

**IEEE Standard for Information Technology—  
Telecommunications and information exchange  
between systems  
Wireless Regional Area Networks (WRAN)—  
Specific requirements**

**Part 22: Cognitive Wireless RAN  
Medium Access Control (MAC) and  
Physical Layer (PHY) Specifications:  
Policies and Procedures for  
Operation in the TV Bands**

IEEE Computer Society

Sponsored by the  
LAN/MAN Standards Committee

---

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

**IEEE Std 802.22™-2011**

1 July 2011



**IEEE Standard for Information Technology—  
Telecommunications and information exchange  
between systems  
Wireless Regional Area Networks (WRAN)—  
Specific requirements**

**Part 22: Cognitive Wireless RAN  
Medium Access Control (MAC) and  
Physical Layer (PHY) Specifications:  
Policies and Procedures for  
Operation in the TV Bands**

Sponsor

**LAN/MAN Standards Committee  
of the  
IEEE Computer Society**

Approved 16 June 2011

**IEEE-SA Standards Board**

Approved 26 July 2012

**American National Standards Institute**

**Abstract:** This standard specifies the air interface, including the cognitive medium access control layer (MAC) and physical layer (PHY), of point-to-multipoint wireless regional area networks comprised of a professional fixed base station with fixed and portable user terminals operating in the VHF/UHF TV broadcast bands between 54 MHz to 862 MHz.

**Keywords:** broadband wireless access network, cognitive radio, fixed user terminals, IEEE 802.22, portable user terminals, radio spectrum sensing, regional area network, WRAN standards

---

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

Copyright © 2011 by the Institute of Electrical and Electronics Engineers, Inc.  
All rights reserved. Published 1 July 2011. Printed in the United States of America.

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

PDF: ISBN 978-0-7381-6723-7      STD97146  
Print: ISBN 978-0-7381-6724-4      STDPD97146

*IEEE prohibits discrimination, harassment and bullying. For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.  
No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.*

**IEEE Standards** documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied “**AS IS**.”

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation, or every ten years for stabilization. When a document is more than five years old and has not been reaffirmed, or more than ten years old and has not been stabilized, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

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

**Interpretations:** Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Recommendations to change the status of a stabilized standard should include a rationale as to why a revision or withdrawal is required. Comments and recommendations on standards, and requests for interpretations should be addressed to:

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

Authorization to photocopy portions of any individual standard for internal or personal use is granted by The Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

## **Introduction**

This introduction is not part of IEEE Std 802.22-2011, IEEE Standard for Information Technology—Telecommunications and information exchange between systems—Wireless Regional Area Networks (WRAN)—Specific requirements—Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands.

This standard specifies the air interface of broadband wireless access (BWA) systems for fixed and portable user terminals supporting multimedia services. The medium access control layer (MAC) supports a point-to-multipoint architecture. The MAC is structured to support a physical layer (PHY) specification especially suited for operation in TV broadcast bands while avoiding interference to the incumbent broadcast services.

## **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 web site 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 web site 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 standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or 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 provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

## Participants

At the time this standard was submitted to the IEEE-SA for approval, the following voting members had participated in the IEEE P802.22 Working Group:

**Apurva N. Mody, Chair**

**Gerald Chouinard, Vice-chair and lead editor**

Kyu Hwan An	Subir Das	Baowei Ji
Chee Wei Ang	W. Carl Day	Ravi Kalavakunta
Kwok Shum Au	Upkar Dhaliwal	Jerome J. Kalke
Mark Austin	Johnny Dixon	Bub-Joo Kang
Anuj Batra	Peter Ecclesine	Mark Kelley
John Benko	Charles Einolf	Ramon Khalona
Robert Berger	Michael Fischer	Thomas Kiernan
Dagnachew Birru	Wen Gao	Chang-Joo Kim
Scott Blue	Ingo Gaspard	Kihong Kim
Monique Bourgeois Brown	Monisha Ghosh	Sangbum Kim
Gregory Buchwald	Joanna Guenin	HakSun Kim
Winston Caldwell	Jin Guo	Byoung-Jo Kim
Ed Callaway	Thomas Gurley	Gwangzeen Ko
Dave Cavalcanti	JaeSong Han	Tom Kolze
Kiran Challapali	Hiroshi Harada	Bruce Kraemer
Soo-Young Chang	Ahren Hartman	Steve Kuffner
Remi Chayer	Robert F. Heile	Denis Kuwahara
Shiu Yuan Chen	Anh Twan Hoang	Jeong Suk Lee
Tao Chen	Michael Hoghooghi	Chang-Ho Lee
Jinxia Cheng	Mark Hopkins	Geunho Lee
Aik Chindapol	Victor Hou	Haeyoung Lee
InHwan Choi	Wendong Hu	Zhongding Lei
Liwen Chu	Junhong Hui	Wing Seng Leon
Joon-Hwa Chun	Sung Hyun Hwang	Barry Lewis
Chris Clanton	Duckdong Hwang	Lingjie Li
Charles Cook	Tae-In Hyon	Ying-Chang Liang
Charles Cooper	Yutaka Ikeda	Kyutae Lim
Carlos Cordeiro	Soon Ik Jeon	Euntack Lim

Jiezen Lin	Mohammad Rahman	Hideki Tanaka
Jinnan Liu	Ranga K. Reddy	Clifford Tavares
Hang Liu	Ivan Reede	Victor Tawil
Michael Lynch	Edgar Reihl	Shawn Taylor
Steve Mace	Jon Walter Rosdahl	Paul Thompson
David Magee	William Rose	James Tomcik
Ben Manny	Luis Escobar Sanz	JungSun Um
David Mazzarese	Shigenobu Sasaki	George Vlantis
Tony Morella	Jeffrey Schiffer	Lei Wang
Peter Murray	Chris Seagren	Jianfeng Wang
Max Muterspaugh	Alireza Seyed	Yunbiao Wang
Mullaguru Naidu	Cheng Shan	Tom Wasilewski
Paul Nikolic	Steve Shellhammer	Alfred Wieczorek
John Notor	Dave Silk	Kelly Williams
Moh Nouroozian	Kirk Skeba	Yuchun Wu
Seungmok Oh	Douglas Smith	Shiquan Wu
Barry O'Mahony	Eli Sofer	Bo Xia
Ashish Pandharipande	Myung Sun Song	Changlong Xu
Juha Pihlaja	Srikathyayani Srikanteswara	ShanShan Xu
Patrick Pirat	Jayne Stancavage	Steve Yao
Ron Porat	Carl Stevenson	Yonghong Zeng
Jeff Poston	William Stiles	Jianwei Zhang
Jim Raab		Xin Zhang

Major contributions to this standard were made by the following individuals:

Kwok Shum Au	Ramon Khalona	Ashish Pandharipande
John Benko	Thomas Kiernan	Patrick Pirat
Winston Caldwell	Kihong Kim	Mohammad Rahman
Dave Cavalcanti	Sangbum Kim	Ranga K. Reddy
Soo-Young Chang	Kak-Sun Kim	Ivan Reede
Gerald Chouinard	Gwangzeen Ko	Shigenobu Sasaki
Carlos Cordeiro	Steve Kuffner	Cheng Shan
Charles Einolf	Zhongding Lei	Steve Shellhammer
Wen Gao	Lingjie Li	Eli Sofer
Monisha Ghosh	Kyutae Lim	Carl Stevenson
Thomas Gurley	Jinnan Liu	Victor Tawil
Anh Twan Hoang	David Mazzarese	JungSun Um
Wendong Hu	Apurva N. Mody	George Vlantis
Sung Hyun Hwang	Peter Murray	Jianfeng Wang
Jerome J. Kalke	Mogh Nouroozian	Yonghong Zeng

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

Iwan Adhicandra  
Thomas Alexander  
Nobumitsu Amachi  
Yafan An  
Butch Anton  
Franklin A. Antony  
Danilo Antonelli  
Kwok Shum Au  
Tuncer Baykas  
Maciej Borowka  
Nancy Bravin  
Vern Brethour  
William Byrd  
Meredith Caldwell  
Radhakrishna Canchi  
Juan Carreon  
Kenneth Carrigan  
Dave Cavalcanti  
Gerald Chouinard  
Keith Chow  
Charles Cook  
Todor Cooklev  
Subir Das  
Patrick Diamond  
Thomas Dineen  
Carlo Donati  
Sourav Dutta  
Peter Ecclesine  
Richard Eckard  
Charles Einolf  
Shulan Feng  
Stanislav Filin  
Avraham Freedman  
Monisha Ghosh  
Pieter-Paul Giesberts  
James Gilb  
Gregory Gillooly  
Reinhard Gloer  
Patrick Gonia  
Randall Groves  
Thomas Gurley  
C. Guy  
Seishi Hanaoka  
Robert F. Heile  
Oliver Hoffmann  
Wendong Hu

Yerang Hur  
Sung Hyun Hwang  
Akio Iso  
Atsushi Ito  
Raj Jain  
Junghoon Jee  
Bobby Jose  
Tal Kaitz  
Shinkyo Kaku  
Masahiko Kaneko  
Piotr Karocki  
Richard Kennedy  
Stuart J. Kerry  
Kihong Kim  
Yongbum Kim  
Gwangzeen Ko  
Bruce Kraemer  
Joseph Kwak  
Jeremy Landt  
Zhongding Lei  
Lingjie Li  
Jan-Ray Liao  
Arthur Light  
Lu Liru  
Daniel Lubar  
Greg Luri  
Michael Lynch  
Elvis Maculuba  
Syam Madanapalli  
Wayne W Manges  
Roger Marks  
Jeffery Masters  
Stephen Mccann  
Michael Mcinnis  
Steven Methley  
Gary Michel  
Apurva Mody  
Jose Morales  
Ronald Murias  
Rick Murphy  
Peter Murray  
Juichi Nakada  
Michael S. Newman  
Nick S. A Nikjoo  
Paul Nikolich  
John Notor  
Chris Osterloh

Satoshi Oyama  
Riku Pirhonen  
Clinton Powell  
Venkatesha Prasad  
Mohammad Rahman  
Ranga K. Reddy  
Ivan Reede  
Alex Reznik  
Maximilian Riegel  
Robert Robinson  
Benjamin Rolfe  
William Rose  
Herbert Ruck  
Randall Safier  
Shigenobu Sasaki  
Naotaka Sato  
Ryo Sawai  
Bartien Sayogo  
Matthew Sherman  
Gil Shultz  
Kapil Sood  
Amjad Soomro  
Chad Spooner  
Thomas Starai  
Rene Struik  
Walter Struppler  
Mark Sturza  
Alourdes Sully  
Chin-Sean Sum  
Jun Ichi Takada  
Victor Tawil  
Ha Nguyen Tran  
Mark-Rene Uchida  
JungSun Um  
Anna Urra  
Dmitri Varsanofiev  
Prabodh Varshney  
Jane Verner  
George Vlantis  
Jianfeng Wang  
Hung-Yu Wei  
Alfred Wieczorek  
Akira Yamaguchi  
Oren Yuen  
Janusz Zalewski  
Xin Zhang

When the IEEE-SA Standards Board approved this on 16 June 2011, it had the following membership:

**Richard H. Hulett, Chair**  
**John Kulick, Vice Chair**  
**Robert M. Grow, Past Chair**  
**Judith Gorman, Secretary**

Masayuki Ariyoshi  
William Bartley  
Ted Burse  
Clint Chaplin  
Wael Diab  
Jean-Philippe Faure  
Alexander Gelman  
Paul Houzé

Jim Hughes  
Joseph L. Koepfinger\*  
David J. Law  
Thomas Lee  
Hung Ling  
Oleg Logvinov  
Ted Olsen

Gary Robinson  
Jon Walter Rosdahl  
Sam Sciacca  
Mike Seavey  
Curtis Siller  
Phil Winston  
Howard L. Wolfman  
Don Wright

\*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Satish Aggarwal, *NRC Representative*  
Richard DeBlasio, *DOE Representative*  
Michael Janezic, *NIST Representative*

Patricia Gerdon  
*IEEE Standards Program Manager, Document Development*

Catherine Berger  
*IEEE Standards Project Editor*

## Contents

1	Overview.....	1
1.1	Scope.....	1
1.2	Purpose.....	2
1.3	Reference application.....	2
2	Normative references .....	3
3	Definitions .....	5
4	Abbreviations and acronyms.....	10
5	System architecture.....	13
5.1	Reference architecture .....	13
5.2	Management reference architecture.....	17
6	Packet Convergence sublayer .....	20
6.1	MAC SDU format .....	20
6.2	Classification.....	20
6.3	IEEE 802.3/Ethernet-specific part.....	22
6.4	IP specific part.....	22
7	MAC Common Part sublayer.....	24
7.1	General .....	24
7.2	Addressing and connections.....	24
7.3	General superframe structure .....	26
7.4	General frame structure .....	27
7.5	Control headers.....	31
7.6	MAC PDU formats.....	35
7.7	Management messages .....	45
7.8	Management of MAC PDUs .....	110
7.9	ARQ mechanism .....	115
7.10	Scheduling services .....	125
7.11	Bandwidth management .....	128
7.12	PHY support.....	132
7.13	Contention resolution .....	134
7.14	Initialization and network association .....	135
7.15	Ranging .....	159
7.16	Channel descriptor management .....	164
7.17	Multicast support.....	166
7.18	QoS.....	169
7.19	Incumbent protection.....	212
7.20	Self-coexistence.....	221
7.21	Quiet periods and sensing.....	237
7.22	Channel management .....	246

7.23	Synchronization of the IEEE 802.22 base stations .....	249
8	Security mechanism in IEEE 802.22 .....	250
8.1	Security Architecture for the Data/Control and Management Planes.....	250
8.2	SCM protocol .....	253
8.3	Key usage .....	275
8.4	Cryptographic methods .....	281
8.5	Certificate profile .....	286
8.6	Security sublayer 2—Security mechanisms for the cognitive functions .....	293
8.7	CPE privacy.....	306
9	PHY .....	307
9.1	Symbol description.....	307
9.2	Data rates.....	310
9.3	Functional block diagram applicable to the PHY layer.....	311
9.4	Superframe and frame structures.....	312
9.5	CBP packet format .....	320
9.6	OFDM subcarrier allocation.....	322
9.7	Channel coding.....	329
9.8	Constellation mapping and modulation.....	348
9.9	Control mechanisms .....	351
9.10	Network synchronization.....	357
9.11	Frequency Control requirements .....	358
9.12	Antenna .....	358
9.13	RF mask.....	362
9.14	Receiver requirements .....	363
10	Cognitive radio capability.....	365
10.1	General .....	365
10.2	Spectrum Manager operation .....	366
10.3	Spectrum Sensing Automaton (SSA) .....	392
10.4	Spectrum sensing.....	406
10.5	Geolocation .....	416
10.6	Database service.....	421
10.7	Primitives for cognitive radio capabilities .....	423
11	Configuration.....	440
12	Parameters and connection management .....	441
12.1	Parameters, timers, message IEs.....	441
12.2	Well-known CIDs.....	450
12.3	ARQ parameters .....	452
13	MIB structure.....	453
13.1	MIB description.....	453
	Annex A (normative) IEEE 802.22 regulatory domains and regulatory classes requirements.....	557

A.1 Regulatory domains, regulatory classes, and professional installation .....	557
A.2 Radio performance requirements .....	558
A.3 Channel availability and sensing requirements .....	560
A.4 Device identification requirements .....	563
A.5 Channelization based on the regulatory domain .....	564
 Annex B (informative) Multicarrier fine ranging method .....	568
B.1 General description .....	568
B.2 Practical embodiment of the proposed multicarrier fine ranging method .....	573
B.3 References.....	575
 Annex C (informative) Sensing .....	576
C.1 Blind sensing techniques.....	576
C.2 Signal specific sensing techniques .....	585
C.3 References.....	627
 Annex D (informative) Summary of the characteristics of the IEEE 802.22.1 beacon signal and protocols .....	629
D.1 General.....	629
D.2 Superframe structure.....	629
D.3 Beacon frame structure .....	630
D.4 Synchronization burst .....	631
D.5 Inter-device communication period (ICP) .....	632
D.6 PHY specifications .....	632
D.7 Reference architecture for the WRAN receiver .....	633
D.8 Sensing and detection at the WRAN receiver.....	634
D.9 Options for detecting the IEEE 802.22.1 beacon signal .....	644
D.10 Operation scenarios for the coexistence of IEEE 802.22.1 and IEEE 802.22.....	646
D.11 References .....	647
 Annex E (informative) Distributed spectrum sensing and authentication to provide protection against thermal noise .....	648
 Annex F (informative) Network security aspects .....	653
F.1 Availability .....	653
F.2 Authentication .....	653
F.3 Authorization.....	654
F.4 Identification .....	654
F.5 Integrity .....	654
F.6 Confidentiality/Privacy.....	655
 Annex G (informative) Bibliography .....	656

**IEEE Standard for Information Technology—  
Telecommunications and information exchange  
between systems**

**Wireless Regional Area Networks (WRAN)—  
Specific requirements**

**Part 22: Cognitive Wireless RAN  
Medium Access Control (MAC) and  
Physical Layer (PHY) Specifications:  
Policies and Procedures for  
Operation in the TV Bands**

***IMPORTANT NOTICE: This standard is not intended to ensure safety, security, health, or environmental protection. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.***

*This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.*

## **1. Overview**

### **1.1 Scope**

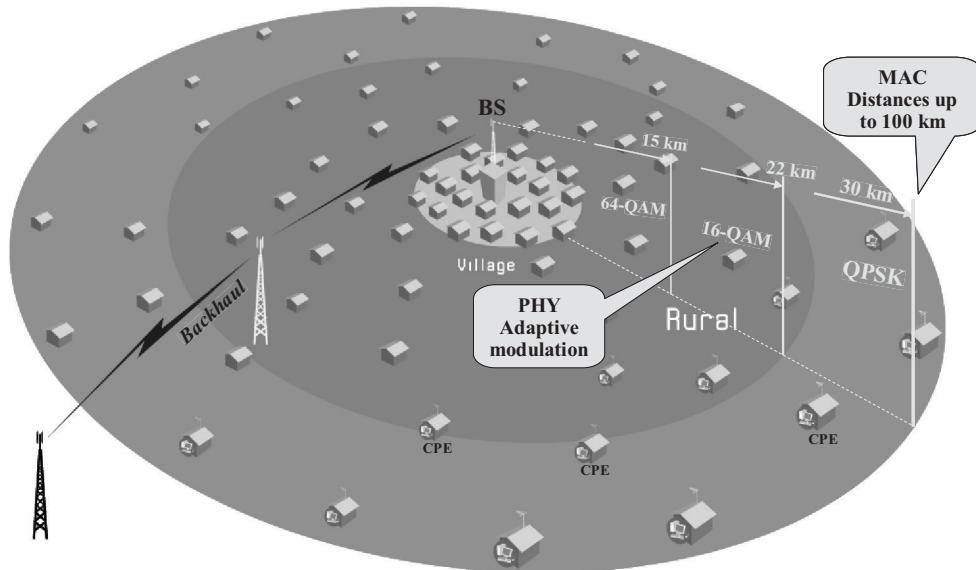
This standard specifies the air interface, including the cognitive medium access control layer (MAC) and physical layer (PHY), of point-to-multipoint wireless regional area networks comprised of a professional fixed base station with fixed and portable user terminals operating in the VHF/UHF TV broadcast bands between 54 MHz to 862 MHz.

## 1.2 Purpose

This standard is intended to enable deployment of interoperable IEEE 802<sup>®</sup> multivendor wireless regional area network products, to facilitate competition in broadband access by providing alternatives to wireline broadband access and extending the deployability of such systems into diverse geographic areas, including sparsely populated rural areas, while preventing harmful interference to incumbent licensed services in the TV broadcast bands.

## 1.3 Reference application

The Wireless Regional Area Networks (WRANs) for which this standard has been developed are expected to operate primarily in low population density areas in order to provide broadband access to data networks. The WRAN systems will use vacant channels in the VHF and UHF bands allocated to the Television Broadcasting Service in the frequency range between 54 MHz and 862 MHz while avoiding interference to the broadcast incumbents in these bands. A typical application can be the coverage of the rural area around a village, as illustrated in Figure 1, within a radius of 10 km to 30 km from the base station depending on its EIRP and antenna height. The MAC can also accommodate user terminals located as far as 100 km with proper scheduling of the traffic in the frame when exceptional RF signal propagation conditions are present. With the PHY implemented in this standard, WRAN systems can cover up to a radius of 30 km without special scheduling.



**Figure 1 — An IEEE 802.22 WRAN cell with a base station and user terminals**

A base station (BS) complying with this standard shall be able to provide high-speed Internet service for up to 512 fixed or portable customer premise equipment (CPE) devices or groups of devices within its coverage area assuming different quality of service (QoS) requirements for various CPEs, while meeting the regulatory requirements for protection of the incumbents.

The standard includes cognitive radio techniques to mitigate interference to incumbents, including geolocation capability, provision to access a database of incumbent services, and spectrum-sensing technology to detect the presence of incumbent services, other WRAN systems, and IEEE 802.22.1 wireless beacons.

## 2. Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. At the time of publication, the editions indicated were valid. All standards and specifications are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the references listed below.

ANSI X9.62-2005, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), November 2005.<sup>1</sup>

ANSI X9.63-2001, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, November 2001.

IEEE Std 802<sup>®</sup>-2001, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture.<sup>2, 3</sup>

IEEE Std 802.16<sup>TM</sup>-2009, IEEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Broadband Wireless Access Systems.

IEEE Std 802.22.1<sup>TM</sup>-2010, IEEE Standard for Local and metropolitan area networks—Part 22.1: Methods to Enhance Protection of Low-Power, Licensed Device Operation in the TV Broadcast Bands from Harmful Interference from License-Exempt Devices Operating in those Bands.

FIPS 180-3, Secure Hash Standard (SHS), October 2008.<sup>4</sup>

FIPS 186-3, Digital Signature Standard (DSS), June 2009.

FIPS 197, Advanced Encryption Standard, November 2001.

IETF RFC 2437, PKCS #1: RSA Cryptography Specification Version 2.0, October 1998.<sup>5</sup>

IETF RFC 2578, “Structure of Management Information Version 2 (SMIV2),” K. McCloghrie, D. Perkins, J. Schoenwaelder, J. Case, M. Rose, S. Waldbusser, April 1999.

IETF RFC 2758, “Definitions of Managed Objects for Service Level Agreements Performance Monitoring,” K. White, February 2000.

IETF RFC 3279, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002.

IETF RFC 4492, Elliptic Curve Cryptography (ECC) for Transport Layer Security (TLS), May 2006.

IETF RFC 5216, The EAP-TLS Authentical Protocol, March 2008.

IETF RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2, August 2008.

<sup>1</sup> ANSI publications are available from the Sales Department, American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (<http://www.ansi.org/>).

<sup>2</sup> IEEE publications are available from the Institute of Electrical and Electronics Engineers, Inc., 445 Hoes Lane, Piscataway, NJ 08854, USA (<http://standards.ieee.org/>).

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

<sup>4</sup> FIPS publications are available from the National Technical Information Service (NTIS), U. S. Dept. of Commerce, 5285 Port Royal Rd., Springfield, VA 22161 (<http://www.ntis.org/>).

<sup>5</sup> Internet Requests for Comments (RFCs) are available on the World Wide Web at the following ftp site: [venera.isi.edu](http://venera.isi.edu); logon: anonymous; password: user's e-mail address; directory: in-notes.

IETF RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008.

IETF RFC 5281, Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0), August 2008.

IETF RFC 5649, Advanced Encryption Standard (AES) Key Wrap Algorithm with Padding, August 2009.

NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007.<sup>6</sup>

NMEA 0183, Interface Standard of the National Marine Electronics Association, Version 4.00  
[http://www.nmea.org/content/nmea\\_standards/nmea\\_083\\_v\\_400.asp](http://www.nmea.org/content/nmea_standards/nmea_083_v_400.asp).

Radio Regulations, International Telecommunications Union, Geneva, Switzerland, Edition of 2008.

SEC 4, Standards for Efficient Cryptography Group (SECG)—SEC 4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV) Working Draft, March 9, 2011, <http://www.secg.org/download/aid-785/sec4-0.97.pdf>.<sup>7</sup>

Trusted Computing Group, “TPM Main Specification Level 2 Version 1.2 (Revision 103)—Part 1—Design Principles,” July 2007, [http://www.trustedcomputinggroup.org/files/resource\\_files/ACD19914-1D09-3519-ADA64741A1A15795/mainP1DPrev103.zip](http://www.trustedcomputinggroup.org/files/resource_files/ACD19914-1D09-3519-ADA64741A1A15795/mainP1DPrev103.zip).

Trusted Computing Group, “TPM Main Specification Level 2 Version 1.2 (Revision 103)—Part 2—Structures of the TPM,” October 2006,  
[http://www.trustedcomputinggroup.org/files/resource\\_files/8D3D6571-1D09-3519-AD22EA2911D4E9D0/mainP2Structrev103.pdf](http://www.trustedcomputinggroup.org/files/resource_files/8D3D6571-1D09-3519-AD22EA2911D4E9D0/mainP2Structrev103.pdf).

Trusted Computing Group, “TPM Main Specification Level 2 Version 1.2 (Revision 103)—Part 3—Commands,” October 2006, [http://www.trustedcomputinggroup.org/files/static\\_page\\_files/ACD28F6C-1D09-3519-AD210DC2597F1E4C/mainP3Commandsrev103.pdf](http://www.trustedcomputinggroup.org/files/static_page_files/ACD28F6C-1D09-3519-AD210DC2597F1E4C/mainP3Commandsrev103.pdf).

U.S. FCC, ET Docket 08-260, “Second Report and Order and Memorandum Opinion and Order in the Matter of Unlicensed Operation in the TV Broadcast Bands,” November 14, 2008.

U.S. FCC, ET Docket 10-174, “Second Memorandum Opinion and Order in the Matter of Unlicensed Operation in the TV Broadcast Bands,” September 23, 2010.

---

<sup>6</sup> NIST SP 800-38D can be found at <http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf>.

<sup>7</sup> At the time this standard published, SEC 4 was still in draft form. The draft can be found at <http://www.secg.org/>. Alternately, users may contact the IEEE to obtain this draft.

### 3. Definitions

For the purposes of this document, the following terms and definitions apply. *The IEEE Standards Dictionary: Glossary of Terms & Definitions* should be referenced for terms not defined in this clause.<sup>8</sup>

**3.1 analog television:** Radio frequency (RF) transmission of audio and video by analog signals [e.g., NTSC, PAL, SECAM] (see ITU-R Recommendation BT.470 [B50]).<sup>9</sup>

**3.2 authenticator:** An entity at one end of a point-to-multipoint Wireless Regional Area Network (WRAN) link that facilitates the authentication of the entity attached at the other end of that link.

**3.3 backup channel:** A channel that has been cleared [i.e., verified that no incumbent service will be affected by Wireless Regional Area Network (WRAN) operation in this channel] to immediately become the operating channel in case the WRAN needs to switch channel.

NOTE—See 10.2.2.<sup>10</sup>

**3.4 base station (BS):** Generalized equipment set providing connectivity, management and control of the customer premise equipment (CPE). The functionalities attributed to the BS, in the context of this standard, may be implemented by a device or a collection of devices.

**3.5 broadcast connection:** A connection established to transport MAC management messages and data from the base station (BS) to all of the CPEs in the cell on the downstream (DS).

**3.6 burst:** A two-dimensional segment of OFDM subchannels (frequency domain) and symbols (time domain). It may comprise multiple MAC PDUs that are encoded with the same physical modulation and coding.

**3.7 candidate channel:** A channel that, once cleared from potential harmful interference to incumbents, can become a backup channel.

NOTE—See 10.2.2.

**3.8 carrier-to-noise ratio (CNR):** Ratio of the power of a subcarrier to the noise power in a bandwidth corresponding to the subcarrier spacing for a set of system parameters as given in Table 199.

**3.9 cell:** An IEEE 802.22 cell (or simply, a cell) is formed by a single IEEE 802.22 BS and zero or more IEEE 802.22 customer premise equipments (CPEs) associated with and under control of this IEEE 802.22 BS. The coverage area of this cell extends up to the point where the signal received from the IEEE 802.22 BS is sufficient to allow IEEE 802.22 CPEs to associate and maintain communication with the BS.

**3.10 channel:** Refers to a specific physical radio frequency channel, a contiguous segment of spectrum in the TV broadcast frequency bands, which may be 6 MHz, 7 MHz, or 8 MHz wide depending on the relevant regulatory domains. *See also: logical channel.*

---

<sup>8</sup> *The IEEE Standards Dictionary: Glossary of Terms & Definitions* is available at <http://shop.ieee.org/>.

<sup>9</sup> The numbers in brackets correspond to those of the bibliography in Annex G.

<sup>10</sup> Notes in text, tables, and figures are given for information only and do not contain requirements needed to implement the standard.

**3.11 cognitive plane:** The cognitive plane consists of all the entities in the IEEE 802.22 reference architecture that relate to cognitive functions. These cognitive functions are the spectrum manager/spectrum automaton, spectrum sensing function, the geolocation function and the security sublayer 2. The spectrum manager/spectrum automaton reside at the same level as the MAC common part sublayer in the data plane whereas the SSF and the geolocation function reside at the same level as the PHY in the data plane.

**3.12 cognitive radio:** A functionality of some wireless communication devices in which either a network or a wireless node can change the devices' transmission and/or reception parameters to communicate efficiently and to avoid interference with licensed or licensed-exempt users. This alteration of parameters is based on the active monitoring of several factors in the external and internal radio environment, such as radio frequency spectrum, location information, user behavior, network state, etc.

**3.13 coexistence:** State by which license-exempt wireless communication systems of various types can share a same RF transmission channel in a common area while minimizing harmful interference to each other by the use of appropriate means.

**3.14 coexistence beacon:** Series of bursts that is transmitted with the goal of improving self-coexistence among overlapping IEEE 802.22 cells, potentially improving coexistence among license-exempt wireless communication systems of various types if so equipped, regularly signaling the identity of the transmission device for potential interference resolution and enhancing geolocation ranging resolution between CPEs within a cell. The beacon is transmitted under the control of the BS during self-coexistence windows.

**3.15 connection:** Data path established between BS and CPE for transport of data.

**3.16 customer premise or portable equipment (CPE):** A generalized equipment set providing connectivity between a BS and a subscriber premise.

**3.17 cyclic prefix (CP):** The portion of an OFDM symbol used to absorb inter-symbol interference caused by transmission channel time dispersion. The cyclic prefix is actually a copy of the last portion of the symbol appended to the front of the same symbol. Its size is defined in terms of a ratio to the useful part of the OFDM symbol.

NOTE—See Table 200.

**3.18 database service:** Service officially operated under the rules of the local regulatory authority that provides a list of available channels and possibly the maximum EIRP allowable on these channels based on queries containing the geolocation of the Wireless Regional Area Network (WRAN) devices.

**3.19 digital television:** Radio frequency (RF) transmission of audio and video by digital signals (e.g., ATSC, DVB-T, ISDB-T) (see ITU-R Recommendation BT-798 [B52]).

**3.20 downstream (DS):** The direction of the transmitted signal from a base station (BS) to a CPE.

**3.21 downstream channel descriptor (DCD):** A medium access control (MAC) message that describes the PHY characteristics of a downstream burst.

**3.22 downstream interval usage code (DIUC):** An interval usage code specific to a downstream burst.  
*See also: interval usage code.*

**3.23 downstream map (DS-MAP):** A MAC message that defines the structure of the downstream subframe, i.e., burst locations in the time and frequency domain of the OFDM.

**3.24 flow ID (FID):** An identifier that identifies a particular flow of traffic assigned to a specific CPE or group of CPEs. *See also: station ID (SID).*

**3.25 frame:** Basic time unit over which BS and CPEs communicate with each other. It is comprised of one downstream subframe, one upstream subframe and a self-coexistence window when present.

**3.26 frame contention source (FC-SRC):** A WRAN cell that is demanding additional spectrum resources (i.e., data frame transmission opportunities on a channel) and is initiating an interactive frame contention process with the target frame contention destination (FC-DST).

**3.27 frame contention destination (FC-DST):** A Wireless Regional Area Network (WRAN) cell that is the target of the frame contention request initiated by a frame contention source (FC-SRC), and is the occupier of the spectrum resources being requested by the frame contention source (FC-SRC).

**3.28 frame contention number (FCN):** Number randomly generated by the FC-SRCs and FC-DSTs for determining by contention the priority of frame access.

**3.29 geolocation:** The process of acquiring the location data of a device, determining its latitude and longitude, and producing the corresponding NMEA string.

**3.30 harmful interference:** Any emission, radiation or induction that endangers the functioning of a radio navigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radiocommunications service operating in accordance with the ITU and local Regulations. [See Article 1 of the ITU Radio Regulations, #1.169 and the FCC 47 CFR 15.3(m).]

**3.31 IEEE 802.22.1 wireless beacon:** An RF device that provides enhanced protection to licensed low power auxiliary devices such as those used in the production and transmission of broadcast programs [e.g., devices licensed as secondary under Title 47 of the Code of Federal Regulations (CFR) in the USA and equivalent devices in other regulatory domains] from harmful interference potentially caused by WRAN operation.

**3.32 in-band:** The operating channel (N) and its first adjacent channels (N-1 and N+1).

**3.33 incumbents:** Licensed transmission systems operating in the TV bands on a primary or secondary basis according to international and local regulatory rules.

**3.34 interval usage code:** A code identifying a particular burst profile that can be used for a downstream or upstream transmission interval.

**3.35 logical channel:** This is the channel number used by the MAC, and does not necessarily reflect a physical channel. This can be mapped into any representation as defined by the PHY. *See also: channel.*

**3.36 MAC PDU:** The smallest unit of transmission/reception to be processed by the MAC. It is comprised of the MAC header, the payload, and Cyclic Redundancy Check (CRC).

**3.37 managed node:** A node that collects and stores the managed objects in the format of a MIB that is made available to the network management system via the Simple Network Management Protocol (SNMP).

**3.38 managed object:** A specific characteristic, among many, of a managed device. Managed objects are comprised of one or more object instances, which are essentially variables. A managed object is also referred to as a MIB object or an object.

**3.39 management connection:** A connection established to transport MAC management messages and data between the BS and a particular CPE.

**3.40 Management Information Base (MIB):** A collection of information that is organized hierarchically. MIBs are accessed using Simple Network Management Protocol (SNMP). They are comprised of managed objects that are identified by object identifiers.

**3.41 multicast management connection:** A connection established to transport MAC management messages and data from the BS to a particular group of CPEs on the DS.

**3.42 multicast transport connection:** A connection established to transport user data from the base station (BS) to a particular group of customer premise equipment (CPE) on the downstream (DS).

**3.43 OFDM slot:** A two-dimensional entity defined as one OFDM symbol by one subchannel.

**3.44 operating channel:** Channel being used by a WRAN system.

**3.45 out-of-band:** Any channel that is not in-band. *See also: in-band.*

**3.46 protected contour:** The regulator-defined boundary of an area within which a TV station is entitled to protection from harmful interference.

**3.47 quiet period:** A specific period of time during which the base station has scheduled a cessation of all transmission in its cell for the purpose of sensing.

**3.48 RSSL:** Received WRAN signal strength level at a base station or customer premise equipment (CPE).

**3.49 RSSI:** Received signal strength indication (estimate) on the sensing signal path or WRAN signal path in sensing mode 2 at a base station or customer premise equipment (CPE).

**3.50 security association (SA):** The set of security information a base station (BS) and one or more of its CPEs share in order to support secure communications. This shared information includes traffic encryption keys (TEKs) and the cipher suite that is to be applied to the SA.

**3.51 security association identifier (SAID):** An identifier shared between the base station (BS) and a customer premise equipment (CPE) that uniquely identifies a security association (SA).

**3.52 security sublayer 1:** Security functions for the Data/Control Plane.

**3.53 security sublayer 2:** Security functions for the Cognitive Plane.

**3.54 self-coexistence:** A state by which wireless communication systems of the same type can share a RF transmission channel in a common area while minimizing harmful interference to each other by the use of appropriate means. In the case of IEEE 802.22, this means coexistence of multiple nearby IEEE 802.22 cells.

**3.55 sensing mode:** A mode of operation of the spectrum sensing function that specifies the valid outputs of the spectrum sensing function.

**3.56 service flow:** Defines the QoS parameters for the PDUs that are exchanged on a connection, and provides a mechanism for upstream and downstream QoS management.

**3.57 service flow identifier (SFID):** A unique identifier for a service flow dealing with how higher layer packets/application sessions are mapped to their QoS requirements and scheduling constraints.

**3.58 signal type array (STA):** A one-dimensional array indicating which signal types the spectrum sensing function is to sense.

**3.59 spectrum manager:** The spectrum manager is the cognitive function at the BS that will use the inputs from the database service based on the geolocation at the BS and the customer premise equipment (CPE), as well as the input from the spectrum sensing automaton (SSA) at the BS and the CPEs to decide on the channel to be used by the WRAN cell as well as the EIRP limits imposed on the specific WRAN devices.

**3.60 spectrum sensing automaton:** Cognitive function resident at the BS and the customer premise equipment (CPE) that includes essential features to allow autonomous and directed sensing at the BS and at the CPE as well as proper CPE operation when it is not under the control of a BS.

**3.61 spectrum sensing function (SSF):** The function that observes the RF spectrum for a defined set of signal types and reports the results of its observations.

**3.62 station ID (SID):** A unique identifier for a customer premise equipment (CPE) under the control of a BS. This can reflect a single CPE, or a group of CPEs (e.g., multicast group).

**3.63 subchannel:** The basic unit of a logical channel used for subcarrier allocation in both downstream and upstream. A subchannel is composed of 28 subcarriers (24 data and 4 pilot subcarriers).

**3.64 subframe:** Formed by a number of bursts transmitted in the same direction (e.g., downstream subframe, upstream subframe).

**3.65 superframe:** Group of 16 frames initiated by the transmission from the BS of the superframe preamble and the Superframe Control header (SCH).

**3.66 Suplicant:** An entity at one end of a point-to-multipoint Wireless Regional Area Network (WRAN) link that seeks to be authenticated by an Authenticator attached to the other end of that link.

**3.67 symbol period:** Fundamental unit of duration in the time domain that is equal to the duration of an OFDM symbol in the time domain.

NOTE—See Table 200.

**3.68 time division duplex (TDD):** A duplex scheme where upstream and downstream transmissions occur at different times but may share the same transmission channel.

**3.69 transport connection:** A connection established to transport user data between the BS and a particular CPE.

**3.70 upstream:** The direction of the transmitted signal from a customer premise equipment (CPE) to the BS.

**3.71 upstream channel descriptor (UCD):** A medium access control (MAC) message that describes the PHY characteristics of an upstream transmission burst.

**3.72 upstream interval usage code (UIUC):** An interval usage code specific to an upstream burst. *See also: interval usage code.*

**3.73 upstream map (US-MAP):** A MAC message that defines the media access parameters (i.e., burst start time, burst length and subchannel usage) for the OFDMA upstream subframe for the CPEs scheduled to transmit toward the BS.

**3.74 wireless microphone:** A wireless microphone with licensed use of the TV broadcast bands (e.g., Part 73 and 74 devices in the U.S.) and equivalent low-power auxiliary devices allowed under the rules of various regulatory domains.

## 4. Abbreviations and acronyms

AAA	Authentication, Authorization, and Accounting
AAD	additional authenticated aata
AES	Advanced Encryption Standard
AK	authorization key
ARQ	Automatic Repeat Request
AU	antenna unit
BCC	binary convolutional coding
BE	best effort
BS	base station
BSN	block sequence number
BTC	Block Turbo Code
C-SAP	Control Service Access Point
CA	Certificate Authority
CBP	Coexistence Beacon Protocol
CC	confirmation code
CDMA	Code Division Multiple Access
CID	connection identifier
CINR	carrier-to-interference and noise ratio
CNR	carrier-to-noise ratio
CoS	class of service
CP	cyclic prefix
CPE	customer premise equipment
CPS	Common Part sublayer
CRC	Cyclic Redundancy Check
CS	Convergence sublayer
CS SAP	Convergence sublayer Service Access Point
CTC	Convolutional Turbo Code
CTR	Counter Mode Encryption
DAMA	Demand Assigned Multiple Access
DCD	Downstream Channel Descriptor
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DIUC	Downstream Interval Usage Code
DS	downstream
DSA	Dynamic Service Addition
DSC	Dynamic Service Change
DSD	Dynamic Service Deletion
DSx	Dynamic Service Addition, Change, or Deletion
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
EIRP	Effective Isotropic Radiated Power
FID	flow ID
FCH	Frame Control Header
FC-DST	Frame Contention Destination
FC-SRC	Frame Contention Source
FCN	Frame Contention Number
FDD	Frequency Division Duplex
FFT	Fast Fourier Transform
GCM	Galois Counter Mode
GMAC	AES-GCM Message Authentication Code
GMH	generic MAC header

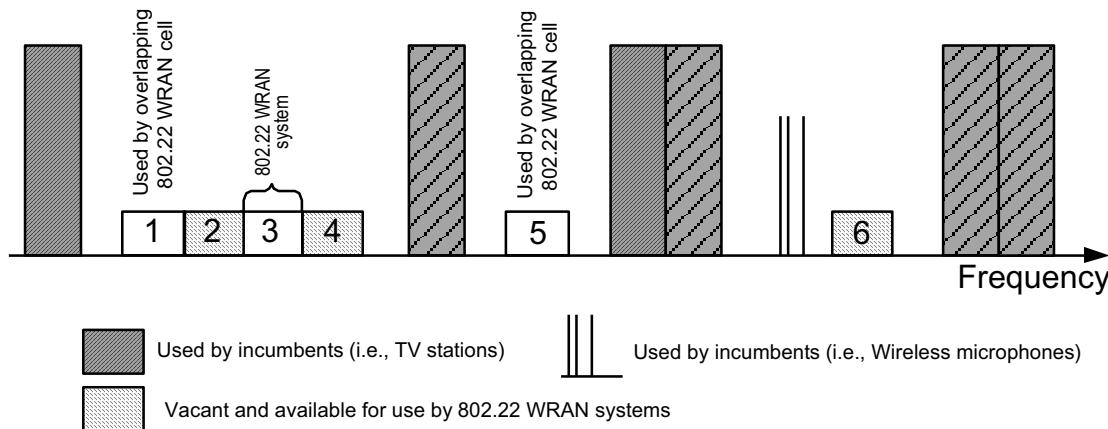
HCS	Header Check Sequence
IANA	Internet Assigned Numbers Authority
ID	identification
IDRP	Incumbent Detection Recovery Protocol
IE	information element
IETF	Internet Engineering Task Force
IFFT	Inverse FFT
IP	Internet Protocol
IUC	Interval Usage Code
LAN	Local Area Network
LBS	Location Based Service
LDPC	Low Density Parity Check Code
LLC	Link Layer Control
LSB	least significant bit
LTS	Long Training Sequence
M-SAP	Management Service Access Point
MAC	Medium Access Control Layer
MAC SAP	Medium Access Control Service Access Point
MIB	Management Information Base
MIC	Message Integrity Check
MPDU	MAC Layer Protocol Data Unit
MPEG	Moving Pictures Experts Group
MPFA	Maximum Probability of False Alarm
MPR	microphone protection radius (MPR)
MSB	most signification bit
MSDU	MAC Layer Service Data Unit
NCMS	Network Control and Management System
NCS	Network Control System
NMEA	National Marine Electronics Association
NMS	Network Management System
nrtPS	Non-real-time Polling Service
ODFC	on-demand frame contention
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access (To align with accepted usage, OFDMA is also used in this Standard to refer to the multi-user variant of OFDM.)
PAPR	Peak-to-Average Power Ratio
PDU	Protocol Data Unit
PER	Packet Error Rate
PHY	Physical Layer
PHY SAP	Physical Layer Service Access Point
PMP	point to multipoint
PN	Packet Number, also used for pseudo-noise
PPDU	Physical Layer Protocol Data Unit (PHY burst)
PRM	Protocol Reference Model
PSDU	Physical Layer Service Data Unit (equivalent to MPDU)
QAM	Quadrature Amplitude Modulation
QoS	quality of service
QPSK	Quadrature Phase-Shift Keying
RAN	Regional Area Network
ROHC	Robust Header Compression
RRM	Radio Resource Management
RS	Reed-Solomon
RSSL	Received WRAN Signal Strength
RSSI	Received Signal Strength Indication on the WRAN signal path or sensing path in sensing mode 2

RTG	Receive/Transmit Transition Gap
rtPS	Real-time Polling Service
SA	security association
SAID	security association identifier
SAP	service access point
SBTC	Shortened Block Turbo Code
SCH	Superframe Control header
SCM	Security for Control and Management
SCW	self-coexistence window
SDU	Service Data Unit
SFID	service flow identifier
SID	station ID
SM	spectrum manager
SM-SSF	Spectrum Manager, Spectrum Sensing Function Service Access Point
SAP	
SM-GL	Spectrum Manager, Geolocation Service Access Point
SAP	
SNMP	Simple Network Management Protocol
SNR	signal-to-noise ratio
SPD	Secondary Protecting Device
SPA	Signal Present Array
SSA	Spectrum Sensing Automaton
SSF	Spectrum Sensing Function
STS	Short Training Sequence
STA	Signal Type Array
SWS	Sensing Window Specification
SWSA	Sensing Window Specification Array
TCP	Transmission Control Protocol
TDD	time division duplex
TDM	Time Division Multiplex
TDMA	Time Division Multiple Access
TEK	Traffic Encryption Key
TFTP	Trivial File Transfer Protocol
TPC	Transmit Power Control
TTG	Transmit/Receive Transition Gap
TU	Time Unit corresponding to a nominal sampling period, (see Table 199)
TRU	transceiver unit
UCD	Upstream Channel Descriptor
UCS	urgent coexistence situation
UGS	Unsolicited Grant Service
UIUC	Upstream Interval Usage Code
US	upstream
WG	working group
WGS	World Geodetic System
WRAN	Wireless Regional Area Network

## 5. System architecture

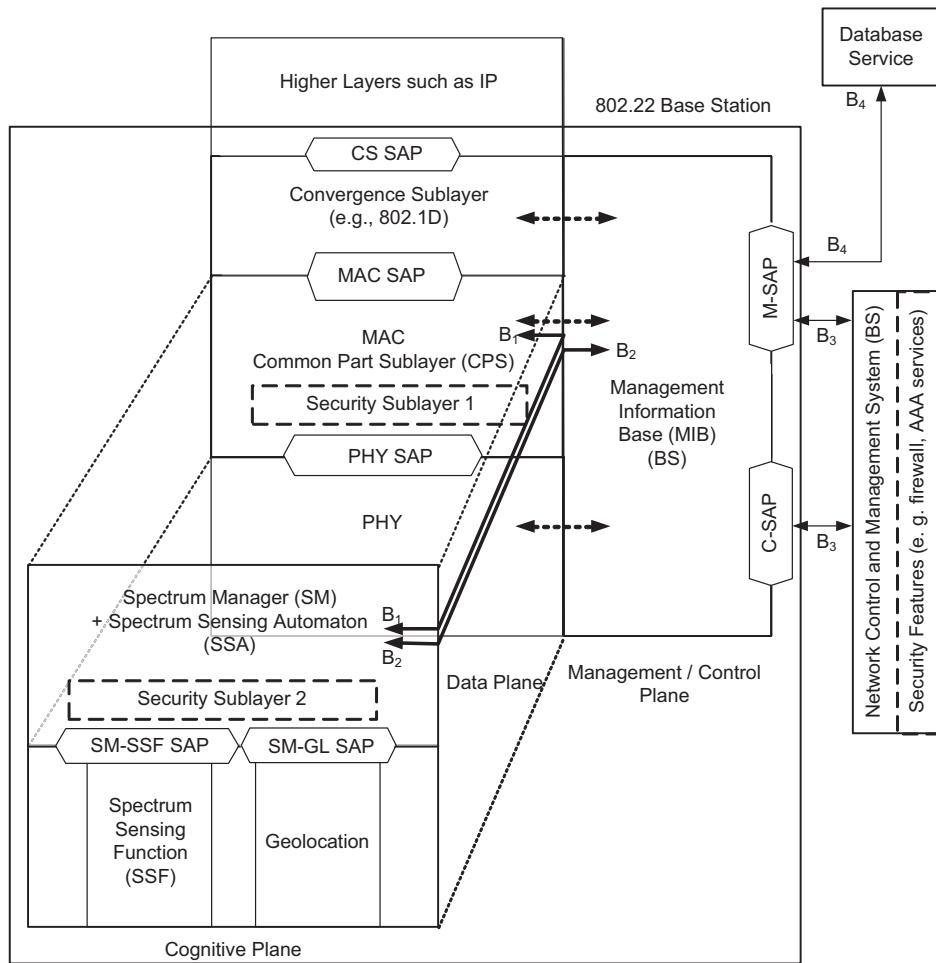
### 5.1 Reference architecture

The IEEE 802.22 reference architecture is depicted in Figure 3 and Figure 4. A unique characteristic of this architecture is its cognitive components. Spectrum availability in the TV bands can be fragmented, i.e., some channels can be occupied by incumbents in an area (see Figure 2) while others can be available for WRAN transmission, and this availability can vary in time. As shown in Figure 2, channel 3 is allocated to the IEEE 802.22 WRAN system, while channels 1 and 5 are in use by overlapping IEEE 802.22 cells. Channels 2, 4, and 6 would be available for more WRAN services in the area. Also, proper frequency separation is enforced in order to protect incumbent services using cognitive radio techniques—the air interface must be frequency agile, must adjust to the fragmented and time-varying spectrum availability, and must avoid interference to the TV band incumbent services. The required functional capabilities of these cognitive radio techniques are established in this standard (see Clause 10). In particular, the cognitive components of the system architecture must keep track of multiple channels, know which of these channels are occupied by incumbents and which can be used for WRAN transmission, allow for dynamic frequency selection, and avoid interference to incumbents on a real-time basis.

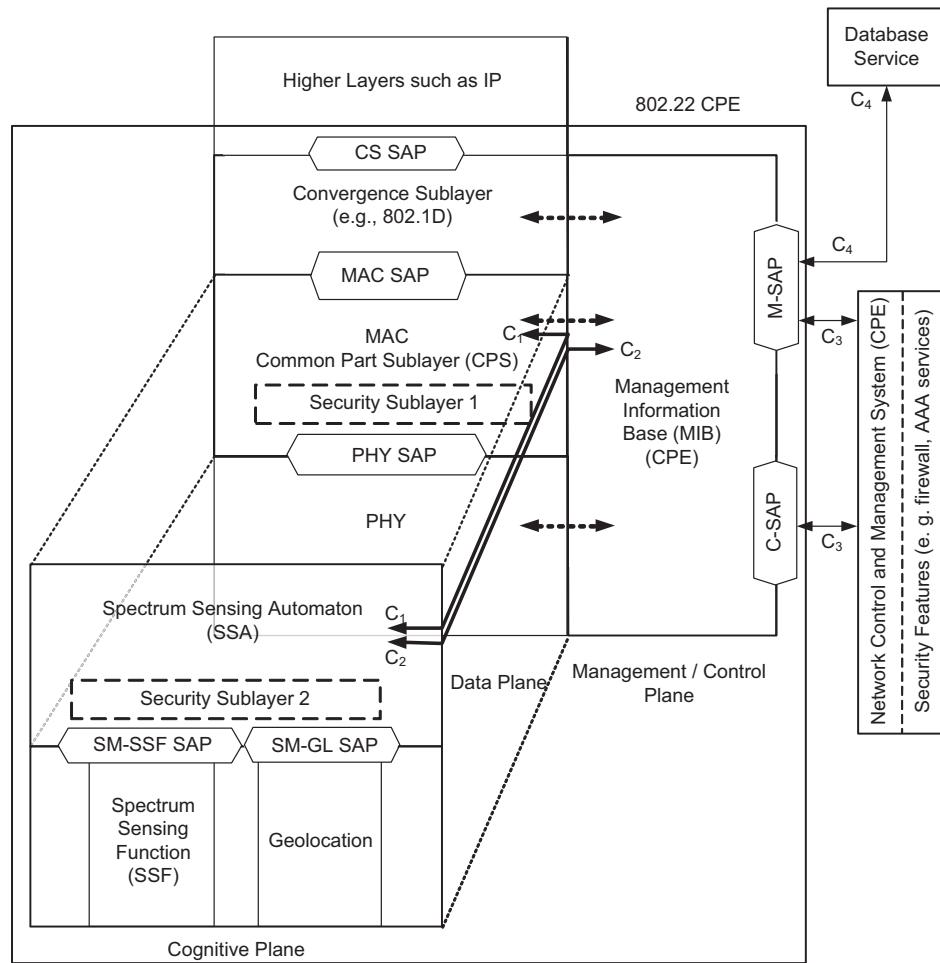


**Figure 2 — Illustrative diagram of spectrum allocations in TV bands**

The Protocol Reference Model (PRM), shown in Figure 3 and Figure 4, keeps the usual data and management/control plane functionality intact, while creating a new cognitive plane to support the cognitive radio capabilities. The data plane must carry the normal data as well as the management and control information. Figure 3 and Figure 4 show the PRMs at the BS and at the CPE respectively.



**Figure 3 — Protocol Reference Model (PRM) of the IEEE 802.22 BS**



**Figure 4 — Protocol Reference Model (PRM) of the IEEE 802.22 CPE**

### 5.1.1 Data plane

The data plane consists of the Physical Layer (PHY), the Medium Access Control (MAC) layer and the Convergence sublayer (CS). Service Access Points (SAPs) are added in between these layers to allow modularization of the system where different components may be disjointed and/or from different vendors. A SAP is provided with a well-defined interface or set of primitives to exchange the information, by virtue of which these different components can talk to each other.

The Data & Control/Management plane of the MAC shall be comprised of three sublayers: service-specific CS, the MAC Common Part sublayer (CPS), and the security sublayer 1. The service-specific CS shall provide transformation or mapping of external network data that is received through the CS SAP, into MAC Service Data Units (SDUs) and data that is received by the MAC CPS through the MAC SAP. This transformation or mapping shall include classifying external network SDUs and associating them to the proper MAC service flow identifier (SFID) and flow identifier (FID). Multiple CS specifications are provided for interfacing with various protocols. The internal format of the CS payload is unique to the CS, and the MAC CPS is not required to understand the format of or parse any information from the CS payload.

The MAC Common Part sublayer shall provide the core MAC functionality of system access, connection establishment, and connection maintenance. The data that the MAC layer receives from the various CSs

through the MAC SAP shall be classified to particular MAC connections. An example of the MAC CPS service definition is given in Clause 6. QoS is applied to the transmission and scheduling of data over the PHY. The MAC security sublayer 1 shall provide mechanisms for authentication, secure key exchange, encryption, etc. Data, PHY control, and monitoring statistics (spectrum sensing, RSSI, RSSL, etc.) shall be transferred between the MAC CPS and the PHY via the PHY SAP.

### **5.1.2 Management/control plane**

The management/control plane shall consist of the Management Information Base (MIB). SNMP is used to communicate with the MIB database and some of its primitives may be used to manage the network entities (BS, CPE, switches, routers, etc.). The MIB primitives shall be used for system configuration, monitoring statistics, notifications, triggers, CPE and session management, Radio Resources Management (RRM), communication with the database service, spectrum sensing and geolocation reporting, etc. The MIB data may be obtained either from the network, pre-defined within the system, or obtained from another device (e.g., BS) after an exchange of information using SNMP over the communication medium.

### **5.1.3 Cognitive plane**

The cognitive plane shall be comprised of the Spectrum Sensing Function (SSF), the Geolocation (GL) function, the Spectrum Manager/Spectrum Sensing Automaton (SM/SSA) and a dedicated security sublayer 2.

The SSF shall implement spectrum sensing algorithms and the GL module shall provide the information to determine the location of the IEEE 802.22 device (BS or CPE). The SSF and the GL modules are described in 10.7.4 and 10.7.5, respectively.

#### **5.1.3.1 Spectrum Manager (SM)**

The SM shall reside in the cognitive plane of the BS at the same layer as the MAC CPS in the data plane as shown in Figure 3. The SM shall maintain spectrum availability information, manage channel lists, manage quiet periods scheduling, and implement coexistence mechanisms. The SM shall also take requests from the MAC/PHY. For example, the MAC must inform the SM if an interference situation has been detected (e.g., with incumbents or other IEEE 802.22 cells) during normal operation in the channel. The SM must then take appropriate actions to resolve the issue such as moving to another channel (as specified in 10.2.3). In order to do this, the SM must first provide sufficient quiet period time for the CPEs to carry out in-band sensing (on channels N and N±1) to clear these channels within the specified channel monitoring requirement (see Annex A), and then keep an updated list of backup and candidate channels in a prioritized order and make sure that the CPEs have enough idle time to clear a sufficient number of backup channels. If an incumbent is found from the in-band sensing, the MAC shall use the informed response from the SM to perform the switching operation.

The SM has a key role in the overall architecture as it is the central point at the BS where all the information on the spectrum availability resulting from the database service and the spectrum sensing function is gathered. Based on this combined information, local regulations, and predefined SM policies (as specified in 10.2.5), the SM shall provide the necessary configuration information to the MAC, which shall remotely configure all the registered CPEs. Explicit connections B<sub>1</sub> and B<sub>2</sub> are shown in Figure 3 . This signifies that different kinds of information are exchanged between the SM and the MAC, and the SM and the MIBs. Connection B<sub>2</sub> shall be used for configuration of the SM at the BS, transmission of the available channel list to the SM, as well as reporting the RF environment information via the MIBs. Connection B<sub>1</sub> shall be used by the SM to initiate channel move, to configure the SSA at the CPE (backup/candidate channel list, specific channels to be sensed, etc.) as well as to gather information from the CPEs (local sensing information, local geolocation information, etc.).

The functions of the SM are described in 10.2.

### 5.1.3.2 Spectrum Sensing Automaton (SSA)

A simpler spectrum management entity, called Spectrum Sensing Automaton, is present at the BS and at the CPEs and independently implements specific procedures for sensing the RF environment at initialization of the BS and before the registration of a CPE with the BS. The SSA at the CPE shall also include essential features to allow proper operation when the CPE is not under the control of a BS such as independent procedures during initialization and channel change and, while the CPE is idle, the SSA shall conduct out-of-band sensing and report to the BS so that it can refresh the status of the channels in the backup/candidate channel list. At any other time, the SSA at the CPE is under the control of the SM. The SSA at the BS is also active when the BS is not transmitting to conduct out-of-band sensing. The SSA located at the BS can also carry-out sensing to clear channels when the base station is not transmitting. The functions of the SSA are described in 10.3.

Explicit connections  $C_1$  and  $C_2$  at the CPE are shown in Figure 4. Connection  $C_2$  shall be used to convey the environment monitoring information (e.g., list of service providers detected) via the MIBs to the CPE local interface in order to allow for the choice of the WRAN service by a professional installer through upper layers at the CPE. Connection  $C_1$  shall be used to convey the local environment information such as sensing and geolocation to the BS.

### 5.1.3.3 Security sublayer 2

In addition to the security sublayer 1 at the data plane, security sublayer 2 is introduced in the cognitive plane. Security sublayer 2 enhances the security for the cognitive radio based access. The detailed operation of the security sublayers 1 and 2 are described in Clause 8. The functions of the security sublayers 1 and 2 must ensure spectrum and service availability; provide data and signal authentication; as well as ensure data, control and management message integrity, confidentiality and non-repudiation. The role of the security sublayer 2 is to provide enhanced protection to the incumbents as well as necessary protection to the IEEE 802.22 systems. If the IEEE 802.22.1 beacon has to be detected in the given regulatory domain and the transmission needs to be authenticated, the security sublayer 2 shall be used along with the security mechanism provided (ECC-based signature) to authenticate this beacon. Similarly, security sublayer 1 shall be used to authenticate a CBP packet originating from a neighboring cell CPE.

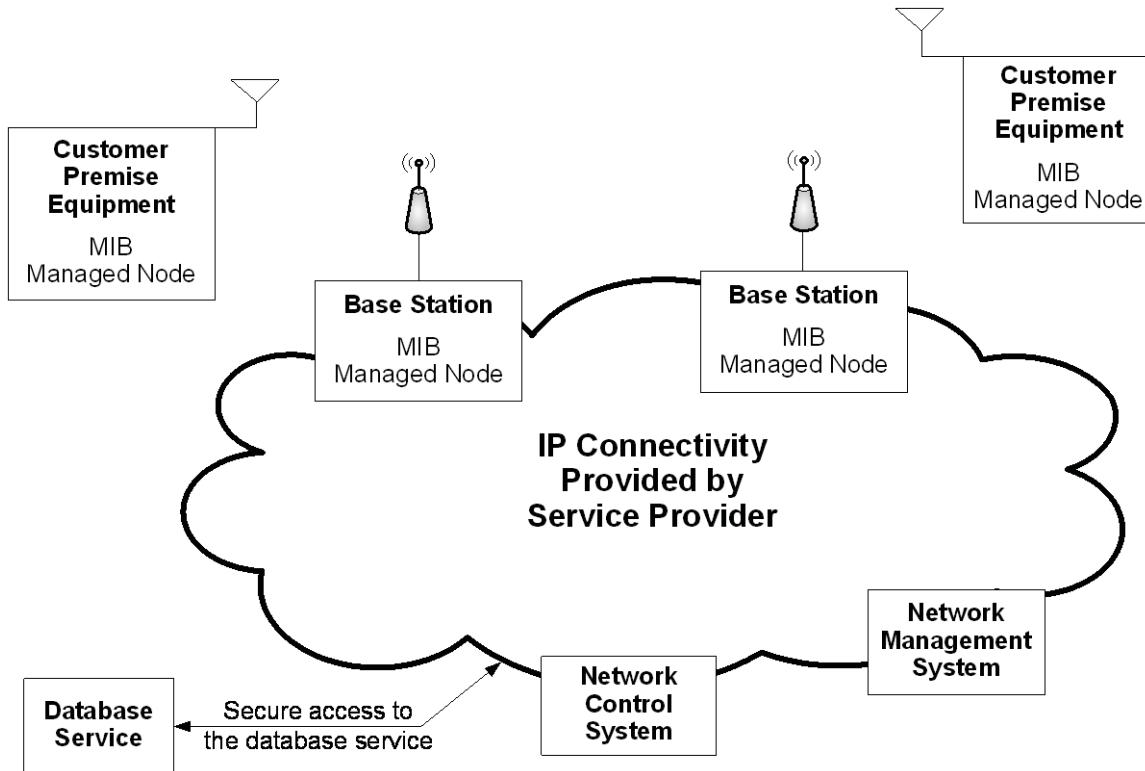
## 5.2 Management reference architecture

IEEE 802.22 network cells consist of a base station and up to 512 Customer Premise Equipment (CPE) devices or groups of devices. IEEE 802.22 networks may contain multiple cells. For multiple cells operation, interfacing with entities for management and control purposes is required. This standard refers to an abstract “black box” Network Control and Management System (NCMS) containing these entities. The NCMS allows the PHY/MAC layers specified in this standard to be independent of the network architecture, the transport network, and the protocols used at the backend and therefore allows greater flexibility. NCMS logically exists at the BS and CPE sides of the radio interface, termed NCMS (BS) and NCMS (CPE) respectively. Any necessary inter-BS coordination is handled through the NCMS (BS).

Figure 5 shows a management reference model for WRAN networks. It consists of a Network Management System (NMS), a Network Control System (NCS) and managed nodes. The BS and CPEs shall collect and store the managed objects (see 5.2.4) in the format as defined in the WRAN Management Information Base (MIB). The MIB is defined and specified in Clause 13. The Network Control System contains the service flow and the associated QoS information that is pre-populated in service classes at the BS and instantiated when a CPE requests services.

Interfaces B4 in Figure 3 and C4 in Figure 4 describe the interface between the CPE/BS and the database service. These interfaces are used to register with the database and request a set of available channels. Interfaces B3 in Figure 3 and C3 in Figure 4 describe the interface between the CPE/BS and the NCMS.

The management information between the CPE and the BS may be carried over a secondary management connection. The management information can also be conveyed using the normal SNMP messages.



**Figure 5 — Management reference model**

Examples of services that may be provided by the NCMS include: Authentication, Authorization, and Accounting (AAA) services, Radio Resources Management (RRM) services, security services, Service Flow Management services, Location-Based services (LBS) management, and Network Management services.

### 5.2.1 PHY/MAC to NCMS interface

The NCMS is interfaced to the MAC and PHY layer entities of the CPE and BS through two Service Access Points (SAPs). The BS and CPE shall include a Control-SAP (C-SAP) and Management-SAP (M-SAP) that provide NCMS access to the control plane and management plane functions from upper layers. The M-SAP is used for less time sensitive Management plane primitives and the C-SAP is used for more time-sensitive Control Plane primitives. The C-SAP and M-SAP interfaces are described in 5.2.1.1 and 5.2.1.2. The NCMS uses the C-SAP and M-SAP to interface with the IEEE 802.22 managed nodes.

#### 5.2.1.1 Management SAP (M-SAP)

The Management SAP may include, but is not limited to primitives related to the following:

- System configuration
- Monitoring statistics
- Notifications/Triggers
- Sensing and Geolocation reporting

- Communication with the database service

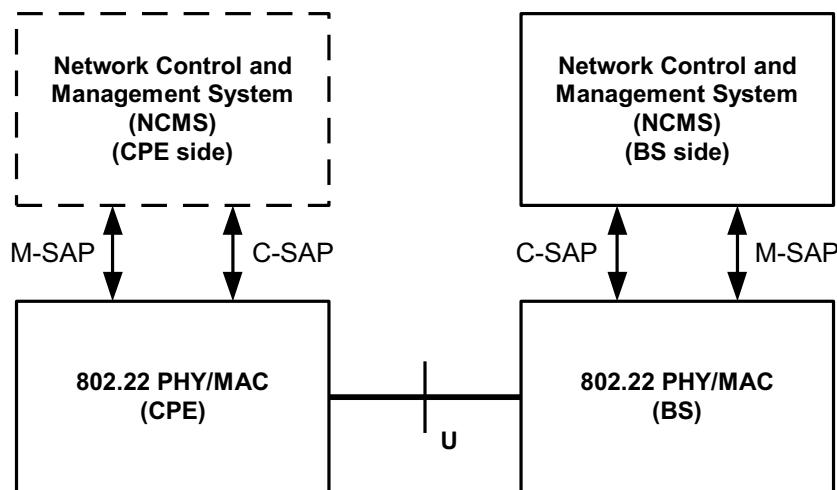
### 5.2.1.2 Control SAP (C-SAP)

The Control SAP may include, but is not limited to primitives related to the following:

- Subscriber and Session management
- Security context management
- Radio Resource Management
- AAA server signaling, etc.

### 5.2.2 Network Reference Model

Figure 6 describes a simplified network reference model. Multiple CPEs may be attached to a BS. CPEs communicate to the BS over the U interface using a Basic Management Connection, a Primary Management Connection, or a Secondary Management Connection (see 7.2).



**Figure 6 — IEEE 802.22 Network Reference Model**

### 5.2.3 CPE and BS Interface

This standard observes the following correlation:

- MAC management PDUs that are exchanged on the basic management connection trigger or are triggered by primitives that are exchanged over the C-SAP.
- MAC management PDUs that are exchanged on the primary management connection trigger or are triggered by primitives that are exchanged over either the C-SAP or the M-SAP depending on the particular management or control operation.
- Messages that are exchanged over the secondary management connection trigger or are triggered by primitives that are exchanged over the M-SAP.

### 5.2.4 Managed objects

The definition of managed objects in this standard is expressed in IETF RFC 2578. It supports a management protocol agnostic approach, including SNMP.

## 6. Packet Convergence sublayer

The Packet Convergence sublayer (CS) resides on top of the MAC Common Part sublayer (CPS). The CS shall perform the following functions using classification governed by rules (see 6.3.2 or 6.4.2) defined by the implementer/operator to process higher layer SDUs so they can be sent and received by the IEEE 802.22 BS and CPE. This process can be broken down into the following four steps, each utilizing the services of the MAC:

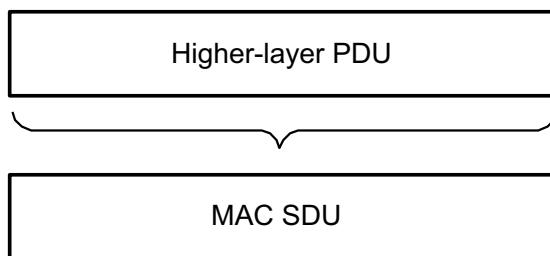
- Receiving higher-layer packet protocol data units (PDUs) from the higher layer
- Classifying the higher-layer PDUs into the appropriate connection
- Delivering the resulting CS PDUs to the MAC SAP associated with the service flow for transport to the peer MAC SAP
- Receiving the CS PDUs from the peer MAC SAP

The sending CS is responsible for delivering the MAC SDU to the MAC SAP. The MAC is responsible for delivery of the MAC SDU to peer MAC SAP in accordance with the QoS, fragmentation, concatenation, and other transport functions associated with the service flow characteristics of a particular connection. The receiving CS is responsible for accepting the MAC SDU from the peer MAC SAP and delivering it to a higher-layer entity.

The packet CS is used for transport of the following two packet-based protocols supported by this standard, i.e., IEEE Std 802.3 (Ethernet) and Internet Protocol (IP).

### 6.1 MAC SDU format

Once classified and associated with a specific MAC connection, a higher-layer PDU shall be encapsulated in a MAC SDU according to the format illustrated in Figure 7.



**Figure 7 — MAC SDU format**

### 6.2 Classification

Classification is the process by which a MAC SDU is mapped onto a particular connection for transmission between MAC peers. The mapping process associates a MAC SDU with a connection, which also creates an association with the service flow characteristics of that connection. This process facilitates the delivery of MAC SDUs with the appropriate QoS constraints.

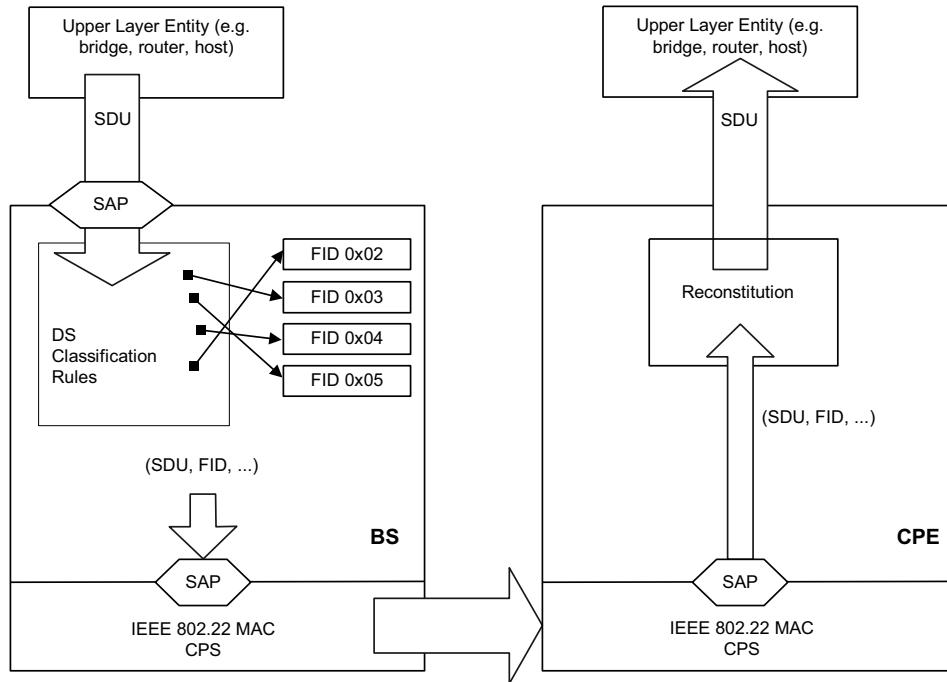
A classification rule is a set of matching criteria applied to each packet entering the IEEE 802.22 network. It consists of some protocol-specific packet matching criteria (destination IP address, for example), a classification priority, and a reference to a flow identifier (FID, see 7.2). If a packet matches the specified packet matching criteria, it is then delivered to the SAP for delivery on the connection defined by the FID and the station identifier (SID, see 7.2) assigned to the CPE. Classification rules, which are to be defined by the WRAN operator, shall be downloadable to the BS and CPEs in a uniform and standardized format at

the MIB level (see Clause 13) and shall be fully interoperable between the BS and CPEs. The service flow characteristics of the connection provide the QoS for that packet.

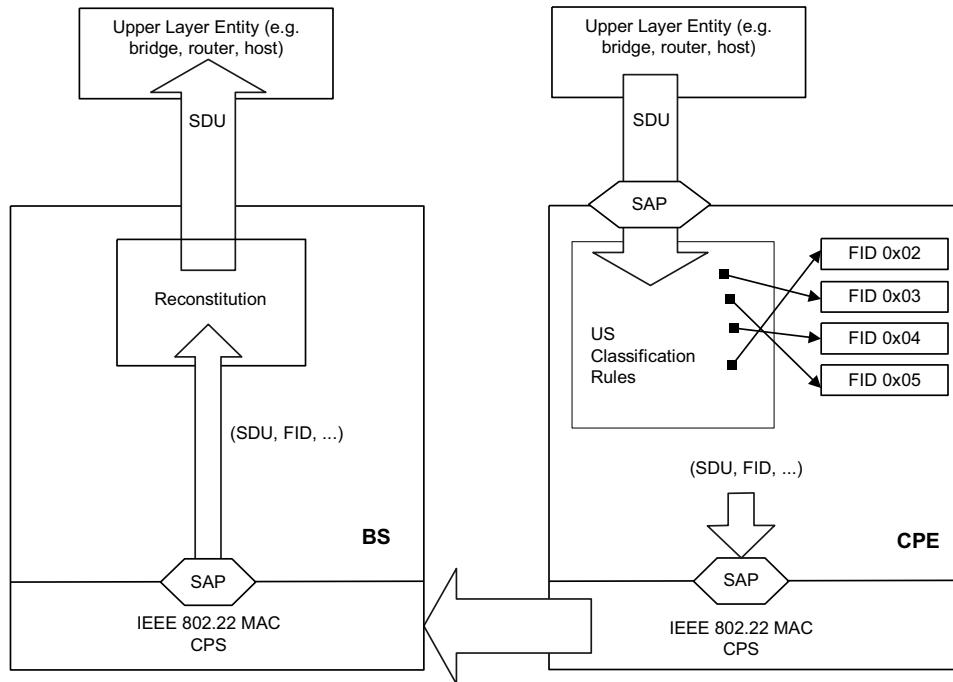
Several classification rules may each refer to the same service flow. The classification priority is used for ordering the application of classification rules to packets. Explicit ordering is necessary because the patterns used by classification rules may overlap. The priority needs not be unique, but care shall be taken within a classification priority to prevent ambiguity in classification. Downstream classification rules are applied by the BS to packets that it transmits and upstream classification rules are applied at the CPE. Figure 8 and Figure 9 illustrate the mappings discussed in the previous paragraph.

It is possible for a packet to fail to match the set of defined classification rules. In this case, the CS shall discard the packet.

The parameters for the classification rules shall be provided as MIB objects at the base station (see 13.1.3) and these parameters shall be downloaded from the BS to its associated CPEs for interoperability and consistency.



**Figure 8 — Classification and FID mapping (BS to CPE)**



**Figure 9 — Classification and FID mapping (CPE to BS)**

## 6.3 IEEE 802.3/Ethernet-specific part

### 6.3.1 IEEE 802.3/Ethernet CS PDU format

An IEEE 802.3/Ethernet packet PDU is directly mapped to a CS PDU (MAC SDU).

### 6.3.2 IEEE 802.3/Ethernet CS classification rules

The following parameters are relevant for IEEE 802.3/Ethernet CS classification rules:

- IEEE 802.3/Ethernet and VLAN headers shall be processed by zero or more of the LLC classification parameters (see 7.7.8.9.18.3.8 to 7.7.8.9.18.3.12).
- For IP over IEEE 802.3/Ethernet, IP headers may be included in classification (see 7.7.8.9.18.3.2 to 7.7.8.9.18.3.7 and 7.7.8.9.18.3.14).
- For IP headers compressed with ROHC (IETF RFC 3095 [B27], IETF RFC 3749 [B31], IETF RFC 3243 [B28], IETF RFC 4995 [B36], IETF RFC 3843 [B32], IETF RFC 4996 [B37]) only the LLC parameters shall be used for classification (see 7.7.8.9.18.3.8 through 7.7.8.9.18.3.12).

Use of IP header compression (ROHC) is negotiated during registration (REG-REQ/RSP) and enabled during service flow setup.

## 6.4 IP specific part

This subclause applies when IP (IETF RFC 791 [B17], IETF RFC 2460 [B23]) is carried over the IEEE 802.22 network.

IPv6 CS requirements are only applicable if IPv6 support is enabled during registration.

#### **6.4.1 IP CS PDU format**

An IP packet PDU is directly mapped to a CS PDU (MAC SDU).

#### **6.4.2 IP classification rules**

IP classification rules operate on the fields of the IP header and the transport protocol. Classification rules shall be the same as long as the MIB is defined. Classification rules will be downloaded from the BS to its associated CPEs for interoperability and consistency (see 6.2). IP classification rules shall be based on the IP classification parameters (see 7.7.8.9.18.3.2 through 7.7.8.9.18.3.7 and 7.7.8.9.18.3.14).

## 7. MAC Common Part sublayer

This clause describes the MAC layer used by the IEEE 802.22 WRAN point-to-multipoint medium access control standard. The MAC provides tools for protection of TV bands incumbent services as well as for coexistence. The MAC is connection-oriented and provides flexibility in terms of QoS support. The MAC regulates downstream medium access by TDM, while the upstream is managed by using a DAMA/OFDMA system. In the MAC, the BS manages all the activities within its IEEE 802.22 cell and the associated CPEs are under the control of the BS.

### 7.1 General

In an IEEE 802.22 cell, multiple CPEs are managed by a single BS that controls the medium access. The downstream is TDM where the BS transmits and the CPE receives. The upstream transmissions, where the CPEs transmit and the BS receives, are shared by CPEs on a demand basis, according to a DAMA/OFDMA scheme. Depending on the class of service (CoS) utilized, a CPE may be issued continuing rights to transmit, or is dynamically allocated by the BS after receipt of a request from the CPE. The MAC supports unicast (addressed to a single CPE), multicast (addressed to a group of CPEs) and broadcast (addressed to all CPEs in a cell) services.

The MAC implements a combination of access schemes that efficiently control contention between CPEs within a cell and overlapping cells sharing the same channel while at the same time attempting to meet the latency and bandwidth requirements of each user application. This is accomplished through four different types of upstream scheduling mechanisms that are implemented using: unsolicited bandwidth grants, polling, and two contention procedures (i.e., MAC header and CDMA based). The use of polling simplifies the access operation and attempts to allow applications to receive service on a deterministic basis if it is required.

The MAC is connection-oriented, and as such, connections are a key component that require active maintenance and hence can be dynamically created, deleted, and changed as the need arises. A connection defines both the mapping between convergence processes at CPEs and BS and the related service flow (one connection per service flow). For the purposes of mapping to services on CPEs and associating varying levels of QoS, all data communications are instantiated in the context of a connection and this provides a mechanism for upstream and downstream QoS management. In particular, the QoS parameters are integral to the bandwidth allocation process as the CPE requests upstream bandwidth on a per connection basis (implicitly identifying the service flow). The BS, in turn, grants bandwidth to a CPE as an aggregate of grants in response to per-connection requests from the CPE.

### 7.2 Addressing and connections

Each IEEE 802.22 base station and CPE shall have a 48-bit universal MAC address, as defined in IEEE Std 802-2001. This address uniquely defines the base station and CPE from within the set of all possible vendors and equipment types. It is used as part of the authentication process by which the BS and CPE each verify the identity of the other at the time of network association. It is used as part of the authentication process by which the BS and CPE each verify the identity of the other at the time of network association. The BS MAC address is broadcast by the BS and is present in every CBP burst, being part of the Superframe Control header (SCH) data. Each WRAN device regularly broadcasts a CBP burst containing its Device ID and Serial Number. This is done as part of the device's self-identification process that helps identify potential interference sources to incumbent services and for coexistence purposes.

Connections are identified by two items, a 9-bit station ID (SID) and a 3-bit flow ID (FID). The SID uniquely identifies a station that is under the control of the BS. A SID can be for a unicast station, when referencing a single CPE, or for a multicast station, when referencing a multicast group (of CPEs). A FID identifies a particular traffic flow assigned to a CPE. The tuple of SID and FID (SID | FID) forms a connection identifier (CID) that identifies a connection for the CPE. The SID is signaled in the DS/US-MAP allocation, and the FID is signaled in the generic MAC header (GMH) of a MAC PDU. This allows for a total of up to 512 stations, each with a maximum of eight flows that can be supported within each downstream and upstream channel.

At CPE initialization, three flows shall be dedicated for management connections (see 12.2) for the purpose of carrying MAC management messages and data between a CPE and the BS. The three flows reflect the fact that there are inherently three different levels of QoS for traffic sent on management connections between a CPE and the BS. The basic flow is used by the BS MAC and CPE MAC to exchange short, time-urgent MAC management messages; whereas, the primary management flow is used by the BS MAC and CPE MAC to exchange longer, more delay-tolerant MAC management messages (Table 19 specifies which MAC management messages are transferred on which type of connections). Finally, the secondary management flow is used by the BS and CPE to transfer more delay tolerant, standards-based (e.g., DHCP, TFTP, and SNMP) messages that are carried in IP datagrams. The secondary management flow may be packed and/or fragmented, similarly to the primary management except that no ARQ should be used for the latter since it is more time critical.

The FIDs for these connections shall be assigned according to the specification in 12.2. The same FID value is assigned to both upstream and downstream members of each connection.

The CID, which is a tuple of SID | FID, can be considered a connection identifier even for nominally connectionless traffic like IP, since it serves as a pointer to destination and context information.

Many higher-layer sessions may operate over the same wireless connection. For example, many users within a company may be communicating with Transmission Control Protocol (TCP)/IP to different destinations, but since they all operate within the same overall service parameters, all of their traffic is pooled for request/grant purposes. A service flow is a unidirectional flow of traffic (BS to CPE, or CPE to BS) that defines the mapping of higher-layer application service parameters (e.g., QoS) to a FID assigned to a particular CPE's unicast SID or multicast group (multicast SID).

The type of service and other current parameters of an application service are implicit in the SFID. A service flow definition may be accessed reading the appropriate service flow MIB (see 13.1.3) indexed by the SFID of the service flow assigned to a particular CPE.

Service flow, once established, may require active maintenance. The maintenance requirements vary depending upon the type of service connected. Modifiable service flows may require maintenance due to stimulus from either the CPE or the network side of the connection.

Service flow may also be terminated. This generally occurs only when a subscriber's service has changed or when the base station has not been able to communicate with the CPE. The BS or CPE can terminate a service flow.

Service Flow Management functions are supported through the use of static configuration and dynamic addition, modification, and deletion of service flow parameters and/or service flows themselves as described in 7.18.

### 7.3 General superframe structure

The IEEE 802.22 WRAN system includes two operational modes: a normal mode and a self-coexistence mode. In normal mode, one WRAN cell occupies one channel and operates on all the frames in a superframe; while in self-coexistence mode, multiple WRAN cells share the same channel and each coexisting WRAN cell operates on one or several different frames exclusively.

When operating in normal mode, a WRAN cell shall transmit the Superframe Control header (SCH) at the beginning of the first frame of a superframe on the operating channel; when operating in self-coexistence mode, a WRAN cell shall transmit its SCH at the beginning of the first frame allocated to it in the superframe. The structure of the SCH for both normal mode and self-coexistence mode can be found in 7.5.1. A WRAN runs in normal mode by default and transits to self-coexistence mode when the WRAN can detect and decode an SCH or a CBP from an adjacent WRAN cell on its operating channel.

#### 7.3.1 General superframe structure for normal mode

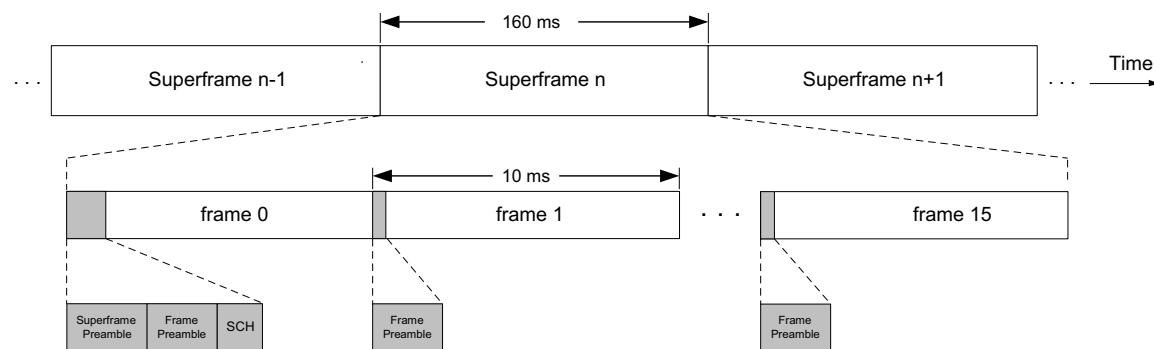
The superframe structure depicted in Figure 10 shall be used and the first frame shall be constituted of the following:

- A PHY superframe preamble, see Clause 9
- A PHY frame preamble, see Clause 9
- A Superframe Control header (SCH), see 7.5.1
- The rest of the first frame including its frame header and data payload

This first frame is then followed by 15 frames that each include a frame preamble, a frame header, and the data payload. See 7.4.

At the beginning of every superframe, the BS shall transmit the superframe preamble and the SCH on the operating channel using the modulation/coding specified in 9.4.1.2 and Table 202 respectively. In order to associate with a base station, a CPE must receive the SCH to establish communication with the BS. During each MAC frame, the BS shall manage the upstream and downstream operations, which may include ordinary data communication, measurement activities, coexistence procedures, and so on.

The superframe shall start with a superframe preamble, followed by the first frame preamble, the SCH, and finally the first frame payload. The first frame payload shall be reduced by two symbols with 1/4 cyclic prefix to keep the frame size consistent.

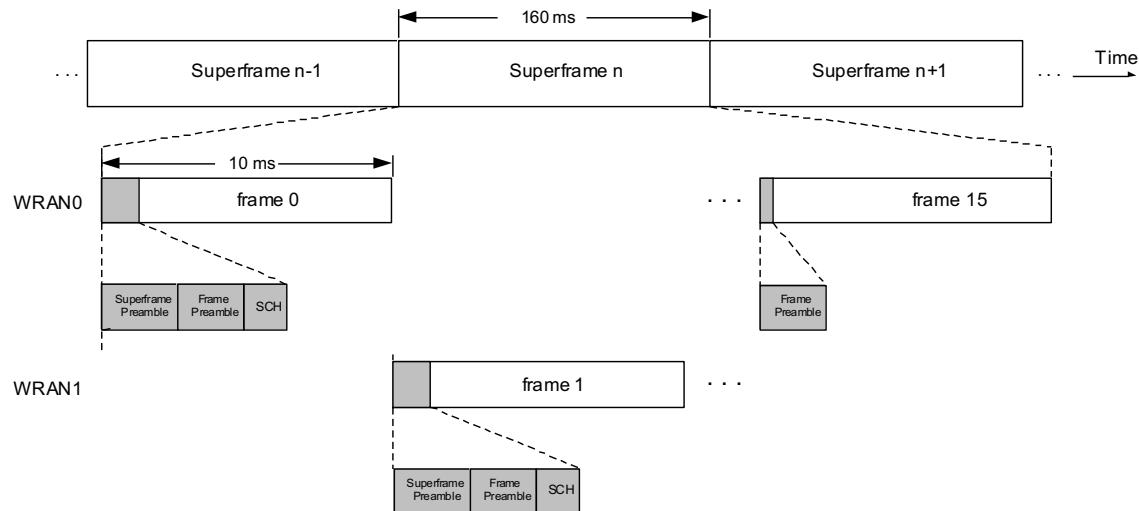


**Figure 10 — General superframe structure**

### 7.3.2 General superframe structure for self-coexistence mode

The superframe structure in self-coexistence mode is shown in Figure 11. The self-coexistence mode is for the scenario when multiple BSs with overlapping coverage have to share the same channel. The frequency reuse factor cannot be maintained as one due to their mutual interference. In this case, these BSs shall share the channel on a per frame basis, i.e., each BS is allocated a subset of the frames of a superframe on a non-interference basis. The negotiation process of frame allocation can be found in 7.20.3.

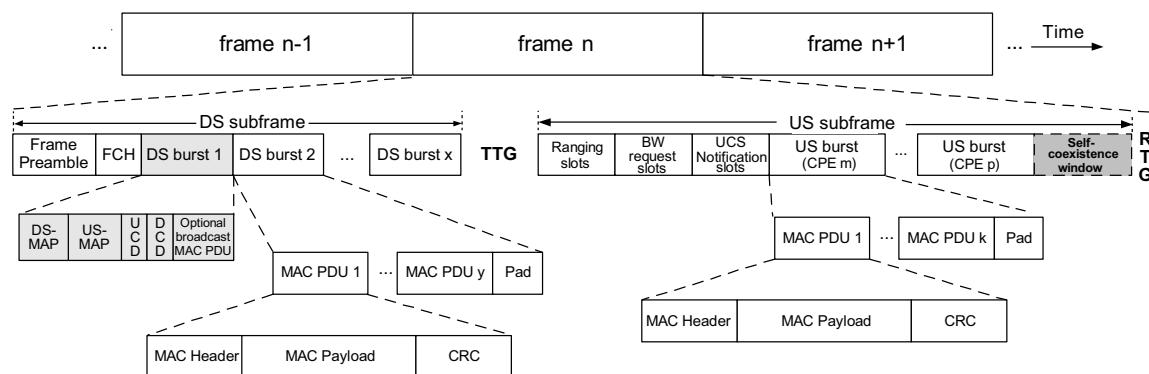
In self-coexistence mode, the BS shall transmit its superframe preamble, frame preamble and SCH during the first active frame allocated to it. The BS and CPEs in a WRAN cell shall only transmit during the active frames allocated to that WRAN cell. They can only transmit during other frames when a self-coexistence window (SCW) has been scheduled. During the frames not allocated to the present cell, the BS and CPEs may monitor the channel for any transmission from neighboring WRAN cells to improve self-coexistence.



**Figure 11 — General superframe structure in the self-coexistence mode**

### 7.4 General frame structure

The top-down time division duplex (TDD) frame structure employed in the MAC is illustrated in Figure 12.



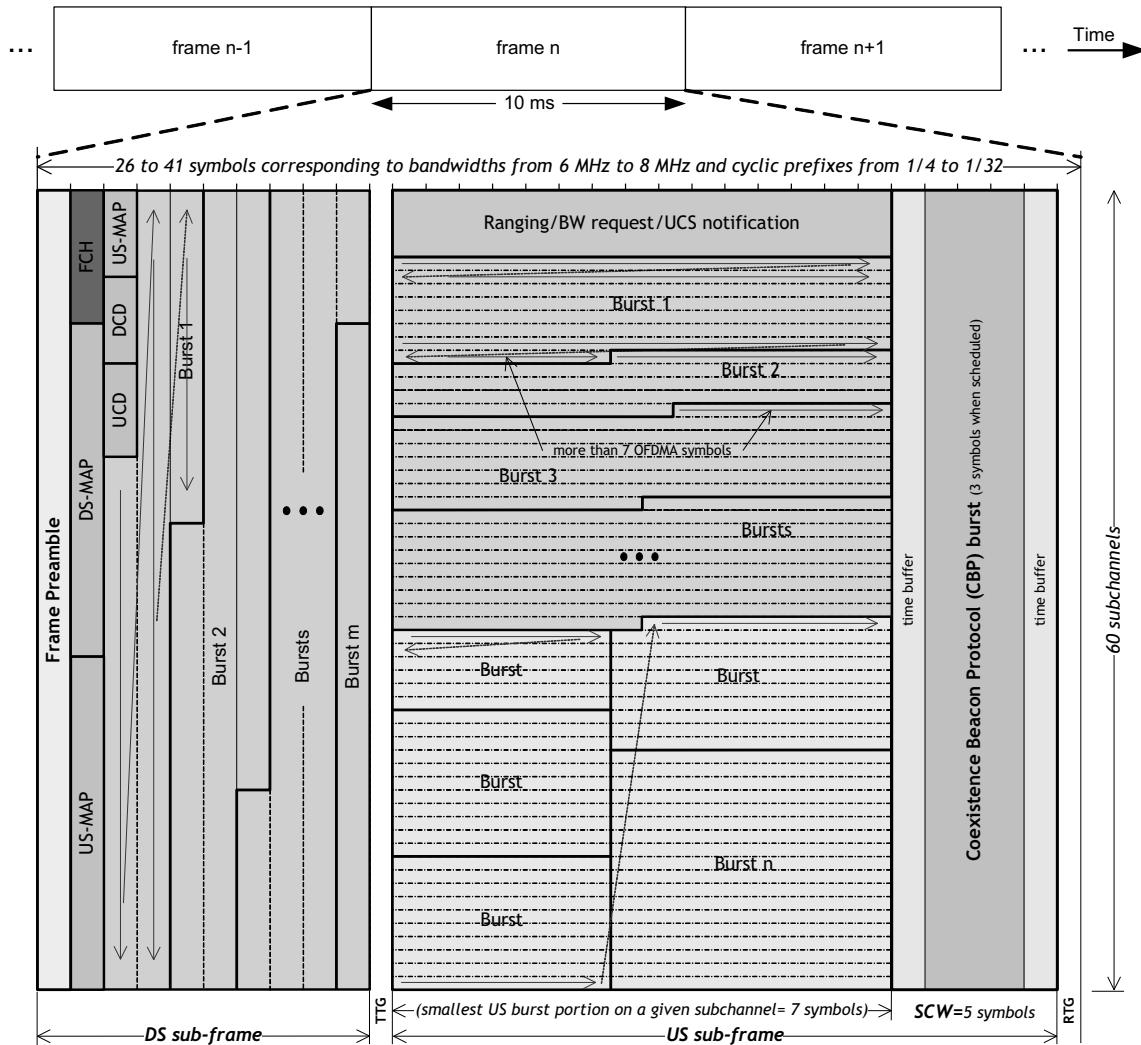
**Figure 12 — MAC Frame structure**

As illustrated in Figure 12, a frame is comprised of two parts: a downstream (DS) subframe and an upstream (US) subframe. A portion of the US subframe may be allocated as a window to facilitate self-coexistence. This SCW may be scheduled by the base station at the end of the US subframe when necessary to allow transmission of opportunistic coexistence beacon protocol bursts. The SCW includes the necessary time buffers to absorb the difference in propagation delay between close-by and distant base stations and CPEs operating on the same channel. The boundary between the DS and US subframes shall be adaptive to adjust to the downstream and upstream relative capacity. The upstream subframe may contain scheduled upstream PHY PDUs, each transmitted from different CPEs for their upstream traffic. It may also include contention intervals scheduled for the following:

- CPE association (initial ranging)
- CPE link synchronization, power control and geolocation (periodic ranging)
- Bandwidth request
- Urgent coexistence situation (UCS) notification
- Quiet period resource adjustment

The definitions of the fields/messages are given in 7.6 and 7.7.

