8}


dot11ESSLinkBeaconFrameErrorRateThresholdExponent OBJECT-TYPE
     SYNTAX Unsigned32
     MAX-ACCESS read-write
     STATUS current
     DESCRIPTION
          "The Beacon frame error rate is stored in scientific notation
          as a significant and exponent. This attribute contains the
          integer value of the exponent."
     ::= { dot11MACStateParameterEntry 9}


dot11ESSLinkBitErrorRateThresholdInteger OBJECT-TYPE
     SYNTAX Unsigned32
     MAX-ACCESS read-write
     STATUS current
     DESCRIPTION
          "The bit error rate is of the network is stored in scientific
          notation as a significant and exponent. This attribute contains
          the integer value of the significand."
     ::= { dot11MACStateParameterEntry 10}


dot11ESSLinkBitErrorRateThresholdFraction OBJECT-TYPE
     SYNTAX Unsigned32
     MAX-ACCESS read-write
     STATUS current
     DESCRIPTION
          "The bit error rate is of the network is stored in scientific
          notation as a significant and exponent. This attribute contains
          the fractional value of the significand."
     ::= { dot11MACStateParameterEntry 11 }
```

```
dot11ESSLinkBitErrorRateThresholdExponent OBJECT-TYPE
        SYNTAX Unsigned32
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
             “The bit error rate is of the network is stored in scientific
             notation as a significant and exponent. This attribute contains
             the integer value of the exponent.”
        ::= { dot11MACStateParameterEntry 12 }


dot11PeakOperationalRate OBJECT-TYPE
        SYNTAX Unsigned32
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
             “The highest operational rate used for transmission of data
             frames, encoded as defined in 7.3.2.2."
        ::= { dot11MACStateParameterEntry 13 }


dot11MinimumOperationalRate OBJECT-TYPE
        SYNTAX Unsigned32
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
             “The lowest operational rate used for transmission of data
             frames, encoded as defined in 7.3.2.2.”
        ::= { dot11MACStateParameterEntry 14 }


dot11ESSLinkDataThroughputInteger OBJECT-TYPE
        SYNTAX Unsigned32
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
             “The data throughput rate is of the network is stored in
             scientific notation as a significant and exponent. This
             attribute contains the integer value of the significand.”
        ::= { dot11MACStateParameterEntry 15 }


dot11ESSLinkDataThroughputFraction OBJECT-TYPE
        SYNTAX Unsigned32
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
             “The data throughput rate is of the network is stored in
             scientific notation as a significant and exponent. This
             attribute contains the fractional value of the significand.”
        ::= { dot11MACStateParameterEntry 16 }


dot11ESSLinkDataThroughputExponent OBJECT-TYPE
        SYNTAX Unsigned32
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
```

```
             “The data throughput rate is of the network is stored in
             scientific notation as a significant and exponent. This
             attribute contains the integer value of the exponent.”
        ::= { dot11MACStateParameterEntry 17 }


-- *********************************************************************
-- * End of dot11MACStateParameter TABLE
-- *********************************************************************


-- *********************************************************************
-- * dot11MACStateESSLink TABLE
-- *********************************************************************


dot11MACStateESSLinkDetectedTable OBJECT-TYPE
        SYNTAX         SEQUENCE OF Dot11MACStateESSLinkEntry
        MAX-ACCESS     not-accessible
        STATUS         current
        DESCRIPTION
             “This table holds the detected 802.11 network list used for MAC
             convergence functions.”
    ::= { dot11MSGCF 3}


dot11MACStateESSLinkDetectedEntry OBJECT-TYPE
        SYNTAX               Dot11MACStateESSLinkDetectedEntry
        MAX-ACCESS not-accessible
        STATUS     current
        DESCRIPTION
             “Each entry represents a conceptual row in the
             dot11MACStateESSLinkTable and provides information about
             available networks for use in the MAC State Generic Convergence
             Function.”
        INDEX { dot11ESSLinkIdentifier, dot11NonAPStationMacAddress }
        ::= { dot11MACStateESSLinkDetectedTable 1 }


dot11MACStateESSLinkDetectedEntry ::=
        SEQUENCE {
             dot11ESSLinkDetectedIndex Unsigned32,
             dot11ESSLinkDetectedNetworkId OCTET STRING,
             dot11ESSLinkDetectedBssidList SEQUENCE OF MacAddress,
             dot11ESSLinkDetectedNetworkDetectTime Unsigned32,
             dot11ESSLinkDetectedNetworkModifiedTime Unsigned32,
             dot11ESSLinkDetectedNetworkMIHCapabilities BITS
             }


dot11ESSLinkDetectedIndex OBJECT-TYPE
        SYNTAX Unsigned32
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
             "Index for ESSLinkDetected elements in
             dot11ESSLinkDetectedTable, greater than 0."
        ::= { dot11MACStateESSLinkDetectedEntry 1 }
```

```
dot11ESSLinkDetectedNetworkId OBJECT-TYPE
        SYNTAX OCTET STRING
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "The string used to identify the network represented by this
             row in the table. It is composed of the SSID of the network
             concatenated with the HESSID, if present."
        ::= { dot11MACStateESSLinkDetectedEntry 2}


dot11ESSLinkDetectedBssidList OBJECT-TYPE
        SYNTAX SEQUENCE OF MacAddress
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "The list of BSSIDs currently detected which are advertisement
             the network described by this row in the table."
        ::= { dot11MACStateESSLinkDetectedEntry 3}


dot11ESSLinkDetectedNetworkDetectTime OBJECT-TYPE
        SYNTAX Unsigned32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "The STA's TSF timer when any BSSID supporting the network was
             first detected."
        ::= { dot11MACStateESSLinkDetectedEntry 4}


dot11ESSLinkDetectedNetworkModifiedTime OBJECT-TYPE
        SYNTAX Unsigned32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
             "The STA's TSF timer value when changes were made to any part
             of this row in the table, such as by addition of a BSSID to the
             BSSID list."
        ::= { dot11MACStateESSLinkDetectedEntry 5}


dot11ESSLinkDetectedNetworkMIHCapabilities OBJECT-TYPE
        SYNTAX     BITS {
              mihIsSupport(0),
              mihCsEsSupport(1)
              }
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
             "The object reports whether the network supports 802.21 MIH
             information services and/or 802.21 MIH command/event services.
             These values are determined by examining the Interworking
             information in frames that caused the network to be detected."
        ::= { dot11MACStateESSLinkDetectedEntry 6}