The PHY PDUs depicted in Figure 12 may be transmitted across several subchannels as shown in Figure 13, which depicts how a frame may be transmitted (in time and frequency) by the PHY layer.



**Figure 13 — Example of a time/frequency structure of a MAC frame**

Figure 13 shows an example of the two-dimensional (time/frequency) structure of the MAC frame that shall consist of an integer number of fixed size OFDM slots. Each slot shall consist of one OFDM symbol by one subchannel (i.e., 1 OFDM slot = 1 symbol × 1 subchannel). To help understand Figure 13, the MAC packets are assumed to be structured in a linear TDM manner (see Figure 12) while the PHY packets are arranged in a two-dimensional time/frequency domain (symbol in the horizontal direction, logical subchannels in the vertical direction). For the FCH, the DS/US-MAP, the DCD, and UCD, as well as for the downstream payload, the MAC information is first laid vertically by subchannels then stepped horizontally in the time direction. This vertical layering allows early scheduling of DS bursts assigned to distant CPEs to compensate for propagation delays and to avoid potential interference at the CPE in the case of overlapping WRAN cells with different DS/US capacity split.

The MAC data elements from Figure 12, starting from the FCH and including the first broadcast burst, shall be entered into the second OFDM symbol, as shown in Figure 13, in the increasing order of logical subchannels until all logical subchannels are occupied. Then, the subsequent data elements, if they have not all been mapped, shall be placed in the same order on the following OFDM symbols. The balance of the last OFDM symbols shall be padded with zeros. The modulation and coding schemes for the padding zeros are defined by the DIUC for the last DS burst in the DS-MAP. Note that the DS-MAP indicates the length of the contiguous DS MAC elements, not their absolute position in the DS subframe.

The MAC data elements that are contained in upstream bursts shall be mapped to the US subframe in a different order as shown in Figure 13. They are first mapped horizontally, OFDM symbol by OFDM symbol, in the same logical subchannel. Once a logical subchannel has been filled to the end of the upstream subframe, the balance of the MAC data elements shall be mapped to the next logical subchannel, in an increasing subchannel order. This process continues until all of the subchannels and symbols allocated to the burst are filled. If the quantity of MAC data elements is insufficient to fill an upstream burst so that an integer number of OFDMA slots is occupied once encoded, zero padding shall be inserted at the end.

Alternatively, the horizontal laying of the MAC data elements may fill one subchannel with at least 7 OFDM symbols at a time and continue on the following subchannels. However, when all logical subchannels have been filled, the next MAC data elements shall be placed in the first available logical subchannel in the following burst. The width of the last vertical burst will be between 7 and 13 symbols depending on the total number of symbols in the upstream subframe.

The long upstream packet structure, where a logical subchannel is completely filled before moving to the next subchannel, is used to maximize the allowed power per subcarrier for a given CPE EIRP limit, i.e., this horizontal laying reduces the EIRP required by the CPE for its upstream burst by minimizing the number of subchannels needed. In the upstream, the shorter burst alternative shown in Figure 13 is used to reduce latency by allowing advance of the US burst in the US subframe to give the base station time to react before the start of the next frame, at the cost of reduced transmit power and efficiency (e.g., video game near real-time versus transmission efficiency).

The format of the FCH MAC burst is described in 7.5.2. The FCH is modulated using the data mode selected (e.g., Mode 4 or 5, see Table 202) in the SCH. Binary convolutional coding (BCC, 9.7.2.1) shall also be applied to the FCH burst. The FCH specifies the burst profile and the length of either the DS-MAP, if transmitted, or the US-MAP. If neither, the DS-MAP nor the US-MAP is transmitted, the value shall be set to zero. The DS-MAP message, if transmitted, shall be the first MAC PDU in the burst following the FCH. A US-MAP message, if transmitted, shall immediately follow either the DS-MAP message, if transmitted, or the FCH. If DCD and UCD messages are transmitted in the frame, they shall immediately follow the DS-MAP and US-MAP messages. The symbols containing these broadcast MAC control messages shall be modulated using data mode 5 as described in Table 202 with the mandatory BCC mode (see 9.7.2.1).

In the upstream direction, if a CPE does not have any data to transmit in its US allocation, it shall transmit an US PHY burst containing a generic MAC header (see 7.6.1.1) with its basic FID, together with a Bandwidth Request subheader (see 7.6.1.2.1). This would allow the BS to reclaim this CPE's allocation in the following frames and use the resource for some other purpose.

The BS may schedule up to five types of contention windows (see 7.13): the Initial Ranging window is used for initializing the association; the periodic ranging window is used for regularly adjusting the timing and power at the CPE; the BW request window is for CPEs to request upstream bandwidth allocation from the BS; the UCS notification window is used by CPEs to report an urgent coexistence situation with incumbents; while the SCW is employed by CBP packets for signaling information to adjacent and overlapping WRAN cells for the purpose of self-coexistence, signal the device identification for resolving interference situations with incumbents when requested by local regulation, and for carrying out terrestrial geolocation between CPEs of the same WRAN cell. However, CBP burst transmissions for terrestrial geolocation purpose shall have lower priority than any other coexistence transmission on the CBP burst.

The SCW shall be scheduled at the end of the frame as depicted in Figure 13. The CBP packets are transmitted by selected CPEs or the BS, and carry information, among other things, about the IEEE 802.22 cell as a whole, the device that transmits it, as well as information to support the self-coexistence mechanism (see 7.20).

A CBP packet shall be transmitted by each CPE associated to a base station as specified by the parameter “T34” in Table 272 for periodic identification of its device ID and serial number and the associated base station ID as may be required by local regulations (see Annex A).

Whenever a CPE is neither receiving nor sending data to its BS (idle state), it shall be capable of decoding CBP packets transmitted by nearby CPEs belonging to other WRAN cells, either on the same channel ( $N$ ), or on adjacent channels ( $N\pm 1$ ), or on alternate channels ( $N\pm 2$  and beyond). This capability shall also be available at CPE initialization. In addition, BS frame synchronization is based on the absolute local start time of their superframe period to the start of every minute referenced to UTC as specified in 7.23. Hence, multiple co-located or nearby IEEE 802.22 cells can efficiently communicate with each other and align their SCW for CBP exchange as well as their quiet periods for sensing incumbents.

## 7.5 Control headers

As can be seen in Figure 10 and Figure 12, there are two mandatory control headers that provide essential information about the superframe (SCH) and the frame (FCH). The content and intent of each of these control headers is described in the following subclauses.

### 7.5.1 Superframe Control header

The SCH specification is shown in Table 1. Since the SCH decoding is critical, the SCH shall be transmitted using the modulation described in 9.4.2.1. The SCH provides information about the IEEE 802.22 cell, in order to protect incumbents, support self-coexistence mechanisms, and support the intra-frame and inter-frame mechanisms for management of quiet periods for sensing as described in 7.21.1.

Transmission of a SCH indicates that the WRAN cell is operating in one of the two possible modes: normal mode or self-coexistence mode. These are described in 7.3.

All bits indicated as “*Reserved*” in tables throughout this standard shall be transmitted as zeros unless otherwise explicitly specified.

**Table 1— Superframe Control header format**

Syntax	Size	Notes
Superframe_Control_Header_Format() {		One OFDM symbol long and transmitted with modulation/coding described in 9.4.2.1
BS ID	48 bits	MAC address that uniquely identifies the BS transmitting the SCH.
Frame Allocation Map	16 bits	Indicates which frames in the present superframe are allocated to the BS transmitting the SCH.
Superframe Number	8 bits	Positive integer that represents the superframe number (modulo 256). This field shall be incremented by 1 upon every new superframe.
CP	2 bits	Cyclic Prefix Factor Specifies the size of the cyclic prefix used by the PHY in the frame transmissions in this superframe (see 9.1.1.1). Pre-determined values are 00: 1/4 $T_{FFT}$ 01: 1/8 $T_{FFT}$ 10: 1/16 $T_{FFT}$ 11: 1/32 $T_{FFT}$
FCH Encoding Flag	2 bit	00: FCH packet encoded with PHY mode 5 (See Table 202) 11: FCH packet encoded with PHY mode 4
Self-coexistence Capability Indicator	4 bits	0000: no self-coexistence capability supported 0001: only Spectrum Etiquette 0010: Spectrum Etiquette and Frame Contention 0011–1111: Reserved
MAC version	8 bits	IEEE 802.22 MAC version to which the message originator conforms.

Syntax	Size	Notes
		0x01: IEEE Std 802.22 0x02–0xFF: Reserved
Current Intra-frame Quiet Period Cycle Length	8 bits	Specified in number of superframes, it indicates the spacing between the superframes for which the intra-frame quiet period specification is valid. For example, if this field is set to 1, the Quiet Period Cycle repeats every superframe; if it is set to 2, the Quiet Period Cycle repeats every 2 superframes, etc. If this field is set to 0, no intra-frame quiet period is scheduled or the current intra-frame quiet period is cancelled.
Current Intra-frame Quiet Period Cycle Offset	8 bits	Valid only if Current Intra-frame Quiet period Cycle Length > 0. Specified in number of superframes, it indicates the offset from this SCH transmission to the beginning of the first superframe in the Current Intra-frame Quiet period Cycle Length.
Current Intra-frame Quiet period Cycle Frame Bitmap	16 bits	Valid only if Current Intra-frame Quiet Period Cycle Length > 0. Valid for each superframe identified by the Current Intra-frame Quiet Period Cycle Length, each bit in the bitmap corresponds to one frame within the superframe. If the bit is set to 0, no intra-frame quiet period shall be scheduled in the corresponding frame. If the bit is set to 1, an intra-frame quiet period shall be scheduled within the corresponding frame for the duration specified by the Current Intra-frame Quiet period Duration.
Current Intra-frame Quiet Period Duration	8 bits	Valid only if Current Intra-frame Quiet Period Cycle Length > 0. If this field is set to a value different from 0 (zero), it indicates the number of symbols starting from the end of the frame during which no transmission shall take place.
Claimed Intra-frame Quiet Period Cycle Length	8 bits	Specified in number of superframes, it indicates the spacing between the superframes for which the intra-frame quiet period specification claimed by a BS would be valid. For example, if this field is set to 1, the Quiet Period Cycle would repeat every superframe; if it is set to 2, the Quiet Period Cycle would repeat every 2 superframes, etc. If this field is set to 0, no intra-frame quiet period is claimed by the BS.
Claimed Intra-frame Quiet Period Cycle Offset	8 bits	Valid only if Claimed Intra-frame Quiet Period Cycle Length > 0. Specified in number of superframes, it indicates the offset from this SCH transmission to the time where the Claimed Quiet Period Cycle resulting from the inter-BS negotiation (see 7.21.2) shall become the Current Intra-frame Quiet Period Cycle.
Claimed Intra-frame Quiet period Cycle Frame Bitmap	16 bits	Valid only if Claimed Intra-frame Quiet Period Cycle Length > 0. Valid for each superframes identified by the Claimed Intra-frame Quiet Period Cycle Length, each bit in the bitmap corresponds to one frame within each specified superframe. If the bit is set to 0, no intra-frame quiet period will be scheduled in the corresponding frame. If the bit is set to 1, an intra-frame quiet period will be scheduled within the corresponding frame for the duration specified by Claimed Intra-frame Quiet period Duration.
Claimed Intra-frame Quiet Period Duration	8 bits	Valid only if Claimed Intra-frame Quiet Period Cycle Length > 0. If this field is set to a value different from 0 (zero): it indicates the number of symbols starting from the end of the frame during which no transmission will take place.
Synchronization Counter for Intra-frame Quiet Period Rate	8 bits	Valid only if Claimed Intra-frame Quiet Period Cycle Length > 0. This field is used for the purpose of synchronizing the Claimed Intra-frame Quiet Period rate among overlapping BSs in order to allow dynamic reduction of the Intra-frame Quiet Period rate. This Quiet Period rate is defined as the number of frames with quiet periods identified by the Cycle Frame Bitmap in the superframes designated by the Cycle Length, divided by this Quiet Period Cycle Length (see 7.21.2).
Synchronization Counter for Intra-frame Quiet Period Duration	8 bits	Valid only if Claimed Intra-frame Quiet Period Duration > 0. This field is used for the purpose of synchronizing the Claimed Intra-frame Quiet Period Durations among overlapping BSs in order to allow dynamic reduction of the Intra-frame Quiet Period Duration (see 7.21.2).

Syntax	Size	Notes
Inter-frame Quiet Period Duration	4 bits	<p>Duration of Quiet Period</p> <p>It indicates the duration of the next scheduled quiet period in number of frames.</p> <p>If this field is set to a value different from 0 (zero), it indicates the number of frames that shall be used to perform in-band inter-frame sensing.</p> <p>If this field is set to 0, no inter-frame quiet period is scheduled or the current inter-frame quiet period is cancelled.</p>
Inter-frame Quiet Period Offset	12 bits	<p>Time to Quiet Period</p> <p>It indicates the time span between the transmission of this information and the next scheduled quiet period for in-band inter-frame sensing.</p> <p>The 8 left most bits (MSB) indicate the superframe number and the 4 right most bits (LSB) indicate the frame number when the next scheduled quiet period for inter-frame sensing shall start.</p>
SCW Cycle Length	8 bits	Specified in number of superframes. If this field is set to 0, then no SCW cycle is scheduled. This field has to be 1 or larger to be effective. To limit the number of possibilities, the field shall be one of five following choices {1, 2, 4, 8, 16}. For example, if this field is set to 1, SCW Cycle repeats every superframe, if it is set to 2, SCW Cycle repeats every 2 superframes, etc.
SCW Cycle Offset	8 bits	Specified in number of superframes, it indicates the offset from this SCH transmission to the superframe where the SCW cycle starts, or repeats (i.e., the superframe contains SCWs and is specified by the SCW Cycle Frame Bitmap). For example, if this field is set to 0, the SCW cycle starts from the current superframe. The value of the field shall be less than SCW Cycle length unless initial countdown. For initial countdown, this field can equal or be larger than SCW Cycle Length. Larger initial countdown gives neighboring WRANs longer time to discover and avoid any potential SCW reservation collision.
SCW Cycle Frame Bitmap	32 bits	<p>Valid for a unit of superframe, each 2-bit in the bitmap corresponds to one frame within the superframe. If the 2-bit is set to 00, this means that there is no SCW scheduled for this frame. If the 2-bit is set to 11, a reservation-based SCW (reserved by the current WRAN) is scheduled in the corresponding frame. If the 2-bit is set to 10, a reservation-based SCW has been scheduled by a direct-neighbor WRAN cell in the corresponding frame and needs to be avoided by other WRAN cells receiving this SCH. If the 2-bit is set to 01, a contention-based SCW (that could be shared with other WRANs) is scheduled by the current WRAN cell in the corresponding frame.</p> <p>The number of reservation-based SCWs cannot exceed 2 per WRAN cell per SCW Cycle. At least one contention-based SCW shall be scheduled in one SCW Cycle (code 01). The BSs shall start scheduling their contention-based SCWs from the last frame of the superframe, going backward for multiple contention-based SCWs.</p> <p>This bitmap applies only to the superframes scheduled by the SCW Cycle.</p> <p>NOTE—Quiet period scheduling should be done prior to the SCW scheduling so that SCWs avoid frames already reserved for QP. If SCW conflicts with QP, QP overrides the SCW.</p>
Current DS/US Split	6 bits	Effective start time (in OFDM symbols from the start of the frame including all preambles) of the first symbol of the upstream allocation when a BS-to-BS interference situation has been identified by direct reception of this parameter by a BS from a SCH or a CBP burst transmitted by another BS. The Allocation Start Time as provided in the US-MAP (see Table 34) shall be equal to this value if BS-to-BS interference has been identified. This value shall be set to zero if no BS-to-BS interference has been identified (i.e., BS has not received this parameter from another BS). In this case, the Allocation Start Time in the US-MAP (see Table 34) can be defined independently on a frame-by-frame basis by the respective BSs based on their traffic requirement.

Syntax	Size	Notes
Claimed US/DS Split	6 bits	Specified by each BS in the case of BS-to-BS interference (i.e., when SCH and/or CBP burst can be received by a BS directly from another BS) indicating the required DS/US split based in the traffic requirement of the transmitting BS and the negotiation process between the BSs (see 7.20.3). This value shall be set to zero if no BS-to-BS interference has been identified.
DS/US Change Offset	12 bits	It indicates the time span between the transmission of this information and the next scheduled change of the DS/US split where the “Claimed DS/US split” value will become the “Current DS/US split” value. The 8 left most bits (MSB) indicate the superframe number and the 4 right most bits (LSB) indicate the frame number when the next DS/US split change shall take place. The value of this parameter is determined by the negotiation process between concerned BSs (see 7.20.3). This value shall be set to zero if no BS-to-BS interference has been identified.
Incumbent detection reporting inhibit timer	32 bits	In the case where the BS is informed by the database service that it can continue operating on the current channel even though its CPEs are repetitively reporting an incumbent detection situation (i.e., on N or $N \pm 1$ ), the BS can use this parameter to inhibit such reporting by the CPEs for a specified period of time. This will avoid the CPEs flooding the upstream subframe with unnecessary incumbent detection reports. Bit 0–4: Signal type (see Table 237) Bit 5–31: Inhibit Period (number of frames)
HCS	8 bits	Header Check Sequence See Table 3.
Padding bits	56 bits	Padding bits to fill the rest of the 360 bits of the SCH symbol. All bits shall be set to 0.
}		

### 7.5.2 Frame Control header

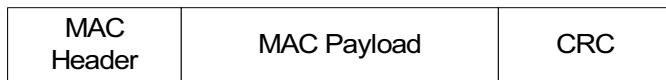
The format of the FCH is shown in Table 2. Since FCH decoding is critical, the FCH shall be encoded using either the modulation specified by the PHY mode 4 or PHY mode 5 as described in Table 202 as signaled in the SCH in Table 1. The FCH contains the length of either the DS-MAP or US-MAP that immediately follows the FCH for which PHY mode 4 shall be used (note that Length = 0 indicates the absence of any burst in the frame). In the case where the DS-MAP is specified, the US-MAP length information shall be contained in the first DS-MAP information element. In the case where the US-MAP length is indicated in the FCH, there shall be no DS burst in the current frame. DCD and UCD messages, if present, are carried by the next DS bursts specified by the DS-MAP. Location and profile of the data bursts are specified in the rest of the DS-MAP and US-MAP management messages. A HCS field occupies the last byte of the FCH.

**Table 2—Frame control header format**

Syntax	Size	Notes
Frame Control Header Format() {		
Length of the frame	6 bits	Indicates the length of the frame in number of OFDM symbols from the start of the frame including all preambles.
Length of the MAP message	10 bits	This field specifies the length of the MAP information element following the FCH in OFDM slots. A length of 0 (zero) indicates the absence of any burst in the frame.
HCS	8 bits	Header Check Sequence See Table 3.
}		

## 7.6 MAC PDU formats

The MAC PDU is illustrated in Figure 14. Figure 12 depicts how the MAC PDU fits in the overall frame structure when used for intra-cell communication. Each PDU begins with a fixed-length generic MAC header, which shall be followed by a Payload. The Payload shall consist of zero or more subheaders, zero or more IEs, and zero or more MAC SDUs and/or fragments thereof. The payload information may vary in length, so that a MAC PDU may represent a variable number of bytes. A CRC shall be applied to all the MAC PDUs transmitted on the broadcast, Initial Ranging, Basic and Multicast transport FIDs. This is because the MAC PDUs transmitted on these FIDs do not have any other protection. For all other FIDs, a MAC PDU may or may not carry a CRC since MAC PDUs belonging to all these FIDs contain an integrity check vector (see 8.4). Such PDU will have to fit in a given integer number of OFDM slots once encoded and this will result in specific data bit lengths possible as indicated in Table 227. Bit padding is used to make each PDU fit these bit lengths as explained in 7.8.6.



**Figure 14 — MAC PDU format**

### 7.6.1 MAC headers

Two MAC headers are defined: the generic MAC header used for intra-cell communication (between BS and CPEs within a cell), and the coexistence beacon MAC header used by the CBP protocol for inter-cell communication to foster appropriate self-coexistence among overlapping IEEE 802.22 cells, to provide a way to identify the transmitting device for potential interference resolution, and for intra-cell communication between the CPEs in the same cell to contribute to terrestrial geolocation.

In addition to these headers, there is also the possibility of including subheaders and special payloads associated to the generic MAC header. In the following subclauses, the MAC headers, together with the subheaders and special payloads, are described.

#### 7.6.1.1 Generic MAC header

The format of the generic MAC header (GMH) is shown in Table 3. This header begins each MAC PDU containing either higher layer traffic or MAC management data.

The IEEE 802.22 MAC is connection-oriented. As discussed in 7.2, these connections are addressed by two components, the station ID (SID) and the flow ID (FID). The SID indicates the allocation assigned to a connection in a DS/US-MAP IE. The FID is a critical field in the GMH, because it indicates a specific flow of traffic mapped to an SID's allocation. To differentiate between PDUs assigned to different flows for QoS (see 7.18), the FID is signaled in the GMH. Another critical field included in the header for the purpose of protecting incumbent services is the UCS bit. This field is used by CPEs that already have an allocated upstream burst to immediately signal the BS of a newly detected UCS with incumbents in the current channel or in either of its adjacent channels by setting the UCS bit to 1 in their upstream burst.

The subheader Type indication field is used to signal the presence and order of subheaders that follow the GMH. For example, if the Type field is equal to 11001, the following subheaders are attached (given in order): Bandwidth Request subheader, ARQ Feedback Payload, and finally the Grant Management subheader. Subheader formats and usage are discussed in 7.6.1.2. The generic MAC header also includes other fields (e.g., security related), and these can be found in Table 3.

**Table 3— Generic MAC header format**

Syntax	Size	Notes
General_MAC_Header_Format() {		
Length	11 bits	The length in bytes of the MAC PDU including the MAC header and the CRC. Any length smaller than 4 bytes shall be reserved for future use and the data shall be discarded by receivers only able to comply with this standard release.
UCS	1 bit	Urgent Coexistence Situation Used by the CPE to alert the BS about an UCS with incumbents in the channel currently being used by the BS or either of its adjacent channels: 0: no incumbent (default) 1: incumbent detected
QPA	1 bit	Quiet Period Adjustment sent by the CPE when it is missing QP opportunities to complete its in-band sensing within the required in-band detection time (see 10.3.3): 0: no adjustment needed (default) 1: increase of the number of quiet periods is needed
EC	1 bit	Encryption control: 0: payload is not encrypted 1: payload is encrypted
EKS	2 bits	Encryption key sequence The index of the traffic encryption key (TEK) and initialization vector used to encrypt the payload. This field is only meaningful if the EC field is set to 1. When transitioning to newer TEK/GTEK (see 8.3.1.4 and 8.3.1.5), EKS is incremented +1 (modulo 4).
Type	5 bits	Indicates the subheaders and special payload types present in the message payload. See Table 4.
FID	3 bits	Flow ID
HCS	8 bits	Header check sequence The transmitter shall calculate the HCS value for the content of the header excluding the HCS field, and insert the result into the HCS field which is the last byte of the header). It shall be the remainder of the division (Modulo 2) by the generator polynomial $g(D = D^8 + D^2 + D + 1)$ of the polynomial $D^8$ multiplied by the content of the header excluding the HCS field. (Example: [Length=0x447, UCS=0, QPA=0, EC=1, EKS=01, Type=11001, FID=010; the resulting GMH=0x88E5CB and the HCS calculated over it = 0x27]).
}		

**Table 4— Encoding of the Type field**

Type bit	Values
4	Bandwidth Request subheader Indicates whether this is a bandwidth request frame, and hence contains a special payload related to bandwidth allocation (see Table 5) 1: present; 0: absent
3	ARQ feedback payload 1: present; 0: absent
2	Extended type Indicates whether the present Packing or Fragmentation subheader is extended 1: Extended 0: not Extended. Applicable to connections where ARQ is not enabled.
1	Fragmentation/Packing subheader 1: present; 0: absent

Type bit	Values
0	In the upstream: Grant Management subheader 1: present; 0: absent

### 7.6.1.2 MAC subheaders and special payloads

Five types of subheaders may be present. The per-PDU subheaders (i.e., Bandwidth Request, Fragmentation/Packing, Grant Management) may be inserted in MAC PDUs immediately following the generic MAC header. If indicated, the Bandwidth Request subheader shall always follow the Generic MAC header. In the upstream, if both the Grant Management subheader and Fragmentation/Packing subheader are indicated, the Grant Management subheader shall come first. If both the Grant Management subheader and Bandwidth Request subheader are indicated, the Grant Management subheader shall come first.

There can be more than one Fragmentation/Packing subheader in a MAC PDU, all configured for packing. There can only be one Fragmentation/Packing subheader in the MAC PDU if configured for fragmentation. The Fragmentation/Packing subheader may be inserted before each MAC SDU if so indicated by setting Bit 1 in the Type field of the generic MAC Header and by setting the “Purpose bit” in Table 6 to 1.

When present, per-PDU subheaders shall always precede the first per-SDU subheader.

#### 7.6.1.2.1 Bandwidth Request subheader

Bandwidth Request subheaders are transmitted by the CPE to the BS to request additional bandwidth for a connection. They shall be sent in a PDU by itself or in a PDU with other subheaders and/or data. (See Table 5.)

**Table 5— Bandwidth Request subheader format**

Syntax	Size	Notes
BW Request Subheader Format() {		
Type	1 bit	Indicates the type of the bandwidth request adjustment 0: incremental 1: aggregate
BR	20 bits	The number of bytes of upstream bandwidth requested by the CPE. The request shall not include any PHY overhead.
}		

#### 7.6.1.2.2 Fragmentation/Packing subheader

Table 6 shows the format of the Fragmentation/Packing subheader.

**Table 6— Fragmentation/Packing subheader format**

Syntax	Size	Notes
Fragmentation/Packing Subheader Format() {		
Purpose	1 bit	0: Fragmentation subheader 1: Packing subheader
FC	2 bits	Indicates the fragmentation state of the payload: 00: no fragmentation 01: last fragment 10: first fragment 11: continuing (middle) fragment
if (ARQ-enabled Connection) {		Type bit 3==1 (see Table 4)
BSN	10 bits	Sequence number of the first block in the current SDU

Syntax	Size	Notes
		fragment
else {		
FSN	10 bits	Sequence number of the current SDU fragment. This field increments by one (modulo 1024) for each fragment, including unfragmented SDUs.
}		
}		
if (Purpose==1) {		
Length	11 bits	Length of SDU fragment being packed
else {		#if (Purpose==0)
Reserved	3 bits	All bits shall be set to zero.
{		
}		
}		

#### 7.6.1.2.3 Grant Management subheader

Table 7 shows the format of the Fragmentation/Packing subheader.

**Table 7— Grant Management subheader format**

Syntax	Size	Notes
Grant Management Subheader Format() {		
if (Type bit 0==1) {		Scheduling service type = Unsolicited Grant Service (UGS) (see Table 4)
SI	1 bit	Slip Indicator 0: No action 1: Used by the CPE to indicate a slip of upstream grants relative to the upstream queue depth.
PM	1 bit	Poll-Me 0: No action 1: Used by the CPE to request a bandwidth poll.
Reserved	6 bits	All bits shall be set to zero.
}		
}		

#### 7.6.1.2.4 ARQ Feedback Payload

If the ARQ Feedback Payload bit in the MAC Type field (see Table 4) is set, the ARQ Feedback Payload shall be transported. If packing is used, it shall be transported as the first packed payload. ARQ feedback is provided for each FID that has ARQ-enabled for service flows carried on it. The format of the ARQ Feedback is described in Table 175 in 7.8.4.3 and Table 176 in 7.9.2.

#### 7.6.1.3 CBP MAC PDU format

The coexistence beacon protocol (CBP) beacons (discussed in 7.20.1) are inter-cell and intra-cell packets that are transmitted with the goal of improving self-coexistence among overlapping IEEE 802.22 cells, of identifying the transmitting device for potential interference resolution, and of enhancing geolocation/ranging resolution between CPEs within a cell (10.5.2). These beacons are transmitted by the BS or CPEs under the control of the BS during a SCW. As discussed in 7.20.1, the coexistence beacon MAC PDU described in Table 8 is utilized by the CBP packets.

**Table 8—CBP MAC PDU format**

Syntax	Size	Notes
CBP_MAC_PDU_Format() {		
Length	8 bits	The length in bytes of the CBP MAC PDU including the MAC header and the CRC.
SCH Data Index	4 bits	SCH Data included in the CBP_MAC_PDU contains the sum of the following elements (see Table 1): 0000: 7 first parameters of the SCH = 11 bytes 1000: 10 parameters related to intra-frame QP = 12 bytes 0100: 2 parameters related to inter-frame QP = 2 bytes 0010: 3 parameters on SCW scheduling = 6 bytes 0001: 3 parameters on DS/US Split = 3 bytes Note that this last 3 parameters segment can only be included in CBP burst transmitted by BSs.
SCH Data	Variable (integer number of bytes)	Data extracted from the SCH transmitted by the BS sourcing this CBP (see Table 1). This data includes the BS_ID. Only the useful information contained in the SCH should be replicated here. This indicates that the SCH should be built with IEs only present when needed. Table 1 should be modified accordingly.
Frame Number	4 bits	The frame number within the current superframe in which the CBP burst is transmitted.
HCS	8 bits	Header Check Sequence.
IEs	Variable (integer number of bytes)	CBP information elements (see 7.6.1.3.1)
}		

#### 7.6.1.3.1 CBP information elements

CBP packets shall carry at least one information element (IE) in their payload among the set described in Table 9 since it provides the basic information required to enable self-coexistence. CBP packets shall at least carry a Backup/Candidate Channel information element (IE) in their payload. This is to allow WRANs to execute the spectrum etiquette mechanism before deciding to execute the other spectrum sharing mechanisms described in 7.20.3.

**Table 9—CBP IEs**

Element ID	Name
0x00	Backup and Candidate Channel List IE
0x01	FC_REQ IE
0x02	FC_RSP IE
0x03	FC_ACK IE
0x04	FC_REL IE
0x05	CBP_Identification IE
0x06	Signature IE
0x07	CERT-REQ IE
0x08	CERT-RSP IE

##### 7.6.1.3.1.1 Backup and Candidate Channel List IE

The Backup and Candidate Channel List IE, as defined in Table 10, carries a list of the current backup channels and identified candidate channels becoming backup channels when “cleared” by all CPEs as defined by the BS. The Backup and Candidate Channel List IE shall be included in the CBP MAC PDU to allow for network discovery and implementation of the spectrum etiquette self-coexistence mechanism.

**Table 10— Backup and Candidate Channel List IE**

Syntax	Size	Description
Backup_and_candidate_channel_list IE Format() {		
Element ID	8 bits	0x00
Number_Backup_and_candidate_TV_Channels	4 bits	Number of backup and candidate channels in the list
Number_Backup_TV_Channels	4 bits	Number of backup channels in the list
For (i=0; i < Number_Backup_and_candidate_TV_Channel; i++) {		List of backup channels in order of priority to be used by CPEs in case of loss of communication with the BS due to incumbents. This list may also include candidate channels, in which case they will follow the backup channels in the list, and will also be included in order of priority. The list shall be a disjoint set with the current operating channel.
Channel Number	Variable	8 bits per channel.
}		
}		

#### 7.6.1.3.1.2 Frame Contention Request IE

The Frame Contention Request (FC\_REQ) IE defined in Table 11 is used in the On-demand Frame Contention Protocol (see 7.20.3.2). The FC\_REQ is transmitted in the payload of a CBP packet by a WRAN cell—the frame contention source, which intends to acquire spectrum resources (data frame transmission opportunities) of a channel currently occupied by another neighboring WRAN cell – the frame contention destination, in order to satisfy the QoS requirements of the frame contention source’s data transmission.

**Table 11— FC\_REQ IE format**

Syntax	Size	Notes
FC_REQ IE Format() {		
Element ID	8 bits	0x01
BS ID of Contention Destination	48 bits	The MAC address of the frame contention destination BS.
Sequence number	8 bits	Incremented by 1 by the source whenever any of the following three fields change. The frame contention destinations shall discard the repeated FC_REQ IEs.
Frame contention number (FCN)	16 bits	A random number indicating the priority for the frame contention on the current channel.
Contention Request Frame Index Vector	16 bits	A bit map indicating the indexes of each data frame within a superframe that the Contention Source WRAN requests to acquire (through the contention process) for its data services starting from a to-be-scheduled next superframe after the current superframe (see Table 12). For each of the 16 bits of the frame bit map, the corresponding frame is requested for the contention when the bit value is set to 1. Otherwise, the bit value of the corresponding frame is set to 0.
}		

#### 7.6.1.3.1.3 Frame Contention Response IE

The Frame Contention Response (FC\_RSP) IE defined in Table 12 is used in the On-demand Frame Contention Protocol (see 7.20.3.2). The FC\_RSP IE is sent in a CBP packet payload by the contention destination WRAN cell in order to inform the contention source WRAN cell of the contention results. This

IE is transmitted by the contention destination WRAN Cell after it has received a FC\_REQ IE from the contention source WRAN cell and has run the contention resolution algorithm.

**Table 12—FC\_RSP IE format**

Syntax	Size	Notes
FC_RSP_IE_Format() {		
Element ID	8 bits	0x02
BS ID of the Frame Contention Source	48 bits	MAC address of the Frame Contention Source copied from the CBP PDU header received (from the included SCH data).
Sequence number	8 bits	Copy from the FC_REQ.
Contention Response Frame Index Vector	16 bits	A bit map indicating the contention results determined by the channel contention algorithm for the data frames that the contention source WRAN requests to acquire. These contention results will be effective starting from a to-be-scheduled next superframe after the current superframe (see Frame Release Time below). For each of the 16 bits of the frame bit map corresponding to a superframe, a frame is granted to the contention source when the corresponding bit value is set to 1. If the bit value is set to 0, the frame is not granted. Also, for a data frame that is not requested by any contention source, the corresponding bit is set to 0. For these two last cases, the frame allocation does not change.
Frame Release Time	8 bits	Starting from the next superframe, the number of superframes after which the channel shall be released by the frame contention destination BS.
}		

#### 7.6.1.3.1.4 Frame Contention Acknowledgment IE

The Frame Contention Acknowledgment (FC\_ACK) defined in Table 13 is used in the On-demand Frame Contention Protocol (see 7.20.3.2). The FC\_ACK is a broadcast acknowledgment message transmitted by the winner of the frame contention (FC-SRC) indicating the confirmation and the scheduling of the frame acquisitions.

**Table 13—FC\_ACK IE format**

Syntax	Size	Notes
FC_ACK_IE_Format() {		
Element ID	8 bits	0x03
BS ID of the granting FC-DST	48 bits	The MAC address of the BS of the frame contention destination (FC-DST) WRAN cell granting access to the data frames that are being acquired by the winning WRAN cell (FC-SRC) (this is used to enable “clear to send”).
Sequence number	8 bits	Same as the corresponding FC_REQ IE. The contention destinations shall discard the repeated FC_ACK IE being received.
Frame Contention Number	16 bits	The winning FCN used in FC_REQ message, showing the priority to contend for the target data frame.
Contention Acknowledgement Frame Index Vector	16 bits	A bit map indicating the frames that the FC-SRC has won through the channel contention algorithm from the FC-DST and that it intends to acquire starting from the scheduled next superframe after the current superframe (see Frame Release Time in the cell below). For each of the 16 bits of the frame bit map corresponding to a superframe, a frame will be occupied by the contention source when the corresponding bit value is set to 1. Otherwise, the allocation of the frame does not change.
Frame Release Time	8 bits	Starting from the next superframe, the number of superframes after which the channel shall be released by the frame contention destination BS.
}		

### 7.6.1.3.1.5 Frame Contention Release IE

Frame Contention Release (FC\_REL) is a broadcast message IE transmitted by the WRAN cell granting the frames (FC-DST) as a result of the frame contention indicating the announcement of the frame releases.

**Table 14—FC\_REL IE format**

Syntax	Size	Notes
FC_REL_IE_Format() {		
Element ID	8 bits	0x04
BS ID of the winning FC-SRC	48 bits	The MAC address of the BS of the frame contention source (FC-SRC) WRAN cell that was granted access to the data frames that are being released by the granting FC-DST (this is used to enable efficient spectrum reuse).
Sequence number	8 bits	Same as the corresponding FC_REQ IE. The contention destinations shall discard the repeated FC_REL IE being received.
Frame Contention Number (FCN)	16 bits	The winning FCN used in FC_REQ message, showing the priority to contend for the target data frames.
Contention Release Frame Index Vector	16 bits	A bit map indicating the frames that will be released to the winning FC-SRC according to the contention results and the acknowledgement from the FC-SRC that it intends to acquire starting from the scheduled next superframe after the current superframe. For each of the 16 bits of the frame bit map corresponding to a superframe, a frame will be occupied by the contention source when the corresponding bit value is set to 1. Otherwise, the allocation of the frame does not change.
}		

### 7.6.1.3.1.6 Device Identification IE

The Device Identification IE to be transmitted regularly by the BS and CPEs according to local regulation is intended for potential interference resolution. This IE is also used for terrestrial geolocation (see 10.5.2). The coordinates represented in this IE are based on the WGS 84 Datum.

**Table 15—Device Identification IE format**

Syntax	Size	Notes
Device_Identification IE {		
Element ID	8 bits	0x05
Device ID	17 bytes	Device identifier (e.g., FCC ID) (see 8.5.1.4.2).
Serial Number	12 bytes	Device serial number (see 8.5.1.4.2).
Latitude	24 bits	Bit 23: 1 bit indicator of hemisphere, N = 0, S = 1 Bit 22–16: 7 bits of degree, sufficient to cover $0^\circ < \text{latitude} < 90^\circ$ Bit 15–0: 16 bits of decimal degree fraction corresponding to a precision of 1.7 m. If Latitude and Longitude are set to zero, this shall indicate that the location is not known.
Longitude	24 bits	Bit 23: 1 bit indicator of hemisphere, E = 0, W = 1 Bit 22–15: 8 bits of degree, sufficient to cover $0^\circ < \text{longitude} < 180^\circ$ Bit 14–0: 15 bits of decimal degree fraction corresponding to a precision of 3.4 m at the equator. If Latitude and Longitude are set to zero, this shall indicate that the location is not known.
}		

### 7.6.1.3.1.7 CBP Protection IEs

The CBP protection method (8.6.2.1) is an optional security procedure that can be used to provide authentication of CBP MAC PDU transmissions. If it is enabled then the three following IEs are required: CBP Signature IE, Certificate Request (CERT-REQ) IE, and Certificate Response (CERT-RSP) IE. The Signature IE is used to provide a signature that is calculated over the CBP MAC PDU, and is verified by the receiving BS. When the CBP Protection is enabled, the Signature shall be transmitted in every CBP MAC PDU.

#### 7.6.1.3.1.7.1 Signature IE

**Table 16— Signature IE format**

Syntax	Size	Description
Signature_IE_Format {		
Element ID	8 bits	0x06
Key ID	9 bits	Identifier of the key associated with the BS implicit certificate used to generate the signature. This identifier is generated by the Certification Authority (CA) when the certificate is created.
Time Stamp	44 bits	Derived from a NMEA 0183 (\$..ZDA) string (each letter represents a digit, encoded by different numbers of bits): <ul style="list-style-type: none"> <li>— X: year= 2010+X, X is 6 bits</li> <li>— M: month, e.g., 01–12, total is 4 bits</li> <li>— D: day, e.g., 01–31, total 5 bits</li> <li>— H: hour, e.g., 00–23, total 5 bits</li> <li>— m: minute, e.g., 00–59, total 6 bits</li> <li>— ss: seconds, e.g., 00–59, total 6 bits</li> <li>— .ss: 10 ms boundary, e.g., .00–99, 7 bits</li> <li>— zZ: hours off of GMT; z is 1 bit ± indication, 2nd Z is number of hours, e.g., 1–13, 4 bits, total 5 bits</li> </ul>
Version	5 bit	00000: ECQV implicit certificates, ECSSR-PV signature scheme, K-233 EC Domain parameters in compressed form and 233 bit keys 00001: ECQV implicit certificates, ECSSR-PV signature scheme, B-233 EC Domain parameters in compressed form and 233 bit keys 00010: ECQV implicit certificates, ECSSR-PV signature scheme, sect233k1 EC Domain parameters in compressed form and 233 bit keys 00011: ECQV implicit certificates, ECSSR-PV signature scheme, sect233r1 EC Domain parameters in compressed form and 233 bit keys 00100–11111: reserved
Padding	6 bits	All bits shall be set to 0.
Signature	Variable	Output of signature process. This includes the <i>Recoverable Message</i> part ( <i>C</i> ) and the Signature Data ( <i>d</i> ) as described in 8.6.2.5.2. The signature is calculated over the entire CBP MAC PDU. The signature process is detailed in 8.6.2.3. If Version==00000 or 00010, Size= 43 bytes If Version==00001 or 00011, Size= 44 bytes
}		

#### 7.6.1.3.1.7.2 Certificate Request (CERT-REQ) IE

**Table 17— Certificate Request (CERT-REQ) IE**

Syntax	Size	Description
CERT-REQ_IE_Format {		
Element ID	8 bits	0x07
Destination BS ID	48 bits	ID of BS to which that request is directed.
CA ID	8 bits	ID of Certificate Authority that issued the certificate to the BS that is initiating the certificate request.
Key ID	9 bits	Identifier of public key associated with certificate as assigned by CA. This identifier is generated by the Certification Authority (CA) when the certificate is created.
Key Validity Date (Not Before)	31 bits	Date that signifies the start of period for which the certificate of the BS that is making the request is valid. Derived from a NMEA 0183 (\$..ZDA) string (each letter represents a digit, encoded by different numbers of bits): <ul style="list-style-type: none"> <li>— X: year= 2010+X, X is 6 bits</li> <li>— M: month, e.g., 01–12, total is 4 bits</li> <li>— D: day, e.g., 01–31, total 5 bits</li> <li>— H: hour, e.g., 00–23, total 5 bits</li> <li>— m: minute, e.g., 00–59, total 6 bits</li> <li>— s: seconds, assumed to be 00, not actually encoded</li> <li>— zZ: hours off of GMT; z is 1 bit ± indication, 2nd Z is the number of hours, e.g., 1–13, 4 bits, total 5 bits</li> </ul>
Key Validity Time Period	7 bits	Amount of time, in 6 month increments, that the certificate is valid.
Version	5 bit	00000: ECQV implicit certificates, ECSSR-PV signature scheme, K-233 EC Domain parameters in compressed form and 233-bit keys 00001: ECQV implicit certificates, ECSSR-PV signature scheme, B-233 EC Domain parameters in compressed form and 233-bit keys 00010: ECQV implicit certificates, ECSSR-PV signature scheme, sect233k1 EC Domain parameters in compressed form and 233-bit keys 00011: ECQV implicit certificates, ECSSR-PV signature scheme, sect233r1 EC Domain parameters in compressed form and 233-bit keys 00100–11111: reserved
Padding	4 bits	All bits shall be set to 0.
Public Key Reconstruction Data	248 bits	Key data used to reconstruct the public key, i.e., 31 bytes for 233 bit ECC keys.
}		

#### 7.6.1.3.1.7.3 Certificate Response (CERT-RSP) IE

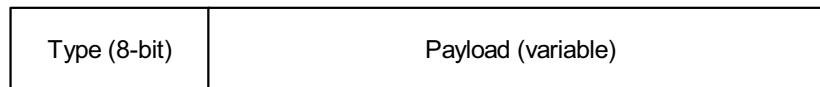
**Table 18— Certificate Response (CERT-RSP) IE**

Syntax	Size	Description
CERT-RSP_IE_Format {		
Element ID	8 bits	0x08

Syntax	Size	Description
Source BS ID	48 bits	ID of BS to which that Certificate Response is directed.
CA ID	8 bits	ID of Certificate Authority that issued the certificate to the BS that is transmitting the certificate response.
Key ID	9 bits	Identifier of public key associated with certificate as assigned by CA. This identifier is generated by the Certification Authority (CA) when the certificate is created.
Key Validity Date (Not Before)	31 bits	Date that signifies the start of period for which the certificate of the BS, that is transmitting the certificate response, is valid. Derived from a NMEA 0183 (\$.ZDA) string (each letter represents a digit, encoded by different numbers of bits): <ul style="list-style-type: none"> <li>— X: year = 2010+X, X is 6 bits</li> <li>— M: month, e.g., 01–12, total is 4 bits</li> <li>— D: day, e.g., 01–31, total 5 bits</li> <li>— H: hour, e.g., 00–23, total 5 bits</li> <li>— m: minute, e.g., 00–59, total 6 bits</li> <li>— s: seconds, assumed to be 00, not actually encoded</li> <li>— zZ: hours off of GMT; z is 1bit ± indication, 2nd Z is the number of hours e.g., 1–13, 4bits, total 5 bits</li> </ul>
Key Validity Time Period	7 bits	Amount of time, in 6 month increments, that the certificate is valid.
Version	5 bit	00000: ECQV implicit certificates, ECSSR-PV signature scheme, K-233 EC Domain parameters in compressed form and 233-bit keys 00001: ECQV implicit certificates, ECSSR-PV signature scheme, B-233 EC Domain parameters in compressed form and 233-bit keys 00010: ECQV implicit certificates, ECSSR-PV signature scheme, sect233k1 EC Domain parameters in compressed form and 233-bit keys 00011: ECQV implicit certificates, ECSSR-PV signature scheme, sect233r1 EC Domain parameters in compressed form and 233-bit keys 00100–11111: reserved
Public Key Reconstruction Data	248 bits	Key data used to reconstruct the public key, i.e., 31 bytes for 233-bit ECC keys.
Time Stamp	44 bits	Copied from Signature IE of the CBP MAC PDU in which the CERT-REQ IE was received.
}		

## 7.7 Management messages

As can be seen in Table 19, the MAC defines a collection of management messages to support and implement its basic functions. All these messages are carried in the payload of a MAC PDU, and share the same message structure as depicted in Figure 15. Management messages begin with a Type field that uniquely identifies the message in question, while its payload varies according to the message type. As for transmission, management messages can only be transmitted in Initial Ranging, Basic, Primary, Multicast Management, or Broadcast type of FIDs (see Table 279, Table 280, and Table 281). No other types of FIDs shall carry management messages.

**Figure 15 — General management message structure**

Each of the management messages shown in Table 19 are described in the following subclauses.

**Table 19 — Management messages**

Type	Message	Description	Reference	Class of connection
0	DCD	Downstream Channel Descriptor	7.7.1	Broadcast
1	DS-MAP	Downstream Access Definition	7.7.2	Broadcast
2	UCD	Upstream Channel Descriptor	7.7.3	Broadcast
3	US-MAP	Upstream Access Definition	7.7.4	Broadcast
4	RNG-REQ	Ranging Request	7.7.5	Initial Ranging or Basic
5	RNG-CMD	Ranging Command	7.7.6	Initial Ranging or Basic
6	REG-REQ	Registration Request	7.7.7.1	Primary Management
7	REG-RSP	Registration Response	7.7.7.2	Primary Management
8	DSA-REQ	Dynamic Service Addition Request	7.7.8.1	Primary Management
9	DSA-RSP	Dynamic Service Addition Response	7.7.8.2	Primary Management
10	DSA-ACK	Dynamic Service Addition Acknowledge	7.7.8.3	Primary Management
11	DSC-REQ	Dynamic Service Change Request	7.7.8.4	Primary Management
12	DSC-RSP	Dynamic Service Change Response	7.7.8.5	Primary Management
13	DSC-ACK	Dynamic Service Change Acknowledge	7.7.8.6	Primary Management
14	DSD-REQ	Dynamic Service Deletion Request	7.7.8.7	Primary Management
15	DSD-RSP	Dynamic Service Deletion Response	7.7.8.8	Primary Management
16	DSX-RVD	Dynamic Service Request acknowledgement before authentication	7.7.8.10	Primary Management
17	MCA-REQ	Multicast Assignment Request	7.7.9	Primary Management
18	MCA-RSP	Multicast Assignment Response	7.7.10	Primary Management
19	CBC-REQ	CPE Basic Capability Request	7.7.11.1	Basic
20	CBC-RSP	CPE Basic Capability Response	7.7.11.2	Basic
21	DREG-CMD	De/Re-register Command	7.7.12	Basic Primary Management
22	DREG-REQ	CPE De-registration Request	7.7.13	Primary Management
23	ARQ-Feedback	Standalone ARQ Feedback	7.7.14	Primary Management
24	ARQ-Discard	ARQ Discard	7.7.15	Primary Management
25	ARQ-Reset	ARQ Reset	7.7.16	Primary Management
26	CHS-REQ	Channel Switch Request	7.7.17.1	Primary Management or Broadcast
27	CHS-RSP	Channel Switch Response	7.7.17.2	Primary Management
28	CHQ-REQ	Channel Quiet Request	7.7.17.3	Primary Management, Multicast Management or Broadcast
29	CHQ-RSP	Channel Quiet Response	7.7.17.4	Primary Management, Multicast Management or Broadcast
30	IPC-UPD	Incumbent Prohibited Channels Update	7.7.17.4	Primary Management, Multicast Management or Broadcast
31	BLM-REQ	Bulk Measurement Request	7.7.18.1	Primary Management, Multicast Management or Broadcast

Type	Message	Description	Reference	Class of connection
32	BLM-RSP	Bulk Measurement Response	7.7.18.2	Primary Management
33	BLM-REP	Bulk Measurement Report	0	Primary Management
34	BLM-ACK	Bulk Measurement Acknowledgement	7.7.18.4	Primary Management
35	TFTP-CPLT	Config File TFTP Complete	0	Primary Management
36	TFTP-RSP	Config File TFTP Complete Response	0	Primary Management
37	SCM-REQ	Security Control Management Request	0	Primary Management
38	SCM-RSP	Security Control Management Response	0	Primary Management
39	FRM_UPD	The first active frame allocation update in self-coexistence mode	7.7.22	Basic
40	CBP_RLY	CBP Relay	7.7.23	Primary Management, Multicast Management

### 7.7.1 Downstream Channel Descriptor (DCD)

The format of a DCD message is shown in Table 20. This message shall be transmitted by the BS at a periodic interval (Table 273) to define the characteristics of a downstream physical channel.

**Table 20— DCD message format**

Syntax	Size	Notes
DCD_Message_Format() {		
Management Message Type = 0	8 bits	
Configuration Change Count	8 bits	Incremented by one (modulo 256) by the BS whenever any of the values of this channel descriptor change. If the value of this count in a subsequent DCD remains the same, the CPE can quickly decide that the remaining fields have not changed and may be able to disregard the remainder of the message. This value is also referenced from the DS-MAP messages (see Table 25).
DCD Channel Information Elements (IEs)	Variable in integer number of bytes	Table 21
Begin PHY Specific Section {		
Number of downstream burst profiles: n	6 bits	Number of burst profiles described in the current DCD message. Its maximum size corresponds to the maximum number of DIUC burst profiles contained in Table 27.
Reserved	2 bits	All bits shall be set to zero.
for ( $i = 1; i \leq n; i++$ ) {		“n” is defined as the “Number of downstream burst profiles” to be described in the current DCD message.
Downstream Burst Profile	Variable	PHY specific (Table 23).
}		
}		
}		

#### 7.7.1.1 DCD Channel information elements

The elements in Table 21 are the allowed information elements that can be included in the DCD message.

**Table 21— DCD channel information elements**

Name	Element ID (1 byte)	Length (bits)	Description
Downstream_Burst_Profile	1	Variable	Value reserved for the burst profile (see Table 23)
EIRP <sub>BS</sub>	2	8	Signed in units of dBm in 0.5 dB steps with a range from -64 dBm (encoded 0x00) to +63.5 dBm (encoded 0xFF). Values outside this range shall be assigned the closest extreme.
TTG	3	8	0x00–0xFF: range of TTG in 2.75 μs increments. Default set to 0x4D to allow for 210 μs for 30 km propagation.
RSS <sub>IR_BS_nom</sub>	4	8	Initial ranging nominal signal strength per subcarrier to be received at the BS by a 0 dBi antenna gain, i.e., corrected for the gain of the BS receive antenna in the direction of the CPE and for 0 coupling and cable loss (see 7.14.2.8.1). Signed in units of dBm in 0.5 dB steps ranging from -104 dBm (encoded 0x00) to +23.5 dBm (encoded 0xFF). Values outside this range shall be assigned the closest extreme.
Channel Action	5	3	Action to be taken by all CPEs in a cell. 000: None 001: Switch 010–111: Reserved
Action Mode	6	1	This is valid only for channel switch (Action = 001). Indicates a restriction on transmission until the specified Channel Action is performed. The BS shall set the Action Mode field to either 0 or 1 on transmission. A value of 1 means that the CPE to which the frame containing this element is addressed shall transmit no further frames until the scheduled Channel Action is performed. An Action Mode set to 0 does not impose any requirement on the receiving CPE.
Action Superframe Number	7	8	The superframe number (modulo 256) at which Channel Action shall be performed.
Action Frame Number	8	4	Integer value greater than or equal to zero that indicates the starting frame number, within the Action Superframe Number, at which the Channel Action shall be performed by all CPEs.
Number of Backup channels	9	4	Number of backup channels in the backup and candidate channel list IE (see Table 22).
Backup and Candidate channel list.	10	Variable	See Table 22 for specification.
MAC version	11	8	IEEE 802.22 MAC version to which the message originator conforms. 0x01: IEEE Std 802.22 0x02–0xFF: Reserved

**Table 22— Backup and Candidate channel list**

Syntax	Size	Notes
Backup_and_candidate_channel_list IE Format() {		
Element ID = 10	8 bits	
Length	8 bits	
Number of Channels in the list	8 bits	
For (i=0; i < Number of Channels in the list; i++) {		List of backup channels in order of priority to be used by CPEs in case of loss of communication with the BS due to incumbents. This list may also include candidate channels, in which case they will follow the backup channels in the list, and will also be included in order of priority. The number of backup channels in the list is

		indicated in DCD Element ID 9 (see Table 21). The list shall be a disjoint set with the current operating channel.
Channel Number [i]	8 bits	
}		
}		

### 7.7.1.2 Downstream burst profile

**Table 23— Downstream burst profile format**

Syntax	Size	Notes
Downstream_Burst_Profile_Format() {		
Type = 1	8 bits	
Length	8 bits	
DIUC	6 bits	7.7.2.1.1
Reserved	2 bits	All bits shall be set to zero
Information elements (IEs)	Variable	Table 24
}		

**Table 24— Downstream Burst Profile information elements**

Name	Element ID (1 byte)	Length (bytes)	Description
DIUC mandatory exit threshold	151	1	–64 dB (encoded 0x00) to +63.5 dB (encoded 0xFF) CINR at or below which this DIUC can no longer be used and where change to a more robust DIUC is required (in 0.5 dB units).
DIUC minimum entry threshold	152	1	–64 dB (encoded 0x00) to +63.5 dB (encoded 0xFF) The minimum CINR required to start using this DIUC when changing from a more robust DIUC is required (in 0.5 dB units)

### 7.7.2 Downstream Map (DS-MAP)

The format of a DS-MAP message is shown in Table 25. The DS-MAP message defines the access to the downstream information. The length of the DS-MAP shall be an integer number of bytes.

**Table 25— DS-MAP message format**

Syntax	Size	Notes
DS-MAP_Message_Format() {		
Management Message Type = 1	8 bits	
DCD Count	8 bits	Matches the value of the configuration change count of the DCD, which describes the downstream burst profiles that apply to this map.
Begin PHY Specific Section {		
Number of IEs: n	12 bits	Number of IEs in the downstream map
for (i = 1; i ≤ n; i++) {		
DS-MAP_IE()	Variable	PHY specific (7.7.2.1)
}		
}		
If(!byte_boundary)		
Padding bits	0–7 bits	Padding to octet alignment—All bits shall be set to 0.
}		

### 7.7.2.1 DS-MAP IE

The format of the DS-MAP IE is shown in Table 26.

**Table 26—DS-MAP information elements**

Syntax	Size	Description
DS-MAP IE() {		
DIUC	6 bits	7.7.2.1.1
If(DIUC == 62)		
Extended DIUC Dependent IE	Variable	7.7.2.1.2
else {		
SID	9 bits	Station ID of CPE or multicast group.
}		
Length	12 bits	Number of OFDM slots linearly allocated to the DS burst specified by this IE.
Boosting	3 bits	111: +9 dB 110: +6 dB 101: +3 dB 100: 0 dB, normal (not boosted) 011: -3 dB 010: -6 dB 001: -9 dB 000: -12 dB
}		
}		

#### 7.7.2.1.1 DIUC allocations

Table 27 illustrates the various DIUC values used in the MAC.

**Table 27—DIUC values**

DIUC	Usage		
0–12	<i>Reserved</i>		
13	Uncoded	NA	BPSK
14	Convolutional Code	FEC rate = 1/2	QPSK
15	Convolutional Code	FEC rate = 2/3	QPSK
16	Convolutional Code	FEC rate = 3/4	QPSK
17	Convolutional Code	FEC rate = 5/6	QPSK
18	Convolutional Code	FEC rate = 1/2	16-QAM
19	Convolutional Code	FEC rate = 2/3	16-QAM
20	Convolutional Code	FEC rate = 3/4	16-QAM
21	Convolutional Code	FEC rate = 5/6	16-QAM
22	Convolutional Code	FEC rate = 1/2	64-QAM
23	Convolutional Code	FEC rate = 2/3	64-QAM
24	Convolutional Code	FEC rate = 3/4	64-QAM
25	Convolutional Code	FEC rate = 5/6	64-QAM
26	CTC	FEC rate = 1/2	QPSK
27	CTC	FEC rate = 2/3	QPSK
28	CTC	FEC rate = 3/4	QPSK
29	CTC	FEC rate = 5/6	QPSK
30	CTC	FEC rate = 1/2	16-QAM
31	CTC	FEC rate = 2/3	16-QAM
32	CTC	FEC rate = 3/4	16-QAM
33	CTC	FEC rate = 5/6	16-QAM
34	CTC	FEC rate = 1/2	64-QAM
35	CTC	FEC rate = 2/3	64-QAM

DIUC	Usage		
36	CTC	FEC rate = 3/4	64-QAM
37	CTC	FEC rate = 5/6	64-QAM
38	LDPC	FEC rate = 1/2	QPSK
39	LDPC	FEC rate = 2/3	QPSK
40	LDPC	FEC rate = 3/4	QPSK
41	LDPC	FEC rate = 5/6	QPSK
42	LDPC	FEC rate = 1/2	16-QAM
43	LDPC	FEC rate = 2/3	16-QAM
44	LDPC	FEC rate = 3/4	16-QAM
45	LDPC	FEC rate = 5/6	16-QAM
46	LDPC	FEC rate = 1/2	64-QAM
47	LDPC	FEC rate = 2/3	64-QAM
48	LDPC	FEC rate = 3/4	64-QAM
49	LDPC	FEC rate = 5/6	64-QAM
50	SBTC	FEC rate = 1/2	QPSK
51	SBTC	FEC rate = 2/3	QPSK
52	SBTC	FEC rate = 3/4	QPSK
53	SBTC	FEC rate = 5/6	QPSK
54	SBTC	FEC rate = 1/2	16-QAM
55	SBTC	FEC rate = 2/3	16-QAM
56	SBTC	FEC rate = 3/4	16-QAM
57	SBTC	FEC rate = 5/6	16-QAM
58	SBTC	FEC rate = 1/2	64-QAM
59	SBTC	FEC rate = 2/3	64-QAM
60	SBTC	FEC rate = 3/4	64-QAM
61	SBTC	FEC rate = 5/6	64-QAM
62	Extended DIUC		
63	End of Map		

### 7.7.2.1.2 DS-MAP Extended DIUC IE

A DS-MAP IE entry with a DIUC value of 62 indicates that the IE carries special information and conforms to the structure shown in Table 28. A CPE shall ignore an extended IE entry with an extended DIUC value for which the CPE has no knowledge. In the case of a known extended DIUC value but with a length field longer than expected, the CPE shall process information up to the known length and ignore the remainder of the IE.

**Table 28—DS-MAP Extended IE general format**

Syntax	Size	Notes
DS_Extended_IE() {		
Extended DIUC	6 bits	
Length	8 bits	Length of this IE in bits.
Unspecified Data	Variable	
}		

#### 7.7.2.1.2.1 DS-MAP Dummy Extended IE

A CPE shall be able to decode the DS-MAP Dummy Extended IE. A BS shall not transmit this IE (unless under test). A CPE may skip decoding downlink bursts scheduled after the start time of this IE within the current frame.

**Table 29— DS-MAP Dummy Extended IE format**

Syntax	Size	Notes
Dummy_IE() {		
Extended DIUC	6 bits	0x00
Length	8 bits	Length of this IE in bits.
Unspecified Data	Variable	
}		

**7.7.3 Upstream Channel Descriptor (UCD)**

The format of a UCD message is shown in Table 30. This message shall be transmitted by the BS at a periodic interval (Table 272) to define the characteristics of an upstream physical channel.

**Table 30— UCD message format**

Syntax	Size	Notes
UCD Message Format() {		
Management Message Type = 2	8 bits	
Configuration Change Count	8 bits	Incremented by one (modulo 256) by the BS whenever any of the values of this channel descriptor change. If the value of this count in a subsequent UCD remains the same, the CPE can quickly decide that the remaining fields have not changed and may be able to disregard the remainder of the message. This value is also referenced from the US-MAP messages (see Table 34).
BW Request Backoff Start	4 bits	Initial backoff window size in units of BW Request opportunity (see Table 31) used by CPEs to contend to send BW requests to the BS, expressed as a power of 2. Values of $n$ range 0–15. Refer in the note to 6.16 on Contention Resolution. Include a subsection that will describe the size and the content of the BW Request US burst and refer to it in the note.
BW Request Backoff End	4 bits	Final backoff window size in units of BW Request opportunity (see Table 39) to contend to send BW requests to the BS, expressed as a power of 2. Values of $n$ range 0–15. All declared opportunities for BW request in subsequent frames are concatenated in this potentially large number.
UCS Notification Backoff Start	4 bits	Initial backoff window size in units of UCS notification opportunity (see Table 31) used by CPEs to contend to send UCS notifications to the BS. This is expressed as a power of 2. Values of $n$ range 0–15.
UCS Notification Backoff End	4 bits	Final backoff window size in units of UCS notification opportunity (see Table 31) used by CPEs to contend to send UCS notifications to the BS. This is expressed as a power of 2. Values of $n$ range 0–15. All declared opportunities for UCS Notifications in subsequent frames are concatenated in this potentially large number.
Information elements (IEs) for the overall channel	Variable	See 7.7.3.1.
Begin PHY Specific Section {		
Number of upstream burst profiles: $n$	6 bits	Number of upstream burst profiles described in the current UCD message. Its maximum size corresponds to the maximum number of UIUC burst profiles contained in Table 36.
for ( $i = 1; i \leq n; i++$ ) {		$n =$ number of upstream burst profiles
Upstream_Burst_Profile	Variable	PHY specific (Table 32)
}		
}		
}		

### 7.7.3.1 UCD Channel IEs

Common channel encodings are provided in Table 31.

**Table 31 — UCD channel information elements**

Name	Element ID (1 byte)	Length (bytes)	Description
Upstream Burst Profile	1	Variable	Value reserved for the burst profile (see Table 32)
Contention-based reservation timeout	2	1	Number of US-MAPs to receive before contention-based reservation is attempted again for the same connection
Bandwidth request opportunity size	3	1	Size (in OFDM slots) of PHY bursts, mapped horizontally in one subchannel at a time as in the case of normal upstream data, that a CPE may use to format and transmit a bandwidth request message in a contention request opportunity. The value includes all PHY overhead as well as allowance for the BW Request MAC subheader that the message will hold (see Table 5).
UCS Notification request opportunity size	4	1	Size (in OFDM slots) of PHY bursts, mapped horizontally in one subchannel at a time as in the case of normal upstream data, that a CPE may use to transmit a UCS notification. The value includes all PHY overhead for the GMH containing the UCS flag (see Table 3).
Initial ranging codes	150	1	Number of initial ranging CDMA codes. Possible values are 0–255.
Periodic ranging codes	151	1	Number of periodic ranging CDMA codes. Possible values are 0–255.
Bandwidth request codes	152	1	Number of bandwidth request CDMA codes. Possible values are 0–255.
UCS notification codes	153	1	Number of UCS notification CDMA codes. Possible values are 0–255.
Start of CDMA codes group	154	1	Indicates the starting number, S, of the group of codes used for this upstream. All the ranging codes used on this upstream will be between S and $(S+N+M+L+I) \bmod 256$ . Where: N is the number of initial-ranging codes M is the number of periodic-ranging codes L is the number of bandwidth-request codes I is the number of UCS notification codes The range of values is $0 \leq S \leq 255$ .

### 7.7.3.2 Upstream burst profile

The format of the upstream burst profile is shown in Table 32, and the information elements contained in the upstream burst profiles are defined in Table 33.

**Table 32 — Upstream burst profile format**

Syntax	Size	Notes
Upstream_Burst_Profile_Format() {		
Type = 1	8 bits	
Length	8 bits	
UIUC	6 bits	Table 36
Reserved	2 bits	All bits shall be set to zero.
Information elements (IEs)	Variable	Table 33
}		

**Table 33—Upstream burst profile information elements**

Name	Element ID (1 byte)	Length (bytes)	Description
Ranging data ratio	151	1	Reduction factor, in units of 0.5 dB, between the EIRP per subcarrier used for this burst and the EIRP per subcarrier that should be used for CDMA Ranging.
Normalized CNR override	152	7	The first byte shall represent a signed integer which specifies, in dB, the first normalized CNR value in Table 228 (i.e., normalized CNR value corresponding to the CDMA code). Bytes 2–7: represent a list of numbers, where each number is encoded by one nibble, and is interpreted as a signed integer. The number encoded by each nibble represents the difference, in dB, in normalized CNR relative to the previous line in Table 228. Thus the left most nibble of the second byte corresponds to the difference between the normalized CNR value for QPSK, rate: 1/2, and the normalized CNR value for the CDMA code.

#### 7.7.4 Upstream Map (US-MAP)

The format of a US-MAP message is shown in Table 34. The US-MAP message defines the access to the upstream channel using US-MAP IEs.

**Table 34—US-MAP message format**

Syntax	Size	Notes
US-MAP_Message_Format() {		
Management Message Type = 3	8 bits	
UCD Count	8 bits	Matches the value of the Configuration Change Count of the UCD, which describes the upstream burst profiles that apply to this map.
Allocation Start Time	6 bits	Effective start time (in OFDM symbols from the start of the frame including all preambles) of the upstream allocation defined by the US-MAP.
Begin PHY Specific Section {		
Number of IEs: n	12 bits	Number of IEs in the upstream map
for ( $i = 1; i \leq n; i++$ ) {		
US-MAP_IE()	Variable	PHY specific (7.7.4.1) Define upstream bandwidth allocations. Each US-MAP message shall contain at least one IE that marks the end of the last allocated burst. (UIUC=63 as defined in Table 36).
}		
}		
If(!byte boundary)		
Padding bits	0–7 bits	Padding to octet alignment—All bits shall be set to 0.
}		

##### 7.7.4.1 US-MAP IE

The SID field carried by the US-MAP IE is associated with a unicast address. When specifically addressed to allocate a bandwidth grant, the FID shall be the Basic FID of the CPE. A UIUC shall be used to define the type of upstream access and the upstream burst profile associated with that access. An Upstream\_Burst\_Profile shall be included in the UCD for each UIUC to be used in the US-MAP. The beginning of the upstream subframe is clearly defined by the allocation start time, which corresponds to the number of symbols from the first preamble symbol of the current frame (e.g., superframe preamble or frame preamble) plus the width of the TTG (see Figure 12). The end of the upstream subframe is defined

either by the SCH in the case of the scheduling of an intra-frame quiet period or by the US-MAP when a SCW is scheduled at the end of the frame by the presence of UIUC's 0 or 1 in the US-MAP.

The US-MAP IE is shown in Table 35, and is used to define the upstream bandwidth allocations. The first US-MAP IE shall start at the lowest numbered subchannel on the first non-allocated symbol defined by the allocation start time field of the US-MAP message. These IEs shall represent the number of OFDM slots provided for the allocation. Each allocation IE shall start immediately following the previous allocation and shall advance in the time domain. If the end of the US subframe has been reached, the allocation shall continue on the next subchannel at the first symbol (defined by the allocation start time field). The US subframe can also be defined in terms of columns as described in 7.3.2. A Burst Descriptor shall be specified in the UCD for each UIUC to be used in the US-MAP.

The SID field in this message can also refer to a group of CPEs, e.g., a multicast group. In this case, only UIUC = 0 or 1 shall be allowed to enable configuration of that group of CPEs to use an SCW (see 7.17.3 and 7.20.1.2).

**Table 35—US-MAP information elements**

Syntax	Size	Description
US-MAP_IE() {		
SID	9 bits	Station ID of the CPE.
UIUC	6 bits	7.7.4.1.1 (see Table 36).
If ((UIUC ≥ 0) && (UIUC ≤ 1)) {		
CBP Frame Number	4 bits	Frame number where the active or passive CBP action is to take place. If the identified frame falls in the next superframe (e.g., current frame is 9 and the CBP Frame Number is 4), the CPE shall make sure that a SCW is still scheduled for this frame as indicated by the upcoming SCH. If not, the CBP action shall be cancelled.
If(UIUC==0) {		Active SCW mode (CPE to transmit a CBP burst as requested by the BS).
Timing advance	16 bits	Signed number in TU corresponding to the advance of the transmission of the CBP burst at the CPE. As the CPE starts to transmit the CBP burst as its fourth symbol before the end of the frame, zero advance corresponds to this signal being received by the BS at the beginning of its fourth symbol before the end of the frame when the CPE is co-located with the BS (see Table 44).
EIRP Density Level	8 bits	EIRP per transmitted subcarrier (see 9.9.4.2). Signed in units of 0.5 dB, ranging from -104 dBm (encoded 0x00) to +23.5 dBm (encoded 0xFF).
}		
If(UIUC==1) {		Passive SCW mode (CPE to receive and demodulate the CBP burst and send content to the BS).
Channel Number	8 bits	Channel number in which the CPE shall listen to the medium for a coexistence beacon.
Synchronization mode	1 bit	= 0 The CPE will capture the CBP burst using its current synchronization (i.e., locked to its BS) for geolocation purposes. = 1 The CPE will re-synchronize on the received CBP burst using the preamble symbol and optionally pilot carriers to decode the payload for self-coexistence purposes.
} else if (UIUC ≥2) && (UIUC ≤ 3) {		
Number of Subchannels	4 bits	Number of subchannels reserved for the BW Request/UCS Notification opportunistic window.
} else if (UIUC ≥4) && (UIUC ≤ 6) {		
Number of Subchannels	4 bits	Number of subchannels reserved for the CDMA Ranging/BW Request/UCS notification opportunistic window. Note that in case where UIUC=8 and any UIUC in the range 4 to 6 are allocated to a

Syntax	Size	Description
		frame, the largest number of subchannel specified shall prevail. Note also that when the CDMA ranging burst is to be used for terrestrially-based geolocation (see 10.5.2), the number of subchannels shall be at least 6.
Number of symbols	5 bits	Number of symbols in the US ranging channel reserved for the opportunistic windows carrying either CDMA Periodic Ranging/BW Request/UCS notification as specified by the respective UIUC. These shall be placed in the ranging channel following the initial ranging window if scheduled and consecutively (see Figure 157).
<code>} else if (UIUC == 7) {</code>		
CDMA_Allocation_IE()	20 bits	See 7.7.4.1.2.
<code>} else if (UIUC == 8) {</code>		The first 5 symbols of the upstream subframe shall be reserved for the opportunistic initial ranging burst.
Number of Subchannels	4 bits	Number of subchannels reserved for the initial ranging burst. Note that in case where UIUC=8 and any UIUC in the range 4 to 6 are allocated to a frame, the largest number of claimed subchannels specified shall prevail.
<code>} else if (UIUC == 9) {</code>		US-MAP EIRP Control IE
US-MAP EIRP Control IE	Variable	See 7.7.4.1.3.
<code>} else if (UIUC == 62) {</code>		
US_Extended_IE()	Variable	See 7.7.4.1.4.
<code>} else {</code>		
Burst_Type	1 bit	This value specifies the burst type for the burst specified by this US-MAP IE. 0: Bursts are mapped in the time axis over the full width of the upstream subframe before incrementing in the frequency axis. 1: Bursts are mapped in the time axis over segments of 7 symbols before incrementing in the frequency axis and then re-tracing to the lowest unused subchannel in the next 7 symbol segment. The width of the last segment is to be between 7 and 13 symbols depending on the width of the upstream subframe.
Duration	12 bits	Number of OFDM slots linearly allocated to the US burst specified by this IE. (Up to 60 by 30 slots can be allocated to a US burst.)
MDP	1 bit	Measurement Data Preferred Used by the BS to indicate to the CPE that this upstream allocation is to be preferably used by the CPE for the specific purpose of reporting back any measurement data. The measurement data to be reported is in connection to the specified Transaction ID. In case the CPE does not have anything to report, it can use this allocation for any other data. This is useful, for example, after a quiet period. 0: Measurement data not required (default) 1: Measurement data preferred
MRT	1 bit	Measurement Report Type In case MDP == 1, this field indicates which type of report the BS wants the CPE to send back. 0: Detailed (see 7.7.18.3.1.1 through 7.7.18.3.1.8) 1: Consolidated (see 7.7.18.3.1.9)
CMRP	1 bit	Channel Management Response Preferred Used by the BS to indicate to the CPE that this upstream allocation is to be used for confirming or not the receipt of the channel management command with the Transaction ID specified. 0: Channel management response not required (default) 1: Channel management response required
<code>}</code>		
<code>}</code>		

### 7.7.4.1.1 UIUC allocations

Table 36 specifies the UIUC incorporated into the MAC. In particular, the self-coexistence UIUCs (in both modes) have the same applicability to their DIUC counterpart (see 7.7.2.1.1).

**Table 36— UIUC values**

UIUC	Usage		
0	Self-Coexistence (Active Mode)		
1	Self-Coexistence (Passive Mode)		
2	UCS Notification		
3	BW Request		
4	CDMA UCS Notification		
5	CDMA BW Request		
6	CDMA Periodic Ranging		
7	CDMA Allocation IE (see Table 37)		
8	CDMA Initial Ranging		
9	US-MAP EIRP Control IE		
10~12	<i>Reserved</i>		
13	Uncoded	N/A	BPSK
14	Convolutional Code	FEC rate = 1/2	QPSK
15	Convolutional Code	FEC rate = 2/3	QPSK
16	Convolutional Code	FEC rate = 3/4	QPSK
17	Convolutional Code	FEC rate = 5/6	QPSK
18	Convolutional Code	FEC rate = 1/2	16-QAM
19	Convolutional Code	FEC rate = 2/3	16-QAM
20	Convolutional Code	FEC rate = 3/4	16-QAM
21	Convolutional Code	FEC rate = 5/6	16-QAM
22	Convolutional Code	FEC rate = 1/2	64-QAM
23	Convolutional Code	FEC rate = 2/3	64-QAM
24	Convolutional Code	FEC rate = 3/4	64-QAM
25	Convolutional Code	FEC rate = 5/6	64-QAM
26	CTC	FEC rate = 1/2	QPSK
27	CTC	FEC rate = 2/3	QPSK
28	CTC	FEC rate = 3/4	QPSK
29	CTC	FEC rate = 5/6	QPSK
30	CTC	FEC rate = 1/2	16-QAM
31	CTC	FEC rate = 2/3	16-QAM
32	CTC	FEC rate = 3/4	16-QAM
33	CTC	FEC rate = 5/6	16-QAM
34	CTC	FEC rate = 1/2	64-QAM
35	CTC	FEC rate = 2/3	64-QAM
36	CTC	FEC rate = 3/4	64-QAM
37	CTC	FEC rate = 5/6	64-QAM
38	LDPC	FEC rate = 1/2	QPSK
39	LDPC	FEC rate = 2/3	QPSK
40	LDPC	FEC rate = 3/4	QPSK
41	LDPC	FEC rate = 5/6	QPSK
42	LDPC	FEC rate = 1/2	16-QAM
43	LDPC	FEC rate = 2/3	16-QAM
44	LDPC	FEC rate = 3/4	16-QAM
45	LDPC	FEC rate = 5/6	16-QAM
46	LDPC	FEC rate = 1/2	64-QAM
47	LDPC	FEC rate = 2/3	64-QAM
48	LDPC	FEC rate = 3/4	64-QAM
49	LDPC	FEC rate = 5/6	64-QAM
50	SBTC	FEC rate = 1/2	QPSK
51	SBTC	FEC rate = 2/3	QPSK

UIUC	Usage		
52	SBTC	FEC rate = 3/4	QPSK
53	SBTC	FEC rate = 5/6	QPSK
54	SBTC	FEC rate = 1/2	16-QAM
55	SBTC	FEC rate = 2/3	16-QAM
56	SBTC	FEC rate = 3/4	16-QAM
57	SBTC	FEC rate = 5/6	16-QAM
58	SBTC	FEC rate = 1/2	64-QAM
59	SBTC	FEC rate = 2/3	64-QAM
60	SBTC	FEC rate = 3/4	64-QAM
61	SBTC	FEC rate = 5/6	64-QAM
62	Extended UIUC		
63	End of Map		

#### 7.7.4.1.2 CDMA Allocation IE

This IE is used by the BS with UIUC = 7 to assign a US bandwidth allocation to a CPE that signaled its wish to either associate through the Initial Ranging CDMA burst, to signal the presence of an incumbent by the CDMA UCS Notification, or to request a BW allocation through the CDMA BW Request burst.

**Table 37 — CDMA allocation IE format**

Syntax	Size	Notes
CDMA_Allocation_IE() {		
Code	8 bits	Indicates the Code sent by the CPE.
Duration	5 bits	Indicates the duration, in OFDMA slots, of the allocation. (Not necessarily on the same subchannel.)
UIUC	6 bits	UIUC to be used by the CPE for this allocation (see Table 36).
Usage	1 bit	If (Code = Incumbent) This field indicates whether the CPE shall transmit only the MAC header with the notification. 1: yes; 0: no
}		

#### 7.7.4.1.3 US-MAP EIRP Control IE

When an EIRP change for the CPE is needed, this UIUC = 9 is used as shown in Table 38. The EIRP control value is an 8-bit signed integer expressing the EIRP per subcarrier (in 0.5 dB units) that the CPE should apply instead of its current transmission EIRP (see 9.9.4.2). The current FID used with this IE shall be the Basic FID of the CPE. The EIRP accuracy shall be  $\pm 1.5$  dB when the level is at least 10 dB below the maximum regulatory power limit and  $\pm 0.5$  dB elsewhere.

**Table 38 — US-MAP EIRP control IE format**

Syntax	Size	Notes
EIRP_Control_IE() {		
UIUC	6 bits	0x09
EIRP_Control	8 bits	Signed integer that indicates the EIRP per subcarrier that the CPE should apply to correct its current transmission EIRP. Signed in units of 0.5 dB, ranging from -104 dBm (encoded 0x00) to +23.5 dBm (encoded 0xFF).
}		

#### 7.7.4.1.4 US-MAP Extended UIUC IE

A US-MAP IE entry with a UIUC value of 62 indicates that the IE carries special information and conforms to the structure shown in Table 39. A BS/CPE shall ignore an extended IE entry with an extended UIUC value for which it has no knowledge. In the case of a known extended UIUC value but with a length field longer than expected, it shall process information up to the known length and ignore the remainder of the IE.

**Table 39—US-MAP extended IE general format**

Syntax	Size	Notes
US_Extended_IE() {		
Extended UIUC	6 bits	Values specific to the Extended IE
Length	8 bits	Length of this IE in bits
Unspecified Data	Variable	
}		

#### 7.7.4.1.4.1 US-MAP Dummy Extended IE

A CPE shall be able to decode the US-MAP Dummy Extended IE. A BS shall not transmit this IE (unless under test). The Length field of Table 40 specifies the size of the Unspecified Data Field.

**Table 40—US-MAP Dummy Extended IE format**

Syntax	Size	Notes
Dummy_IE() {		
Extended UIUC	6 bits	0x00
Length	8 bits	Length of this IE in bits
Unspecified Data	Variable	
}		

#### 7.7.5 RNG-REQ

The format of a Ranging Request (RNG-REQ) message is shown in Table 41. An RNG-REQ shall be transmitted by the CPE at initialization and periodically to determine network delay and to request EIRP and/or downstream burst profile change. The RNG-REQ message may be sent in Initial Ranging and data grant intervals.

The FID field carried in the MAC header of the PDU, and the SID in the US-MAP IE indicating from which CPE this message is transmitted shall assume the following values when sent in the granted Initial Ranging upstream interval:

- SID = Cell SID, FID = Initial ranging FID if the CPE is attempting to join the network.
- SID = Cell SID, FID = Initial ranging FID if the CPE has not yet registered and is changing channel.
- For periodic ranging, the SID is a unicast SID assigned to the CPE in a RNG-CMD MAC message whereas the FID is the Basic FID.

If sent in a data grant interval, the FID is always equal to the Basic FID.

**Table 41—RNG-REQ message format**

Syntax	Size	Notes
RNG-REQ Message Format() {		
Management Message Type = 4	8 bits	
Information elements (IEs)	Variable	Table 42
If (!byte_boundary)		
Padding Bits	0–7 bits	Padding to octet alignment—All bits shall be set to 0.
}		

**Table 42— RNG-REQ information elements**

Name	Element ID (1 byte)	Length	Description
Downstream burst profile	1	6 bits	Burst profile that can be received by the CPE for the RNG-CMD.
CPE MAC address	2	6 bytes	CPE MAC address that is assigned universally by manufacturers.
MMP_PN	3	3 bytes	MMP_PN of MMP_Key associated with active authorization key (AK) context installed on CPE (see 8.2.4.6).
Ciphertext ICV	4	8 bytes	Ciphertext ICV calculated over the RNG-REQ message, excluding the MMP_PN IE (see 8.2.4.6).
Ranging anomalies	5	3 bits	A parameter indicating a potential error condition detected by the CPE during the ranging process. Setting the bit associated with a specific condition indicates that the condition exists at the CPE. Bit 0—CPE already at maximum EIRP. Bit 1—CPE already at minimum EIRP. Bit 2—Timing advance is too large.

### 7.7.6 RNG-CMD

The format of a Ranging Command (RNG-CMD) message is shown in Table 43. An RNG-CMD shall be transmitted by the BS in response to a received RNG-REQ. In addition, it may also be transmitted without a specific RNG-REQ message received by the BS to send corrections based on measurements that have been made on other received data or MAC messages from the CPE. As a result, the CPE shall be prepared to receive an RNG-CMD at any time, not just following an RNG-REQ transmission.

**Table 43— RNG-CMD message format**

Syntax	Size	Notes
RNG-CMD_Message_Format() {		
Management Message Type = 5	8 bits	
Information elements (IEs)	Variable	Table 44
If (!byte_boundary)		
Padding Bits	0–7 bits	Padding to octet alignment—All bits shall be set to 0.
}		

Information elements 1–7 of Table 44 are used for normal CDMA ranging purposes. Information elements 6–9 of Table 44 are used for CDMA geolocation re-try purposes.

**Table 44— RNG-CMD information elements**

Name	Element ID (1 byte)	Length (bits)	Description
Timing advance	1	16	Unsigned timing advance at the CPE, in number of TU, to compensate for the signal propagation delay on both, the downstream and the upstream RF paths, so that the upstream burst arrives at the BS within the tolerance specified in 9.9.2. The timing advance shall be set to 0 when the CPE is co-located with the BS and shall increase as the CPE is located further away from the BS.
EIRP per subcarrier	2	8	P <sub>range</sub> : EIRP per transmitted subcarrier (see 9.9.4.2). Signed in units of 0.5 dB and ranging from –104 dBm (encoded 0x00) to +23.5 dBm (encoded 0xFF). Values outside this range shall be assigned the closest extreme.
Offset frequency adjust	3	16	Signed number in Hertz

Name	Element ID (1 byte)	Length (bits)	Description
Ranging status	4	3	000: Continue 001: Abort 010: Success 011: Re-range 100: Reauthenticate 101: Re-range and Re-register 110–111: Reserved
CPE MAC address	6	48	CPE MAC address that's assigned universally by manufacturer.
Station ID	7	9	Required parameter when RNG-CMD is sent in response to initial ranging. This may be temporary if the CPE Privacy is enabled (see 8.6).
Action Superframe Number	8	8	The superframe number (modulo 256) at which Channel Action shall be performed.
Action Frame Number	9	4	Integer value greater than or equal to zero that indicates the starting frame number, within the Action Superframe Number, at which the Channel Action shall be performed by all CPEs.
CDMA code	10	1	A unique code assigned to the CPE, to be used for dedicated ranging. Code is from the initial ranging codeset.
Transmission opportunity offset	11	1	A unique transmission opportunity assigned to the CPE, to be used for dedicated ranging in units of symbol duration.

### 7.7.7 REG-REQ/RSP

CPEs shall register with a BS before receiving or being provided any type of service. In the following subclauses, the registration process incorporated in the MAC as well as a series of IEs that may be carried by these messages are presented.

#### 7.7.7.1 REG-REQ

The format of a REG-REQ message is shown in Table 45. This message shall be transmitted by CPEs at initialization phase.

The FID field carried in the MAC header of the PDU where this message is transmitted shall be the primary management FID for this CPE, which is assigned during the RNG-CMD message.

**Table 45—REG-REQ message format**

Syntax	Size	Notes
REG-REQ Message Format() {		
Management Message Type = 6	8 bits	
Information elements (IEs)	Variable	7.7.7.3
}		

#### 7.7.7.2 REG-RSP

The format of an REG-RSP message is shown in Table 46. This message shall be transmitted by the BS in response to a REG-REQ.

The FID field carried in the MAC header of the PDU where this message is transmitted shall be the primary management FID of the CPE for which this message is intended.

**Table 46— REG-RSP message format**

Syntax	Size	Notes
REG-RSP Message Format() {		
Management Message Type = 7	8 bits	
Response	8 bits	0x00: OK 0x01: Failure (e.g., authentication)
Information elements (IEs)	Variable	7.7.7.3
Confirmation code	8 bits	Code defining error status of registered capability configuration request (see 7.7.24)
}		

### 7.7.7.3 REG-REQ/RSP information elements

REG-REQ and REG-RSP management messages may carry a number of IEs that support the registration process. The REG-REQ message shall include the CPE NMEA Location String IE. These IEs are described in detail in the following subclauses.

#### 7.7.7.3.1 CPE NMEA Location String

This is the location data string pertaining to the CPE's location. It shall be in the NMEA 0183 ASCII format. This IE shall be added to the REG-REQ message during initial registration during network entry, as well as in the transmission of a REG-REQ that is in response to a RNG-CMD sent with ranging status set to "Re-range and Re-register" (see 7.14.2.11).

**Table 47— CPE NMEA Location String information element**

Syntax	Size	Remarks
CPE_NMEA_Location_String() {		
Element ID	1 byte	1
Length	2 bytes	length of location data string in octets
Location Data String	Variable	NMEA 0183 ASCII string
}		

#### 7.7.7.3.2 Convergence sublayer configuration

The Convergence sublayer configuration parameter dictates how the provider intends to operate the CPE on an ongoing basis. If the IE= 0, the CPE shall use the Ethernet CS. This allows the CPE to either act as a bridge or other Ethernet device. If IE = 1, the CPE shall use the IP CS. This allows the CPE to either act as a router, or other IP-based device.

**Table 48— Convergence Sublayer Specification information element**

Element ID	Length (bytes)	Value	Scope
3	1	0x00: Ethernet CS 0x01: IP CS 0x02–0xFF: Reserved	REG-REQ, REG-RSP

#### 7.7.7.3.3 IP Version

This field indicates the version of Internet Protocol used on the Secondary Management Connection. IPv6 is not mandatory. The omission of the IP Version parameter in the REG-REQ message shall be interpreted as IPv4 support only.

**Table 49—IP Version information element**

Element ID	Length (bytes)	Value	Scope
4	1	0x00: IPv4 0x01: IPv6	REG-REQ, REG-RSP

#### 7.7.7.3.4 CPE capability

Through the registration process a BS shall become aware of the capabilities of the registering CPEs. The following subclauses describe the IEs that convey the CPE capability information to the BS.

##### 7.7.7.3.4.1 IP ROHC support

This IE indicates the ability of the CPE to support IP Robust Header Compression (ROHC).

**Table 50—IP ROHC Support information element**

Element ID	Length (bytes)	Value	Scope
5	1	0x00: No IP ROHC support 0x01: IP ROHC supported 0x02–0xFF: Reserved	REG-REQ, REG-RSP

##### 7.7.7.3.4.2 ARQ support

This field indicates the availability of CPE support for ARQ. If ARQ is enabled for Secondary Management flow, the IEs that are defined in 7.7.8.9.17.2 to 7.7.8.9.17.8 shall be added to the REG-REQ or REG-RSP to facilitate configuration of ARQ that is to be applied on PDUs traversing the Secondary Management flow.

**Table 51—ARQ Support information element**

Element ID	Length (bytes)	Value	Scope
6	1	0x00: No ARQ support 0x01: ARQ supported on Secondary Management flow only 0x02: ARQ supported on Transport flows only 0x03: ARQ supported on Secondary Management and Transport flows 0x04–0xFF: Reserved	REG-REQ, REG-RSP

##### 7.7.7.3.4.3 ARQ parameters

This field provides the fragmentation and ARQ parameters applied during the establishment of the secondary management connection. This field is related to the ARQ parameters described in 7.7.8.9.17.

**Table 52—ARQ information elements**

Element ID	Length (bytes)	Value	Scope
2	Variable	Compound	REG-REQ, REG-RSP

##### 7.7.7.3.4.4 DSx Flow Control

This field specifies the maximum number of concurrent DSA, DSC, or DSD transactions that may be outstanding.

**Table 53— DSx Flow Control information element**

Element ID	Length (bytes)	Value	Scope
7	1	0: no limit (default) 1–255: indicate maximum concurrent transactions	REG-REQ, REG-RSP

#### 7.7.7.3.4.5 MCA Flow Control

This field specifies the maximum number of concurrent MCA transactions that may be outstanding.

**Table 54— MCA Flow Control information element**

Element ID	Length (bytes)	Value	Scope
8	1	0: no limit (default) 1–255: indicate maximum concurrent transactions	REG-REQ, REG-RSP

#### 7.7.7.3.4.6 Maximum number of Multicast Groups supported

This field indicates the maximum number of simultaneous Multicast Groups to which the CPE is capable of belonging.

**Table 55— Maximum number of Multicast Groups supported information element**

Element ID	Length (bytes)	Value	Scope
9	1	0–255 0 (default)	REG-REQ, REG-RSP

#### 7.7.7.3.4.7 Measurement support

The CPE adds this IE in the REG-REQ to indicate to the BS what sensing capabilities the CPE supports, as well as how well the CPE can sense for particular signals. In the REG-RSP, the BS sets this IE to configure what sensing capabilities the CPE will make use of and how sensing for particular signals is to be executed. Note that if the “No Sensing” bit (Bit 0) in the Sensing Mode Support Bitmap is set to True, Bits 1, 2, and 3 shall be set to False. When the BS configures the IE for transmission in a REG-RSP, then sensing would be disabled at the CPE.

**Table 56— Measurement Support information element**

Syntax	Size	Description	Scope
MS IE0 {			
Element ID	8 bits	10	
Length	16 bits	n×7+5 (bytes) where “n” is equal to the number of ones in the Signal Type Array.	
Sensing Mode Support Bitmap	8 bits	Bit 0: No Sensing Bit 1: Sensing Mode 1 Bit 2: Sensing Mode 2 Bit 3: Sensing Mode 3 Bit 4–7: Reserved, set to 0 0: False, 1: True	REG-REQ, REG-RSP
Signal Type Array	32 bits	Signal Type Array that Spectrum Sensing Function is capable of sensing (see Table 237).	
for (i = 1; i ≤ n; i++) {		n = number of ones in the Signal Type Array.	

Syntax	Size	Description	Scope
Sensitivity Threshold	12 bits	Only applies for incumbent profiles. Signed number that indicates the threshold (in dBm) to be used by CPEs for detection (see Table 247).	
PD	8 bits	Probability of Detection. 0x00 indicates ‘0’ and 0xFF indicates ‘1’	
MPFA	8 bits	Maximum Probability of False Alarm—0x00 indicates ‘0’ and 0xFF indicates ‘0.256’	
Recommended NumSensingPeriods	7 bits	See Table 238—Number of sensing periods required.	
Recommended SensingPeriodDuration	10 bits	See Table 238—Sensing Period Duration as specified as an integer number of symbols	
Recommended SensingPeriodInterval	11 bits	See Table 238—Sensing Period Interval as specified in the integer number of frames	
}			
Padding Bits	6 bits	To make this IE an integer number of bytes.	
}			

#### 7.7.7.3.4.8 Manufacturer-specific Antenna Model

**Table 57 — Manufacturer-specific Antenna Model information element**

Element ID	Length (bytes)	Value	Scope
11	2	Length in bytes	REG-REQ, REG-RSP

#### 7.7.7.3.4.9 CPE Antenna Gain

This information provided by the CPE at registration can be used by the BS to prioritize its list of backup/candidate channels based on the receiving performance of its CPE.

**Table 58 — CPE Antenna Gain information element**

Syntax	Size	Notes	Scope
AG IE() {			
Element ID	8 bits	12	
Number of channels	8 bits	Total number of channels for which the antenna gain is defined.	
for ( $i = 1; i \leq n; i++$ ) {		$n =$ the number of channels	
Channel number	8 bits		
On-axis gain	8 bits	Maximum on-axis antenna gain in the specified channel in 0.25 dB units from –22.0 dBi (0x01) to 41.0 dBi (0xFD) 0x00: the CPE or BS shall refrain from transmitting on this channel 0x01: also used for antenna gain smaller than –22.0 dBi 0xFE: antenna gain larger than 41.0 dBi 0xFF is not allowed.	REG-REQ
}			
}			

#### **7.7.7.3.4.10 CPE residual delay**

This residual delay shall be measured by the manufacturer when the CPE is co-located with the BS (i.e., BS and CPE antennas are co-located or the BS and CPE are connected through the proper lengths of feed cables) and the Timing Advance (see Table 44) is set to zero. The manufacturer shall record this residual delay in the CPE, which shall be reported to the BS at the time of registration on the network.

**Table 59—CPE MAC address**

Element ID	Length (bytes)	Value	Scope
13	3	CPE Residual Delay Signed integer representing the CPE residual delay in nano-seconds. Positive value indicates a delay. Negative value indicates an advance. Accuracy shall be within $\pm 30$ ns for 10 m distance accuracy.	CBC-REQ

#### **7.7.7.3.4.11 Method for allocating IP addresses on secondary management connections**

**Table 60—IP address allocation information element**

Element ID	Length (bytes)	Value	Scope
14	1	Bit 0: DHCPv4 Bit 1: Mobile IPv4 Bit 2: DHCPv6 Bit 3: IPv6 Stateless Address Autoconfiguration Bit 4–7: <i>Reserved, shall be set to 0.</i>	REG-REQ, REG-RSP

#### **7.7.7.3.4.12 Permanent Station ID**

This field specifies the permanent SID assigned to a CPE. This IE is included if the CPE Privacy (see Clause 8) during network entry is supported by the operator.

**Table 61—Permanent Station ID information element**

Element ID	Length (bytes)	Value	Scope
15	2	Permanent SID (Bit 0000 000b bbbb bbbb)	REG-REQ

#### **7.7.7.3.4.13 CPE Operational Capability**

This field allows the CPE to signal to the BS that it is to be operated as a Fixed or Portable terminal.

**Table 62—CPE Operational Capability information element**

Element ID	Length (bytes)	Value	Scope
16	1	0x00- Fixed 0x01: Portable 0x02–0xFF: <i>Reserved</i>	REG-REQ/RSP

### 7.7.7.3.5 CPE Registration Timer

This timer is used to govern how long a CPE and BS maintain context of each other after registration has been completed. This value is set based on the type of CPE, either portable or fixed, that is currently attempting registration. This value is used to set T30.

**Table 63—CPE Registration Timer information element**

Element ID	Length (bytes)	Remarks	Scope
17	2	= 0x0000, Reserved = 0x0001–0xFFFF, in units of 160 ms	REG-REQ, REG-RSP

## 7.7.8 Dynamic Service Messages (DSx-REQ/RSP/ACK)

To manage the various traffic flows between CPEs and the BS, the MAC protocol shall have the capability to dynamically manage the addition, deletion, and change of service flows.

### 7.7.8.1 DSA-REQ

The format of a Dynamic Service Addition Request (DSA-REQ) message is shown in Table 64. This message is sent either by a CPE or BS and is to create a new service flow, and shall not contain parameters for more than one service flow.

The FID field carried in the MAC header of the PDU where this message is transmitted shall be the primary management FID of the CPE.

**Table 64—DSA-REQ message format**

Syntax	Size	Notes
DSA-REQ Message Format() {		
Management Message Type = 8	8 bits	
Transaction ID	16 bits	Unique identifier for this transaction assigned by the sender.
Information elements (IEs)	Variable	7.7.8.9
}		

### 7.7.8.2 DSA-RSP

A DSA-RSP message shall be generated in response to a received DSA-REQ message. The format of a DSA-RSP message shall be as shown in Table 65. If the transaction is successful, the DSA-RSP message may contain the following: Service Flow parameters (the complete specification of the service flow shall be included in the DSA-RSP if it includes a newly assigned FID or an expanded service class name) and CS parameter encodings (specification of the service flow's CS-specific parameters).

**Table 65—DSA-RSP message format**

Syntax	Size	Notes
DSA-RSP Message Format() {		
Management Message Type = 9	8 bits	
Transaction ID	16 bits	
Confirmation code	8 bits	7.7.24
Information elements (IEs)	Variable	7.7.8.9
}		

### 7.7.8.3 DSA-ACK

A DSA-ACK message shall be generated in response to a received DSA-RSP message. The format of a DSA-ACK message shall be as shown in Table 66.

**Table 66— DSA-ACK message format**

Syntax	Size	Notes
DSA-ACK Message Format() {		
Management Message Type = 10	8 bits	
Transaction ID	16 bits	
Confirmation code	8 bits	7.7.24
Information elements (IEs)	Variable	7.7.8.9
}		

### 7.7.8.4 DSC-REQ

A Dynamic Service Change Request (DSC-REQ) message is sent by a CPE or BS to dynamically change the parameters of an existing service flow. A CPE or BS shall generate DSC-REQ messages in the form shown in Table 67. A DSC-REQ message shall carry parameters for only one service flow. A DSC-REQ message shall contain Service Flow parameters that specify the service flow's new traffic characteristics and scheduling requirements. The admitted and active QoS parameter sets are the ones currently in use by the service flow. If the DSC message is successful and it contains service flow parameters, but does not contain replacement sets for both admitted and active QoS parameter sets, the omitted set(s) shall be set to null. The Service Flow parameters shall contain a SFID.

**Table 67— DSC-REQ message format**

Syntax	Size	Notes
DSC-REQ Message Format() {		
Management Message Type = 11	8 bits	
Transaction ID	16 bits	
Information elements (IEs)	Variable	7.7.8.9
}		

### 7.7.8.5 DSC-RSP

A DSC-RSP shall be generated in response to a received DSC-REQ. The format of a DSC-RSP shall be as shown in Table 68. If the transaction is successful, the DSC-RSP may contain the Service Flow parameters in which the complete specification of the service flow shall be included in the DSC-RSP only if it includes a newly assigned FID or an expanded service class name. If a Service Flow parameter set contains an upstream admitted QoS parameter set and this service flow does not have an associated FID, the DSC-RSP shall include a FID. If a Service Flow parameter set contains a service class name and an admitted QoS parameter set, the DSC-RSP shall include the QoS parameter set corresponding to the named service class. If specific QoS parameters are also included in the classed service flow request, these QoS parameters shall be included in the DSC-RSP instead of any QoS parameters of the same type of the named service class. Additionally, the DSC-RSP may contain the CS parameter encodings that specify the CS-specific parameters of the service flow.

**Table 68— DSC-RSP message format**

Syntax	Size	Notes
DSC-RSP Message Format() {		
Management Message Type = 12	8 bits	
Transaction ID	16 bits	
Confirmation code	8 bits	7.7.24
Information elements (IEs)	Variable	7.7.8.9
}		

### 7.7.8.6 DSC-ACK

A DSC-ACK shall be generated in response to a received DSC-RSP. The format of a DSC-ACK shall be as shown in Table 69.

**Table 69— DSC-ACK message format**

Syntax	Size	Notes
DSC-ACK_Message_Format() {		
Management Message Type = 13	8 bits	
Transaction ID	16 bits	
Confirmation code	8 bits	7.7.24
Information elements (IEs)	Variable	7.7.8.9
}		

### 7.7.8.7 DSD-REQ

A Dynamic Service Deletion Request (DSD-REQ) is sent by a CPE or BS to delete an existing service flow. The format of a DSD-REQ shall be as shown in Table 70.

**Table 70— DSD-REQ message format**

Syntax	Size	Notes
DSD-REQ_Message_Format() {		
Management Message Type = 14	8 bits	
Transaction ID	16 bits	
Service Flow ID	32 bits	
Information elements (IEs)	Variable	7.7.8.9
}		

### 7.7.8.8 DSD-RSP

A DSD-RSP shall be generated in response to a received DSD-REQ. The format of a DSD-RSP shall be as shown in Table 71.

**Table 71— DSD-RSP message format**

Syntax	Size	Notes
DSD-RSP_Message_Format() {		
Management Message Type = 15	8 bits	
Transaction ID	16 bits	
Confirmation code	8 bits	7.7.24
Service Flow ID	32 bits	
Information elements (IEs)	Variable	7.7.8.9
}		

### 7.7.8.9 Service Flow encodings

Table 72 and the subsequent subclauses define the parameters associated with upstream/downstream scheduling for a service flow. The encapsulated upstream and downstream flow classification configuration setting strings share the same subtype field numbering plan because many of the subtype fields defined are valid for both types of configuration settings except service flow encodings. One major parameter of the service flow definition is the direction of the service flow (see 7.7.8.9.1). This parameter determines if subsequent service flow parameters are applied in the downstream (BS to CPE) or upstream (CPE to BS) service flow. Classification rule parameterization (see 7.7.8.9.18) is made of a compound set of IEs defined in 7.7.8.9.18.1 through 7.7.8.9.18.3.14.

**Table 72—Service flow encodings information elements**

Element ID	Parameter
1	Service Flow Direction
2	Service Flow Identifier
3	Service Class Name
4	QoS Parameter Set Type
5	Maximum Sustained Traffic Rate
6	Maximum Traffic Burst
7	Minimum Reserved Traffic Rate
8	Minimum Tolerable Traffic Rate
9	Service Flow Scheduling Type
10	Request/Transmission Policy
11	Tolerated Jitter
12	Maximum Latency
13	Fixed-length versus Variable-length SDU Indicator
14	SDU Size
15	Target SAID
16	Maximum Tolerable Packet Loss Rate
17.1–17.9	ARQ Parameter IEs for ARQ-enabled Connections (Compound)
18	Classification Rule Convergence Sublayer Specification
19	Classifier DSC Action
20.1–20.14	Packet Classification Rule (Compound)
21–255	<i>Reserved</i>

#### 7.7.8.9.1 Service Flow Direction

This parameter is used to indicate the direction of the service flow. Service flows are unidirectional and are DS (BS to CPE) or US (CPE to BS).

**Table 73—Service Flow Direction IE**

Element ID	Length (bytes)	Value	Scope
1	1	0x00: Downstream 0x01: Upstream 0x02–0xFF: <i>Reserved</i>	DSx-REQ, DSx-RSP, DSx-ACK

#### 7.7.8.9.2 SFID

The format of the Service Flow Identifier (SFID) is defined in Table 74.

**Table 74—SFID definition information element**

Element ID	Length (bytes)	Value	Scope
2	4	1-4 294 967 295	DSx-REQ, DSx-RSP, DSx-ACK

#### 7.7.8.9.3 Service Class Name

The format of the Service Class Name is defined in Table 75.

**Table 75— Service Class Name definition information element**

Element ID	Length (bytes)	Value	Scope
3	2 to 128	Null-terminated string of ASCII characters. The length of the string, including null-terminator, may not exceed 128 bytes	DSx-REQ, DSx-RSP, DSx-ACK

#### 7.7.8.9.4 QoS Parameter Set Type

The format of the QoS Parameter Set Type is defined in Table 76 as the three first bits of the octet, and Table 77 enumerates all the combinations for these 3 bits that define controls for how QoS parameter sets are applied to the service flow that is being configured.

**Table 76— QoS Parameter Set Type definition**

Element ID	Length (bytes)	Value	Scope
4	1	Bit 0: Provisioned Set Bit 1: Admitted Set Bit 2: Active Set Bits 3–7: Reserved	DSx-REQ, DSx-RSP, DSx-ACK

**Table 77— Value used in Dynamic Service messages**

Value	Messages
001	Apply to Provisioned set only
011	Apply to Provisioned and Admitted sets, and perform admission control
101	Apply to Provisioned and Admitted sets, perform admission control, and activate this service flow
111	Apply to Provisioned, Admitted, and Active sets, perform admission control, and activate this service flow
000	Set Active and Admitted sets to Null
010	Perform admission control and apply admitted set
100	Check against Admitted set in separate service flow encoding, perform admission control if needed, active this service flow, and apply to Active set
110	Perform admission control and activate this service flow, apply parameters to both Admitted and Active sets

#### 7.7.8.9.5 Maximum Sustained Traffic Rate

The format of the Maximum Sustained Traffic Rate is defined in Table 78.

**Table 78— Maximum Sustained Traffic Rate definition**

Element ID	Length (bytes)	Value	Scope
5	3	Rate (in bits per second)	DSx-REQ, DSx-RSP, DSx-ACK

#### 7.7.8.9.6 Maximum Traffic Burst

The format of the Maximum Traffic Burst is defined in Table 79.

**Table 79— Maximum Traffic Burst definition**

Element ID	Length (bytes)	Value	Scope
6	3	Burst size (bytes)	DSx-REQ, DSx-RSP, DSx-ACK

#### **7.7.8.9.7 Minimum Reserved Traffic Rate**

The format of the Minimum Reserved Traffic Rate is defined in Table 80.

**Table 80— Minimum Reserved Traffic Rate definition**

Element ID	Length (bytes)	Value	Scope
7	3	Rate (in bits per second)	DSx-REQ, DSx-RSP, DSx-ACK

#### **7.7.8.9.8 Minimum Tolerable Traffic Rate**

The format of the Minimum Tolerable Traffic Rate is defined in Table 81.

**Table 81— Minimum Tolerable Traffic Rate definition**

Element ID	Length (bytes)	Value	Scope
8	3	Rate (in bits per second)	DSx-REQ, DSx-RSP, DSx-ACK

#### **7.7.8.9.9 Service Flow Scheduling Type**

The format of the Service Flow Scheduling Type is defined in Table 82.

**Table 82— Service Flow Scheduling Type definition**

Element ID	Length (bytes)	Value	Scope
9	1	0x00: <i>Reserved</i> 0x01: for Undefined (BS implementation dependent) 0x02: for BE (Default) 0x03: for nrtPS 0x04: for rtPS 0x05: <i>Reserved</i> 0x06: for UGS 0x07–0xFF: <i>Reserved</i>	DSx-REQ, DSx-RSP, DSx-ACK

#### **7.7.8.9.10 Request/Transmission Policy**

The format of the Request/Transmission Policy is defined in Table 83.

**Table 83— Request/Transmission Policy definition**

Element ID	Length (bytes)	Value	Scope
10	1	Bit 0: Service flow shall not use broadcast bandwidth request opportunities (Upstream only) Bit 1: <i>Reserved (shall be set to zero)</i> Bit 2: The service flow shall not piggyback requests with data (Upstream only) Bit 3: The service flow shall not fragment data Bit 4: The service flow shall not suppress payload headers (CS parameters) Bit 5: The service flow shall not pack multiple SDUs (or fragments) into single MAC PDUs Bit 6: <i>Reserved (shall be set to zero)</i> Bit 7: <i>Reserved (shall be set to zero)</i>	DSx-REQ, DSx-RSP, DSx-ACK

#### 7.7.8.9.11 Tolerated Jitter

The format of the Tolerated Jitter is defined in Table 84.

**Table 84— Tolerated Jitter definition**

Element ID	Length (bytes)	Value	Scope
11	3	ms	DSx-REQ, DSx-RSP, DSx-ACK

#### 7.7.8.9.12 Maximum Latency

The format of the Maximum Latency is defined in Table 85.

**Table 85— Maximum Latency definition**

Element ID	Length (bytes)	Value	Scope
12	3	ms	DSx-REQ, DSx-RSP, DSx-ACK

#### 7.7.8.9.13 Fixed-length vs. Variable-length SDU Indicator

The format of the Fixed-length vs Variable-length SDU Indicator is defined in Table 86.

**Table 86— Fixed-length vs. Variable-length SDU Indicator definition**

Element ID	Length (bytes)	Value	Scope
13	1	0: variable-length SDU (default) 1: fixed-length SDU	DSx-REQ, DSx-RSP, DSx-ACK

#### 7.7.8.9.14 SDU Size

The format of the SDU Size is defined in Table 87.

**Table 87— SDU Size definition**

Element ID	Length (bytes)	Value	Scope
14	1	Number of bytes Default = 49	DSx-REQ, DSx-RSP, DSx-ACK

#### 7.7.8.9.15 Target SAID

The format of the Target SAID is defined in Table 88.

**Table 88— Target SAID definition**

Element ID	Length (bytes)	Value	Scope
15	2	SAID onto which SF is mapped.	DSx-REQ, DSx-RSP

#### 7.7.8.9.16 Maximum Tolerable Packet Loss Rate

The format of the Maximum Tolerable Packet Loss Rate is defined in Table 89.

**Table 89— Maximum Tolerable Packet Loss Rate definition**

Element ID	Length (bytes)	Value	Scope
16	1	Maximum percentage of packet loss rate tolerated on a logarithm scale before a flow is dropped. Coding: first four bits: mantissa, last four bits: fraction i.e.,: 0x00: $1/\{2^{(0+[0/16])}\} = 100\%$ packet loss 0x37: $1/\{2^{(3+[7/16])}\} = 9.2\%$ packet loss 0xFF: $1/\{2^{(16+[16/16])}\}=0.0016\%$ packet loss)	DSx-REQ, DSx-RSP, DSx-ACK

#### 7.7.8.9.17 ARQ parameter IEs for ARQ-enabled connections

Parameters related to ARQ configuration are encoded in a compound attribute (Element ID = 17) as shown in Table 90, made up of subattributes described in 7.7.8.9.17.1 through 7.7.8.9.17.8.

**Table 90— ARQ common attribute format**

Element ID	Length (bytes)	Value
17	Variable	Compound

#### 7.7.8.9.17.1 ARQ Enable

The format of the ARQ Enable IE is defined in Table 91.

**Table 91— ARQ Enable definition**

Element ID	Length (bytes)	Value	Scope
17.1	1	0: ARQ not requested/accepted 1: ARQ requested/accepted	DSA-REQ, DSA-RSP, REG-REQ, REQ-RSP

#### **7.7.8.9.17.2 ARQ\_WINDOW\_SIZE**

The format of the ARQ\_WINDOW\_SIZE IE is defined in Table 92.

**Table 92— ARQ\_WINDOW\_SIZE definition**

Element ID	Length (bytes)	Value	Scope
17.2	2	> 0 and $\leq$ (ARQ_BSN_MODULUS/2)	DSx-REQ, DSx-RSP, REG-REQ, REQ-RSP

#### **7.7.8.9.17.3 ARQ\_RETRY\_TIMEOUT**

The format of the ARQ\_RETRY\_TIMEOUT IE is defined in Table 93.

**Table 93— ARQ\_RETRY\_TIMEOUT definition**

Element ID	Length (bytes)	Value	Scope
17.3	2	TRANSMITTER_DELAY 0–655350 (10 $\mu$ s granularity)	DSA-REQ, DSA-RSP, REG-REQ, REQ-RSP
17.4	2	RECEIVER_DELAY 0–655350 (10 $\mu$ s granularity)	DSA-REQ, DSA-RSP, REG-REQ, REQ-RSP

#### **7.7.8.9.17.4 ARQ\_BLOCK\_LIFETIME**

The format of the ARQ\_BLOCK\_LIFETIME IE is defined in Table 94.

**Table 94— ARQ\_BLOCK\_LIFETIME definition**

Element ID	Length (bytes)	Value	Scope
17.5	2	0: Infinite 1–65535 (10 $\mu$ s granularity)	DSA-REQ, DSA-RSP, REG-REQ, REQ-RSP

#### **7.7.8.9.17.5 ARQ\_SYNC\_LOSS\_TIMEOUT**

The format of the ARQ\_SYNC\_LOSS\_TIMEOUT IE is defined in Table 95.

**Table 95— ARQ\_SYNC\_LOSS\_TIMEOUT definition**

Element ID	Length (bytes)	Value	Scope
17.6	2	0: Infinite 1–65535 (10 $\mu$ s granularity)	DSA-REQ, DSA-RSP, REG-REQ, REQ-RSP

#### **7.7.8.9.17.6 ARQ\_DELIVER\_IN\_ORDER**

The format of the ARQ\_DELIVER\_IN\_ORDER IE is defined in Table 96.

**Table 96— ARQ\_DELIVER\_IN\_ORDER definition**

Element ID	Length (bytes)	Value	Scope
17.7	1	0: Order of delivery is not preserved 1: Order of delivery is preserved	DSA-REQ, DSA-RSP, REG-REQ, REQ-RSP

#### **7.7.8.9.17.7 ARQ\_RX\_PURGE\_TIMEOUT**

The format of the ARQ\_RX\_PURGE\_TIMEOUT IE is defined in Table 97.

**Table 97— ARQ\_RX\_PURGE\_TIMEOUT definition**

Element ID	Length (bytes)	Value	Scope
17.8	2	0: Infinite 1–65535 (10 µs granularity)	DSA-REQ, DSA-RSP, REG-REQ, REQ-RSP

#### **7.7.8.9.17.8 ARQ\_BLOCK\_SIZE**

The format of the ARQ\_BLOCK\_SIZE IE is defined in Table 98.

**Table 98— ARQ\_BLOCK\_SIZE definition**

Element ID	Length (bytes)	Value	Scope
17.9	2	0: <i>Reserved</i> 1–2040: Desired/Agreed size in bytes 2041–65535: <i>Reserved</i>	DSA-REQ, DSA-RSP, REG-REQ, REQ-RSP

#### **7.7.8.9.18 Packet CS encodings for configuration and MAC messaging**

The following encoded parameters shall be used in Dynamic Service messages (DSx-REQ/RSP).

The following configuration settings shall be supported by all CPEs that are compliant with this specification.

##### **7.7.8.9.18.1 Classification Rule Convergence Sublayer Specification**

Each classification rule defines a set of parameters that are encoded within selection of IEs listed in 7.7.8.9.18.3.1 through 7.7.8.9.18.3.14. This IE defines what CS is applied to the classification rule (see Table 99). In the cases of IP over IEEE 802.3 (or IEEE 802.1Q), the relevant IP and IEEE 802.3 (or IEEE 802.1Q) parameters shall be included in the definition of the classification rule contained within a DSx-REQ message. The Convergence Sublayer Specification IE (see 7.7.7.3.2) determines what CS and what rule parameters can be applied in building classification rules.

**Table 99— CS Sublayer Parameter Encoding Rules definition**

Element ID	Length (bytes)	Value	Scope
18	1	0x00: No CS 0x01: ETH-CS (802.3/VLAN with IPv4, IPv6) 0x02: IP CS (IPv4, IPv6) 0x03–0xFF: <i>Reserved</i>	DSA-REQ, DSC-REQ

##### **7.7.8.9.18.2 Classifier DSC Action**

When received in a DSC-REQ, the action to be taken with this classifier is indicated in Table 100.

**Table 100 — Classifier DSC Action**

Element ID	Length (bytes)	Value
19	1	0: DSC Add Classifier 1: DSC Replace Classifier 2: DSC Delete Classifier

#### **7.7.8.9.18.3 Packet Classification rule**

This compound parameter for which the format is shown in Table 101 contains the parameters of the classification rule. All parameters pertaining to a specific classification rule shall be included in the same “Packet Classification Rule” compound parameter. A packet classification rule containing only the classification rule index (see 7.7.8.9.18.3.13) and with no other classification parameters matches all packets entering the convergence sublayer. The current version of the standard only defines a simple set of packet classification rules. More elaborate rules will be developed in a later version of the standard.

**Table 101 — Packet Classification Rule common attribute format**

Element ID	Length (bytes)	Value
20	Variable	Compound

##### **7.7.8.9.18.3.1 Classification Rule Priority Field**

Several classification rules may each refer to the same service flow. The classification priority is used for ordering the application of classification rules to packets. Explicit ordering is necessary because the patterns used by classification rules may overlap.

The value of this field specifies the priority for the classification rule, which is used for determining the order of the classification rule, which may have priorities in the range 0–255 with the default value being 0. A larger value indicates a higher priority.

Element ID	Length (bytes)	Value
20.1	1	0–255

The following six fields (7.7.8.9.18.3.2 to 7.7.8.9.18.3.7) are designed for IPv4/IPv6, which should be referenced by the IP Classification Rules in 6.4.2.

##### **7.7.8.9.18.3.2 IP Type of Service/Differentiated Services Codepoint Range and Mask Field**

The values of this field specify the matching parameters for the IP type of service (ToS)/differentiated services codepoint (DSCP) octet of the IP packet. IETF RFC 2474 [B24] defines the DSCP values that can be set to the 6 MSBs of this field. The remaining 2 bits are set to 00. If this field is omitted, then the comparison of the IP packet ToS byte for this entry is irrelevant.

Element ID	Length (bytes)	Value
20.2	3	tos-low, tos-high, tos-mask

#### **7.7.8.9.18.3.3 Protocol field**

The value of this field specifies a matching value for the IP Protocol Field. For IPv6 (IETF RFC 2460 [B23]), this refers to the next header entry in the last header of the IP header chain. The encoding of the value field is that defined by the IANA document “Protocol Numbers”. If this parameter is omitted, then the comparison of the IP Header Protocol Field for this entry is irrelevant.

Element ID	Length (bytes)	Value
20.3	1	Protocol

#### **7.7.8.9.18.3.4 IP Masked Source Address parameter**

This parameter specifies an IP source address (designated “src”) and its corresponding address mask (designated “smask”). An IP packet with IP source address “ip-src” matches this parameter if  $\text{src} = (\text{ip-src} \text{ AND } \text{smask})$ . If this parameter is omitted, then the comparison of the IP packet source address for this entry is irrelevant.

Element ID	Length (bytes)	Value
20.4	8 (IPv4) 32 (IPv6)	src, smask

#### **7.7.8.9.18.3.5 IP Masked Destination Address parameter**

This parameter specifies an IP destination address (designated “dst”) and its corresponding address mask (designated “dmask”). An IP packet with IP destination address “ip-dst” matches this parameter if  $\text{dst} = (\text{ip-dst} \text{ AND } \text{dmask})$ . If this parameter is omitted, then the comparison of the IP packet destination address for this entry is irrelevant.

Element ID	Length (bytes)	Value
20.5	8 (IPv4) 32 (IPv6)	dst, dmask

#### **7.7.8.9.18.3.6 Protocol Source Port Range field**

The value of this field specifies a range of protocol source port values. Classification rules with port numbers are protocol-specific, i.e., a rule on port numbers without a protocol specification shall not be defined. An IP packet with protocol port value “src-port” matches this parameter if “src-port” is greater than or equal to “sportlow” and “src-port” is less than or equal to “sporthigh”. If this parameter is omitted, the protocol source port is irrelevant. This parameter is irrelevant for protocols without port numbers.

Element ID	Length (bytes)	Value
20.6	4	sportlow, sporthigh

#### **7.7.8.9.18.3.7 Protocol Destination Port Range field**

The value of this field specifies a range of protocol destination port values. Classification rules with port numbers are protocol-specific, i.e., a rule on port numbers without a protocol specification shall not be

defined. An IP packet with protocol port value “dst-port” matches this parameter if “dst-port” is greater than or equal to “dportlow” and “dst-port” is less than or equal to “dporhigh”. If this parameter is omitted, the protocol destination port is irrelevant. This parameter is irrelevant for protocols without port numbers.

Element ID	Length (bytes)	Value
20.7	4	dportlow, dporhigh

#### 7.7.8.9.18.3.8 IEEE 802.3/Ethernet Destination MAC Address parameter

This parameter specifies a MAC destination address (designated “dst”) and its corresponding address mask (designated “msk”). An IEEE 802.3/Ethernet packet with MAC destination address “etherdst” corresponds to this parameter if dst = (etherdst AND msk). If this parameter is omitted, then the comparison of the IEEE 802.3/Ethernet destination MAC address for this entry is irrelevant.

Element ID	Length (bytes)	Value
20.8	12	dst, msk

#### 7.7.8.9.18.3.9 IEEE 802.3/Ethernet Source MAC Address parameter

This parameter specifies a MAC source address (designated “src”) and its corresponding address mask (designated “msk”). An IEEE 802.3/Ethernet packet with MAC source address “ethersrc” corresponds to this parameter if src = (ethersrc AND msk). If this parameter is omitted, then the comparison of the IEEE 802.3/Ethernet source MAC address for this entry is irrelevant.

Element ID	Length (bytes)	Value
20.9	12	src, msk

#### 7.7.8.9.18.3.10 Ethertype/IEEE 802.2 SAP

The format of Layer 3 protocol ID in the Ethernet packet is indicated by “type,” “eport1,” and “eport2” as follows.

- If type = 0, the rule does not use the Layer 3 protocol type as a matching criteria. In addition, eport1 and eport2 are ignored when considering whether a packet matches the current rule.
- If type = 1, the rule applies only to SDUs that contain an Ethertype value. Ethertype values are contained in packets using the DEC-Intel-Xerox (DIX) encapsulation or the Sub-Network Access Protocol (SNAP) encapsulation (IEEE 802.2, IETF RFC 1042) format. In this case, eport1 and eport2 give the 16 bit value of the Ethertype that the packet shall match in order to match the rule.
- If type = 2, the rule applies only to SDUs using the IEEE 802.2 encapsulation format with a Destination Service (DSAP) other than 0xAA (which is reserved for SNAP). In this case, the lower 8 bits of eport1 and eport2 shall match the DSA byte of the packet in order to match the rule.

If the Ethernet SDU contains an IEEE 802.1D and IEEE 802.1Q tag header (i.e., Ethertype 0x8100), this object applies to the embedded Ethertype field within the IEEE 802.1D and IEEE802.1Q header.

Other values of type are reserved. If this parameter is omitted, then the comparison of either the Ethertype or IEEE 802.2 SAP for this rule is irrelevant.

Element ID	Length (bytes)	Value
20.10	3	type, eport1, eport2

#### 7.7.8.9.18.3.11 IEEE 802.1D User Priority field

The values of this field specify the matching parameters for the IEEE 802.1D user\_priority bits. An Ethernet packet with IEEE 802.1D user\_priority value “priority” matches these parameters if priority is greater than or equal to “pri-low” and priority is less than or equal to “pri-high”.

If this parameter is specified for an entry, then Ethernet packets without IEEE 802.1Q encapsulation shall not match this entry. If this parameter is specified for an entry on a CPE that does not support forwarding of IEEE 802.1Q encapsulated traffic, then this entry shall not be used for any traffic.

If this field is omitted, then the comparison of the IEEE 802.1D user-priority bits for this entry is irrelevant.

Element ID	Length (bytes)	Value
20.11	2	pri-low, pri-high Valid range: 0–7 for pri-low and pri-high

#### 7.7.8.9.18.3.12 IEEE 802.1Q VLAN ID Field

The value of this field specifies the matching value for the IEEE 802.1Q vlan\_id bits. Only the first (i.e., the leftmost) 12 bits of the specified vlan\_id field are significant; the final 4 bits shall be ignored for comparison.

If this parameter is specified for an entry, then Ethernet packets without IEEE 802.1Q encapsulation shall not match this entry. If this parameter is specified for an entry on a CPE that does not support forwarding of IEEE 802.1Q encapsulated traffic, then this entry shall not be used for any traffic.

If this field is omitted, then the comparison of the IEEE 802.1Q vlan\_id bits for this entry is irrelevant.

Element ID	Length (bytes)	Value
20.12	2	vlan_id1, vlan_id2

#### 7.7.8.9.18.3.13 Packet Classification Rule Index field

The Packet Classification Rule Index field identifies a packet classification rule. The packet classification rule index is unique per service flow.

Element ID	Length (bytes)	Value
20.13	2	Packet Classification Rule Index

#### 7.7.8.9.18.3.14 IPv6 Flow Label field

The value of this field specifies a matching value for the IPv6 Flow Label field. As the Flow Label field has a length of 20 bits, the first 4 bits of the most significant byte shall be set to 0x0 and disregarded.

Element ID	Length (bytes)	Value
20.14	3	Flow Label

#### 7.7.8.10 DSX-RVD

The DSX-RVD is used by the BS to indicate that it has received a DSx-REQ message from a CPE when a CPE initiates a DSx-REQ transaction. The BS uses this message to indicate to the CPE that it received the DSx-REQ message, but has not authenticated the DSx-REQ and had a chance to formulate a DSx-RSP.

**Table 102 — DSX-RVD message**

Syntax	Size	Notes
DSX-RVD_Message_Format() {		
Management Message Type = 16	8 bits	
Transaction ID	16 bits	
Confirmation code	8 bits	See Table 173.
}		

#### 7.7.9 Multicast Assignment Request (MCA-REQ)

The MCA-REQ message is sent to a CPE to assign it to or remove it from a multicast polling group. The format of the message is shown in Table 103.

**Table 103 — MCA-REQ message format**

Syntax	Size	Notes
MCA-REQ_Message_Format() {		
Management Message Type = 17	8 bits	
Transaction ID	16 bits	
Station ID	9	Station ID to represent a multicast group to which CPEs are being assigned.
Assignment	8	0x00: Leave multicast group 0x01: Join multicast group
Multicast group type	8	0x00: transport-only multicast flows, 0x01: management-only multicast flows, 0x02: polling-only multicast flows, 0x03: signaling SCW, 0x04: management & polling-only multicast flows, 0x05: signaling SCW as well as management and polling-only multicast flows, 0x06: transport/polling/management multicast flows, 0x07: transport, polling, multicast management flows, as well as signaling SCW 0x08–0xF: Reserved
Periodic allocation parameters	32	This field is only applicable when a CPE is being requested to join a multicast group and the Multicast Group Type is set to 0x02, 0x04, 0x05 or 0x06. Byte 0 (LS byte) = m Byte 1 = k Byte 2 = n Byte 3 = Reserved An upstream allocation is made available to CPEs (see 7.11.3.2) to send a Bandwidth Request at the end of the frame #N if: N mod k = m; size of allocation is n.
}		

### **7.7.10 Multicast Assignment Response (MCA-RSP)**

The MCA-RSP is sent by the CPE in response to a MCA-REQ. The message format shall be as shown in Table 104.

**Table 104 — MCA-RSP message format**

Syntax	Size	Notes
MCA-RSP_Message_Format() {		
Management Message Type = 18	8 bits	
Transaction ID	16 bits	
Confirmation code	8 bits	7.7.24
}		

### **7.7.11 CPE Basic Capability Request/Response (CBC-REQ/RSP)**

The motivation of basic capability negotiation is to facilitate effective communication between the BS and the CPE during the remainder of the initialization protocols, e.g., key exchange, registration. The following shows the CBC-REQ and CBC-RSP message formats, along with their information elements and the physical parameters involved.

#### **7.7.11.1 CBC-REQ**

The CPE CBC-REQ shall be transmitted by the CPE during initialization. A CPE shall generate CBC-REQ messages in the form shown in Table 105. Basic Capability Requests contain those CPE capabilities IEs that are necessary for effective communication with the CPE during the remainder of the initialization protocols. Only the following parameters shall be included in the Basic Capabilities Request (see 7.14.2.9), namely the Physical Parameters Supported and the Bandwidth Allocation Supported. Capabilities for Construction and Transmission of MAC PDUs may be supported if needed.

**Table 105 — CBC-REQ message format**

Syntax	Size	Notes
CBC-REQ_Message_Format() {		
Management Message Type = 19	8 bits	
Information elements (IEs)	Variable	See 7.7.11.3.1 and 7.7.11.3.2
}		

#### **7.7.11.2 CBC-RSP**

The CPE CBC-RSP shall be transmitted by the BS in response to a received CBC-REQ. The following parameters shall be included in the CBC-RSP if found in the CPE CBC-REQ, namely the Physical Parameters Supported (7.7.11.3.2) and the Capabilities for Construction and Transmission of MAC PDUs (7.7.11.3.1). In addition, the BS responds to the subset of CPE capabilities present in the CBC-REQ message. The BS responds to the CPE capabilities to indicate whether they may be used. If the BS does not recognize a CPE capability, it may return this as “off” in the CBC-RSP. Only capabilities set to “on” in the CBC-REQ may be set “on” in the CBC-RSP, as this is the handshake indicating that they have been successfully negotiated.

**Table 106 — CBC-RSP message format**

Syntax	Size	Notes
CBC-RSP Message Format() {		
Management Message Type = 20	8 bits	
Information elements (IEs)	Variable	See 7.7.11.3.1 and 7.7.11.3.2.
Confirmation code	8 bits	Code defining error status of basic capability configuration request (see 7.7.24)
}		

### 7.7.11.3 CBC-REQ/RSP information elements

The information elements include the following:

- 1) Capabilities for construction and transmission of MAC PDUs (see Table 107)
- 2) Physical parameters supported (see Table 108 , Table 109, and Table 110)

#### 7.7.11.3.1 Capabilities for of MAC PDUs

**Table 107 — Construction and transmission information element**

Element ID	Length (bytes)	Value	Scope
1	1	Bit 0: Ability to receive requests piggybacked with data Bits 1–7: Reserved (set to zero)	CBC-REQ, CBC-RSP

#### 7.7.11.3.2 Physical parameters supported

##### 7.7.11.3.2.1 Maximum CPE Transmit EIRP

The Maximum CPE Transmit EIRP information element indicates the maximum EIRP achievable at the CPE for the transmission of a full multiplex (60 subchannels) while still meeting the required RF mask (see 9.13) or other performance limits set by the manufacturer. The maximum EIRP parameters are reported in dBm and quantized in 0.5 dB steps ranging from –64 dBm (encoded 0x00) to 63.5 dBm (encoded 0xFF). Values outside this range shall be assigned the closest extreme. The EIRP accuracy shall be  $\pm 1.5$  dB when the level is at least 10 dB below the maximum regulatory power limit and  $\pm 0.5$  dB elsewhere.

**Table 108 — Maximum CPE Transmit EIRP information element**

Element ID	Length (bytes)	Value	Scope
2	1	Maximum CPE transmitted EIRP assuming all 60 subchannels are in use.	CBC-REQ

#### 7.7.11.3.2.2 PHY-specific parameters

##### 7.7.11.3.2.2.1 CPE Demodulator

This field indicates the different demodulator options supported by a CPE for the downstream reception. A bit value of 0 indicates “not supported” while 1 indicates “supported.”

**Table 109 — CPE Demodulator information element**

Element ID	Length (bytes)	Value	Scope
3	1	For a particular mode being represented, see the corresponding index in Table 27 (DIUC values)	CBC-REQ, CBC-RSP

#### 7.7.11.3.2.2.2 CPE Modulator

This field indicates the different modulator options supported by a CPE for upstream transmission. A bit value of 0 indicates “not supported” while 1 indicates “supported.”

**Table 110 — CPE Modulator information element**

Element ID	Length (bytes)	Value	Scope
4	1	For a particular mode being represented, see the corresponding index in Table 36 (UIUC values)	CBC-REQ, CBC-RSP

#### 7.7.11.3.3 Security parameters supported

These parameters are provided to negotiate some pre-authentication security parameters. These parameters may be renegotiated during the REG-REQ/RSP.

##### 7.7.11.3.3.1 SCM version support

This IE allows for negotiation of what version of the SCM protocol the BS and CPE support. Only one version of the SCM protocol may be employed at a given time.

**Table 111 — SCM version support**

Element ID	Length (bytes)	Value	Scope
5	1	0x00: SCM Version 1 (SCMv1) 0x01–0xFF: Reserved	CBC-REQ, CBC-RSP, REG-REQ, REG-RSP

##### 7.7.11.3.3.2 PN Window Size

This IE allows for negotiation of the size of the PN\_WINDOW (see 8.4).

**Table 112 — PN Window Size**

Element ID	Length (bytes)	Value	Scope
6	2	Size of the PN_WINDOW parameter (see 8.4).	CBC-REQ, CBC-RSP, REG-REQ, REG-RSP

##### 7.7.11.3.3.3 SCM Flow Control

This IE allows for negotiation of the maximum number of SCM transactions that can be ongoing.

**Table 113 — SCM Flow Control**

Element ID	Length (bytes)	Value	Scope
7	1	0: No Limit 1–255: Maximum number of ongoing SCM transactions	CBC-REQ, CBC-RSP, REG-REQ, REG-RSP

### 7.7.12 De/Re-Register Command (DREG-CMD)

The DREG-CMD message shall be transmitted by the BS on a CPE's Basic or Primary Management FID to force the CPE to change its access state. The BS may transmit the DREG-CMD unsolicited or in response to a CPE DREG-REQ message. Upon receiving a DREG-CMD, the CPE shall take the action indicated by the action code.

The format of the message is shown in Table 114.

**Table 114 — DREG-CMD message format**

Syntax	Size	Notes
DREG-CMD_Message_Format() {		
Management Message Type = 21	8 bits	
Action Code	8 bits	Table 115
Next Channel Number	8 bits	Corresponding to action codes 0 in Table 115 to indicate the channel that the CPE should tune to after de-registration.
}		

**Table 115 — Action codes**

Action Code	Action
0x00	CPE shall leave the current channel and attempt to access another channel.
0x01	CPE shall listen to the current channel but shall not transmit until a DREG-CMD with an Action Code that allows transmission is received.
0x02	CPE shall listen to the current channel but only transmit on the Basic, Primary Management, and Secondary Management Connections.
0x03	CPE shall return to normal operation and may transmit on any of its active connections.
0x04	CPE shall terminate current Normal Operations with the BS and shutdown. The BS shall transmit this action code in response to CPE DREG-REQ message or when directed to by a governing policy (see Table 234).
0x05	CPE forced to reset itself, reinitialize its MAC, and repeat initial system access on current operating channel. This message may be used if a CPE is unresponsive to the BS or if the BS detects continued abnormalities in the upstream transmission from the CPE.
0x06–0xFF	Reserved

### 7.7.13 CPE De-Registration Request (DREG-REQ)

A CPE may send a DREG-REQ message to a BS in order to notify the BS of CPE de-registration from Normal Operation service from the BS. The MAC Management Message Type for this message is given in Table 19. The format of the message is shown in Table 116.

**Table 116 — DREG-REQ message format**

Syntax	Size	Notes
DREG-REQ_Message_Format() {		
Management Message Type = 22	8 bits	
De-registration Request Code	8 bits	Action Codes are listed in Table 115.
Next channel number	8 bits	Channel that the CPE should tune to after de-registration resulting from actions codes 0x00 or 0x04 in Table 115.
}		

#### 7.7.14 ARQ-Feedback

A system supporting ARQ shall be able to receive and process the ARQ Feedback message.

The ARQ Feedback message, as shown in Table 117, can be used to signal any combination of different ARQ ACKs (cumulative, selective, selective with cumulative). The message shall be sent on the appropriate basic management connection.

**Table 117 — ARQ-Feedback message format**

Syntax	Size	Notes
ARQ_Feedback_Message_Format() {		
Management Message Type = 23	8 bits	
ARQ Feedback Payload	Variable	See 7.8.4.3.
}		

#### 7.7.15 ARQ-Discard

This message is applicable to ARQ-enabled connections only.

The transmitter sends this message when it wants to skip a certain number of ARQ blocks. The ARQ-Discard message shall be sent as a MAC management message on the basic management connection of the appropriate direction. Table 118 shows the format of the Discard message.

**Table 118 — ARQ-Discard message format**

Syntax	Size	Notes
ARQ_Discard_Message_Format() {		This message is sent when the transmitter wants to skip a certain number of ARQ blocks
Management Message Type = 24	8 bits	
Flow ID	3 bits	FID to which message refers
<i>Reserved</i>	5 bits	All bits shall be set to zero
BSN	10 bits	Sequence number of the last block in the transmitter window that the transmitter wants to discard
}		

#### 7.7.16 ARQ-Reset

This message is applicable to ARQ-enabled connections only.

The BS or the CPE may send this message. The message is used in a dialog to reset the parent connection's ARQ transmitter and receiver state machine. The ARQ Reset message shall be sent as a MAC management message on the basic management connection of the appropriate direction. Table 119 shows the format of the Reset message.

**Table 119 — ARQ-Reset message format**

Syntax	Size	Notes
ARQ_Reset_Message_Format() {		The transmitter or the receiver may send this message. The message is used in a dialog to reset the parent connection's ARQ transmitter and receiver state machines.
Management Message Type = 25	8 bits	
Flow ID	3 bits	FID to which the message refers
Type	2 bits	00 :Original message from Initiator 01: Acknowledgment from Responder 10: Confirmation from Initiator 11: Reserved
<i>Reserved</i>	2 bits	All bits shall be set to zero.
}		

### 7.7.17 Channel management

The MAC provides a comprehensive set of messages that allows the BS to dynamically manage the channel operations, and so support many essential features such as effective self-coexistence and measurements. This subclause presents the mandatory channel management messages supported by the MAC.

All channel management messages possess a Transaction ID field that uniquely identifies the message in an IEEE 802.22 network. If two or more management messages are received with the same Transaction ID, the parameters of the last message received shall override those of all previously received management messages with the same Transaction ID.

#### 7.7.17.1 Channel Switch Request (CHS-REQ)

This message (Table 120) is sent by the BS in order to switch the entire cell operation (BS and CPEs) to a different channel. Transmission of this message may result from various conditions such as protection of incumbent services or availability of larger number or better quality channel(s).

**Table 120 — CHS-REQ message format**

Syntax	Size	Notes
CHS-REQ Message Format() {		
Management Message Type = 26	8 bits	
Transaction ID	16 bits	
Confirmation Needed	1 bit	Indicates whether the CPE is required by the BS to confirm the receipt of this message. 0: No confirmation needed (default) 1: Confirmation needed
Switch Mode	1 bit	Indicates any restrictions on transmission until a channel switch. The BS shall set the Switch Mode field to either 0 or 1 on transmission. A value of 1 means that the CPE to which the frame containing the element is addressed shall transmit no further frames until the scheduled channel switch. A Channel Switch Mode set to 0 does not impose any requirement on the receiving CPE.
Switch Count	8 bits	This field either shall be set to the number of frames until the BS sending the Channel Switch message switches to the new channel or shall be set to 0. For example, a value of 1 indicates that the switch will occur immediately before the next frame. A value of 0 indicates that the switch will occur at any time after the frame containing the element is transmitted.
}		

### 7.7.17.2 Channel Switch Response (CHS-RSP)

This message (Table 121) is sent by the CPE in response to the receipt of a CHS-REQ. This message shall only be transmitted by the CPE if the Confirmation Needed field in the received CHS-REQ is set.

**Table 121 — CHS-RSP message format**

Syntax	Size	Notes
CHS-RSP_Message_Format() {		
Management Message Type = 27	8 bits	
Transaction ID	16 bits	
Confirmation code	8 bits	See 7.7.24.
}		

### 7.7.17.3 Channel Quiet Request (CHQ-REQ)

This CHQ-REQ message (Table 122) is sent by the BS in order to quiet any transmission activity in the channel currently used by the BS for communication with its associated CPEs. This message shall be used to configure quiet periods in non-coexistence situations. In self-coexistence mode, the quiet period scheduling shall be set in the SCH (see 7.5.1, Table 1) to synchronize the quiet periods across nearby WRAN cells operating on N and N±1.

**Table 122 — CHQ-REQ message format**

Syntax	Size	Notes
CHQ-REQ_Message_Format() {		
Management Message Type = 28	8 bits	
Transaction ID	16 bits	
Confirmation Needed	1 bit	Indicates whether the CPE is required by the BS to confirm the receipt of this message. 0: No confirmation needed (default) 1: Confirmation needed
Intra-frame Quiet Period Cycle Length	8 bits	Specified in number of superframes, it indicates the spacing between the superframes for which the intra-frame quiet period specification is valid. For example, if this field is set to 1, the Quiet Period Cycle repeats every superframe; if it is set to 2, the Quiet Period Cycle repeats every 2 superframes, etc. = 0, no intra-frame quiet period is scheduled or the current intra-frame quiet period is canceled.
Intra-frame Quiet Period Cycle Offset	8 bits	Valid only if intra-frame Sensing Cycle Length > 0. Used for in-band intra-frame sensing. Specified in number of superframes, it indicates the offset from this SCH transmission to the beginning of the first superframe in the current intra-frame sensing cycle.
Intra-frame Quiet Period Cycle Frame Bitmap	16 bits	Valid only if Intra-frame Quiet Period Cycle Length > 0. Valid for each superframe identified by the Intra-frame Quiet Period Cycle Length, each bit in the bitmap corresponds to one frame within the superframe. If the bit is set to 0, no intra-frame quiet period shall be scheduled in the corresponding frame. If the bit is set to 1, an intra-frame quiet period shall be scheduled within the corresponding frame for the duration specified by Intra-frame Quiet period Duration.
Intra-frame Quiet Period Duration	4 bits	Valid only if Intra-frame Quiet Period Cycle Length > 0. If this field is set to a value different from 0 (zero): it indicates the number of symbols starting from the end of the frame during which no transmission shall take place.

Syntax	Size	Notes
Inter-Frame Quiet Period Duration	4 bits	Used for in-band inter-frame sensing, it indicates the duration of the next scheduled quiet period. $> 0$ , it indicates the number of frames starting from Inter-frame Quiet Period Offset that shall be used to perform inter-frame sensing. $= 0$ , it cancels the next scheduled quiet period for inter-frame sensing or indicates that no inter-frame sensing are currently scheduled
Inter-Frame Quiet Period Offset	12 bits	Used for in-band inter-frame sensing, it indicates the time span between the transmission of this information and the next scheduled quiet period for inter-frame sensing. Bit 11–4: index the superframe number Bit 3–0: index the frame number when the next scheduled quiet period for inter-frame sensing will start.
<i>Reserved</i>	3 bits	All bits shall be set to zero.
}		

#### 7.7.17.4 Channel Quiet Response (CHQ-RSP)

This message (Table 123) is sent by the CPE in response to the receipt of a CHQ-REQ. This message shall only be transmitted by the CPE if the Confirmation Needed field in the received CHQ-REQ is set.

**Table 123 — CHQ-RSP message format**

Syntax	Size	Notes
CHQ-RSP Message Format() {		
Management Message Type = 29	8 bits	
Transaction ID	16 bits	See 7.7.24.
Confirmation code	8 bits	
}		

#### 7.7.17.5 Incumbent Prohibited Channels Update (IPC-UPD)

This IPC-UPD message (Table 124) is sent by the BS in order to inform CPEs of the channels upon which broadcast incumbent operation is prohibited and thus spectrum sensing is not needed (see A.5.5). This will allow the SSA to skip these channels during its in-band channel sensing process to clear N and  $N \pm 1$  and out-of-band sensing process to clear the backup/candidate channel list to shorten the sensing time at the CPE.

**Table 124 — IPC-UPD message format**

Syntax	Size	Notes
IPC-UPD Message Format() {		
Management Message Type = 30	8 bits	
Transaction ID	16 bits	
Number of Channels	8 bits	
for ( $i = 1; i \leq$ Number of Channels; $i++$ ) {		
Channel number	8 bits	
}		
}		

## 7.7.18 Measurements management

This subclause presents the mandatory measurements management component of the MAC, which is a critical component for many features of the protocol including incumbent system protection.<sup>11</sup>

The BS can transmit the Bulk Measurement request (BLM-REQ) management message (see 7.7.18.1) via unicast, multicast, or broadcast to one or multiple CPEs. This message contains instructions on the type of measurements to be performed, when to perform it, the measurement duration, which channels to be measured, and so on. Since the correct receipt of these management messages may be critical to the correct system behavior (especially for in-band measurements—see 7.19.1), the BS may require CPEs to acknowledge the receipt of BLM-REQ messages. This is done through Bulk Measurement response (BLM-RSP) messages, and these are covered in 7.7.18.2. Next, 7.7.18.3 deals with Bulk Measurement report (BLM-REP) messages that, as the name suggests, allows CPEs to report back to the BS all the measurement data they have collected as per requested by the BS in the corresponding BLM-REQ message.

### 7.7.18.1 Bulk Measurement request (BLM-REQ)

Table 125 illustrates the format of a BLM-REQ message. BLM-REQ messages can contain a multitude of single measurement messages (see Table 127). Each of these single measurement requests can be associated with a different type of measurement.

**Table 125 — BLM-REQ message format**

Syntax	Size	Notes
BLM-REQ Message Format() {		
Management Message Type = 31	8 bits	
Transaction ID	16 bits	Shall be set to a nonzero value chosen by the BS sending the measurement request to identify the request/report transaction.
Channel List	Variable	See Table 126
Confirmation Needed	1 bit	Indicates whether or not the CPE is required by the BS to confirm, with a BLM-RSP message, the receipt of this message. 0: No confirmation needed (default) 1: Confirmation needed
Number of Single Measurement Requests	3 bits	The number of single measurement requests contained in this message
Single Measurement Requests	Variable	A series of single measurement requests. See Table 127.
}		

**Table 126 — Channel list**

Syntax	Size	Notes
Channel List Format() {		
Number_of_Channels	8 bits	The number of channels in the current interval.
For ( $i=0; i < \text{Number\_of\_Channels}; i++$ ) {		
Channel Number [i]	8 bits	Channels contained in the list.
}		
}		

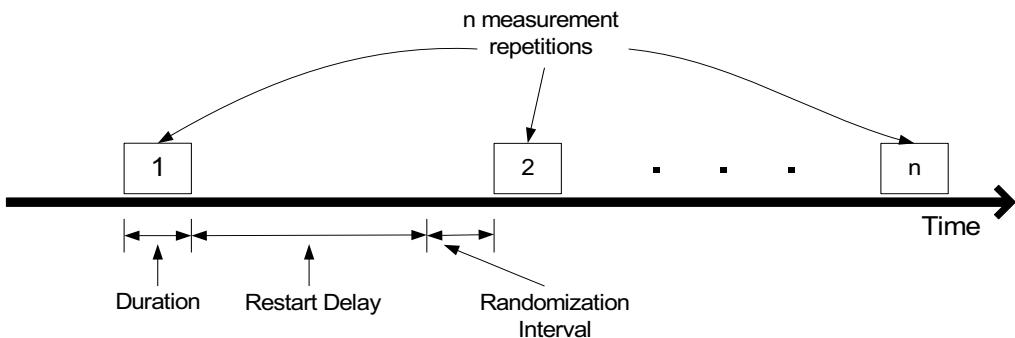
<sup>11</sup> The protocol for using the spectrum measurement messages is described in 10.4.

### 7.7.18.1.1 Single measurement request

Table 127 gives the format of single measurement requests, which are carried in the body of BLM-REQ management messages. These single measurement requests shall be of various types as shown in Table 131. Also, as seen from Table 127, various timing parameters are associated with measurement requests. Figure 16 depicts how these parameters are related to a measurement activity (the Randomization Interval and Duration parameters are introduced in the next subclauses).

**Table 127 — Single measurement request message format**

Syntax	Size	Notes
Single_Measurement_Request_Format() {		
Element ID	8 bits	Table 131
Length	8 bits	
Transaction ID	16 bits	
Number of Repetitions	8 bits	Contains the requested number of repetitions per channel for the periodic measurement request elements in this frame. A value of zero in the Number of Repetitions field indicates measurement request elements are executed only once.
Report Frequency	8 bits	This field indicates how often a CPE shall report measurements back to the BS 0: This field is not used to request a measurement report. That is, the CPE will report measurements either autonomously or whenever requested by the BS. 1: The CPE shall either report immediately to the BS (if this is in regards to an existing Transaction ID) or will report to the BS at the end of each repetition interval (in the case of a new Transaction ID). Note that in the case of an existing Transaction ID and Report Frequency == 1, the local information maintained by the CPE shall only be updated for this transaction if Number of Repetitions is not zero. 2–255: The CPE shall send a report to the BS at the end of every number of repetitions indicated by the code.
Restart Delay	16 bits	This field indicates the delay between two measurement repetitions. As shown in Table 128, the Measurement Period is divided into two subfields: Time Scale and Restart Delay. The Time Scale subfield defines the scale for the Restart Delay subfield as shown in Table 129. The subfield consists of a 15 bit unsigned integer number representing the fixed time delay between the completion of the last periodic measurement and the time when the measurement activity is restarted.
Request Mode	3 bits	Table 130
Request Element	Variable	Table 131
}		



**Figure 16 — Illustration of the timing parameters used in measurement requests**

**Table 128 — Repetition delay interval**

Bits: 1	15
Time Scale	Restart delay

**Table 129 — Time unit (TU) and time scale definitions**

Time Unit	Time Scale value
TU (see Table 199)	0
1000 TU	1

**Table 130 — Request mode**

Syntax	Size	Notes
Request_Mode_Format() {		
Parallel	1 bit	Indicates whether the measurement should start in series or in parallel with the measurement described by any immediately previous Measurement Request element in the same Measurement Request frame. A value of 0 shall mean that the measurement shall start after the previous measurement request has completed. A value of 1 shall mean the measurement shall start at the same time as the previous measurement. The Parallel bit shall be set to 0 in the first or only measurement request element in the frame.
Autonomous Report	1 bit	Indicates whether the CPE receiving the request shall enable or disable autonomous measurement reports for the measurements specified in this request. The Report bit shall be set to 1 when enabling autonomous measurement report. The Report bit shall be set to 0 when disabling an autonomous measurement report.
Duration Mandatory	1 bit	Indicates whether the measurement duration contained within the Measurement Request should be interpreted as mandatory by the CPE receiving the request. A value of 0 indicates that the duration is an upper bound and that the measurement can be done over a portion of this duration whereas 1 indicates that the CPE has to do the measurement over the entire specified duration.
}		

**Table 131 — Request information elements**

<b>Element ID (1 byte)</b>	<b>Length (bytes)</b>	<b>Description</b>
0	6	TV System Related Measurement Request—7.7.18.1.1.1
1	6	Wireless Microphone Related Measurement Request—7.7.18.1.1.1
2	10	Beacon (IEEE 802.22 BS and CPE Related) Measurement Request—7.7.18.1.1.2
3	1	Backup/candidate channel list clearance depth
4	2	Measurement Stop Request—7.7.18.1.1.3.
5	1	Status of CPE out-of-band sensing results—7.7.18.1.1.4
6	Variable	Location Data Request—7.7.18.1.1.5
7	10	IEEE 802.22.1 Beacon Measurement Request—7.7.18.1.1.2
8	2	Frequency response of active OFDM subcarriers at the CPE—7.7.18.1.1.6
9	2	Silent period FFT output—7.7.18.1.1.7
10–128		<i>Reserved</i>

### **7.7.18.1.1.1 Signal-Specific Measurement Request**

This refers to a particular incumbent signal specific measurement. Incumbent detection thresholds are specified during the registration procedure (see 7.7.7.3.4.7).

**Table 132 — Signal-Specific Measurement request message format**

<b>Syntax</b>	<b>Size</b>	<b>Notes</b>
Signal_Specific_Measurement_Request_Format() {		
Signal Type	5 bits	Table 237
Randomization Interval	16 bits	<p>It specifies the upper bound of the random delay that can be used by the CPE prior to making the measurement. It is specified in units of TU (see Table 129).</p> <p>This field can be used for out-of-band measurements in channels that are not occupied by any other WRANs, as in-band measurements as well as out-of-band measurements in channels occupied by WRANs are driven by quiet periods of the WRAN(s) operating in the corresponding channel.</p>
Duration	16 bits	Shall be set to the preferred duration of the requested measurement, expressed in TUs.
Sensing Mode	3 bits	<p>Specifies which SSF outputs are valid and in some cases it specifies the behavior of the SSF.</p> <p>000 – Sensing Mode 0 001 – Sensing Mode 1 010 – Sensing Mode 2 011 – Sensing Mode 3 (see definition of Sensing Modes in Table 239)</p>
Maximum Probability of False Alarm	8 bits	As defined in the SSF (10.4.1.3.1)
}		

### **7.7.18.1.1.2 Beacon Measurement Request**

**Table 133 — Beacon Measurement request message format**

<b>Syntax</b>	<b>Size</b>	<b>Notes</b>
Beacon_Measurement_Request_Format() {		
Randomization Interval	16 bits	This field only applies to out-of-band measurements,

Syntax	Size	Notes
		as in-band measurements are driven by quiet periods. It specifies the upper bound of the random delay that can be used by the CPE prior to making the measurement. It is specified in units of TU (see Table 129).
Duration	16 bits	Shall be set to the preferred duration of the requested measurement, expressed in TUs.
ID	48 bits	Specifies the ID (e.g., MAC ID) to listen to. Can be a broadcast ID or a specific CPE ID. (CBP burst ID or IEEE 802.22.1 beacon ID)
}		

#### 7.7.18.1.1.3 Measurement Stop Request

**Table 134 — Stop Measurement Request message format**

Syntax	Size	Notes
Stop_Measurement_Request_Format() {		
Stop Time	16 bits	Consists of an unsigned integer number representing the time at which the CPE shall stop conducting all measurements activities. The Stop Time field consists of a Time Scale subfield and a Stop Time subfield as shown in Table 135. The Time Scale subfield is defined in Table 129 and represents the time units for the integer in the Stop Time subfield.
}		

**Table 135 — Pause time field**

Bits: 1	15
Time Scale	Pause time

#### 7.7.18.1.1.4 Status of CPE out-of-band sensing results

**Table 136 — Status of out-of-band sensing results request message format**

Syntax	Size	Notes
Status_Measurement_Request_Format() {		
Number of channels	8 bits	Consists of an unsigned integer number representing the number of channels for which the out-of-band sensing results are requested.
}		

#### 7.7.18.1.1.5 Location Configuration Measurement Request

**Table 137 — Location data request message format**

Syntax	Size	Notes
Location_Data_Request_Format() {		
Length	16 bits	Length of the location data string in octets (0 to 4095 characters)
}		

#### 7.7.18.1.1.6 Measurement request for frequency response of active OFDM subcarriers at the CPE

**Table 138—Measurement request format for frequency response of active OFDM subcarriers at CPE**

Syntax	Size	Notes
Frequency response of active OFDM subcarriers at the CPE() {		1680 subcarriers mandatory, 2048 recommended
Measurement Frame	8 bits	Frame number (see Table 21) in which the channel measurement is scheduled
Measurement symbol	8 bits	Symbol number during which the measurement is to be made in the frame. This will likely be the frame preamble symbol for which the signature is known. Another measurement should be the status of the corrections for each carrier maintained and updated at the CPE to remove the channel response from the data at the output of the FFT and before the modulation detection. These carriers are to be updated with the pilot carrier information throughout the frame. This would be better and more stable than the preamble information because of the integration over time.
}		

#### 7.7.18.1.1.7 Silent period channel FFT output measurement request

**Table 139—Silent period FFT output measurement request format**

Syntax	Size	Notes
Frequency response of OFDM subcarriers at the CPE() {		
Measurement Frame	8 bits	Frame number (see Table 21) in which the channel measurement is scheduled
Measurement symbol	8 bits	Symbol number during which the measurement is to be made in the frame
}		

#### 7.7.18.2 Bulk Measurement response (BLM-RSP)

A BLM-RSP management message (shown in Table 140) is sent in response to a BLM-REQ and serves to confirm the receipt of the BLM-REQ message by the CPE. The need to send a BLM-RSP message is indicated by the BS in the corresponding BLM-REQ message, through the use of the Confirmation Needed field.

**Table 140—BLM-RSP message format**

Syntax	Size	Notes
BLM-RSP Message Format() {		
Management Message Type = 32	8 bits	
Transaction ID	16 bits	
Confirmation code	8 bits	7.7.24
}		

### 7.7.18.3 Bulk Measurement report (BLM-REP)

A BLM-REP management message (see Table 141) is sent from a CPE to a BS, and contains the measurement data collected by the CPE as per requested by the BS in a preceding BLM-REQ message. Unsolicited BLM-REP management messages can also be sent from a CPE to a BS for the purpose of signaling backup channels that are no longer available.

**Table 141 — BLM-REP message format**

Syntax	Size	Notes
BLM-REP Message Format() {		
Management Message Type = 33	8 bits	
Transaction ID	16 bits	
Number of Single Measurement Reports	8 bits	The number of single measurement reports contained in this message
Single Measurement Reports	Variable	7.7.18.3.1
}		

#### 7.7.18.3.1 Single Measurement Report

**Table 142 — Single measurement report message format**

Syntax	Size	Notes
Single_Measurement_Report_Format() {		
Element ID	8 bits	Table 143
Length	8 bits	
Transaction ID	16 bits	
Report Information element	Variable	Table 143
}		

**Table 143 — Report information elements**

Element ID (1 byte)	Length (bytes)	Description
129	10	TV Measurement Report—7.7.18.3.1.1
130	10	Wireless Microphone Measurement Report—7.7.18.3.1.1
131	Variable	Beacon (IEEE 802.22 related) Measurement Report—7.7.18.3.1.2
132	2	Unavailable backup channel—7.7.18.3.1.3
133	2	Backup channel list clearance depth—7.7.18.3.1.4
134	2	Backup/candidate channel list clearance depth—7.7.18.3.1.5
135	12	Status of CPE out-of-band sensing results—7.7.18.3.1.6
136	Variable	Location Data Report—7.7.18.3.1.7
137	Variable	IEEE 802.22.1 Beacon Measurement Report—7.7.18.3.1.8
138	Variable	Consolidated Spectrum Occupancy Measurement Report—7.7.18.3.1.9
139	3362	Frequency response of active OFDM subcarriers at the CPE—7.7.18.3.1.10 .
140	3362	Silent period FFT output Measurement Report, see 7.7.18.3.1.11.
141–255		Reserved

### 7.7.18.3.1.1 Signal-Specific Measurement Report

**Table 144 — Signal-Specific Measurement Report message format**

Syntax	Size	Notes
Signal_Specific_Measurement_Report_Format() {		
Signal Type	5 bits	Table 237
Report Mode	8 bits	Table 145
Start Frame	8 bits	Frame number (see Table 21) in which the channel measurement started
Duration	16 bits	The actual duration, in units of symbol period, of the measurement
Channel Number	8 bits	
Sensing Mode	3 bits	Specifies which SSF outputs are valid and in some cases it specifies the behavior of the SSF. 000: Sensing Mode 0 001: Sensing Mode 1 010: Sensing Mode 2 011–111: <i>Reserved</i> (see definition of Sensing Modes in Table 239)
Signal Present Output	1 bit	Indicates the decision from the CPE sensing function regarding the presence of the target signal in the channel measured: 0 – FALSE: Indicates the signal is NOT present in the channel (see 10.4.1.3) 1 – TRUE: Indicates the signal is present in the channel (see 10.4.1.3)
Confidence Metric	8 bits	This number indicates confidence level in the signal present decision reported in the Signal Present Output. A confidence metric varies between a minimum of zero (0x00) indicating no confidence in the signal present decision and a maximum of one (0xFF) indicating total confidence in the signal present decision.  If Sensing Mode =0, the confidence metric shall be set to zero (0x00).
RSSI	10 bits	Received signal strength indication (RSSI) (estimate) measured at the base station or CPE. This RSSI shall be measured in dBm and shall be normalized for a 0 dBi antenna gain and 0 dB coupling and cable loss (see definition in 10.4.1.3). The value will represent the estimated mean when reported for a number of measurements. Signed in units of dBm in 0.5 dB steps ranging from -104 dBm (encoded 0x00) to +23.5 dBm (encoded 0xFF). Values outside this range shall be assigned the closest extreme.
Standard Deviation	8 bits	The standard deviation of the RSSI estimated when reported for a number of measurements (see 0). Expressed in units of dB in 0.1 dB steps ranging from 0.0 dB (encoded 0x00) to +25.5 dB (encoded 0xFF). Values beyond +25.5 dB shall be encoded as 0xFF.
<i>Reserved</i>	5 bits	All bits shall be set to zero.
}		

**Table 145 — Report mode**

Syntax	Size	Notes
Report Mode Format() {		
Late	1 bit	Indicates whether this CPE is unable to carry out a measurement request because it received the request after the requested measurement time. The Late bit shall be set equal to 1 to indicate the request was too late. The Late bit shall be set to 0 to indicate the request was received in time for the measurement to be executed, or if no start time was specified.
Incapable	1 bit	Indicates whether this CPE is incapable of generating this report requested by the BS. The Incapable bit shall be set to 1 to indicate

Syntax	Size	Notes
		the CPE is incapable. The Incapable bit shall be set to 0 to indicate the CPE is capable or the report is autonomous.
Refused	1 bit	Indicates whether this CPE is refusing to generate this report requested by the BS. The Refused bit shall be set to 1 to indicate the CPE is refusing. The Refused bit shall be set to 0 to indicate the CPE is not refusing or the report is autonomous.
Unmeasured	1 bit	CPE did not measure the channel.
No_decision	1 bit	This bit shall be set to 1 to indicate the measurement was carried out but no decision was made (see 10.4.1.3).
<i>Reserved</i>	3 bits	All bits shall be set to zero.
}		

#### 7.7.18.3.1.2 Beacon Measurement report

A Beacon Measurement report (see Table 146) is sent from a CPE to its corresponding BS, and conveys information about one single overhead SCH (transmitted by other BSs) and/or CBP packet (transmitted by other CPEs).

**Table 146 — Beacon Measurement report message format**

Syntax	Size	Notes
Beacon_Measurement_Report_For mat() {		
Element ID	8 bits	131
Length	8 bits	Length in bytes.
Report Mode	5 bits	Table 145
<i>Reserved</i>	3 bits	All bits shall be set to zero.
Start Frame	8 bits	Table 144
Duration	16 bits	Table 144
Frame Number	8 bits	The frame number in which the beacon was received. See definition in Table 21.
Reception Offset	8 bits	Indicates the offset (in units of symbols) relative to the start of the first symbol of the PHY PDU (including preamble) frame where the beacon was received. The time instants indicated by the Reception Offset values are the reception times of the first symbol of the beacon including preamble (if present).
Channel Number	8 bits	
RCPI	8 bits	Received Carrier Power Indicator (in dBm)
Received CBP MAC PDU	Variable	See 7.6.1.3.1 and 7.20.1.2
}		

#### 7.7.18.3.1.3 Unavailable Backup Channel

This information element is transmitted by the CPE as an unsolicited BLM-RSP message to signal that a backup channel is no longer available after an incumbent has been detected in this backup channel or either of its adjacent channels. This unsolicited message is to be carried by a normal upstream bandwidth allocation assigned to the CPE in the US-MAP or, if not present, using the opportunistic BW Request mechanism to allow reporting to the BS as soon as possible.

**Table 147 — Unavailable Backup Channel report message format**

Syntax	Size	Notes
Backup channel list clearance depth Report Format() {		
Report Mode	8 bits	Table 145
Channel number	8 bits	Channel number for the channel that is found to be no longer available after an incumbent has been detected in this backup channel or either of its adjacent channels.
}		

**7.7.18.3.1.4 Backup channel list clearance depth**

This report is provided by the CPE upon request by the BS (Table 131). It can also be sent as an opportunistic message by the CPE when the backup channel list clearance depth becomes smaller than the number of backup channels indicated by the DCD IE10 in Table 21.

**Table 148 — Backup channel list clearance depth report message format**

Syntax	Size	Notes
Backup channel list clearance depth Report Format() {		
Report Mode	8 bits	Table 145
Clearance depth	8 bits	Number of backup channels that the CPE has had the time to verify for absence of incumbents during its idle time.
}		

**7.7.18.3.1.5 Backup/candidate channel list clearance depth**

This report is provided by the CPE upon request by the BS (Table 131).

**Table 149 — Backup/candidate channel list clearance depth report message format**

Syntax	Size	Notes
Backup/candidate channel list clearance depth Report Format() {		
Report Mode	8 bits	Table 145
Clearance depth	8 bits	Number of backup/candidate channels that the CPE has had the time to verify for absence of incumbents during its idle time.
}		

**7.7.18.3.1.6 Status of CPE out-of-band sensing results****Table 150 — Status of CPE out-of-band sensing results**

Syntax	Size	Notes
Status of CPE out-of-band sensing results Report Format() {		
Report Mode	8 bits	Table 145
for ( $i = 1; i \leq$ Number of Channels; $i++$ ) {		The order in which the channel results shall be presented will be in the order of the most recent sensed channel to the earliest one fitting in the list.
Channel number	8 bits	Transmission channel number.

Syntax	Size	Notes
Time since last sensing	16 bits	Time since last sensing in symbol periods
Time of last positive	24 bits	Time since the last detection of an incumbent in the channel in symbol periods
Sensing path RSSI	8 bits	Received signal strength indication at the RF sensor normalized for a 0 dBi antenna gain and 0 dB coupling and cable loss, signed in units of dBm in 0.5 dB steps, ranging from -104 dBm (encoded 0x00) to +23.5 dBm (encoded 0xFF). Values outside this range shall be assigned the closest extreme.
Data path RSSL	8 bits	Received signal level at the WRAN detector normalized for a 0 dBi antenna gain and 0 dB coupling and cable loss signed in units of dBm in 0.5 dB steps ranging from -104 dBm (encoded 0xFF) to +23.5 dBm (encoded 0xFF). Values outside this range shall be assigned the closest extreme.
Signal Type	8 bits	See Table 237
Sensing path RSSI during quiet period	8 bits	Received signal strength at the RF sensor normalized for a 0 dBi antenna gain and 0 dB coupling and cable loss, measured during WRAN systems quiet periods, signed in units of dBm in 0.5 dB steps, ranging from -104 dBm (encoded 0x00) to +23.5 dBm (encoded 0xFF). Values outside this range shall be assigned the closest extreme.
Signal type during quiet period	8 bits	See Table 237
}		
}		

#### 7.7.18.3.1.7 Location Data report

A Location Data report (see Table 151), includes a string of location data that the CPE has obtained from satellite. The report format shall be as described in NMEA 0183, and the length shall be the length of the NMEA 0183 ASCII string plus 3 octets.

**Table 151 — Location Data report message format**

Syntax	Size	Notes
Location_Data_Report_Format() {		
Element ID	8 bits	
Length	12 bits	Length of the location data string in octets (0 to 4095 characters)
Report Mode	8 bits	Table 145
Location Data String	Variable	NMEA 0183 ASCII string
}		

#### 7.7.18.3.1.8 IEEE 802.22.1 Beacon Measurement report

An IEEE 802.22.1 Beacon Measurement report (see Table 152) is transmitted from a CPE to its corresponding BS, and conveys information from the IEEE 802.22.1 beacon PPDU when it is acquired. This report shall not be sent if the CPE did not receive any IEEE 802.22.1 beacon (i.e., below the required minimum level, see Table 247). If an IEEE 802.22.1 beacon was received, the report should indicate the level of the received beacon signal at detection. In such case, the size of the beacon PPDU shall be indicated by a bitmap depending on which part of the PPDU could be properly decoded. See Annex D for more information on this feature.

**Table 152 — IEEE 802.22.1 beacon measurement report message format**

Syntax	Size	Notes
IEEE 802.22.1_Beacon_Measurement_Report_Format() {		
Element ID	8 bits	
Length	8 bits	
Report Mode	5 bits	Table 145
Start Frame	16 bits	Table 144
Duration	16 bits	Table 144
RSSI	8 bits	Received signal strength indication at the IEEE 802.22.1 beacon detector, signed in units of dBm in 0.5 dB steps, ranging from -104 dBm (encoded 0x00) to +23.5 dBm (encoded 0xFF). Values outside this range shall be assigned the closest extreme.
IEEE 802.22.1 Beacon_Payload_Bitmap	3 bits	000 :Sync Burst 001: PPDU MSF1 011: PPDU MSF1+MSF2 111: PPDU MSF1+MSF2+MSF3
IEEE 802.22.1 Beacon_Payload	Variable	The possible sizes for the payload are as follows: MSF1 (17 bytes) MSF1 + MSF2 (68 bytes) MSF1 + MSF2 + MSF3 (101 bytes) This field is not included if the Beacon_Payload_Bitmap field is set to 000 (Sync Burst).
}		

#### 7.7.18.3.1.9 Consolidated Spectrum Occupancy Measurement report

A Consolidated Spectrum Occupancy Measurement report (see Table 153) is sent from a CPE to its corresponding BS, and conveys a brief summary about the overall spectrum occupancy from the viewpoint of the CPE.

**Table 153 — Consolidated spectrum occupancy measurement report message format**

Syntax	Size	Notes
Consolidated_Spectrum_Occupancy_Measurement_Report_Format() {		
Start Frame	8 bits	Frame number (see Table 21) in which the channel measurement started
Duration	16 bits	The actual duration of the measurement
Starting Channel Number	8 bits	
Number of Channels	8 bits	
for ( $i = 1; i \leq$ Number of Channels; $i++$ ) {		
Channel State	3 bits	000: Unmeasured 001: Vacant 010: Occupied 011: Occupied by TV service 100: Occupied by wireless microphones 101: Occupied by IEEE 802.22 110–111: Reserved
}		
Padding bits	0–7 bits	Padding to octet alignment—set all bits to 0.
}		

### 7.7.18.3.1.10 Frequency response of the OFDM subcarriers measurement report

A frequency response of the OFDM subcarriers measurement report (see Table 154) is sent from a CPE to its corresponding BS, and conveys the I&Q values of each 1680 active subcarriers representing the state of the transmission channel (impulse response) in the frequency domain from the viewpoint of the CPE. These values represent the estimated transmission channel state values stored at each CPE and used to correct the received carrier phase and amplitude of each data subcarrier before demodulation.

**Table 154 — Frequency response of the OFDM message format**

Syntax	Size	Notes
Frequency response_of_OFDM_Report_Format() {		
Measurement Frame	8 bits	Frame number (see Table 21) in which the channel measurement is scheduled.
WRAN RF path RSSL	8 bits	Received signal strength at the WRAN detector normalized for a 0 dBi antenna gain and 0 dB coupling and cable loss, signed in units of dBm in 0.5 dB steps, ranging from -104 dBm (encoded 0x00) to +23.5 dBm (encoded 0xFF). Values outside this range shall be assigned the closest extreme.
for ( $i = 1; i \leq 1680; i++$ ) {		
I_Carrier State	8 bits	
Q_Carrier State	8 bits	
}		
}		

### 7.7.18.3.1.11 Silent period FFT output measurement report

A channel FFT output measurement report for the OFDM subcarriers during a silent period (see Table 155) is sent from a CPE to its corresponding BS, and conveys the I&Q values of each subcarrier representing the state of interference and noise in the transmission channel from the viewpoint of the CPE. These values represent the raw output of the FFT process done over one selected symbol at the CPE.

**Table 155 — Silent period FFT output message format**

Syntax	Size	Notes
Silent period FFT output_Report_Format() {		
Measurement Frame	8 bits	Frame number (see Table 21) in which the channel measurement is scheduled.
WRAN RF path RSSL	8 bits	Received signal strength at the WRAN detector normalized for a 0 dBi antenna gain and 0 dB coupling and cable loss, signed in units of dBm in 0.5 dB steps, ranging from -104 dBm (encoded 0x00) to +23.5 dBm (encoded 0xFF). Values outside this range shall be assigned the closest extreme.
for ( $i = 1; i \leq 1680; i++$ ) {		
I_Carrier State	8 bits	
Q_Carrier State	8 bits	
}		
}		

#### **7.7.18.4 Bulk Measurement Acknowledgement (BLM-ACK)**

A BLM-ACK management message (shown in Table 156) shall be sent from the BS to the CPE in response to a received BLM-REP. It serves to confirm to the CPE the reception of the BLM-REP message by the BS.

**Table 156 — BLM-ACK message format**

Syntax	Size	Notes
BLM-ACK Message Format() {		
Management Message Type = 34	8 bits	
Transaction ID	16 bits	
Confirmation code	8 bits	7.7.24
}		

#### **7.7.19 Config File TFTP Complete (TFTP-CPLT)**

The Config File TFTP-CPLT message shall be generated by the CPE whenever it has successfully retrieved its configuration file from the provisioning server (see 7.14). If the CPE does not need a config file, it shall send the TFTP-CPLT message to the BS anyway to indicate that it has completed secondary management connection initialization and is ready to accept services. The format of the TFTP-CPLT shall be as shown in Table 157.

**Table 157 — TFTP-CPLT message format**

Syntax	Size	Notes
TFTP-CPLT_Message_Format() {		The FID in the MAC header shall be set to the CPE's primary management FID
Management Message Type = 35	8 bits	
}		

#### **7.7.20 Config File TFTP Complete Response (TFTP-RSP)**

The Config File TFTP-RSP message shall be generated by the BS in response to a TFTP-CPLT message from the CPE (see 7.14). The format of the TFTP-RSP shall be as shown in Table 158.

**Table 158 — TFTP-RSP message format**

Syntax	Size	Notes
TFTP-RSP_Message_Format() {		The FID in the MAC header shall be set to the CPE's primary management FID
Management Message Type = 36	8 bits	
Response	8 bits	0: OK 1: Message authentication failure
}		

#### **7.7.21 Security Control Management (SCM) messages (SCM-REQ/RSP)**

SCM employs two MAC message types: SCM Request (SCM-REQ) and SCM Response (SCM-RSP), as described in Table 159.

**Table 159 — SCM MAC messages**

Type Value	Message name	Message description
37	SCM-REQ	Security Control Management Request [CPE → BS]
38	SCM-RSP	Security Control Management Response [BS → CPE]

These MAC management message types distinguish between SCM requests (CPE-to-BS) and SCM responses (BS-to-CPE). Each message encapsulates one SCM message in the Management Message Payload.

SCM protocol messages transmitted from the CPE to the BS shall use the form shown in Table 160. They are transmitted on the CPEs Primary Management Connection.

**Table 160 — SCM-REQ message format**

Syntax	Size	Notes
SCM-REQ Message Format() {		
Management Message Type = 41	8 bits	
Element ID	8 bits	Identifies the type of SCM packet. When a packet is received with an invalid Code, it shall be silently discarded. The code values are defined in Table 162.
Transaction ID	16 bits	<p>A CPE uses the identifier Transaction ID to match a BS response to the CPE's requests.</p> <p>The CPE shall increment (modulo 256) the Transaction ID field whenever it issues a new SCM message.</p> <p>A “new” message is an EAP Start, EAP Transfer, or Key Request that is not a retransmission being sent in response to a Timeout event. For retransmissions, the Transaction ID field shall remain unchanged.</p> <p>The Transaction ID field in a BS's SCM-RSP message shall match the Transaction ID field of the SCM-REQ message to which the BS is responding. The Transaction ID field in TEK Invalid messages, which are not sent in response to SCM-REQs, shall be set to zero.</p> <p>On reception of a SCM-RSP message, the CPE associates the message with a particular state machine (the Authentication state machine in the case of indication of EAP Success, or EAP Failure events; a particular TEK state machine in the case of Key Replies, Key Rejects, and TEK Invalids).</p> <p>A CPE shall keep track of the Transaction ID of its latest, pending authentication requests. The CPE shall discard any EAP Start or EAP Transfer messages with Transaction ID fields not matching that of the pending authentication requests.</p> <p>A CPE shall keep track of the Transaction IDs of its latest, pending Key Request for each SA. The CPE shall discard Key Reply and Key Reject messages with Transaction ID fields not matching those of the pending Key Request messages.</p>
Encoded Attributes	Variable	SCM attributes carry the specific authentication and key management data exchanged between client and server. Each SCM packet type has its own set of required and optional attributes. Unless explicitly stated, there are no requirements on the ordering of attributes within a SCM message. The end of the list of attributes is indicated by the <u>Length</u> field of the MAC PDU header.
}		

SCM protocol messages transmitted from the BS to the CPE shall use the form shown in Table 161. They are transmitted on the CPEs Primary Management Connection.

**Table 161 — SCM-RSP message format**

Syntax	Size	Notes
SCM- RSP Message Format() {		
Management Message Type = 42	8 bits	
Element ID	8 bits	Table 160
Transaction ID	16 bits	Table 160
Encoded Attributes	Variable	Table 160
}		

**Table 162 — SCM message codes**

Element ID	SCM message type	MAC Management Message Name
1	SCM EAP Start	SCM-REQ
2	SCM EAP Transfer	SCM-REQ/RSP
3	SCM Key-Request	SCM-REQ
4	SCM Key-Reply	SCM-RSP
5	SCM Key-Reject	SCM-RSP
6	SCM GSA-Add	SCM-RSP
7	SCM GSA-Remove	SCM-RSP
8	SCM TEK-Invalid	SCM-RSP
9–255	<i>Reserved</i>	

Formats for each of the SCM messages are described in the following subclauses.

#### 7.7.21.1 SCM EAP Start

SCM EAP Start shall be used during network entry to initiate an EAP session. The BS shall be capable of initiating an EAP session with EAP Start if the network authenticator does not. The “Key Sequence Number” attribute shall only be present in EAP Start messages transmitted during reauthentication. Note that during reauthentication, the EAP Start message shall be protected by the MMP key.

**Table 163 — SCM EAP Start-Message attributes**

Syntax	Size	Notes
Key Sequence Number	4 bits	AK Sequence Number

#### 7.7.21.2 SCM EAP Transfer

EAP Transfer shall be used when an EAP payload has to be transferred between the CPE and the network authenticator (through the BS). The EAP Payload attribute shall be present in all EAP Transfer messages. The “Key Sequence Number” attribute shall only be present in EAP Transfer messages during reauthentication. Note that during reauthentication, the EAP Start message shall be protected by the MMP key.

**Table 164 — SCM EAP Transfer-Message attributes**

Syntax	Size	Notes
Key Sequence Number	4 bits	AK Sequence Number
Length of EAP Payload	16 bits	Length of EAP Payload (in octets)
EAP Payload	Variable	Contains EAP authentication Data

#### 7.7.21.3 SCM Key-Request

A CPE sends a SCM Key-Request message to the BS to request new TEK and TEK-related parameters or GTEK and GTEK-related parameters for the multicast or broadcast service.

**Table 165 — SCM Key-Request attributes**

Syntax	Size	Notes
Key Sequence Number	4 bits	AK sequence number
SAID	16 bits	Security association identifier – GSAID for multicast or broadcast service
Group Key Indicator	1 bit	0: this key request is for a TEK 1: this key request is for a GTEK, only applicable if SAID refers to a GSA.
CPE Random	64 bits	A 64-bit random number generated in the CPE.

Once a CPE has completed authentication, it has keying material (MMP\_KEY) that can be used to sign and/or encrypt further MAC management messages. If SCM Key-Request is only to be signed, then CPE will use MMP\_KEY derived from the AK identified by AK Sequence Number in Key-Request will be used to generate the Ciphertext ICV (see 8.4.2.1.2). If SCM Key-Request is to be encrypted, then CPE will use the MMP\_KEY derived from the most current of its AKs to generate the Ciphertext ICV and encrypt the message (see 8.4.2.1.3).

#### 7.7.21.4 SCM Key-Reply

The BS responds to a CPE's SCM Key-Request message with a SCM Key-Reply message.

**Table 166 — SCM Key-Reply attributes**

Syntax	Size	Notes
Key Sequence Number	4 bits	AK sequence number
SAID	16 bits	Security association identifier—GSAID for multicast or broadcast service.
Older TEK/GTEK	128 bits	Older generation of TEK/GTEK relevant to SAID/GSAID.
Older TEK/GTEK Sequence Number	2 bits	Sequence Number for older generation of TEK/GTEK. This maps to the value to which the EKS field is set in GMH of PDU encrypted with this TEK/GTEK.
Remaining Lifetime for Older TEK/GTEK	24 bits	Remaining time for older TEK/GTEK in units of 10 ms frames.
Newer TEK/GTEK	128 bits	Newer generation TEK/GTEK relevant to SAID/GSAID.

Syntax	Size	Notes
New TEK/GTEK Sequence Number	2 bits	Sequence Number for newer generation of TEK/GTEK. This maps to the value to which the EKS field is set in GMH of PDU encrypted with this TEK/GTEK.
Remaining Lifetime for New TEK/GTEK	24 bits	Remaining time for new generation of TEK/GTEK in units of 10 ms frames.
CPE Random	64 bits	The same random number included in the SCM Key Request message.
BS Random	64 bits	Random number generated by the BS.

The GKEK-Parameters attribute is a compound attribute containing all of the GKEK-related parameters corresponding to a GSAID. This would include the GKEK, the GKEK's remaining key lifetime, and the GKEK's key sequence number.

Once the AAA has completed authentication with a particular CPE, both the CPE and BS have keying material (MMP\_KEY) that can be used to sign and/or encrypt further MAC management messages. If SCM Key-Reply is only to be signed, then BS will use MMP\_KEY derived from the AK identified by AK Sequence Number in Key-Reply will be used to generate the Ciphertext ICV (see 8.4.2.1.2). If SCM Key-Reply is to be encrypted, then BS will use the MMP\_KEY derived from the most current of its AK's to generate the Ciphertext ICV and encrypt the message (see 8.4.2.1.3).

GKEK parameters shall only be included in Key-Reply message, when responding to Key-Request that is conducted immediately after completion of Authentication exchange. To update GKEK parameters for an existing GSA, the BS shall add new GKEK parameters to the list of SA descriptors in an SA Add message.

#### 7.7.21.5 SCM Key-Reject

The BS responds to a CPE's SCM Key-Request message with a SCM Key-Reject message if the BS rejects the CPE's traffic keying material request.

Confirmation code is set to 0x0E when the Key Request was made for a SA for which the CPE is not currently authorized. Confirmation code is set to 0x0B when the Key Request message cannot be properly authenticated and decrypted.

**Table 167 — SCM Key-Reject attributes**

Syntax	Size	Notes
Key Sequence Number	4 bits	AK sequence number
SAID	16 bits	Security association identifier
Confirmation code	8 bits	Error code (see 7.7.24) identifying reason for rejection of the SCM Key-Request message
CPE Random	64 bits	A same random number included in the SCM Key Request message
BS Random	64 bits	Random number generated by the BS

Once a BS has completed authorization with a particular CPE, both have keying material (MMP\_KEY) that can be used to sign and/or encrypt further MAC management messages. If SCM Key-Reject is only to be signed, then BS will use MMP\_KEY derived from the AK identified by AK Sequence Number in Key-Reject will be used to generate the Ciphertext ICV (see 8.4.2.1.2). If SCM Key-Reject is to be encrypted, then BS will use the MMP\_KEY derived from the most current of its AK's to generate the Ciphertext ICV and encrypt the message (see 8.4.2.1.3).

#### 7.7.21.6 SCM GSA-Add

This message is sent by the BS to the CPE to establish one or more additional GSAs, after completion of the Authentication exchange. BS shall use this method to update material (e.g., GKEKs and associated parameters) for existing GSAs.

**Table 168 — SCM GSA-Add attributes**

Syntax	Size	Notes
Key Sequence Number	4 bits	AK sequence number
Multicast SID	9 bits	SID of multicast group
SAID	16 bits	SAID for GSA applied to the multicast group
Cryptographic Suite for GTEK application and transport	8 bits	Cryptographic suite that controls how GTEK is applied and transported to CPE. This can be either 0x03 or 0x04 (see Table 193).
Cryptographic Suite for GKEK/GTEK Generation	8 bits	Cryptographic suite that controls how GKEK is generated at BS. This can be either 0x06 or 0x07 (see Table 193).
GKEK	128 bits	GKEK for GSA used to protect GTEK when transported to CPE in Key-Reply. This field is protected with the KEK associated with the AK.
Remaining GKEK Lifetime	24 bits	Remaining lifetime in which GKEK can be used to protect GTEKs in SCM Key-Reply messages. In units of 10 ms frames.

Once the AAA has completed authentication with a particular CPE, both the CPE and BS have keying material (MMP\_KEY) that can be used to sign and/or encrypt further MAC management messages. If SCM GSA-Add is only to be signed, then BS will use MMP\_KEY derived from the AK identified by AK Sequence Number in GSA-Add will be used to generate the Ciphertext ICV (see 8.4.2.1.2). If SCM GSA-Add is to be encrypted, then BS will use the MMP\_KEY derived from the most current of its AKs to generate the Ciphertext ICV and encrypt the message (see 8.4.2.1.3). The format of the GSA Descriptor is described in 8.2.7.

#### 7.7.21.7 SCM GSA-Remove

This message is sent by the BS to the CPE to remove one or more additional GSAs. This message shall only be transmitted to CPEs after the BS has removed those CPEs from the multicast group to which the GSA was applied.

**Table 169 — SCM GSA-Remove attributes**

Syntax	Size	Notes
Number of SAID	8 bits	“N” Number of SAIDs for GSA (GSAIDs) that are to be removed
SAID(s)	N×16 bits	List of SAIDs for GSAs that are to be removed

#### 7.7.21.8 SCM TEK-Invalid

The BS sends a SCM TEK-Invalid message to a client CPE if the BS determines that the CPE encrypted an upstream PDU with an invalid TEK (i.e., an SAID’s TEK key sequence number), contained within the received packet’s MAC header, is out of the BS’s range of known, valid sequence numbers for that SAID.

Message Response Code is set to 0x02 when sending TEK Invalid message.

**Table 170 — SCM TEK-Invalid attributes**

Syntax	Size	Notes
Key Sequence Number	4 bits	AK sequence number
SAID	16 bits	Security association identifier
Confirmation code	8 bits	Error code (see 7.7.24) identifying reason for SCM TEK-Invalid message

Once the AAA has completed authentication with a particular CPE, both the CPE and BS have keying material (MMP\_KEY) that is used to sign and encrypt further MAC management messages. The SCM TEK-Invalid is to be encrypted, so the BS shall use the MMP\_KEY derived from the most current of its AKs to generate the Ciphertext ICV and encrypt the message (see 8.4.2.1.3).

### 7.7.22 Frame Allocation Management

In self-coexistence mode, multiple WRAN cells share the same channel by per frame-based access. The active frame allocation may change from one superframe to another. When the location of the first active frame is changed in the next superframe, the BS shall send the first active frame allocation update information within the present superframe to indicate all its associated CPEs.

**Table 171 — Frame Allocation Management**

Syntax	Size	Notes
FRM-UPD Message Format() {		
Management Message Type = 39	8 bits	
Transaction ID	16 bits	
Frame Index of the first frame allocated to the present cell in next superframe	4 bits	Indicate the frame index (0–15) of the first frame allocated in next superframe.
<i>Reserved</i>	4 bits	All bits shall be set to zero.
}		

### 7.7.23 CBP Relay message

This message is used by the BS to relay CBP MAC PDUs that it has formulated to a CPE or group of CPEs so that these CPEs can transmit the CBP burst in the next available (active) SCW. CBP MAC PDU generation and transmission is discussed in 7.20.1.2.

**Table 172 — CBP-RLY message format**

Syntax	Size	Notes
CBP -RLY Message Format() {		
Management Message Type = 40	8 bits	
CBP MAC PDU	Variable	A CBP MAC PDU formulated as per the process described in 7.20.1.2 and is made up by a combination of IEs that are listed in Table 9.
}		

### 7.7.24 Confirmation codes

The codes in Table 173 are used to set the status of responses in dynamic service configuration (DSx-RSP), security configuration (SCM-RSP), multicast group assignment (MCA-RSP), as well as basic (CBC-RSP) and registered (REG-RSP) capability configuration.