-- *********************************************************************
-- * End of dot11MACStateESSLink TABLE
-- *********************************************************************
```

Annex K

(informative)

Admission Control

K.2 Recommended practices for contention-based admission control

K.2.1 Use of ACM (admission control mandatory) subfield

Change the text of K.2.1 as follows

It is recommended that admission control not be required for the access categories AC_BE and AC_BK. The ACM subfield for these categories should be set to 0. The AC parameters chosen by the AP should account for unadmitted traffic in these ACs.

When dot11SSPNInterfaceEnabled is true, it is recommended that any STA authenticated through an SSPN interface use admission control to access categories AC_VO and AC_VI to ensure network utilization consistent with the policy imposed by the SSPN for admission. AC parameters chosen by the AP should further account for any unadmitted traffic in AC_VO and AC_VI that may be reserved for users of a particular SSPN.

K.3 Guidelines and reference design for sample scheduler and admission control unit

K.3.1 Guidelines for deriving service schedule parameters

Insert the following paragraph at the end of K.3.1:

When dot11SSPNInterfaceEnabled is true, the HC polices all traffic flows from a non-AP STA authenticated against the maximum authorized data rates stored in the dot11InterworkingTable. Each SSPN-authenticated STA is given a maximum bandwidth allowance by the SSPN for each access category as well as scheduled access. The AP polices the SSPN-authenticated STA traffic flows to the maximum bandwidth allowance provided by the SSPN.

Annex P

(Informative)

Bibliography

P.1 General

Insert the following entries in P.1, renumbering as necessary

[B38] 3GPP IMS emergency sessions architecture: http://www.3gpp.org/ftp/Specs/html-info/23167.htm.

[B39] 3GPP TR 21.905, Vocabulary for 3GPP Specifications.

[B40] 3GPP TS 22.067: Enhanced Multi-Level Precedence and Pre-emption service (EMLPP); Stage 1.

[B41] 3GPP2 IMS emergency sessions architecture: http://www.3gpp2.org/Public_html/specs/X.S0060-0_v1.0_080729.pdf.

[B42] Extended ECRIT architecture supporting unauthenticated emergency services: http://www.ietf.org/internet-drafts/draft-schulzrinne-ecrit-unauthenticated-access-01.txt.

[B43] GSMA, IR.34 v4.6, Inter-Service Provider IP Backbone Guidelines, http://gsmworld.com/documents/IR3446.pdf, April 2009.

[B44] IETF RFC 1334, PPP Authentication Protocols, B. Lloyd, W. Simpson, October 1992

[B45] IETF RFC 1994, PPP Challenge Handshake Authentication Protocol (CHAP), W. Simpson, August 1996

[B46] IETF RFC 2433, Microsoft PPP CHAP Extensions, G. Zorn, S. Cobb, October 1998 (status: informational).

[B47] IETF RFC 2759, Microsoft PPP CHAP Extensions, Version 2, G. Zorn, January 2000 (status: informational).

[B48] IETF RFC 2903, Generic AAA architecture, C. de Laat, G. Gross, L. Gommans, J. Vollbrechtm and D. Spence, August 2000 (status informational).

[B49] IETF RFC 3580, IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines, P. Congdon, B. Aboba, A. Smith, G. Zorn, and J. Roese, Sept 2003.

[B50] IETF RFC 4776, Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information, H. Schulzrinne, November 2006.

[B51] IETF RFC 5139, Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO), M. Thomson, February 2008.

[B52] International Code Council, Inc., “International Building Code 2006”, November 2006, ISBN-13: 978-1-58001-251-5.

[B53] ISO 639, Codes for the Representation of Names of Languages.

[B54] ISO 14962:1997, Space data and information transfer systems - ASCII encoded English.

[B55] NENA 08-002, Functional and Interface Standards for Next Generation 9-1-1 (i3), Version 1.0, http://www.nena.org/standards/technical/voip/functional-interface-NG911-i3.

Insert the following annex to the proper sequence of annexes:

Annex W

(informative)

Interworking with External Networks

The purpose of this informative annex is to describe and clarify the support for Interworking with External Networks including the support for Network Discovery and Selection, QoS mapping, SSPN interface and Emergency Services, providing some background information and recommended practices.

W.1 Network Discovery and Selection

Interworking Service provides features to support the network discovery and selection process a STA uses to choose the network with which to associate. Generic Advertisement Service (GAS) provides a non-AP STA access to an information server (e.g. an IEEE 802.21 IS) which can provide a rich set of information to aid the network discovery and selection process. In addition, Interworking Service provides lightweight features which also facilitate this process. The following paragraphs describe several use cases illustrating how these features can be used to aid in network discovery and selection. The use cases are:

- **Airport:** A business traveler needs to connect via an airport hotspot to his/her enterprise network to download email and information from the customer database.
- **Shopping:** A shopper visits a shopping mall and wants to use his/her smartphone to discover items on sale.
- **Sales meeting:** A sales representative visiting a customer accesses his/her guest network.
- **Museum:** A visitor to a museum uses a smartphone to obtain virtual docent service.

W.1.1 Airport

A business traveler arrives for the first time into an airport having a WLAN. The user wants to download email onto their laptop utilizing the airport’s hotspot, a chargeable network. Once associated, the user needs to connect via VPN connection back to their company’s servers to access email and information from the customer database.

1) The laptop’s non-AP STA performs an active scan by transmitting a Probe Request frame containing the wildcard SSID and an Interworking element with Network Type subfield set to “Chargeable Public Network”. In response, it receives Probe Response frames from several of the airport’s APs, in the immediate neighborhood, for the SSID “Narita Hotspot”.