**Table 173 — Confirmation codes**

CC	Status
0x00	OK/success
0x01	reject-other
0x02	reject-unrecognized-configuration-setting
0x03	reject-temporary / reject-resource
0x04	reject-permanent / reject-admin
0x05	reject-not-owner
0x06	reject-service-flow-not-found
0x07	reject-service-flow-exists
0x08	reject-required-parameter-not-present
0x09	reject-header-suppression
0x0A	reject-unknown-transaction-id
0x0B	reject-authentication-failure
0x0C	reject-add-aborted
0x0D	reject-exceed-dynamic-service-limit
0x0E	reject-not-configured-for-the-request-SAID
0x0F	reject-fail-to-establish-the-requested-SA
0x10	reject-not-supported-parameter
0x11	reject-not-supported-parameter-value
0x12	reject-invalid-key-sequence-number
0x13–0xFF	Reserved

## 7.8 Management of MAC PDUs

### 7.8.1 Conventions

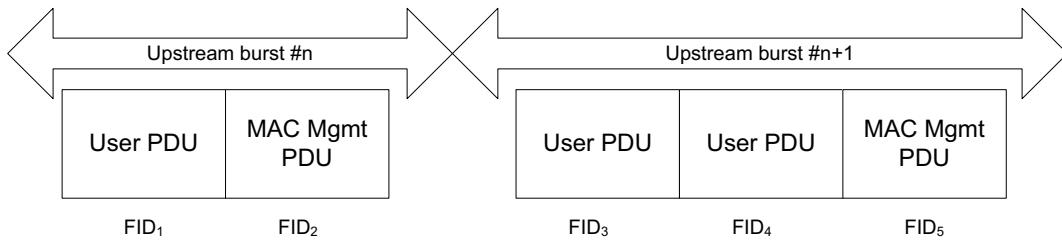
Data shall be transmitted in accordance with the following rules:

- a) Data fields of messages are transmitted in the same order as they appear in the corresponding tables and figures in this document.
- b) Data fields messages that are specified as binary numbers, are transmitted as a sequence of their binary digits, starting from MSB (here, bit masks are also considered numerical fields). For signed numbers, MSB is allocated for the sign. Length field in the “definite form” of ITU-T X.690 is also considered a numerical field.
- c) Data fields specified as SDUs or SDU fragments (e.g., MAC PDU payloads) are transmitted in the same order of bytes as received from upper layers.
- d) Data fields specified as strings are transmitted in the order of symbols in the string.

In item c) and item d), bits within a byte are transmitted in the order “MSB first.”

### 7.8.2 Concatenation

Multiple MAC PDUs may be concatenated into a single transmission in either the upstream or downstream directions, as depicted in Figure 17 for an upstream burst transmission. Each MAC PDU within that allocation is identified by a unique FID; the receiving MAC entity is able to present the MAC SDU (after reassembling the MAC SDU from one or more received MAC PDUs) to the correct instance of the MAC SAP. MAC PDUs containing management messages or user data may be concatenated into the same transmission.



**Figure 17 — Concatenation of MAC PDUs**

### 7.8.3 Fragmentation

Fragmentation and packing (discussed in 7.8.4) are mandatory features. Fragmentation is the process by which a MAC SDU is divided into one or more MAC PDUs. This process is undertaken to allow efficient use of available bandwidth relative to the QoS requirements of a connection's service flow. Upon the creation of a connection by the MAC SAP, fragmentation capability is defined. Fragmentation may be initiated by a BS for downstream connections and by a CPE for upstream connections. For ARQ-enabled connections, enabling of fragmentation is optional.

Fragments are tagged with their position in their parent SDU in accordance with Table 174.

**Table 174 — Fragmentation rules**

Fragment	Fragmentation Control
First fragment	10
Continuing fragment	11
Last fragment	01
Unfragmented	00

#### 7.8.3.1 Non-ARQ connections

For non-ARQ connections, fragments are transmitted once and in sequence. The sequence number assigned to each fragment allows the receiver to recreate the original payload and to detect the loss of any intermediate packets. A connection may be in only one fragmentation state at any given time.

Upon loss, the receiver shall discard all MAC PDUs on the connection until a new first fragment or a non-fragmented MAC PDU is detected.

#### 7.8.3.2 ARQ-Enabled connections

For ARQ-enabled connections, fragments are formed for each transmission by concatenating sets of ARQ blocks with adjacent sequence numbers (see 7.9). The BSN value carried in the fragmentation subheader is the BSN for the first ARQ block appearing in the segment (see Table 6).

### 7.8.4 Packing

In the MAC, the transmitting side has full discretion whether or not to pack a group of MAC SDUs into a single MAC PDU. BSs and CPEs shall both have the capability of unpacking. If packing is turned on for a connection, the MAC may pack multiple MAC SDUs into a single MAC PDU. Also, packing makes use of the connection attribute indicating whether the connection carries fixed-length or variable-length packets.

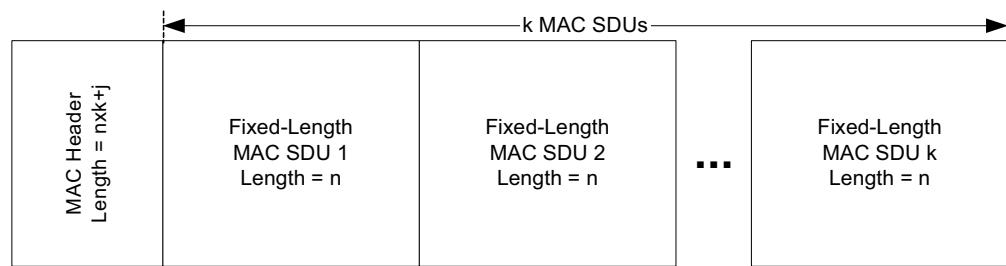
The construction of PDUs varies for ARQ and non-ARQ connections with respect to packing and fragmentation syntax. The packing and fragmentation mechanisms for both the ARQ and non-ARQ connections are specified in 7.8.4.1.

#### 7.8.4.1 Non-ARQ connections

For connections that do not utilize ARQ, the packing procedure described in 7.8.4.1.1 may be used when the connection carries fixed-length MAC SDUs. For all other non-ARQ connections, the variable-length packing algorithm described in 7.8.4.1.2 shall be employed. Please refer to 7.7.8.9.13 for more information on the indication whether a connection carries fixed-length or variable-length SDUs.

##### 7.8.4.1.1 Fixed-length MAC SDUs

For packing with fixed-length blocks, the Request/Transmission Policy (7.7.8.9.10) shall be set to allow packing and prohibit fragmentation, and the SDU size (7.7.8.9.14) shall be included in DSA-REQ message when establishing the connection. The length field of the MAC header implicitly indicates the number of MAC SDUs packed into a single MAC PDU. If the MAC SDU size is  $n$  bytes, the receiving side can unpack simply by knowing that the length field in the MAC header will be  $n \times k + j$ , where  $k$  is the number of MAC SDUs packed into the MAC PDU and  $j$  is the size of the MAC header and any appended MAC subheaders. A MAC PDU containing a packed sequence of fixed-length MAC SDUs would be constructed as in Figure 18. Note that there is no added overhead due to packing in the fixed-length MAC SDU case.

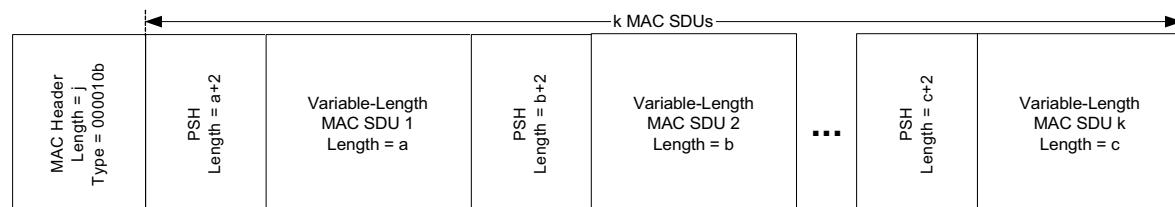


**Figure 18 — Packing fixed-length MAC SDUs into a single MAC PDU**

##### 7.8.4.1.2 Variable-length MAC SDUs

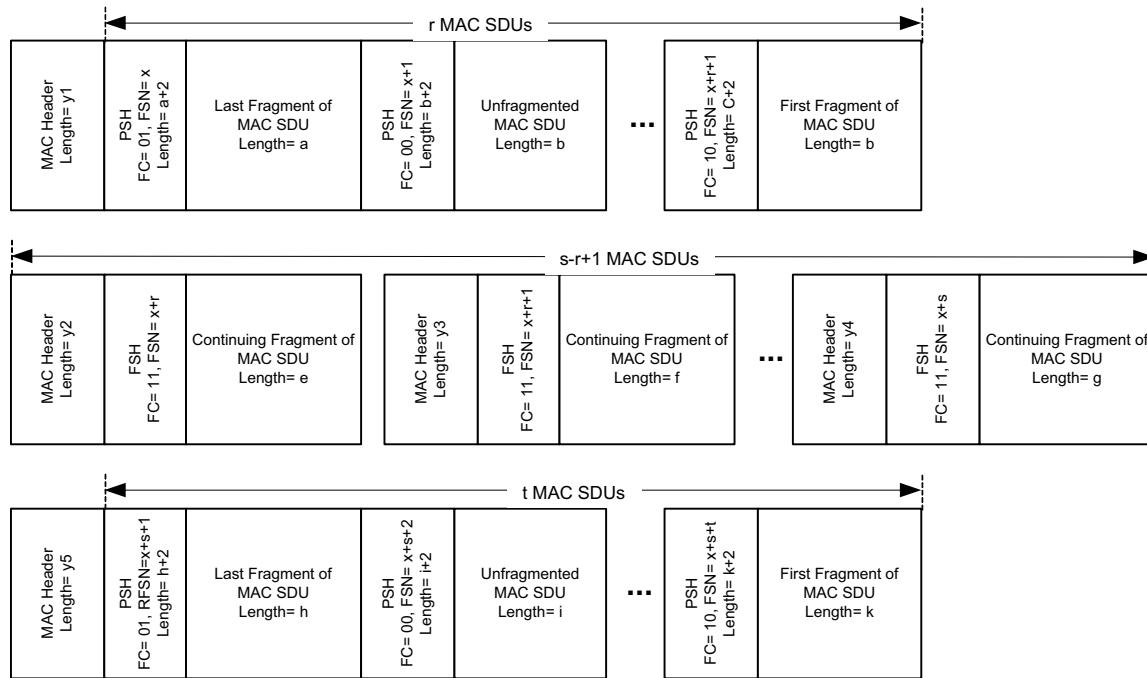
When packing variable-length SDU connections (e.g., IEEE 802.3/Ethernet), the  $n \times k + j$  relationship between the MAC header's length field and the higher-layer MAC SDUs no longer holds. Therefore, it is necessary to indicate where one MAC SDU ends and another begins. In the variable-length MAC SDU case, the MAC attaches a Packing subheader (PSH) to each MAC SDU. This subheader is described in 7.6.1.3.1.2.

A MAC PDU containing a packed sequence of variable-length MAC SDUs is constructed as shown in Figure 19. If more than one MAC SDU is packed into the MAC PDU, the type field in the MAC header indicates the presence of PSHs. Note that unfragmented MAC SDUs and MAC SDU fragments may both be present in the same MAC PDU (see Figure 20).



**Figure 19 — Packing variable-length MAC SDUs into a single MAC PDU**

Simultaneous fragmentation and packing allows efficient use of the wireless channel, but requires guidelines to be followed so it is clear which MAC SDU is currently in a state of fragmentation. To accomplish this, when a PSH is present, the fragmentation information for individual MAC SDUs or MAC SDU fragments is contained in the corresponding PSH. If no PSH is present, the fragmentation information for individual MAC SDU fragments is contained in the corresponding Fragmentation subheader (FSH). This procedure is shown in Figure 20.



**Figure 20 — Packing with fragmentation**

Finally, note that while it is acceptable to have continuation fragments packed with other fragments, the circumstances for creating continuation fragments would preclude this from happening.

#### 7.8.4.2 ARQ-enabled connections

The use of PSH for ARQ-enabled connections is similar to that for non-ARQ connections as described in 7.8.4.1.2, except that ARQ-enabled connections shall set the Extended Type bit (Table 4) in the generic MAC header to 1. The packing of variable-length MAC SDUs for the ARQ-enabled connections is similar to that of non-ARQ connections, when fragmentation is enabled. The BSN of the PSH shall be used by the ARQ protocol to identify and retransmit lost fragments.

For ARQ-enabled connections, when the type field indicates that PSHs are in use, fragmentation information for each individual MAC SDU or MAC SDU fragment is contained in the associated PSH. When the type field indicates that packing is not in use, fragmentation information for the MAC PDU's single payload (MAC SDU or MAC SDU fragment) is contained in the FSH appearing in the message. Figure 21 illustrates the use of FSH without packing.

Generic MAC Header	Other Subheaders	Fragmentation subheader	Payload (one SDU or fragment of an SDU)	CRC-32
--------------------	------------------	-------------------------	--	--------

**Figure 21 — Example of a MAC PDU with extended fragmentation subheader**

Figure 22 depicts the structure of a MAC PDU with ARQ PSHs. Each of the packed MAC SDU or MAC SDU fragments or ARQ feedback payload requires its own PSH, and some of them may be transmissions while others are retransmissions.

A MAC SDU may be partitioned into multiple fragments that are then packed into the same MAC PDU for the first transmission. MAC PDUs may have fragments from the same or different SDUs, including a mix of first transmissions and retransmissions. The 10-bit BSN and 2-bit FC fields uniquely identify each fragment or non-fragmented SDU.

Generic MAC Header	Grant Management Subheader (US only)	Packing subheader	Payload (one SDU or SDU fragment or a set of ARQ Feedback IEs)	...	Packing subheader	Payload (one SDU or SDU fragment)	CRC-32
--------------------	--------------------------------------	-------------------	---	-----	-------------------	--------------------------------------	--------

**Figure 22 — Example of a MAC PDU with ARQ packing subheader**

#### 7.8.4.3 ARQ Feedback IEs

The ARQ Feedback Payload (see Table 175) may be sent on an ARQ or non-ARQ connection, and consists of one or more ARQ Feedback IEs (see 7.9). However, policies based on implementation and/or QoS constraints may restrict the use of certain connections for transporting ARQ Feedback Payload. The ARQ Feedback Payload is treated like any other payload (SDU or fragments) from the packing perspective, except that only one ARQ Feedback Payload shall be present within a single MAC PDU.

The presence of an ARQ Feedback Payload in a MAC PDU is indicated by the value of the ARQ Feedback Payload bit in the Type field (see Table 4) in the generic MAC header. When present, the first packed payload shall be the ARQ Feedback Payload. The PSH preceding the ARQ Feedback Payload indicates the total length of the payload including the PSH and all ARQ Feedback IEs within the payload. The FSN/BSN field of the PSH shall be ignored for the ARQ Feedback Payload and the FC bits shall be set to 00.

**Table 175 — ARQ Feedback Message format**

Syntax	Size	Notes
ARQ_Feedback_Payload_Format() {		
do		
ARQ_Feedback_IE(last)	Variable	Include as many as needed until last == TRUE. See 7.9.
until(last)		
}		

#### 7.8.5 CRC calculation

CRC shall be calculated as defined in IEEE Std 802.3. The CRC shall be appended to the payload of the MAC PDU containing MAC management messages sent before the completion of authentication and to data PDUs that are mapped to the Secondary SA (e.g., only protected by encryption). MAC PDUs that do not contain a payload may choose not to use CRC and be unprotected. MAC PDUs that contain a payload and are either mapped to the Primary SA (e.g., to be signed and/or encrypted) or MAC management messages sent after the completion of authentication shall not have a CRC appended to them. The CRC

shall cover the MAC header and the Payload of the MAC PDU. In addition, the CRC shall be calculated after encryption, that is, it protects both the header and the ciphered Payload.

### 7.8.6 Padding

Allocated space within a data burst that is unused shall be initialized to a known state. This shall be accomplished by setting each unused byte to the stuff byte value (0x00).

Furthermore, only some specific PPDU lengths shall be permitted to fill some specific integer numbers of OFDM slots depending on the modulation and forward error coding selected (see 9.7). Such specific lengths shall be realized by adding the necessary padding bytes, all set to zero, at the end of the MAC PPDU, i.e., following the CRC so that the total length of the packet [i.e., MAC Header (4 bytes), MAC Payload (variable), the CRC (4 bytes), and the padding bytes] adds up to one of these specific lengths that, once the forward error coding overhead is included, will result in one of the specified integer numbers of OFDM slots depending on the modulation and channel coding selected for the PPDU.

## 7.9 ARQ mechanism

When implemented, ARQ may be enabled on a per-connection basis. The per-connection ARQ shall be specified and negotiated during connection creation. A connection cannot have a mixture of ARQ and non-ARQ traffic. Similar to other properties of the MAC protocol, the scope of a specific instance of ARQ is limited to one unidirectional connection. When the ARQ mechanism is not implemented in a CPE, the CPE will need to respond to a BS request for a FID with ARQ support with the confirmation code “reject-not-supported-parameter,” as indicated in 7.7.24.

For ARQ-enabled connections, enabling of fragmentation is optional. When fragmentation is enabled, the transmitter may partition each SDU into fragments for separate transmission based on the value of the ARQ\_BLOCK\_SIZE parameter. When fragmentation is not enabled, the connection shall be managed as if fragmentation was enabled. In this case, regardless of the negotiated block size, each fragment formed for transmission shall contain all the blocks of data associated with the parent SDU.

The ARQ feedback information can be sent as a standalone MAC management message on the appropriate basic management connection, or it can be piggybacked on an existing connection. ARQ feedback cannot be fragmented.

### 7.9.1 ARQ block usage

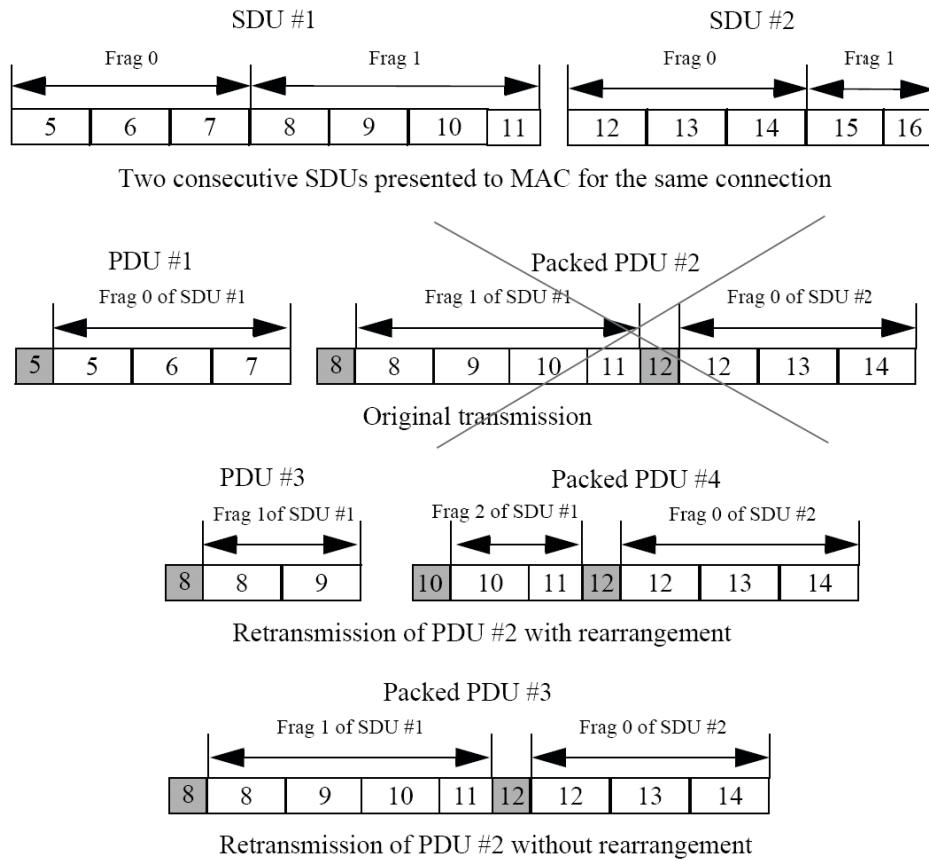
A MSDU is logically partitioned into blocks whose length is specified by the connection TLV parameter ARQ\_BLOCK\_SIZE. When the length of the SDU is not an integer multiple of the connection’s block size, the final block of the SDU is formed using the SDU bytes remaining after the final full block has been determined.

Once an SDU is partitioned into a set of blocks, that partitioning remains in effect until all blocks of the SDU are successfully delivered to the receiver, or the SDU is discarded by the transmitter state machine.

Sets of blocks selected for transmission or retransmission are encapsulated into a PDU. A PDU may contain blocks that are transmitted for the first time as well as those being retransmitted. Fragmentation shall occur only on ARQ block boundaries. If a PDU is not packed, all the blocks in that PDU shall have contiguous block numbers. When a PDU is packed, the sequence of blocks immediately between MAC subheaders and the sequence of blocks after the last PSH shall have contiguous block numbers.

If ARQ is enabled at the connection, FSH and PSH contain a BSN, which is the sequence number of the first ARQ block in the sequence of blocks following the subheader. It is a matter of transmitter policy

whether a set of blocks once transmitted as a single PDU should be retransmitted also as a single PDU. Figure 23 illustrates the use of blocks for ARQ transmissions and retransmissions; two options for retransmission are presented—with and without rearrangements of blocks.



**Figure 23 — Block usage examples for ARQ with and without rearrangement**

### 7.9.2 ARQ Feedback IE format

Table 176 defines the ARQ Feedback IE used by the receiver to signal positive or negative acknowledgments. A set of IEs of this format may be transported either as a packed payload (“piggybacked”) within a packed MPDU or as a payload of a standalone MPDU.

**Table 176 — ARQ Feedback IE format**

Syntax	Size	Notes
ARQ feedback IE (LAST) {		
FID	3 bits	The FID of the connection being referenced
LAST	1 bit	0: More ARQ feedback IE in the list 1: Last ARQ feedback IE in the list
ACK Type	2 bits	0x0: Selective ACK entry 0x1: Cumulative ACK entry 0x2: Cumulative with Selective ACK entry 0x3: Cumulative ACK with Block Sequence ACK entry
BSN	10	

Syntax	Size	Notes
	bits	
Number of ACK Maps	2 bits	If ACK Type == 01, the field is reserved and set to 00. Otherwise the field indicates the number of ACK maps: 0x0: 1, 0x1: 2, 0x2: 3, 0x3: 4
if(ACK Type!=01) {		
for (i=0; i< Number of ACK Maps +1; i++) {		
if(ACK Type!=3) {		
Selective ACK MAP	16 bits	
}		
else {		Start of Block Sequence ACK Map definition (16 bits)
Sequence Format	1 bit	Number of block sequences associated with descriptor 0: 2 block sequences, 1: 3 block sequences
if(Sequence Format = 0) {		
Sequence ACK MAP	2 bits	
Sequence 1 Length	6 bits	
Sequence 2 Length	6 bits	
Reserved	1 bit	
}		
else {		
Sequence ACK Map	3 bits	
Sequence 1 Length	4 bits	
Sequence 2 Length	4 bits	
Sequence 3 Length	4 bits	
}		
}		
}		
}		
}		

The following parameters in the ARQ Feedback IE are defined as follows:

### BSN

If (ACK Type == 0x0): BSN value corresponds to the MSB of the first 16-bit ARQ ACK map and follows an MSB first approach with the BSN incremented by 1 for each bit in the ARQ ACK map, following through for the subsequent ARQ ACK maps.

If (ACK Type == 0x1): BSN value indicates that its corresponding block and all blocks with lesser (see 6.3.4.6.1) values within the transmission window have been successfully received.

If (ACK Type == 0x2): Combines the functionality of types 0x0 and 0x1. If (ACK Type == 0x3): Combines the functionality of type 0x1 with the ability to acknowledge reception of ARQ blocks in terms of block sequences. A block sequence is defined as a set of ARQ blocks with consecutive BSN values. With this option, members of block sequences are identified and associated with the same reception status indication.

### Selective ACK Map

Each bit set to one indicates the corresponding ARQ block has been received without errors. The bit corresponding to the BSN value in the IE is the MSB of the first map entry. The bits for succeeding block numbers are assigned left-to-right (MSB to LSB) within the map entry. If the ACK Type is 0x2, then the MSB of the first map entry shall be set to one and the IE shall be interpreted as a cumulative ACK for the BSN value in the IE. The rest of the bitmap shall be interpreted similar to ACK Type 0x0.

**Sequence ACK Map**

Each bit set to one indicates the corresponding block sequence has been received without error. The MSB of the field corresponds to the first sequence length field in the descriptor. The bits for succeeding length fields are assigned left-to-right within the map entry.

Since the block sequence described by the first descriptor of the first map entry of the IE corresponds to the sequence of blocks immediately after the Cumulative ACK, the ACK map bit for this sequence shall be zero indicating this sequence has not yet been received.

**Sequence Length:** This value indicates the number of blocks that are members of the associated sequence. The BSN of the first block of the block sequence described by the first descriptor of the first IE map entry is the value of the Cumulative ACK plus one. The BSN of the first block of each block sequence is determined by adding the BSN of the first block of the previous block sequence to the length of that sequence. Within a map entry, Sequence Map/Length ordering follows the rule specified in the definition of Sequence ACK Map. Across map entries, ordering moves from the first map entry ( $i = 0$ ) to the last map entry ( $i = \text{Number of ACK Maps}$ ).

**7.9.3 ARQ state machine parameters****7.9.3.1 ARQ\_BSN\_MODULUS**

ARQ\_BSN\_MODULUS is equal to the number of unique BSN values, i.e.,  $2^{10}$ .

**7.9.3.2 ARQ\_WINDOW\_SIZE**

ARQ\_WINDOW\_SIZE is the maximum number of unacknowledged ARQ blocks at any given time. An ARQ block is unacknowledged if it has been transmitted but no acknowledgment has been received.

ARQ\_WINDOW\_SIZE shall be less than or equal to half of the ARQ\_BSN\_MODULUS.

**7.9.3.3 ARQ\_BLOCK\_LIFETIME**

ARQ\_BLOCK\_LIFETIME is the maximum time interval an ARQ block shall be managed by the transmitter ARQ state machine, once initial transmission of the block has occurred. If transmission (or subsequent retransmission) of the block is not acknowledged by the receiver before the time limit is reached, the block is discarded.

**7.9.3.4 ARQ\_RETRY\_TIMEOUT**

ARQ\_RETRY\_TIMEOUT is the minimum time interval a transmitter shall wait before retransmission of an unacknowledged block for retransmission. The interval begins when the ARQ block was last transmitted. This interval shall be used to compensate for delays on both transmitter and receiver side. On the transmitter side, this includes time to transmit MAC PDUs and ARQ blocks. On the receiver side, this includes the amount of time to receive and process MAC PDUs as well as transmit ARQ feedback. The transmitter-side and receiver-side delays are distinguished in Table 105, distinctly. These delays may include scheduling and propagation when the BS is the transmitter or the receiver. An ARQ block is unacknowledged if it has been transmitted but no acknowledgment has been received.

### 7.9.3.5 ARQ\_SYNC\_LOSS\_TIMEOUT

ARQ\_SYNC\_LOSS\_TIMEOUT is the maximum time interval ARQ\_TX\_WINDOW\_START or ARQ\_RX\_WINDOW\_START shall be allowed to remain at the same value before declaring a loss of synchronization of the sender and receiver state machines when data transfer is known to be active. The ARQ receiver and transmitter state machines manage independent timers. Each has its own criteria for determining when data transfer is “active” (see 7.9.6.2 and 7.9.6.3).

### 7.9.3.6 ARQ\_PURGE\_TIMEOUT

ARQ\_RX\_PURGE\_TIMEOUT is the time interval the receiver shall wait after successful reception of a block that does not result in advancement of ARQ\_RX\_WINDOW\_START, before advancing ARQ\_RX\_WINDOW\_START (see 7.9.6.3).

### 7.9.3.7 ARQ\_BLOCK\_SIZE

ARQ\_BLOCK\_SIZE is the length used for partitioning an SDU into a sequence of ARQ blocks prior to transmission (see 7.8.4.1).

## 7.9.4 ARQ procedures

### 7.9.4.1 ARQ state machine variables

All ARQ state machine variables are set to 0 at connection creation or by an ARQ reset operation.

#### 7.9.4.1.1 Transmitter variables

ARQ\_TX\_WINDOW\_START: All BSN up to (ARQ\_TX\_WINDOW\_START – 1) have been acknowledged.

ARQ\_TX\_NEXT\_BSN: BSN of the next block to send. This value shall reside in the interval ARQ\_TX\_WINDOW\_START to (ARQ\_TX\_WINDOW\_START + ARQ\_WINDOW\_SIZE), inclusive.

#### 7.9.4.1.2 Receiver variables

ARQ\_RX\_WINDOW\_START: All BSN up to (ARQ\_RX\_WINDOW\_START – 1) have been correctly received.

ARQ\_RX\_HIGHEST\_BSN: BSN of the highest block received, plus one. This value shall reside in the interval ARQ\_RX\_WINDOW\_START to (ARQ\_RX\_WINDOW\_START + ARQ\_WINDOW\_SIZE), inclusive.

## 7.9.5 ARQ-enabled connection setup and negotiation

Connections are set up and defined dynamically through the DSA/DSC class of messages. CRC-32 shall be used for error detection of PDUs for ARQ-enabled connections that carry data PDUs mapped to the Secondary SA and MAC management messages transmitted before authentication is complete. Data PDUs mapped to the Primary SA and that contain MAC management messages sent after the completion of authentication shall rely on the verification of the Ciphertext ICV (see 8.2.4) to determine if an ARQ retransmission is necessary. All the ARQ parameters (see 7.9.3) shall be set when an ARQ-enabled

connection is set up. The transmitter and receiver variables (defined in 7.9.4.1) shall be reset on connection setup.

## 7.9.6 ARQ operation

### 7.9.6.1 Sequence number comparison

Transmitter and receiver state machine operations include comparing BSNs and taking actions based on which is larger or smaller. In this context, it is not possible to compare the numeric sequence number values directly to make this determination. Instead, the comparison shall be made by normalizing the values relative to the appropriate state machine base value and the maximum value of sequence numbers, ARQ\_BSN\_MODULUS, and then comparing the normalized values. Normalization is accomplished by using the following equation.

$$\text{bsn}' = (\text{bsn} - \text{BSN\_base}) \bmod \text{ARQ\_BSN\_MODULUS}$$

The base values for the receiver and transmitter state machines are ARQ\_TX\_WINDOW\_START and ARQ\_RX\_WINDOW\_START, respectively.

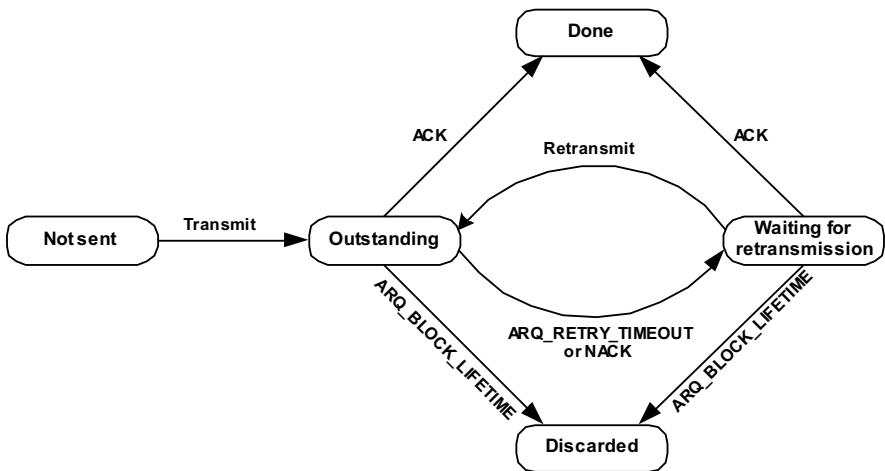
### 7.9.6.2 Transmitter state machine

An ARQ block may be in one of the following four states—not-sent, outstanding, discarded, and waiting-for-retransmission. Any ARQ block begins as not-sent. After it is sent it becomes outstanding for a period of time termed ARQ\_RETRY\_TIMEOUT. While a block is in outstanding state, it is either acknowledged and discarded, or it transitions to waiting-for-retransmission after ARQ\_RETRY\_TIMEOUT or NACK. An ARQ block can become waiting-for-retransmission before the ARQ\_RETRY\_TIMEOUT period expires if it is negatively acknowledged. An ARQ block may also change from “waiting-for-retransmission” to “discarded” when an ACK message is received for it or after a timeout ARQ\_BLOCK\_LIFETIME.

For a given connection the transmitter shall first handle (transmit or discard) blocks in “waiting-for-retransmission” state and only then blocks in “notsent” state. Blocks in “outstanding” or “discarded” state shall not be transmitted. When blocks are retransmitted, the block with the lowest BSN shall be retransmitted first.

The ARQ Tx block state sequence is shown in Figure 24.

MPDU formation continues with a connection’s “not-sent” MSDUs. The transmitter builds each MPDU using the rules for fragmentation and packing as long as the number of blocks to be sent plus the number of block already transmitted and awaiting retransmission does not exceed the limit imposed by ARQ\_WINDOW\_SIZE. As each “not-sent” block is formed and included in a MPDU, it is assigned the current value of ARQ\_TX\_NEXT\_BSN, which is then incremented.



**Figure 24 — ARQ Tx block states**

When an acknowledgment is received, the transmitter shall check the validity of the BSN. A valid BSN is one in the interval ARQ\_TX\_WINDOW\_START to ARQ\_TX\_NEXT\_BSN – 1 (inclusive). If BSN is not valid, the transmitter shall ignore the acknowledgment.

When a cumulative acknowledgment with a valid BSN is received, the transmitter shall consider all blocks in the interval ARQ\_TX\_WINDOW\_START to BSN (inclusive) as acknowledged and set ARQ\_TX\_WINDOW\_START to BSN + 1.

When a selective acknowledgment is received, the transmitter shall consider as acknowledged all blocks so indicated by the entries in the bitmap for valid BSN values. As the bitmap entries are processed in increasing BSN order, ARQ\_TX\_WINDOW\_START shall be incremented each time the BSN of an acknowledged block is equal to the value of ARQ\_TX\_WINDOW\_START.

When ARQ\_TX\_WINDOW\_START has been advanced by either of the above methods and acknowledgment of reception has already been received for the block with the BSN value now assigned to ARQ\_TX\_WINDOW\_START, the value of ARQ\_TX\_WINDOW\_START shall be incremented until a BSN value is reached for which no acknowledgment has been received.

A bitmap entry not indicating acknowledgement shall be considered a NACK for the corresponding blocks.

Selective ACK bit-maps are referenced to a specific BSN, which indicates to absolute number of the block referenced by the first bit in the bit-map. It is the responsibility of the ARQ feedback sender to assign the BSN so that all bits in the bit-map define either ACK or NAK for a specific ARQ block. This can be achieved by assigning the BSN low enough (modulo  $2^{10}$ ) so that every bit in the bit map provides correct feedback information.

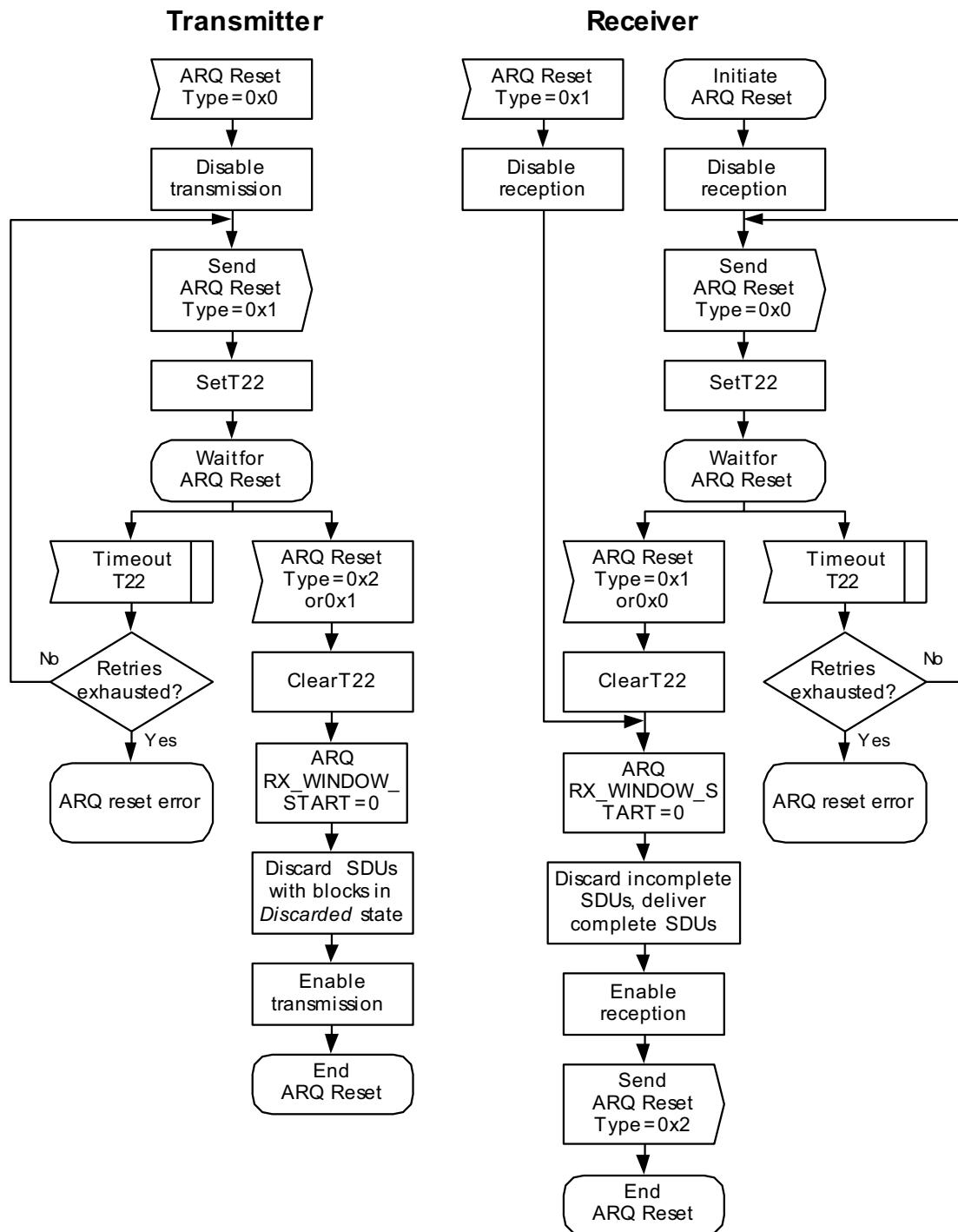
When a cumulative with selective acknowledgment and a valid BSN is received, the transmitter performs the actions described above for cumulative acknowledgment, followed by those for a selective acknowledgment.

All timers associated with acknowledged blocks shall be cancelled.

A Discard message shall be sent following violation of ARQ\_BLOCK\_LIFETIME. The message may be sent immediately or may be delayed up to ARQ\_RX\_PURGE\_TIMEOUT + ARQ\_RETRY\_TIMEOUT. Following the first transmission, subsequent discard orders shall be sent to the receiver at intervals of

ARQ\_RETRY\_TIMEOUT until an acknowledgment to the discarded BSN has been received. Discard orders for adjacent BSN values may be accumulated in a single Discard message.

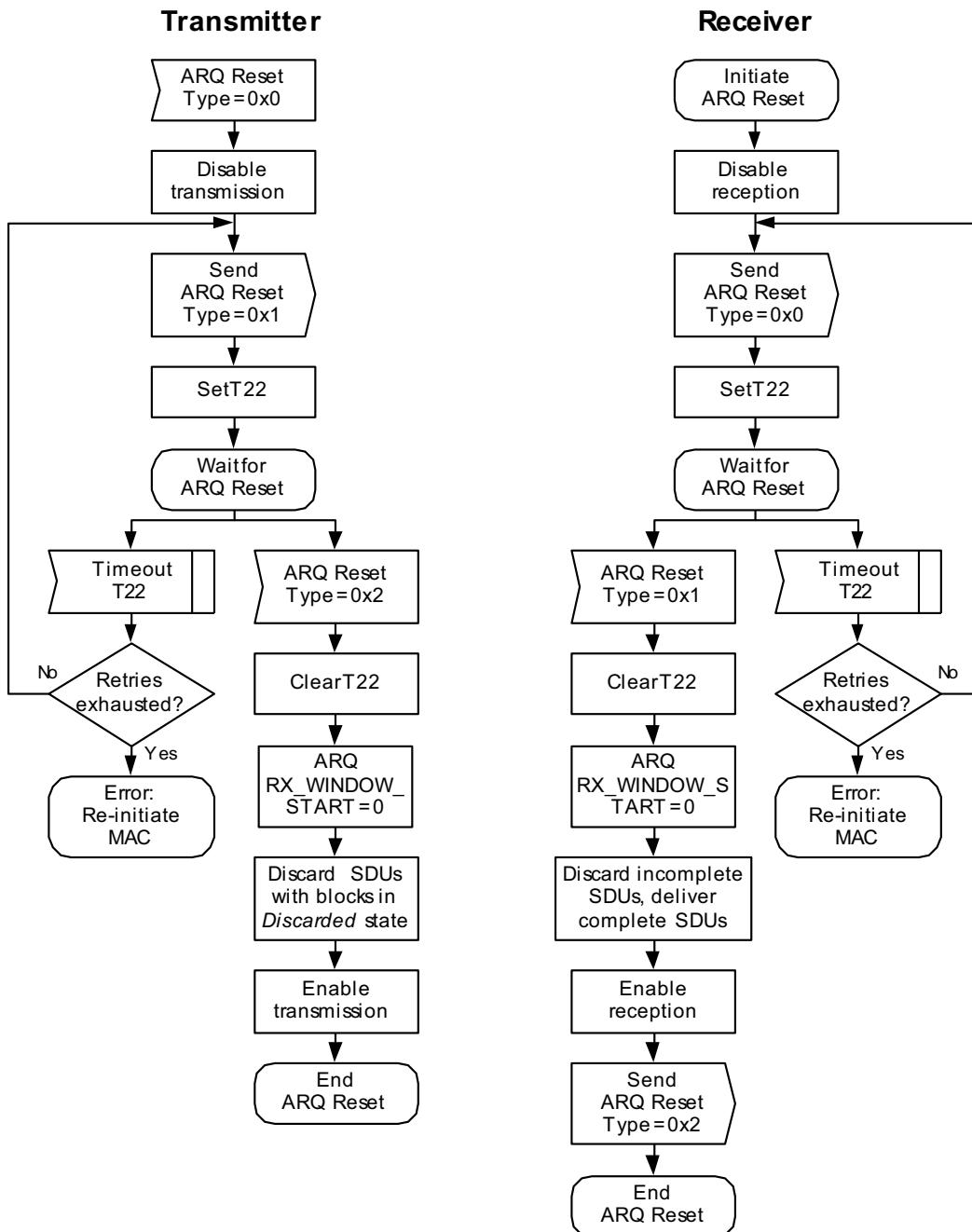
The actions to be taken by the transmitter state machine when it wants to initiate a reset of the receiver ARQ state machine are provided in Figure 25. The actions to be taken by the receiver state machine when it initiates an ARQ Reset message are provided in Figure 26.



**Figure 25 — ARQ Reset message dialog—Transmitter-initiated**

Synchronization of the ARQ state machines is governed by a timer managed by the transmitter state machine. Each time ARQ\_RX\_WINDOW\_START is updated, the timer is set to zero. When the timer exceeds the value of ARQ\_SYNC\_LOSS\_TIMEOUT, the transmitter state machine shall initiate a reset of the connection's state machines as described in Figure 25.

When in ARQ reset error state in Figure 25 and Figure 26, the CPE shall reinitialize its MAC, and the behavior for BS is implementation dependent.

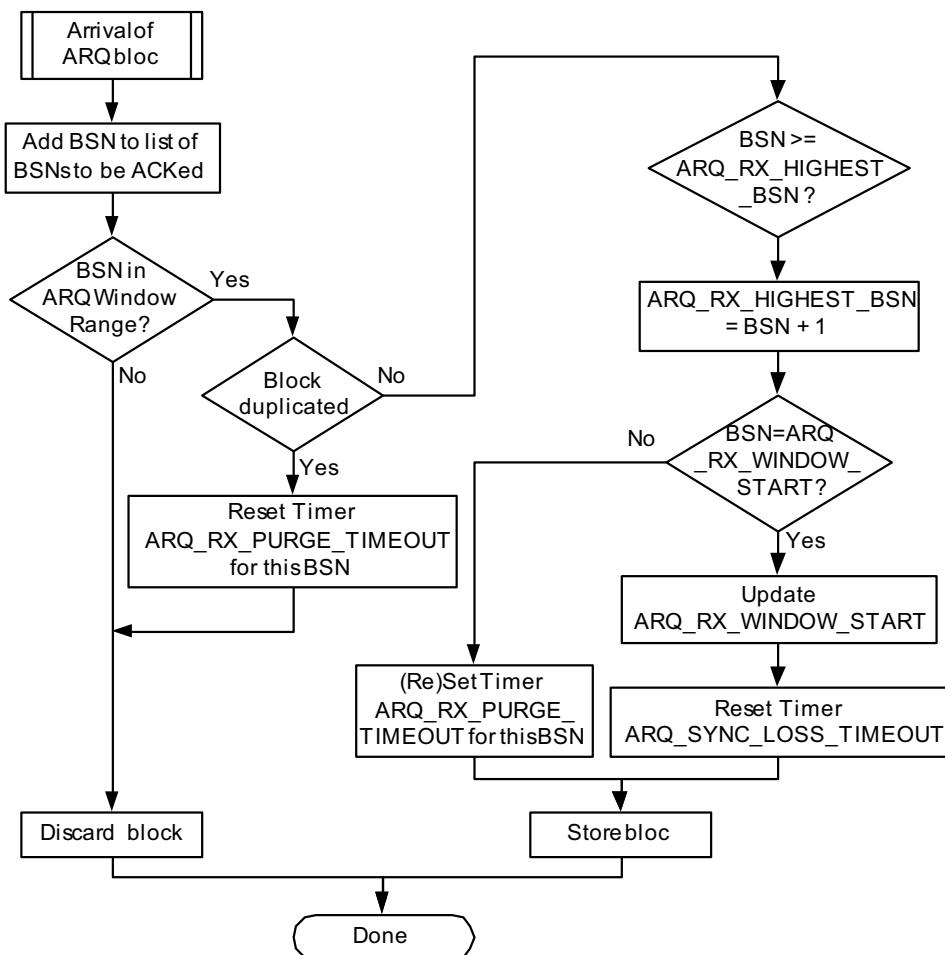


**Figure 26 — ARQ Reset message dialog—Receiver-initiated**

A Discard message may be sent to the receiver when the transmitter wants to skip ARQ blocks up to the BSN value specified in the Discard message. Upon receipt of the message, the receiver updates its state information to indicate the specified blocks were received and forwards the information to the transmitter through an ARQ Feedback IE at the appropriate time.

### 7.9.6.3 Receiver state machine

When a PDU is received, its integrity is determined based on the CRC-32 checksum or verifying the Ciphertext ICV (see 8.2.4). If a PDU passes the checksum, it is unpacked and defragmented, if necessary. The receiver maintains a sliding-window defined by ARQ\_RX\_WINDOW\_START state variable and the ARQ\_WINDOW\_SIZE parameter. When an ARQ block with a number that falls in the range defined by the sliding window is received, the receiver shall accept it. ARQ block numbers outside the sliding window shall be rejected as out of order. The receiver should discard duplicate ARQ blocks (i.e., ARQ blocks that were already received correctly) within the window. See Figure 27.



**Figure 27 — ARQ block reception**

The sliding window is maintained so that the ARQ\_RX\_WINDOW\_START variable always points to the lowest numbered ARQ block that has not been received or has been received with errors. When an ARQ block with a number corresponding to the ARQ\_RX\_WINDOW\_START is received, the window is advanced (i.e., ARQ\_RX\_WINDOW\_START is incremented modulo ARQ\_BSN\_MODULUS) so that the ARQ\_RX\_WINDOW\_START variable points to the next lowest numbered ARQ block that has not been

received or has been received with errors. The timer associated with ARQ\_SYNC\_LOSS\_TIMEOUT shall be reset.

When a block does not result in an advance of the ARQ\_RX\_WINDOW\_START, the ARQ\_RX\_PURGE\_TIMEOUT for that block shall be started. When the value of the timer for a block exceeds ARQ\_RX\_PURGE\_TIMEOUT, the timeout condition is marked. When the timeout condition is marked, ARQ\_RX\_WINDOW\_START is advanced to the BSN of the next block not yet received after the marked block. Timers for delivered blocks remain active and are monitored for timeout until the BSN values are outside the receive window.

When ARQ\_RX\_WINDOW\_START is advanced, any BSN values corresponding to blocks that have not yet been received residing in the interval between the previous and current ARQ\_RX\_WINDOW\_START value shall be marked as received and the receiver shall send an ARQ Feedback IE to the transmitter with the updated information. Any blocks belonging to complete SDUs shall be delivered. Blocks from partial SDUs shall be discarded.

When a discard message is received from the transmitter, the receiver shall discard the specified blocks, advance ARQ\_RX\_WINDOW\_START to the BSN of the first block not yet received after the BSN provided in the Discard message, and mark all not received blocks in the interval from the previous to new ARQ\_RX\_WINDOW\_START values as received for ARQ Feedback IE reporting.

For each ARQ block received, an acknowledgment shall be sent to the transmitter. Acknowledgment for blocks outside the sliding window shall be cumulative. Acknowledgments for blocks within the sliding window may be either for specific ARQ blocks (i.e., contain information on the acknowledged ARQ block numbers), or cumulative (i.e., contain the highest ARQ block number below which all ARQ blocks have been received correctly) or a combination of both (i.e., cumulative with selective). Acknowledgments shall be sent in the order of the ARQ block numbers they acknowledge. The frequency of acknowledgment generation is not specified here and is implementation dependent.

A MSDU is ready to be handed to the upper layers when all of the ARQ blocks of the MSDU have been correctly received within the time-out values defined.

When ARQ\_DELIVER\_IN\_ORDER is enabled, a MSDU is handed to the upper layers as soon as all the ARQ blocks of the MSDU have been correctly received within the defined time-out values and all blocks with sequence numbers smaller than those of the completed message have either been discarded due to time-out violation or delivered to the upper layers.

When ARQ\_DELIVER\_IN\_ORDER is not enabled, MSDUs are handed to the upper layers as soon as all blocks of the MSDU have been successfully received within the defined time-out values.

The actions to be taken by the receiver state machine when an ARQ Reset message is received are provided in Figure 25. The actions to be taken by the receiver state machine when it wants to initiate a reset of the transmitter ARQ state machine are provided in Figure 26.

Synchronization of the ARQ state machines is governed by a timer managed by the receiver state machine. Each time ARQ\_RX\_WINDOW\_START is updated, the timer is set to zero. When the timer exceeds the value of ARQ\_SYNC\_LOSS\_TIMEOUT the receiver state machine shall initiate a reset of the connection's state machines as described in Figure 26.

## 7.10 Scheduling services

Scheduling services represent the data handling mechanisms supported by the MAC scheduler for data transport on a connection. Each connection is associated with a single data service. Each data service is associated with a set of QoS parameters that quantify aspects of its behavior (these parameters are managed

using the DSA and DSC messages). Four services (7.7.8.9.9) are supported: Unsolicited Grant Service (UGS), Real-time Polling Service (rtPS), Non-real-time Polling Service (nrtPS), and best effort (BE). A description of each of these services and some of the applications they aim at supporting are described in the paragraphs that follow. Mandatory QoS parameters associated with each of these services are also identified. A detailed description of all supported QoS parameters can be found in 7.7.8.9.

The UGS is designed to support real-time data streams consisting of fixed-size data packets sent at periodic intervals, such as T1/E1 and Voice over IP without silence suppression. The mandatory QoS service flow parameters for this scheduling service are Maximum Sustained Traffic Rate, Maximum Latency, Tolerated Jitter, and Request/Transmission Policy. If present, the Minimum Reserved Traffic Rate parameter shall have the same value as the Maximum Sustained Traffic Rate parameter.

The rtPS is designed to support real-time data streams consisting of variable-sized data packets that are issued at periodic intervals, such as MPEG video. The mandatory QoS service flow parameters for this scheduling service are Minimum Reserved Traffic Rate, Maximum Sustained Traffic Rate, Maximum Latency, and Request/Transmission Policy.

The nrtPS is designed to support delay-tolerant data streams consisting of variable-sized data packets for which a minimum data rate is required, such as FTP. The mandatory QoS service flow parameters for this scheduling service are Minimum Reserved Traffic Rate, Maximum Sustained Traffic Rate, Traffic Priority, and Request/Transmission Policy.

The BE service is designed to support data streams for which no minimum service level is required and therefore may be handled on a space-available basis. The mandatory QoS service flow parameters for this scheduling service are Maximum Sustained Traffic Rate, Traffic Priority, and Request/Transmission Policy.

### **7.10.1 Data transmission scheduling**

Data transmission scheduling selects the data for transmission in a particular frame/bandwidth allocation and is performed by the BS for downstream, and by the CPE for upstream. In addition to whatever other factors the scheduler may deem pertinent, the following items shall be taken into account for each active service flow:

- The scheduling service specified for the service flow.
- The values assigned to the service flow's QoS parameters.
- The availability of data for transmission.
- The capacity of the granted bandwidth.

### **7.10.2 Upstream request/grant scheduling**

Upstream request/grant scheduling is performed by the BS with the intent of providing each associated CPE with bandwidth for upstream transmissions or opportunities to request bandwidth. By specifying a scheduling service and its associated QoS parameters, the BS scheduler can anticipate the throughput and latency needs of the upstream traffic and provide polls and/or grants at the appropriate times. Table 177 summarizes the scheduling services and the poll/grant options available for each. The following subclauses define service flow scheduling services for upstream operations.

**Table 177 — Scheduling services and corresponding poll/grant options**

Scheduling Type	PiggyBack Request	Bandwidth Stealing	Polling
UGS	Not Allowed	Not Allowed	PM bit is used to request a unicast poll for bandwidth needs of non-UGS connections.
rtPS	Allowed	Allowed	Scheduling only allows unicast polling.
nrtPS	Allowed	Allowed	Scheduling may restrict a service flow to unicast polling via the transmission/request policy; otherwise all forms of polling are allowed.
BE	Allowed	Allowed	All forms of polling allowed.

#### 7.10.2.1 UGS

The UGS service offers fixed-size grants on a real-time periodic basis, which eliminate the overhead and latency of CPE requests and assure that grants are available to meet the flow's real-time needs. The BS shall provide allocations to the CPE, in both the DS or US via MAP IEs, at periodic intervals based upon the Maximum Sustained Traffic Rate of the service flow. The size of these grants shall be sufficient to hold the fixed-length data associated with the service flow (with associated generic MAC header and Grant management subheader) but may be larger at the discretion of the BS scheduler. In order for this service to work correctly, the Request/Transmission Policy (7.7.8.9.10) setting shall be such that the CPE is prohibited from using any contention request opportunities for this connection.

The Grant Management subheader (7.6.1.2.3) is used to pass status information from the CPE to the BS regarding the state of the UGS service flow. The most significant bit of the Grant Management field is the Slip Indicator (SI) bit. The CPE shall set this flag once it detects that this service flow has exceeded its transmit queue depth. Once the CPE detects that the service flow's transmit queue is back within limits, it shall clear the SI flag. The flag allows the BS to provide for long-term compensation for conditions, such as lost maps or clock rate mismatches, by issuing additional grants. The poll-me (PM) bit may be used to request to be polled for a different, non-UGS connection.

The BS shall not allocate more bandwidth than the Maximum Sustained Traffic Rate parameter of the Active QoS parameter set, excluding the case when the SI bit of the Grant Management field is set. In this case, the BS may grant up to 1% additional bandwidth for clock rate mismatch compensation.

#### 7.10.2.2 rtPS

The rtPS service offers real-time, periodic, unicast request opportunities, which meet the flow's real-time needs and allows the CPE to specify the size of the desired grant. This service requires more request overhead than UGS, but supports variable grant sizes for optimum data transport efficiency.

The BS shall provide periodic unicast request opportunities. In order for this service to work correctly, the Request/Transmission Policy setting (7.7.8.9.10) shall be such that the CPE is prohibited from using any contention request opportunities for that connection. The BS may issue unicast request opportunities as prescribed by this service even if prior requests are currently unfulfilled. This results in the CPE using only unicast request opportunities in order to obtain upstream transmission opportunities. The CPE could still send a bandwidth request by sending the BR subheader in a MAC PDU on an existing upstream transmission as well. All other bits of the Request/Transmission Policy are irrelevant to the fundamental operation of this scheduling service and should be set according to network policy.

#### 7.10.2.3 nrtPS

The nrtPS offers unicast polls on a regular basis, which assures that the service flow receives request opportunities even during network congestion. The BS typically polls nrtPS FID on a CPE on an interval on the order of one second or less.

The BS shall provide timely unicast request opportunities. In order for this service to work correctly, the Request/Transmission Policy setting (7.7.8.9.10) shall be set such that the CPE is allowed to use contention request opportunities. This results in the CPE using contention request opportunities as well as unicast request opportunities and unsolicited bandwidth request via the Bandwidth Request subheader. All other bits of the Request/Transmission Policy are irrelevant to the fundamental operation of this scheduling service and should be set according to network policy.

#### **7.10.2.4 Best effort**

The intent of the BE service is to provide efficient service for best effort traffic. In order for this service to work correctly, the Request/Transmission Policy setting shall be set such that the CPE is allowed to use contention request opportunities. This results in the CPE using contention request opportunities as well as unicast request opportunities and unsolicited bandwidth request via the Bandwidth Request subheader. All other bits of the Request/Transmission Policy are irrelevant to the fundamental operation of this scheduling service and should be set according to network policy.

### **7.11 Bandwidth management**

During network entry and initialization, every CPE is assigned up to three dedicated FIDs for the purpose of sending and receiving control messages. These connection pairs are used to allow differentiated levels of QoS to be applied to the different connections carrying MAC management traffic. Increasing (or decreasing) bandwidth requirements are necessary for all services except incompressible constant bit rate UGS connections. The needs of incompressible UGS connections do not change between connection establishment and termination. The requirements of compressible UGS connections, such as channelized T1, may increase or decrease, depending on traffic. DAMA services are given resources on a demand assignment basis, as the need arises.

There are numerous methods by which a CPE can send a bandwidth request message to the BS, and these are described in the following subclauses.

#### **7.11.1 Bandwidth Requests**

Bandwidth Requests (or simply, Requests) refer to the mechanism that CPEs use to indicate to the BS that they need upstream bandwidth allocation. Two types of bandwidth requests are available in the MAC layer (with proper PHY support).

##### **7.11.1.1 Contention-based Request**

In this case, a Request comes as a subheader appended to the generic MAC header (see 7.6.1.2.1), which may or may not contain payload. Typically, a Request will not contain a payload if it is the first Request made for the connection. It may contain a payload otherwise.

Because the upstream burst profile can change dynamically, all requests for bandwidth shall be made in terms of the number of bytes needed to carry the MAC header and payload, but not the PHY overhead. The Bandwidth Request message may be transmitted during any upstream allocation, except during any initial ranging interval, UCS notification interval, and SCW.

Bandwidth Requests may be incremental or aggregate. When the BS receives an incremental Bandwidth Request, it shall add the quantity of bandwidth requested to its current perception of the bandwidth needs of the connection. When the BS receives an aggregate Bandwidth Request, it shall replace its perception of the bandwidth needs of the connection with the quantity of bandwidth requested. The Type field in the bandwidth request header indicates whether the request is incremental or aggregate. The self-correcting

nature of the request/grant protocol requires that CPEs shall periodically use aggregate Bandwidth Requests. The period may be a function of the QoS of a service and of the link quality.

### 7.11.1.2 CDMA Request

In addition to the transmission of bandwidth requests by the CPE, the PHY also supports the use of a CDMA-based mechanism for the purpose of upstream bandwidth allocation.

As detailed in the PHY spec, the PHY has available a subset of Ranging codes that shall be used for CDMA Bandwidth Requests. The CPE, upon needing to request bandwidth, shall select, with equal probability, a Ranging Code from the code subset allocated to Bandwidth Requests. This Ranging Code shall be modulated onto a Ranging Subchannel and transmitted during the appropriate upstream allocation. The Ranging Subchannel shall be selected among the ones reserved by the MAC for the upstream transmission.

Upon detection, the BS shall provide an upstream allocation for the CPE. The BS does not respond with an allocation on the CPE's Basic FID. Instead, it broadcasts a CDMA\_Allocation\_IE, which specifies the transmit region and Code that were used by the CPE. This allows a CPE to determine whether it has been given an allocation by matching these parameters with the parameters it used. The CPE shall use the allocation to transmit a MAC PDU with the Bandwidth Request subheader and/or data (this is indicated by the Usage field—see Table 37). The CPE may only omit the Bandwidth Request PDU when the BS indicated so in the CDMA\_Allocation\_IE (see Table 37).

If the BS does not issue the upstream allocation described above, or the MAC PDU with the bandwidth request subheader does not result in a subsequent allocation of any bandwidth, the CPE shall assume that the Ranging Code transmission resulted in a collision and follow the contention resolution as specified in 7.13.

### 7.11.2 Grants

For a CPE, bandwidth requests reference individual FIDs while each bandwidth grant is addressed to the CPE's SID, not to individual FIDs. Since it is nondeterministic which request is being honored, when the CPE receives a shorter transmission opportunity than expected (scheduler decision, request message lost, etc.), no explicit reason is given. In all cases, based on the latest information received from the BS and the status of the request, the CPE may decide to perform backoff and request again, discard the SDU, or possibly fragment the SDU to fit the allocation.

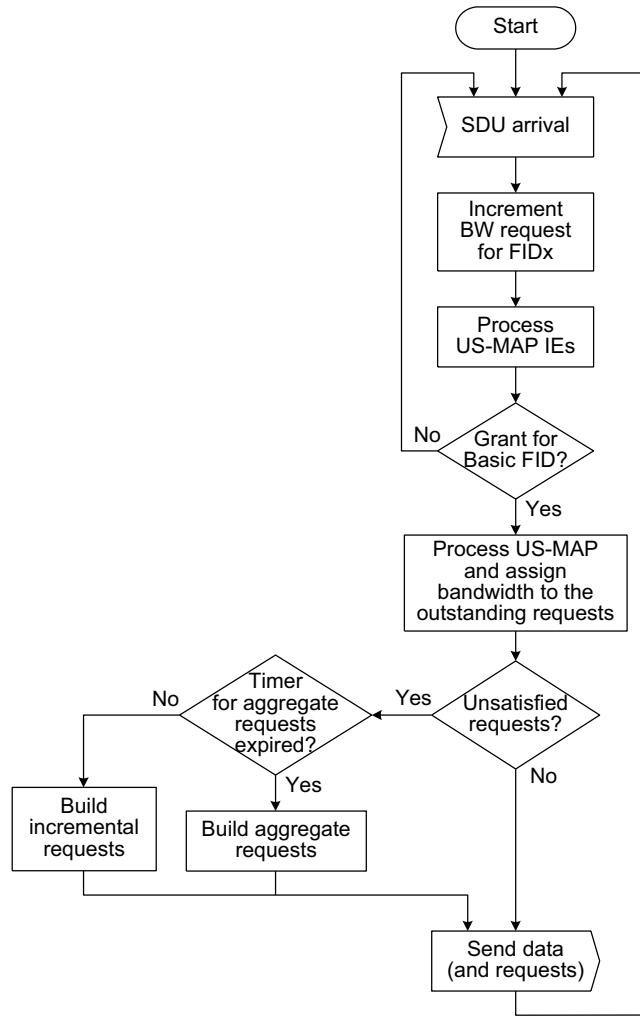
A CPE may make use of a US-MAP IE that is broadcast, directed at a multicast polling group of which it is a member, or directed at its SID. In all cases, the US-MAP IE burst profile (e.g., UIUC = 3, 5, or 7) is used, even if the BS is capable of receiving the CPE with a more efficient burst profile. To take advantage of a more efficient burst profile, the CPE should transmit a Bandwidth Request to the BS on its Basic FID using the Bandwidth Request subheader. Unicast polling of a CPE would normally be done by allocating a US-MAP IE directed at its SID. Also note that, in a US-MAP IE directed at its SID, the CPE may make bandwidth requests for any of its connections.

The procedure followed by CPEs is shown in Figure 28. Note that it is the CPE's local scheduler that decides which connections get the granted bandwidth.

### 7.11.3 Polling

Polling is the process by which the BS allocates to the CPEs bandwidth specifically for the purpose of making bandwidth requests. These allocations may be to individual CPEs or to groups of CPEs. Allocations to groups of connections and/or CPEs actually define bandwidth request contention IEs. The allocations are not in the form of an explicit message, but are contained as a series of IEs within the US-MAP.

Note that polling is done on CPE basis. Bandwidth is always requested on a FID basis and bandwidth is allocated on a CPE basis.



**Figure 28 — Request/grant mechanism**

#### 7.11.3.1 Unicast

When a CPE is polled individually, no explicit message is transmitted to poll the CPE. Rather, the BS reserves in the US-MAP enough bandwidth for the CPE to respond with a Bandwidth Request. If the CPE does not need bandwidth, the allocation is padded in accordance with 7.8.6. CPEs that have an active UGS connection of sufficient bandwidth shall not be polled individually unless they set the PM bit in the header of a packet on the UGS connection. This saves bandwidth over polling all CPEs individually. Note that unicast polling would normally be done on a per-CPE basis by signaling an allocation in a US-MAP IE (with UIUC = 3, 5, or 7), thereby allowing a CPE to transmit a Bandwidth Request directed at its SID.

#### 7.11.3.2 Multicast and broadcast

If insufficient bandwidth is available to individually poll many inactive CPEs, some CPEs may be polled in multicast groups or a broadcast poll may be issued. Certain SIDs are reserved for multicast groups and for broadcast, as described in 12.2. As with individual polling, the poll is not an explicit message, but

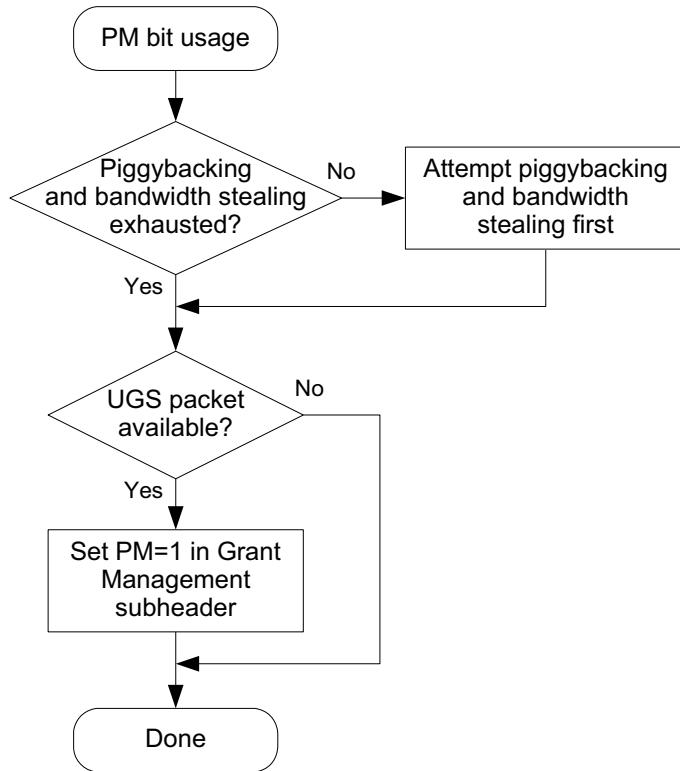
bandwidth allocated in the US-MAP. The difference is that, rather than associating allocated bandwidth with a CPE's Basic FID, the allocation is to the Polling FID (see 12.2) for a multicast group (multicast SID) or Broadcast FID (see 12.2) for the entire cell (Cell SID).

When the poll is directed at a multicast group or via broadcast, a CPE belonging to the polled group may request bandwidth during any request interval allocated to that SID in the US-MAP by a US-MAP IE. In order to reduce the likelihood of collision with multicast and broadcast polling, only CPEs needing bandwidth reply; they shall apply the contention resolution algorithm as defined in 7.13 to select the interval in which to transmit the initial bandwidth request. Zero-length bandwidth requests shall not be used in multicast or broadcast Request Intervals.

The CPE shall assume that the transmission has been unsuccessful if no grant has been received in the number of subsequent US-MAP messages specified by the parameter Contention-based reservation timeout (see 7.7.3.1). If the retransmission of the request is made in a multicast or broadcast opportunity, the CPE continues to run the contention resolution algorithm in 7.13. Note that the CPE is not restricted to retransmitting the request in a multicast or broadcast Request Interval only.

### 7.11.3.3 PM bit

CPEs with currently active UGS connections may set the PM bit (see 7.6.1.2.3) to the BS that they need to be polled to request bandwidth for non-UGS connections. To reduce the bandwidth requirements of individual polling, CPEs with active UGS connections need be individually polled only if the PM bit is set (or if the interval of the UGS is too long to satisfy the QoS of the CPE's other connections). Once the BS detects this request for polling, the process for individual polling is used to satisfy the request. The procedure by which a CPE stimulates the BS to poll it is shown in Figure 29. To minimize the risk of the BS missing the PM bit, the CPE may set the bit in all UGS MAC Grant Management subheaders in the upstream scheduling interval.



**Figure 29 — PM bit usage**

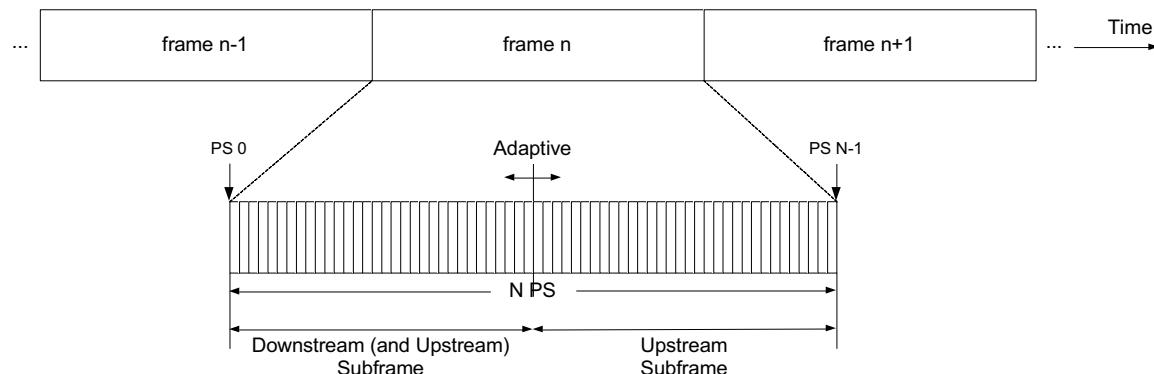
## 7.12 PHY support

In this subclause, aspects of the MAC that may impact the design of the PHY layer are discussed.

### 7.12.1 Duplexing

TDD is the only duplexing mode currently supported by this standard.

In TDD, the upstream and downstream transmissions occur at different times and share the same channel. As depicted in Figure 30, a TDD frame in the MAC typically has a fixed duration and contains two subframes: a predominantly downstream and an upstream (see 7.4 for further details). The frame is divided into an integer number of OFDM symbols, which help to partition the bandwidth easily. The TDD framing is adaptive in that the bandwidth allocated to the downstream versus the upstream can vary. The split between upstream and downstream is a parameter that is controlled at higher layers within the system. Note that when multiple WRAN cells have overlapping coverage, they shall share the available bandwidth in frame-based TDMA according to the self-coexistence procedure defined in 7.20.3.2.



**Figure 30 — TDD frame structure**

### 7.12.2 DS-MAP

The broadcast message DS-MAP defines the usage of the downstream intervals.

### 7.12.3 US-MAP

The broadcast message US-MAP defines the usage of the upstream intervals in terms of the offset of the upstream burst relative to the Allocation Start Time parameter.

#### 7.12.3.1 Timing

The upstream timing is relative to the beginning of the downstream subframe. The Allocation Start Time in the US-MAP is relative to the start of the downstream subframe, and is such that the US-MAP references some point in the current frame (see 7.12.4). The CPE shall always adjust its concept of upstream timing based upon the timing adjustments sent in the RNG-CMD messages.

#### 7.12.3.2 Allocations

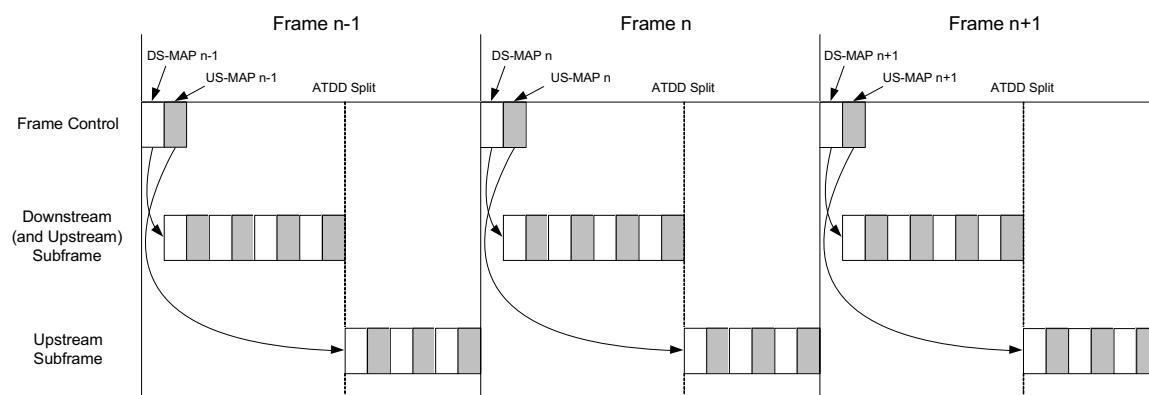
The upstream bandwidth allocation map (US-MAP) employs units of symbols and logical channels (i.e., OFDM slots) to manage resource allocation among CPEs.

#### 7.12.4 MAP timing

The DS-MAP and US-MAP messages provide relative timing information. The following time instants are used as a reference for timing information:

- DS-MAP: The start of the first symbol (including the preamble if present) of the frame in which the message was transmitted.
- US-MAP: The start of the first symbol (including the preamble if present) of the frame in which the message was transmitted plus the value of the Allocation Start Time.

Information contained in both the DS-MAP and US-MAP messages pertain to the current frame (i.e., the frame in which this message was received)<sup>12</sup> as shown in Figure 31. In addition, information carried in the US-MAP pertains to a time interval starting at the Allocation Start Time measured from the beginning of the current frame and ending after the last specified allocation. The Allocation Start Time value shall be equal to the Adaptive TDD (ATDD) split, where ATDD split is the time instant within the frame that divides the downstream subframe and the upstream subframe.



**Figure 31 — Time relevance of DS-MAP and US-MAP**

#### 7.12.5 Channel use policy for the protection of TV incumbents

WRAN CPEs and BSs shall not operate on the same channel or on the first adjacent channels of a TV operation within the TV protected contour. However, they may operate on co-channels or adjacent channels outside this protected contour as long as they are located at sufficient separation distances beyond this protected contour.

Consequently, if there is a TV operation on channel N, a WRAN CPE located within the TV protected contour of that TV station:

- Shall not transmit on channel N-1
- Shall not transmit on channel N
- Shall not transmit on channel N+1
- May be constrained from transmitting on alternate channels (N±2 and beyond), as defined by up-to-date information from the database service.

Furthermore, if there is a TV operation on channel N, a WRAN CPE outside of the TV protected contour of that TV station:

- Shall not transmit on channel N within a separation distance from the TV protected contour.

<sup>12</sup> It is important to note that, from a scheduling perspective, allocations specified in a DS-MAP and US-MAP messages shall remain, as much as possible, valid across multiple frames. This way, self-coexistence issues can be best managed.

- Shall not transmit within a separation distance from the TV protected contour on channel N-1
- Shall not transmit within a separation distance from the TV protected contour on channel N+1.

## 7.13 Contention resolution

The BS controls assignments on the upstream channel through the US-MAP messages and determines which symbol periods are subject to collisions. Collisions may occur during Initial Ranging, Periodic Ranging, Bandwidth Request, UCS notification, and the SCW defined by their respective IEs. The potential occurrence of collisions in the Intervals is dependent upon the number of SIDs whose US-MAP IEs are (simultaneously) configured to use an Interval for a specific purpose (e.g., Ranging, UCS notification, BW Request). The CPE has to make a decision in order to resolve collision in the upstream direction for Initial Ranging, Periodic Ranging, and BW Request. Since in the case of UCS notification and SCW (CBP packet transmission in the SCW) no explicit feedback is expected to be received from the BS, collision resolution does not apply.

In the case of Initial Ranging and Periodic Ranging, collision resolution is to be done by a CDMA method (see Table 31 and Table 37). In the case of Bandwidth Request and UCS notification, both methods, CDMA as well as exponential time backoff, explained later in this subclause, can be used. In the case of collision resolution in the SCW, a special scheduling scheme, described in 7.20.1.2, shall be used.

Since a CPE may need to service multiple upstream service flows (each with its own FID), it makes these decisions on a per FID or on a QoS (see 7.17) basis. The method of contention resolution that shall be supported for BW Request and UCS notification is based on a truncated binary exponential backoff, with the initial backoff window and the maximum backoff window controlled by the BS (see Table 30). The values, expressed in units of opportunity (see Table 31) are specified as part of the UCD message and represent a power-of-two value. For example, a value of 4 indicates a window between 0 and 15 opportunities; a value of 10 indicates a window between 0 and 1023 opportunities. When a CPE has information to send and wants to enter the contention resolution process, it sets its internal backoff window equal to the BW Request or UCS Notification Backoff Start defined in the UCD message referenced by the UCD Count in the US-MAP message currently in effect (the map currently in effect is the map whose allocation start time has occurred but which includes IEs that have not occurred).

Note that the number of these opportunities per frame depends on the size of the opportunity window in number of subchannels defined by the US-MAP for UIUC 2 or 3 (see Table 35) and the opportunity size for the BW Request and UCS notification defined in Table 31. These opportunities shall be mapped horizontally in the time domain and fill a subchannel before moving to the next subchannel as is done for the upstream data PDU mapping.

The CPE shall randomly select a number within its backoff window. This random value indicates the number of contention transmission opportunities that the CPE shall defer before transmitting. A CPE shall consider only contention transmission opportunities for which this transmission would have been eligible. These are defined by the BW Request or UCS notification IE in the US-MAP messages. Note that each IE may consist of multiple contention transmission opportunities.

Using bandwidth request as an example, consider a CPE whose initial backoff window is 0 to 15 and assume it randomly selects the number 11. The CPE must defer a total of 11 contention transmission opportunities. If the first available US-MAP IE is for 6 requests, the CPE does not use this and has 5 more opportunities to defer. If the next US-MAP IE is for 2 requests, the CPE has 3 more to defer. If the third US-MAP IE is for 8 requests, the CPE transmits on the fourth opportunity, after deferring for 3 more opportunities.

After a contention transmission, the CPE waits for an allocation in a US-MAP IE in a subsequent map. Once received, the contention resolution is complete. The CPE shall consider the contention transmission

lost if no data grant has been given within T16 (or no response within T3 for initial ranging). The CPE shall now increase its backoff window by a factor of two, as long as it is less than the maximum backoff window. The CPE shall randomly select a number within its new backoff window and repeat the deferring process described previously.

This retry process continues until the maximum number (i.e., BW Request Retries) of retries has been reached. At this time, the PDU shall be discarded. Note that the maximum number of retries is independent of the initial and maximum backoff windows that are defined by the BS. If the CPE receives an allocation in a (unicast) US-MAP IE with UIUC = 3, 5, or 7 at any time while deferring for this FID, it shall stop the contention resolution process and use the explicit transmission opportunity.

The BS has flexibility in controlling the contention resolution. At one extreme, the BS may choose to set up the BW Request/UCS Notification Backoff Start and BW Request/UCS Notification Backoff End to emulate an Ethernet-style backoff with its associated simplicity and distributed nature as well as its fairness and efficiency issues. This would be done by setting the BW Request/UCS Notification Backoff Start = 0 and BW Requestor UCS Notification Backoff End = 10 in the UCD message. At the other end, the BS may make the BW Request/UCS Notification Backoff Start and BW Request/UCS Notification Backoff End identical and frequently update these values in the UCD message so that all CPE are using the same, and hopefully optimal, backoff window.

### 7.13.1 Transmission opportunities

A transmission opportunity is defined as an allocation provided in a US-MAP or part thereof intended for a group of CPEs authorized to transmit initial ranging requests, periodic ranging requests, bandwidth requests, or UCS notifications. This group may include either all CPEs that have an intention to join the cell or all registered CPEs or a multicast polling group. The number of transmission opportunities associated with a particular IE in a map is dependent on the total size of the allocation as well as the size of an individual transmission.

The size of an individual transmission opportunity for each type of contention IE shall be published in each transmitted UCD message. The BS may allocate bandwidth for contention IEs. When it does so, it shall use integer multiples of the published values.

## 7.14 Initialization and network association

Before a CPE can enter the network, it needs to be serviced by a BS and its capabilities need to be negotiated with the BS. This may involve many tasks (e.g., geolocation and sensing channels) and handshaking between the CPE and the BS, and this whole procedure is hereby referred to as initialization and network association. More importantly, during this process the BS needs to minimize the CPE communication so as potentially not to cause harmful interference with incumbents. In other words, the initialization and network association process is *incumbent safe*, which essentially means that incumbent system protection shall be maximized.

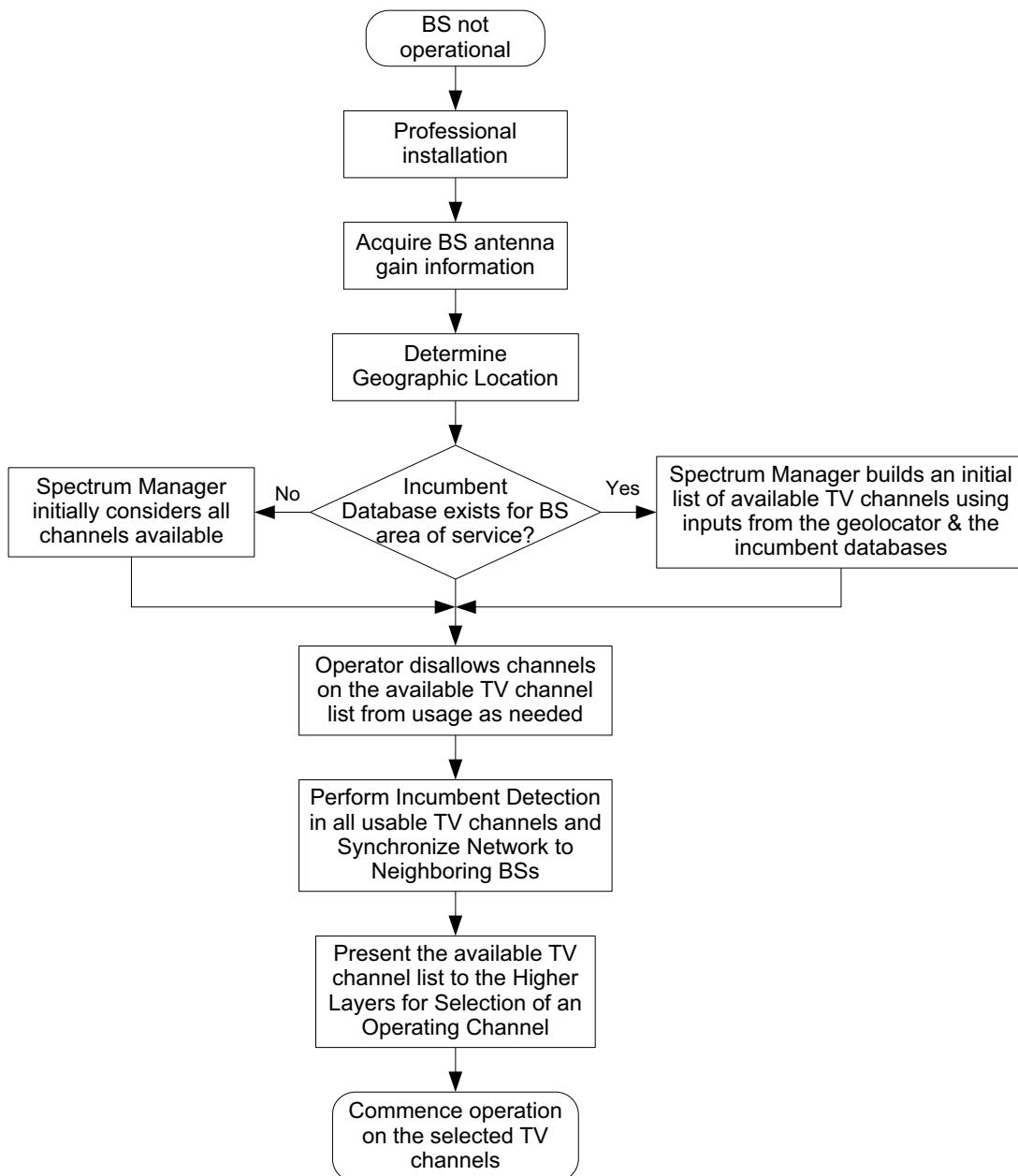
### 7.14.1 BS initialization

The WRAN BS initialization procedure shall consist of the following steps:

- 1) BS is professionally installed.
- 2) BS acquires the antenna gain information.
- 3) Determine the BS geographic location.

- 4) If a database service exists for BS area of service, the SM at the BS receives an initial list of available channels from the database service. If there is no database service, the SM initially considers all channels available.
- 5) Operator disallows channels on the available channel list as needed.
- 6) Perform incumbent detection in all usable channels and synchronize network to neighboring BSs.
- 7) Presentation of the available channel list to the higher layers for selection of an operating channel.
- 8) Commence operation on the selected operating channel(s).

This BS initialization procedure is depicted in Figure 32.



**Figure 32 — BS initialization procedure**

#### **7.14.1.1 Professional installation**

The BS shall be installed by a professional who will be responsible for assuring that its installation is compliant with local regulations (see Annex A) and the IEEE P802.22.2.<sup>13</sup> The professional installer should make sure that the antenna pattern meets the pattern specified in 9.12.1 and that the antenna is directed toward the selected BS.

#### **7.14.1.2 BS antenna gain information acquisition**

The BS shall determine if its antenna is integrated or not by querying it using the M-ANTENNA-INTEGRATED primitive structure described in 10.7.6.1 and 10.7.6.2. The BS shall acquire the antenna information including the maximum antenna gain information for the channels that can be used in the regulatory domain of interest. This information is stored in a MIB, *wranIfBsCpeAntennaGainTable*. If the antenna is integrated to the BS TRU, this MIB object shall be pre-populated by the manufacturer of the BS. If the antenna is not integrated into the BS TRU, the MIB object shall be populated by querying the antenna unit (AU) through the interface defined in 9.12.2. This information at the antenna shall be pre-populated by the antenna manufacturer.

#### **7.14.1.3 Determine geographic location**

The geolocation requirement for the BS is that the WRAN system shall know the latitude and longitude of the BS transmitting antenna within a radius of 15 m and its altitude above mean sea level. The BS geographic location information shall be stored in the BS memory.

#### **7.14.1.4 Access TV bands database service and receive list of available channels**

The BS shall access a TV bands database service if one exists.

The BS SM communicates with the TV bands database service using the primitives that are defined in 10.7.1. Each WRAN device shall enlist with the TV bands database service by providing information that is required for access to the TV bands. The BS SM, which shall act as a proxy for all of its registered client devices, shall perform enlistment using the M-DEVICE-ENLISTMENT primitives. Each instance that a device is required to get a new set of available channels, the BS SM shall provide its geographic coordinates or those of one of its registered client devices to the TV bands database service using the M-DB-AVAILABLE-CHANNEL-REQUEST primitive. The BS shall receive the available channels from the TV bands database service using the M-DB-AVAILABLE-CHANNEL-INDICATION primitive. The SM shall generate the composite available channel list using only those channels that have been indicated as available for every device on the network.

The BS shall prohibit WRAN operation on any channel not on this initial list of available channels.

#### **7.14.1.5 Operator disallows channels**

Access shall be provided for the operator to disallow channels that are listed on the available channel list from being selected for WRAN operation. The operator shall not have access to channels that are not listed on the available channel list. To further classify channels on the available list, the BS SM shall submit an M-AVAIL-TV-CH-REPORT primitive with the mode set equal to 1 to provide the available channel list to the higher layers. Once channels on the available channel list are further classified as disallowed, the SM shall receive an M-DISALLOWED-TV-CHS primitive submitted by the SM.

---

<sup>13</sup> IEEE P802.22.2 is currently under development. For information on obtaining drafts, please contact the IEEE.

#### **7.14.1.6 Perform incumbent detection and synchronize network with neighboring networks**

The BS shall perform incumbent detection in each of the channels listed on the available channel list and each adjacent channel if its EIRP is beyond the limit specified by the regulatory domain classes in Annex A (e.g., 40 mW in the USA) to detect other legitimate incumbent services that do not exist in the database service. The BS's SM shall use the output from the BS spectrum sensing function to identify occupied channels on the available channel list.

The BS shall perform neighboring IEEE 802.22 network discovery on selected channels according to 7.20.1.3. The BS shall synchronize with neighboring BSs using its installed satellite-based geolocation technology.

#### **7.14.1.7 Present the available channel list to the higher layers**

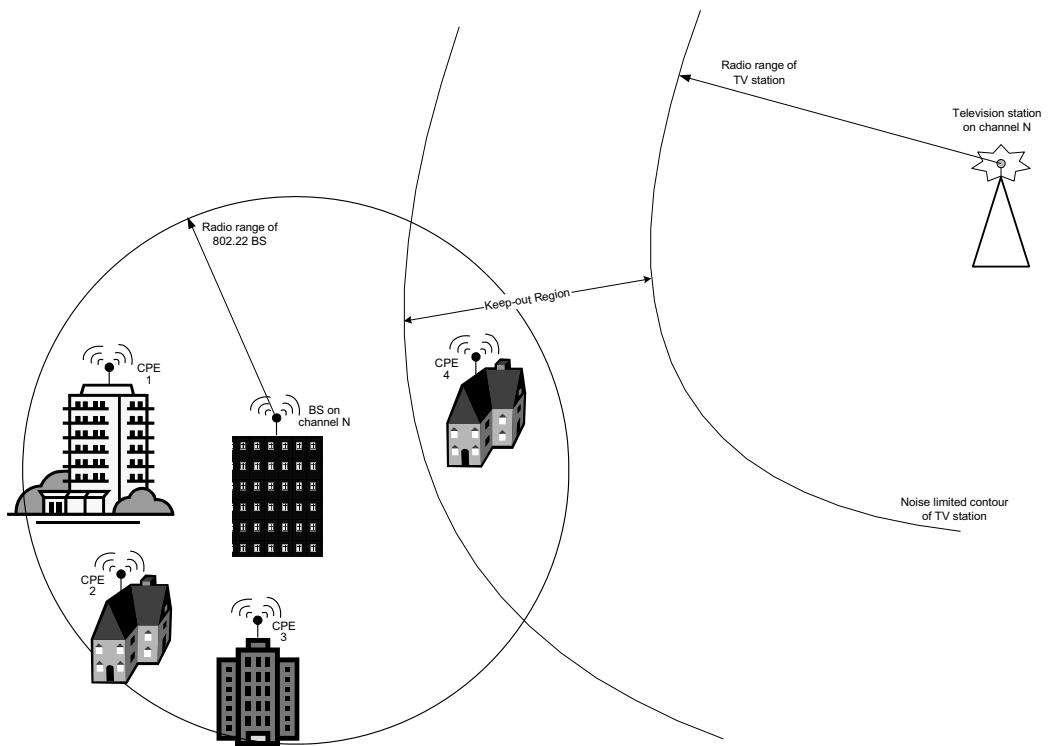
After incumbent detection during which channels may have been identified as protected or occupied, the resulting list shall be presented to the higher layers using an M-AVAIL-TV-CH-REPORT primitive with the mode set equal to 2 for selection of an operating channel. The required information presented shall be each channel number that is available for the BS to commence WRAN service and the maximum allowed EIRP for each channel. Additional information can be provided to the higher layers to help with the selection of an optimal channel, such as a list of channels where other wireless services were detected during the incumbent detection stage. As a result of the selection from the higher layer, the SM shall receive an M-OPERATING-TV-CH primitive from the NCMS.

#### **7.14.1.8 Commence operation**

The BS may now commence operation on any one channel listed on the available channel list.

### **7.14.2 CPE initialization**

Figure 33 illustrates a scenario where the need for the definition of an incumbent safe CPE initialization can be easily seen. In this figure, consider that CPE 4 is powered down whereas the BS is transmitting in the cell that is under normal operation. Further, assume that the TV station in Figure 33 is powered up and starts transmitting in the same channel (i.e., channel #N in this example) that is being used by the BS for its transmissions in the cell. CPE 4 should be capable of detecting that the BS is operating in a channel that is occupied by an incumbent service. The BS must be capable of determining if CPE 4 is located within interference range of the TV station protected contour (i.e., in the keep-out region). If the CPE4 is already registered with the BS, it will alert the BS. If the CPE4 is not registered with the BS, it shall not transmit. See 10.2.5, policies 5 and 6. In response to the alert from the CPE, the SM at the BS may or may not decide to switch channel to accommodate the CPE (see 10.2.6.6). The purpose of the sensing and geolocation capabilities of the WRAN system shall be to prevent harmful interference to the primary TV service by providing the necessary information to the BS's SM that generates the list of available channels. The definition of an incumbent safe CPE initialization phase is critical for cognitive radio systems. The SM incorporates algorithms to address this need (see Table 234, policies 5 and 6).



**Figure 33 — Scenario where a safe bootstrap operation is required to protect incumbents**

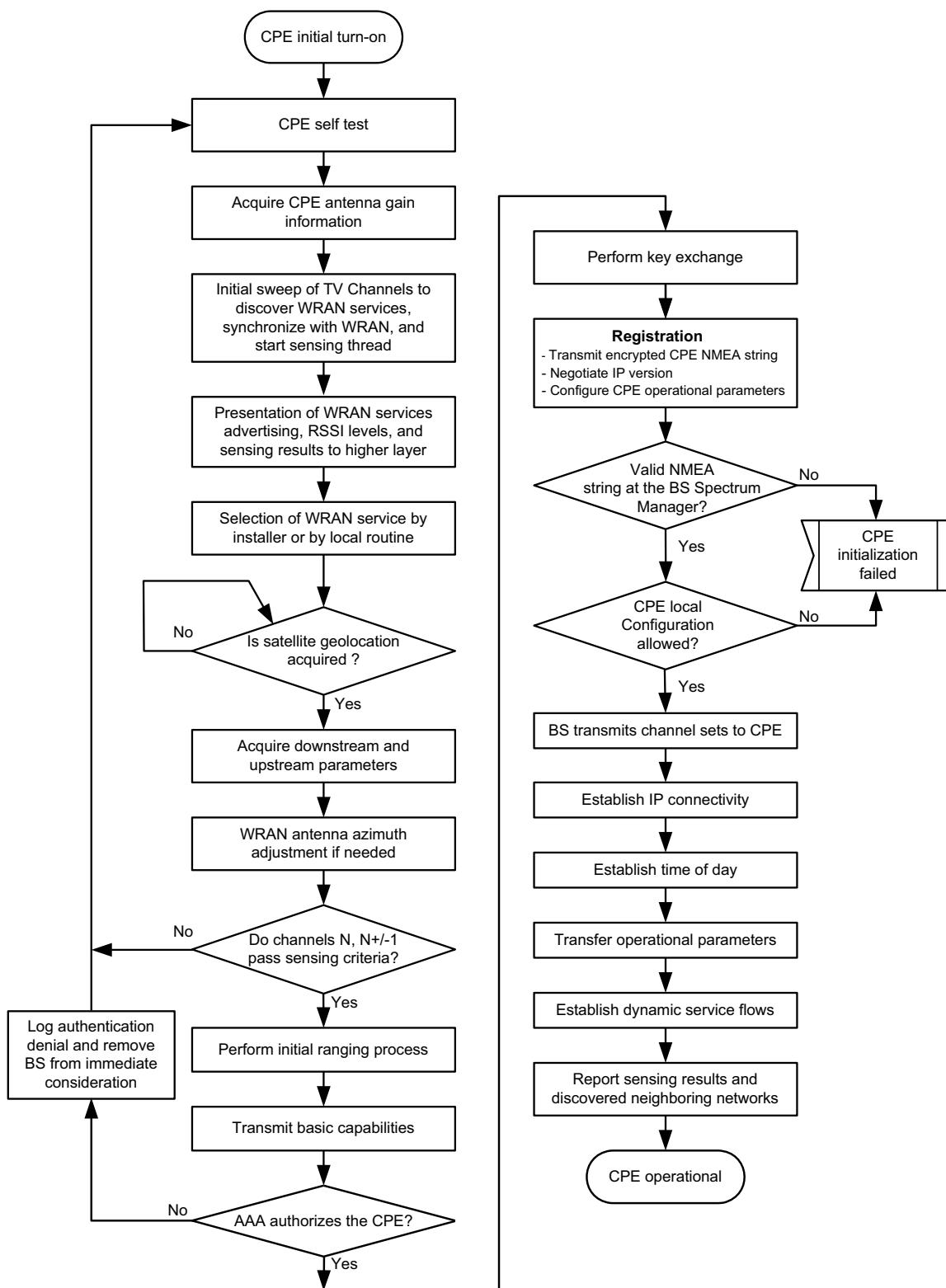
First and foremost, the MAC does not presuppose any preassigned channel where a CPE is able to look for a BS given the time-varying and unpredictable nature of channel occupancy. Hence, the first task a CPE must perform in attempting to join a network is to scan the set of channels for BSs and incumbent services on which the transmissions of the CPE might interfere. Since the BS shall send concentrated OFDM symbols composed of a superframe preamble, a frame preamble and an SCH once every superframe in its operating channel (see 7.3), the CPE will recognize the existence of a BS transmission and, if appropriate, proceed with the CPE initialization procedure with the corresponding BS.

The procedure carried out by the BS and the CPE to perform CPE network entry and initialization shall be as follows:

- CPE performs self test.
- CPE acquires the antenna gain information.
- CPE senses for and synchronizes to WRAN services. The sensing thread also begins during this step to detect broadcasting incumbents.
- CPE presents sensing results to the higher layers.
- CPE chooses a WRAN service.
- CPE acquires valid geolocation data from the satellites. If the data acquisition is unsuccessful, CPE initialization shall not continue.
- CPE acquires the downstream and upstream parameters from the selected WRAN service.
- CPE directional antenna azimuth adjustment.

- i) If channels N and N±1 pass the sensing and timing requirements, BS and CPE perform initial ranging (see 7.15.2.1).
- j) CPE transmits basic capabilities.
- k) If all required basic capabilities are present in the CPE, the AAA authenticates the CPE and key exchange is performed; otherwise, the CPE does not proceed to registration and the BS de-registers the CPE.
- l) Perform Registration (REG-REQ/RSP). Registration entails the following:
  - 1) Exchange and verification of CPE NMEA string
  - 2) Configuration of CPE operational parameters including configuration of IP version to be used by the CPE.
- m) Upon completing registration, BS transmits channel sets to CPE.
- n) Establish IP connectivity.
- o) Establish time of day.
- p) Transfer operational parameters.
- q) Establish dynamic service flows.
- r) CPE reports sensing results and discovered neighboring networks.

Figure 34 summarizes the network entry of the CPE and its initialization procedure. Note that these steps taken by the CPE consist of a set of actions and error verification. In the following subclauses, a more detailed description of these steps and their individual responsibilities are provided.



**Figure 34 — CPE initialization procedure**

#### **7.14.2.1 CPE performs self test**

On initialization or after signal loss, the CPE shall perform a self test.

#### **7.14.2.2 CPE antenna gain information acquisition**

The CPE shall determine if its antenna is integrated or not by querying it using the M-ANTENNA-INTEGRATED primitive structure described in 10.7.6.1 and 10.7.6.2. The CPE shall acquire the antenna information including the maximum antenna gain information for the channels that can be used in the regulatory domain of interest. This information is stored in a MIB, *wranIfBsCpeAntennaGainTable*. If the antenna is integrated to the CPE TRU, this MIB object shall be pre-populated by the manufacturer of the CPE. If the antenna is not integrated into the CPE TRU, the MIB object shall be populated by querying the AU through the interface defined in 9.12.2. The information at the antenna shall be pre-populated by the antenna manufacturer.

#### **7.14.2.3 CPE senses for and identifies WRAN services and incumbents**

The CPE shall perform spectrum sensing to detect the BS and to detect and identify legitimate incumbent services that are to be protected on each active WRAN channel in the area and its adjacent channels as described in 10.3.2.

#### **7.14.2.4 Present sensing results to the higher layers**

As a result of spectrum sensing, the available BSs in the area are presented to the application layer program via connection C2 and MIBs through M-SAP as shown in IEEE 802.22 reference architecture (Figure 7). The application may be running on the CPE or on an attached computer. The data presented includes the operating channel of the BS and RSSI in addition to the WRAN service being advertised.

#### **7.14.2.5 CPE chooses a WRAN service**

A WRAN service is selected at the higher layers of the CPE after preliminary sensing and identification of available BSs and the presence of incumbents in the area as the previous subclauses describe. The CPE SSA shall issue an M-WRAN-SERVICE-REPORT primitive to request the higher layers through the NCMS to select a channel from the available WRAN service list that is included in the primitive, as described in 10.7.4.1. The SSA shall receive an M-WRAN-SERVICE-RESPONSE primitive with the selected channel from the NCMS, as described in 10.7.4.3. Once the channel is selected, it and its adjacent channels are more rigorously sensed in order to detect the presence of a weak incumbent service that might be masked by the selected WRAN service. This procedure is described in more detail in 10.3.2.

#### **7.14.2.6 CPE performs satellite-based geolocation**

The CPE shall acquire geolocation data from a satellite-based geolocation receiver. A CPE shall not progress to the next step of initialization until the satellite-based geolocation technology successfully establishes lock and acquires valid geolocation data from the satellites. The CPE sends the NMEA string to the BS during registration (see 7.14.2.11).

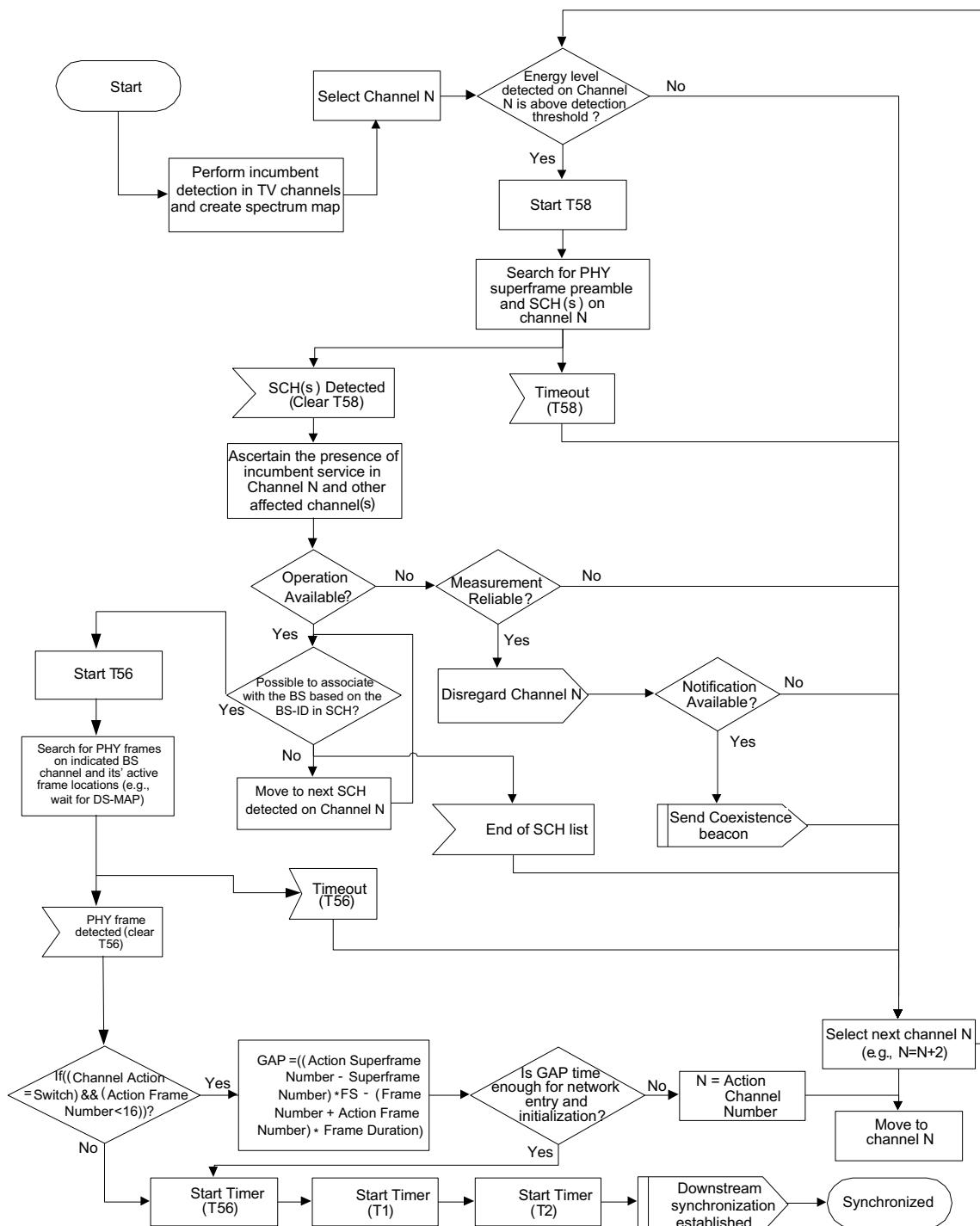
### 7.14.2.7 Acquire downstream and upstream parameters

#### 7.14.2.7.1 Obtaining downstream parameters

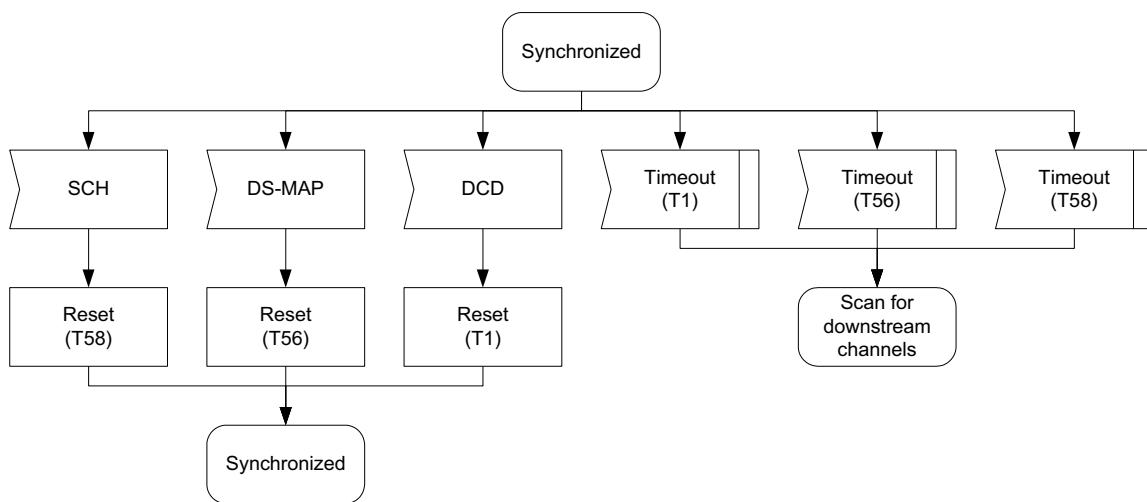
The MAC shall search for the SCH from the BS, which indicates the beginning of the superframe in normal mode, and the first allocated frame of the superframe in self-coexistence mode. To improve the joining latency, the CPE shall use energy detection to help ascertain about the presence/absence of an IEEE 802.22 BS in a particular channel. If the energy detected is below the detection threshold, the CPE can safely move to the next channel.

After having received an SCH in a channel, the CPE shall perform sensing not only in the set of channels indicated in the SCH, but also in all other affected channels. During this sensing, the CPE shall attempt to identify incumbent operation. If incumbents are detected on the operating channel or either first adjacent channel, the MAC shall cause the CPE to cease transmitting application traffic on the channel and, at the first transmit opportunity send a short control message to the BS indicating that it is using a channel occupied by an incumbent. In case the BS receives such notification, it may take numerous actions as described in Figure 96. The aggregate duration of the short control messages shall not exceed the Channel Closing Transmission Time (see Table 276) of transmissions by the WRAN system before remedying the interference condition (changing channels, backing off transmit EIRP, terminating transmissions, etc.).

Provided no incumbents are found, the CPE may proceed to the next step. Here, the MAC shall search for the DS-MAP MAC management messages. The CPE achieves MAC synchronization once it has received at least one DS-MAP message. A CPE MAC remains in synchronization as long as it continues to successfully receive the SCH, DS-MAP, and DCD messages for its channel(s). If the Lost DS-MAP Interval (Table 273) has elapsed without a valid DS-MAP message or the T1 interval (Table 273) has elapsed without a valid DCD message or Lost SCH counts of SCH are missed, a CPE shall try to re-establish synchronization. The process of acquiring synchronization is illustrated in Figure 35. The process of maintaining synchronization is illustrated in Figure 36.



**Figure 35 — Obtaining downstream parameters**



**Figure 36 — Maintaining downstream parameters**

#### 7.14.2.7.2 Obtaining upstream parameters

After synchronization, the CPE shall wait for a UCD message from the BS in order to retrieve a set of transmission parameters for a possible upstream channel. These messages are transmitted periodically from the BS for all available upstream channels and are addressed to the MAC broadcast address.

If no upstream channel can be found after a suitable timeout period, then the CPE shall continue scanning to find another downstream channel. The process of obtaining upstream parameters is illustrated in Figure 37.

The CPE shall determine from the channel description parameters whether it may use the upstream channel. If the channel is not suitable, then the CPE shall continue scanning to find another downstream channel. If the channel is suitable, the CPE shall extract the parameters for this upstream from the UCD. It then shall wait for the next DS-MAP message and extract the time synchronization from this message. Then, the CPE shall wait for a bandwidth allocation map for the selected channel. It may begin transmitting upstream in accordance with the MAC operation and the bandwidth allocation mechanism.

The CPE shall perform initial ranging at least once. If initial ranging is not successful, the procedure is restarted from scanning to find another downstream channel.

The CPE MAC is considered to have valid upstream parameters as long as it continues to successfully receive the SCH, US-MAP, and UCD messages. If at least one of these messages is not received within the time intervals specified in Table 273, the CPE shall not use the upstream. This is illustrated in Figure 38.

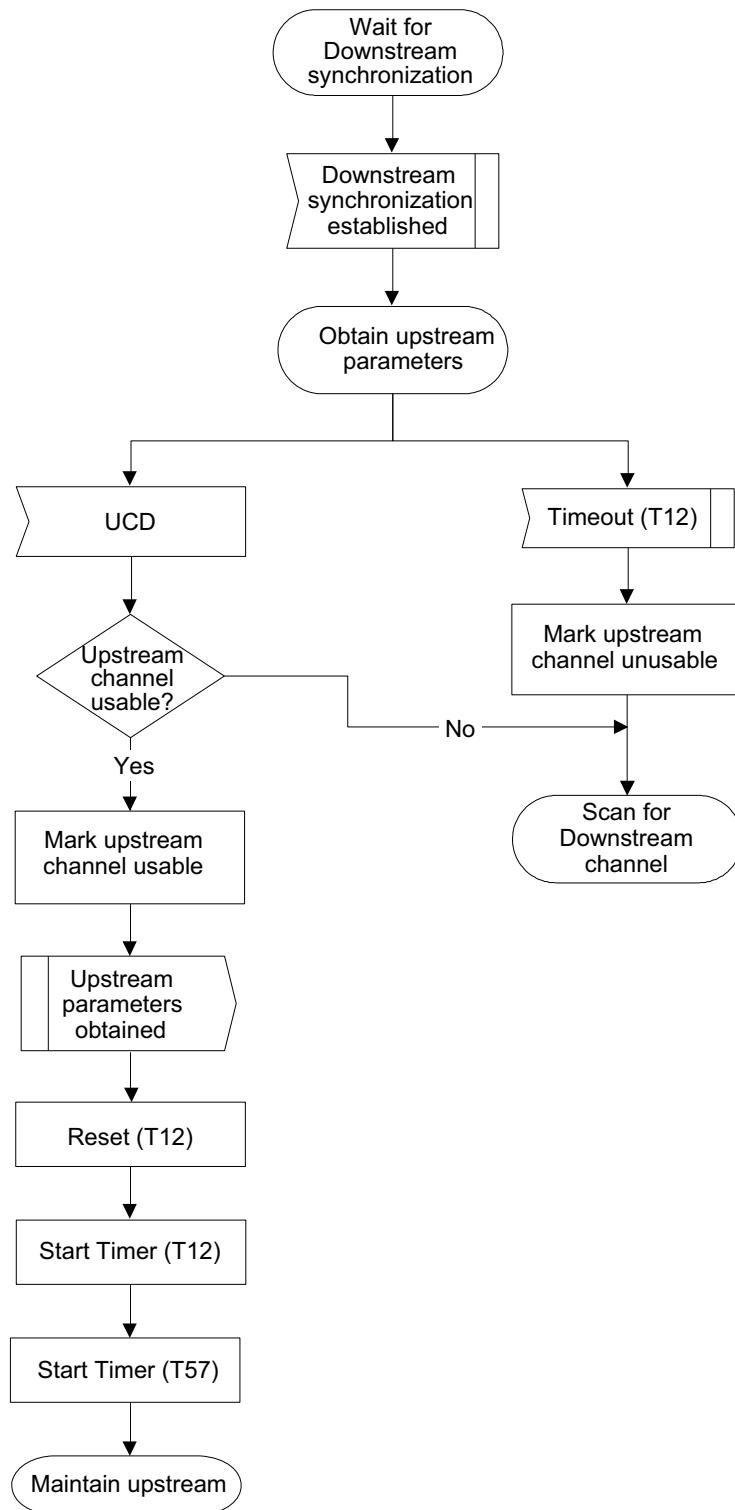
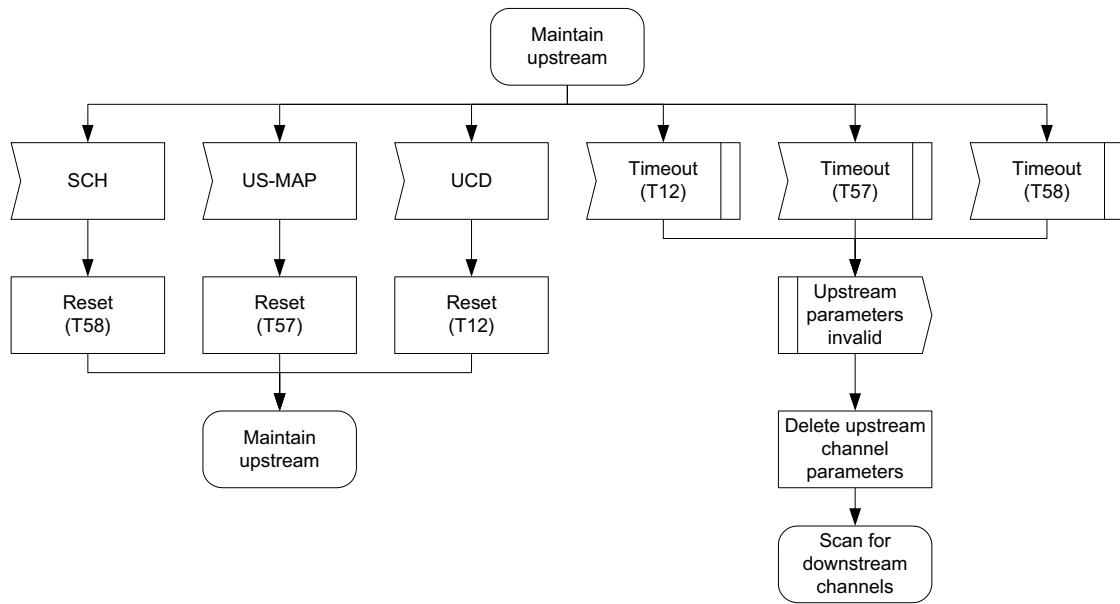


Figure 37 — Obtaining upstream parameters



**Figure 38 — Maintaining upstream parameters**

#### 7.14.2.8 CPE transmits ranging/CDMA burst

The selected channel is analyzed to determine if it passes the restrictions specified in 10.3.2. If the selected channel does not pass these restrictions, the association with the selected BS is unsuccessful and the selected channel shall be removed from further consideration. Available BSs are again presented to the higher layers for selection if there exist any other BSs with which to associate.

Next the selected channel and the channels that could be harmfully interfered by operation on this selected channel shall be more finely sensed as to determine if there exists a weak protected incumbent signal that was not detected at an earlier stage in the CPE initialization procedure. This process is described in 10.3.2.

Time in this subclause shall be referenced to two positions in space. One position will be that of the BS and the other position will be that of the CPE. Many such CPE positions will exist. Ranging is the process of acquiring the correct timing offset and EIRP adjustments such that the CPE's transmissions are aligned at the BS position. Ranging also adjusts transmit EIRP of the various CPEs such that the OFDMA signal received at the BS arrives with compatible amplitudes from all the CPEs. The timing delays through the PHY shall be constant to within 25% of the shortest symbol cyclic prefix as indicated in 9.9.1.

##### 7.14.2.8.1 CDMA initial ranging and automatic adjustments

First, a CPE shall synchronize to the downstream superframe and frame preamble. At this point, the CPE shall scan the US-MAP message to find an Initial Ranging Interval. The BS may allocate an Initial Ranging Interval consisting of one or more transmission opportunities. The CPE shall extract the number of initial ranging codes (see Table 31, element ID 150) from the UCD MAC management message.

The CPE randomly selects the CDMA code as described in 7.15.2.1 and sends the initial ranging CDMA code on the US allocation dedicated for that purpose. The BS receives the CDMA code. As many CPEs may contend for ranging, the CDMA code received may be the sum of many CPE transmissions. The BS isolates each of these transmissions and computes the ranging adjustments based on the relative time of

arrival of each CPE upstream burst, i.e., the timing offset, so that all these bursts arrive at the BS at the beginning of the symbol period within sufficient tolerance.

Ranging adjusts each CPE's timing offset such that each CPE appears to be co-located with the BS. The CPE shall set its initial timing offset to "zero advance" as if it was physically co-located with the BS. When the Initial Ranging transmission opportunity occurs, the CPE shall send a CDMA code. After reception and decoding of this CDMA code, the BS will react by sending a RNG-CMD MAC message in a following frame with the same CDMA code and indicate the timing advance that the CPE should use for its upstream transmissions (see Table 46) so that the beginning of its bursts is aligned with the center of the cyclic prefix within the tolerance indicated in 9.9.1.

When the Initial Ranging transmission opportunity occurs, the CPE shall send a CDMA code. Thus, the CPE sends the message as if it were co-located with the BS.

The CPE shall calculate the transmit EIRP per subcarrier for initial ranging,  $EIRP_{IR\_CPE}$ , from the following equation:

$$EIRP_{IR\_CPE} = EIRP_{BS} + RSS_{IR\_BS\_nom} - (RSS_{IR\_CPE} - GRX_{CPE}) + 10 \times \log(N_{IR\_sub}/1680)$$

where

$RSS_{IR\_BS\_nom}$  and  $EIRP_{BS}$  are defined in a DCD IE (see Table 23)

$GRX_{CPE}$  is the antenna gain at the CPE

$RSS_{IR\_CPE}$  is the RSSL measured by the CPE, which is then corrected by the CPE antenna gain to represent the RSSL for an isotropic antenna

$N_{IR\_sub}$  is the number of subcarriers used by the CPE for initial ranging

NOTE—The value of  $RSS_{IR\_BS\_nom}$  corresponds to the nominal signal strength that should be measured at the output of a 0 dBi gain receive antenna at the BS for normal operation. The  $EIRP_{BS}$  is the equivalent isotropic radiated power of the base station in the direction of the CPE, which would be computed for a simple single-antenna transmitter as  $P_{TX\_BS} + G_{TX\_BS}$ , where  $P_{TX\_BS}$  is the transmit power and  $G_{TX\_BS}$  is the BS transmit antenna gain in the direction of the CPE.<sup>14</sup>

The CPE shall send a CDMA code with a power level resulting in the  $EIRP_{IR\_CPE}$  per subcarrier. If the CPE does not receive a response after waiting at least one frame to allow processing at the BS, the CPE shall send a new CDMA code at the next appropriate Initial Ranging transmission opportunity with 1 dB higher power level. The CPE shall, however, stop increasing the power level at the following condition:

$$EIRP_{IR\_MAX} + 10 \times \log(N_{IR\_sub}) > EIRP_{CPE\_MAX}$$

where

$EIRP_{CPE\_MAX}$  is the upper bound in maximum transmitted EIRP for the CPE on the current operating channel as described in Table 108 of 7.7.11.3.2.1 or 4 Watt whichever is the smallest

$EIRP_{IR\_CPE\_MAX}$  is the upper bound for the increased  $EIRP_{IR\_CPE}$

If the CPE receives a RNG-CMD message containing the parameters of the code it has transmitted and the status "continue," it shall consider the transmission attempt unsuccessful but implement the corrections specified in the RNG-CMD and issue another CDMA code after the appropriate backoff delay. If the CPE receives an US-MAP containing a CDMA allocation IE with the parameters of the code it has transmitted,

---

<sup>14</sup> If the BS antenna is not omni-directional, this single  $EIRP_{BS}$  value provided in the DCD may at first sight not be sufficient but the process for calculating the initial ranging CPE EIRP level will be self-correcting. The actual EIRP towards the CPE would be reduced by the directivity of the transmit antenna in the direction of the CPE. As a result, the CPE will assume that the additional loss is due to the RF path and it will try to compensate for it by increasing its EIRP on the upstream. Such higher EIRP will then compensate for the receive antenna discrimination toward the CPE if the same directional antenna with the same azimuth is used for reception. This will result in the proper signal level reaching the BS receiver.

it shall consider the RNG-CMD reception successful, and proceed to send a unicast RNG-REQ (on Initial Ranging FID, allocated to Cell SID) on the allocated BW.

Once the BS has successfully received the RNG-REQ message, it shall return a RNG-CMD message using the initial ranging connection (see 12.2). Within the RNG-CMD message shall be the Station ID (SID) assigned to this CPE. The message shall also contain information on the required CPE EIRP level, offset frequency adjustment as well as the proper timing advance when needed. At this point the BS shall start using invited Initial Ranging Intervals addressed to the CPE's Basic FID to complete the ranging process, unless the status of the RNG-CMD message is "success," in which case the initial ranging procedure shall end.

If the status of the RNG-CMD message is "continue," the CPE shall wait for an individual Initial Ranging Interval assigned to its Basic FID. Using this interval, the CPE shall transmit another RNG-REQ message using the Basic FID along with any power level and timing offset corrections.

The BS shall return another RNG-CMD message to the CPE with any additional fine-tuning required. The ranging request/response steps shall be repeated until the response contains a "Ranging Successful" notification or the BS aborts ranging. Once successfully ranged (timing, frequency and EIRP are within tolerance at the BS), the CPE shall join normal data traffic in the upstream. In particular, the retry counts and timer values for the ranging process are defined in Table 273.

NOTE 1—The burst profile to use for any upstream transmission is defined by the Upstream Interval Usage Code (UIUC). Each UIUC is mapped to a burst profile in the UCD message.

NOTE 2—The BS shall allow the CPE sufficient time to have processed the previous RNG-CMD (i.e., to modify the transmitter parameters) before sending the CPE a specific ranging opportunity. This is defined as CPE Ranging Response Processing Time in Table 273.

On receiving a RNG-CMD instruction to move to a new channel during initial ranging, the CPE shall obtain a new SID via initial ranging and registration.

It is possible that the RNG-CMD may be lost after transmission by the BS. The CPE shall recover by timing out and reissuing its Initial RNG-REQ. Since the CPE is uniquely identified by the source MAC address in the Ranging Request, the BS may immediately reuse the SID previously assigned. If the BS assigns a new SID, it shall immediately age out the old SID and associated CPE.

#### **7.14.2.8.2 Ranging parameter adjustment**

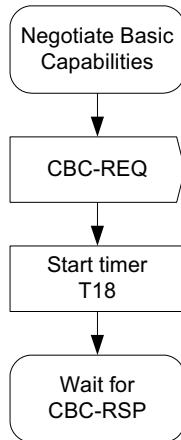
Adjustment of local parameters (e.g., transmit EIRP) in a CPE as a result of the receipt or non-receipt of a RNG-CMD message is considered to be implementation-dependent with the following restrictions:

- a) All parameters shall be within the approved range at all times.
- b) EIRP adjustment shall start from the initial value selected with the algorithm described in 7.14.2.8.1 unless a valid EIRP setting is available from non-volatile storage, in which case this value may be used as the starting point.
- c) EIRP adjustment shall be capable of being reduced or increased by the specified amount in response to the RNG-CMD messages.
- d) If, during initialization, EIRP is increased to the maximum value as determined in 7.14.2.8.1 without a response from the BS, it shall go back to the minimum EIRP and ramp up to its maximum EIRP four (4) times before aborting the ranging process with this base station.

On receiving a RNG-CMD message, the CPE shall not transmit until the RF signal has been adjusted in accordance with the RNG-CMD and has stabilized.

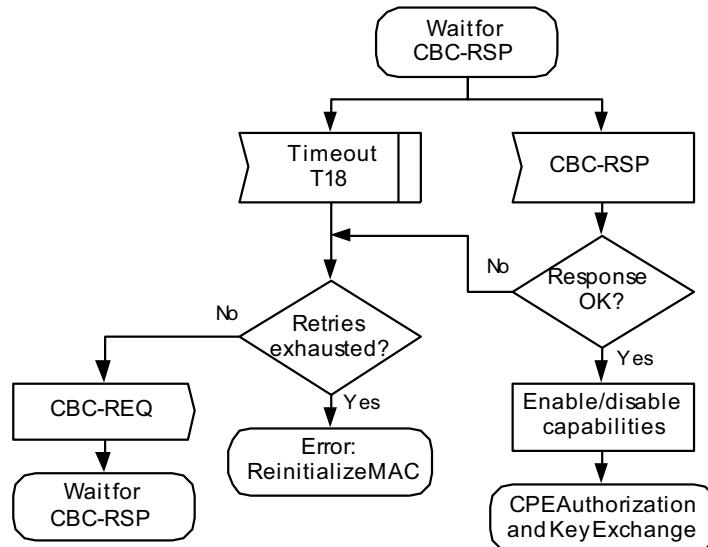
### 7.14.2.9 CPE transmit basic capabilities

Immediately following the completion of initial ranging, the CPE informs the BS of its basic capabilities by transmitting a CBC-REQ message (see Table 105) with its capabilities set to “on” (see Figure 39). Note that T18 is a timer used to wait for CBC-RSP timeout and the default value is indicated in Table 272.

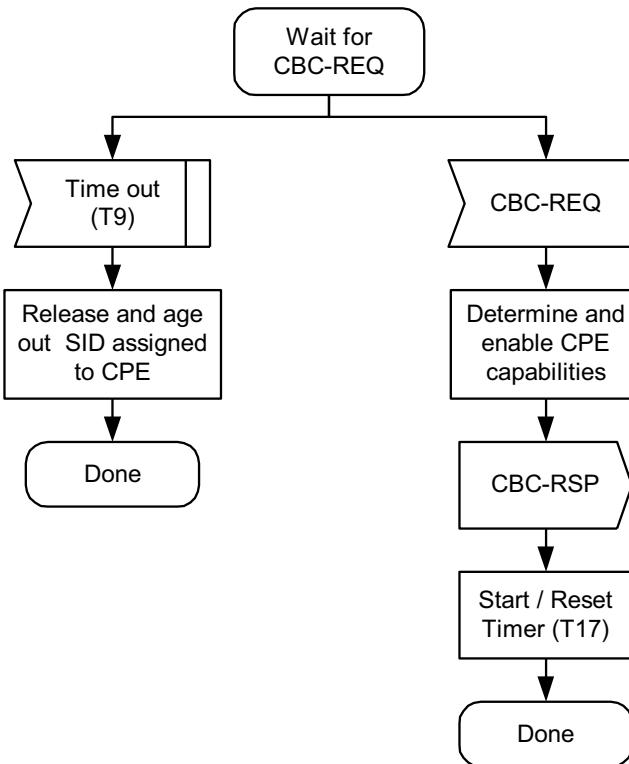


**Figure 39 — Negotiate basic capabilities – CPE**

The BS responds with a CBC-RSP message (see Table 106) with the intersection of the CPE’s and BS’s capabilities set to “on” (see Figure 40 and Figure 41, respectively). The timer T9 refers to the time allowed between the BS sending a RNG-CMD to a CPE, and receiving a CBC-REQ from that same CPE, and the minimum value is specified in Table 272. Note that the CPE capability information is presented in 7.7.7.3.4. When T9 expires, the SID assigned during ranging shall be aged out and the CPE shall have to attempt ranging process over again while not exceeding the maximum number of CDMA ranging retries indicated in Table 273.



**Figure 40 — Wait for CBC-RSP at CPE**



**Figure 41 — Negotiate basic capabilities at BS**

#### 7.14.2.10 CPE authentication and key exchange

Once configuration of the required basic capabilities is completed, the CPE and AAA continue with performing authentication and exchanging keys, as described in Clause 8. If the AAA and CPE can not authenticate each other, authentication of the CPE fails for the selected WRAN service. This WRAN service on the selected channel is removed from further consideration. If there are any other BSs available with which to associate, the updated list of available WRAN services is presented to the higher user layers.

#### 7.14.2.11 Registration

Registration is the process by which the CPE verifies its configuration with the BS. If the CPE supports a configuration that is set by the BS, it is allowed entry into the network and thus becomes manageable. To register with a BS, the CPE shall send a REG-REQ message to the BS. The REG-REQ message shall include a CPE NMEA Location string IE.

During registration, the CPE's NMEA Location String and various operational parameters are configured (see 7.7.7.3). The CPE sends its location data string (see 7.6.1.3.1.6) upon initial registration and re-registration. When the IP Address Allocation Information Element (see 7.7.7.3.4.11) is present in the REG-REQ message, the BS shall include this IP address allocation parameter in the REG-RSP message to command the CPE to use the indicated version of IP on the secondary management connection. The BS shall command the use of exactly one of the IP versions supported by the CPE.

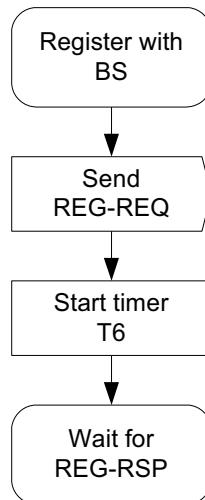
The BS shall determine the location of the antenna of each associated CPE with the accuracy as specified in Table A.9 for the specific regulatory domain. The BS's SM shall receive the generated NMEA string and validate its contents.

The BS's SM shall provide the geolocation data to the database service. The BS shall refuse to serve the CPE if

- The geographic location of the CPE has not been successfully determined as indicated by a failed validation of the data in the NMEA string. Validation shall fail if
  - a) The NMEA string contains data that is outside the allowable range of values or;
  - b) The distance between the initializing CPE and the BS or other associated CPEs is outside the allowable range of values.
- The database service has indicated that the CPE cannot operate on the channel on which the WRAN network intends to operate.

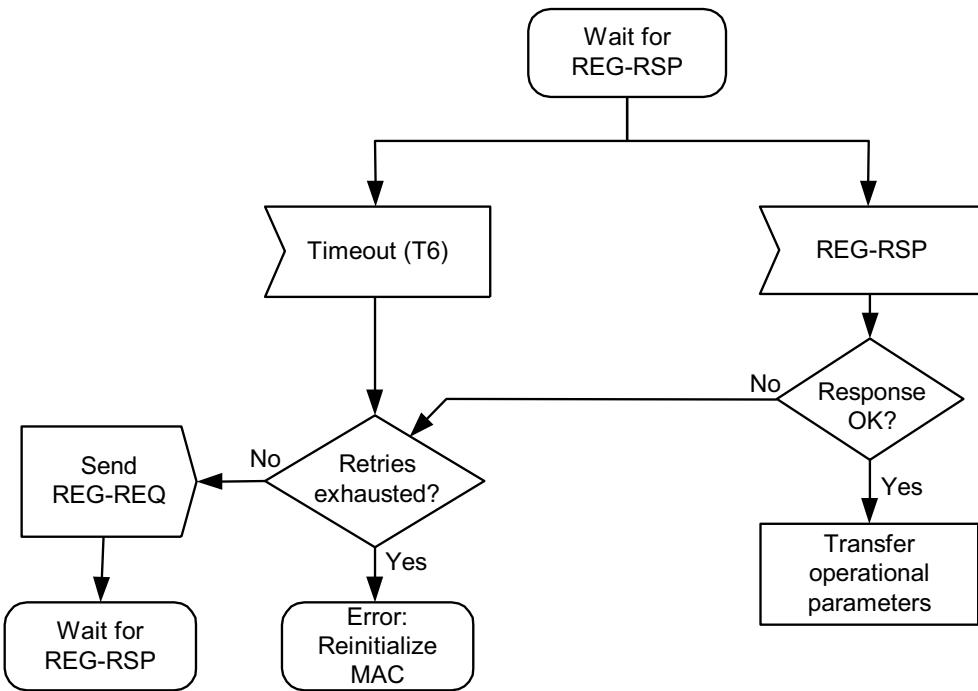
In the first case, validation of the NMEA string fails and CPE initialization fails, in the second case, the CPE initialization fails on the current channel and shall proceed to the next channel on its available WRAN services list.

The BS shall respond with a REG-RSP message. The REG-RSP message shall include the Permanent Station ID (see Table 61), if CPE Privacy (see 8.7) is enabled. Figure 42 shows the procedure that shall be followed by the CPE to initiate registration.



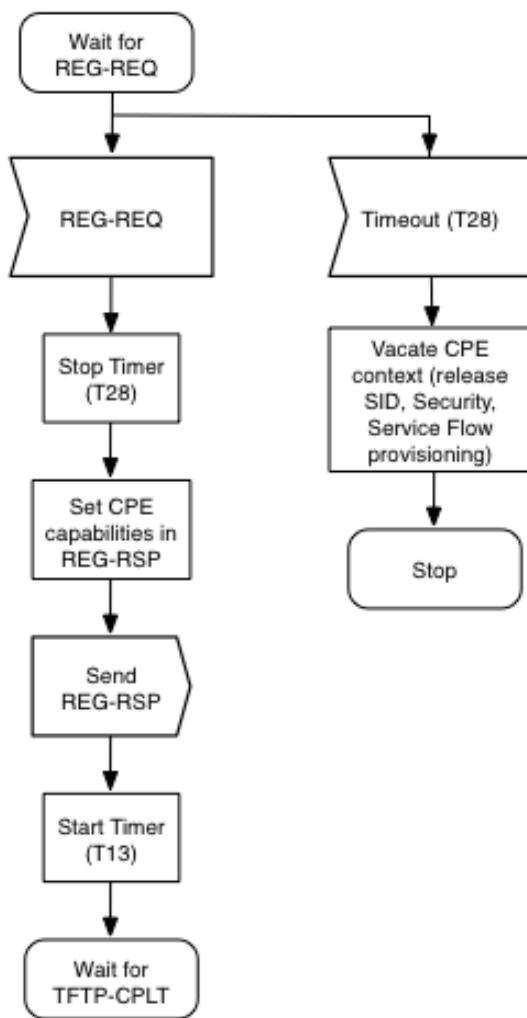
**Figure 42 — CPE registration**

Once the CPE has sent a REG-REQ to the BS, it shall wait for a REG-RSP to authorize it to forward traffic to the network. Figure 43 shows the waiting procedure that shall be followed by the CPE.



**Figure 43 — Wait for REG-RSP—CPE**

The BS shall perform the operations shown in Figure 44. Note that the Timer T13 represents the time allowed for a CPE, following receipt of a REG-RSP message, to send a TFTP-CPLT message to the BS, and its minimum time is specified in Table 272. In addition, the Timer T28 is the time allowed for the BS to complete the transmission of channel sets; its default value is specified in Table 272.



**Figure 44 — Registration at BS**

IEEE 802.22 CPEs are managed devices. Network entry is not considered complete until after the TFTP-CPLT/RSP (see 7.7.19). When the BS and CPE complete the TFTP-CPLT/RSP exchange, timer T30 is scheduled for the value set in CPE Registration Timer ( 7.7.7.3.5 ) IE. When T30 expires the BS and CPE shall delete all information pertaining to their associations (e.g., SIDs, registered capabilities, active service-flow parameters, remaining security context), regardless of whether or not the CPE is currently being served by the BS.

Prior to expiration of T30, the BS may attempt to verify connectivity to a CPE via periodic ranging. This can be facilitated by the BS sending an unsolicited RNG-CMD message with Ranging Status field set to “Re-range & Re-register” (see Table 44). Upon receiving said RNG-CMD, the CPE shall attempt to re-range with the BS, as well as send a REG-REQ with the current configuration of the CPE NMEA Location String IE (7.6.1.3.1.6) and Manufacturer-specific Antenna Model IE (7.7.7.3.4.8) to inform the BS of its current position and antenna information. Upon sending this REG-REQ to the BS, the CPE should use the signaling in 9.12.2 to re-populate the MIBs used to configure these IEs (see *wranIfCpeAntennaGainTable* and *wranIfAntennaModel* in 13.1) and update the configuration of these IEs by reading the information. If the CPE finds out that this information has changed, it shall re-initialize itself. If the BS does not receive

either the RNG-REQ or the REG-REQ (with the location information) from the CPE in the allocated opportunity, the BS shall wait until T30 expires before de-registering the CPE.

If the CPE is currently being served by the BS, the BS can force the CPE to delete the pertinent information before expiration of T30 by the following:

- a) Send a DREG-CMD to CPE with Action Code = 0x04 (see Table 115) to shutdown the CPE. This is done if the BS detects that the CPE has moved outside the current coverage area of the BS and is not able to service it.
- b) Send a DREG-CMD to CPE with Action Code = 0x05 (see Table 115) to force CPE to reinitialize on the current operating channel. This is done if the CPE's movement is beyond the movement threshold of  $\pm 25$  m (see policy 8 in Table 234), but the CPE's movement does not result in a new backup/candidate channel list upon query of the database service.
- c) Send a DREG-CMD to the CPE with Action Code = 0x01 and subsequently another DREG-CMD with Action Code = 0x03 (see Table 115) to temporarily disable the CPE's transmission. This is done, to temporarily disable the CPE's transmission when a CPE's movement is within the movement threshold of  $\pm 25$  m (see Policy 8 in Table 234), but the CPE's movement does not result in a new backup/candidate channel list upon query of the database service. This avoids having to reinitialize the CPE.

For case a), T30 shall be cleared when the CPE is shutdown. For case b), the T30 shall be reset upon completion of re-registration. For case c), the T30 shall be reset upon sending the DREG-CMD to re-enable CPE.

If the SM (upon interrogating the SSA) detected that the CPE has moved, the BS shall request de-registration by sending a DREG-CMD message to the CPE set with the appropriate Action Code as mentioned above.

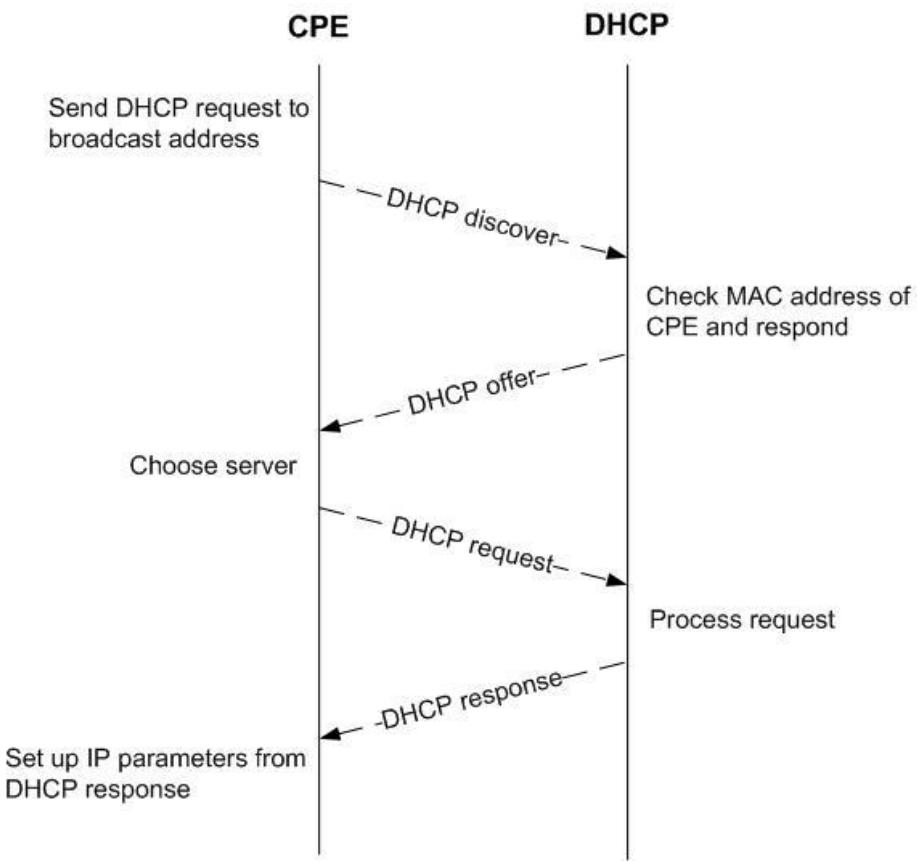
#### **7.14.2.12 BS transmit channel sets to CPE**

The BS shall send the channel sets to the new CPE. The channel sets are described in 10.2.3. The channel sets that are sent to the initializing CPE are the backup channels and the candidate channels. The channel sets are sent in a DCD message, as described in 7.7.1 and in Table 24 to Table 26. The BS shall send DCD channel information elements 11 and 12. Table 26 describes information element 12 as the backup and candidate channel list. It is a prioritized list of the channels with the backup channel set higher in priority than the candidate channel set. The two sets are identified by sending information element 11, which provides the number of the higher prioritized backup channel set. Each channel in DCD information element 12 is characterized by both the channel number.

#### **7.14.2.13 Establish IP connectivity**

The CPE shall invoke DHCP mechanism (IETF RFC 2131 [B20]) in order to obtain an IP address and any other parameters needed to establish IP connectivity. If the CPE has a configuration file, the DHCP response shall contain the name of a file that contains further configuration parameters.

Establishment of IP connectivity shall be performed on the CPE's secondary management connection as shown in Figure 45.

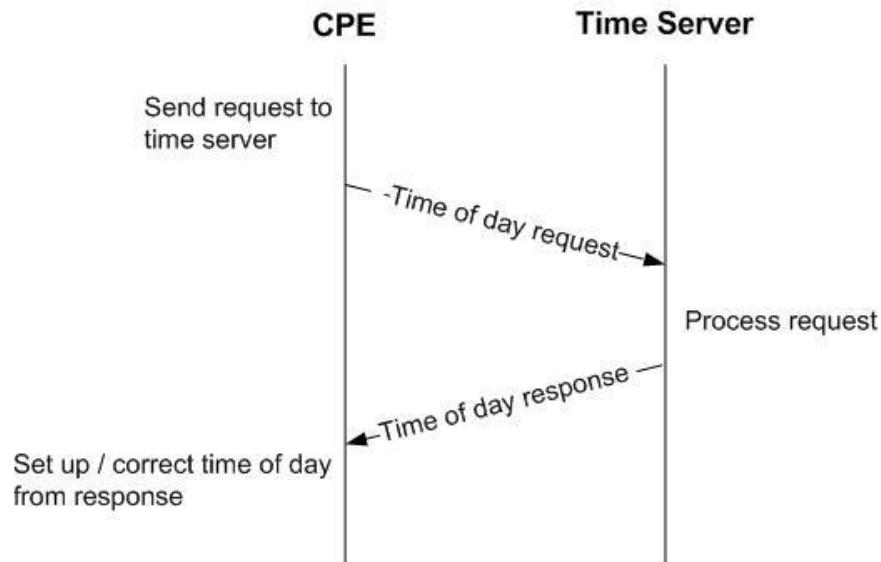


**Figure 45 — Establishing IP connectivity**

In case where dynamic IP configuration is not preferred, the CPE shall obtain an IP address from its base station.

#### 7.14.2.14 Establish time of day

The CPE and BS need to have the current date and time. This is required for time-stamping logged events for retrieval by the management system. This needs not be authenticated and needs to be accurate only to the nearest second. The current date and time may be obtained from a local time source or a remote service such as an NTP server.

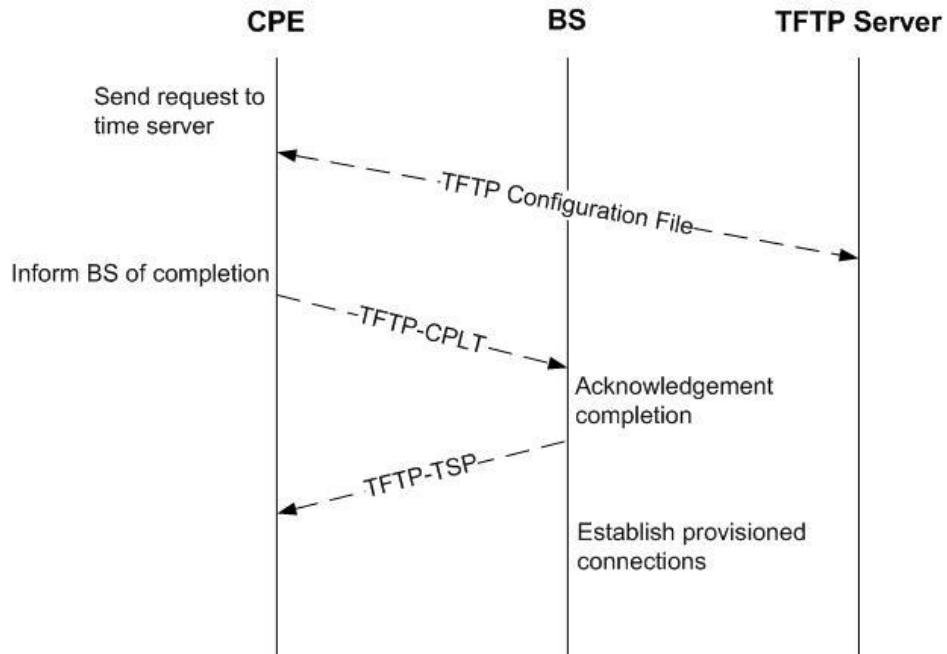


**Figure 46 — Establishing time of day**

Successfully acquiring the Time of Day is not mandatory for a successful registration, but is necessary for ongoing operation. The specific timeout for Time of Day Requests is implementation dependent.

#### 7.14.2.15 Transfer operational parameters

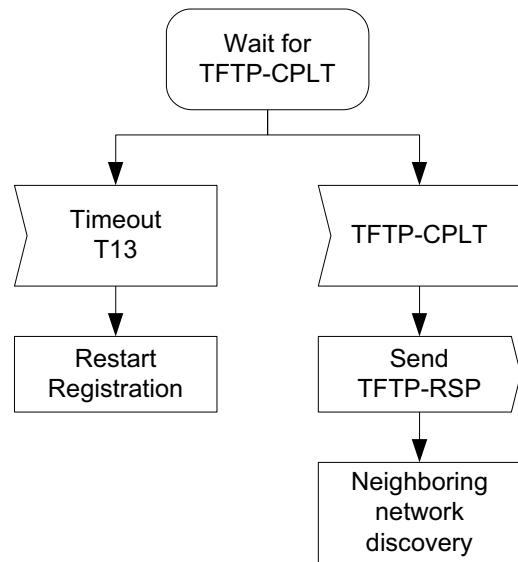
The CPE shall download the CPE's configuration file using TFTP on its own secondary management connection as shown in Figure 47. The CPE shall use an adaptive timeout for TFTP based on binary exponential backoff (IETF RFC 1123 [B19], IETF RFC 2349 [B21]).



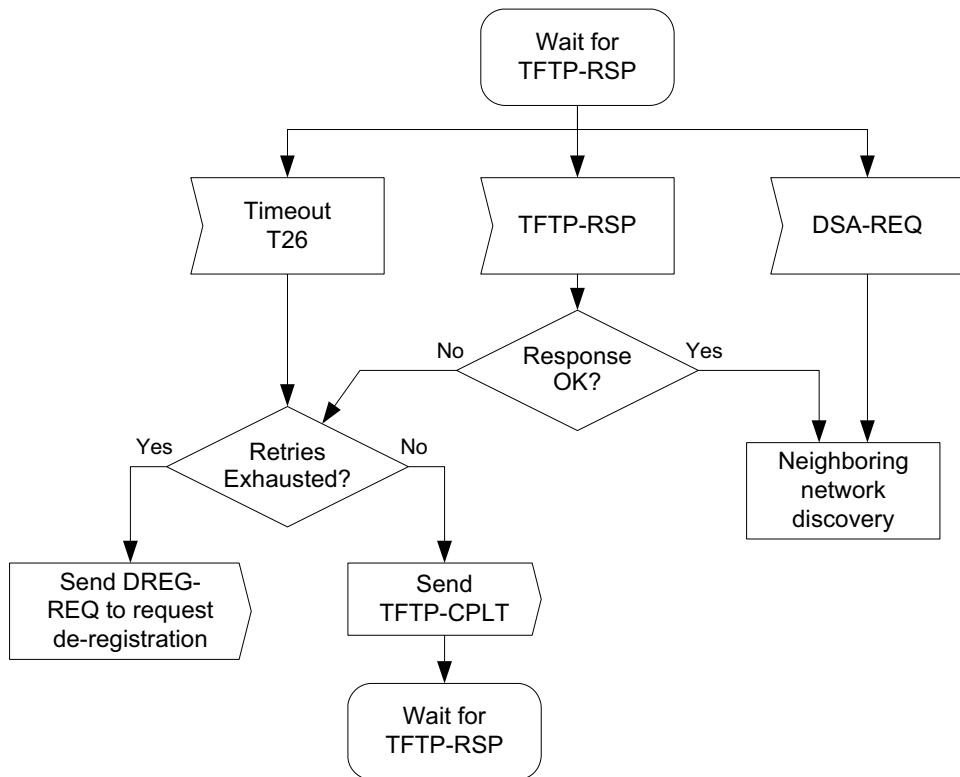
**Figure 47 — Transferring operational parameters**

When the configuration file download has completed successfully, the CPE shall notify the BS by transmitting the TFTP-CPLT message on the CPE's primary management connection. Transmissions shall continue successfully until a TFTP-RSP message is received with response "OK" from the BS (see Figure 48 and Figure 49) or the CPE terminates retransmission due to retry exhaustion.

Upon sending a REG-RSP, the BS shall wait for a TFTP-CPLT. If the timer T13 (defined in Table 272) expires, the BS shall restart the registration process (REG-REQ/RSP) with the CPE (see Figure 48). Note that the Timer T26 refers to the time waited for TFTP-RSP. If T26 expires, then TFTP-CPLT is attempted until the maximum number of retries is exhausted. Upon the exhaustion, the CPE shall be deregistered (i.e., forced to reinitialize MAC) by sending a DREG-REQ with Action Code set to 0x05 to force itself to reattempt system access or 0x04 to shut itself down (see Figure 49).



**Figure 48 — Wait for TFTP-CPLT at the BS**



**Figure 49 — Wait for TFTP-RSP at the CPE**

#### 7.14.2.16 Establish dynamic service flows

After the transfer of operational parameters for the CPE, the BS shall send DSA-REQ messages (Table 64) to the CPE to set up pre-provisioned service flows belonging to the CPE. The CPE responds with DSA-RSP messages. This is described further in 7.18.7.1.

#### 7.14.2.17 Neighboring network discovery

After a CPE has registered with a WRAN BS, it shall perform neighboring network discovery in order to identify other nearby WRANs and enable efficient self-coexistence, if the CPE has not already done so. The neighboring network discovery involves listening to the medium for CBP packets or BS SCH transmitted by other WRAN BSs. This network discovery mechanism is described in 7.20.1.3.

### 7.15 Ranging

To deal with the large propagation delays and varying RF signal quality between CPEs and the BS, the MAC incorporates a *ranging* procedure. Ranging is a collection of processes by which the CPE and BS maintain synchronization as well as quality of the RF communication link between them. Distinct processes are used for managing downstream and upstream.

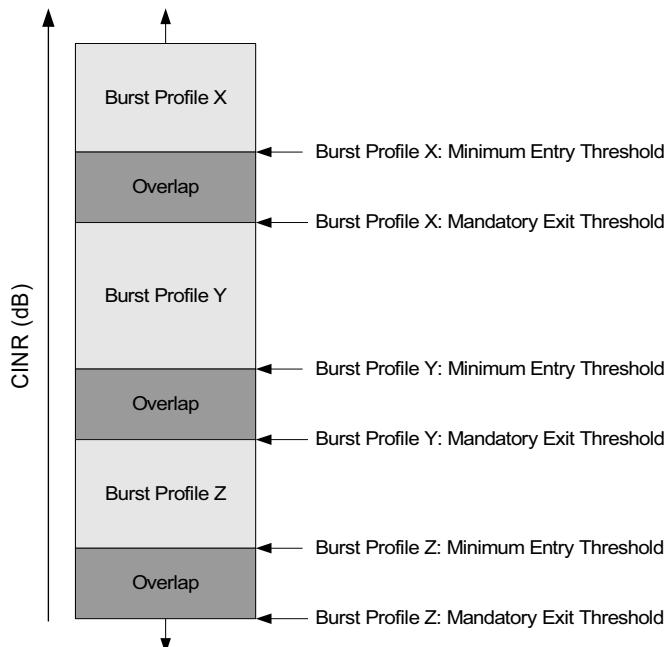
#### 7.15.1 Downstream management

To maintain efficient operation between the BS and CPEs, the downstream burst profile is determined by the BS according to the quality of the signal that is received by each CPE. To reduce the volume of

upstream traffic, the CPE monitors the CINR and compares the average value against the allowed range of operation. As shown in Figure 50, threshold levels bound this region. These thresholds parameters are specified in the DCD message, and shall be used by CPEs to determine their optimal burst profile. If the received CINR falls outside of the allowed operating region as determined by the threshold parameters, the CPE requests a change to a new burst profile using one of the following two methods:

- If the CPE has been granted upstream bandwidth (a data grant allocation to the CPE's Basic FID), the CPE shall send a RNG-REQ message in that allocation. The BS responds with a RNG-CMD message.
- If a grant is not available and the CPE requires a more robust burst profile on the downstream, the CPE shall send a RNG-REQ message in an Initial Ranging interval.

In either of these methods, the message is sent using the CPE's Basic FID. The coordination of message transmission and reception relative to actual change of modulation is different depending upon whether a CPE is transitioning to a more or less robust burst profile. Figure 51 shows the case where a CPE is transitioning to a more robust profile, while Figure 52 illustrates the transition to a less robust profile.



**Figure 50 — Burst profiles and threshold utilization**

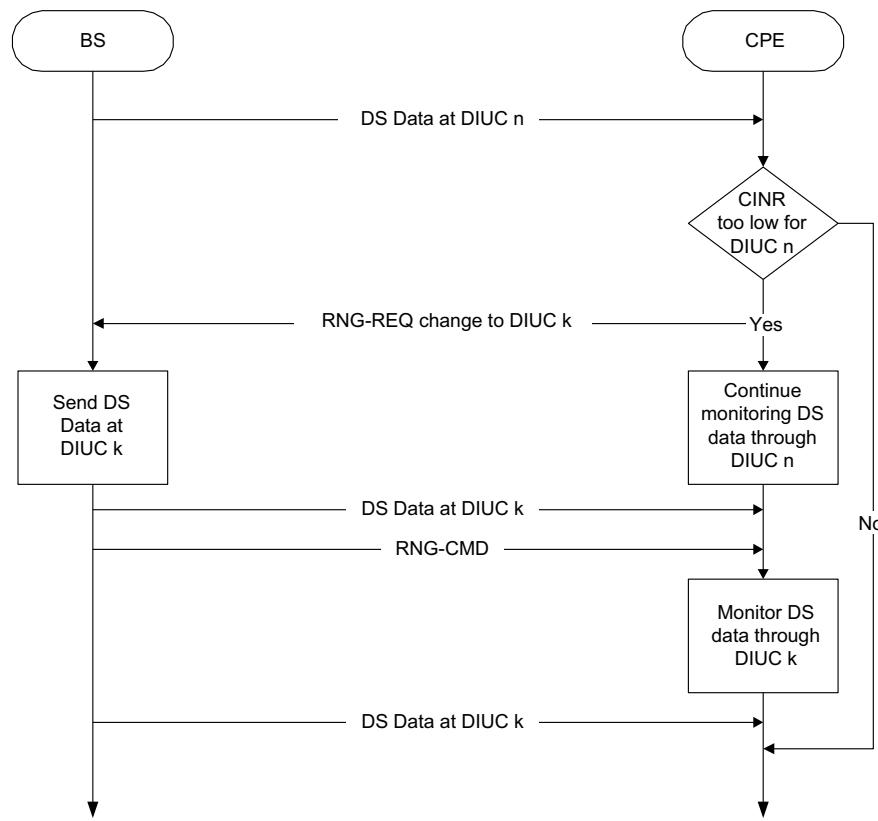
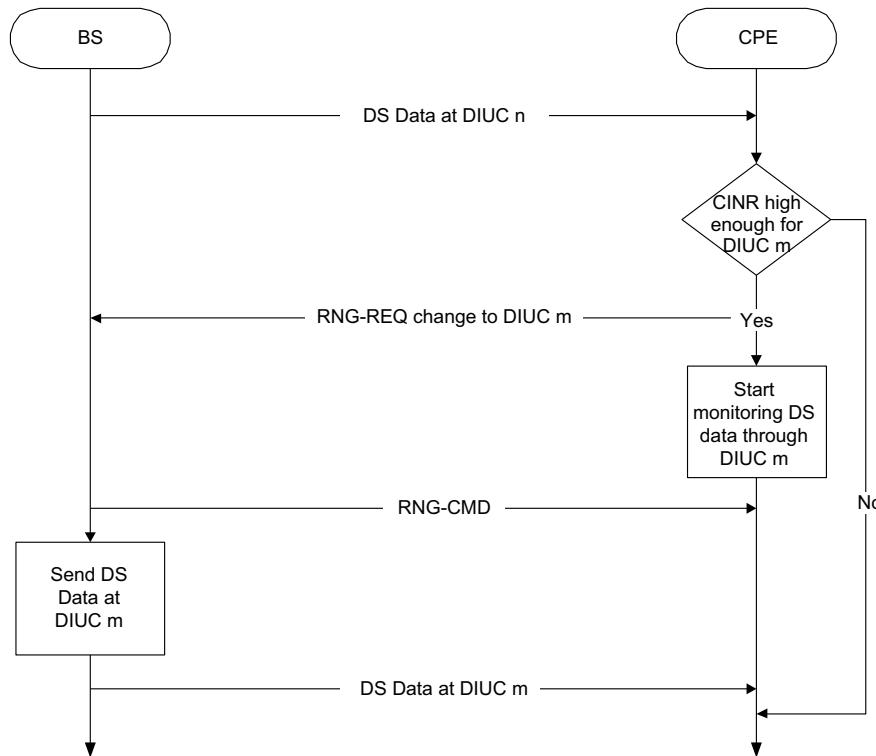


Figure 51 — Change to a more robust profile



**Figure 52 — Change to a less robust profile**

### 7.15.2 Upstream management

Upstream ranging management consists of two procedures: initial ranging and periodic ranging. Initial ranging (see 7.14) allows a CPE joining the network to acquire correct transmission parameters, such as time offset and Tx EIRP level, so that the CPE can communicate with the BS. The WRAN PHY specifies a ranging subchannel and a set of special pseudo-noise ranging codes. Subsets of codes shall be allocated in the UCD channel encoding for initial ranging, periodic ranging requests, and BRs so that the BS can determine the purpose of the received code by the subset to which the code belongs. CPEs that wish to perform one of the aforementioned operations shall select, with equal probability, one of the codes of the appropriate subset, modulate it onto the ranging subchannel, and subsequently transmit in the ranging slot selected with equal probability from the available ranging slots on the upstream subframe. A CPE shall select one Ranging Slot from all available ranging slots in the upstream frame using a uniform random process. Details on the modulation and ranging codes are specified in 9.9.2. Following initial ranging, periodic ranging allows the CPE to adjust transmission parameters so that it can maintain upstream communications with the BS.

The following subclauses summarize the general algorithm for initial ranging and periodic ranging.

#### 7.15.2.1 CDMA initial ranging and automatic adjustments

A CPE that wishes to perform initial ranging with CDMA code shall take the following steps:

- a) The CPE, after acquiring downlink synchronization and uplink transmission parameters, shall select one Ranging Slot using the random backoff. The random backoff shall use a binary truncated exponent algorithm. After selecting the Ranging Slot, the CPE shall choose a Ranging Code (from the Initial Ranging domain) using a uniform random process. The selected Ranging Code is sent to the BS (as a CDMA code) in the selected Ranging Slot.
- b) The BS cannot tell which CPE sent the CDMA ranging request; therefore, upon successfully receiving a CDMA ranging code, the BS broadcasts a ranging response message that advertises the received ranging code as well as the ranging slot (OFDMA symbol number, etc.) where the CDMA ranging code has been identified. This information is used by the CPE that sent the CDMA ranging code to identify the ranging response message that corresponds to its ranging request. The ranging response message contains all the needed adjustments (e.g., time, EIRP, and possibly frequency corrections) and a status notification.
- c) Upon receiving a ranging response message with the “Continue” status, the CPE shall continue the ranging process as done on the first entry (using random selection rather than random backoff) with ranging codes randomly chosen from the initial ranging domain sent on the ranging slots.
- d) When the BS receives an initial-ranging CDMA code that requires no corrections, the BS shall provide BW allocation for the CPE using the CDMA\_Allocation\_IE to send an RNG-REQ message. Sending the RNG-CMD message with status “Success” is optional.
- e) The initial ranging process is over after receiving RNG-CMD message, which includes a valid SID (following a RNG-REQ transmission on a CDMA Allocation IE). If this RNG-CMD message includes a “continue” indication, the ranging process should be continued using the ranging mechanism.
- f) The timeout required for the CPE to wait for RNG-CMD, following or not following a CDMA Allocation IE, is defined by the timer T3.

### 7.15.2.2 CDMA Periodic ranging and automatic adjustments

The following summarizes the general algorithm for CDMA periodic ranging:

- a) The CPE shall choose randomly a Ranging Slot (with random selection with equal probability from available Ranging Slots in a single frame) at the time to perform the ranging, and then it chooses randomly a Periodic Ranging Code and sends it to the BS (as a CDMA code).
- b) If the CPE does not receive a response, the CPE may send a new CDMA code at the next appropriate ranging transmission opportunity at one step higher EIRP level.
- c) The BS cannot tell which CPE sent the CDMA ranging request; therefore, upon successfully receiving a CDMA periodic ranging code, the BS broadcasts a ranging response message that advertises the received periodic ranging code as well as the ranging slot (OFDMA symbol number, etc.) where the CDMA periodic ranging code has been identified. This information is used by the CPE that sent the CDMA periodic ranging code to identify the ranging response message that corresponds to its ranging request. The ranging response message contains all the needed adjustments (e.g., time, EIRP, and possibly frequency corrections) and a status notification.
- d) Upon receiving a Ranging Response message with the “Continue” status, the CPE shall continue the ranging process with further periodic ranging codes randomly chosen. Upon receiving an RNG-CMD message with success status, the CPE shall restart timer T4 with the appropriate value depending whether the CPE is fixed or portable (see Table 273).
- e) The BS may send an unsolicited RNG-CMD as a response to a CDMA-based bandwidth-request or any other data transmission from the CPE.

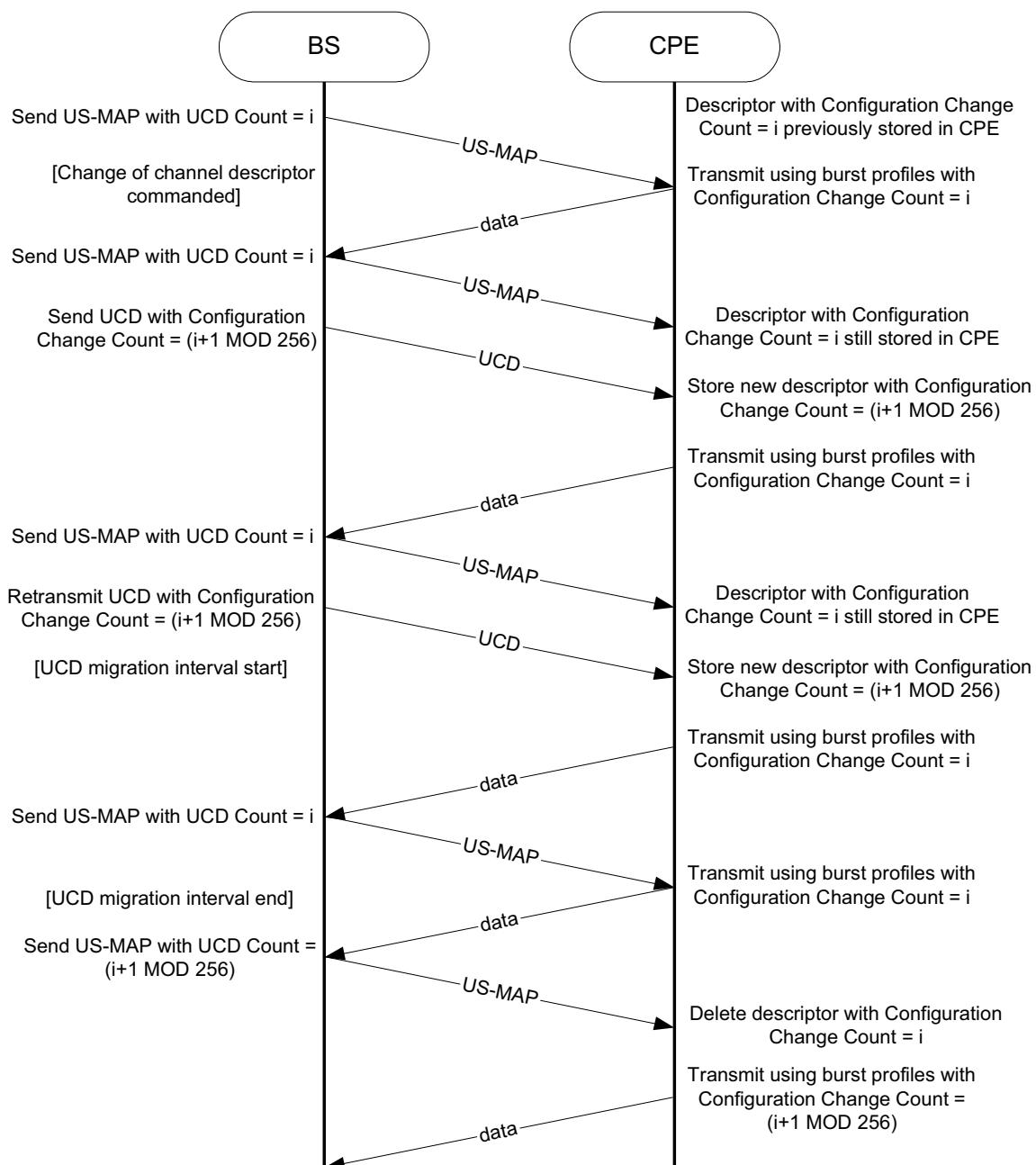
- f) Upon timeout of the CPE internal T4 timer, the CPE shall perform Periodic Ranging according to the procedure above.
- g) When the CPE receives an unsolicited RNG-CMD message, it shall reset the periodic ranging timer and adjust the parameters (timing, EIRP, etc.) as notified in the RNG-CMD message.

## 7.16 Channel descriptor management

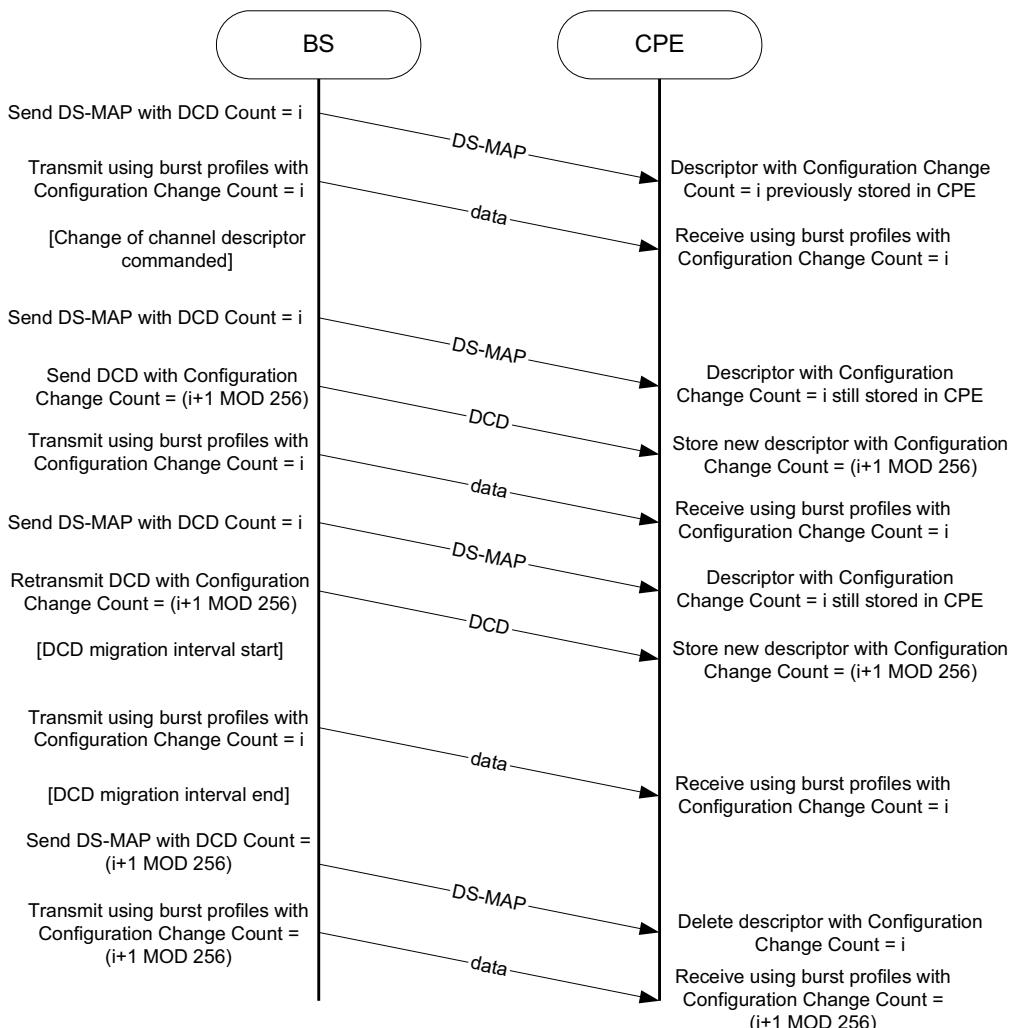
As previously presented, channel descriptor messages (i.e., DCD and UCD) are broadcast by the BS to all CPEs at periodic intervals. Among other things, these channel descriptors define burst profiles, which are used by US-MAP and DS-MAP messages for allocating upstream and downstream transmissions, respectively. Once broadcast by the BS and received by associated CPEs, a given channel descriptor shall remain valid until a new channel descriptor message with a different value for the Configuration Change Count field, is again broadcast by the BS. When this happens, this new channel descriptor shall overwrite all the information of the previous descriptor.

Once channel descriptors are known to all CPEs in an IEEE 802.22 cell, the BS shall set the UCD/DCD Count value, contained in US-MAP and DS-MAP messages, equal to the Configuration Change Count of the desired channel descriptor. This way, a BS can easily indicate to the CPEs which burst profile is to be used for a given allocation, and hence provide high flexibility to the BS in controlling which burst profile to use at any given time by simply changing the UCD/DCD Count value.

Figure 53 describes the procedure to migrate from one upstream channel descriptor to the next, while Figure 54 focuses on the same procedure but for the downstream channel.



**Figure 53 — UCD channel descriptor update**



**Figure 54 — DCD channel descriptor update**

Finally, note that the Configuration Change Count shall be incremented by 1 modulo 256 for every new migration of channel descriptor. After issuing a DS-MAP or US-MAP message with the Configuration Change Count equal to that of the new generation, the old channel descriptor ceases to exist and the BS shall not refer to it anymore. When migrating from one generation to the next, the BS shall schedule the transmissions of the UCD and DCD messages in such a way that each CPE has the possibility to successfully hear it at least once.

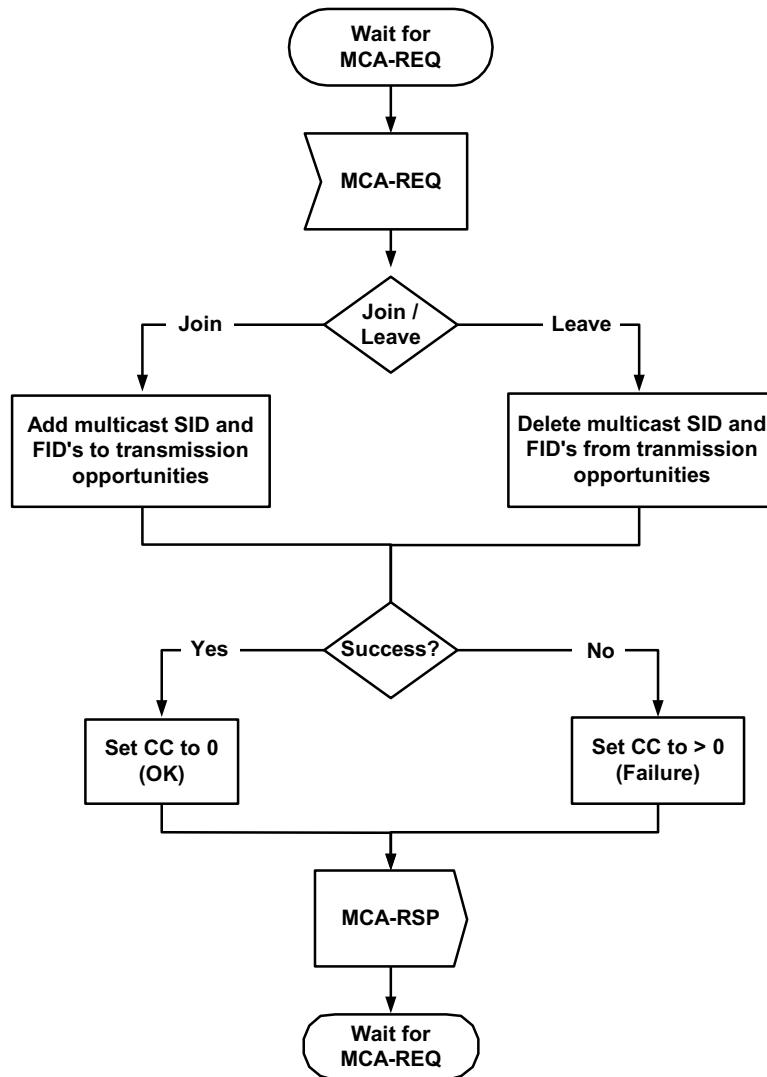
## 7.17 Multicast support

Multicast support is an important and integral part of the MAC. In the MAC, multicast groups are used not only for their traditional application of data delivery (e.g., streaming), but also for sending management commands to a set of CPEs. For example, the BS may wish to implement clustering algorithms for measurements and use the feature of multicast group to create such clusters. In this case, the BS could, for instance, simultaneously address a set of CPEs and share the load of measurements across clusters. That is, the BS could make certain clusters responsible for DTV measurements while other clusters would target Part 74 services. Another possible use of multicast connections is for CBP (see 7.20.1). In this case, the BS can maximize the use of the self-coexistence IUC by properly selecting the CPEs who will transmit CBP packets.

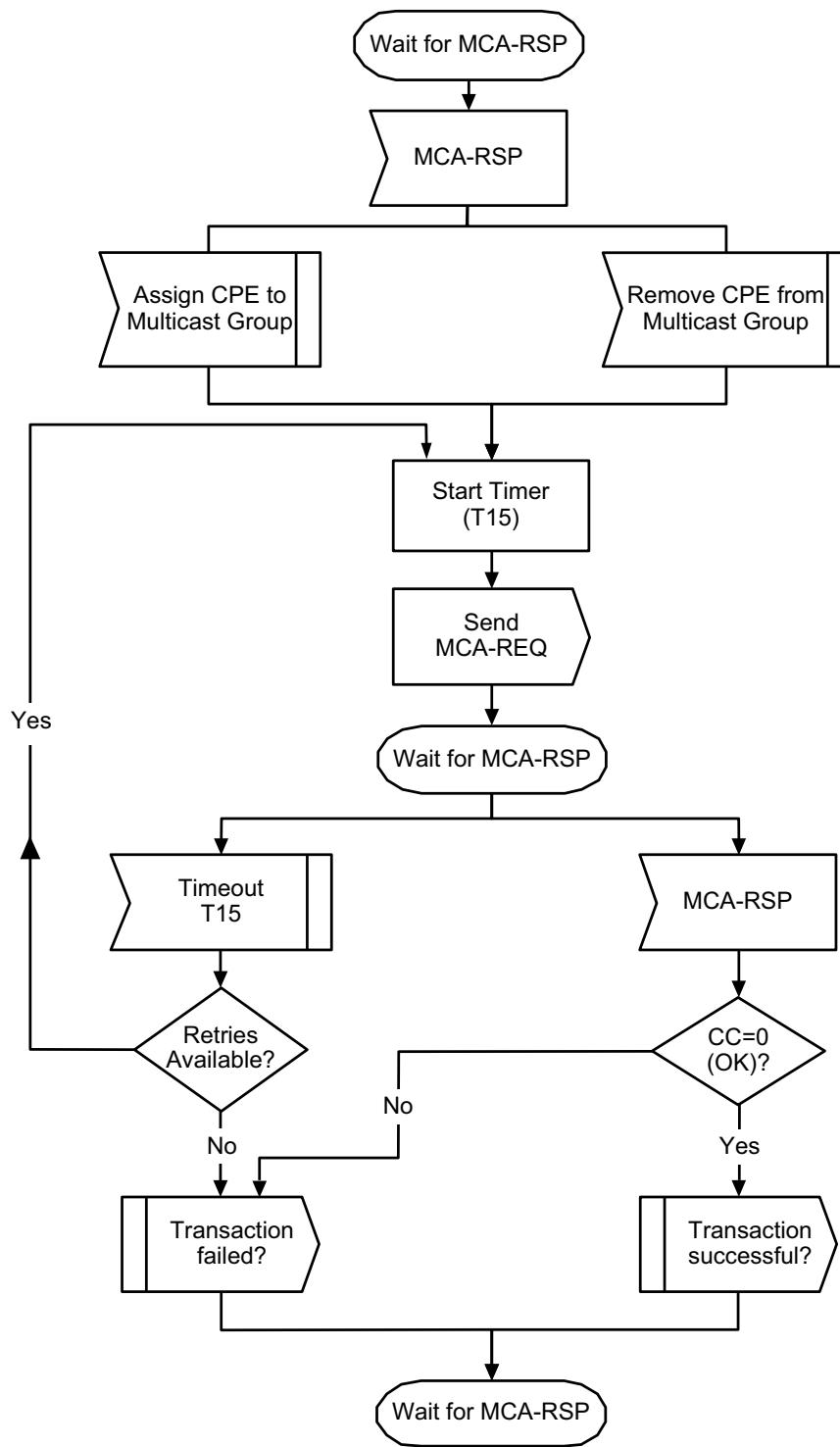
In order to support multicast services with the purpose of transporting traffic on connections for DS management and transport traffic, the MAC defines a special type of multicast SIDs (which represent a group of one or more CPEs) as well as FIDs for polling, DS management, and DS traffic. In this subclause, the multicast feature of the MAC is described.

### 7.17.1 Group management

The BS may add a CPE to a multicast group by sending an MCA-REQ message with the Join command. Upon receiving a MCA-REQ message, the CPE shall respond by sending an MCA-RSP message. A similar procedure is employed in the case of leaving a group. The protocol is shown in Figure 55 and Figure 56.



**Figure 55 — Group management at CPE**



**Figure 56 — Group management at BS**

#### 7.17.2 Multicast connections

The BS may establish downstream multicast service by creating a connection with each CPE to be associated with the service. To provide proper multicast operation, two things shall happen. The FID used

for the service as well as the “purpose” (see 7.7.9) shall be the same for all CPEs on the same channel that participate in the multicast group. Except for multicast management FIDs, the CPEs need not be aware that the connection is a multicast connection. The data transmitted on the connection with the given FID shall be received and processed by the MAC of each involved CPE. Since a multicast transport connection is associated with a service flow, that multicast transport connection is associated with the QoS and traffic parameters for that service flow.

ARQ is not applicable to multicast connections.

Each CPE participating in the multicast group whose “purpose” (see 7.7.9) is configured for multicast management, polling, and/or SCW setup shall have a group security association (GSA), allowing that connection to be encrypted using keys that are independent of those used for other encrypted transmissions between the CPEs and the BS. The GSA shall be established at the CPEs assigned to the multicast group via the SCM GSA. This message shall be sent prior to any transmission on the Multicast SID. The SAID of the GSA shall be the Multicast Management SID of the multicast group. The GSA shall remain installed on the CPE until it is asked by the BS to leave the multicast group and it has received a SCM GSA Remove message.

No protection shall be afforded for traffic on a downstream multicast transport FID. Traffic on multicast transport FIDs shall be mapped to the null SAID (i.e., the null SA). Only, management messages that are mapped to a downstream multicast management FID (Table 30) are to be encrypted.

### **7.17.3 Multicast-enabled SCW configuration**

Normally, multicast service is used for DS multicast management, polling, or transport traffic. Multicast service, can also be used to configure a group of CPEs for passive SCW monitoring or active SCW for CBP PDU transmission. This can be done by addressing a US-MAP IE to a SID that represents a multicast group and setting the UIUC to either 0 or 1 (see 7.7.4.1).

Prior to transmitting the US-MAP IE, the CPEs must be added to the multicast group (via MCA-REQ/RSP), which is configured for the 0x03, 0x05, or 0x07 purpose (see 7.7.9).

## **7.18 QoS**

The MAC adopts a similar QoS service model as specified in IEEE Std 802.16-2009, 6.3.14 (see also Kay [B69]). It defines several QoS related concepts, which include the following:

- Service Flow QoS Scheduling
- Dynamic Service Establishment
- Two-phase Activation Model

### **7.18.1 Theory of operation**

The various protocol mechanisms described in this standard may be used to support QoS for both upstream and downstream traffic through the CPE and the BS. This subclause provides an overview of the QoS protocol mechanisms and their part in providing end-to-end QoS.

The requirements for QoS include the following:

- A configuration and registration function for pre-configuring CPE-based QoS service flows and traffic parameters.
- A signaling function for dynamically establishing QoS-enabled service flows and traffic parameters.

- Utilization of MAC scheduling and QoS traffic parameters for upstream service flows.
- Utilization of QoS traffic parameters for downstream service flows.
- Grouping of service flow properties into named Service Classes, so upper-layer entities and external applications (at both the CPE and BS) may request service flows with desired QoS parameters in a globally consistent way.

The principal mechanism for providing QoS is to associate packets traversing the MAC interface into a service flow as identified by the transport FID assigned to a unicast SID (an individual CPE) or multicast transport FID assigned to a multicast SID (a multicast group of CPEs). A service flow is a unidirectional flow of packets that is provided with a particular QoS. The CPE and BS provide this QoS according to the QoS parameter set defined for the service flow.

The primary purpose of the QoS features defined here is to define transmission ordering and scheduling on the air interface. However, these features often need to work in conjunction with mechanisms beyond the air interface in order to provide end-to-end QoS or to police the behavior of CPEs.

Service flows exist in both the upstream and downstream direction and may exist without actually being activated to carry traffic. All service flows have a 32-bit SFID; admitted and active service flows also have a 3-bit transport FID assigned to a unicast SID (an individual CPE) or multicast transport FID assigned to a multicast SID (a multicast group of CPEs).

### 7.18.2 Service flows

A service flow is a MAC transport service that provides unidirectional transport of packets either to upstream packets transmitted by the CPE or to downstream packets transmitted by the BS.<sup>15</sup> A service flow is characterized by a set of QoS parameters such as latency, jitter, and throughput assurances. In order to standardize operation between the CPE and BS, these attributes include details of how the CPE requests upstream bandwidth allocations and the expected behavior of the BS upstream scheduler.

A service flow is partially characterized by the following attributes:<sup>16</sup>

- SFID: An SFID is assigned to each existing service flow. The SFID serves as the principal identifier for the service flow in the network. A service flow has at least an SFID and an associated direction.
- FID: Mapping to an SFID that exists only when the connection has an admitted or active service flow.
- ProvisionedQoSPParamSet: A QoS parameter set provisioned via means outside of the scope of this standard, such as the network management system.
- AdmittedQoSPParamSet: Defines a set of QoS parameters for which the BS (and possibly the CPE) is reserving resources. The principal resource to be reserved is bandwidth, but this also includes any other memory or time-based resource required to subsequently activate the flow.
- ActiveQoSPParamSet: Defines a set of QoS parameters defining the service actually being provided to the service flow. Only an Active service flow may forward packets.
- Authorization Module: A logical function within the BS that approves or denies every change to QoS parameters and Classification rules associated with a service flow. As such, it defines an “envelope” that limits the possible values of the AdmittedQoSPParamSet and ActiveQoSPParamSet.

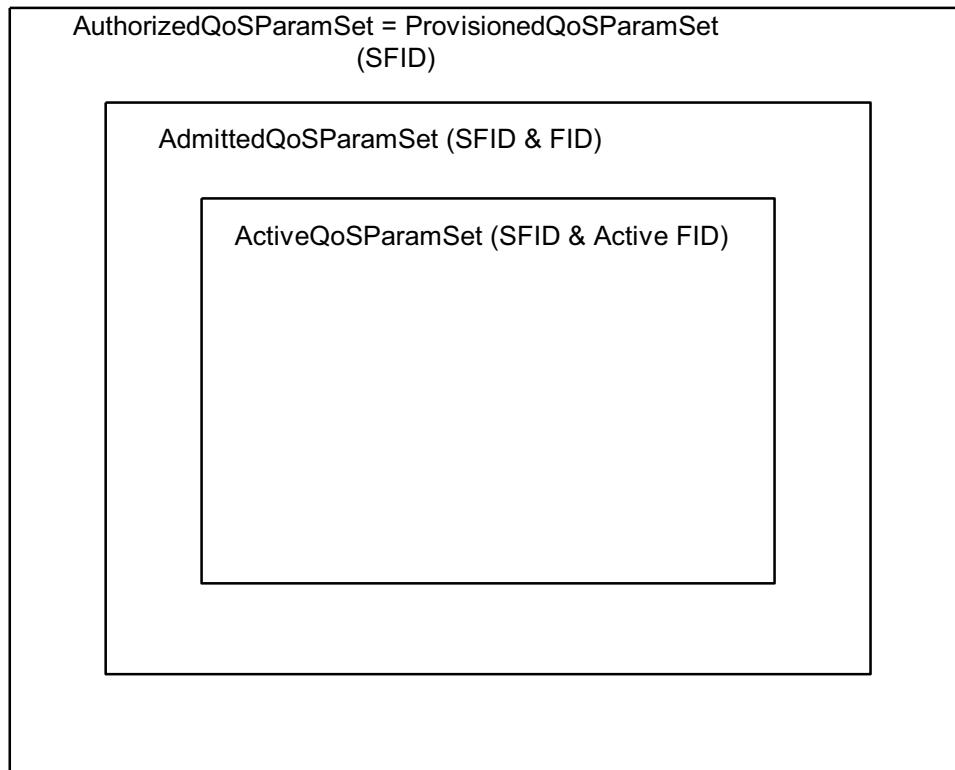
---

<sup>15</sup> A service flow, as defined here, has no direct relationship to the concept of a “flow” as defined by the IETF Integrated Services (intserv) Working Group (IETF RFC 2212). An intserv flow is a collection of packets sharing transport-layer endpoints. Multiple intserv flows can be served by a single service flow.