2) The Probe Response received by the laptop indicated the following capabilities:
    a) Extended capabilities element indicates: AP provides Interworking Service.
    b) Interworking element indicates: venue group = 1 (Assembly) and 802.11 Venue Type = 3 (passenger terminal), Internet = 1 (Internet access available), ASRA = 1 (there is an additional step required for network access).
    c) Advertisement Protocol element indicating AP supports Non-Native GAS for IEEE 802.21-IS.
    d) Roaming Consortium element present containing an OI for “Hotspot Roaming International”.
    e) There is no RSN element present in the received beacon frame.

3) Since the laptop's SME does not recognize the Roaming Consortium OI, it invokes the GAS protocol to query the network's IEEE 802.21-IS. The IEEE 802.21-IS's response indicates the roaming partners for "Narita Hotspot" and the laptop has security credentials for one of them.

4) Since the AP indicated ASRA = 1, the SME again invokes the GAS protocol to retrieve the Network Authentication Type information. The response indicates that https redirection is in use and provides the Re-direct URL of "hotspot.narita.co.jp". Note that this is helpful since some networks use conditional re-direction—that is, access to a walled garden is provided for free, but a subscription fee is required to access the Internet.

5) Since the Laptop's SME now knows it should be able to successfully authenticate with the network, the STA associates to the AP.

6) The following operations are then carried out by higher layers operating within the laptop:

    a) The laptop's SME autonomously launches an http client providing to it the URL of hotspot.narita.co.jp which provides the proper security credentials to the network, thereby successfully authenticating it to the network.

    b) The VPN client is autonomously launched, establishing a secure session to user's corporate network. Then the user launches the email application to download email and other required information.

W.1.2 Shopping

A shopper visits a shopping mall and wants to use a smartphone to discover items on sale. In this mall, the mall's IT department is providing WLAN facilities for all the stores in the mall, so there is only one SSID for shoppers (i.e., there is not a different SSID for each store in the mall). The user arrives at the mall and taps an icon on the screen to put the smartphone in "shopping mode". The smartphone's shopping application causes the non-AP STA to carry out the following steps:

1) The smartphone's non-AP STA performs an active scan by transmitting a Probe Request frame containing the wildcard SSID and an Interworking element with Network Type subfield set to "Free Public Network". In response, it receives Probe Response frames from several of the mall's APs, but only one SSID is provided which is "Silicon Valley Mall". The mall's APs did not transmit Probe Responses for the SSIDs "Engineering", "Deliveries" and "Janitorial" since their Network Type is "Private network".

2) The Probe Response received by the smartphone indicated the following capabilities:

    a) Extended capabilities element indicates: AP provides Interworking Service.

    b) Interworking element indicates: venue group = 6 (mercantile) and 802.11 Venue Type = 4 (shopping mall), Internet = 0 (unspecified).

    c) RSN element indicates: IEEE 802.1X authentication.

3) Since the AP indicated Interworking service is available, the smartphone's non-AP STA use the MLME-GAS.request primitive to invoke Native GAS to request the Capabilities List (see 7.3.4.1). In the Capabilities List, the AP has indicated support for Venue Name and Domain Name List. Subsequent to receipt of the Capabilities List, the non-AP STA invokes the MLME-GAS.request primitive to retrieve the other two lists.

4) Next, the non-AP STA's supplicant searches the received Domain Name list to determine whether it has any stored credentials for these domains. If so:

    a) The smartphone autonomously associates to the "Silicon Valley Mall Shopping" SSID and displays the information shown below:

        i) Venue Name: Silicon Valley Mall, 1234 Main Street, Rownhams, CA 98765-1234

        ii) SSID: Silicon Valley Mall

        iii) 802.11 Venue type: Shopping Mall

b) The supplicant autonomously provides the security credentials for the selected domain.

5) Higher-layer protocols then download discount coupons being offered for items on sale.

W.1.3 Sales Meeting

A sales person travels across town to a meeting at ACME manufacturing. While there, the sales person needs to send email to get a document from engineering. On a laptop, the user requests the WLAN via the laptop's UI to search for guest networks. The laptop performs steps described in the following bullets.

1) The laptop's non-AP STA performs an active scan by transmitting a Probe Request frame containing the wildcard SSID and an Interworking element with Network Type subfield set to "Private Network with Guest Access". In response, it receives Probe Response frames from several of ACME Manufacturing's APs, but only one SSID is provided which is "Guest". ACME Manufacturing's APs did not transmit Probe Responses for the SSIDs "Engineering" and "Finance" since their Network Type is "Private network".

2) The Probe Response received by the laptop indicated the following capabilities:

   a) Extended capabilities element indicates: AP provides Interworking Service

   b) Interworking element indicates: Internet is available, venue group = 2 (Business) and 802.11 Venue Type = 8 (Research and Development Facility).

   c) RSN element indicates: IEEE 802.1X authentication with CCMP pairwise and group cipher suites.

3) Since the AP indicated Interworking service is available, the laptop's non-AP STA uses the MLME-GAS.request primitive to invoke Native GAS to request the Capabilities List (see 7.3.4.1). In the Capabilities List, the AP has indicated support for Venue Name. Upon receipt of the Capabilities List, the non-AP STA again invokes the MLME-GAS.request primitive to retrieve the Venue Name.

4) The laptop's UI displays the following information, and automatically associates to the network:

   a) SSID: Guest (Type: Private network with Guest access)

   b) Venue Name: ACME Manufacturing, 1234 Main Street, Rownhams, CA 98765-1234

   c) 802.11 Venue Type: Research and Development Facility

   d) Internet is available

5) Upon prompt, the user enters the username and password supplied by their point of contact from ACME Manufacturing and is then able to send and receive email.

W.1.4 Museum

A visitor enters a Museum which is advertising virtual docent service (audio tracks describing each of the major exhibits). The visitor taps an icon on a smartphone, requesting it to search for free networks. The smartphone then carries out the following:

1) The smartphone's non-AP STA performs an active scan by transmitting a Probe Request frame containing the wildcard SSID and an Interworking element with Network Type subfield set to "Free Public Network". In response, it receives Probe Response frames from several of the museums APs, but only one SSID is provided which is "Visitors". The museum's APs did not transmit Probe Responses for the SSID "Maintenance" since its Network Type is "Private network".

2) The Probe Response received by the smartphone indicated the following capabilities:

   a) Extended capabilities element indicates: AP provides Interworking Service

   b) Interworking element indicates: venue group = 1 (assembly), 802.11 Venue Type = 9 (museum), and ASRA = 0 (no additional steps are required for access)

3) Since the AP indicated Interworking service is available, the smartphone's non-AP STA use the MLME-GAS.request primitive to invoke Native GAS to request the Capabilities List (see 7.3.4.1). In the Capabilities List, the AP has indicated support for Venue Name. Upon receipt of the Capabilities List, the non-AP STA again invokes the MLME-GAS.request primitive to retrieve the Venue Name.

4) The smartphone's UI displays the following information, asking the users whether or not they wish to connect to the network:

   a) Venue Name: Museum of Modern Art (MOMA)

   b) SSID: Visitors

   c) 802.11 Venue Type: Museum

   d) No authentication required

5) The user taps the "Connect" icon on the smartphone's display. Note that the smartphone's non-AP STA knows that the network uses open system authentication since there is no RSN element present in the beacon and ASRA = 0.

W.2 QoS Mapping Guidelines for Interworking with External Networks

The EDCA and HCCA mechanism defined in 9.9 provide QoS control at the MAC layer. However, the QoS control parameters used by the EDCA and HCCA can not match directly with other QoS control parameters of the interworked external networks, e.g., SSPN. For example, the SSPN could have different metrics for defining the QoS levels. Destination Network 1 (DN1) and DN2 can use DSCP values differently, in which case, STA1 and STA2 would require different QoS mapping information. Therefore, mapping from these external QoS control parameters to the QoS parameters of this standard is necessary.

The QoS parameters mapping can be used for both uplink and downlink data transmission:

- For uplink: at the non-AP STA, external QoS parameters are mapped to IEEE 802.11 QoS parameters, e.g., DSCP to IEEE 802.11 User Priority and in turn to EDCA ACs. This mapping helps the non-AP STA to construct correct QoS requests to the AP, e.g., ADDTS Request and to transmit frames at the correct priority.
- For downlink: at the AP, DSCP values are mapped to EDCA UPs. Optionally, the non-AP STA can use TSPEC and TCLAS elements in an ADDTS Request frame to setup a traffic stream in the BSS. In this method, the User Priority is specified in the TCLAS element. The policy used by the AP to choose a specific method to map frames to user priorities is outside the scope of 802.11.

Different external networks can use different DSCP sets for the same services as described in Annex W.2.2. For example, a 3GPP network can use different code points from that of an enterprise network. The QoS Map distribution mechanism defined in 11.23.7 provides means to communicate to the STA's mapping information from the network.

W.2.1 Determination of the mapping for a STA

The QoS mapping to be applied depends upon the network the non-AP STA is accessing. In an interworking IEEE 802.11 infrastructure setting, the same physical AP can serve non-AP STAs from different SSPNs on different BSSIDs. As such, these STAs are separated into different BSSs. Figure W-1 presents an example of the scenario. In Figure W-1, AAA Server 1 controls access to DN-1 and AAA Server 2 controls access to DN-2.

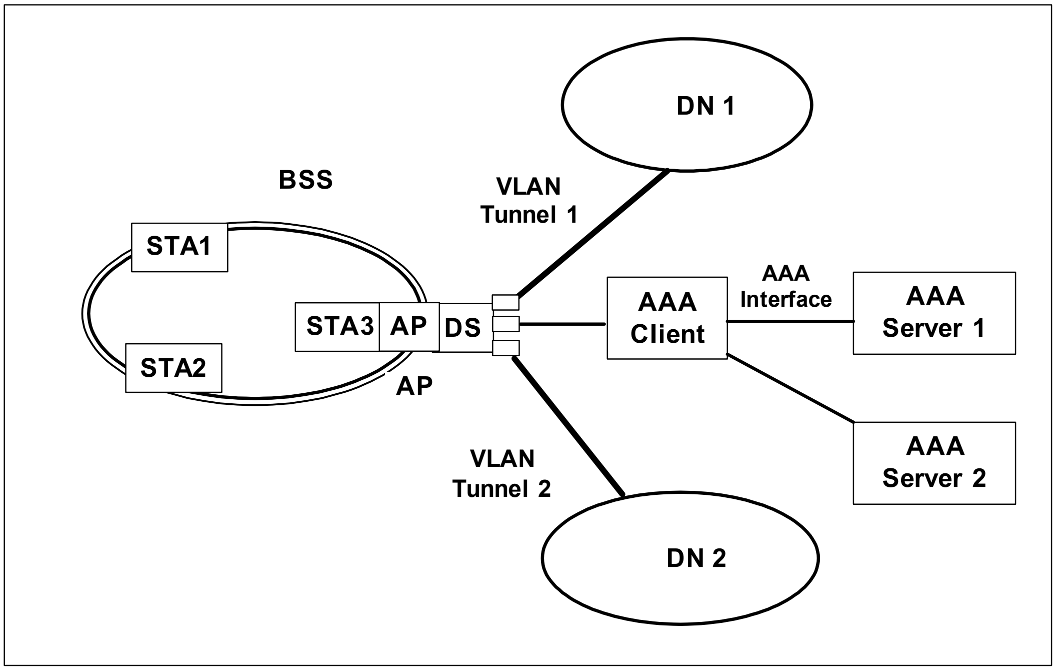

Figure W-1—Interworking IEEE 802.11 infrastructure supporting multiple SSPNs

W.2.2 Example of QoS Mapping from different networks

IEEE 802.1d UPs map to EDCA ACs, as described in Table 9-1 UP-to-AC mappings. The use of DSCP sets differs from network to network. Table W-1 shows examples of DCSP mappings.

Table W-1—Mapping Table of DSCP to 3GPP QoS Info and EDCA ACs

3GPP QoS Information		**DiffServ PHB**	**DSCP**	**QoS Requirement on GRX**				**EDCA Access Category**	**UP (as in 802.1d)**
Traffic Class	THP			Max Delay	Max Jitter	MSDU Loss	MSDU Error Ratio		
Conversational	N/A	EF	101110	20 ms	5 ms	0.5%	10^{-6}	AC_VO	7, 6
Streaming	N/A	$AF4_1$	100010	40 ms	5 ms	0.5%	10^{-6}	AV_VI	5, 4
Interactive	1	$AF3_1$	011010	250 ms	N/A	0.1%	10^{-8}	AC_BE	3
	2	$AF2_1$	010010	300 ms	N/A	0.1%	10^{-8}	AC_BE	3
	3	$AF1_1$	001010	350 ms	N/A	0.1%	10^{-8}	AC_BE	0
Background	N/A	BE	000000	400 ms	N/A	0.1%	10^{-8}	AC_BK	2,1

NOTE—The mapping of the DSCP to 3GPP Traffic Class is available in GSMA, IR.34 v4.6 [B43] (similar to that of GSMA IREG34). See TR 21.905 [B39] for definition of GRX. The Table W-1 is extended to cover the EDCA ACs mapping. This mapping can also apply to other networks that adopt the 3GPP QoS definitions, e.g., 3GPP2.

Table W-2—Example Enterprise DSCP to UP/AC mapping

Application Class	PHB	802.1d User Priority	Access Category
Network Control	CS6	7	AC_VO
Telephony	EF	6	AC_VO
RT Interactive	CS4	6	AC_VO
Multimedia Conference	AF4x	5	AC_VI
Signaling	CS5	5	AC_VI
Broadcast Video	CS3	4	AC_VI