<sup>16</sup> Some attributes are derived from the above attribute list. The Service Class Name is an attribute of the ProvisionedQoSPParamSet. The activation state of the service flow is determined by the ActiveQoSPParamSet. If the ActiveQoSPParamSet is null, then the service flow is inactive.

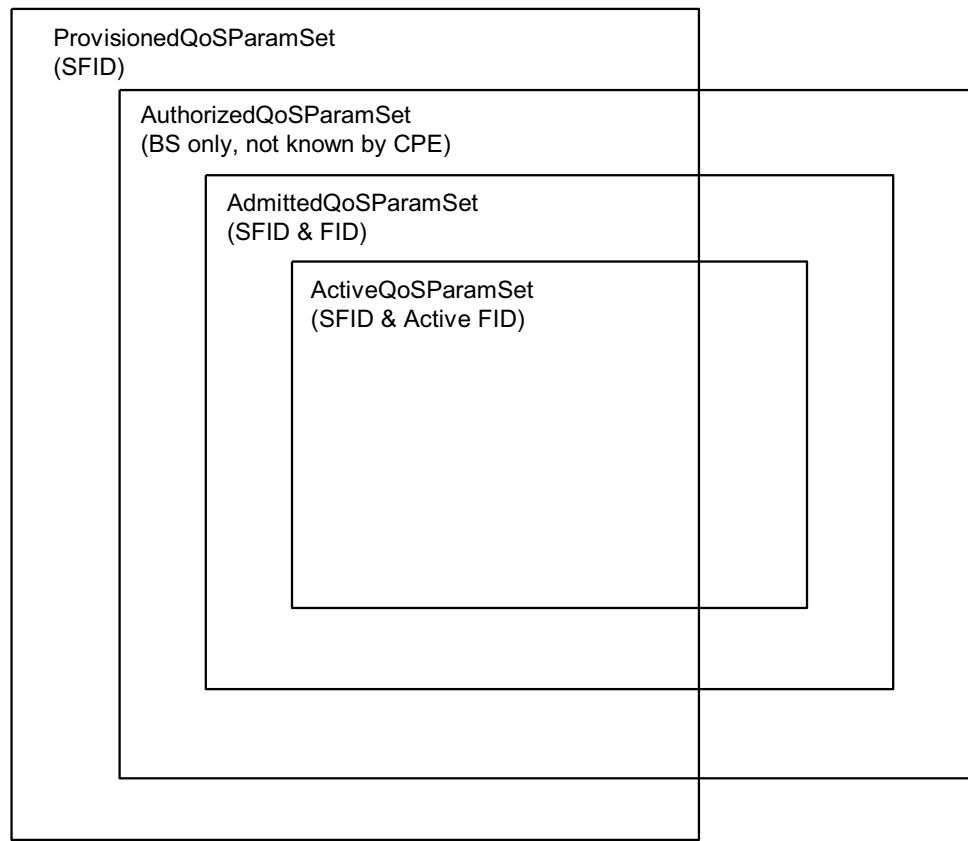
The relationship between the QoS parameter sets is as shown in Figure 57 and Figure 58. The ActiveQoSPParamSet is always a subset of the AdmittedQoSPParamSet, which is always a subset of the authorized “envelope.”<sup>17</sup> In the dynamic authorization model, this envelope is determined by the Authorization Module (labeled as the AuthorizedQoSPParamSet). In the provisioned authorization model, this envelope is determined by the ProvisionedQoSPParamSet. It is useful to think of the following three types of service flows:

- Provisioned: This type of service flow is known via provisioning by, for example, the network management system. Its AdmittedQoSPParamSet and ActiveQoSPParamSet are both null.
- Admitted: This type of service flow has resources reserved by the BS for its AdmittedQoSPParamSet, but these parameters are not active (i.e., its ActiveQoSPParamSet is null). Admitted Service Flows may have been provisioned or may have been signaled by some other mechanism.
- Active: This type of service flow has resources committed by the BS for its ActiveQoSPParamSet, (e.g., is actively sending maps containing unsolicited grants for a UGS based service flow). Its ActiveQoSPParamSet is non-null.



**Figure 57 — Provisioned authorization model “envelopes”**

<sup>17</sup> To say that QoS Parameter Set A is a subset of QoS Parameter Set B, the following shall be true for all QoS Parameters in A and B:  
 if (a smaller QoS parameter value indicates less resources, e.g., Maximum Traffic Rate);  
 A is a subset of B if the parameter in A is less than or equal to the same parameter in B;  
 if (a larger QoS parameter value indicates less resources, e.g., Tolerated Grant Jitter);  
 A is a subset of B if the parameter in A is greater than or equal to the same parameter in B;  
 if (the QoS parameter is not quantitative, e.g., Service Flow Scheduling Type);  
 A is a subset of B if the parameter in A is equal to the same parameter in B.



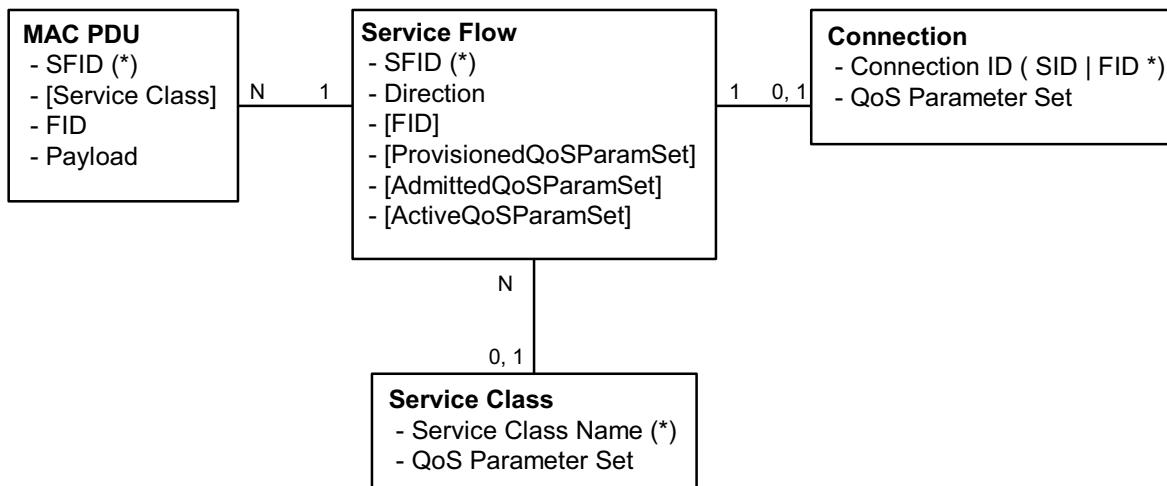
**Figure 58 — Dynamic authorization model “envelopes”**

### 7.18.3 Object model

The major objects of the architecture are represented by named rectangles in Figure 59. Each object has a number of attributes; the attribute names that uniquely identify it are marked with an “\*”. Optional attributes are denoted with brackets. The relationship between the number of objects is marked at each end of the association line between the objects. For example, a service flow may be associated with from 0 to N (many) PDUs, but a PDU is associated with exactly one service flow. The service flow is the central concept of the MAC protocol. It is uniquely identified by a 32-bit (SFID). Service flows may be in either the upstream or downstream direction. Admitted and active service flows are mapped to one of the 3-bit FIDs assigned to each SID (see 12.2).

Outgoing user data is submitted to the MAC SAP by a CS process for transmission on the MAC interface. The information delivered to the MAC SAP includes the SID indicated in the DS- or US-MAP IE (that describes the DS/US allocation for that CPE) and the FID in the GMH of the MAC PDU. The tuple, or concatenation of SID and FID (see 7.2 and 12.2) forms a connection identifier that identifies the connection across which the information is delivered. The service flow for the CPE (SID) is mapped to MAC connection identified by the FID.

The Service Class is an optional object that may be implemented at the BS. It is referenced by an ASCII name, which is intended for provisioning purposes. A Service Class is defined in the BS to have a particular QoS parameter set. The QoS parameter sets of a service flow may contain a reference to the Service Class Name as a “macro” that selects all of the QoS parameters of the Service Class. The service flow QoS parameter sets may augment and even override the QoS parameter settings of the Service Class, subject to authorization by the BS.



**Figure 59 — Object model of the QoS service**

#### 7.18.4 Service classes

The Service Class serves the following purposes:<sup>18</sup>

- It allows operators, who so wish, to move the burden of configuring service flows from the provisioning server to the BS. Operators provision the CPEs with the Service Class Name; the implementation of the name is configured at the BS. This allows operators to modify the implementation of a given service to local circumstances without changing CPE provisioning. For example, some scheduling parameters may need to be tweaked differently for two different BSs to provide the same service. As another example, service profiles could be changed by time of day.
- It allows higher-layer protocols to create a service flow by its Service Class Name. For example, telephony signaling may direct the CPE to instantiate any available provisioned service flow of class “G711.”

Any service flow may have its QoS parameter set specified in any of the following three ways:

- By explicitly including all traffic parameters.
- By indirectly referring to a set of traffic parameters by specifying a Service Class Name.
- By specifying a Service Class Name along with modifying parameters.

The Service Class Name is “expanded” to its defined set of parameters at the time the BS successfully admits the service flow. The Service Class expansion can be contained in the following BS-originated messages: DSA-REQ, DSC-REQ, DSA-RSP, and DSC-RSP. In all of these cases, the BS shall include a service flow encoding that includes the Service Class Name and the QoS parameter set of the Service Class. If a CPE-initiated request contained any supplemental or overriding service flow parameters, a successful response shall also include these parameters.

When a Service Class name is given in an admission or activation request, it is possible that the returned QoS parameter set may change from activation to activation. This can happen because of administrative changes to the Service Class’s QoS parameter set at the BS. If the definition of a Service Class Name is

<sup>18</sup> Service classes are merely identifiers for a specific set of QoS parameter set values. Hence, the use of service classes is optional. A service identified by a service class is treated no differently, once established, than a service that has the same QoS parameter set explicitly specified.

changed at the BS (e.g., its associated QoS parameter set is modified), it has no effect on the QoS parameters of existing service flows associated with that Service Class. A BS may initiate DSC transactions to existing service flows that reference the Service Class Name to affect the changed Service Class definition.

When a CPE uses the Service Class Name to specify the Admitted QoS parameter set, the expanded set of IE encodings of the service flow shall be returned to the CPE in the response message (DSA-RSP or DSC-RSP). Use of the Service Class Name later in the activation request may fail if the definition of the Service Class Name has changed and the new required resources are not available. Thus, the CPE should explicitly request the expanded set of IEs from the response message in its later activation request.

#### **7.18.5 Authorization**

An authorization module shall approve every change to the service flow QoS parameters. This includes every DSA-REQ message to create a new service flow and every DSC-REQ message to change a QoS parameter set of an existing service flow. Such changes include requesting an admission control decision (e.g., setting the AdmittedQoSParamSet) and requesting activation of a service flow (e.g., setting the ActiveQoSParamSet). The authorization module also checks reduction requests regarding the resources to be admitted or activated.

In the static authorization model, the authorization module stores the provisioned status of all “deferred” service flows. Admission and activation requests for these provisioned service flows shall be permitted, as long as the Admitted QoS parameter set is a subset of the Provisioned QoS parameter set, and the Active QoS parameter set is a subset of the Admitted QoS parameter set. Requests to change the Provisioned QoS parameter set shall be refused, as shall requests to create new dynamic service flows. This defines a static system where all possible services are defined in the initial configuration of each CPE.

In the dynamic authorization model, the authorization module also communicates through a separate interface to an independent policy server. This policy server may provide the authorization module with advance notice of upcoming admission and activation requests, and it specifies the proper authorization action to be taken on those requests. Admission and activation requests from a CPE are then checked by the Authorization Module to verify that the ActiveQoSParamSet being requested is a subset of the set provided by the policy server. Admission and activation requests from a CPE that are signaled in advance by the external policy server are permitted. Admission and activation requests from a CPE that are not pre-signaled by the external policy server may result in a real-time query to the policy server or may be refused.

Prior to initial connection setup, the BS shall retrieve the Provisioned QoS Set for a CPE. This is handed to the Authorization Module within the BS. The BS shall be capable of caching the Provisioned QoS parameter set and shall be able to use this information to authorize dynamic flows that are a subset of the Provisioned QoS parameter set. The BS should implement mechanisms for overriding this automated approval process (such as described in the dynamic authorization model). For example, it could

- Deny all requests whether or not they have been pre-provisioned.
- Define an internal table with a richer policy mechanism but seeded by the Provisioned QoS Set.
- Refer all requests to an external policy server.

#### **7.18.6 Types of service flows**

It is useful to think about three basic types of service flows. This subclause describes these three types of service flows in more detail. However, it is important to note that there are more than just these three basic types (see 7.7.8.9.4).

### 7.18.6.1 Provisioned

A service flow may be provisioned but not immediately activated (sometimes called “deferred”). That is, the description of any such service flow contains an attribute that provisions but defers activation and admission (see 7.7.8.9.4). The network assigns a SFID for such a service flow. The BS may also require an exchange with a policy module prior to admission.

As a result of external action beyond the scope of this specification, the CPE may choose to activate a provisioned service flow by passing the SFID and the associated QoS parameter sets to the BS in the DSC-REQ message. If authorized and resources are available, the BS shall respond by mapping the service flow to a FID.

As a result of external action beyond the scope of this specification, the BS may choose to activate a service flow by passing the SFID as well as the FID and the associated QoS parameter sets to the CPE in the DSC-REQ message. Such a provisioned service flow may be activated and deactivated many times (through DSC exchanges). In all cases, the original SFID shall be used when reactivating the service flow.

### 7.18.6.2 Admitted

This protocol supports a two-phase activation model that is often utilized in telephony applications. In the two-phase activation model, the resources for a “call” are first “admitted,” and then once the end-to-end negotiation is completed (e.g., called party’s gateway generates an “off-hook” event), the resources are “activated.” The two-phase model serves the following purposes:

- Conserving network resources until a complete end-to-end connection has been established
- Performing policy checks and admission control on resources as quickly as possible, and in particular, before informing the far end of a connection request
- Preventing several potential theft-of-service scenarios

For example, if an upper-layer service were using UGS, and the addition of upper-layer flows could be adequately provided by increasing the Maximum Sustained Traffic Rate QoS parameter, then the following procedure might be used. When the first higher-layer flow is pending, the CPE issues a DSA-REQ with the admitted Maximum Sustained Traffic Rate parameter equal to that required for one higher-layer flow, and the active Maximum Sustained Traffic Rate parameter equal to zero. Later when the higher-layer flow becomes active, it issues a DSC-REQ with the instance of the active Maximum Sustained Traffic Rate parameter equal to that required for one higher-layer flow. Admission control was performed at the time of the reservation, so the later DSC-REQ, having the active parameters within the range of the previous reservation, is guaranteed to succeed. Subsequent higher-layer flows would be handled in the same way. If there were three higher-layer flows establishing connections, with one flow already active, the service flow would have admitted Maximum Sustained Traffic Rate equal to that required for four higher-layer flows, and active Maximum Sustained Traffic Rate equal to that required for one higher-layer flow.

An activation request of a service flow where the new ActiveQoSPParamSet is a subset of the AdmittedQoSPParamSet shall be allowed, except in the case of catastrophic failure. An admission request where the AdmittedQoSPParamSet is a subset of the previous AdmittedQoSPParamSet shall succeed, so long as the ActiveQoSPParamSet remains a subset of the AdmittedQoSPParamSet.

A service flow that has resources assigned to its AdmittedQoSPParamSet, but whose resources are not yet completely activated, is in a transient state. It is possible in some applications that a long-term reservation of resources is necessary or desirable. For example, placing a telephone call on hold should allow any resources in use for the call to be temporarily allocated to other purposes, but these resources shall be available for resumption of the call later. The AdmittedQoSPParamSet is maintained as “soft state” in the BS; this state shall be maintained without releasing the non-activated resources. Changes may be signaled with a DSC-REQ message.

### 7.18.6.3 Active

A service flow that has a non-NULL ActiveQoSParamSet is said to be an active service flow. It is requesting (according to its Request/Transmission Policy, as in 7.7.8.9.10) and being granted bandwidth for transport of data packets. An admitted service flow may be activated by providing an ActiveQoSParamSet, signaling the resources actually desired at the current time. This completes the second stage of the two-phase activation model (see 7.18.6.2).

A service flow may be provisioned and immediately activated. Alternatively, a service flow may be created dynamically and immediately activated. In this case, two-phase activation is skipped and the service flow is available for immediate use upon authorization.

## 7.18.7 Service Flow creation

The provisioning of service flows is done via means outside of the scope of this standard, such as the network management system. During provisioning, a service flow is instantiated, gets a SFID and a “provisioned” type. For some service flows it may be specified that DSA procedure must be activated by Network Entry procedure. Enabling service flows follows the transfer of the operational parameters (see Figure 34). In this case, the service flow type may change to “admitted” or to “active”; in the latter case, the Service Flow is mapped onto a certain connection.

Service flow encodings contain either a full definition of service attributes (omitting defaultable items if desired) or a service class name. A service class name is an ASCII string, which is known at the BS and which indirectly specifies a set of QoS parameters.

Triggers, other than network entry, also may cause creation, admission, or activation of service flows. Such triggers lay outside the scope of the standard.

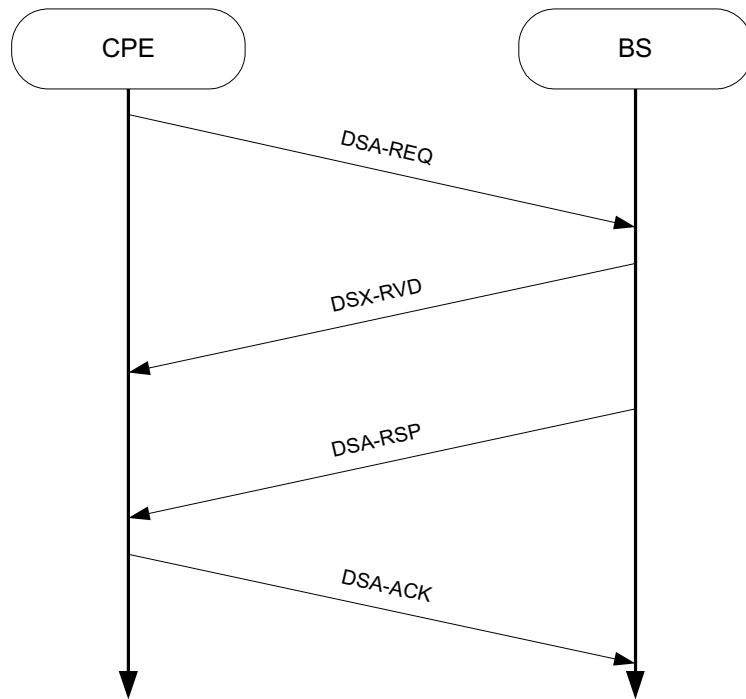
Capability of handling each specific Service Flow parameter is optional.

### 7.18.7.1 Dynamic Service Flow creation

#### 7.18.7.1.1 CPE-initiated

Creation of service flows may be initiated by either BS (mandatory capability) or by CPE (optional capability).

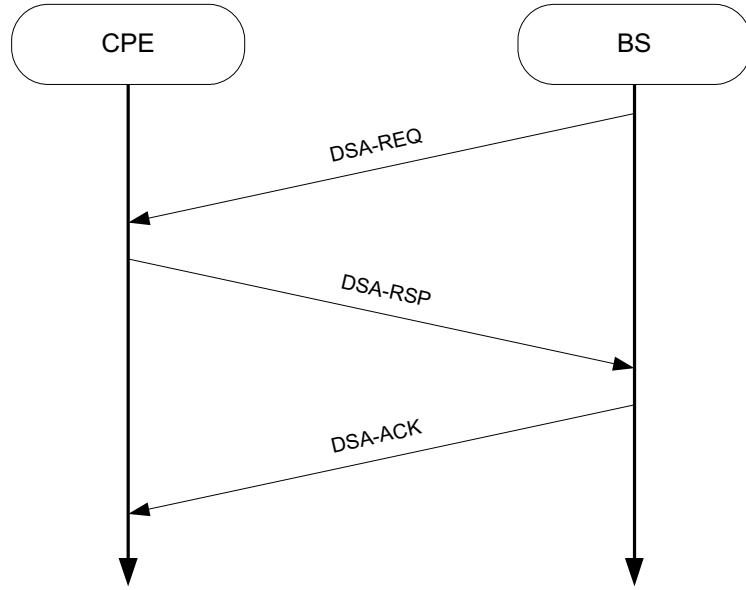
The CPE-initiated protocol is illustrated in Figure 60 and described in detail in 7.18.9. A DSA-REQ from a CPE contains a service flow reference and QoS parameter set (marked either for admission-only or for admission and activation). BS responds with DSA-RSP indicating acceptance or rejection. In the case when rejection was caused by presence of non-supported parameter of non-supported value, specific parameter may be included into DSA-RSP.



**Figure 60 — DSA message flow (CPE-initiated)**

#### 7.18.7.1.2 BS-initiated

A DSA-REQ from a BS contains an SFID for either one upstream or one downstream Service flow, possibly its associated FID, and a set of active or admitted QoS parameters. The protocol is illustrated in Figure 61 and is described in detail in 7.18.9. The CPE responds with DSA-RSP indicating acceptance or rejection. In the case when rejection was caused by presence of a non-supported parameter of non-supported value, specific parameter may be included into DSA-RSP.



**Figure 61 — DSA message flow (BS-initiated)**

### 7.18.8 Dynamic Service Flow modification and deletion

In addition to the methods presented in 7.18.7.1 for creating service flows, protocols are defined for modifying and deleting service flows (see 7.18.9).

Both provisioned and dynamically created service flows are modified with the DSC message, which can change the Admitted and Active QoS parameter sets of the flow. A successful DSC transaction changes a service flow's QoS parameters by replacing both the Admitted and Active QoS parameter sets. If the message contains only the Admitted set, the Active set is set to null and the flow is deactivated. If the message contains neither set ("000" value used for QoS parameter set type—see 7.7.8.9.4), then both sets are set to null and the flow is de-admitted. When the message contains both QoS parameter sets, the Admitted set is checked first, and if admission control succeeds, the Active set in the message is checked against the Admitted set in the message to verify that it is a subset. If all checks are successful, the QoS parameter sets in the message become the new Admitted and Active QoS parameter sets for the service flow. If either of the checks fails, the DSC transaction fails and the service flow QoS parameter sets remain unchanged.

### 7.18.9 Service Flow Management

#### 7.18.9.1 Overview

Service flows may be created, changed, or deleted. This is accomplished through a series of MAC management messages referred to as DSA, DSC, and DSD. The DSA messages create a new service flow. The DSC messages change an existing service flow. The DSD messages delete an existing service flow. This is illustrated in Figure 62.

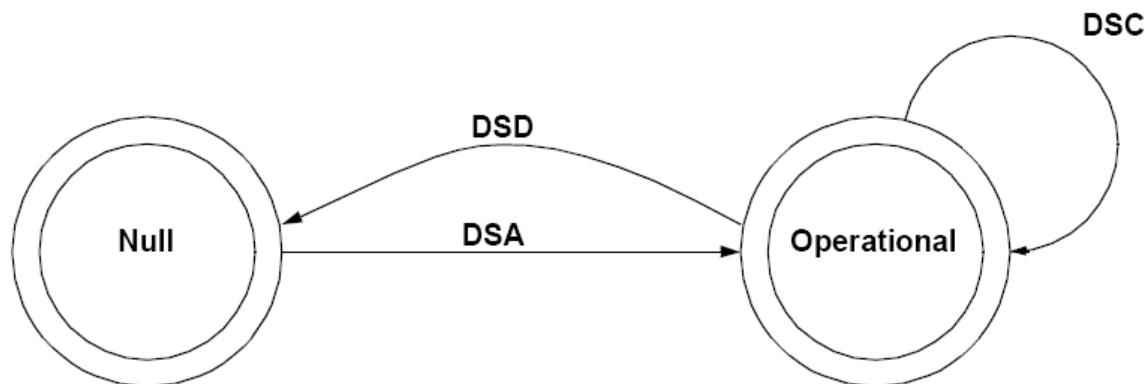


Figure 62 — Dynamic service flow overview

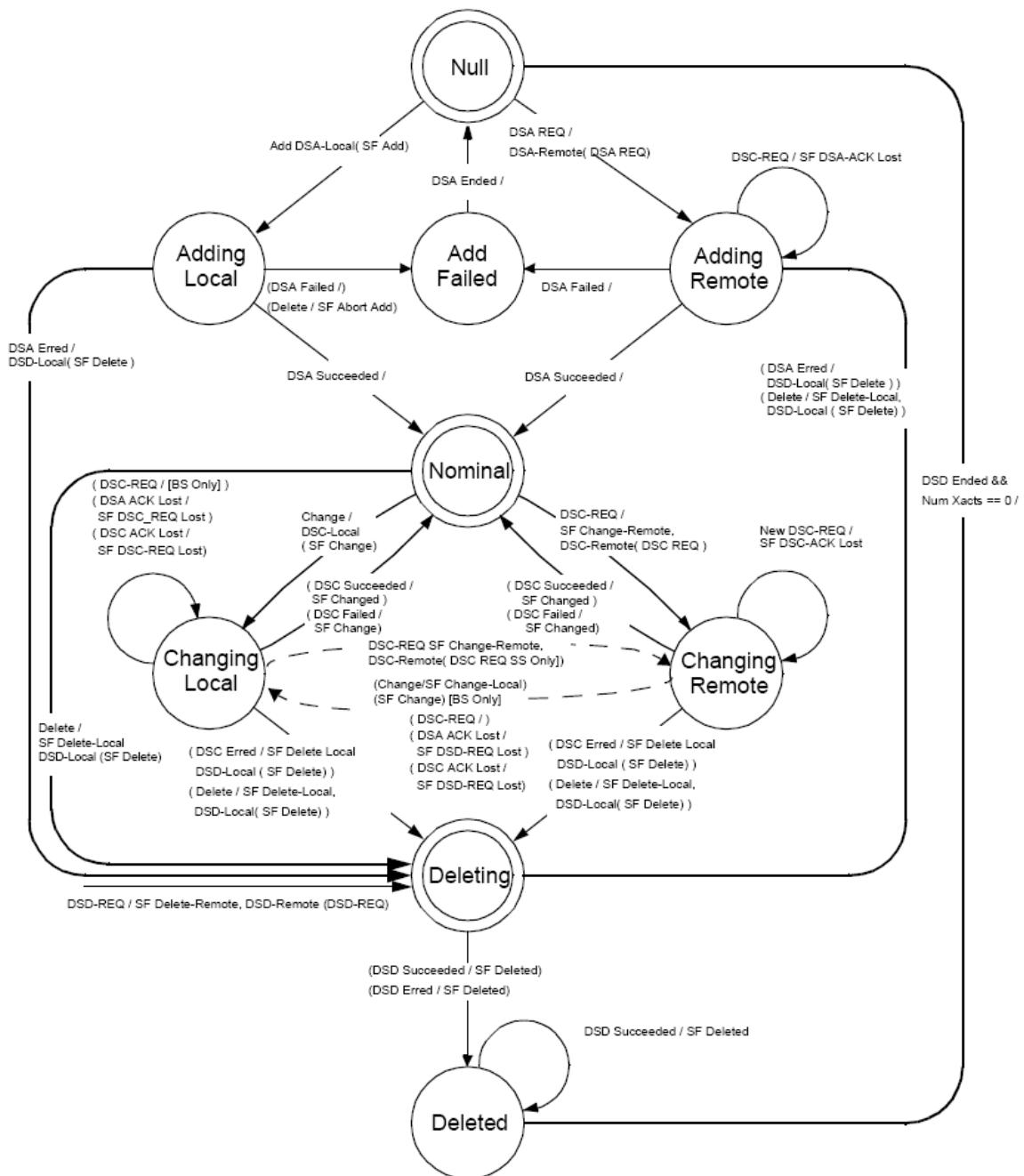
The Null state implies that no service flow exists that matches the SFID and/or Transaction ID in a message. Once the service flow exists, it is operational and has an assigned SFID. In steady-state operation, a service flow resides in a Nominal state. When DSx messaging is occurring, the service flow may transition through other states, but remains operational. Since multiple service flows may exist, there may be multiple state machines active, one for every service flow. DSx messages only affect those state machines that match the SFID and/or Transaction ID. Both the CPE and BS shall decrypt and verify the Ciphertext ICV (see 8.4.2) for the PDUs of all DSx messages before processing them, and discard any messages that fail.

Transaction IDs are unique per transaction and are selected by the initiating device (CPE or BS). To help prevent ambiguity and provide simple checking, the Transaction ID number space is split between the CPE and BS. The CPE shall select its Transaction IDs from the first half of the number space (0x0000 to 0x7FFF). The BS shall select its Transaction IDs from the second half of the number space (0x8000 to 0xFFFF).

Each DSx message sequence is a unique transaction with an associated unique transaction identifier. The DSA/DSC transactions consist of a request/response/acknowledge sequence. The DSD transactions consist of a request/response sequence. The response messages shall return a CC of OK unless some exception condition was detected. The acknowledge messages shall return the CC in the response unless a new exception condition arises. A more detailed state diagram, including transition states, is shown in Figure 63 through Figure 69. The detailed actions for each transaction shall be given in the following subclauses.

#### 7.18.9.2 Dynamic Service Flow state transitions

The Dynamic Service Flow state transition diagram (Figure 63) is the top-level state diagram and controls the general service flow state. As needed, it creates transactions, each represented by a Transaction state transition diagram, to provide the DSA, DSC, and DSD signaling. Each Transaction state transition diagram communicates only with the parent Dynamic Service Flow state transition diagram. The top-level state transition diagram filters DSx messages and passes them to the appropriate transaction based on SFID, service flow reference number, and Transaction ID.



**Figure 63 — Dynamic Service Flow state transition diagram**

There are six different types of transactions, which are locally initiated or remotely initiated for each of the DSA, DSC, and DSD messages (Figure 63—Figure 69). Most transactions have three basic states—pending, holding, and deleting. The pending state is typically entered after creation and is where the transaction is waiting for a reply. The holding state is typically entered once the reply is received. The purpose of this state is to allow for retransmissions in case of a lost message, even though the local entity has perceived that the transaction has completed. The deleting state is only entered if the service flow is being deleted while a transaction is being processed.

The flow diagrams provide a detailed representation of each of the states in the Transaction state transition diagrams. All valid transitions are shown. Any inputs not shown should be handled as a severe error condition.

With one exception, these state diagrams apply equally to the BS and CPE. In the Dynamic Service Flow Changing-Local state, there is a subtle difference in the SS and BS behaviors. This is called out in the state transition and detailed flow diagrams.

**NOTE**—The “Num Xacts” variable in the Dynamic Service Flow state transition diagram is incremented every time the top-level state diagram creates a transaction and is decremented every time a transaction terminates. A dynamic service flow shall not return to the Null state until it is deleted and all transactions have terminated.

The inputs for the state diagrams are identified below.

Dynamic Service Flow state transition diagram inputs from unspecified local, higher level entities:

- a) Add
- b) Change
- c) Delete

Dynamic Service Flow state transition diagram inputs from DSx Transaction state transition diagrams:

- a) DSA Succeeded
- b) DSA Failed
- c) DSA-ACK Lost
- d) DSA Erred
- e) DSA Ended
  
- a) DSC Succeeded
- b) DSC Failed
- c) DSC-ACK Lost
- d) DSC Erred
- e) DSC Ended
  
- a) DSD Succeeded
- b) DSD Erred
- c) DSD Ended

DSx Transaction state transition diagram inputs from the Dynamic Service Flow state transition diagram:

- a) SF Add
- b) SF Change
- c) SF Delete
  
- a) SF Abort Add
- b) SF Change-Remote
- c) SF Delete-Local
- d) SF Delete-Remote
  
- a) SF DSA-ACK Lost
- b) SF DSC-REQ Lost
- c) SF DSC-ACK Lost
- d) SF DSC-REQ Lost
  
- a) SF Changed
- b) SF Deleted

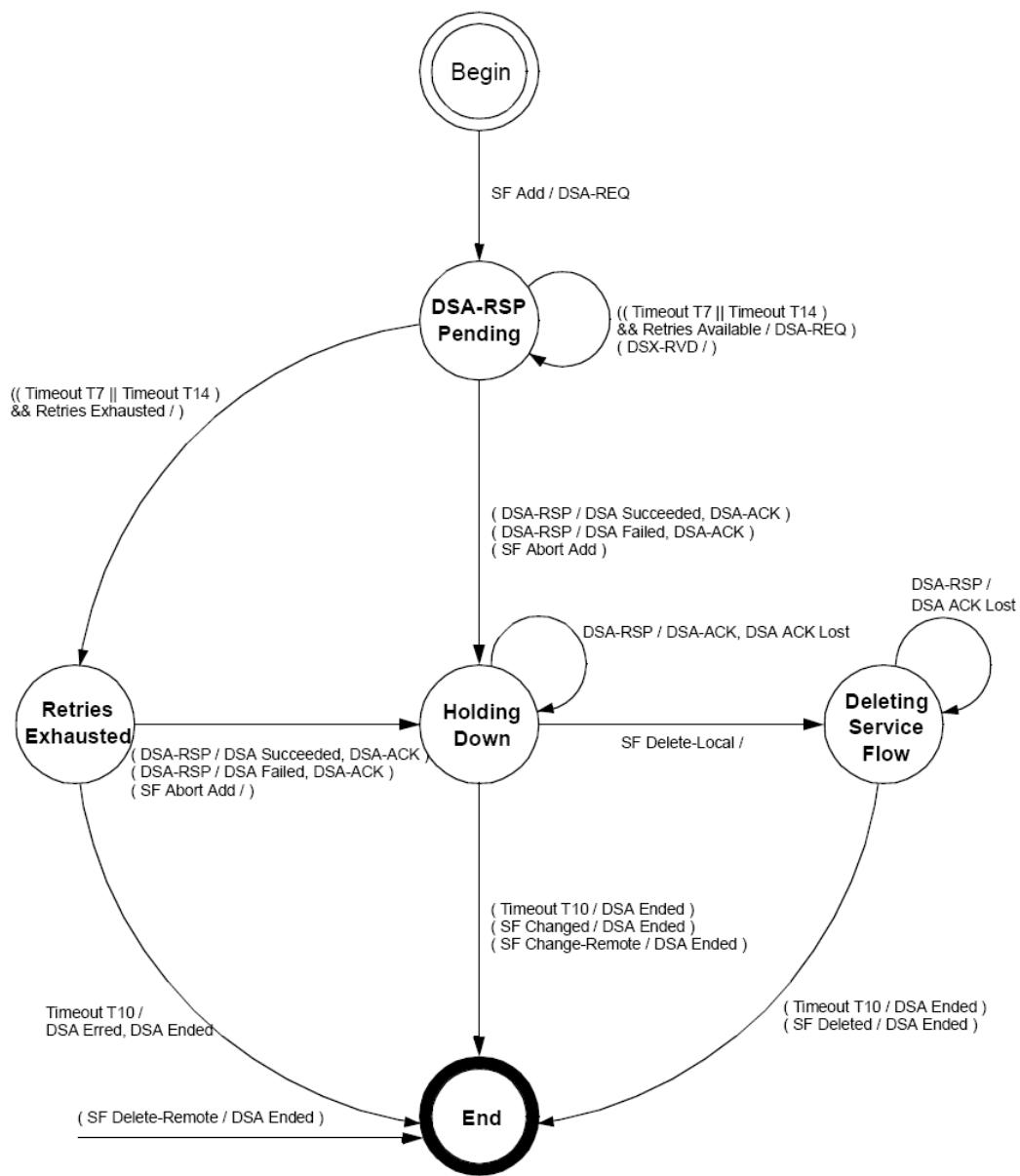
The creation of DSx transactions by the Dynamic Service Flow state transition diagram is indicated by the notation:

DSx – [ Local | Remote ] ( initial\_input )

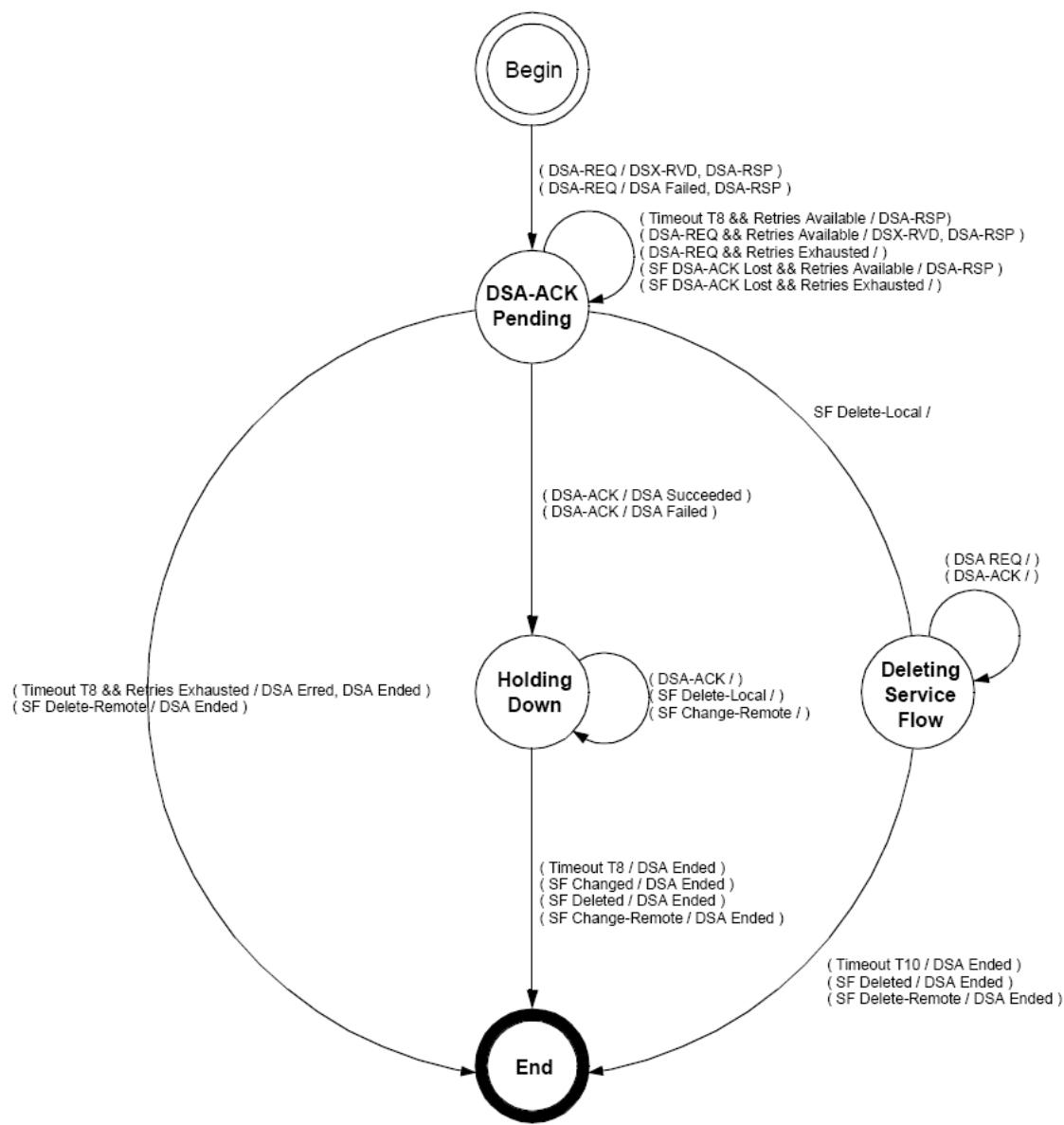
where initial\_input may be SF Add, DSA-REQ, SF Change, DSC-REQ, SF Delete, or DSD-REQ, depending on the transaction type and initiator.

State transitions (i.e., the lines between states) are labeled with <what causes the transition>/<messages and events triggered by the transition>. If there are multiple events or messages before the slash “/” separated by a comma, any of them can cause the transition. If there are multiple events or messages listed after the slash, all of the specified actions shall accompany the transition.

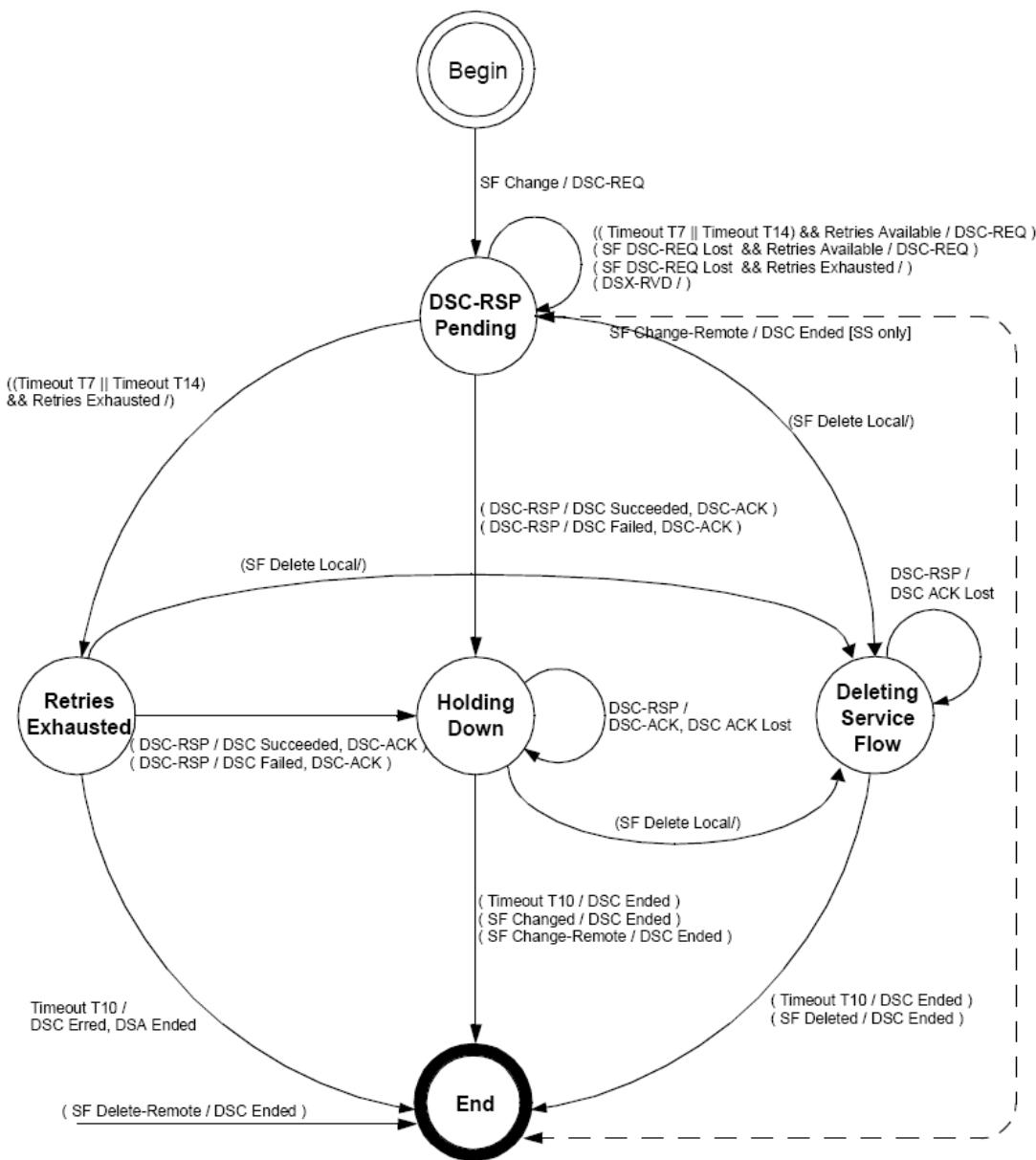
For example, “DSD-REQ/SF Delete Remote, DSD-Remote (DSD-REQ)” should be read as follows: Once DSD-REQ is received, it triggers sending a “SF Delete Remote” event to transactions running for this service flow AND starting the “DSD-Remote” transaction and pass the event DSD-REQ to it.



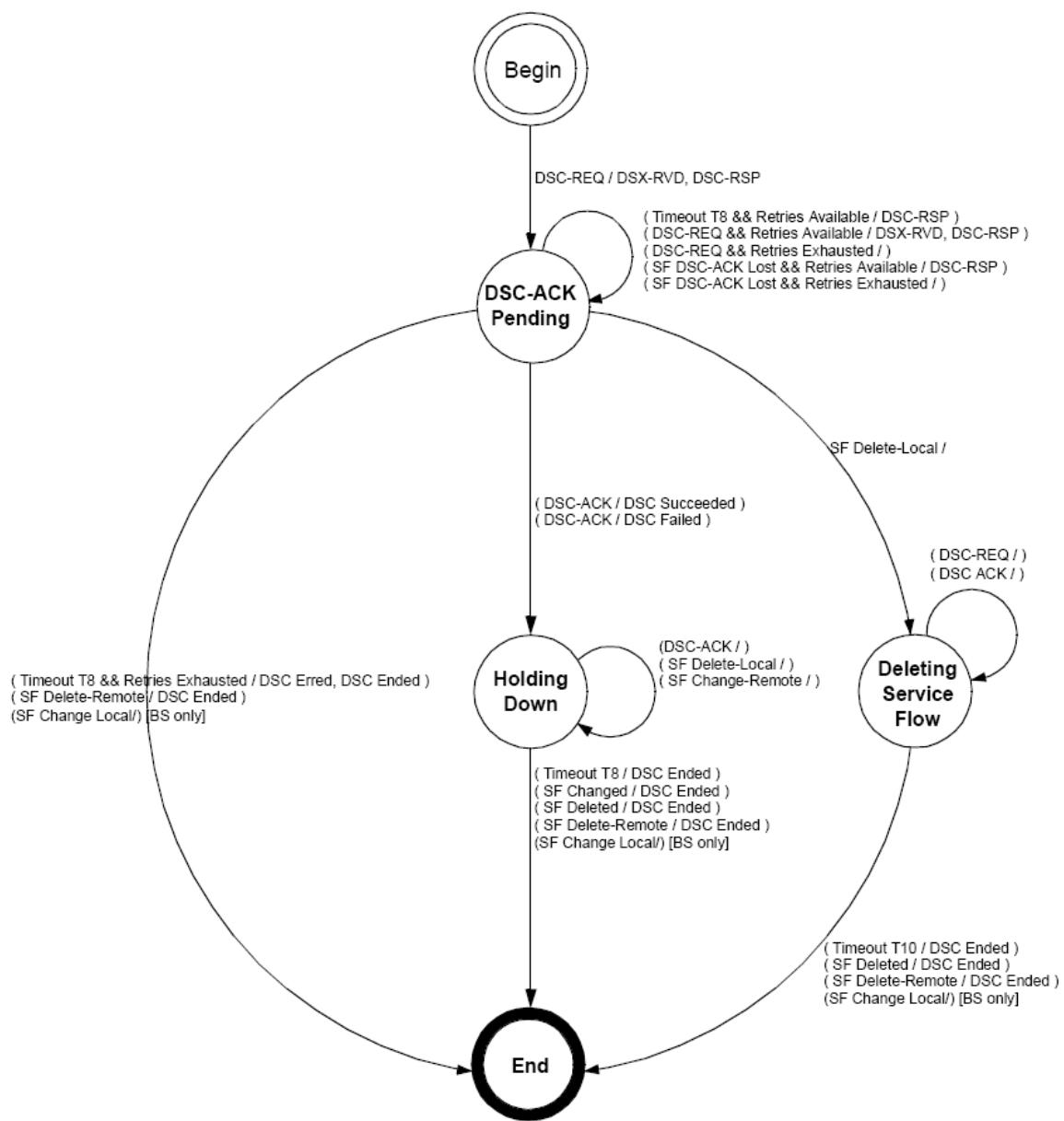
**Figure 64 — DSA—Locally-Initiated Transaction state transition diagram**



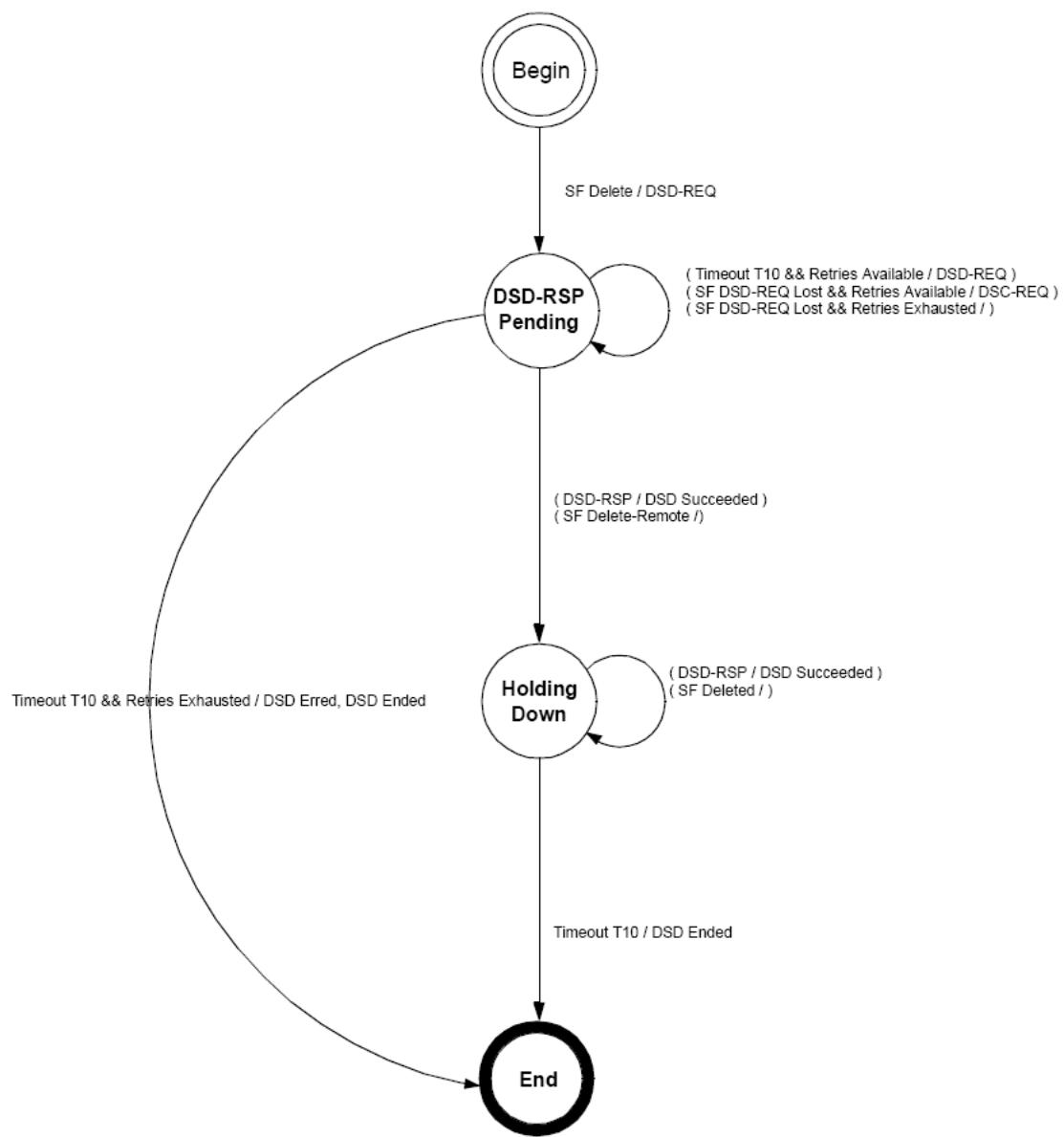
**Figure 65 — DSA—Remotely-Initiated Transaction State Transition Diagram**



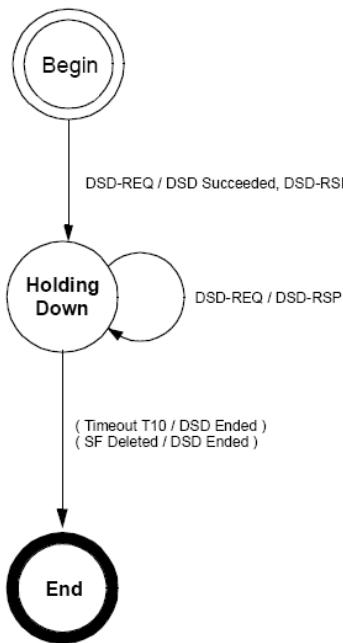
**Figure 66 — DSC—Locally-Initiated Transaction State Transition Diagram**



**Figure 67 — DSC—Remotely-Initiated Transaction State Transition Diagram**



**Figure 68 — DSD—Locally-Initiated Transaction State Transition Diagram**



**Figure 69 — DSD—Remotely-Initiated Transaction State Transition Diagram**

### 7.18.9.3 Dynamic Service Addition

#### 7.18.9.3.1 CPE-initiated DSA

A CPE wishing to create either an upstream or downstream service flow sends a request to the BS using a DSA-REQ message. The BS checks the integrity of the message and, if the message is intact, sends a message received (DSx-RSP) response to the CPE. The BS checks the CPE's authorization for the requested service and whether the QoS requirements can be supported, generating an appropriate response using a DSA-RSP message. The CPE concludes the transaction with an acknowledgment message (DSA-ACK). This process is illustrated in Table 178.

**Table 178 — CPE-initiated DSA**

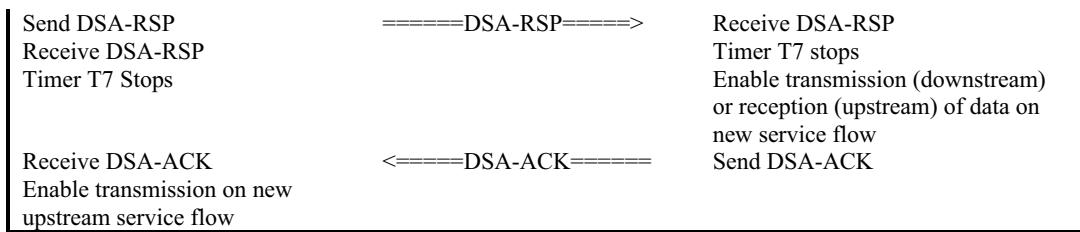
CPE	BS
New service flow needed	
Check if resources are available	
Send DSA-REQ	=====DSA-REQ=====
Set Timers T7 and T14	
Timer T14 stops	=====DSx-RVD=====
Receive DSA-RSP	=====DSA-RSP=====
Timer T7 stops	
If ActiveQoSPParamSet is non-null, enable transmission and/or reception of data on new service flow	
Send DSA-ACK	=====DSA-ACK=====
	=====DSA-ACK=====

#### 7.18.9.3.2 BS-initiated DSA

A BS wishing to establish either an upstream or a downstream dynamic service flow with a CPE performs the following operations. The BS checks the authorization of the destination CPE for the requested CoS and to determine whether the QoS requirements can be supported. If the service can be supported, the BS generates a new SFID with the required CoS and informs the CPE using a DSA-REQ message. If the CPE checks that it can support the service, it responds using a DSA-RSP message. The transaction completes with the BS sending the acknowledge message (DSA-ACK). This process is illustrated in Table 179.

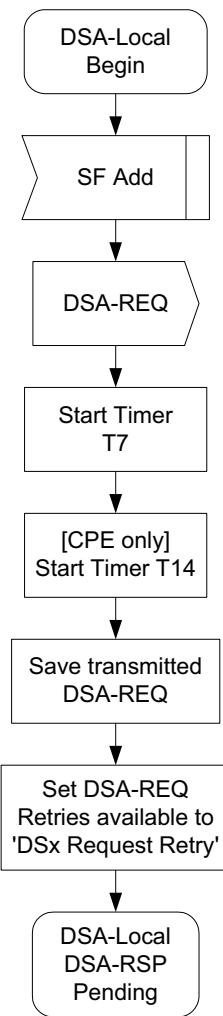
**Table 179 — BS-initiated DSA**

CPE	BS
Receive DSA-REQ	=====DSA-REQ=====
Confirm that CPE can support service flow	
Add Downstream SFID (if present)	
Enable reception on any new downlink service flow	

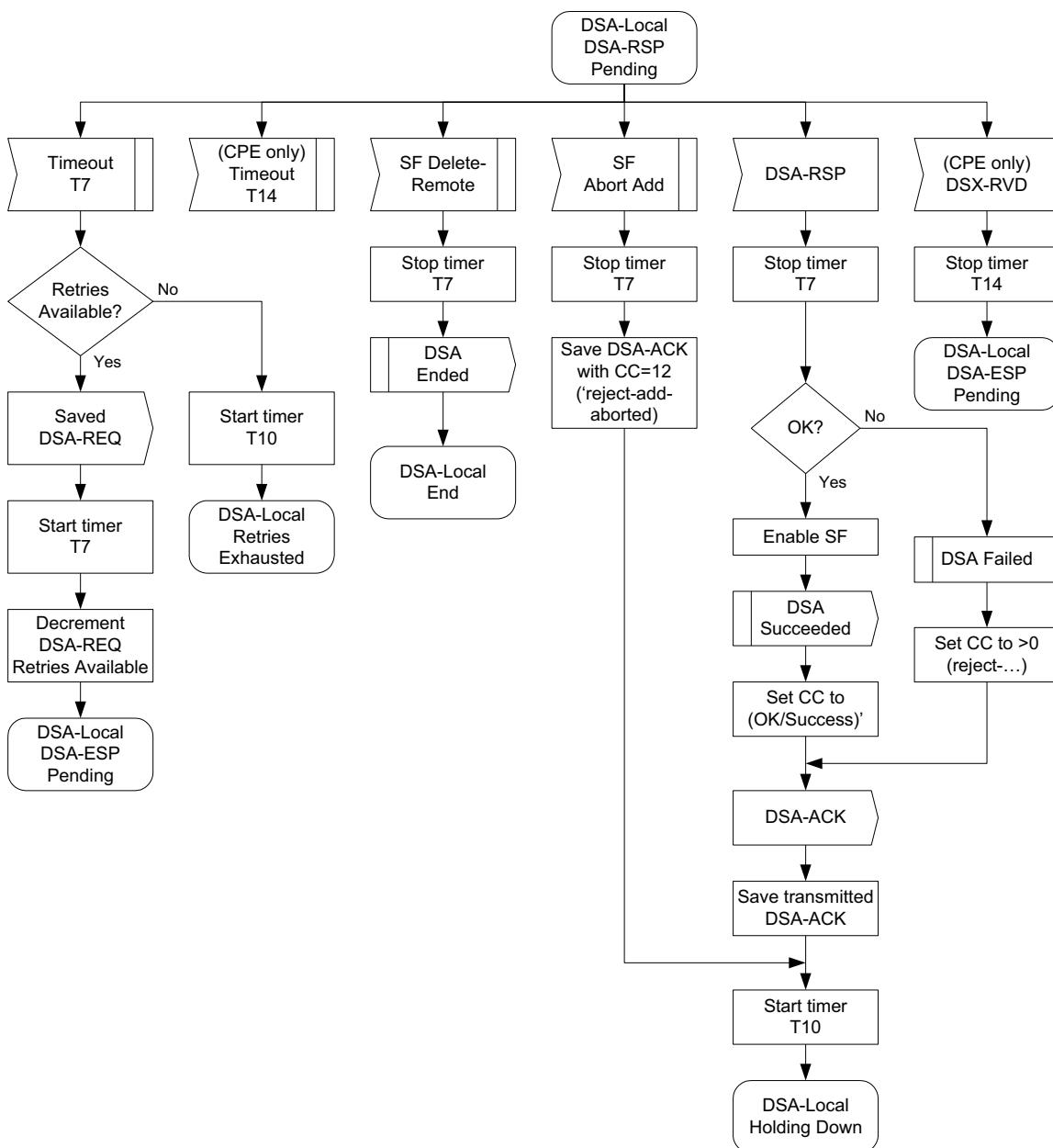


### 7.18.9.3.3 DSA state transition diagrams

DSA state transition diagrams are shown in Figure 70 through Figure 78.



**Figure 70 — DSA—Locally-Initiated Transaction Begin state flow diagram**



**Figure 71 — DSA—Locally-Initiated Transaction DSA-RSP Pending state flow diagram**

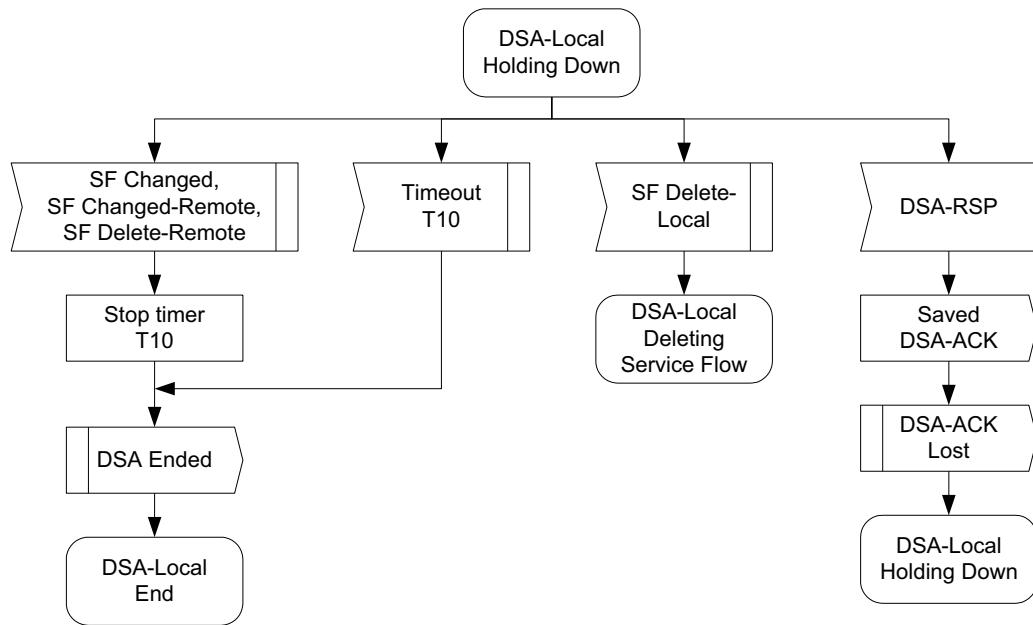
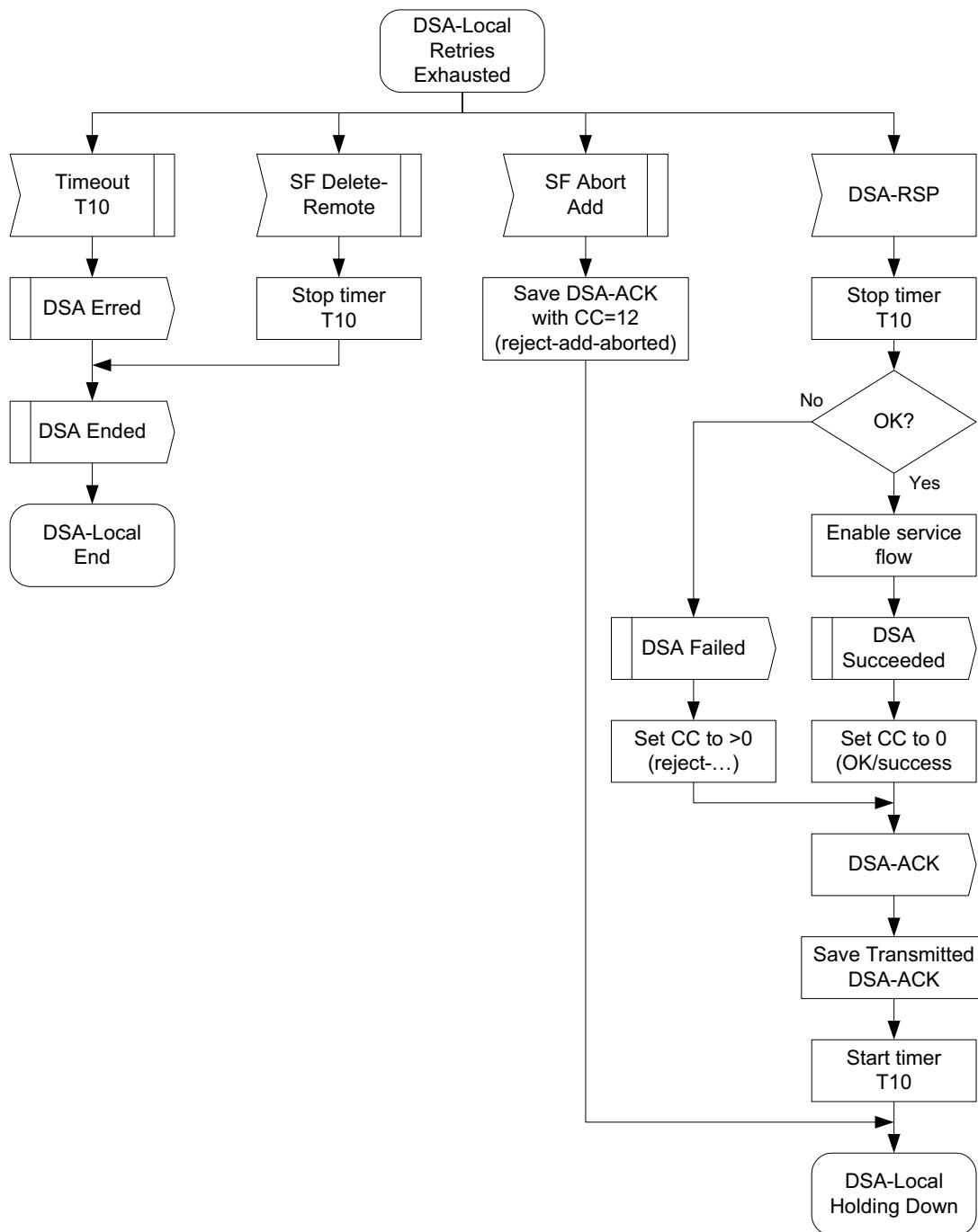


Figure 72 — DSA—Locally-Initiated Transaction Holding state flow diagram



**Figure 73 — DSA—Locally Initiated Transaction Retries Exhausted state flow diagram**

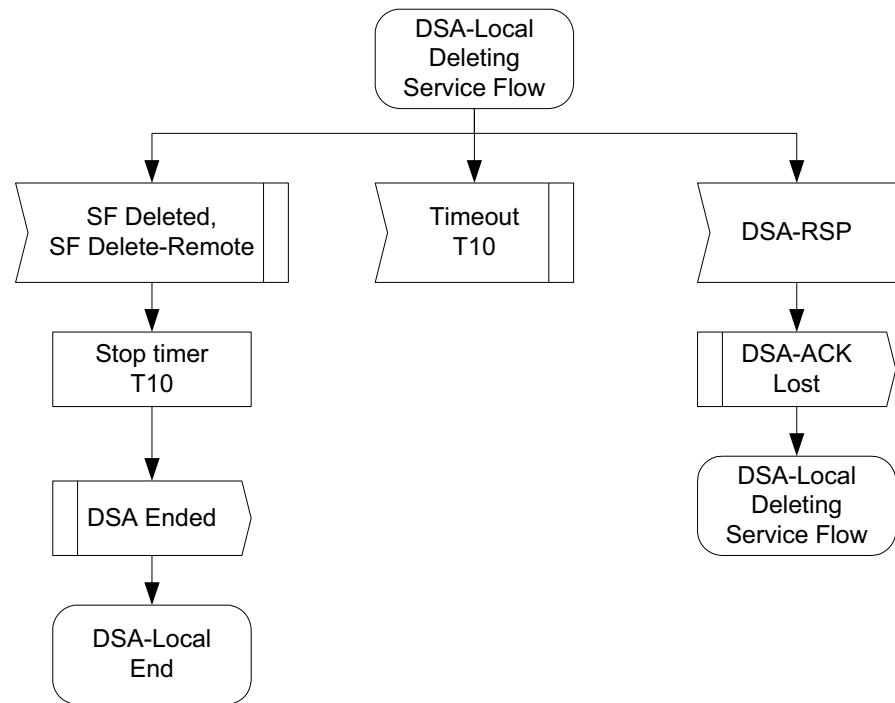
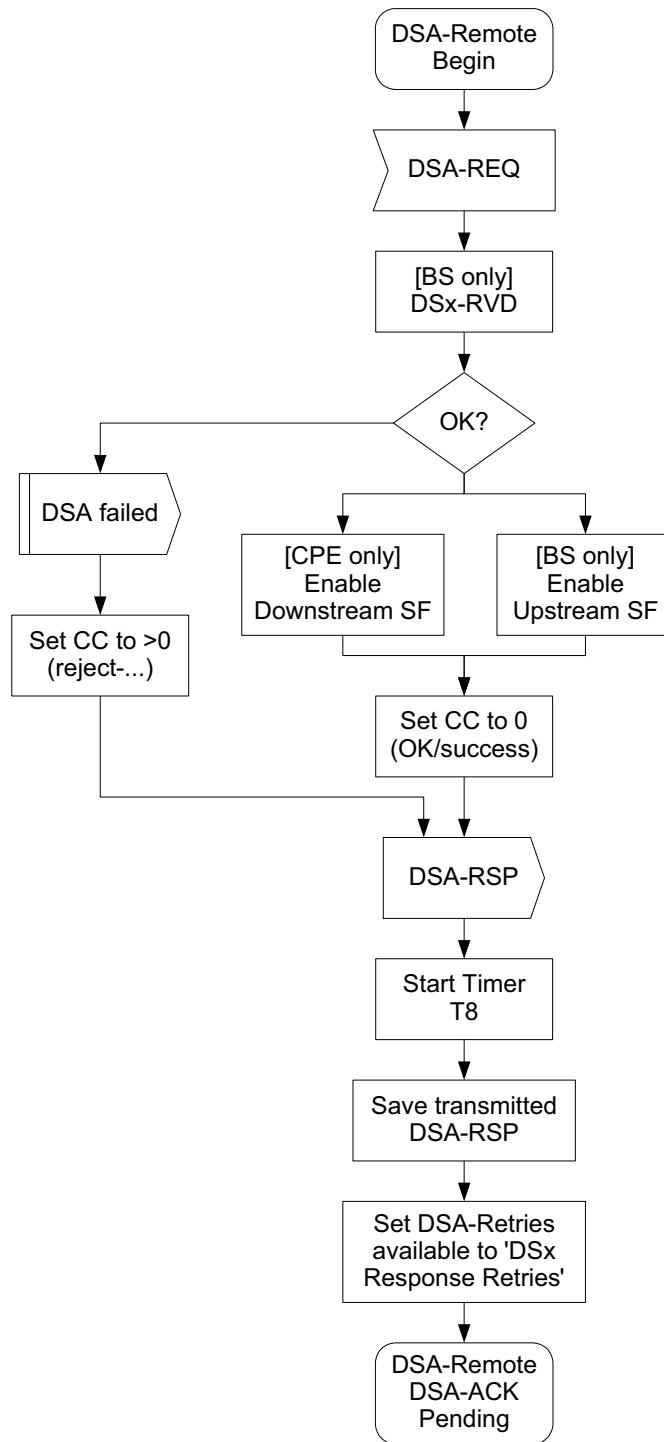
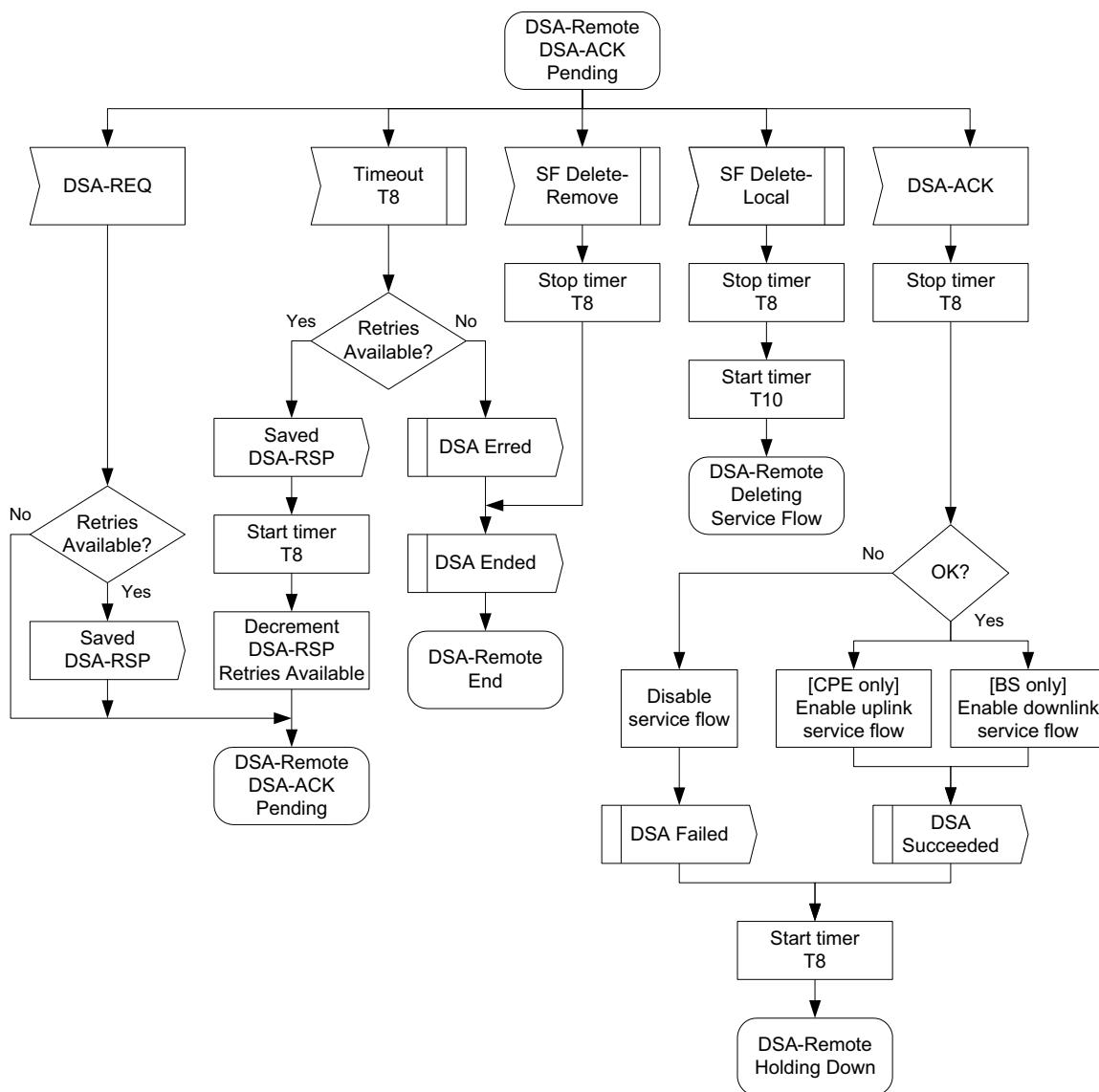


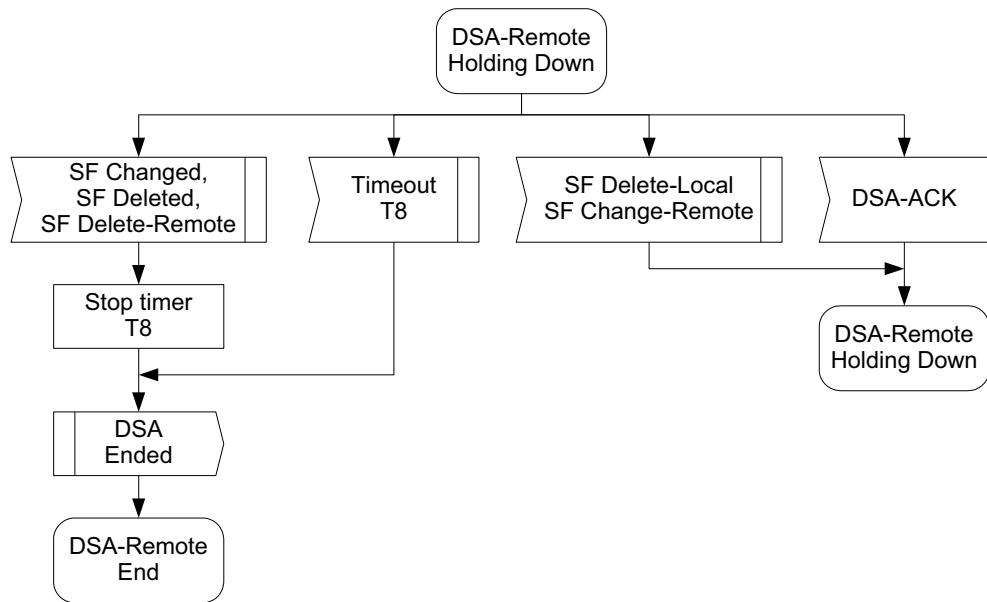
Figure 74 — DSA—Locally Initiated Transaction Deleting Service Flow state flow diagram



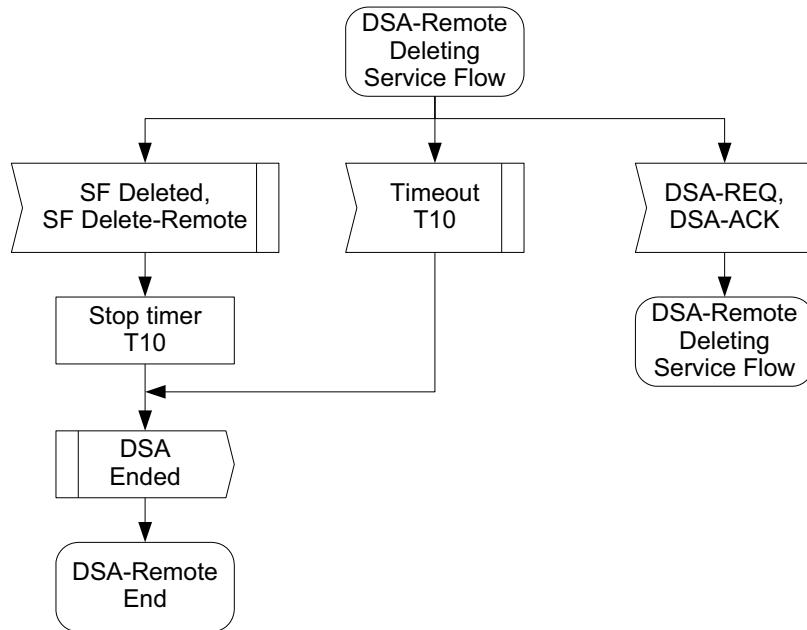
**Figure 75 — DSA—Remotely Initiated Transaction Begin state flow diagram**



**Figure 76 — DSA—Remotely Initiated Transaction DSA-ACK Pending state flow diagram**



**Figure 77 — DSA—Remotely Initiated Transaction Holding Down state flow diagram**



**Figure 78 — DSA—Remotely Initiated Transaction Deleting Service state flow diagram**

#### 7.18.9.4 Dynamic Service Change

The DSC set of messages is used to modify the flow parameters associated with a service flow. Specifically, DSC can modify the service flow Specification.

A single DSC message exchange can modify the parameters of either one downlink service flow or one upstream service flow.

To prevent packet loss, any required bandwidth change is sequenced between the CPE and BS.

The BS controls both upstream and downstream scheduling. The timing of scheduling changes is independent of direction AND whether it is an increase or decrease in bandwidth. The BS always changes scheduling on receipt of a DSC-REQ (CPE-initiated transaction) or DSC-RSP (BS-initiated transaction).

The BS also controls the downstream transmit behavior. The change in downstream transmit behavior is always coincident with the change in downstream scheduling (i.e., BS controls both and changes both simultaneously).

The CPE controls the upstream transmit behavior. The timing of CPE transmit behavior changes is a function of which device initiated the transaction and whether the change is an “increase” or “decrease” in bandwidth.

If an upstream service flow’s bandwidth is being reduced, the CPE reduces its payload bandwidth first and then the BS reduces the bandwidth scheduled for the service flow. If an upstream service flow’s bandwidth is being increased, the BS increases the bandwidth scheduled for the service flow first and then the CPE increases its payload bandwidth.

Any service flow can be deactivated with a DSC command by sending a DSC-REQ message, referencing the SFID, and including a null ActiveQoSParamSet. However, if a service flow that is mapped to either Basic, Primary Management, or Secondary Management Connection of a CPE is deactivated, that CPE is considered de-registered. The CPE must attempt an initial entry and re-register with the BS to continue operation. Therefore, care should be taken before deactivating such service flows. If a service flow that was provisioned is deactivated, the provisioning information for that service flow shall be maintained until the service flow is reactivated.

A CPE shall have only one DSC transaction outstanding per service flow. If it detects a second transaction initiated by the BS, the CPE shall abort the transaction it initiated and allow the BS-initiated transaction to complete.

A BS shall have only one DSC transaction outstanding per service flow. If it detects a second transaction initiated by the CPE, the BS shall abort the transaction that the CPE initiated and allow the BS-initiated transaction to complete.

The following service flow parameters may not be changed, and shall not be present in the DSC-REQ or DSC-RSP messages:

- Service Flow Scheduling type
- Request/Transmission Policy
- Convergence Sublayer Specification
- Fixed-length versus variable-length SDU indicator
- SDU size
- ARQ parameters, in accordance with individual TLV definitions
- Target SAID, service flow can only be mapped to one SA while operating

NOTE—Currently anticipated applications would probably control a service flow through either the CPE or BS, and not both. Therefore, the case of a DSC being initiated simultaneously by the CPE and BS is considered as an exception condition and treated as one.

#### 7.18.9.4.1 CPE-initiated DSC

A CPE that needs to change a service flow definition performs the following operations.

The CPE informs the BS using a DSC-REQ. The BS checks the integrity of the message and, if the message is intact, sends a message received (DSx-RSP) response to the CPE. The BS shall decide if the referenced service flow can support this modification. The BS shall respond with a DSC-RSP indicating acceptance or rejection. In the case when rejection was caused by presence of non-supported parameter of non-supported value, specific parameter may be included into DSC-RSP. The CPE reconfigures the service flow if appropriate, and then shall respond with a DSC-ACK. This process is illustrated in Table 180.

**Table 180 — CPE-initiated DSC**

BS	CPE
Receive DSC-REQ	<=====DSC-REQ=====>
DSC-REQ integrity valid	=====DSx-RVD=====>
Validate Request	Set Timers T7 and T14
Modify service flow	Timer T14 Stops
Increase Channel Bandwidth if required	
Send DSC-RSP	<=====DSC-RSP=====>
	Receive DSC-RSP
	Timer T7 Stops
	Modify service flow
	Adjust Payload Bandwidth
Receive DSC-ACK	<=====DSC-ACK=====>
Decrease Channel Bandwidth if required	Send DSC-ACK

#### 7.18.9.4.2 BS-initiated DSC

A BS that needs to change a service flow definition performs the following operations.

The BS shall decide if the referenced service flow can support this modification. If so, the BS informs the CPE using a DSC-REQ. The CPE checks that it can support the service change, and shall respond using a DSC-RSP indicating acceptance or rejection. In the case when rejection was caused by presence of non-supported parameter of non-supported value, specific parameter may be included into DSC-RSP. The BS reconfigures the service flow if appropriate, and then shall respond with a DSC-ACK. This process is illustrated in Table 181.

**Table 181 — BS-initiated DSC**

BS	CPE
Service flow requires modifying	
Send DSC-REQ	<=====DSC-REQ=====>
Set Timer T7	Receive DSC-REQ
	Validate request
	Modify service flow
	Decrease Payload Bandwidth if required
Receive DSC-RSP	<=====DSC-RSP=====>
Timer T7 Stops	Send DSC-RSP
Modify service flow	
Adjust Channel Bandwidth	
Send DSC-ACK	<=====DSC-ACK=====>
	Receive DSC-ACK
	Increase Payload Bandwidth if required

#### 7.18.9.4.3 DSC state transition diagrams

DSC state transition diagrams are shown in Figure 79–Figure 87.

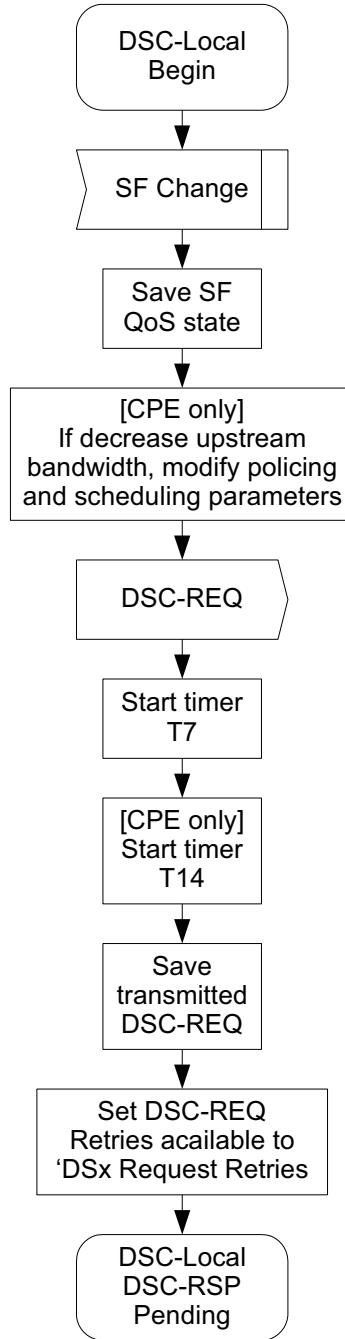
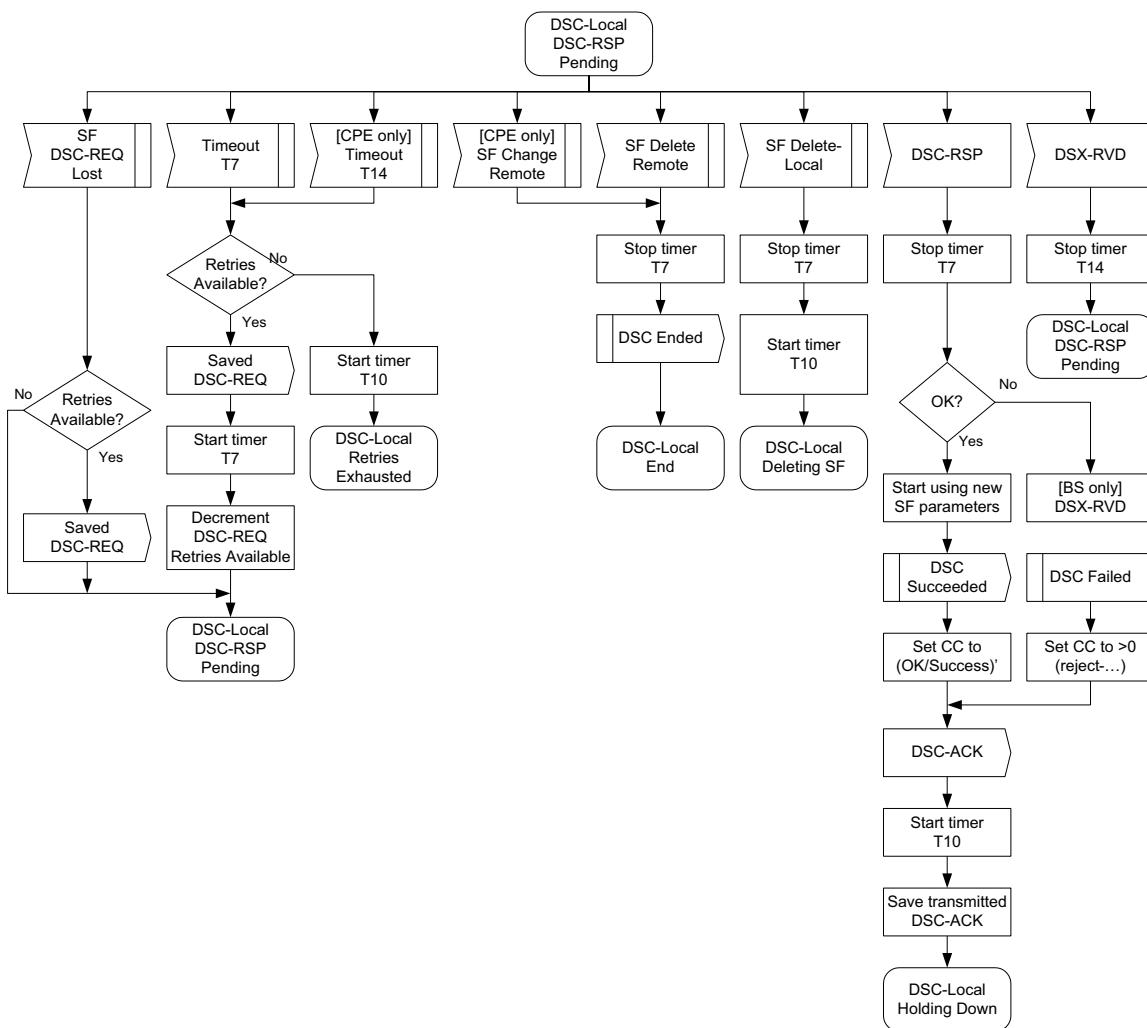
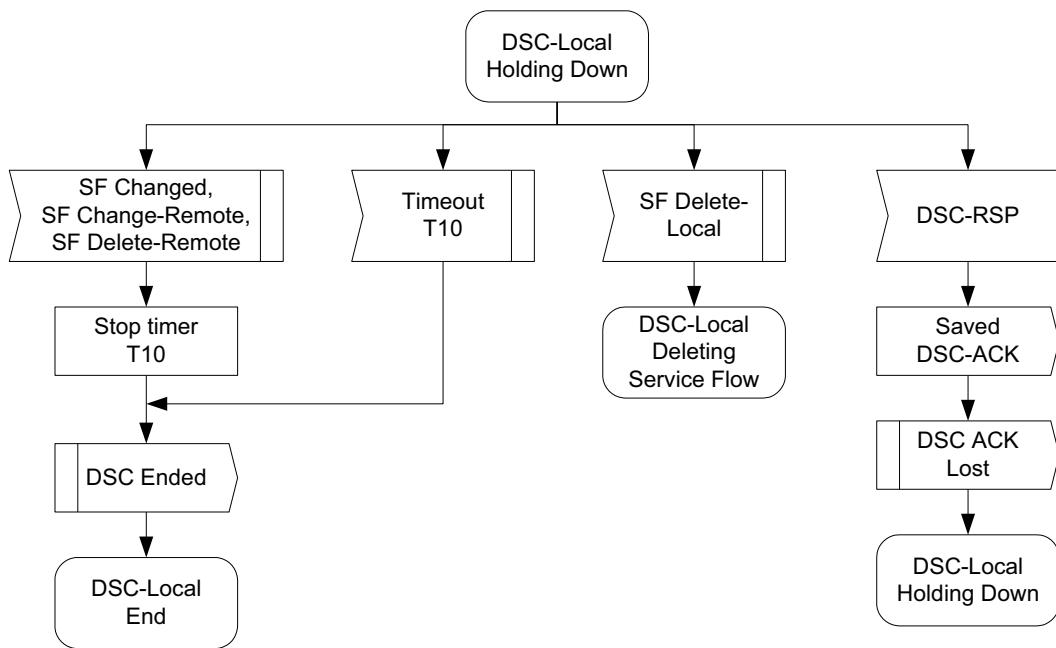


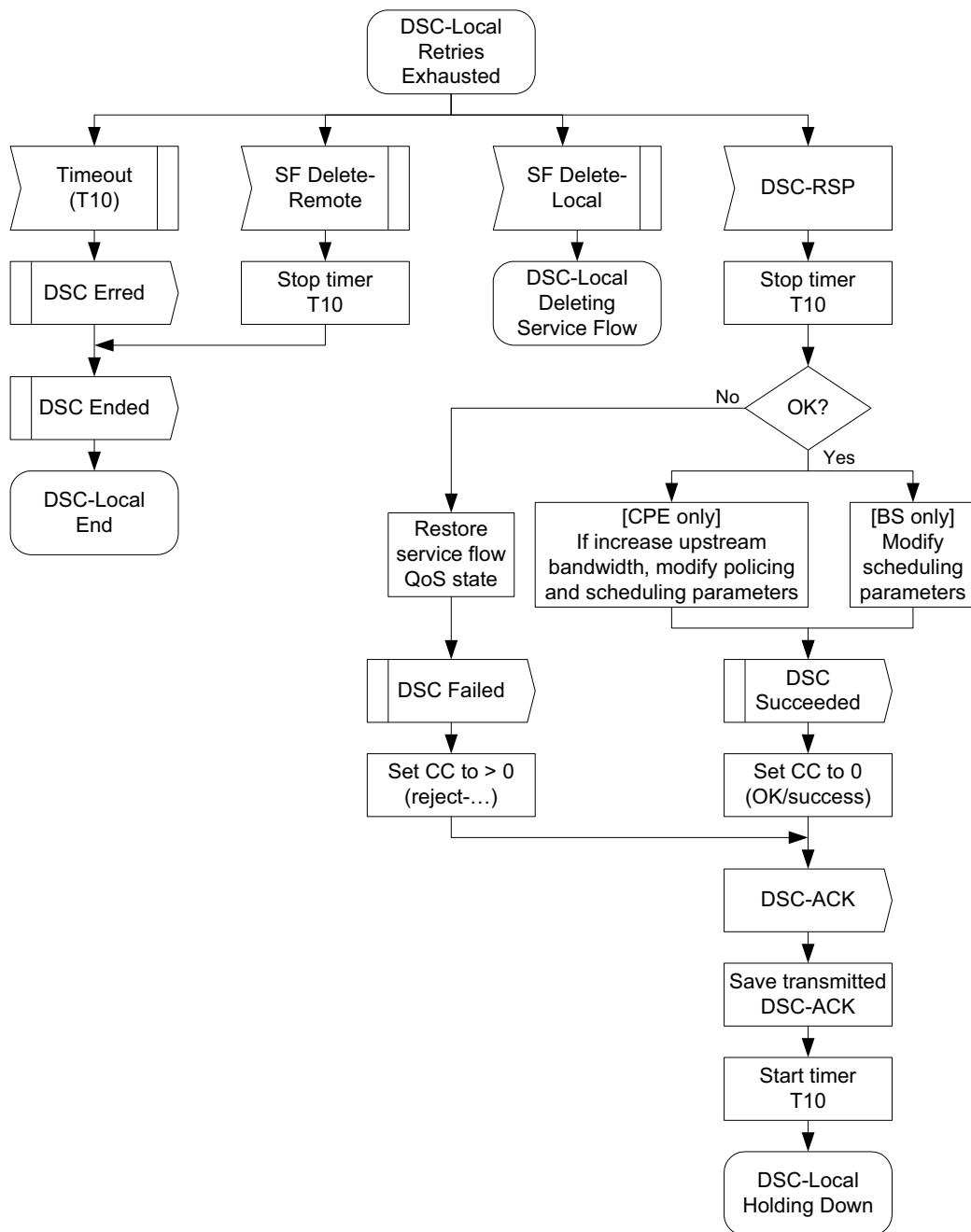
Figure 79 — DSC—Locally-Initiated Transaction Begin state flow diagram



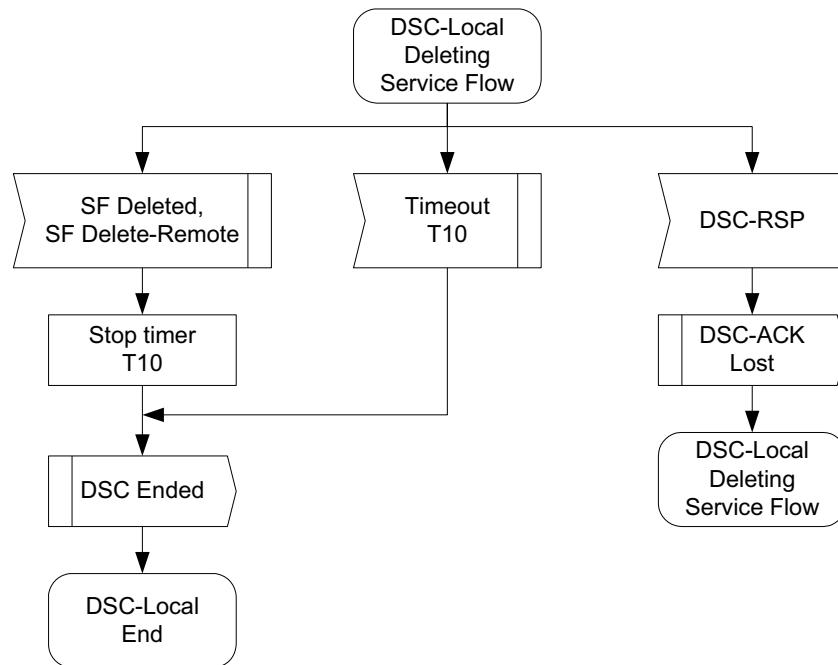
**Figure 80 — DSC—Locally-Initiated Transaction DSC-RSP Pending state flow diagram**



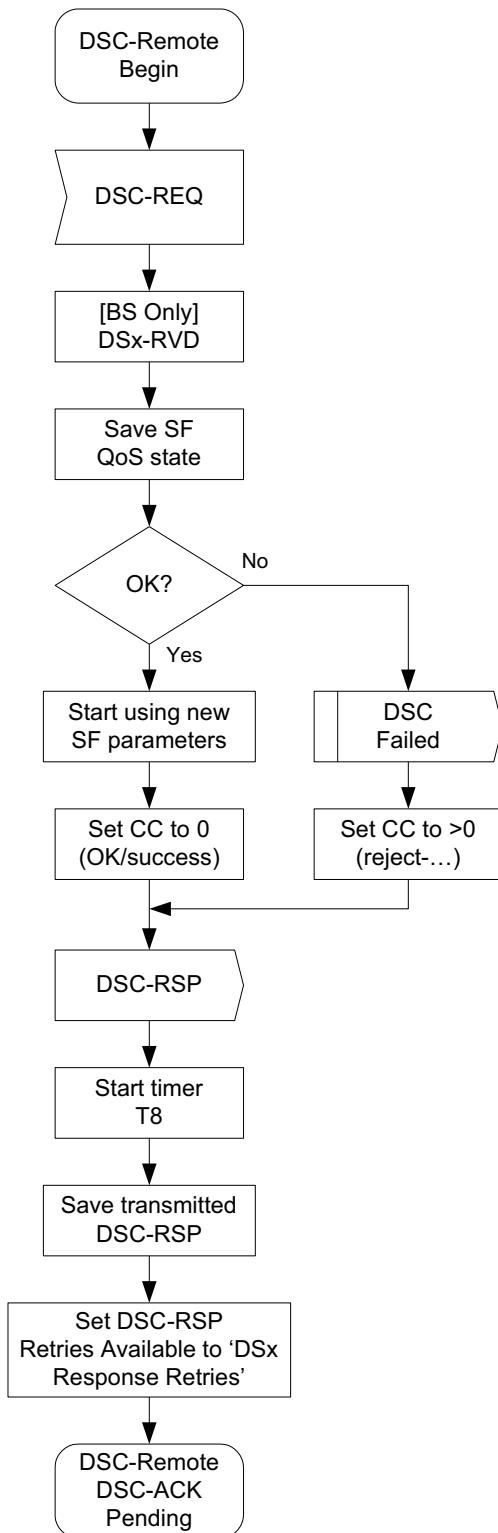
**Figure 81 — DSC—Locally-Initiated Transaction Holding Down state flow diagram**



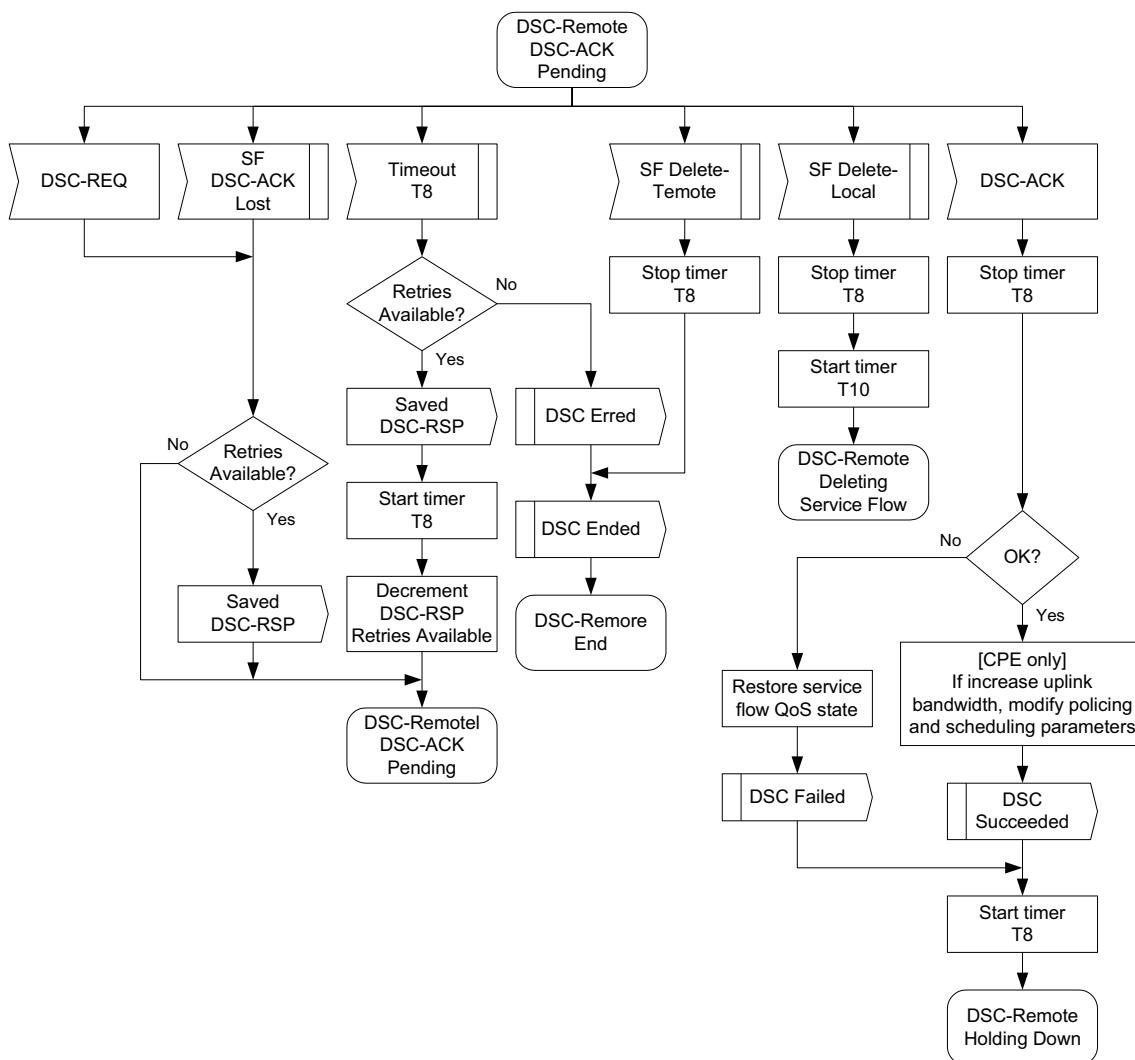
**Figure 82 — DSC—Locally-Initiated Transaction Retries Exhausted state flow diagram**



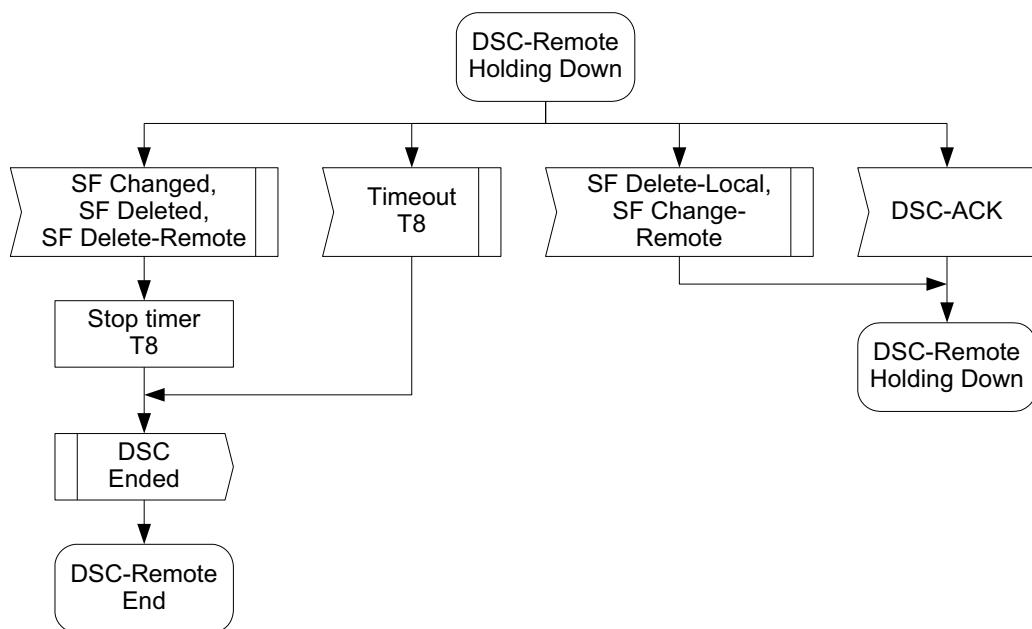
**Figure 83 — DSC—Locally-Initiated Transaction Deleting Service Flow state flow diagram**



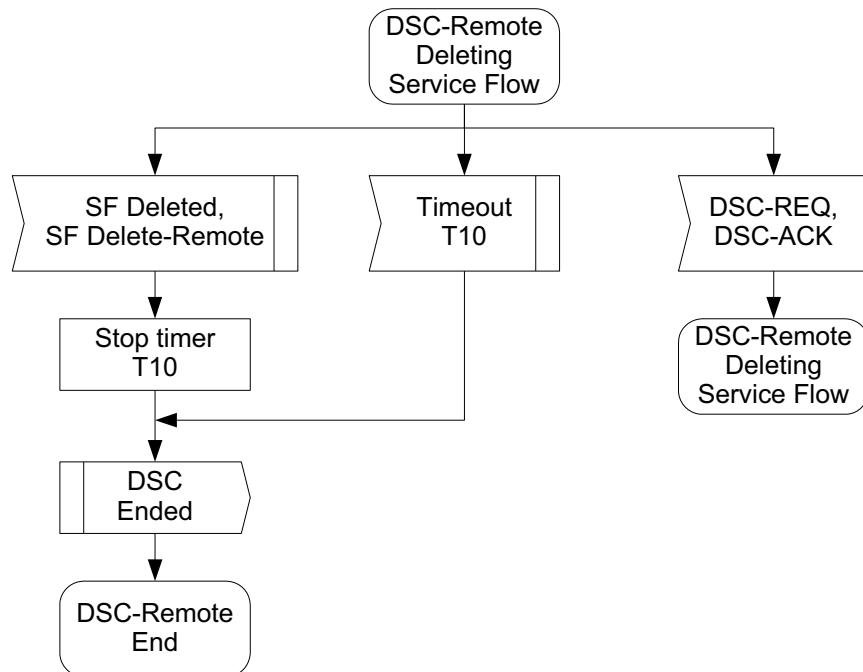
**Figure 84 — DSC—Remotely-Initiated Transaction Begin state flow diagram**



**Figure 85 — DSC—Remotely-Initiated Transaction DSC-ACK Pending state flow diagram**



**Figure 86 — DSC—Remotely-Initiated Transaction Holding Down state flow diagram**



**Figure 87 — DSC—Remotely-Initiated Transaction Deleting Service Flow state flow diagram**

### 7.18.9.5 Dynamic Service Deletion

Any service flow can be deleted with the DSD messages. When a service flow is deleted, all resources associated with it are released. If a service flow for a provisioned service is deleted, the ability to re-establish the service flow for that service is network management dependent. Therefore, care should be taken before deleting such service flows. However, the deletion of a provisioned service flow shall not cause a CPE to reinitialize.

#### 7.18.9.5.1 CPE-initiated DSD

A CPE wishing to delete a service flow generates a delete request to the BS using a DSD-REQ message. The BS removes the service flow and generates a response using a DSD-RSP message. This process is illustrated in Table 182. Only one service flow can be deleted per DSD-REQ.

**Table 182 — DSD-initiated from CPE**

CPE	BS
Service flow no longer needed	
Delete service flow	
Send DSD-REQ	=====DSD-REQ=====>
Set Timer T7	Receive DSD-REQ Verify CPE is service flow “owner”
	Delete service flow
Receive DSD-RSP	<=====DSD-RSP=====
	Send DSD-RSP

#### 7.18.9.5.2 BS-initiated DSD

A BS wishing to delete a dynamic service flow generates a delete request to the associated CPE using a DSD-REQ. The CPE removes the service flow and generates a response using a DSD-RSP. This process is illustrated in Table 183. Only one service flow can be deleted per DSD-REQ.

**Table 183 — DSD-initiated from BS**

CPE	BS
	Service flow no longer needed Delete service flow Determine associated CPE for this service flow
Receive DSD-REQ Delete service flow	<=====DSD-REQ=====> Send DSD-REQ
Send DSD-RSP	=====DSD-RSP=====> Delete service flow Receive DSD-RSP

#### 7.18.9.5.3 DSD state transition diagrams

DSD state transition diagrams are shown in Figure 88–Figure 92.

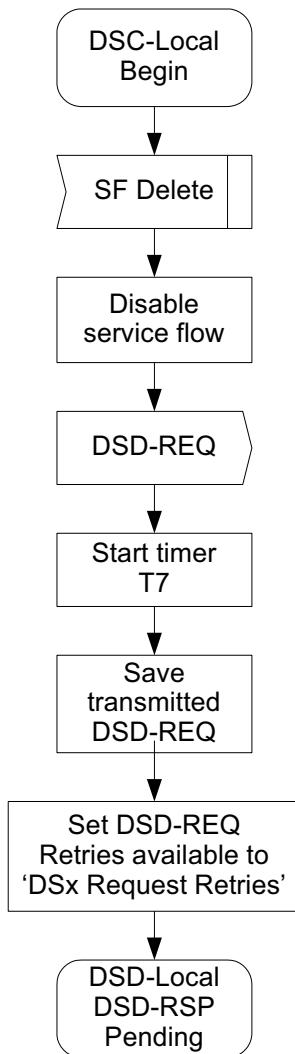


Figure 88 — DSD—Locally-initiated Transaction Begin state flow diagram

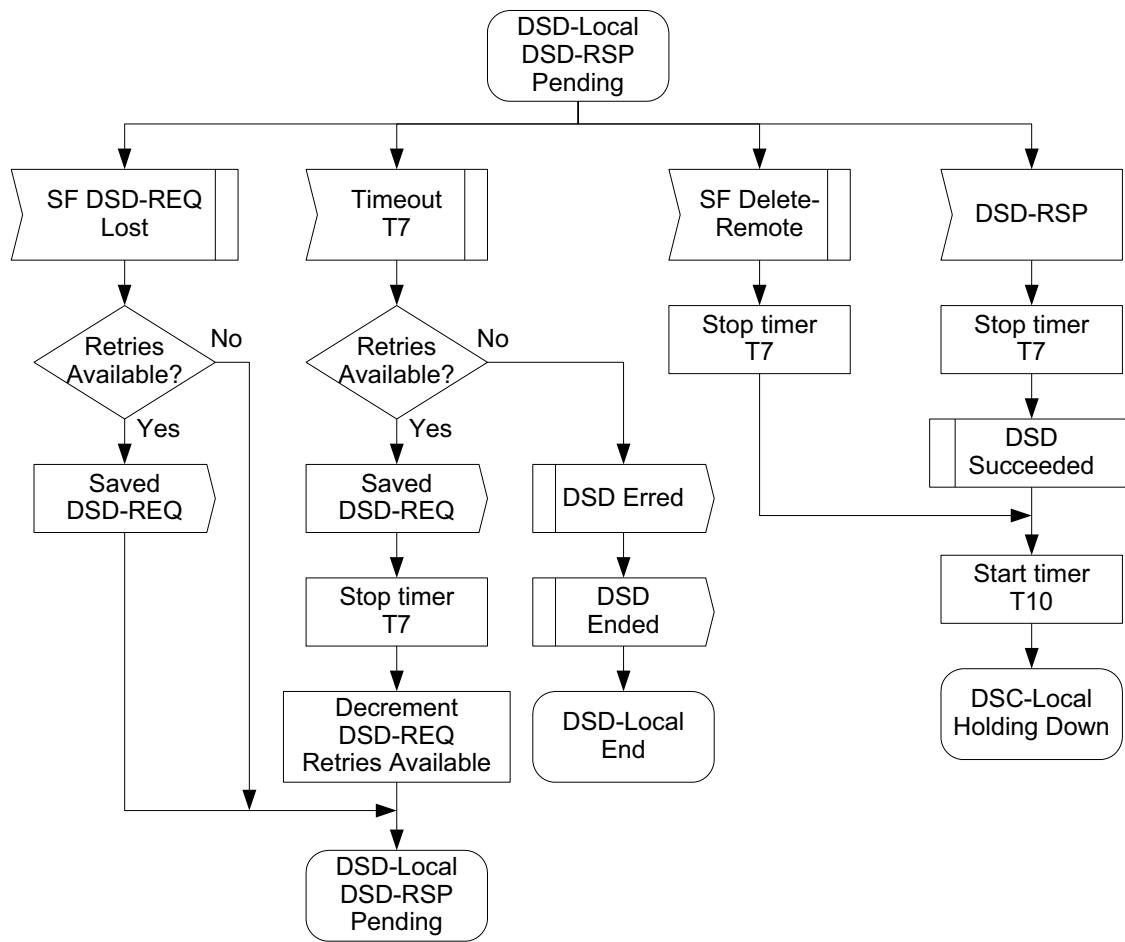


Figure 89 — DSD—Locally-initiated Transaction DSD-RSP Pending state flow diagram

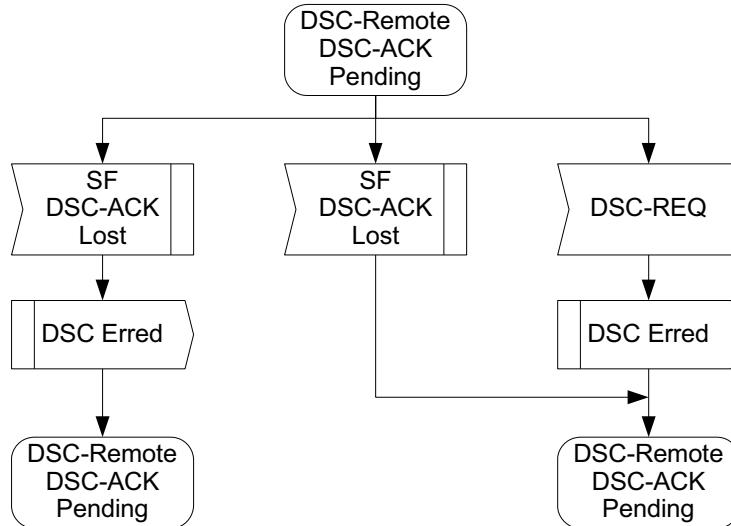


Figure 90 — DSD—Locally-initiated Transaction Holding Down state flow diagram

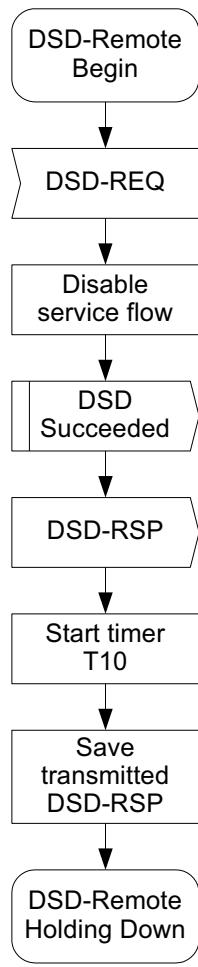
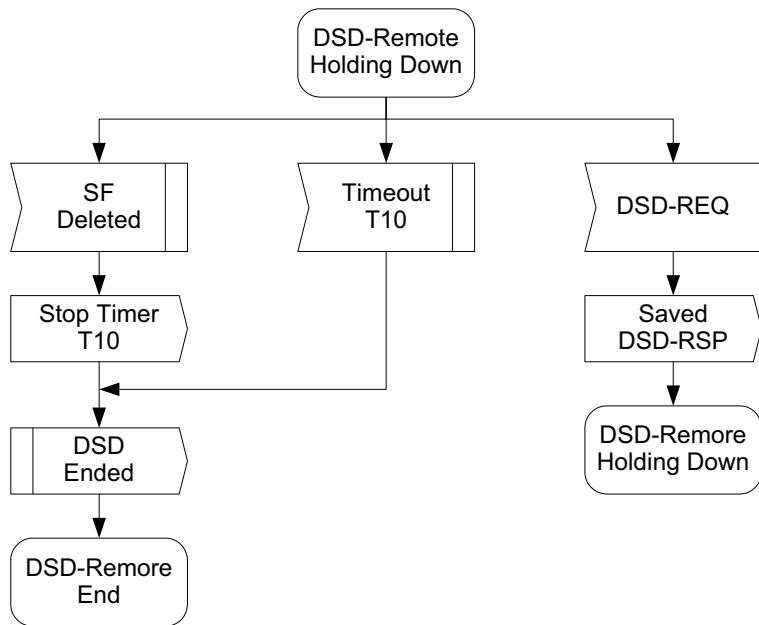


Figure 91 — DSD—Remotely-initiated Transaction Begin state flow diagram



**Figure 92 — DSD—Remotely-initiated Transaction Holding Down state flow diagram**

## 7.19 Incumbent protection

To address incumbents' detection and protection, numerous techniques are available by means of spectrum management, quiet period management, distributed spectrum sensing, detection algorithms, and measurements. The MAC provides all the capabilities for the effective detection and protection of incumbent services. A comprehensive set of spectrum management and measurement commands is available, which gives the BS the necessary flexibility to manage CPEs and obtain a reliable spectrum occupancy map of its cell and, if needed, change its operating parameters.

CPEs also have various ways to report measured information to the BS. In addition to a pool of MAC management messages, UCSs can also be reported either through fields located in the generic MAC header itself, or through the UCS contention or CDMA messages. The simplified lifecycle of a single measurement activity is depicted in Figure 94. Each of the phases of this lifecycle requires special handling, and specific protocols and algorithms are described in this subclause and in 10.3 to address their requirements. In the following subclauses, a detailed overview of the mandatory mechanisms available in the MAC for the management of incumbent measurements throughout their lifecycle is provided.

### 7.19.1 Measurements classification

Measurements can be of the following types: in-band (i.e., measurements made on the operating channel and its first adjacent channels), and out-of-band (i.e., measurements made on other channels than the above three channels).

### 7.19.2 Measurements management

Besides the automated sensing measurements that are carried out autonomously by the SSA (see 10.3.3 and 10.3.4), which allow for detection of urgent interference situations for in-band sensing and which allow for clearing a minimum number of channels on the backup list (see 10.3.4) for out-of-band sensing, the MAC also supports a hierarchical measurement philosophy implemented by four management messages,

namely, BLM-REQ, BLM-RSP, BLM-REP, and BLM-ACK (see Table 19 and 7.7.18). These management messages are used between the SM at the BS and the SSA at the BS and CPEs to perform a wide range of measurement activities, either related to incumbents or to self-coexistence. With these messages, both in-band and out-of-band specific measurements can be performed.

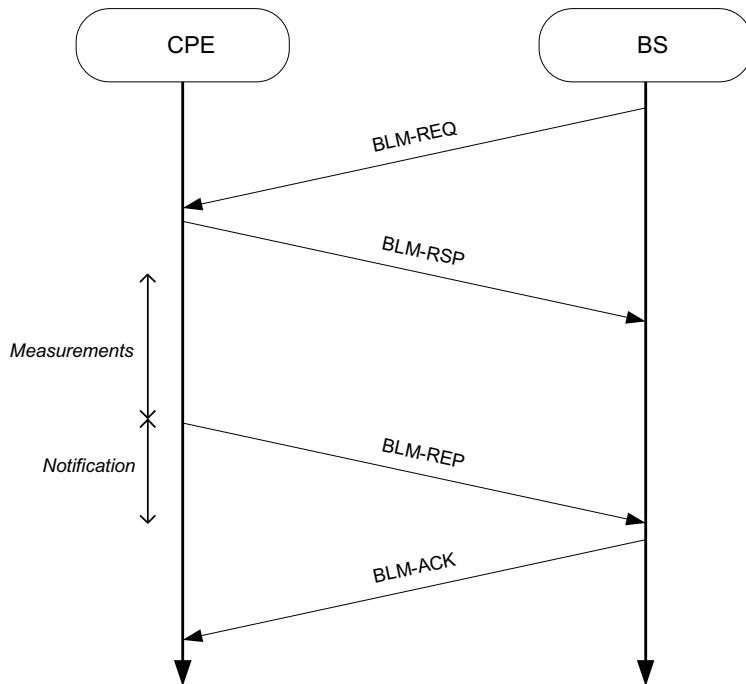
In a single BLM-REQ command, the BS may simultaneously request SSAs to perform several types of measurements in a number of channels. Thus, a BLM-REQ is formed by a collection of single measurement requests. Each single measurement request specifies several parameters such as the periodicity with which the BS wants SSAs to report back to it or if reports are to be autonomous. Furthermore, single measurement requests also define timing parameters, as illustrated in Figure 16. Upon receiving a BLM-REQ message, the SSA shall examine this message's header and determine whether it is required to respond back with a BLM-RSP message. In all cases, the SSA shall carry out all the measurements as requested by the BS, if these are supported. SSAs shall report back to the BS with a BLM-REP message that contains measurement results of what has been requested by the BS in the corresponding BLM-REQ message. These reports shall be sent with the periodicity specified by the BS in the corresponding BLM-REQ message. Once the measurement report message is successfully received at the BS, the BS shall respond back to the SSA with a BLM-ACK message to acknowledge its reception. In case the SSA does not hear the BLM-ACK message from the BS after some pre-specified timeout T29 (see Table 276), it shall assume that its BLM-REP message was lost and shall initiate retransmission of this BLM-REP message. The SSA shall attempt retransmission of measurement report messages up to the values specified for BLM-REP Retries (see Table 276). Once the BLM-ACK message is successfully received at the SSA, it shall then clear its local statistics to prepare for future measurements. Figure 93 illustrates the measurement message flow between the BS and a SSA.

The nature of the SSA reports received by the SM at the BS can be essentially of two types: regular or urgent. Regular reports refer to the cases where the BS has explicitly requested SSAs to report back to it with a certain periodicity (and so the BS can allocate sufficient upstream resources beforehand), and also when SSAs are allowed to report autonomously, for example, whenever enough data has been collected (in this case, CPEs may have to request for upstream resource allocation).

Urgent reports are those that take place as a result of the automated in-band sensing carried out by the SSA (see 10.3.3) whenever an incumbent is detected in the current operating channel of an IEEE 802.22 cell or on either of its adjacent channels. The BS shall provide upstream UCS contention periods on a regular basis. The CPEs can then notify the BS about potential interference by sending the UCS notification bit in the GMH and sending in its own upstream allocations or using one of these UCS contention periods.

Subsequent reports can then be requested through the BLM-REQ MAC message immediately after detection of an incumbent to further quantify the situation (see 7.19.4). In this case, the BS shall provide periodic bandwidth request opportunities during which CPEs can report critical measurement results, or else the CPE can use any of its own reservations for this purpose.

In case the CPE uses UCS notification, the BS does not send an acknowledgment. The BS can then send a BLM-REQ message and allocate bandwidth for the CPE to transmit the complete measurement report message (BLM-REP), and the corresponding acknowledgment (BLM-ACK) is sent on the next downstream opportunity following the reception of the measurement report.



**Figure 93 — Measurement message flow between BS and CPE**

Once the BS receives a UCS notification from its various CPEs, it may wish to take steps to resolve any potential interference situation with incumbents. To this end, a rich set of channel management messages is supported through the Incumbent Detection Recovery Protocol (IDRP) (see Table 19 and 7.7.17) that enables the BS to act promptly and effectively. The IDRP shall also be used as part of the recovery procedure (see 7.19.5). In case of self-coexistence interference situations, other mechanisms available are “spectrum etiquette” and “on-demand frame-based contention,” and their use is discussed in 7.20.

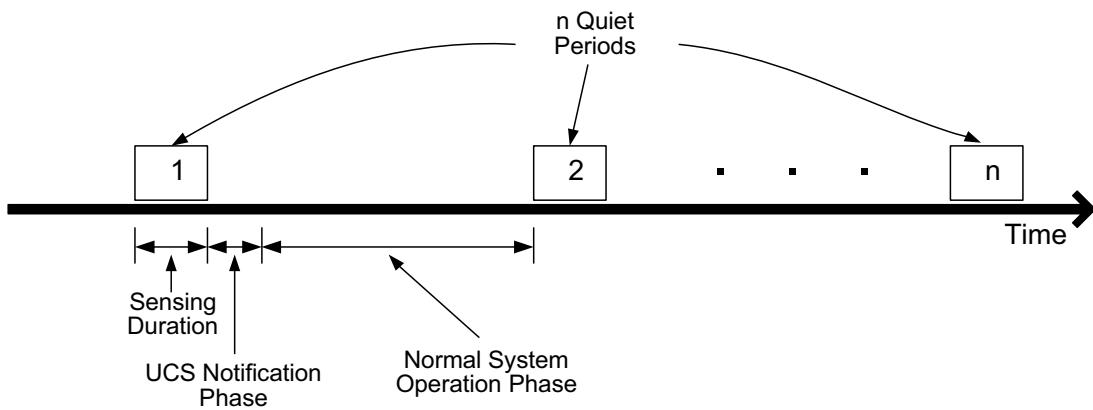
In order for the BS to poll measurements from a group of CPEs, the BS shall establish a multicast group and assign said CPEs to the group (see 7.17), as well as establish a Group Security Association (GSA) and keying mechanism to protect the DS measurement report request messages.

### 7.19.3 Incumbent detection

The MAC is able to fully manage periodic sensing of incumbent transmissions. This is done through the quiet period management mechanisms described in 7.21.

### 7.19.4 Measurement report and notification

Channels occupied by incumbents change over time, and this is the reason why CPEs and BSs shall periodically sense the medium to determine the presence or absence of incumbents. In a situation where an incumbent is operating on the same channel or on adjacent channels relative to the channel used by the IEEE 802.22 cell (i.e., in-band), certain CPEs (or even the BS itself) will detect the incumbent’s transmitted signal through the distributed sensing technique. Whenever this happens, the CPE shall immediately notify and report this situation to the BS. The SSAs at both BS and CPEs shall execute automatic algorithms that allow the reliable detection of incumbent signals. The procedure is described in 10.3.3.



**Figure 94 — Incumbent notification phases**

#### 7.19.4.1 Notification phase for sensing

After a quiet period, the SSA at both the BS and CPEs will have performed incumbent measurements. If the BS itself detected the presence of an in-band incumbent, it can proceed as discussed in 7.19.2. Regardless of that, in the next frame (and optionally in subsequent frames) right after the end of the quiet period the BS may limit its downstream transmissions to the minimum necessary, and devote most of its frame allocation for upstream traffic.<sup>19</sup>

More specifically, the BS may decide to provide for more upstream bandwidth allocation for those CPEs that indicated the presence of incumbents, and hence obtain a more comprehensive report.

Those CPEs who have not been allocated dedicated upstream bandwidth, but who have detected the presence of an incumbent during the quiet period, shall use the UCS notification intervals for the purpose of notifying the BS. If no such UCS notification intervals are available, the CPE shall wait for subsequent frames where the BS will either allocate upstream bandwidth for this particular CPE or schedule UCS notification intervals. In the case of the contention-based UCS interval, the burst shall contain 7 symbols to allow the pilot carriers to properly correct for the transmission channel distortion.

It is important to note that only those CPEs that have not been allocated upstream bandwidth in a frame are allowed to use the UCS notification intervals in that frame (see 7.19.4.1.2 for further details). Those CPEs having upstream bandwidth allocation shall use the UCS flag bit in the generic MAC header of their upstream transmission (see 7.6.1.1).

To improve the reliability and performance of the system, two types of UCS notification windows are possible (see 7.19.4.1.2). In the case of a contention-based UCS notification, the BS shall allocate the size of a UCS notification interval to be big enough to fit one or a few generic MAC headers (which is the smallest unit of information for incumbent notification purposes—see 7.6.1.1). The CPEs that have detected an incumbent in-band shall then contend for this UCS notification interval to immediately send their MAC header with the UCS flag set.

In the case of a CDMA UCS notification, the CPE shall transmit its CDMA code in the corresponding CDMA UCS opportunistic allocation. This will allow the BS to identify right away that there is an UCS and allow it to take the necessary measures but it will not tell the BS with which CPE this situation occurred. To identify which CPE has detected an incumbent, the BS will need to issue a CDMA\_Allocation\_IE for the CPE to respond. This bandwidth grant will allow the CPE the opportunity to

<sup>19</sup> The number of frames will highly depend on the number of CPEs.

report on its UCS. The use of both of these types of notification schemes will provide a quick and reliable report from the CPEs to the BS to be made in the first stage, and allow the BS to query for a more detailed report on the UCS, in a second stage, by sending a BLM-REQ message and granting more upstream bandwidth resources to those CPEs that claim having detected the presence of incumbents.

At any time, the BS should allocate a minimum number of UCS notification intervals for the purpose of incumbent notification. If the detection of an incumbent by a CPE takes place during normal operation, the CPE can notify the BS through its granted upstream bandwidth allocation in the frame or, if not available, through UCS notification. These are discussed in the subclauses that follow.

#### **7.19.4.1.1 CPEs with upstream bandwidth allocation**

In case the CPE has an upstream bandwidth allocation to send the UCS notification to the BS by setting the UCS flag in the generic MAC header (see Table 3), it shall do so in the first available opportunity. By setting this field, it will indicate to the BS that there is an UCS. Where incumbent protection is concerned, the UCS notification messages take precedence over all other messages. Once the BS receives the UCS notification message, it proceeds as outlined in 7.19.2 and takes any necessary steps to resolve the coexistence situation.

Once the BS is notified through the UCS notification flag in the MAC header, it can proceed in different ways. For example, once it receives this UCS notification, it may query the reporting CPE through the BLM-REQ message and allocate more upstream resources to this CPE in the following frame so that this CPE can send a more detailed report via a BLM-REP. Alternatively, the BS may set the MRT field in the corresponding allocation of this CPE in the US-MAP message (see Table 35), and this will specifically solicit from this CPE more detailed measurement information that shall be sent in its next upstream allocation. Another possibility is for the BS to play safe and immediately issue channel management messages for a channel switch in order to resolve the situation. Finally, one last option could be for the BS to delay taking any immediate action and wait for feedback from other CPEs.

#### **7.19.4.1.2 CPEs without upstream bandwidth allocation**

Even if the CPE does not have any upstream bandwidth allocation with its BS, it still needs to report to the BS about the UCS with incumbents. In this case, the CPE shall use the opportunistic upstream UCS notification intervals in order to reach the BS and indicate the UCS with incumbents. The opportunistic UCS notification intervals shall always be allocated by the BS in the same time/frequency region across frames. This will allow even those CPEs who have suddenly started to experience harmful interference from an incumbent service to reliably notify the BS about the presence of the incumbent service, as the location of the UCS notification intervals is always known. The CPE shall notify the BS in the UCS notification interval immediately after the incumbent service is detected, while it is still synchronized to the BS.

It is important to highlight that the only situation when CPEs are allowed to use UCS notification intervals is when they do not have upstream bandwidth allocation but yet need to reach the BS and report a UCS with incumbents. There are two possible ways a BS can allocate opportunistic UCS notification windows in its upstream: Contention-based UCS notification and CDMA UCS notification. The CPEs shall use these intervals in accordance with their specific type.

##### **7.19.4.1.2.1 Contention-based UCS notification**

In reporting a UCS through the use of the contention-based UCS notification intervals, the CPE shall transmit only the generic MAC header, typically without any payload. In this MAC header, the CPE shall set the UCS field accordingly so as to allow the BS to be notified of the UCS. Upon receiving the message from the CPE, the BS shall proceed as discussed in 7.19.2. If requested by the BS through either a BLM-REQ message or by the MRT field in the US-MAP (see Table 35), the CPE shall send a single measurement report describing the potential interference situation in a subsequent field (see 7.7.18.3.1.1).

#### 7.19.4.1.2.2 CDMA UCS notification

In addition to the contention-based UCS notification window described previously, the PHY also supports the use of a CDMA mechanism for the purpose of UCS notification.

As specified in 7.7.3.1, the PHY has available a subset of UCS notification codes that shall be used for CDMA UCS notification. The CPE, upon needing to make a UCS notification, shall select, with equal probability, a UCS notification code from the code subset allocated to UCS notification. This UCS notification code shall be modulated onto the specified upstream opportunistic subchannels and transmitted during the appropriate CDMA UCS notification window (see Table 35 for UIUC=4).

Upon detection, the BS shall grant an upstream allocation for the CPE. The BS does not respond with an allocation on the CPE's SID and Basic FID since it is not yet known at that time. Instead, it broadcasts a CDMA\_Allocation\_IE, which specifies the code that was used by the CPE. This allows the CPE to determine whether it has been given an allocation by matching the CDMA code that he used for the CDMA UCS notification message and the code broadcast by the BS. The CPE shall use the allocation to transmit a MAC PDU with the UCS field in the MAC header properly set. In addition, if allowed by the BS, data could also be transmitted in this allocation as indicated by the Usage field—see Table 37).

If the BS does not issue the CDMA\_Allocation\_IE described above, the CPE shall assume that the Code transmission resulted in a collision and follow the contention resolution as specified in 7.13.

#### 7.19.5 Incumbent detection recovery

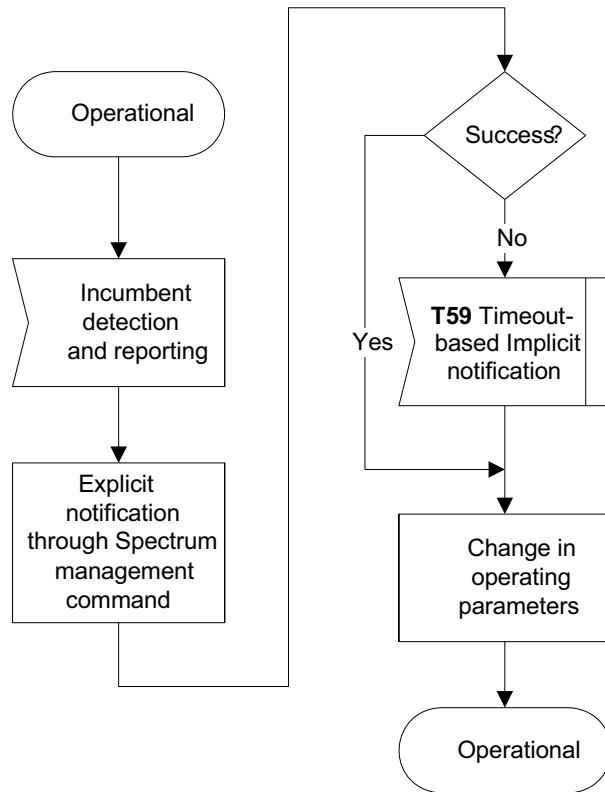
This subclause describes the incumbent detection recovery protocol (IDRP), which is used by the BS and CPEs to restore service under an UCS due to incumbent detection.

The IDRP is executed by BS and CPEs. When the CPE detects and reports an incumbent on the operating channel or its adjacent channels, it expects a notification from the BS. There are two types of notification: explicit and implicit. The explicit notification is used by the BS if it decides to execute a spectrum management command, in which case the BS transmits a spectrum management message to CPEs (e.g., a channel switching request message CHS-REQ) providing a way to notify CPEs and re-establish normal operation in a timely manner on another operating channel. However, if the reporting CPE does not receive the spectrum management message, it uses a timer to identify whether action is needed to protect the detected incumbent and maintain connectivity with the BS. Therefore, after sending the incumbent detection notification, the CPE starts the timer T56 that is preset at the value given in Table 276, and if this timer expires before an explicit notification is received from the BS, the CPE concludes that the operating channel is under interference and immediately switches to the first backup channel on its list. Figure 95 depicts the explicit and implicit notification mechanisms, while Figure 96 and Figure 97 show the details of IDRP for the BS and CPE, respectively.

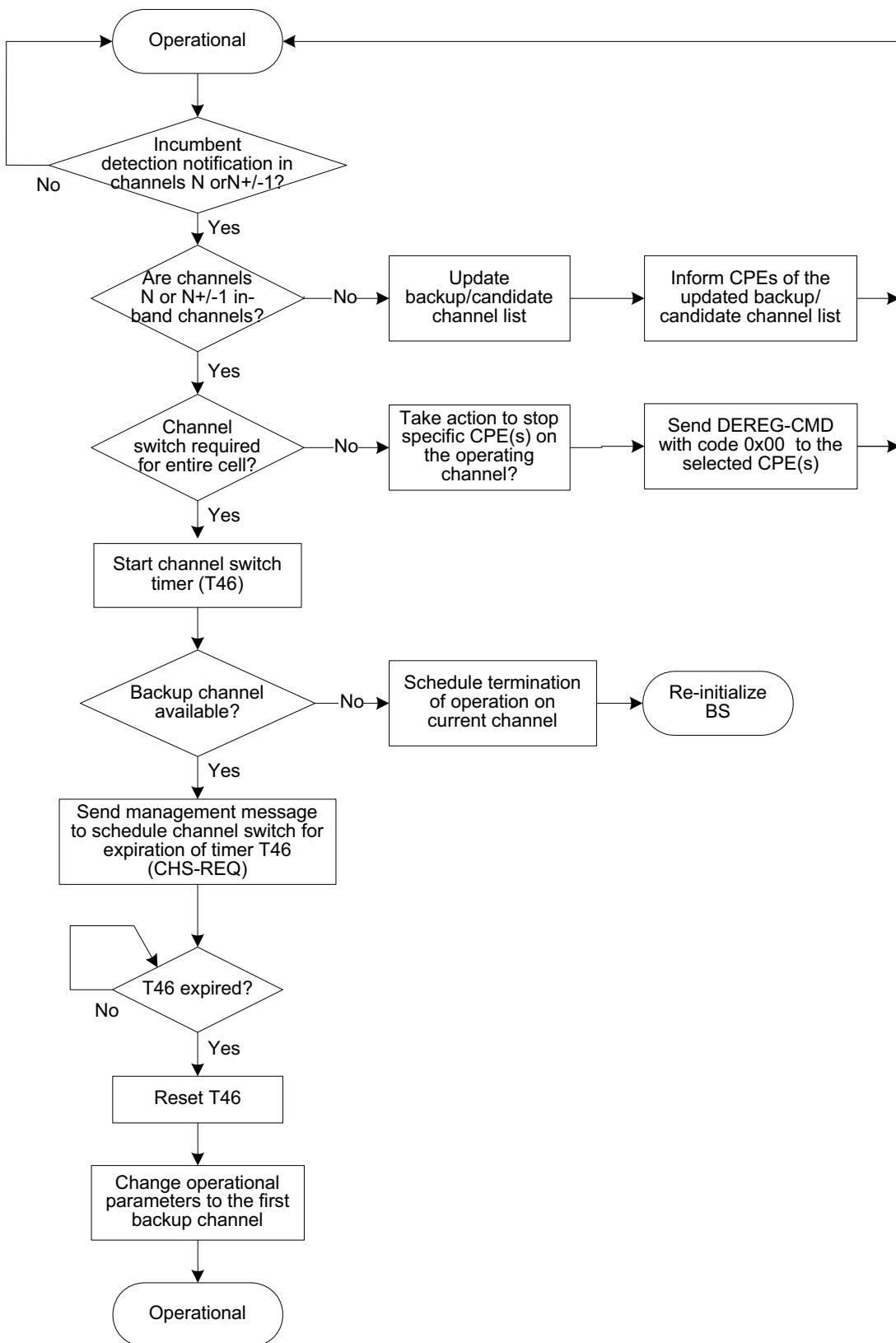
Figure 96 describes the detailed procedure executed by the BS, which starts with an incumbent detection event, which can be triggered by an incumbent detection notification received from one or more CPEs, or by the BS's own measurements or external information (e.g., database updates). In such a situation, the BS shall update its local channel status information and if the affected channel is the operating channel, the BS shall notify the CPEs of the action to be taken by sending a spectrum management command. As part of the procedure, the BS shall also update the list of backup channels when needed.

In the case of a CPE (see Figure 97), the first step in IDRP upon detection of a primary radio service is to notify the BS and await further instructions (this can be done a few times up to a pre-determined amount of repetitions). In case the CPE does not receive a spectrum management message from the BS, the CPE shall try to find the transmission from the BS and continue its operation on the first backup channel, if not, on the second backup channel and so on. If the CPE cannot re-establish communication with the BS on any of the backup channels, the CPE initialization procedure shall be triggered.

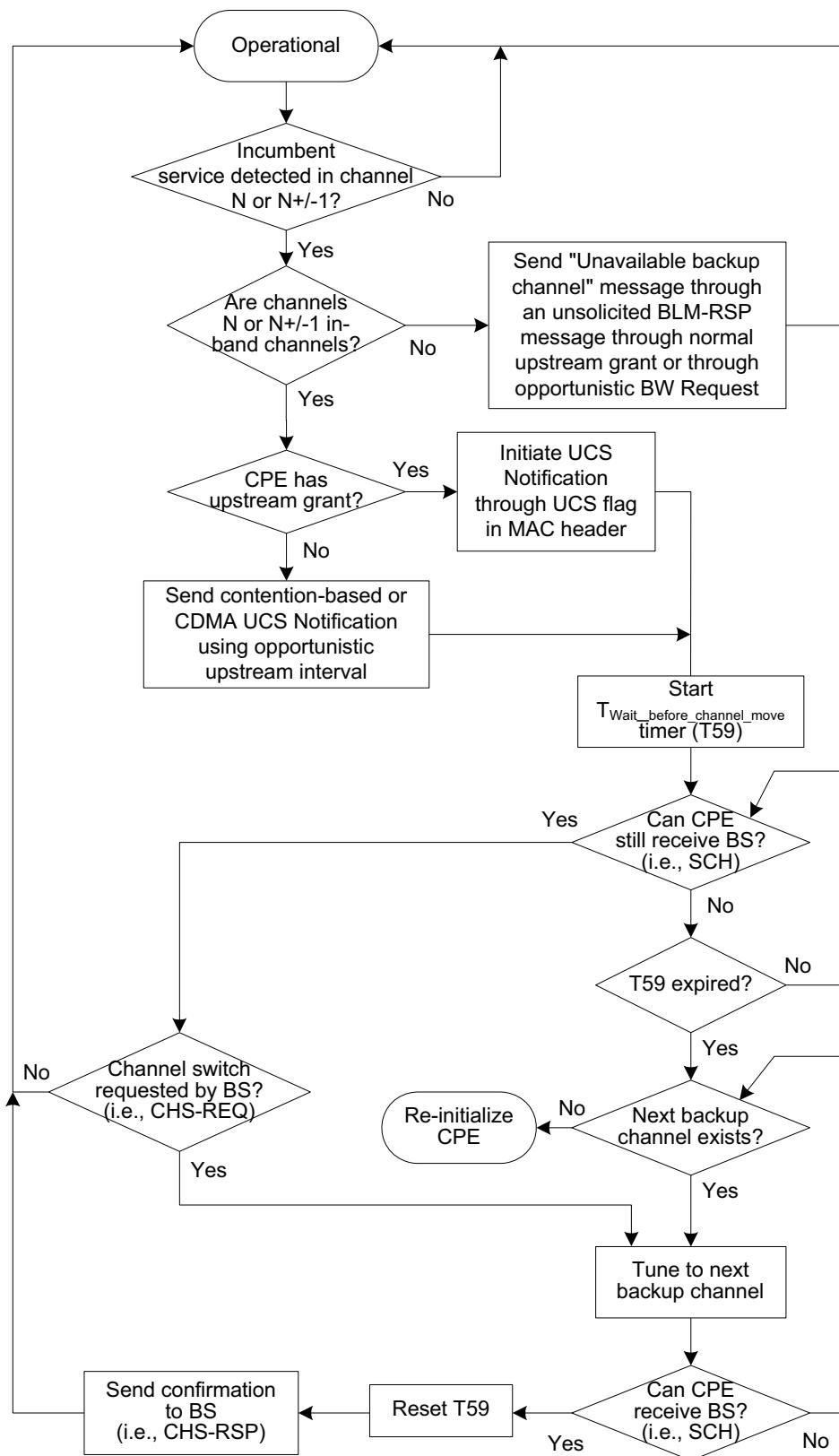
The success of the recovery procedure will depend on the availability of backup channels and in order to maintain a list of available backup channels, CPEs shall use their idle time to perform measurements to keep track of the availability of backup channels as described in 10.3.4. For this purpose, the BS shall provide sufficient idle time to the CPEs for them to “clear” a sufficient number of backup channels (see Figure 180 and 7.7.18.3.1.4). The BS can also request CPEs to sense some backup channels through the BLM-REQ message (see 7.7.18.1). Every CPE shall perform this procedure according to a repetition period of execution as specified by the Channel Monitoring Requirement for acquiring a channel in Table A.13.



**Figure 95 —Explicit and implicit notification mechanisms in IDRP**



**Figure 96 — IDRP at BS**



**Figure 97 — IDRP at CPE**

### 7.19.6 DFS for incumbent protection

The DFS model is supported through the quiet period management mechanism (see 7.21), measurement messages (see 7.7.18), and channel management messages (see 7.7.17). This framework allows for the BS to control and implement the necessary behavior to sense and protect the incumbent services.

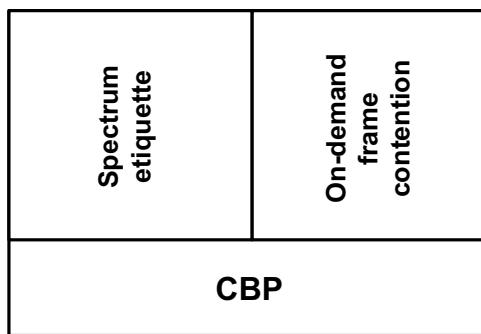
## 7.20 Self-coexistence

Coexistence is critical for the IEEE 802.22 air interface, which is required to include incumbent detection and protection mechanisms as discussed in 7.19 as well as self-coexistence measures. With regards to self-coexistence, the CBP protocol is used to exchange coexistence beacons to achieve efficient self-coexistence among overlapping IEEE 802.22 cells. The combination of the incumbent protection and self-coexistence mechanisms forms a MAC layer that is highly flexible and adaptive to the environment, and can react to sudden changes. This subclause discusses the various coexistence aspects available to address self-coexistence.

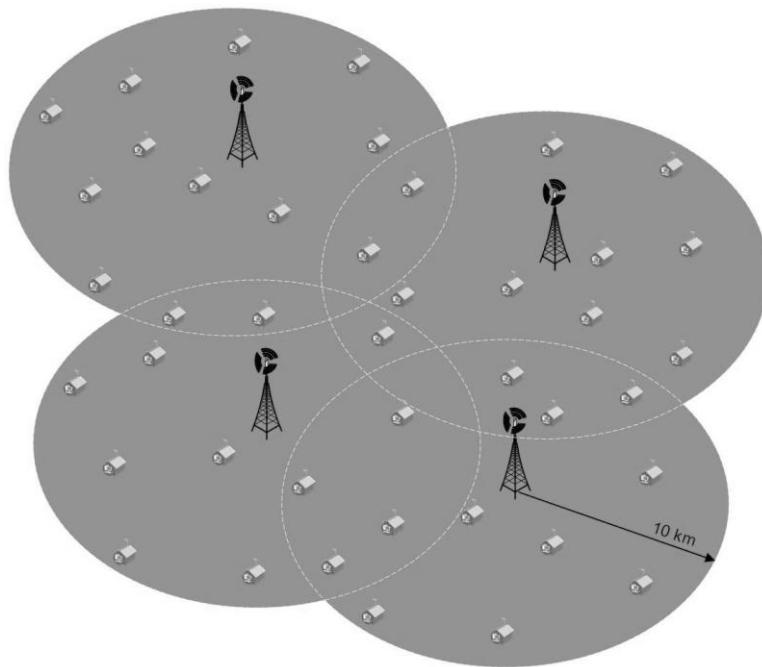
As depicted in Figure 99, multiple IEEE 802.22 BSs and CPEs may operate in the same vicinity and unless appropriate measures are taken at the air interface level, self-interference may render the IEEE 802.22 system useless. Even if directional antennas are used at the CPEs, self-coexistence issues are not at all overcome due to the fact that CPEs can be in line with more than one BS and also that the CPE antenna discrimination is relatively limited in the TV broadcast bands (see 9.12.1.1). This is further aggravated by the fact that IEEE 802.22 coverage range can potentially go up to 100 km, and hence its interference range and impact on other collocated IEEE 802.22 cells is larger than in any other existing unlicensed technology.

Because of the issues identified in the previous paragraph, the MAC layer shall address self-coexistence using a mandatory mechanism including the two following elements: spectrum etiquette (see 7.20.3.1) and on-demand frame contention (see 7.20.3.2). This self-coexistence mechanism as well as the required inter-WRAN communication architecture is depicted in Figure 98.

The Coexistence Beacon protocol (CBP) is the transport mechanism for the coexistence elements supported in this standard and CBP packets can be transmitted over-the-air or through the backhaul. The BSs and CPEs shall be capable of transmitting and receiving CBP packets over-the-air as specified in 9.5. In order to implement eventual coexistence mechanism over the backhaul, the CBP information from IEEE 802.22 base stations shall be encapsulated in IP packets for transport over the backhaul. A WRAN runs in normal mode by default and transits to self-coexistence mode when the WRAN can detect and decode an SCH or a CBP burst from an adjacent WRAN cell.



**Figure 98 — CBP as a transport mechanism for inter-WRAN communications and self-coexistence**



**Figure 99 — Example of IEEE 802.22 deployment configuration**

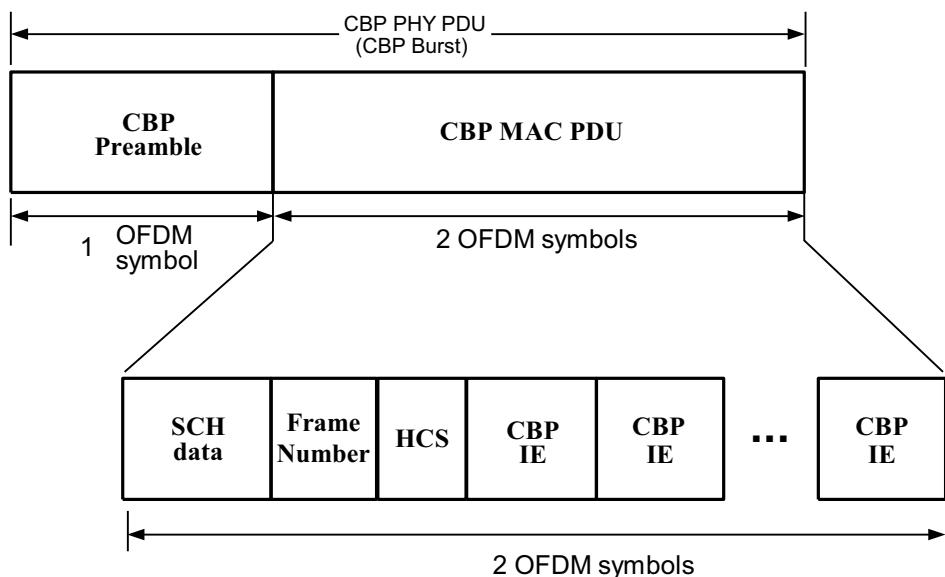
### 7.20.1 Coexistence Beacon Protocol (CBP)

To cope with serious self-interference issues that may arise in a real deployment scenario, the CBP protocol shall be employed. The CBP is a best-effort protocol based on coexistence beacon transmissions. Given the mechanism for synchronization of overlapping BSs (see 7.23) and that many CPEs can be used to augment redundancy of the transmission, successful delivery of coexistence beacon transmissions can be made highly reliable.

#### 7.20.1.1 CBP packet structure

The structure of a CBP packet (i.e., CBP PHY PDU) is shown in Figure 100. The burst starts with a CBP preamble that shall be common across all IEEE 802.22 networks (see 9.4.1.1), and that shall be different

from the superframe preamble. After the CBP preamble, the CBP MAC PDU as described in Table 8 shall be transmitted. The CBP MAC PDU shall be two OFDM symbols long.



**Figure 100 —Structure of a CBP packet**

By including the SCH data (which contains information about the IEEE 802.22 cell) as part of the beacon MAC header, the transmitting CPE or BS conveys necessary information to allow neighboring network discovery and coordination of quiet periods and SCWs. Including the SCH is a way to advertise the schedule of QPs and SCWs to CPEs in other neighboring cells.

The SCH information is needed in situations where WRANs are operating in different channels as well as when they are operating co-channel or adjacent channels. In the first case, the SCH information obtained through detecting and demodulation the SCH or through reception of the CBPs allows other WRANs to discover the schedule of QPs, which can be used for out-of-band sensing. In case WRANs are operating co-channel or on adjacent channels, the SCH, received through the CBPs, will signal the schedule of QPs and SCWs in addition to containing other IEs that can be used to signal frame allocations, when needed.

For communication using CBP over the backhaul, the CBP MAC PDU (see Figure 100) shall be encapsulated into an IP packet.

#### 7.20.1.2 SCW schedule and CBP Packet Transmission/Reception scheduling

IEEE 802.22 base stations and CPEs are capable of transmitting coexistence beacons (see 7.6.1.2) which can provide its recipients enough information to achieve reliable self-coexistence among overlapping IEEE 802.22 cells. The CBP also allows for device identification, as may be required by local regulation, for interference resolution as well as enhancement to the terrestrial geolocation process between CPEs within a cell (see 10.5.2.3).

Coexistence beacons are scheduled by the BS through the use of UIUCs 0 and 1 for Passive and Active modes respectively as indicated by the US-MAP (see Table 36). When selecting a UIUC equal to 0 or 1 for SCW scheduling, the SID contained in the MAP IE indicates which CPEs shall send the beacon, in case of Active mode, or which CPEs shall listen to the medium for detecting a beacon, in case of Passive mode, within the scheduled time of the SCW. This SID is either unicast (for a single CPE) or multicast (for a group of CPEs). The self-coexistence UIUC (see Table 41) can be unicast and multicast in active mode (UIUC=0) and it can be unicast, multicast, as well as broadcast when it is in passive mode (UIUC=1).

CBP packet transmissions shall be performed in the operating channel, but base stations and CPEs shall be capable of receiving CBP packets in any channel in which it is capable of operating. The BS specifies the channel number in which the CPE shall listen to the medium for a coexistence beacon (SCW in Passive mode). The channel number is included in the US-MAP for the UIUC=1. This allows the self-coexistence among IEEE 802.22 systems operating in the same channel and the monitoring of the quiet period scheduling carried by the CBP bursts in different channels for proper RF detection of incumbent signals in those channels that would otherwise be hidden by nearby WRAN transmissions.

The coexistence UIUCs identify the presence of a SCW at the end of the frame during which CBP packets can be exchanged. The SCW, when scheduled, occupies the last 5 symbols of the frame (see 7.7.4.1) and consists in one symbol buffer to absorb the propagation time, 3 symbols for the CBP PHY PDU and one last symbol to absorb propagation time.

The BS controls access to the medium within the SCW. The BS shall decide which CPEs transmit CBP packets in each scheduled active UIUC=0. Example of mechanisms that can be used by the BS for the selection of which CPEs are to transmit in each SCW in Active mode can be based on location information, clustering, or be as simple as selecting all CPEs.

All BSs involved in self-coexistence on the operating channel will need to align their operation with all of the declared SCWs of neighboring WRANs so that none continue its normal operation during these SCWs. All overlapping WRAN cells need to comply with the SCW scheduling either through active or passive use. When a WRAN cell reserves a SCW, this means that only that BS and its CPEs will be able to be active (i.e., transmit CBP bursts) during this SCW. For contention-based SCWs, all neighboring WRAN cells could be active during the SCW. This SCW scheduling takes place and applies only to the operating channel.

The CBP protocol can be used for communication and self-coexistence of WRANs on the same operating channel as well as synchronization to scheduled quiet periods across channels, which is enabled by setting the UIUC=0 in the US-MAP for a CPE or a group of CPEs once the CBP Relay message (7.7.23) has provided these CPEs with the proper content of the CBP burst to be transmitted. Note that different CPEs associated to the same BS can simultaneously communicate using CBP. For example, if two CPEs are associated with the same BS, during the same SCW, both can be transmitting in active mode, one of them can be transmitting a CBP packet on the operating channel while the other could be receiving on the same channel or on another channel. This is controlled by the BS when it schedules the SCWs in the US-MAP. It is assumed that within a cell, the BS will have the intelligence to select the right number and the right location of the “active” CPEs to minimize collisions while trying to maximize the communication redundancy.

In order to facilitate network discovery and to enable self-coexistence with neighboring WRANs, the BS shall maintain a minimal regular pattern of Active CBP transmissions (UIUC=0). Beyond inter-WRAN communication, the BS shall schedule Active and Passive mode SCW operation to enable mandatory CPE identification and optional terrestrial geolocation.

The BS shall schedule SCWs through the SCH when the BS initiates its normal operation and continuously thereafter according to its varying requirement as well as the requirements of the other WRAN cells in the area through coordination of these schedules by exchange of the SCH information through the CBP mechanism. If a BS wants to co-own a frame, it will be signaled as “01” whereas a frame that the BS does not want to co-own will be signaled as “00”.

The SCH includes SCW Cycle Length, SCW Cycle Offset, and SCW Cycle Frame Bitmap for the purpose of SCW scheduling, as defined in Table 1. SCW Cycle Length represents the cycle interval length between each successive superframe carrying SCWs, in number of superframes. The SCW Cycle Frame Bitmap specifies which frames (in a scheduled superframe) at the end of which a SCW is scheduled as well as the

SCW mode (reservation-based SCW vs. contention-based SCW). The field encoding of SCW Cycle Frame Bitmap is specified in Table 1.

The SCW Cycle Length and SCW Cycle Frame Bitmap parameters should be set according to the requirements for self-coexistence and inter-WRAN communications, and it should be based on a trade-off between the performance of inter-WRAN communications and the overhead represented by these SCWs.

Multiple WRANs operating on the same channel may share the same SCWs via contention or each WRAN may reserve its own SCWs depending on how they set up their regular SCWs patterns. Sharing of SCWs reduces the total overhead in the channel, but on the other hand, reservation of SCWs enables contention-free CBP transmissions. The decision on whether to share or reserve SCWs will depend on the total overhead generated by SCWs and the self-coexistence scenarios (e.g., number of neighboring WRANs on the same channel and number of CPEs in the overlap area that can provide a non-negligible transmission redundancy and, hence, probability of successful CBP transmission using contention-based SCWs). Moreover, the WRANs may change the schedule of their SCWs dynamically and therefore they may adjust the schedule to adapt to the self-coexistence scenarios.

The reservation of SCWs facilitates the contention-free CBP transmissions among the neighboring WRAN cells sharing the same channel, and it can be achieved by scheduling the SCWs such that it does not overlap with those of other neighboring WRANs. The procedure for this type of operation is as follows:

- During the initialization stage, the WRAN monitors the channel for at least 16 superframes (the maximum SCW Cycle Length) to discover neighboring WRANs and identifies their schedule of reservation-based SCWs by capturing and decoding the CBP packets from these neighboring WRANs.
- If a WRAN identifies another WRAN's schedule of reservation-based SCW (specified in SCW Cycle Frame Bitmap with 2-bit set to 11 or 10 in the corresponding frame, see Table 1), it shall regard these SCWs as reserved and shall set its own schedule of reservation-based SCWs so that it does not overlap with the SCWs reserved by the neighboring WRAN(s).
- With the above mechanism, the reservation conflict is low but it could still happen. To detect a potential conflict after the reservation is done, a WRAN can purposely skip the transmission of CBPs in its reserved SCWs and schedule its associated CPE to listen to the channel (using US-MAP with UIUC=1, passive mode) once in a while (irregularly) during the reserved SCWs. If a reservation conflict is identified, the WRAN will restart the process of scheduling SCWs.
- A WRAN can change its schedule of SCWs by updating SCW related parameters in the SCH.

Contention-based SCWs can be shared by neighboring WRANs. In other words, its neighbors can use these contention-based SCWs (combined with its own scheduled SCWs if available) for the transmission of CBPs following the random backoff mechanism defined later in this subclause. However, the WRAN scheduling those contention-based SCWs has the ownership of those SCWs. Other WRANs cannot use those SCWs for other purposes of transmissions nor can they cancel the schedules of these contention-based SCWs. The WRAN owning the contention based SCWs can reduce the frequency of these contention-based SCWs by cancelling some of its occurrences. At least one contention-based SCW shall be scheduled per SCW Cycle.

Co-ownership of these contention-based SCWs would avoid one BS removing the SCW used by other BSs. Hence, two neighboring WRANs can be the co-owners of a certain set of contention-based SCWs by each scheduling them in their SCH. In that case, if one WRAN cancels the schedule, the contention-based SCW stays scheduled until all other WRAN cells co-owning this SCW decide to cancel it. These other WRAN cells as well as the neighbor WRANs can still share those contention-based SCWs.

To mitigate collision of contention with neighboring WRANs, access to contention-based SCW shall use random backoff in units of contention-based SCWs. When a BS schedules its associated CPEs to transmit CBPs via contention-based SCWs, it shall wait for a random number (from 0 to 15 with uniform probability) of next available contention-based SCWs. For example, if the random number chosen is 0, the

BS shall schedule a CBP transmission via an US-MAP IE by accessing the first available contention based SCW from the transmission of the US-MAP IE. If the random number is 5, the BS shall schedule a CBP transmission via an US-MAP IE by accessing the sixth available contention based SCWs from the transmission of the US-MAP IE. A new base station shall have higher priority to access contention-based SCWs by using smaller backoff window. When a new BS attempts to transmit CBPs via contention-based SCWs, it shall wait for a random number from 0 to 7 with uniform probability (as opposed to 0 to 15 for an in-band/established network) of next available contention-based SCWs.

A BS can schedule CPEs in Passive mode (via US-MAP IEs) during SCWs reserved or shared by other neighboring WRANs in order to receive CBP packets from its own WRAN cell (from the BS and/or CPEs) or from the neighboring WRANs operating on the same channel. A BS can also schedule CPEs in Passive mode to listen to CBP burst on either of the adjacent channels for the purpose of localizing and synchronizing the quiet periods for proper in-band sensing. CPEs executing out-of-band sensing during their idle time shall listen to CBP bursts on other channels for the purpose of localizing the quiet periods for proper out-of-band sensing in coexistence situations in these channels (see 10.3.4). For the SCW in Passive mode, the BS shall define the schedule such that it can capture the required self-coexistence information from neighboring WRANs that may impact the WRAN operation. By definition, no other type of transmission shall be allowed during the SCWs. Therefore, any CPE may be scheduled in Passive mode during SCWs. Note that scheduling SCWs in Passive mode do not increase the overhead in the channel since it only requires listening for other CBP transmissions from neighboring cells.

The BS could also use other information available at the MAC layer to decide when and in which mode to generate a Coexistence UIUC, as long as the above generation rules are satisfied. One example can be found in 7.7.18.3.1.3, where the BS uses the CPE statistics report as the basis for triggering the execution of CBP (see 7.7.18.2).

When configuring an SCW for Active mode, the BS shall form the CBP MAC PDU by selecting which IEs (see Table 9) are to be included in the PDU, then setting the fields for those IEs. If CBP Protection is enabled (see 8.6.2.1), than the signature shall be calculated over the other IEs and fields of the Signature IE as the CBP MAC PDU is being assembled.

Once the CBP MAC PDU is assembled it shall be encapsulated in a CBP Relay message (see 7.7.23), and sent on the Primary Management FID if assigned to a single CPE SID or on the Multicast Management FID when assigned to the SID for a (multicast) group of CPEs. This shall be done no later than one frame prior to the frame for which the CPE is configured to use the SCW in Active mode. Upon receiving the CBP Relay message the CPE or CPEs shall un-encapsulate the CBP MAC PDU and transmit it on their next opportunity (e.g., Active mode SCW).

If the CBP MAC PDU is being transmitted during an Active mode SCW for the purpose of facilitating geolocation, then the CBP Device Identification IE (see 7.6.1.3.1.6) shall be added to the CBP MAC PDU when it is being formulated and sent to each CPE (e.g., unicast by the CBP Relay message on each CPE's Primary Management FID) that is being asked to participate in the current Active mode SCW.

### **7.20.1.3 CBP-based Neighboring Network Discovery**

In order to achieve self-coexistence, overlapping IEEE 802.22 systems must first discover the presence of each other, which can be done in two ways depending on the operational state of the BS or CPE—network entry and initialization or normal operation.

#### **7.20.1.3.1 Network Discovery during entry and initialization**

During network entry and initialization and before any data transmission takes place, the BS and CPE shall perform a network discovery procedure by scanning the wireless medium for CBP packets or SCH (transmitted in the beginning of every superframe). This discovery procedure is part of the BS and CPE initialization procedures described in 7.14.

In the case of BS initialization (see 7.14.1), this procedure is performed before the selection of the operating channel and it may be performed after or at the same time as the BS performs incumbent detection in all usable channels.

In the case of a CPE, this discovery procedure shall scan, at least, the BS's operating channel (N), its adjacent channels (i.e., N+1, and N-1), and channels N+2 and N-2. This is the minimal requirement so that other IEEE 802.22 cells operating in these channels are discovered and reported to the BS, such that sensing quiet periods are synchronized whenever needed to provide reliable TV sensing on N and N±1 since WRAN systems cannot operate on channels adjacent to TV operation and sensing needs to quiet down WRAN transmissions on the channel that it tries to sense as well as its adjacent channels.

A procedure to discover nearby IEEE 802.22 cells is also performed during normal operation as described in 7.20.1.3.2.

### **7.20.1.3.2 Network Discovery during normal operation**

During normal operation, the BS and CPEs can discover other nearby IEEE 802.22 cells by listening to the medium on the look out for CBP packets from other cells and, possibly, BS SCH transmissions from other IEEE 802.22 cells on different channels. This can be accomplished through the scheduling of the Coexistence UIUC = 1 for passive mode SCW. If a CBP packet or SCH is received by the CPE, it shall package that information and transport it to its BS (see Table 172).

The BS may use these mechanisms to discover other IEEE 802.22 cells operating in any channel, but in order to enable efficient coordination among neighboring IEEE 802.22 cells for self-coexistence and to allow efficient sensing, the BS shall use these mechanisms to discover other IEEE 802.22 cells operating in the same channel, in adjacent channels (N+1 and N-1), and in channels N+2 and N-2, and synchronize its quiet periods for sensing accordingly, using the procedure described in 7.21.2.

#### **7.20.1.3.2.1 Discovery with SCW**

The BS can discover other WRAN cells by scheduling SCWs in passive mode, during which, it may request one or more of its CPEs to listen to the current operating channel to look for CBP packets from other WRANs or to listen to other channels for CBP packets or SCH transmissions from other BSs or CPEs associated with other BSs. This mechanism is not only useful to discover new IEEE 802.22 cells, but it is also required to maintain coordination with existing neighboring cells to achieve self-coexistence.

In order to satisfy the requirements for coexistence and reliable and timely on-channel sensing, the BS shall schedule a sufficient number of passive SCWs for scanning for CBP packets on channels N, N+1, and N-1. In order to satisfy the requirements for reliable and timely on-channel sensing on N+1 and N-1, the BS shall schedule a sufficient number of SCW in passive mode to scan for CBP packets on channels N+2 and N-2.

The specific procedure of selecting the CPEs to receive the CBP packets should take into account location information of the CPEs as well as the reported information by the CPEs during their initialization procedure. Furthermore, operators should make sure that they have reliable CBP communication with their adjacent WRAN cells through either the BSs or by locating CPEs at proper distances.

In case a BS discovers a neighboring IEEE 802.22 cells, given the minimum required frequency of CBP transmissions, the BS will be able to regularly schedule SCWs in passive mode to capture the CBP packets in the corresponding channels.

### **7.20.1.3.2.2 Discovery during frames not allocated in self-coexistence mode**

In self-coexistence mode, both BS and associated CPEs in the WRAN cell can listen to the medium for network discovery during those frames not allocated to the present cell. During these periods, discovery can be facilitated by searching for a coexistence beacon or SCH from neighbor cells.

### **7.20.2 CBP-based inter-BS communication**

Inter-BS communications can be enabled by CBP transmission (as discussed in 7.20.1). The BS and CPEs shall be capable of transmitting CBP packets, and shall also be capable of receiving them during the SCW. With the basic information carried in CBP packets (see 7.6.1.3), the BS would have not only information about channels being used, but also about specific time schedules. This would allow a finer control of self-coexistence, which may be desirable especially in the case where there are no other free channels to which BSs can switch.

### **7.20.3 Mechanism for inter-BS self-coexistence**

The self-coexistence operations among IEEE 802.22 WRAN cells shall follow the top-level procedure illustrated in Figure 101 and described as follows:

- 1) The BS of an IEEE 802.22 WRAN cell is powered on.
- 2) The BS performs network discovery, which includes discovering
  - TV channel occupancies of the neighboring WRAN cells
  - Self-coexistence window (SCW) reservations of the neighboring WRAN cells
  - Frame reservation patterns of the neighboring WRAN cells on specific channels (this information can be obtained from the received CBP packets)
- 3) The BS performs channel acquisition based on the Spectrum Etiquette algorithm (as described in 7.20.3.1).
- 4) If the BS successfully acquires a channel, it goes to the normal mode of data service operations on the acquired channel [as described in step 5) below].

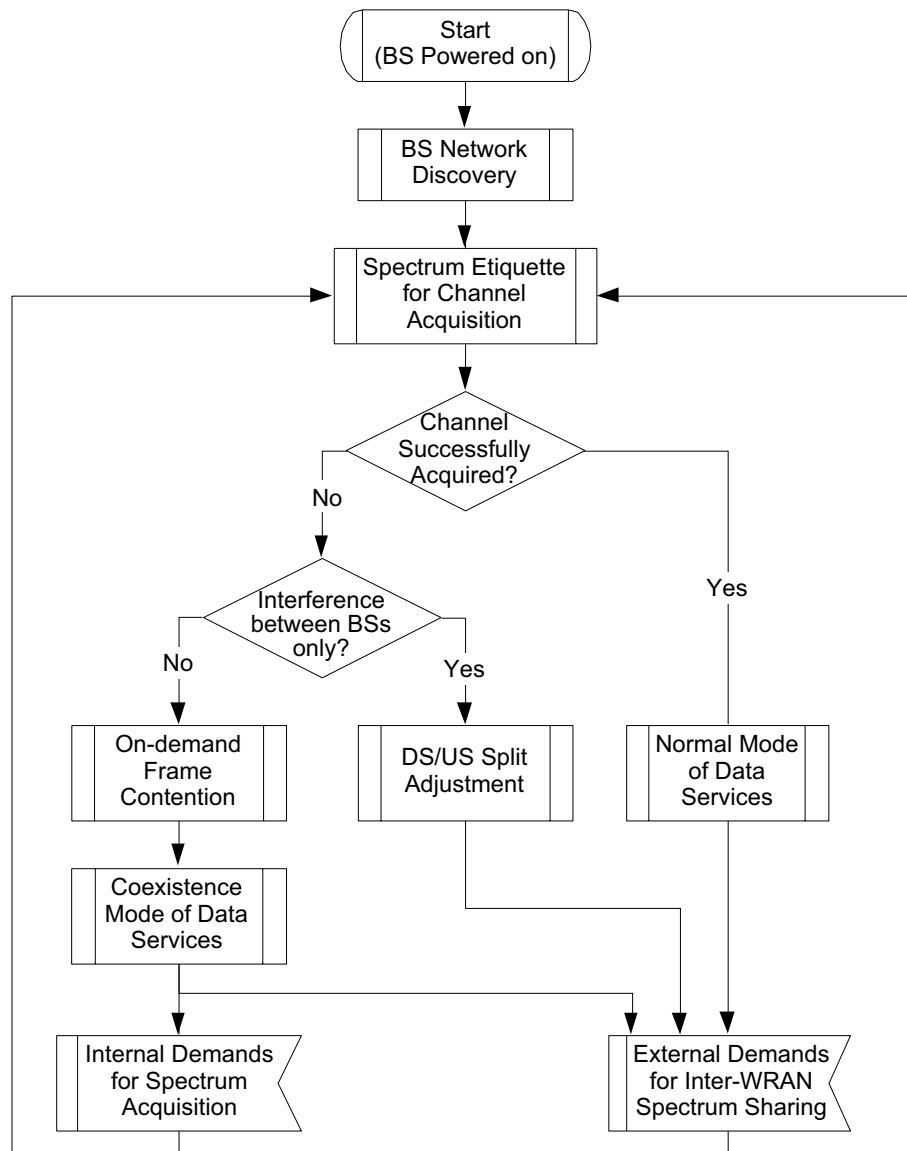
If the BS fails to acquire any empty channel, it selects a channel occupied by one or more other WRAN cells and identifies whether the potential interference comes directly from the other BSs or from the CPEs belonging to the other WRAN cells, or both. If it comes only from the other BSs, the new BS initiates the DS/US Split adjustment mechanism [i.e., skips step 5) and goes to step 6)]. If the potential interference comes from the CPEs, it performs the Inter-WRAN On-demand Frame Contention operations on the selected channel by accessing a contention-based SCW (see 7.20.1.2) [i.e., skips step 5) and step 6) and goes to step 7)]. Note that since the new BS arriving on the channel does not have a frame for itself yet, it cannot involve its CPEs in this initial contention process. Only CBP bursts transmitted directly from the new BS will be able to support the frame contention process in this initial phase. As a result, the process may go initially to step 6) but then move to step 7) when the CPEs belonging to the new WRAN cell start to operate and report potential interference through their CBP bursts.

- 5) The BS enters the normal mode of data service operations (see 7.3).

During the normal service operations, the BS may receive external demands (received from other WRAN cells) for sharing its occupied data frames on the operating channel. When this occurs and when the BS cannot find another empty channel for its operation through the Spectrum Etiquette algorithm, the BS performs the Inter-WRAN On-demand Frame Contention operations on its operating channel [as described in step 6)]. If an empty channel is found, then the BS moves its cell to this new channel and enters the normal mode of data service operations (see 7.3).

- 6) The BS performs the DS/US Split adjustment mechanism using the relevant parameter exchange carried by the SCH (see Table 1) and/or by the CBP burst received directly from the other BSs. Once it has acquired information on the Current DS/US Split, Claimed DS/US Split and the DS/US Change Offset, it applies the same basic algorithm as used for Quiet Period Scheduling described in Table 184 and transmits its updated parameters to the other BSs so that they do the same and converge towards a common DS/US Split, which will vary depending on the compound traffic requirements for the BSs involved. The adjustment of the DS/US Split through this distributed negotiation process, based on the fact that all BSs have their frames aligned (see 9.10), will allow the concurrent use of the same frames by these BSs while avoiding interference caused by a BS that would be still transmitting while the other BSs have started their upstream subframe and try to receive signals from their CPEs. Note that this will cover the cases where BSs would interfere with each other even though there is no CPE being interfered (i.e., no CPE in the overlap area). There may also be cases where CPEs will receive interference from various BSs while these BSs do not interfere with each other as a result of clever BS antenna installation that will block the signal path between the BSs. The normal case will however be when both BSs and CPEs are interfered with. For these two latter cases, step 7) will be needed to distribute the frames to the various BSs and, since there would not be concurrent use of these frames, there is then no longer a need to synchronize the DS/US split in these cases.
- 7) The BS performs the On-demand Frame Contention operations with a neighboring WRAN cell on the selected channel, and then goes to the self-coexistence mode of data services operations (as described in step 8). A neighboring WRAN cell can contend for some of the frames used by the current BS as long as it occupies a number of frames that is larger than the minimum stated in variable Frame\_Contention\_Min (see Table 274). The required message flow and the On-Demand Frame Contention Protocol are described in 7.20.3.2.
- 8) The BS enters the self-coexistence mode of data services operations (see 7.3).

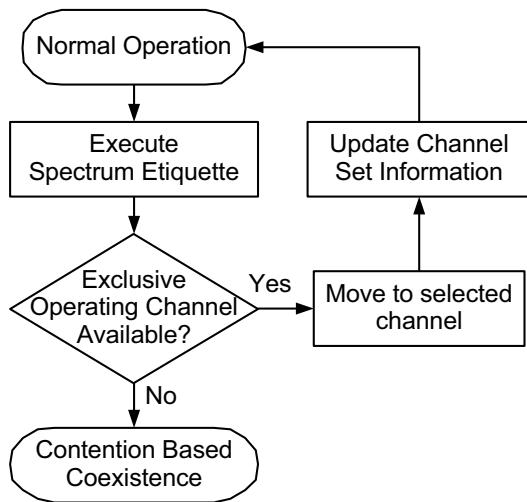
During the self-coexistence mode of data service operations, the BS may receive either internal demands (received from the inside of the BS's own cell) for additional spectrum resources, or external demands (received from other WRAN cells) for sharing its occupied frames on the operating channel. When either of these events occurs, the BS re-initiates the spectrum acquisition process starting from step 3) (Spectrum Etiquette for channel acquisition).



**Figure 101 — Execution flow of inter-BS self-coexistence mechanisms**

#### 7.20.3.1 Spectrum etiquette

The details of the scheme for prioritizing the backup and candidate channels based on spectrum etiquette are given in 10.2.3.2. Once this has taken place, the selection of the next operating channel is done according to the flow chart given in Figure 102.



**Figure 102 — Flow chart of the Spectrum Etiquette process**

### 7.20.3.2 On-demand Frame Contention (ODFC)

#### 7.20.3.2.1 Message Flow of the On-demand Frame Contention protocol

##### 7.20.3.2.1.1 Control messages

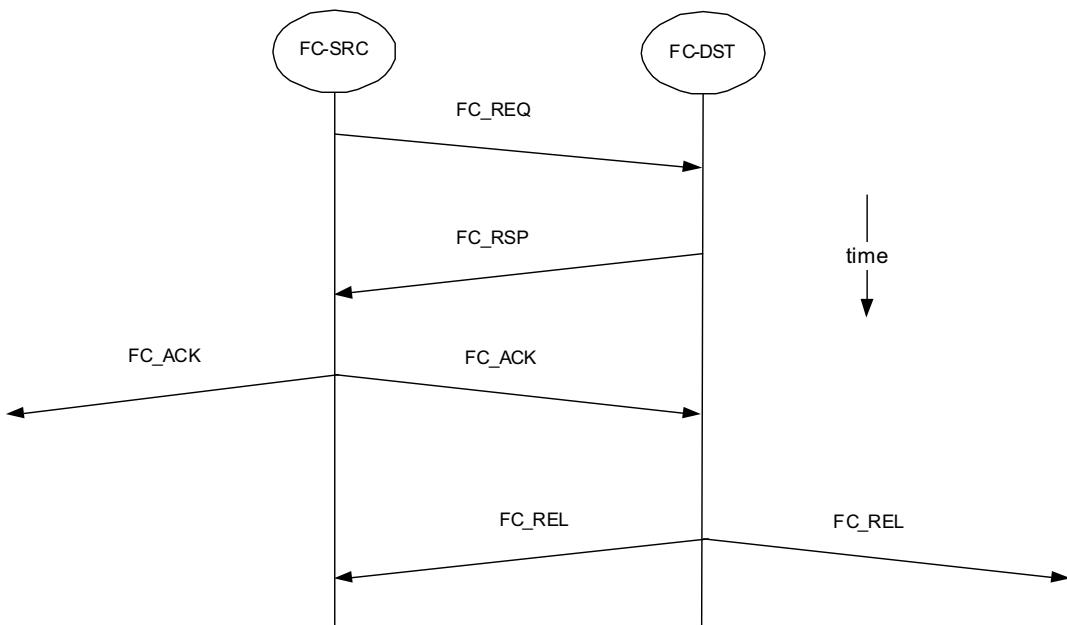
Each of the following control messages of the On-demand Frame Contention protocol is encapsulated by one CBP information element (IE).

- a) Frame Contention Request (FC\_REQ)—This is a unicast request message transmitted by the FC-SRC for initiating the frame contention process. It contains the following information:
  - 1) The FC-DST's ID as the destination.
  - 2) The frame index-vector of the data frames claimed by the requesting FC-SRC within a superframe.
  - 3) The frame contention number (one FCN is used by the requesting FC-SRC for the contention of all the data frames claimed by the requesting FC-SRC as indicated in the frame index vector).
- b) Frame Contention Response (FC\_RSP)—This is a unicast response message transmitted by the FC-DST responding to a requesting FC-SRC with regard to the contention results. It contains the following information:
  - 1) The FC-SRC's ID as the destination.
  - 2) The frame index containing the contention results for each of the claimed data frame within the superframe.
- c) Frame Contention Acknowledgement (FC\_ACK)—This is a broadcast acknowledgement message transmitted by the winner FC-SRC indicating the confirmation and the scheduling of the frame acquisitions. It contains the following information:

- 1) The frame index indicating a confirmation or not of the spectrum acquisition for each of the claimed data frame within the superframe.
  - 2) The winning FCN (used to resolving possible collisions of frame acquisition).
  - 3) The ID of the granting FC-DST, which is the FC-DST WRAN cell granting the access to the data frames that are being acquired by the winning FC-SRC (this is used to enable “clear to send”).
- d) Frame Contention Release (FC\_REL) is a broadcast message transmitted by the granting FC-DST indicating the announcement of the frame releases. It contains the following information:
- 1) The frame index indicating an announcement of the frame release for each of the granted data frames within the superframe.
  - 2) The FCN of the winning FC-SRC (used to resolving possible collisions of frame acquisition).
  - 3) The ID of the winning FC-SRC, which is the FC-SRC WRAN cell granted the access to the data frame that are being released by the granting FC-DST (this is used to enable efficient frame reuse).

#### **7.20.3.2.1.2 Message flow**

The message flow of the On-demand Frame Contention protocol in the time domain is shown in Figure 103.



**Figure 103 — Message Flow of the On-demand Frame Contention protocol**

#### **7.20.3.2.2 On-demand Frame Contention protocol**

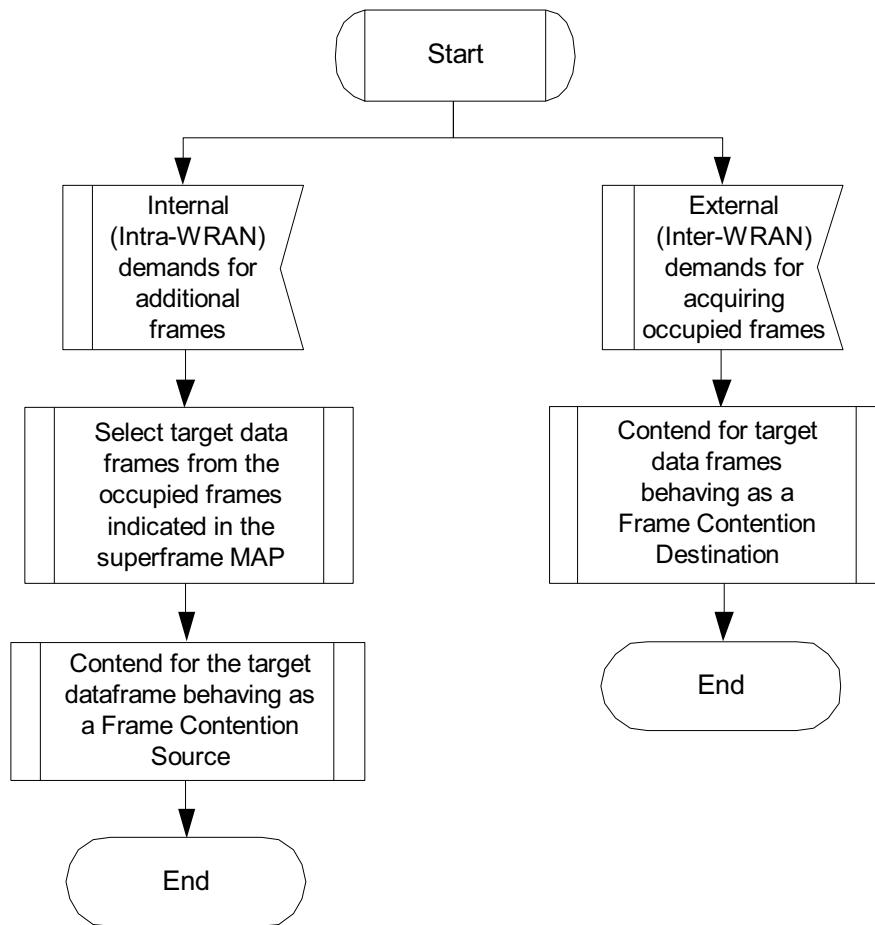
The On-demand Frame Contention protocol is used to resolve contentions of frame resource among the neighboring WRAN cells. It is assumed that when an operating BS switches from the normal mode of operation to the self-coexistence mode of operation, it initially occupies all 16 frames of the superframe. Once in self-coexistence mode, the BS shall schedule at least one contention SCW to monitor potential

frame requests from new overlapping WRAN cells. Those WRAN cells will then be able to schedule more SCWs (reservation-based or contention-based) as needed, as described in 7.20.1.2 and contend for frames used by the original WRAN cell by sending the appropriate CBP bursts during these SCWs.

Once these CBP bursts are received by the original BS or any of its associated CPEs that shall relay it to the BS, the content of these CBP bursts shall be decoded and the On-demand Frame Contention protocol described in this subclause shall be applied to determine whether the distribution of the 16 frames of future superframes should be changed.

#### **7.20.3.2.2.1 Top-level procedure of the On-demand Frame Contention protocol**

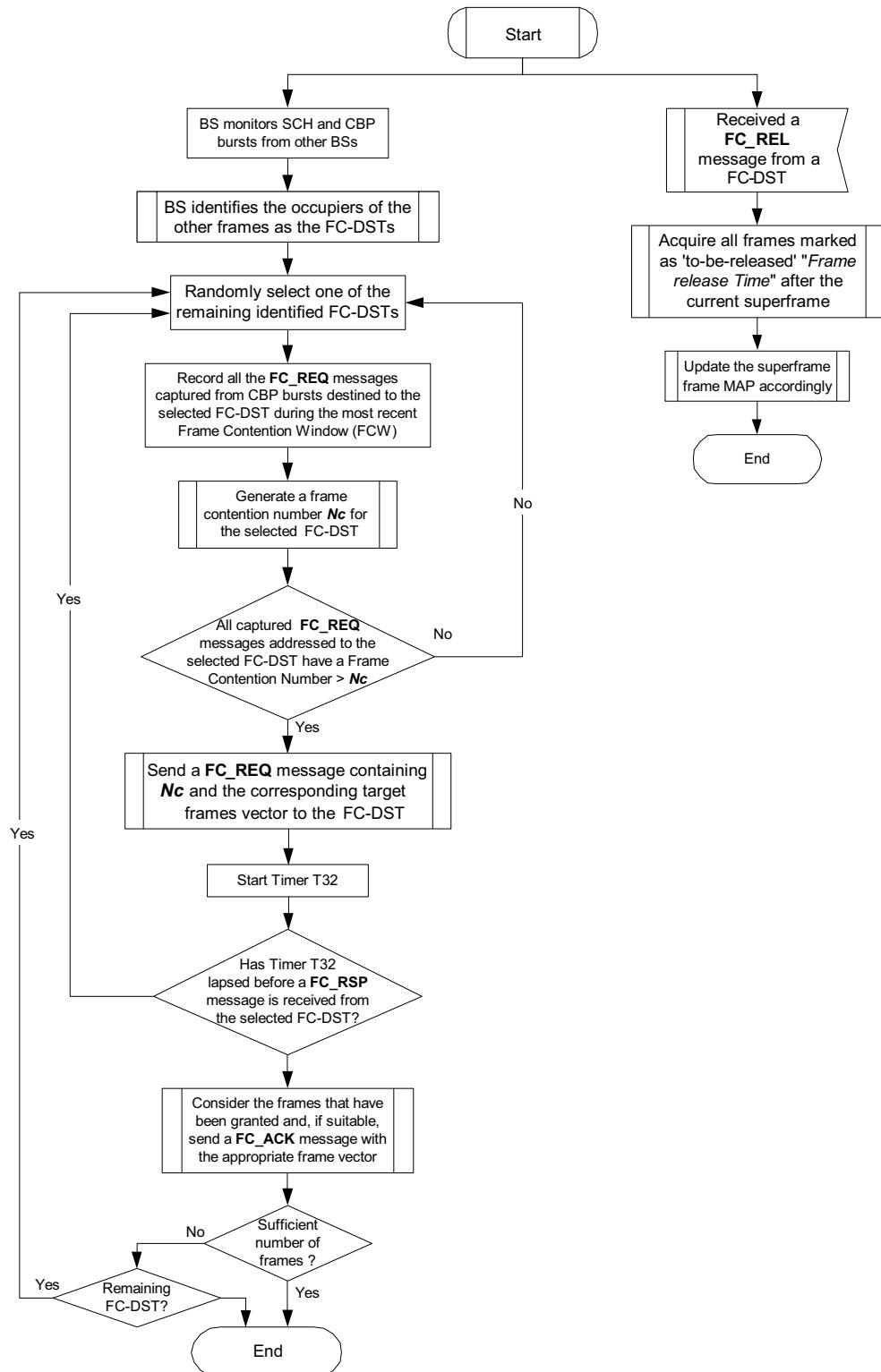
On an on-going basis, each BS in self-coexistence mode shall execute the ODFC procedure shown in Figure 104 every time it receives an internal (intra-WRAN) or external (inter-WRAN) request for additional frames.