Multimedia Stream	AF3x	4	AC_VI
Low Latency Data	AF2x	3	AC_BE
High Throughput Data	AF1x	2	AC_BE
OAM	CS2	2	AC_BE
Standard	DF	0	AC_BE
Low Priority/Background	CS1	1	AC_BK

Table W-2 shows an example mapping based on application classes defined in RFC 4594. Mapping between DSCP and UP can be done using Exception fields or by range. The use of Exception fields will map a DSCP to a UP according to Table W-2. Mapping by range will require the setting of DSCP ranges as shown in Table W-3.

Table W-3—UP to DSCP Range Mapping example

UP Range	DSCP Low	DSCP High
UP 0 Range	0	0
UP 1 Range	1	9
UP 2 Range	10	16
UP 3 Range	17	23
UP 4 Range	24	31
UP 5Range	32	40
UP 6Range	41	47
UP 7Range	48	63

Furthermore mapping by range will require an additional exceptional element to map DSCP 32 to UP 6.

NOTE—21 Exception fields are provided to give more flexibility in defining the QoSMap and it is currently the number of PHBs defined by the IETF.

W.3 Interworking and SSPN Interface Support

The Interworking Service architecture defines the scope of the SSPN interface. This interface is provided by the IEEE 802.11 MAC to support the Interworking Service. In an interworking scenario, the IEEE 802.11 infrastructure is operating in infrastructure mode.

Figure W-2 shows an example implementation of the control aspect of the Interworking Interface. As shown in the figure, the Interworking Interface consists of two parts: the generic SSPN Interface between the AP and the AAA Client; and the AAA Interface between the AAA Client and the corresponding AAA Server in the SSPN. Depending on the implementation the AAA Client can be co-located with the AP or stand alone serving as a proxy or translation agent between the SSPN Interface and AAA Interface. The AAA Interface serves as a transparent carrier of the SSPN interface.

The possible interactions over the SSPN interface are defined in 11.23.4. The information transferred over the SSPN Interface is defined in Annex W.3.1. This interface results in parameters being set in the dot11InterworkingTable MIB. The AP's SME thereafter uses these parameters to permit or deny, as appropriate, services to non-AP STAs.

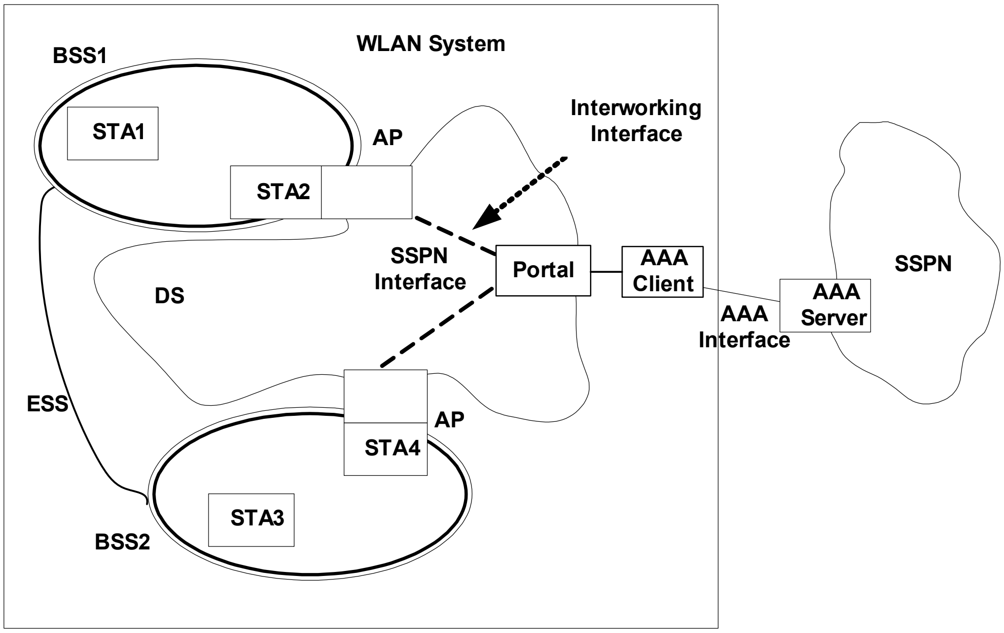

Figure W-2—Basic Architecture of the Interworking Service

W.3.1 SSPN Interface Parameters

The parameters for each associated non-AP STA defined in this clause cross the SSPN Interface, i.e. between AP and AAA Client as shown in Table W-3.

Table W-3—SSPN Interface information or permission parameters

Information or Permission Name	From AN to SSPN	From SSPN to AN	Per non-AP STA Entry
Non-AP STA MAC	+		+
Non-AP STA User ID	+	+	+
Non-AP STA Interworking Capability	+		+
Link Layer Encryption Method	+		+
Authorized Priority		+	+
Authorized Rate		+	+
Authorized Delay		+	+
Authorized Service Access Type		+	+
Authorized Service Access Information		+	+
non-AP STA Transmission Count	+		+
non-AP STA Location Information	+		+
non-AP STA state Information	+		+

The SSPN Interface parameters are stored in the AP with corresponding MIB attributes as defined in Annex D, and are used by the Interworking Service Management function in the SME. The MIB variables themselves, which are used by the APs SME, are read only.

W.3.1.1 Non-AP STA MAC

This is the MAC address of the non-AP STA accessing the interworking service through the AP. It can be requested by the external network, e.g., a 3GPP network, for fraud prevention. The non-AP STA MAC address is normally available through MLME-SAP, e.g., MLME-ASSOCIATE.indication, and should be forwarded by the AS to the AAA server entity in the SSPN through the AAA Interface.

The AP stores the non-AP STA MAC address in the corresponding dot11NonAPStationMacAddress element of its MIB.

W.3.1.2 Non-AP STA User ID

This parameter contains the subscriber information of the non-AP STA for the Interworking Service. It is provided by the non-AP STA through the RSNA establishment process to the AAA server; in turn, the AAA server provides it back to the AP via the SSPN interface. It is in the form of a NAI, i.e. it contains both the user's identity and its SSP information.

NOTE—The reason the AAA server provides the user identity back to the AP is that some EAP methods use encrypted tunnels to maintain confidentiality of the user and thus the AP might not otherwise be able to learn the user's identity.

The AP stores the associated non-AP STA User ID in the corresponding dot11NonAPStationUserIdentity element of its MIB.

W.3.1.3 Non-AP STA Interworking Capability

This parameter is derived from the non-AP STA's extended capabilities element, which is included in (re)association request frames.The AP SME obtains this information from the MLME-SAP, e.g., MLME-ASSO-

CIATE.indication. This information needs to be passed over the SSPN interface since the service authorization decisions can depend on the non-AP STA capabilities.

The AP stores the associated non-AP STA Interworking Capability in the corresponding dot11NonAPStationInterworkingCapability element of its MIB.

W.3.1.4 Link Layer Encryption Method

This parameter indicates the link layer encryption method selected during the RSNA establishment process for protecting the unicast communication between the non-AP STA and the AP. The cipher suite format of this element is drawn from the RSN information element defined in clause 7.3.2.25. AP obtains this information about the STA via the MLME SAP.

In the Interworking Service, the SSPN also participates in the selection of the cipher suite selection, as described in 11.23.4. Therefore, the link layer encryption method selected will meet or exceed the security requirement of the SSPN.

NOTE—In interworking, the SSPN can require visibility and configurability of the STA access.

With this information available to the SSPN, the operator would be able to have better control, e.g., barring access to IEEE 802.11 networks if null encryption is used. This is also related to the operator network's configuration, e.g., if pre-authentication should be supported.

The AP stores the information in the corresponding dot11NonAPStationCipherSuite element of its MIB.

W.3.1.5 Authorized Priority

This parameter is used for admission control and user-priority policing at the AP. It is based on the Infrastructure Authorization Information delivered from the SSPN during the AAA procedure. The Authorized Priority specifies the authorized User Priorities that the non-AP STA is allowed to use during the Interworking access. It also specifies whether the non-AP STA can use HCCA.

For EDCA operation, the AP stores the information in its corresponding dot11NonAPStationAuthAccessCategories element of its MIB after mapping the priority according to Table 9-1. For HCCA operation, the AP stores the information in dot11NonAPStationAuthHCCAHEMM.

W.3.1.6 Authorized Maximum Rate

This parameter is used for admission control decisions or policing actions at the AP. It is based on the Infrastructure Authorization Information delivered from the SSPN during the AAA procedure. For EDCA operation, this element contains a list of four MaxRate subelements indicating the maximum rate allowed for the access categories. For HCCA operation, there is one MaxRate subelement. Each of the MaxRate is an unsigned integer and in the unit of kilobits per second. An additional subelement provides the maximum rate at which a non-AP STA can source group addressed frames.

The AP stores the information in the corresponding dot11NonAPStationAuthMaxVoiceRate, dot11NonAPStationAuthMaxVideoRate, dot11NonAPStationAuthMaxBestEffortRate, dot11NonAPStationAuthMaxBackgroundRate, dot11NonAPStationAuthMaxHCCAHEMMRate and dot11NonAPStationAuthMaxSourceMulticastRate elements of its MIB.

W.3.1.7 Authorized Service Access Type

This per-non-AP STA parameter indicates the access type allowed for the non-AP STA based on the SSPN decision. The AP will use this information for authorization requests from the STA, e.g., allow or disallow direct link operation and group addressed services. The information element uses TruthValues to indicate the service type authorized. The following MIB variables are used:

- dot11NonAPStationAuthDls is to authorize a non-AP STA to use DLS
- dot11NonAPStationAuthSinkMulticast is to authorize a non-AP STA to request group addressed stream(s) from the network
- dot11NonAPStationAuthMaxSourceMulticastRate is to authorize a non-AP STA to source group addressed stream(s) to towards the network

W.3.1.8 Authorized Delay

This parameter is used for admission control decisions at the AP. It is based on the Infrastructure Authorization Information delivered from the SSPN during the AAA procedure. This element is only used for HCCA operation, and contains one subelement. An AP should deliver frames to a non-AP STA within the time period specified in this attribute. Furthermore, when a non-AP STA requests admission control, the requested delay is only approved if it is equal to or greater than the value stored in the corresponding element. Each element is an unsigned integer that measures delay in units of microseconds.

The AP stores the information in the corresponding dot11NonAPStationAuthHCCAHEMMDelay elements of its MIB.

W.3.1.9 Authorized Service Access Information

This parameter contains the relevant information for the AP to enforce the authorized service access type indicated in the Authorized Service Access Type element.

The Authorized Service Access parameters provide the VLAN assignment (VLAN ID and name) to which frames to or from the non-AP STA are bridged. The element includes VLAN ID (dot11NonAPStationVLANId) and VLAN Name (dot11NonAPStationVLANName).

W.3.1.10 non-AP STA Transmission Count

This parameter indicates the count of the data traffic transmitted to and received from a non-AP STA. Such information would be used by the on-line charging and accounting function, especially for the IEEE 802.11 WLAN local service, where the data traffic does not necessarily go through the SSPN network. In such cases, Layer 3 accounting/charging information is not reliable since addresses could be spoofed. Layer 2 would be a better place to collect such information since due to the cryptographic security association that exists between the non-AP STA and AP.

The non-AP STA Transmission Count element includes information stored in the corresponding dot11NonAPStationVoiceMSDUCount, dot11NonAPStationVideoMSDUCount, dot11NonAPStationBestEffortMSDUCount, dot11NonAPStationBackgroundMSDUCount, dot11NonAPStationHCCAHEMMMSDUCount, dot11NonAPStationMulticastMSDUCount, dot11NonAPStationVoiceOctetCount, dot11NonAPStationVideoOctetCount, dot11NonAPStationBestEffortOctetCount, dot11NonAPStationBackgroundOctetCount, dot11NonAPStationHCCAHEMMOctetCount, dot11NonAPStationMulticastOctetCount elements of the AP’s MIB.

W.3.1.11 non-AP STA Location Information

This parameter provides information about the STA’s location to the SSPN. It is required by the SSPN applying location based service control. In the IEEE 802.11 network, the non-AP STA location is approximated using the AP’s location information. This includes two type of formats, Geospatial and Civic Location.

The information to be placed in the non-AP STA Location information element is obtained from the dot11APGeoLocation and dot11APCivicLocation elements of the AP MIB.

W.3.1.12 non-AP STA State Information

This parameter indicates whether non-AP STA is Active Mode or Power Saving. Information in this element is obtained from the corresponding dot11NonAPStationPowerManagementMode element of the associated AP MIB.

W.4 Interworking with External Networks and Emergency Call Support

Emergency Services define the IEEE 802.11 functionality to support an Emergency Call (e.g., E911) service as part of an overall multi-layer solution, specifically capability advertisement and access to ES by STAs not having proper security credentials. “Multi-layer” indicates that Emergency Services will be provided by protocols developed in part by other standards bodies, see [B42], [B38] and [B41]. Three features of Interworking with External Networks support emergency call services.

The first feature is a mechanism for a non-AP STA to signal to an AP that a call is an emergency call. This is useful in the case where the access category to be used to carry the emergency call traffic (typically AC_VO) is configured for mandatory admission control. If the WLAN is congested, then the AP can deny the TSPEC request for bandwidth to carry the call. However, if the AP is able to determine that the call is an emergency call, then it can invoke other options to admit the TSPEC request.

The second and third features provide the means for a client without proper security credentials to be able to place an emergency call. The second feature makes use of Interworking information element which can be included in Association request frames in order to bypass the IEEE 802.1X port at an AP for un-authenticated access to emergency services. This is described further in Annex W.4.4. The third feature makes use of an SSID configured for Open Authentication to provide emergency services and is described in Annex W.4.2.

The STA has the burden to confirm the availability of emergency services from the 802.11 network, including that the network is authorized for emergency services. The time it takes for a client to find an authorized emergency services network is related to the speed of forward progress the authorized network can make over the air with the STA, relative to all of the other networks (attackers as well), and is inversely related to the number of false advertisements. A STA can confirm the availability of emergency services by observing the value of the ESC and UESA bits in the Interworking element of any received Beacon or Probe response frame.

W.4.1 Background on Emergency Call Support Over 802.11 infrastructure

Special handling for emergency service calls is required over IEEE 802.11. To use a public hotspot a user will go typically through an authentication process (e.g., EAP-based, or http/https redirect or DNS redirection) before being able to use it for emergency calls.

There is a need to support these emergency services both when the user has a relationship with the IEEE 802.11 network (credentials to access the network) and when it does not have any relationship with the IEEE 802.11 network.

The former case requires no changes to the authentication process—the user, having already been authenticated to and associated with the WLAN, simply dials the emergency number thereby placing the call.

In the latter case, the non-AP STA will be able to gain access to the network without using security credentials and make an emergency call.

Another difficulty is that once the user gains access to the network, there is no mechanism to prioritize their emergency traffic in the IEEE 802.11 MAC over that of other users, even with 802.11 QoS capability.

Supporting emergency services, such as E911 calling requires a multi-layer solution with support at various protocol layers. Apart from MAC level access and support for transfer of data between non-AP STA and AP with appropriate QoS at layer 2, there is a clear need, above this layer, to setup the call, conduct call control and management, and use an appropriate audio codec.

One specific example is when a user arrives in a new country and needs to make an emergency call in a public hotspot where there is no prior relationship with the available WLAN network or WLAN hotspot operator.

NOTE—The callback feature, if required in a regulatory domain, is dealt with at a higher layer.

W.4.2 System Aspects for Emergency Call Support

An IEEE 802.11 infrastructure by itself cannot ensure that all factors are compatible for an Emergency Service call to actually take place. The client device may have to register with a call manager (SIP agent or some other signaling endpoint) for the call to be placed successfully. Different signaling systems such as SIP, H.323, etc., can be deployed for supporting Emergency Service calling. Higher layers can also verify an Emergency Service call is being placed so that appropriate level of resources can be granted to the emergency call. Voice endpoints (e.g., non-AP STAs) can use different codecs such as G.711, AMR, and iLBC. All these functionalities are out of scope of this standard.

IEEE 802.11 can provide priority for emergency traffic both for the initial call establishment and during an ongoing emergency call, which assumes advertisement of this functionality supported in the BSS.

This section describes general design assumptions to support ES with IEEE 802.11:

a) It is assumed that there is a higher layer (above IEEE 802.11 Layer 2) protocol (or protocol suite) for making emergency calls or using any other ES.

b) In order to make the emergency call procedure work properly, the non-AP STA has the following responsibilities:

    1) Recognize the user’s request to make an emergency call

    2) Non-AP STA will associate to the AP if it is not already done so. In an RSN, if the user does not have valid authentication credentials for network access then non-AP STA can bypass the RSN that will provide access to the network to make emergency calls,

    3) Select an AP that supports QoS and EBR capability.

    4) If location information is required in a particular regulatory domain, request location information from the WLAN. If the STA can not determine it's own location by its own means, then Location information should be obtained from the network prior to initiating the emergency call request. There are two methods a non-AP STA can use to obtain location services from the 802.11 network:

        i) If the non-AP STA can use location information in geospatial format (i.e., latitude, longitude and altitude), then the RRM capability can be used to obtain this information. The AP advertises RRM capability in its Beacon management frame (bit1 set to 1 in the Capability information field). In this case, the non-AP STA transmits an LCI Request to the AP using the procedures in 11.10.8.6.

NOTE—The non-AP STA can receive an LCI Report with the incapable field set. According to the procedures in 11.10.8.6, the non-AP STA can re-submit an LCI Request with a location subject of “remote”. If the AP still responds with incapable, then location services are not available from the AP via RRM capability.

ii) If the non-AP STA requires location information in civic or geospatial formats, then an AP's wireless network management capability can be used. In this case, an AP advertises its ability to provide its location in with Civic or Geo format by setting the Civic Location or Geo Location field in the Extended Capabilities Element to 1. in the Beacon frame. A non-AP STA requests its location using the procedures in 11.23.6. Unlike an AP providing RRM capability, an AP Advertisement location capability will not return an "incapable" response if the non-AP STA requests the "remote" location.

5) Selects one of possibly several SSPNs advertising support for ES and VoIP service.

c) There are two methods described in this annex by which a user lacking security credentials can gain access to the network. The method selected in any particular deployment is at the discretion of the IEEE 802.11 infrastructure provider, SSPN or system administrator as appropriate. The AP and non-AP STA should permit users lacking security credentials to gain access to a network using one of the methods provided. The two methods are:

i) Using an ES association (see 7.3.2.89) in a BSS configured for RSNA. Using this type of association means the AP and non-AP STA will exchange un-protected frames for Emergency Service access only during the lifetime of the association. In this situation, cryptographic keys are not exchanged, the IEEE 802.1X uncontrolled port is bypassed without invoking the IEEE 802.1X state machine. Since protection is used for authenticated STAs, their traffic is protected.

ii) Using an SSID configured for open access (see Annex W.4.4) and designated to be suitable for obtaining ES only (i.e., and not suited for obtaining other services such as internet access). Network elements necessary to complete an emergency call are reachable via this SSID. How to reach these network elements (e.g., a Call Manager) and which protocol to use (e.g., SIP) are outside the scope of this standard. The non-AP STA can also use the NQP to determine if there is a SSID configured for Open Authentication/Association along with the corresponding SSID information.

d) The AP can separate the backhaul of ES traffic from other traffic, typically via a dedicated VLAN.

To ease burden of implementation on the network side, some basic means should exist to allow easy filtering, routing and basic access control of "regular" BSS traffic and emergency-type BSS traffic.

W.4.3 Description of the Expedited Bandwidth Request element

For access categories configured for mandatory admission control, a non-AP STA requests bandwidth using a TSPEC element in an ADDTS Request Action frame. The TSPEC Request includes parameters describing the characteristics of the traffic stream, but no information on the use of the traffic stream. The Expedited Bandwidth Request (EBR) element describes the "use" of a traffic stream. To use this element, it is the responsibility of the station to transmit this element in response to certain call signaling messages. How this is done is out of scope for the Interworking Service. The following bandwidth uses are provided in the EBR element:

- Emergency call, defined in [B55]
- Public first responder (e.g., fire department)
- Private first responder (e.g., enterprise security guard)
- Multi-level precedence and pre-emption

Multi-level precedence and pre-emption (MLPP) services are provided by other voice networking technologies such as 3GPP (see TS 22.067 [B40]), H.323 (see ITU-T H4.60.14) and other proprietary signaling protocols. MLPP is used as a subscription service to provide differentiated levels of consumer service; it is also used by military organizations so that commanding officers won't get a network busy signal.

If the AP is provided additional information regarding the nature of the Traffic Stream, it can invoke additional policy which can be configured on the AP to accept the TSPEC request when it would be otherwise denied. Policy configured at AP defines how bandwidth is allocated. Specification of these policies is out of scope of Interworking with External Networks. Policy examples include:

- No action
- Pre-emptive action: delete a TS of lower priority if necessary to make room for new TS
- Use capacity allocated for non-voice services if priority is above a certain value (assuming TSPEC is for AC_VO)
- Interpret MLPP codes as defined 3GPP specification
- Interpret MLPP codes as defined in proprietary specification

W.4.4 Access to Emergency Services in an RSN

If a network requires authentication and encryption with RSN, a non-AP STA placing an emergency call associates and authenticate to the network by using an ES association (see 7.3.2.89). If the non-AP STA has user credentials that allow it to use a particular network, the non-AP STA can use its credentials to authenticate to the SSPN through the IEEE 802.11 infrastructure.

To use an ES association, a STA lacking security credentials can associate to a BSS in which Emergency Services are accessible by including an Interworking Element with the UESA field set to 1 in a (Re)-association Request frame. An AP receiving this type of (Re)-assocation request recognizes this as a request for un-authenticated emergency access. The AP can look up the VLAN ID to use with a AAA server, or it can have an emergency services VLAN configured. Similarly, it can also have other policies configured locally for quality of service parameters and network access restrictions, or it can also look them up through external policy servers.

When an ES association is used, the IEEE 802.11 infrastructure should be designed to restrict access to emergency call users. Methods of such restriction are beyond the scope of IEEE 802.11, but can include an isolated VLAN for emergency services, filtering rules in the AP or network entity (e.g., router) in an external network to limit network access to only network elements involved in emergency calls, and per-session bandwidth control to place an upper limit on resource utilization.