**Figure 104 — Top-level procedure of the On-demand Frame Contention protocol**

#### **7.20.3.2.2.2 Frame contention procedure at the frame contention source**

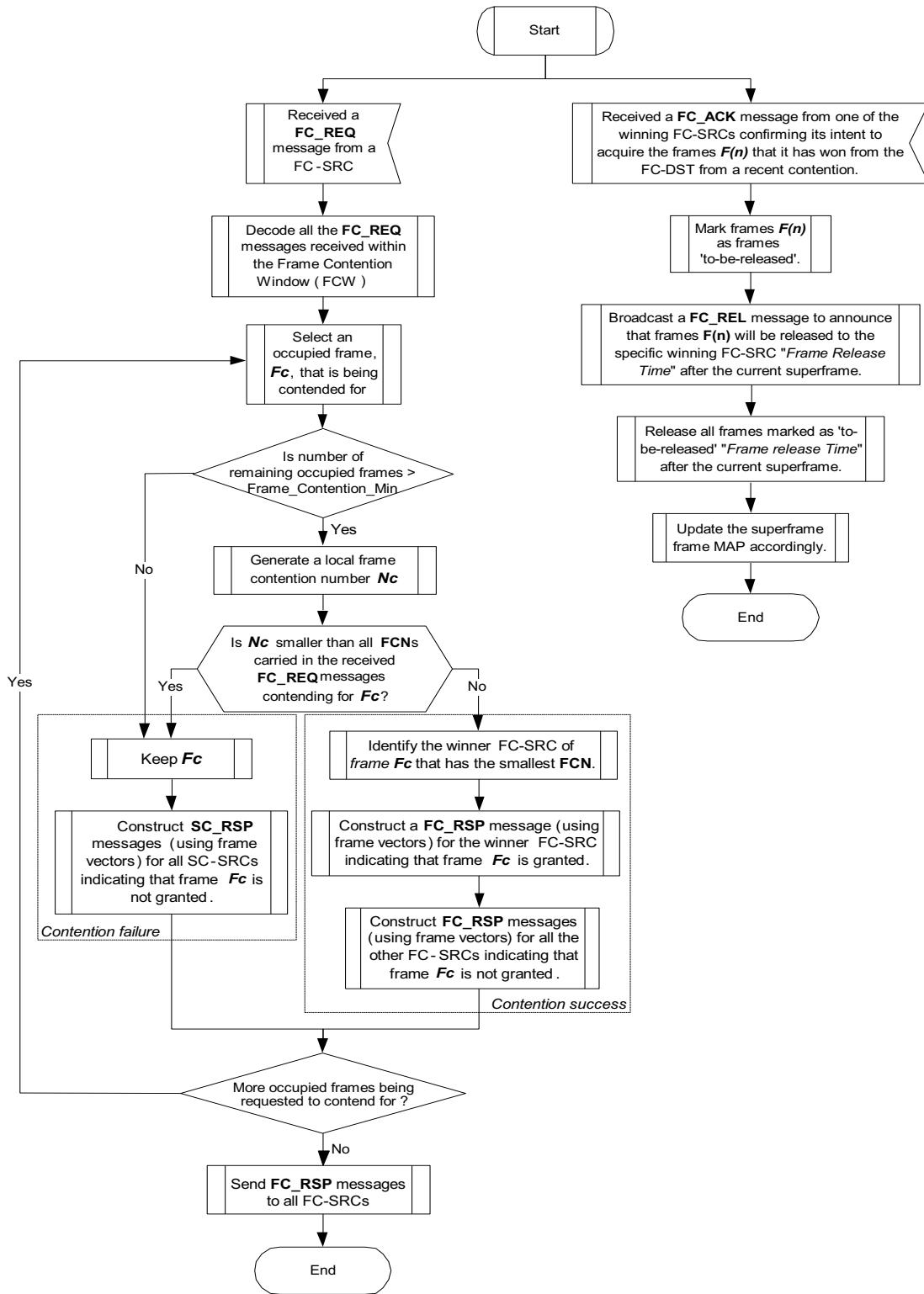
Figure 105 shows the frame contention procedure that is followed by the contention source.



**Figure 105 — Frame contention procedure at the contention source**

### 7.20.3.2.2.3 Frame contention procedure at the frame contention destination

Figure 106 shows the frame contention procedure that is followed by the contention destination.



**Figure 106 — Frame contention procedure at the contention destination**

#### 7.20.3.2.2.4 Algorithm for generation of frame contention number

The frame contention number, indicated in Figure 105 and Figure 106, FCN [i], for WRAN cell  $i$ , i.e., WRAN [i], shall be generated as follows:

$$FCN[i] = \text{RANDOM}(0, 2^n - 1)$$

where  $n = \text{FCN\_Range}$ , an adjustable parameter appearing in Table 272.

The random number generator shall generate a uniform distribution from 0 to  $2^n - 1$ .

#### 7.20.3.2.2.5 Algorithm to identify the winner FC-SRC

The On-demand Frame Contention algorithm is used to resolve contentions of frame resource among the neighboring WRAN cells when the frame contention number (FCN) of the destination cell is not the smallest one (see Figure 106). For each frame that is contended for, the algorithm shall identify the frame contention source (FC-SRC) that has the smallest frame contention number. The algorithm can be implemented as follows:

##### On-Demand Frame Contention ( $N$ , $WRAN$ , $FCN$ , $Frame$ )

- 1)  $FCN_{winner}(Frame) \leftarrow \text{MIN}(FCN[1] : FCN[N])$
- 2) **for**  $i \leftarrow 1$  **to**  $N$
- 3) **if**  $FCN[i] == FCN_{winner}(Frame)$
- 4) **return**  $WRAN_{winner}(Frame) \leftarrow WRAN[i]$ ,  
 $FCN_{winner}(Frame)$

where in the algorithm:

$N$  : total number of contending WRAN cells

$WRAN$  : the array of IDs of the contending WRAN cells,  $WRAN[i]$  for  $i \leftarrow 1$  to  $N$

$FCN$  : the array of frame contention numbers of the contending WRAN cells, in which

$FCN[i]$  is the frame contention number of  $WRAN[i]$  for  $i \leftarrow 1$  to  $N$

$Frame$  : the data frame (spectrum resource) being contended for;

$FCN_{winner}(Frame)$ : the winner frame contention number for accessing the  $Frame$

$WRAN_{winner}(Frame)$ : the ID of the winner WRAN cell to access the  $Frame$

If the algorithm finds more than one smallest frame contention number, it shall select randomly one winner frame contention source among the FC-SRCs represented by these equal frame contention numbers.

#### 7.20.3.2.2.6 Algorithm to prioritize the transmission of frame contention requests

This algorithm allows a reduction of the number of contention request messages required to decide on the winner WRAN in the frame contention protocol. A frame contention source shall monitor the FC\_REQ messages related to a specific frame and addressed to a specific FC-DST being broadcast in the area and shall forego the transmission of its own request for the same frame and toward the same FC-DST if it is to lose the contention at the FC-DST as indicated in Figure 105, given the value of its frame contention number. The algorithm can be implemented as follows:

##### Prioritized transmission of Frame Contention Requests ( $FC\_SRC[i]$ , $FCN[i]$ , $SCWBackoffMax$ )

- 1)  $FC\_SRC[i]$  generates  $FCN[i] = \text{Random}(0, 2^{16} - 1)$

- 2) Select  $SCWBackoffMax[i]$  as follows:

$$SCWBackoffMax[i] = \frac{SCWBackoffMax}{2^{16}-1} FCN[i]$$

- 3)  $FC\_SRC[i]$  generates a random backoff timer as follows:

$$SCW\_Backoff\_Timer[i] = Random(i)$$

where  $Random(i)$  is an integer uniformly generated over the interval  $[0, SCWBackoffMax[i]]$  in terms of next upcoming SCW window available opportunities.

- 4) Before the expiration of the **SCW\_Backoff\_Timer[i]**, if  $FC\_SRC[i]$  receives  $FC\_REQ[k]$  from  $FC\_SRC[k]$  contending for frame s;

- If  $FCN[i] < FCN[k]$ ,  $FC\_SRC[i]$  make the frame x as a loser frame;
- Else if  $FCN[i] \geq FCN[k]$ ,  $FC\_SRC[i]$  continues to c;
- Go back to step 4)

- 5) At the expiration of the **SCW\_Backoff\_Timer[i]**,

- If there exist frames on the request list not marked as loser frames, terminate the algorithm and proceed to the next step where  $FC\_SRC[i]$  sends  $FC\_REQ[i]$ ;
- Else, terminate the algorithm and exit contention request procedure.

where in the above algorithm:

**N**: the number of frame contention sources (FC\_SRCS)

**FC\_SRC**: array of the FC\_SRCS IDs

**FC\_SRC[i]**: refers to the BS ID executing this algorithm while  $FC\_SRC[k]$  refers to a neighboring BS of the  $FC\_SRC[i]$

**FCN**: array of the frame contention number generated by the WRANs

**SCWBackoff\_Timer**: array of the maximum backoff window for each WRAN

**SCWBackoffMax**: an integer denoting the maximum backoff window parameter as defined in Table 272

## 7.21 Quiet periods and sensing

In order to meet the Channel Detection Time for detecting the presence of incumbents in the operating channel, an IEEE 802.22 network shall schedule network-wide quiet periods for sensing. During these quiet periods, all network traffic is suspended and base stations and CPEs shall perform in-band sensing. This process is coordinated by the BS, which is responsible for scheduling the quiet periods.

The BSs must manage the quiet periods in order to protect the incumbents, while attempting to support the QoS required by IEEE 802.22 users. The two-stage quiet period management mechanism that enables dynamic adjustment of the repetition rate and duration of quiet periods and that shall be supported by the BSs and CPEs are described in 7.21.1. The BS determines the repetition rate and duration of the quiet periods based on the sensing algorithms used and type of signals that the CPEs has to sense. Once this information is determined, the BS can schedule the quiet periods either in the explicit mode, which is done through the use of CHQ-REQ MAC message as described in 7.7.17.3, or in the implicit mode using the sensing related fields in the SCH as specified in Table 1. Subclauses 7.21.1.1 and 7.21.1.2 describe in more details the process of scheduling the quiet periods.

According to the IEEE 802.22 MAC, base stations and CPEs can also perform sensing in channels outside the operating channel and its adjacent channels. However, out-of-band sensing does not require scheduling of network-wide quiet periods in the operating channel and its adjacent channels but it needs to rely on the

quiet periods in the channels to be sensed. CPEs can perform out-of-band sensing whenever not engaged in communication with their BS during normal cell operation (see 10.3.4). The BS can also specifically request CPEs to perform out-of-band sensing during normal IEEE 802.22 cell operation in order to keep track of a sufficient number of potential backup channels (see 7.19.5) in case of an UCS. This can be done through BLM management messages (see 7.7.18).

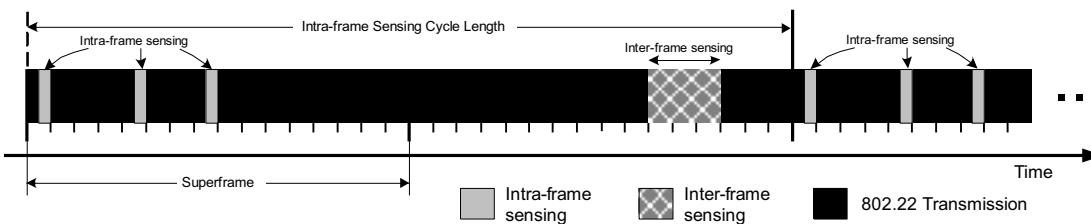
### 7.21.1 Two-stage sensing mechanism and quiet period management

The mechanism for quiet period management is illustrated in Figure 107 and it consists of the following two sensing stages, which are realized through the use of network-wide quiet periods, but which have different time scales:

- Intra-frame sensing: The intra-frame sensing stage is comprised of one sensing period per frame, during which sensing algorithms that require quiet periods of less than one frame size are employed. Intra-frame sensing allows quiet periods to be scheduled with minimal impact on the QoS for IEEE 802.22 base stations and CPEs. Based on the consolidation of all measurements done during the intra-frame sensing stage over a number of frames, the BS may still decide to schedule an inter-frame quiet period over multiple frames in order to perform longer sensing.
- Inter-frame sensing: The inter-frame sensing stage is used to support sensing algorithms that require longer sensing durations and is defined as taking longer than one frame size. Since a long quiet period may degrade the performance for QoS sensitive traffic, the allocation and the duration of the inter-frame sensing stage are dynamically adjustable by the BS. In order to meet the QoS requirements of the IEEE 802.22 base stations and CPEs while protecting primary users, the BS can use the feedback obtained during the intra-frame sensing stage to determine whether or not inter-frame sensing is needed.

The intra-frame sensing stage may be able to detect the presence of an incumbent in the measured channel within the required Channel Detection Time without the need of long quiet periods. However, if longer and finer sensing were needed to detect the incumbent, for example, to detect the incumbent signal signature, the inter-frame sensing stage would then be needed. This way, support of better QoS to IEEE 802.22 base stations and CPEs can be provided through this flexible two-stage mechanism.

The implicit quiet period scheduling structure carried by the SCH allows the BS to flexibly schedule quiet periods of any length, whether less than, equal, or larger than one frame size. To implement a quiet period longer than one frame size but that is not an integral number of frames, the BS could allocate an intra-frame quiet period immediately followed by an inter-frame quiet period. For example, if the quiet period duration needs to be one and a half frame long, the BS could allocate an intra-frame quiet period of half a frame followed by an inter-frame quiet period of one frame size. Note that an inter-frame quiet period has precedence over an intra-frame quiet period when both are scheduled in the same frame.



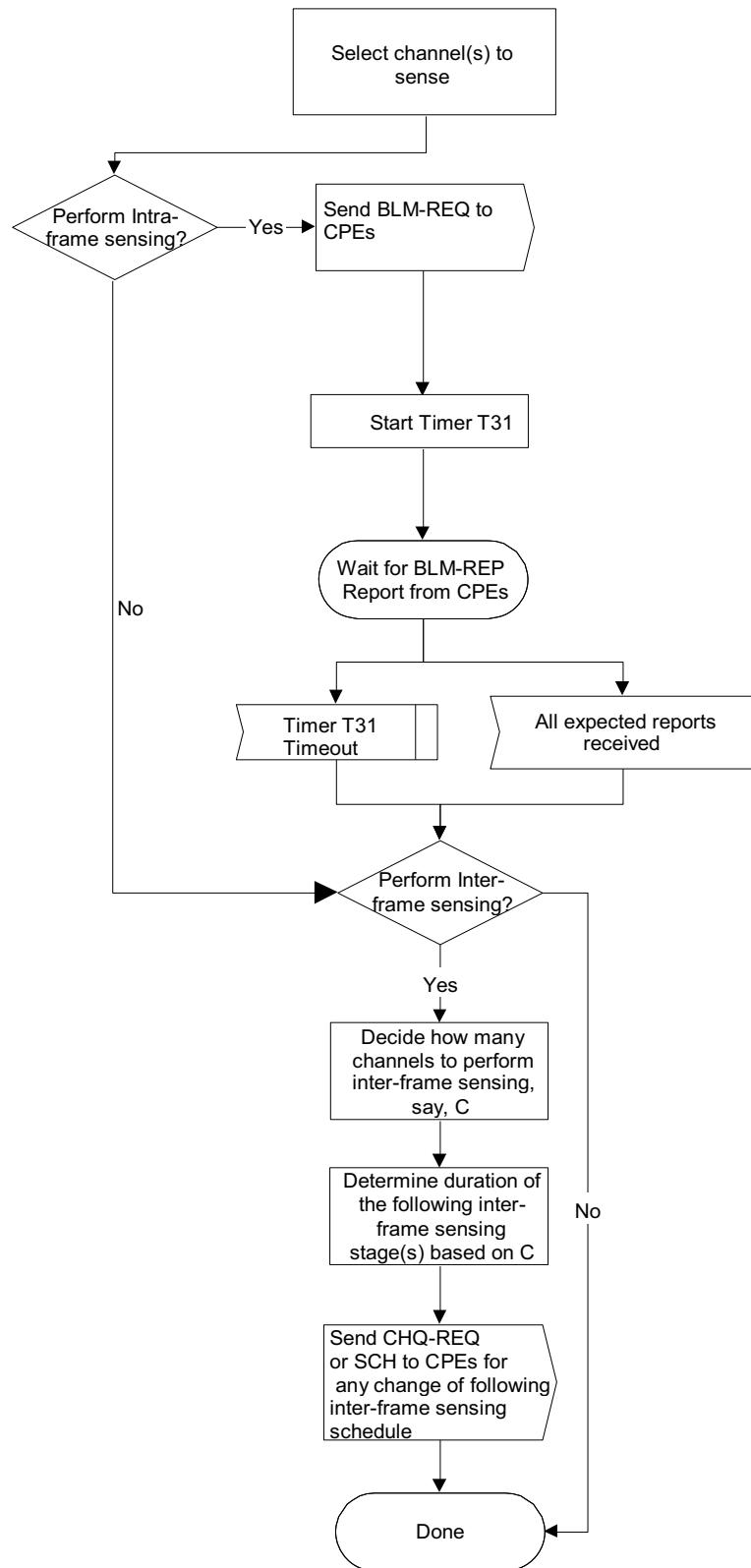
**Figure 107 — Illustration of the two-stage mechanism for quiet period management**

Note that in-band sensing is done automatically by all CPEs during quiet periods scheduled by the implicit QP scheduling mechanism using the SCH, see 10.3.3. In this case, CPEs only signal the presence of

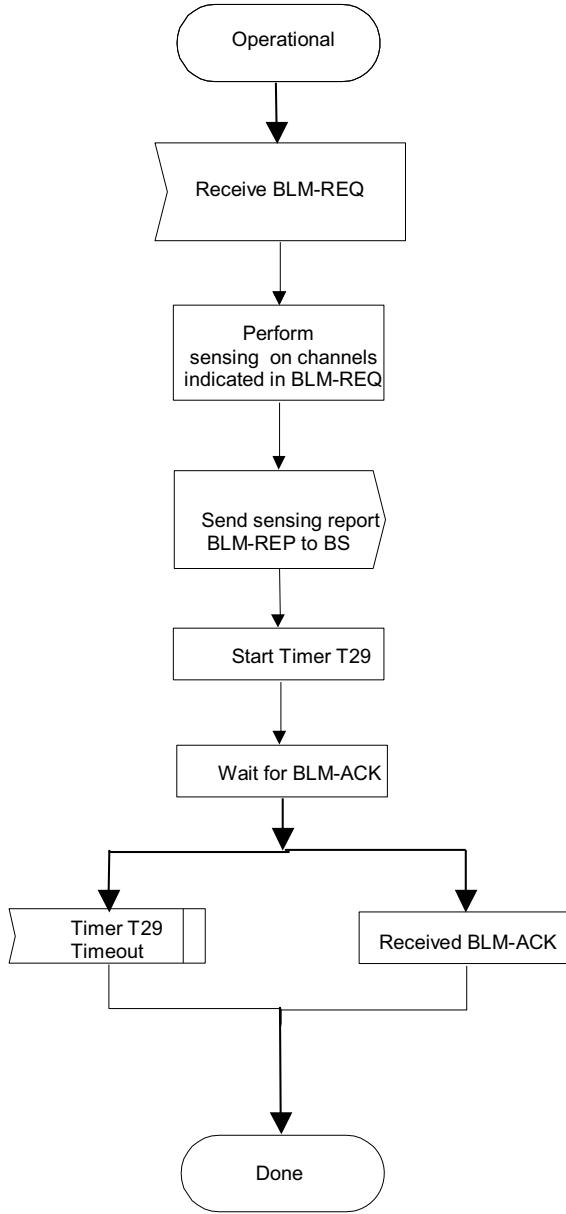
incumbents, when detected, by setting the UCS flag in the generic MAC header sent back to the BS in the granted upstream packet or, if not available, through the UCS opportunistic burst.

Figure 108 and Figure 109 show in detail how the two-stage mechanism on the operating channel N and two adjacent channels  $N \pm 1$  directed by the BLM-REQ message from the BS shall be implemented at the BS and the CPEs, respectively. Note that the BLM-REQ MAC message can also be used to request sensing of channels other than N and  $N \pm 1$ . In such case, the CPE will need to acquire the scheduling of the quiet periods on these channels from their CBP bursts and carry out sensing at the appropriate times.

Inter-frame sensing is needed when acquisition of the payload of the IEEE 802.22.1 beacon is required for authentication purpose (see Annex D). Unfortunately, inter-frame sensing can substantially impact the WRAN system QoS since the data transmissions may be interrupted for unacceptable long periods. A way to resolve such demanding requirement is by detecting the IEEE 802.22.1 sync burst using intra-frame quiet periods and, when the IEEE 802.22.1 sync burst is detected, the WRAN system can switch to its first backup channel and then, if need be, attempt to acquire the IEEE 802.22.1—payload from its previous operating channel through out-of-band sensing to acquire the beacon payload for additional data such as the location of the beacon and the data needed for its authentication. This special sensing can be signaled to the CPEs by the BLM-REQ message. If the beacon cannot be authenticated, the WRAN system could switch back to its previous channel or, at least add this channel to its list of available backup channels. This process would avoid the requirement for inter-frame sensing, hence preserving the WRAN QoS. If an IEEE 802.22.1 beacon sync burst is detected through intra-frame sensing but the switch to a backup channel is not possible, and then the WRAN system will have to use inter-frame sensing to verify the authenticity of the IEEE 802.22.1 beacon if it wants to continue operating.



**Figure 108 — Two-stage directed sensing procedure at the BS**



**Figure 109 — Two-stage directed sensing procedure at the CPE**

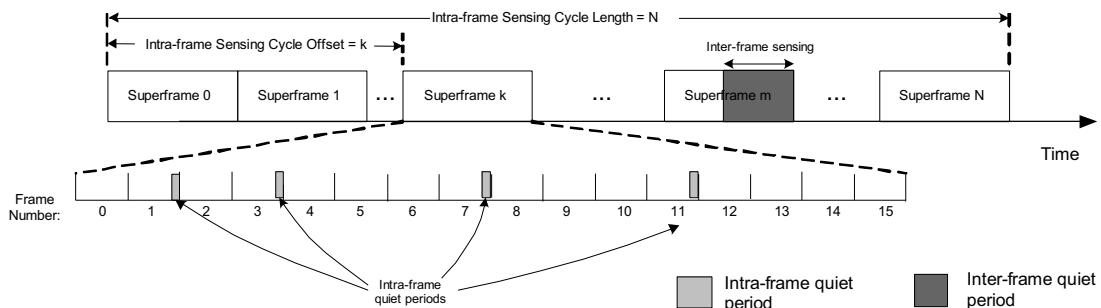
#### 7.21.1.1 Intra-frame quiet period allocation

Intra-frame quiet periods shall be scheduled at the end of the MAC frame and they must not conflict with the SCWs. Since nearby IEEE 802.22 networks are synchronized (see 7.21.2), intra-frame sensing shall be done simultaneously and hence, its effectiveness in detecting incumbent signals will be increased.

The BS shall inform CPEs in which frame intra-frame quiet periods are scheduled and their duration. The BS uses the implicit mode or the explicit mode to indicate the intra-frame quiet period schedule to the CPEs. In the explicit mode, the BS uses the CHQ-REQ MAC message described in 7.7.17.3 to advertise the intra-frame sensing schedule and all the relevant parameters for sensing. This explicit mode should not

be used in a self-coexistence operation since the quiet period scheduling information may not be made available to the other WRAN systems operating in the area. Only the implicit mode should be used in a self-coexistence situation.

In the implicit mode, this is done using the Current Intra-frame Quiet Period Cycle Length, Current Intra-frame Quiet Period Cycle Offset, Current Intra-frame Quiet Period Cycle Frame Bitmap, and Current Intra-frame Quiet Period Duration fields in the SCH as specified in Table 1. The Intra-frame Quiet Period Cycle Length is the distance in number of superframes between the superframes that contain intra-frame quiet periods assigned to specific frames according to the Intra-frame Quiet Period Cycle Frame Bitmap. Figure 110 illustrates the concept of Intra-frame Quiet Period Cycle and shows an example of a bitmap in which intra-frame quiet periods are scheduled in frames 1, 3, 5, 7, 9, and 11. The duration of the intra-frame quiet period in each frame is specified by the Intra-frame Quiet Period Duration field in the SCH. As shown in Figure 110, the Current Intra-frame Quiet Period Offset indicates the offset in number of superframes with respect to the next superframe belonging to the current intra-frame quiet period cycle. If the BS decides to change the scheduling of the quiet periods, it shall do so by transmitting a new set of Current Intra-frame Quiet Period scheduling parameters in the SCH in normal operation. If the BS operates in a self-coexistence situation, it shall send this information as a new set of Claimed Intra-frame Quiet Period scheduling parameters in the SCH to allow negotiation among the coexisting WRAN cells to align their quiet periods before declaring the new quiet period schedule as “current” (see 7.21.2.1).



**Figure 110 — Scheduling of quiet periods for intra-frame and inter-frame sensing using information provided in the SCH**

### 7.21.1.2 Inter-frame quiet period allocation

Once the BS receives the reports from the CPEs about their intra-frame sensing measurement results, it can make a decision with respect to the need for an inter-frame sensing stage. The BS can also decide to perform inter-frame sensing without going through intra-frame sensing. The BS can use either implicit or explicit mode to schedule the quiet periods for inter-frame sensing.

In the explicit mode, the BS uses the measurement frames described in 7.7.17.3 and 7.7.18.1 to adaptively control the quiet periods. In the implicit mode, the BS uses the Inter-frame Quiet Period Duration and Inter-frame Quiet Period Offset fields in the SCH (see Table 1) to schedule or cancel quite periods for inter-frame sensing. Note that the explicit mode does not allow the quiet period scheduling information to be made available to the other WRAN systems operating in the area and should not be used in a self-coexistence operation.

The inter-frame quiet period may last up to an entire superframe. It is especially suited for spectrum sensing algorithms that require longer quiet periods, such as for the detection of the IEEE 802.22.1 beacon payload confirming the presence of wireless microphone operation.

### 7.21.1.3 CPE-initiated dynamic quiet period scheduling adjustment

On occasion a CPE may need to request more quiet periods in order to complete its own in-band sensing actions. Quiet period adjustment request is signaled by the CPE by setting the QPA bit in the GMH (Table 3).

If the CPE currently has an US allocation it shall be done immediately and sent in the GMH of the MAC PDU during the next US transmission opportunity.

If the CPE does not currently have an US allocation, CPE shall first request an allocation (see 7.11), and once granted, shall transmit an empty payload MAC PDU with the QPA bit set in the GMH (Table 3).

Upon receiving a MAC PDU with the QPA bit set in the GMH, the BS then determines the new schedule/configuration.

When the cell is operating in normal mode, the BS shall respond to the quiet period adjustment request by either sending the CPEs a CHQ-REQ message for immediate reaction or modify its SCH accordingly. When the cell is in a self-coexistence situation, the BS shall respond to the request by transmitting the new quiet period schedule in the SCH once the negotiation with the nearby WRAN cells operation on the operating channel and its adjacent channels will have taken place (see 7.21.2).

### 7.21.2 Synchronization of overlapping quiet periods

Due to the possibility of multiple nearby IEEE 802.22 cells operating on the same channel or adjacent channels, quiet periods of these cells shall be synchronized. This will considerably improve the reliability of detection of incumbent signals, and will also enable better self-coexistence among nearby IEEE 802.22 cells. It is assumed that the BSs will have already synchronized their superframes as discussed in 7.23. Also, the intra-frame sensing quiet periods always start at the end of a frame. This makes the quiet period synchronization procedure described in this subclause considerably simpler.

Hence, BSs shall synchronize their quiet periods with other nearby BSs. This is done using the fields available in the SCH (see Table 1) that are used to schedule quiet periods for intra-frame (see 7.21.1.1) and inter-frame sensing (see 7.21.1.2), and which are also carried in CBP packets (see 7.6.1.3.1). The BS shall be responsible for setting these fields whenever transmitting a SCH. These QP scheduling fields are sent in the following three sets of parameters in a self-coexistence situation:

- Current Intra-frame Quiet Period Cycle Length, Cycle Offset, Frame Bitmap, and Duration;
- Claimed Intra-frame Quiet Period Cycle Length, Cycle Offset, Frame Bitmap and Duration, Synchronization Counter for Intra-frame Quiet Period repetition rate and Synchronization Counter for Intra-frame Quiet Period Duration; and
- Inter-frame Quiet Period Duration and Inter-frame Quiet Period Offset.

#### 7.21.2.1 Intra-frame quiet period synchronization

The “current” set of intra-frame quiet period parameters is used by the BS to indicate to its CPEs the quiet periods that are currently scheduled. Before becoming “current,” this set of QP scheduling parameters has to be confirmed by all coexisting WRAN cells through the CBP mechanism following a negotiation among these WRAN cells. The “claimed” set of intra-frame quiet period parameters is used by each BS to announce its new scheduling requirement for quiet periods considering the performance of the sensing techniques used by its CPEs, i.e., the sensing time needed to meet the required sensing threshold. This “claimed” set is broadcast by the SCH and retransmitted to the other coexisting WRAN cells by the CBP mechanism so that negotiation can take place to arrive at a common quiet period schedule that meets the maximum QP requirement while minimizing the overhead by reducing the non-concurrent quiet periods as much as possible. This “claimed” quiet period schedule, once it has become common to all coexisting

WRAN cells can then be scheduled to become the “current” quiet period parameter set after sufficient time is given for the negotiation to cover for inter-cell propagation.

The BS that receives information about other collocated IEEE 802.22 cells (either directly or reported through the CPEs) shall synchronize with all quiet periods scheduled through negotiation among coexisting BSs. At that time, the common “claimed” intra-frame QP schedule replaces the “current” schedule. The intra-frame QP negotiation mechanism shall be as follows:

Each BS sends its claim to other coexisting BSs through the SCH, which is then carried by the CBP mechanism. Each BS that receives a new “claim” shall compare it to its own claim and either replace the incoming claim by its larger claim for the QP repetition rate (i.e., number of 1’s in the bitmap/cycle length) and/or QP duration or keep it as is if its own claim is smaller. If its own claim is larger and the updating results in a new claim that is larger than the “current” QP repetition rate and/or duration, the BS shall reset the Claimed Intra-frame Quiet Period Offset to the minimum number of frames required to make sure that all coexisting BSs have received the claim (e.g., 2 hops, that is 2 superframes) before sending it in the SCH and relaying it through the CBP mechanism. If the new claim is smaller than the “current” scheduling, the Claimed QP Offset parameter is repeater unchanged and the incoming scheduling parameters are also repeated unchanged.

In order to allow the synchronized Intra-frame Quiet Period Duration to adapt to the variation found at different BSs, each BS, denoted as  $BS(i)$ , should maintain a variable named Synchronization Counter for Intra-frame Quiet Period Duration, denoted as  $SC_D(i)$ . This value is sent together with the “claimed” Intra-frame Quiet Period Duration, denoted  $D^{Claimed}(i)$ , in the SCH and CBP.  $D^{Claimed}_{syn}(i)$  is the latest Intra-frame Quiet Period Duration claimed by  $BS(i)$  and  $D^{Claimed}_{min}(i)$  is the minimum required Intra-frame Sensing Duration by  $BS(i)$ . Initially,  $SC_{max}$  is a value predefined and common to all WRAN cells in an area that corresponds to the extent of propagation of the QP scheduling (e.g., 8 hops). This initial value shall be agreed upon and used by all operators in the area and should be updated according to the algorithm described in Table 184 below. For the values given above as examples, an increase in QP duration as compared to the “current” value would take place after 2 frames whereas a release of unused quiet period duration as compared to the “current” value would take 8 frames to become “current”.

The algorithm described in Table 184 shall be used to come up with a Claimed Intra-frame Quiet Period Duration that will converge to a common value for all overlapping WRAN cells within the given extent of reach (e.g., 8 hops). It will also produce a value for the “claimed” offset, denoted as  $Offset^{Claimed}$ , in number of superframe, representing the delay required before transferring this “claimed” QP duration into the “current” QP duration, allowing the convergence scheme to stabilize at all BSs involved in the process, thus isolating the “current” QP scheduling values from the temporary instability of the transition on the “claimed” values.

**Table 184 — Quiet Period Scheduling Convergence algorithm**

<b>% When initializing <math>BS(i)</math> sets:</b>	
$D^{Current}(i) = 0$	
$D^{Claimed}_{syn}(i) = D^{Claimed}_{min}(i)$	
$SC_D(i) = SC_{max}$	
<b>% For <math>BS(i)</math>, before sending out a SCH or CBP packet:</b>	
if $D^{Claimed}_{syn}(i) < D^{Claimed}_{min}(i)$ , then	% Case covering increase in QP
$D^{Claimed}_{syn}(i) = D^{Claimed}_{min}(i)$	
$Offset^{Claimed}(i) = 2$	% 2 superframes for fast reaction time
endif	% (adjustable) when QP requirement increases
if $D^{Claimed}_{syn}(i) == D^{Claimed}_{min}(i)$ , then	
$SC_D(i) = SC_{max}$	
endif	

<pre> if D<sup>Claimed</sup><sub>syn(i)</sub> &gt; D<sup>Claimed</sup><sub>min(i)</sub>, then % Case covering de-increase in QP     SC<sub>D(i)</sub> = SC<sub>D(i)</sub>-1     if SD<sub>D(i)</sub> == 0, then         D<sup>Claimed</sup><sub>syn(i)</sub> = D<sup>Claimed</sup><sub>min(i)</sub>         SC<sub>D(i)</sub> = SC<sub>max</sub>         Offset<sup>Claimed</sup><sub>(i)</sub> = 9 % 9 superframes for slow release of QPs (adjustable)     endif endif </pre>
<p><b>% When BS(i) receives a SCH or CBP packet from BS(j):</b></p> <pre> if D<sup>Claimed</sup><sub>syn(j)</sub> &gt; D<sup>Claimed</sup><sub>syn(i)</sub>, then     D<sup>Claimed</sup><sub>syn(i)</sub> = D<sup>Claimed</sup><sub>syn(j)</sub>     SC<sub>D(i)</sub> = SC<sub>D(j)</sub> else if D<sup>Claimed</sup><sub>syn(j)</sub> == D<sup>Claimed</sup><sub>syn(i)</sub>     and SC<sub>D(j)</sub> &gt; SC<sub>D(i)</sub>, then         SC<sub>D(i)</sub> = SC<sub>D(j)</sub>; endif </pre>
<p><b>% Countdown at every BS in superframe: to fetch 'claimed' value into 'current' value</b></p> <pre> Offset<sup>Claimed</sup><sub>(i)</sub> = Offset<sup>Claimed</sup><sub>(i)</sub> - 1 % Offset decremented by 1 if Offset<sup>Claimed</sup><sub>(i)</sub> == 0, then % every start of superframe     D<sup>Current</sup><sub>(i)</sub> = D<sup>Claimed</sup><sub>syn(i)</sub> endif </pre>

The same algorithm shall be used to converge on a common Claimed Inter-frame Quiet Period repetition rate with the same initial value for SCmax in order to converge on the lowest common quiet period repetition rate where all the Ds (Duration) will be replaced by Rs (Repetition rate). Adjustment of the Claimed Intra-frame Quiet Period Cycle Length and the Claimed Cycle Frame Bitmap shall result from the common repetition rate found.

### 7.21.2.2 Inter-frame Quiet Period Synchronization

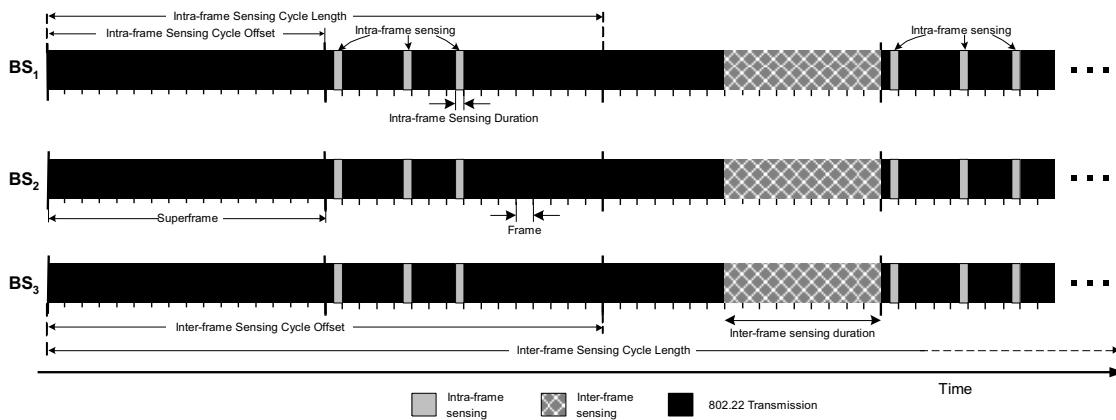
The BS that receives information about other collocated IEEE 802.22 cells (either directly or reported through CPEs) shall synchronize with all quiet periods scheduled by the other cells for the inter-frame QP schedule. To synchronize inter-frame sensing quiet periods, the BS uses the information contained in the SCH, but in addition to that, the BS shall apply a random mechanism to decide whether to change its quiet period schedule. This mechanism will considerably mitigate the ping-pong effect and it is based on the following rule:

- A BS 1 shall only modify its inter-frame sensing quiet period schedule to synchronize with the inter-frame sensing quiet period of another nearby BS 2 if the remaining time to BS 1's next inter-frame sensing quiet period is larger than the remaining time to BS 2's next inter-frame sensing quiet period.

For example, consider that BS 1 received information on the SCH transmitted by a collocated BS 2. In this case, BS 1 shall modify its inter-frame quiet period schedule in order to synchronize with that of BS 2 if the Inter-frame Quiet Period Offset of BS1 is larger than that of BS2. If this rule is validated, BS 1 can proceed with the synchronization of its quiet period with that of BS 2. To this end, BS 1 shall schedule the change in its quiet period to take place N frames away, where  $N = \text{rand}(0, Q_{\text{Thresh}})$  and  $\text{rand}(a, b)$  is a function that returns an integer number t, where  $a \leq t < b$ , and  $Q_{\text{Thresh}}$  is defined in units of superframe. If up until N superframes later BS 1 does not receive any more information regarding the next quiet period of BS 2, it shall proceed with its quiet period change to achieve synchronization. This is done by modifying the values of the Inter-frame Quiet Period Offset and Duration in the SCH when initiating the new superframe, or by transmitting an updated CHQ-REQ command.

If, before advertising the change in its quiet period, BS 1 receives information about BS 2, which indicates that BS 2 has already changed its quiet period to align with that of BS 1, BS 1 shall then cancel its scheduled quiet period change. Another possibility is that the new information about the quiet period that BS 1 receives about BS 2 changed since the last notification. In this case, BS 1 shall cancel the current scheduled change of its quiet period and reschedule it if appropriate (using the same procedure as described previously), taking into consideration the new parameters received from BS 2. BS 1 shall proceed with changing its quiet period in all other cases.

In a region with multiple nearby BSs, the synchronization of the superframes (described in 7.23) and the synchronization of the quiet periods using the mechanisms described above will result in the scenario depicted in Figure 111. The nearby cells will synchronize not only their frames but also their quiet periods. This will render the results of the intra-frame and inter-frame sensing as accurate as can be, since all nearby IEEE 802.22 networks will quiet at the same time and only the signal from the incumbent user, if any, will remain on the channel.



**Figure 111 — Illustration of the two-stage quiet period mechanism with multiple overlapping cells**

### 7.21.3 CPE report

While intra-frame or inter-frame sensing stages are taking place, the CPE shall report the presence of any incumbent either through the UCS opportunistic burst in the contention window or through the UCS flag in the MAC header if the CPE already has bandwidth granted on its upstream. Sensing measurement results shall be reported to the BS when requested through the BLM-REQ MAC message. In this case, the CPE shall use the BLM-REP message (see 7.7.18.3) to report to the BS the results of its sensing.

Reporting can be done after each individual sensing interval for sensing mode 2 or once the CPE sensing device has carried out sensing during sufficient time to meet the required sensing threshold for sensing mode 0.

## 7.22 Channel management

A robust and efficient channel management component is a critical feature. In fact, the channel management component incorporated in the MAC allows IEEE 802.22 systems to efficiently and dynamically use the available channels as the radio environment utilization changes. In the MAC, two modes of channel management are possible: embedded (see 7.7.1.1) and explicit (see 7.7.17). The BS and

CPEs shall support both these schemes, while the decision on which one to use and when is at the discretion of the BS.

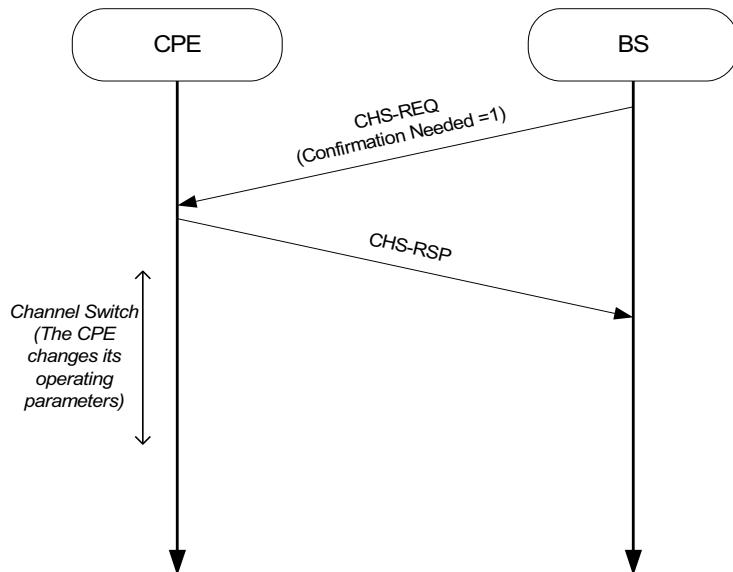
The embedded mode of channel management has the advantage that individual channel management commands need not be sent (as it is the case in the explicit mode), and hence better spectrum utilization can be achieved. Another advantage of the embedded mode is that it addresses all CPEs in a cell, and hence is an effective way to take corrective actions in case an incumbent user starts operating in a channel occupied by all CPEs in an IEEE 802.22 cell. Similar to all other IEs, the IEs related to the embedded channel management (see 7.7.1.1) scheme shall only be transmitted by the BS when this feature is used.

The explicit approach to channel management, on the other hand, provides greater flexibility and is relatively independent of the MAC protocol used. Furthermore, this allows channel management to be implemented in different granularities, that is, these standalone messages could be sent by the BS to CPEs, for example, through unicast (i.e., destined to a single CPE), multicast (i.e., destined to a group of CPEs), or broadcast (i.e., all CPEs in a cell). These messages would also allow the BS to request confirmation of receipt, in case guaranteed delivery is required. In addition, contrary to the embedded mode where the BS has to wait for the next MAC frame in order to send a channel management command, this mode of operation of supporting individual channel management frames allows the MAC to rapidly react to changes in the radio spectrum occupation. This quick reaction is critical especially when we consider incumbent protection.

Irrespective of the channel management mode, CPEs and BSs shall treat channel management commands with high priority, especially when they refer to the protection of incumbent services. Once the BS detects or receives the report about the presence of an incumbent system on the operating channel (see 7.19.1 and 7.19.3), it should send channel management commands to the effected receivers. Depending of the urgency of the channel management command (the requirements of certain incumbent users may be more strict than others), the BS shall calculate the expected time the channel management message should arrive at the CPEs and appropriately set the scheduling fields (e.g., count, offset, duration, period) in the message header. This will dictate the urgency of the message and how it shall be treated at the receivers.

Also, depending upon the situation, correct reception of channel management frames by all CPEs involved may be required by the BS. In this case, the BS shall set the ‘Confirmation Needed’ field existing in the header of the channel management frame, which allows for the BS to specifically request the CPEs to send back a confirmation message. If we take the CHS-REQ message, Figure 112 depicts the message flow between BS and CPE when the ‘Confirmation Needed’ field is set.

Once the destination receives the channel management command from the BS, it shall give higher priority for these types of messages. As such, the receiver shall inspect the message control fields and proceed as instructed by the BS. If a confirmation is needed (in particular, this may be useful in case of transmissions of individual messages as these are unreliable), the receiver shall immediately send back a response message to the BS with the appropriate confirmation code. If a required acknowledgement message is not received within a pre-determined timeout, the BS may send another channel management message to the receiver in question. The receivers shall also check the scheduling fields in the management message in order to ascertain how urgent the message is, and how it should be treated internally. The receiver shall then change its operating parameters, at the scheduled time, as instructed by the BS.



**Figure 112 — Message flow between BS and CPE when confirmation is required**

### 7.22.1 Initialization and Channel Sets Updating

For efficient channel management, 10.2.3 addresses channel classification and selection rules. In this subclause, procedure of channel list initialization and updating are addressed.

In order to maintain the channel sets, each BS maintains the following available channel sets: Operating, Backup, Candidate, Protected, Occupied, and Unclassified. Each CPE maintains only the first three channel sets: Operating, Backup and Candidate. These individual sets have different update steps. For example, on the CPE side, the Operating set is confirmed by every received SCH and the Backup and Candidate sets are updated after receiving the DCD. After synchronization, the BS should send an IPC-UPD message to the CPE to update the set of channels prohibited from incumbent operation for the newly connected CPE to allow skipping these channels to speed up the sensing process. These relations are summarized in Table 185. In the case of the BS, channel sets are updated after each quiet period either at a periodic interval or aperiodic intervals.

**Table 185 — Update channel set information in CPE**

Message	Field	Information
SCH	BS_ID	Operating channel on which the SCH is received
DCD	Number for Backup channels	Number of backup channels
	Backup and candidate channel list	List of backup and candidate channels
IPC-UPD	Incumbent Prohibited Channels Update	Channels that cannot carry incumbent signals since their operation is prohibited (e.g., channel 37 in the USA) and thus do not need to be sensed for the presence of incumbents

When a CPE turns on, it scans the channels to identify the available WRAN operations and proceeds with the selection of one of these services (see 10.3.2). Such selection identifies the operating channel. As part of the CPE initialization, the list of backup and candidate channels is sent in the DCD message by the BS. This procedure is closely related with obtaining downlink parameters procedure (see 7.14.2). After

association of a new CPE, the BS shall send the IPC-UPD message to indicate the list of channels prohibited from incumbent operation to the CPE so that it can skip incumbent sensing on these channels. Channel sets in the CPE are updated after periodically receiving the DCD message. In the case of the BS, if channel sets are changed as a result of BLM-REP messages, the BS sends the backup and candidate channel list in its DCD message.

### 7.22.2 Scheduling of channel switching time

When the BS decides to switch channels during normal operation, it shall execute the following procedure to determine when to schedule the channel switching operation.

- The BS selects the first backup channel from its backup/candidate channel list, it shall select a waiting time T46 to make sure that all its CPEs are prepared for the channel switch. The value of T46 is a configuration parameter that could be set by the management interface. The first requirement is that the value of T46 shall be smaller or equal to the maximum allowed channel moving time and the second requirement is that is long enough for the CPEs to recover from an incumbent detection.
- Then, the BS schedules the channel switch using the channel management procedure described in 7.19.5.

## 7.23 Synchronization of the IEEE 802.22 base stations

The BSs shall synchronize the absolute local start time of their superframe period, to the start of every minute referenced to UTC to a tolerance of less than or equal to  $\pm 2 \mu\text{s}$ .

All base stations shall use a common clock derived from a global navigational systems such as GPS to synchronize their MAC frames. Every BS upon activation will, as a first step, derive its system clock based on this common clock.

Every base station shall be equipped with a global navigational system receiver capable of receiving a UTC synchronized 1 pps timing signal. The accuracy of the clock pulses derived from the global navigational system are accurate to  $\pm 100 \text{ ns}$  and the pulses that are derived typically have rise times within  $\pm 2.5 \text{ ns}$ . Although the IEEE 802.22 specification requires the presence of a GPS receiver, other techniques (e.g., IEEE Std 1588-2008 [B13]) may be considered as long as they meet the required tolerance.

## 8. Security mechanism in IEEE 802.22

Security features defined in this clause provide protection for the IEEE 802.22 users, service providers and most importantly, the incumbents, who are the primary users of the spectrum. As a result, the protection mechanisms in IEEE 802.22 are divided into two security sublayers that target non-cognitive as well as cognitive functionality of the system and the interactions between the two. This clause does not discuss methods to protect the access to the IEEE 802.22 system and the ability to configure it. Required methods for protecting the hardware and software running on BSs and CPEs are discussed in Clause 11.

The security sublayer 1 provides subscribers with authentication, or confidentiality for user data and MAC management messages transmitted across the broadband wireless network. It does this by applying cryptographic transforms to MAC PDUs carried across connections between CPE and BS. In addition, these security sublayers provide operators with strong protection from theft of service.

The security sublayers employ an authenticated client/server key management protocol in which the BS operator controls distribution of keying material to client CPE. This material is used to protect MAC management messages, and may be optionally used to protect user data. The basic security mechanisms are strengthened by adding EAP-based CPE device-authentication to the key management protocol.

All CPEs attempting access to the network shall be authenticated. If the authentication exchange is successfully completed, the BS shall consider the CPE to be authenticated, and proceed to authorize (via registration, see 7.14.2.11) the CPE to access the network. If the authentication exchange is not successfully completed, the BS shall deny the CPE access (via de-registering the CPE, see 7.14.2.11) to the network. In this case, the CPE may attempt access on one of the other WRAN services it detected during initialization (see 7.14.2). If during authentication exchange, the CPE specifies that it does not support IEEE 802.22 security for protection of user data, then after successful completion of authentication, the key exchange used to setup protection of user data shall be skipped.

In cognitive radio systems, confidentiality and privacy mechanisms need to protect data and sensitive spectrum occupancy information from the competitors, as well as the spectrum management information used by the BS to configure the operation of the CPEs. The standard attempts to protect against unauthorized access to these data transport services by securing the associated service flows over the air.

To enhance the security for the cognitive functionality in IEEE 802.22, security sublayer 2 is introduced. The security mechanisms validate the availability of spectrum for the primary and the secondary users by employing mechanisms such as distributed sensing and decision making. This includes authentication of the incumbent sensing information to avoid Denial of Service (DoS) attacks, authentication of the IEEE 802.22.1 beacon frame utilizing the security features that are already embedded in it, authentication of the geolocation and co-existence information, etc. Some cognitive plane security related mechanisms are an integral part of other cognitive functions required for the system implementation such as Spectrum Sensing Function, geolocation, spectrum manager, Spectrum Automaton, Management Plane procedures and functions etc.

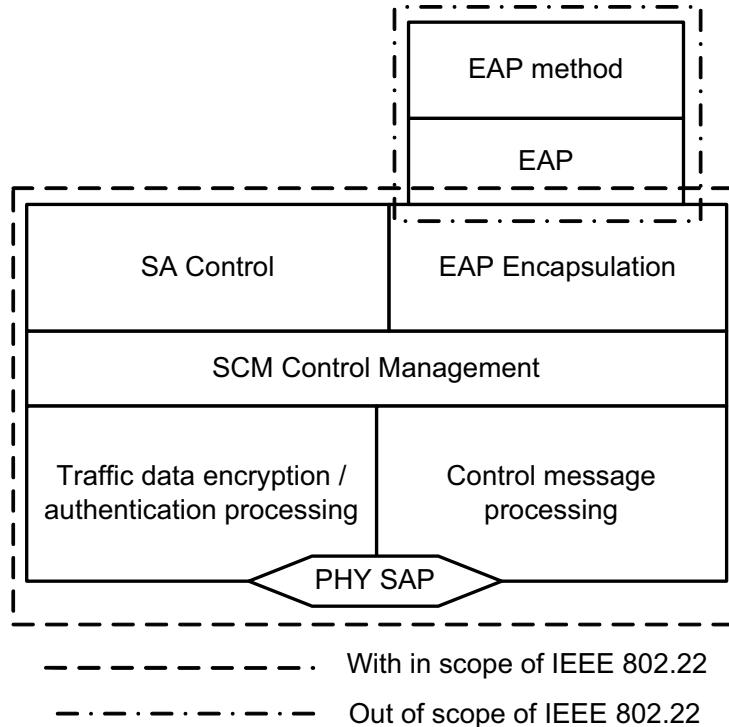
### 8.1 Security Architecture for the Data/Control and Management Planes

Privacy has two component protocols as follows:

- a) An encapsulation protocol for securing packet data over the air. This protocol defines a set of supported *cryptographic suites*, i.e., pairings of data encryption and authentication algorithms, and the rules for applying those algorithms to a MAC PDU payload.
- b) A Security for Control and Management (SCM) protocol providing the secure distribution of keying data from the BS to the CPE. Through this key management protocol, the CPE and the BS

synchronize keying data; in addition, the BS uses the protocol to enforce conditional access to network services.

The protocol stack for the security components of the system are shown in Figure 113.



**Figure 113 — Security sublayer 1**

- SCM Control Management: This stack controls all security components. Various keys are derived and generated in this stack.
- Traffic Data Processing: This stack encrypts or decrypts the traffic data and executes the authentication function for the traffic data.
- Control Message Processing: This stack processes the various SCM-related MAC messages, and provides either authentication and/or encryption of such messages.

### 8.1.1 Secure encapsulation of MAC PDUs

Encryption services are defined as a set of capabilities within the MAC security sublayer. MAC header information specific to encryption is allocated in the generic MAC header format.

Encryption is always applied to the MAC PDU payload when required by the selected ciphersuite; the generic MAC header is not encrypted. MAC management messages sent to the cell SID for broadcast and initial ranging, as well as the basic FID for a CPE SID, shall be sent in the clear to facilitate such functions as network entry, basic capability negotiation, and authentication exchange. All other management messages shall be protected by the MMP\_Key that is setup during the authentication exchange.

The format of MAC PDUs carrying encrypted or un-encrypted packet data payloads is specified in 8.4.2.1.

### 8.1.2 Key management and authentication overview

The SCM protocol allows for mutual authentication where both the network and CPEs authenticate each other. It also supports periodic reauthentication and key refresh. It uses strong encryption algorithms to perform key exchanges between a CPE and BS.

The SCM's authentication protocol establishes a shared secret (i.e., the AK) between the CPE and the BS. The shared secret is then used to secure subsequent SCM exchanges of TEKs. This two-tiered mechanism for key distribution permits refreshing of TEKs without incurring the overhead of computation-intensive operations.

EAP-based authentication uses Extensible Authentication Protocol framework (IETF RFC 3748 [B30]). EAP offers the operator to select an EAP Method (e.g., EAP-TLS; IETF RFC 2716 [B25]) to execute the authentication. Each EAP Method specifies a credential that is used to perform authentication and verify the device's/user's identity. For example, EAP-TLS uses a X.509 certificate, while EAP-SIM uses a Subscriber Identity Module.

EAP-TLS or EAP-TTLS shall be used; 8.5 defines the profile for the X.509 credential. In order to avoid security vulnerabilities, the EAP Method implemented in an IEEE 802.22 network shall comply with the mandatory requirements stated in Section 2.2 of IETF RFC 4017 [B33].

During initial authentication EAP transfer messages are not protected. For reauthentication, the EAP transfer messages are protected (encrypted and authenticated) using the MMP\_Key (8.2.4.6.2). If EAP reauthentication messages fail their authentication verification (8.3.2) or are not protected, they shall be ignored by the BS and CPE.

The AAA server and a client CPE authenticate each other during the initial authentication exchange. The AAA and CPE present their credentials to each other. Since the AAA and CPE mutually authenticate each other, there is protection against an attacker employing a cloned CPE that masquerades as a legitimate subscriber's CPE. Once authentication is completed, the BS and CPE have keying that is used to protect management messages (e.g., MMP\_Key) and keying used in transportation of keys for protection of user data (e.g., KEK). During authentication exchange, if a CPE indicates that it does not support protection of user data, no key exchange and state machines used to maintain keying to protect user data will be executed.

The traffic key management portion of the SCM protocol adheres to a client/server model, where the CPE (a SCM "client") requests keying material and the AAA server (a SCM "server") responds to those requests. This model provides for an individual CPE to receive keying material for security associations (SAs), for which they are configured.

The SCM protocol uses MAC management messaging, i.e., SCM-REQ and SCM-RSP messages defined in 7.7.21. The SCM protocol is defined in detail in 8.2.

### 8.1.3 Mapping of connections to SAs

The following rules for mapping connections to SAs apply:

- All transport connections shall be mapped to an existing SA.
- Multicast management connections shall be mapped to any Static or Dynamic GSA.
- The primary and secondary management connection shall be mapped to the null SA, i.e., the Null SAID.

The actual mapping for transport connections is achieved by including the SAID of an existing SA in the DSA-REQ/RSP and DSC-REQ/RSP messages together with the FID.

### 8.1.4 Cryptographic suite

A cryptographic suite is the SA's set of methods for data encryption, data authentication, and TEK exchange. The available cryptographic suites are specified as described in 8.4.1. The cryptographic suite shall be one of the ones listed in Table 193.

## 8.2 SCM protocol

### 8.2.1 Security associations (SAs)

A security association (SA) is the set of security information a BS and one or more of its client CPEs share in order to support secure communications across the IEEE 802.22 network. There are three basic types of SAs: Null, Unicast, and Group that can be defined. The Null SA and Unicast SAs shall only be static, i.e., they remain persistent for as long as the CPE is operational. Group SAs shall be either static or dynamic. GSAs are made dynamic by use of the SCM GSA Remove message.

Each CPE establishes the Null SA. The cryptographic suites that are to be used are negotiated during the authentication exchange that happens before the CPE registration during CPE initialization. If the BS configures the CPE for no other no other cryptographic suites (see 8.2.2.6 and 8.4.1) besides “no protection,” then no Unicast SAs shall be setup on the CPE. If other cryptographic suites, besides “no protection,” are configured for the CPE during the CPE authentication process, then at most two Unicast SAs that are distinct and unique to the CPE will be used. These SAs are known as the Primary and Secondary SAs.

The Primary SA shall be installed if the “authentication only” or “authentication+encryption” cryptographic suites are selected for the CPE. The Secondary SA shall only be installed on the CPE if the “encryption only” cryptographic suite is to be supported by the CPE. For complete description of the cryptographic suites, refer to 8.2.2.5. All of the unicast data traffic to/from the CPE shall be protected by the keying material provided by the Primary and/or Secondary SA. All of the unicast management traffic, e.g., on the primary/secondary management FIDs, shall be protected by the Null SA.

Establishment of Group SAs (GSAs) is optional. Group SAs are to be used for providing keying material for multicast transmission of management message traffic. GSAs are installed on a CPE using the SCM GSA Add message. A CPE is configured for a GSA, when the BS transmits the GSA add message to it. After assigning a CPE or group of CPEs to a multicast group (see 7.17), the BS may transmit the SCM GSA Add message to those CPEs to install the GSA on them. The SCM GSA message shall only be transmitted to the multicast group if the group was configured to support multicast via the Multicast Group Type parameter of the MCA-REQ (see 7.7.9).

Only after the GSA is established at the CPE, is it allowed to receive DS traffic on the multicast management FID mapped to the multicast group associated with the GSA. A GSA will only be established after the process to join a multicast group (see 7.17.1) has concluded. After the BS issues a MCA-REQ asking the CPE to leave the multicast group, it shall send a SCM GSA Remove message to CPE, requiring the CPE to delete any context information relating to the GSA associated with multicast group it was previously asked to leave.

An SA's shared information shall include the cryptographic suite employed within the SA. The shared information may include TEKs. The exact content of the SA is dependent on the SA's cryptographic suite.

SAs are identified using SAIDs. The Primary SA shall be identified by an SAID that is equal to the Basic FID of that CPE. The SAID of a GSA will be the Multicast FID of the group to which the CPE is assigned.

Using the SCM protocol, a CPE requests from its BS an SA's keying material.

The BS shall allow access by each client CPE to the SAs for which it is configured.

An SA's keying material has a limited lifetime. When the BS delivers SA keying material to a CPE, it also provides the CPE with that material's remaining lifetime. It is the responsibility of the CPE to request new keying material from the BS before the set of keying material that the CPE currently holds expires at the BS. Should the current keying material expire before a new set of keying material is received, the CPE shall perform reauthentication as described in 8.2.2. If a CPE is being shutdown or attempting affiliation with another BS, it shall stop any current authentication and TEK state machines, and delete any SAs for which it is currently configured.

In all cryptographic suites, key lifetime may be limited by the exhaustion rate of a number space, e.g., the PN of AES in GCM. In this case, the key ends either at the expiry of the key lifetime or the exhaustion of the number space, whichever is earliest. Note that in this case, security is not determined by the key lifetime.

SAs are not applicable to the protection of CBP bursts. CBP bursts will not be encrypted and/or authenticated by the methods and materials that are configured in a CPE's SAs. CBP protection mechanism only provides authentication. The CBP protection mechanism is defined in detail 8.6.2.

### **8.2.1.1 Dynamic Creation of GSA**

The BS may dynamically establish GSAs by issuing a GSA Add message/Remove message (via SCM-REQ/RSP). Upon receiving a GSA Add message, the CPE shall start a TEK state machine to establish and maintain GTEKs for each GSA listed in the message. Upon receiving a GSA Remove message, the CPE shall stop the GTEK state machine as well as delete the GKEK context (see 8.2.8.2). If a CPE is being shutdown or attempting association with another BS, it shall stop any TEK state machines associated with GSAs it is configured for and delete those GSAs.

### **8.2.1.2 Mapping of DS Multicast Traffic to SAs**

When creating a new DS multicast service flow for a multicast transport connection, the BS shall map this traffic to the null SA. Prior to scheduling traffic on a DS multicast group (see 7.17) and checks the CPEs authentication for the GSA that is assigned to the multicast group.

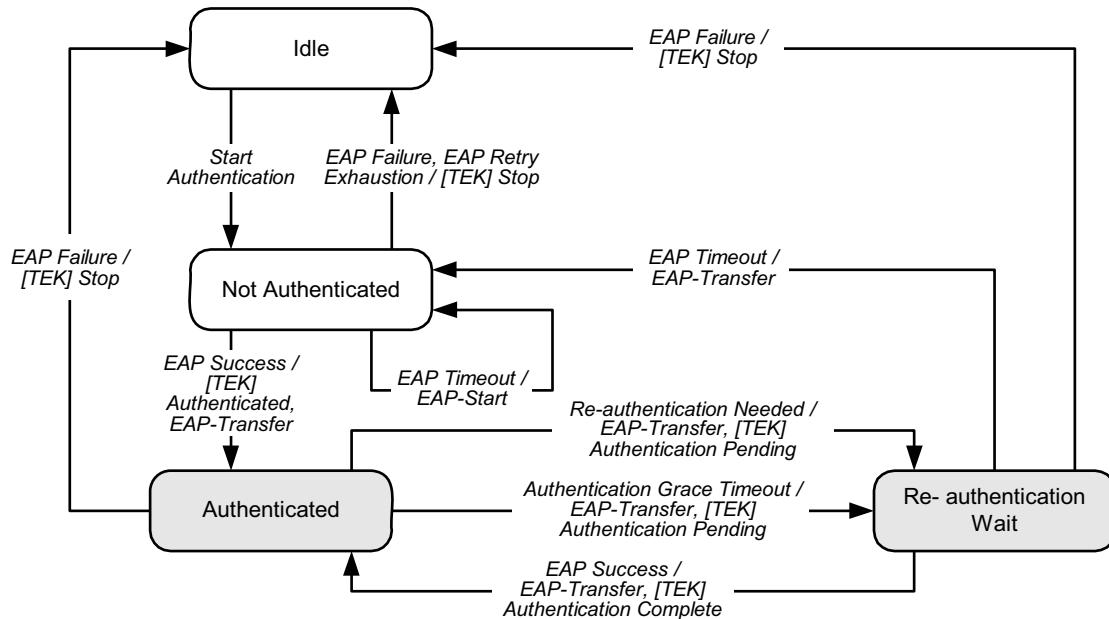
## **8.2.2 Authentication state machine**

The Authentication state machine (ASM) adopts an authentication framework similar to the model specified in IEEE Std 802.16-2009. The ASM incorporates EAP authentication and is made up of four states and thirteen events and messages that are used to communicate with other aspects of the SCM framework. The ASM has to interoperate with the TEK state machine (TSM, see 8.2.3) and the EAP Process.

### **8.2.2.1 ASM Flow Diagram and State Transition Table**

The ASM interacts with the EAP Process component of the CPE, known as the Supplicant. On the network side, the AAA service that the CPE authenticates to interacts with a component of the EAP Process known as the Authenticator. Specifications of most aspects related to the configuration, as well as operation of the EAP Process is out of scope of this standard. For details on how to operate and configure either the Supplicant or the Authenticator, refer to IETF RFC 3748 [B30], IETF RFC 4072 [B35], as well as IEEE Std 802.1X-2004 [B10].

Figure 114 presents the ASM as a state flow diagram, while Table 186 presents the ASM in a state transition table. In Figure 114 transitions are defined by the following format: ‘Trigger’/‘Action’. Shaded states in Figure 114 represent states whereby message exchanges (e.g., SCM EAP-Start and EAP-Transfer) shall be protected by the MMP\_Key derived from the currently active AK. Shaded fields of Table 186 represent non-valid state transitions that are not allowed or described in Figure 114.



**Figure 114 — Authentication state machine—Flow diagram**

**Table 186 — Authentication state machine—State transition matrix**

State Event or receive message	(A) <i>Idle</i>	(B) <i>Not Authenticated</i>	(C) <i>Reauthentication Wait</i>	(D) <i>Authenticated</i>
(1) <i>Start Authentication</i>	Not Authenticated			
(2) <i>EAP Timeout</i>		Not Authenticated	Not Authenticated	
(3) <i>EAP Failure</i>		Idle	Idle	Idle
(4) <i>EAP Retry Exhaustion</i>		Idle		
(5) <i>EAP Success</i>		Authenticated	Authenticated	
(6) <i>Reauthentication Needed</i>				Re-authentication Wait
(7) <i>Authentication Grace Timeout</i>				Re-authentication Wait

### 8.2.2.2 States

*Idle*: Initial state of the ASM.

*Not Authenticated:* The ASM, thus the CPE, is not authenticated. The CPE is awaiting an indication from the EAP Process that EAP authentication. The EAP Process accomplishes this with signaling an *EAP Success* event, and transferring the MSK to the BS and CPE. This state is only left when an EAP Success or EAP Failure event is signaled by the EAP Process, as well as exhaustion of the ‘Max # EAP Authentication Attempts’. If entering this state from the Reauthentication Wait state, the CPE shall protect the SCM EAP-Start/Transfer messages with the MMP\_Key of the current AK.

*Reauthentication Wait:* The ASM is halted, pending a reauthentication request. This state is entered when the operator triggers reauthentication or the current authentication is about to expire. SCM EAP-Start/Transfer messages shall be protected with the MMP\_Key of the current AK.

*Authenticated:* The ASM has completed the EAP authentication. The EAP process has delivered the MSK to the CPE and BS. Both have then subsequently derived the PMK from the MSK. If this state was entered from the Reauthentication Wait state, all subsequent SCM EAP-Start/Transfer messages, as well as the SCM Key-Request/Reply messages shall be protected by the MMP\_Key of the current active AK. While in this state, two active AK contexts can be maintained at the CPE. This process is described further in 8.3.1.1–8.3.1.3.

### 8.2.2.3 Messages

*SCM EAP-Start:* The Supplicant on the CPE uses this message is used to start authentication. The Supplicant on the CPE may also use this message to start reauthentication. When used during reauthentication, this message shall be protected using the MMP\_Key of the currently active AK.

*SCM EAP-Transfer:* The Supplicant (CPE) and Authenticator (AAA) use this message to exchange EAP data packets to conduct the EAP authentication exchange. In the Not Authenticated state, this message is not protected. During reauthentication this message is protected using the MMP\_Key of the currently active AK.

### 8.2.2.4 Events

*Start Authentication:* This event is generated to start the ASM after the conclusion of the basic capabilities exchange (CBC-REQ/RSP) during network entry.

*EAP Timeout:* ASM generates this event when ‘EAP Authentication Timer’ has expired prior to reception of SCM EAP-Start/Transfer messages during initial authentication or reauthentication. When this happens, the ‘Current # of Authentication Attempts’ is incremented and the ‘EAP Authentication Timer’ is restarted.

*EAP Failure:* The EAP Process generates this message to tell the ASM that the EAP Process has not resulted in successful authentication being verified.

*EAP Retry Exhaustion:* This event is generated by the ASM when the ‘Max # EAP Authentication Attempts’ has been reached without successful completion of authentication or reauthentication.

*EAP Success:* The EAP Process generates this even to tell ASM that EAP Process, during initial authentication or reauthentication, has completed successfully. The ‘Current # of Authentication Attempts’ is set to zero upon indication of this event.

*Reauthentication Needed:* Generated when the network operator or AAA service decides to force re-authentication prior to expiration of current AK or to update successive/concurrent AK contexts (see 8.3.1.1–8.3.1.3) that are operating on the CPE. Reception of an (unsolicited) SCM EAP-Start/Transfer message prior to expiration of current AK, while in the Authenticated state, can trigger this event.

*Authentication Grace Timeout:* When ‘Authentication Grace Timer’ expires, reauthentication process is automatically restarted.

The ASM also sends the following events to the TEK state machine:

- *[TEK] Stop*: Sent by the ASM to stop the TEK state machine governing the key management for Primary and Secondary SAs, as well as GSAs set up on the CPE.
- *[TEK] Authentication Complete*: Sent by ASM to TEK state machine to tell TEK state machine to continue operation from the Op Reauth Wait and Rekey Reauth Wait states, when authentication is pending.
- *[TEK] Authentication Pending*: Sent by ASM to TEK state machine to halt TEK state machine while ASM conducts reauthentication. This event is sent to the Op Reauth Wait and Rekey Reauth Wait states when reauthentication is initiated.
- *[TEK] Authenticated*: Sent by ASM to start a TEK state machine for either the Primary or the Secondary SA, as well as any configured GSA.

#### 8.2.2.5 Parameters

*EAP Authentication Timer*: Time period between 1) sending SCM EAP-Start message after not receiving an EAP-Transfer or *EAP Success* indication during initial authentication (e.g., while in Not Authenticated state) or 2) between resending SCM EAP-Transfer or *EAP Success* indication during reauthentication (e.g., while in Reauthentication Wait state).

*Authentication Grace Timer*: Amount of time after authentication is complete that must pass before reauthentication is triggered.

*Max # EAP Authentication Attempts*: Maximum number times a CPE is allowed to attempt EAP authentication.

*Current # EAP Authentication Attempts*: Current count of attempts to complete EAP authentication.

#### 8.2.2.6 Actions

1-A: Idle (Start Authentication) → Not Authenticated

- a) Enable SCM EAP-Start or EAP-Transfer messages to be transferred between ‘Supplicant’ and ‘Authenticator’

2-B: Not Authenticated (EAP Timeout) → Not Authenticated

- a) Enable SCM EAP-Start message to be transferred between ‘Supplicant’ and ‘Authenticator’
- b) Increment ‘Current # of EAP Authentication Attempts’
- c) Reset ‘EAP Authentication Timer’

2-C: Not Authenticated (EAP Timeout) → Not Authenticated

- a) Enable SCM EAP-Transfer message to be transferred between ‘Supplicant’ and ‘Authenticator’
- b) Increment ‘Current # of EAP Authentication Attempts’
- c) Reset ‘EAP Authentication Timer’

3-B: Not Authenticated (EAP Failure) → Idle

- a) Stop ASM

3-C: Reauthentication Wait (EAP Failure) → Idle

- a) Stop all TEK state machines
- b) Stop ASM

3-D: Authenticated (EAP Failure) → Idle

- a) Stop all TEK state machines

- b) Stop ASM

4-B: Not Authenticated (EAP Retry Exhaustion) → Idle

- a) Stop ASM (e.g., ‘Current # of EAP Authentication Attempts’ should be  $\geq$  ‘Max # of EAP Authentication Attempts’)

5-B: Not Authenticated (EAP Success) → Authenticated

- a) Start TEK state machine
- b) Start ‘Authentication Grace Timer’
- c) Follow procedures in 8.3.1 to manage successive/concurrent AKs
- d) Reset ‘Current # of EAP Authentication Attempts’

5-C: Reauthentication Wait (EAP Success) → Authenticated

- a) Start ‘Authentication Grace Timer’
- b) Follow procedures in 8.3.1 to manage successive/concurrent AKs
- c) Reset ‘Current # of EAP Authentication Attempts’
- d) Continue operation of TEK state machine

6-D: Authenticated (Reauthentication Needed) → Reauthentication Wait

- a) Enable SCM EAP-Transfer message to be transferred between ‘Supplicant’ and ‘Authenticator’
- b) Reset ‘Current # of EAP Authentication Attempts’
- c) Reset ‘EAP Authentication Timer’
- d) Halt operation of TEK state machine

7-D: Authenticated (Authentication Grace Timeout) → Reauthentication Wait

- a) Enable SCM EAP-Transfer message to be transferred between ‘Supplicant’ and ‘Authenticator’
- b) Reset ‘Current # of EAP Authentication Attempts’
- c) Reset ‘EAP Authentication Timer’

### 8.2.2.7 Security capabilities negotiation

As part of their EAP Process, the Supplicant (CPE) provides the BS and Authenticator (AAA service) with a list of all the cryptographic suites (pairing of data encryption and data authentication algorithms) the CPE supports during initiation of initial authentication or reauthentication. The Supplicant may also provide the Authenticator negotiate values for SCM-related parameters (Table 187) that it will use. This information is carried in Attribute Value Pairs (AVPs) of EAP packets encapsulated in either an SCM EAP-Start or EAP-Transfer message.

The format of the data that is exchanged between the Supplicant and the Authenticator shall conform to the methods specified by the AAA service (e.g., RADIUS/RFC 2865 [B26] or DIAMETER/RFC 3588 [B1]) that operator will deploy. The parameters that describe the cryptographic suite options are in 8.4.1. Other SCM-related parameters are described in Table 187. If these items are not negotiated during the authentication procedure, then the default cryptographic suite that is selected is ‘No Protection’ and the default values for other SCM-related parameters in Table 187 are used.

Upon verifying the Supplicant’s credential (e.g., *EAP Success* event), the Authenticator selects from this list a single cryptographic suite to employ with the requesting CPE’s Primary and Secondary SA, as well as the (default) cryptographic suite to be applied to multicast management traffic assigned to any GSAs the CPE may be a part of in the future. This information will be carried in the SCM EAP-Transfer message that carries the MSK to the BS and CPE (upon completion of EAP authentication). Table 188 defines the format of the CPE’s SCM configuration information that the Authenticator provides to the Supplicant. The Authenticator shall reject the authentication request if it determines that none of the offered cryptographic suites are satisfactory.

Each static SA-Descriptor identifies the cryptographic suite employed within the SA. The selection of a static SA's cryptographic suite is typically made independent of the requesting CPE's cryptographic capabilities. An Authenticator may include in its EAP-Transfer message, SA-Descriptors identifying the cryptographic suites for SAs for which the AAA authenticates the CPE. The CPE shall not start TEK state machines for static SAs for cryptographic suites that the CPE does not support, nor if "no protection" is the suite chosen for the SA.

SA-Descriptors for the Primary and Secondary SAs shall only be provided in EAP-Transfer messages. SA-Descriptors for GSAs shall not be provided for in EAP-Transfer messages. Only the default cryptographic suite to be employed by GSAs shall be sent in an EAP-Transfer message. One or more GSAs may be installed on the CPE via the SCM GSA-Add message, following addition of that CPE to a multicast group (see 7.17).

If the "no protection" suite is the only cryptographic suite that a CPE supports, then no unicast or group SAs shall be configured for the CPE and no TEK state machines shall be started and any traffic that the CPE transmits will be mapped to the Null SA when a service flow is defined.

Table 187 gives an example of how the list of cryptographic suites and SCM-related parameters that the IEEE 802.22-based Suplicant supports can be signaled to the Authenticator.

**Table 187 — CPE SCM configuration request**

Syntax	Size	Notes
Num_crypto_suites	8 bits	Number of cryptographic suites supported.
for ( $i=1; i < \text{Num\_crypto\_suites}; i++\{\right.$		
Cryptographic Suite	8 bits	See 8.4.1
$\}$		
EAP Authentication Timer	24 bits	Timeout period between sending SCM EAP-Start or EAP-Transfer, in seconds (see 8.2.2.5).
Authentication Grace Timer	24 bits	Amount of time after authentication is complete that must pass before reauthentication is complete, in seconds (see 8.2.2.5).
Max # of EAP Authentication attempts	8 bits	Maximum # of attempts a CPE can attempt EAP authentication (see 8.2.2.5).
Operational Wait Timeout	24 bits	Timeout between sending of Key Request messages from the Op Wait state, in seconds (see 8.2.3.2.4).
Rekey Wait Timeout	24 bits	Timeout between sending of Key Request messages from the Rekey Wait state, in seconds (see 8.2.3.2.4).
GTEK/TEK Grace Time	24 bits	Time interval, in seconds, before the estimated expiration of a GTEK/TEK that the CPE starts rekeying for a new GTEK/TEK.
SCM Version Support	8 bits	Version of SCM protocol the CPE supports.
SCM Flow Control	8 bits	Number of ongoing SCM transactions the CPE will allow.
PN Window Size	8 bits	Size of PN_WINDOW (see 8.4).

Table 188 gives an example of how the Authenticator can signal the Suplicant with the values for SCM parameters as well as the cryptographic suite configuration for any SAs for which the CPE is configured.

**Table 188 — CPE SCM configuration reply**

Syntax	Size	Notes
Num_SA_Descriptors	8 bits	Number of SAs being configured
for ( $i=0; i < \text{Num\_SA\_Descriptors}; i++\{\right.$		
SAID	16 bits	SAID of SA
SA-Type	1 bit	Type of SA: 0: Primary (Unicast) SA 1: Secondary (Unicast) SA

Syntax	Size	Notes
Cryptographic Suite	8 bits	Cryptographic Suite to be employed by the SA, see Table 193. Only suite = 0x05 can be selected for the Secondary (Unicast) SA.
}		
Default Cryptographic Suite for GSAs	8 bits	Either 0x03 or 0x04, see Table 193.
Default Cryptographic Suite for GKEK/GTEK Generation	8 bits	Either 0x06 or 0x07, see Table 193.
EAP Authentication Timer	24 bits	Timeout period between sending SCM EAP-Start or EAP-Transfer, in seconds (see 8.2.2.5).
Authentication Grace Timer	24 bits	Amount of time after authentication is complete that must pass before reauthentication is complete, in seconds (see 8.2.2.5).
Max # of EAP Authentication attempts	8 bits	Maximum number of attempts a CPE can attempt EAP authentication (see 8.2.2.5).
Operational Wait Timeout	24 bits	Timeout between sending of Key Request messages from the Op Wait state, in seconds (see 8.2.3.2.4).
Rekey Wait Timeout	24 bits	Timeout between sending of Key Request messages from the Rekey Wait state, in seconds (see 8.2.3.2.4).
GTEK/TEK Grace Time	24 bits	Time interval, in seconds, before the estimated expiration of a GTEK/TEK that the CPE starts rekeying for a new GTEK/TEK.
Max # of Key Request Attempts	8 bits	Max number of attempts a CPE can attempt a Key Request.
SCM Version Support	8 bits	Version of SCM protocol the CPE supports.
SCM Flow Control	8 bits	Number of ongoing SCM transactions the CPE will allow.
PN Window Size	8 bits	Size of PN_WINDOW (see 8.4).

If the SA defines use of authentication only or “no protection” method, all MAC PDUs sent with FIDs linked to this SA must have EC bit set to ‘0’ in the generic MAC header. Otherwise, if only “authentication+encryption” or “encryption only” is supported the EC bit must be set to ‘1’ in the generic MAC header. Other combinations are not allowed; MAC PDUs presenting other combinations should be discarded.

The capabilities defined in an SA are not applicable to management messages transmitted on the Initial Ranging, Basic, as well as Broadcast connections. Only data traffic mapped to the Null SA will be allowed to be transmitted without any authentication or encryption information.

### 8.2.3 TEK exchange overview

#### 8.2.3.1 TEK exchange overview for PMP topology

If the CPE and BS decide “No authentication” as their authentication policy, the CPE and BS shall not perform the Key Request/Key Reply handshake. In this case, target SAID value, which may be included in DSA-REQ/RSP messages, shall be Null SAID.

Upon achieving authentication, a CPE starts a separate TEK state machine for each of the SAIDs identified in the Authentication Reply message. Each TEK state machine operating within the CPE is responsible for managing the keying material associated with its respective SAID. TEK state machines periodically send Key Request messages to the BS, requesting a refresh of keying material for their respective SAIDs.

TEK state machines periodically cause the CPE to send Key Request messages to the BS, requesting a refresh of keying material for their respective SAIDs. The BS responds to a Key Request with a Key Reply message, containing the BS’s active keying material for a specific SAID.

The TEK is encrypted using appropriate KEK derived from the AK. For AES-GCM, the TEK is a 128 bit key and the KEK is derived from the AK using a 128 bit key and 128 bit block size.

Note that at all times the BS maintains two active sets of keying material per SAID. The lifetimes of the two generations overlap so that each generation becomes active halfway through the life of its predecessor and expires halfway through the life of its successor. A BS includes in its Key Replies *both* of an SAID's active generations of keying material.

For SAs using a ciphersuite employing AES-GCM mode, the Key Reply provides the requesting CPE, in addition to the TEK, the remaining lifetime of each of the two sets of keying material. The receiving CPE uses these remaining lifetimes to estimate when the BS will invalidate a particular TEK and, therefore, when to schedule future Key Requests so that the CPE requests and receives new keying material before the BS expires the keying material the CPE currently holds. For AES-GCM mode, when more than half the available PN numbers in the 24-bit PN number space are exhausted, the CPE shall schedule a future Key Request in the same fashion as if the key lifetime was approaching expiry.

The operation of the TEK state machine's Key Request scheduling algorithm, combined with the BS's regimen for updating and using an SAID's keying material (see Figure 115 and Table 189), provides for the CPE to be able to continually exchange encrypted traffic with the BS.

A TEK state machine remains active as long as

- 1) The CPE is authenticated and allowed to operate in the BS's security domain, i.e., it has a valid AK, and
- 2) The CPE is configured to participate in that particular SA, i.e., the BS continues to provide fresh keying material during rekey cycles.

The parent Authentication state machine stops *all* of its child TEK state machines when the TEK state machine sends a *[TEK] Stop* message during a reauthentication cycle. Individual TEK state machines can be started or stopped during a reauthentication cycle if a CPE's Static SAID authentications changed between successive reauthentications.

Communication between Authentication and TEK state machines occurs through the passing of events and protocol messaging. The Authentication state machine generates events (i.e., Stop, Authenticated, Authentication Pending, and Authentication Complete events) that are targeted at its child TEK state machines. TEK state machines do not target events at their parent Authentication state machine. The TEK state machine affects the Authentication state machine indirectly through the messaging a BS sends in response to a CPE's requests: a BS may respond to a TEK machine's Key Requests with a failure response (i.e., Stop or Authentication Pending events) to be handled by the Authentication state machine

### **8.2.3.2 TEK state machine**

The TEK state machine consists of seven states and eleven events (including receipt of messages) that may trigger state transitions. Like the Authentication state machine, the TEK state machine is presented in both a state flow diagram (Figure 115) and a state transition matrix (Table 189). As was the case for the Authentication state machine, the state transition matrix shall be used as the definitive specification of protocol actions associated with each state transition.

Shaded states in Figure 115 (Operational, Rekey Wait, Rekey Reauthenticate Wait, and Multicast Rekey Interim Wait) have valid keying material and encrypted traffic may be sent. Shaded blocks in Table 186 highlight transitions that shall not be allowed.

The SAID may be replaced by the GSAID for the multicast service. And, the TEK may be also replaced by the GTEK for the multicast service.

The Authentication state machine starts an independent TEK state machine for each SA for which a CPE is configured. As mentioned in 8.2.2, the BS maintains two active TEKs/GTEKs per SA. Each SA is uniquely identified by its security association identifier (SAID).

For the unicast service, the BS includes in its Key Replies both of these TEKs, along with their remaining lifetimes. For the multicast service, the BS includes in its Key Replies both of the GTEKs, along with their remaining lifetimes.

The BS encrypts downlink traffic with the older of its two TEKs and decrypts uplink traffic with either the older or newer TEK, depending upon which of the two keys the CPE was using at the time. The CPE encrypts uplink traffic with the newer of its two TEKs and decrypts downlink traffic with either the older or newer TEK, depending upon which of the two keys the BS was using at the time. See 8.3 for details on CPE and BS key usage requirements.

For the multicast service, the BS shall install a GSA on the CPEs prior to transmitting traffic if any multicast management connections are to be mapped to the GSA using the SCM GSA Add message. The SCM GSA Add message (see Table 168) contains the SAID of the GSA, the GKEK, and the remaining lifetime of the GKEK. When a CPE receives this message it shall issue a Key Request message to the BS. The BS will respond with a Key-Reply, which uses the GKEK to protect both generations of GTEKs. The BS shall update the GKEK by sending another SCM GSA Add message to the CPE, prior to expiration of the amount of “Remaining GKEK Lifetime” as specified in the last SCM GSA Add message. If an amount of time greater than the “Remaining GKEK Lifetime” of the SCM GSA Add message has passed, it shall not start any key exchange transaction (e.g., Key-Request/Reply) until a SCM GSA Add message is sent by the BS. The CPE verifies and/or decrypts downlink traffic with either the older or newer GTEK, depending upon which of the two keys the BS is using at the time. See 8.3 for details on CPE and BS key usage requirements.

Through operation of a TEK state machine, the CPE attempts to keep its copies of SAID’s TEKs synchronized with those of its BS. A TEK state machine issues Key Requests to refresh copies of its SAID’s keying material soon after the scheduled expiration time of the older of its two TEKs and before the expiration of its newer TEK. To accommodate for CPE/BS clock skew and other system processing and transmission delays, the CPE schedules its Key Requests a configurable number of seconds before the newer TEK’s estimated expiration occurs at the BS. With the receipt of the Key Reply, the CPE shall always update its records with the TEK parameters from both TEKs/GTEKs contained in the Key Reply message.

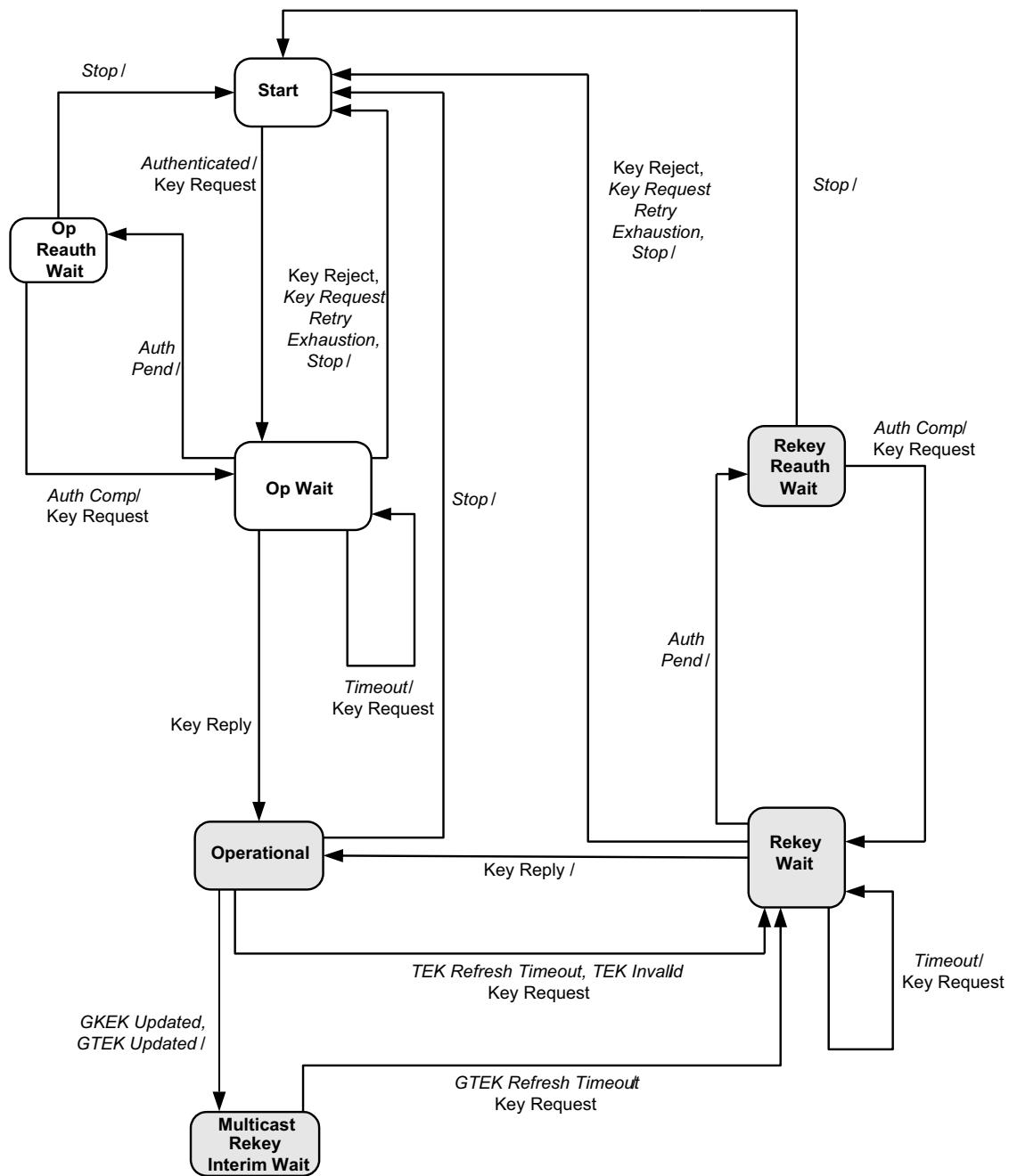


Figure 115 — TEK state machine flow diagram

**Table 189 — TEK State Transition Finite state machine**

<b>State / Event or Recvd Msg</b>	<b>(A) Start</b>	<b>(B) Op Wait</b>	<b>(C) Op Reauth Wait</b>	<b>(D) Op</b>	<b>(E) Rekey Wait</b>	<b>(F) Rekey Reauth Wait</b>	<b>(G) Multicast Rekey Interim Wait</b>
<i>(1) Stop</i>		Start	Start	Start	Start	Start	
<i>(2) Authenticated</i>	Op Wait						
<i>(3) Auth Pend</i>		Op Reauth Wait			Rekey Reauth Wait		
<i>(4) Auth Comp</i>			Op Wait			Rekey Wait	
<i>(5) TEK Invalid</i>				Rekey Wait			
<i>(6) Timeout</i>		Op Wait			Rekey Wait		
<i>(7) TEK Refresh Timeout</i>				Rekey Wait			
<i>(8) GTEK Refresh Timeout</i>							Rekey Wait
<i>(9) Key Reply</i>		Operational			Operational		
<i>(10) Key Reject</i>		Start			Start		
<i>(11) GKEK Updated</i>				Multicast Rekey Interim Wait			
<i>(12) GTEK Updated</i>				Multicast Rekey Interim Wait			
<i>(13) Key Request Retry Exhaustion</i>		Start			Start		

### 8.2.3.2.1 States

*Start:* This is the initial state of the FSM. No resources are assigned to or used by the FSM in this state—e.g., all timers are off, and no processing is scheduled.

*Operational Wait (Op Wait):* The TEK state machine has sent its initial request (Key Request) for its SAID's keying material (TEK), and is waiting for a reply from the BS.

*Operational Reauthenticate Wait (Op Reauth Wait):* The wait state the TEK state machine is placed in if it does not have valid keying material while the Authentication state machine is in the middle of a reauthentication cycle.

*Operational:* The CPE has valid keying material for the associated SAID.

*Rekey Wait:* The TEK Refresh Timeout has expired or the TEK Invalid message has been received and the CPE has requested a key update for this SAID. Note that the newer of its two TEKs has not expired and may still be used for both encrypting and decrypting data traffic.

*Rekey Reauthenticate Wait (Rekey Reauth Wait):* The wait state the TEK state machine is placed in if the TEK state machine has valid traffic keying material, has an outstanding request for the latest keying material, and the Authentication state machine initiates a reauthentication cycle.

*Multicast Rekey Interim Wait (Multicast Rekey Interim Wait):* This state is defined only for the multicast service. This state is the wait state the TEK state machine is placed in if the TEK state machine has valid traffic keying material and receives the new GKEK from the BS after receiving a SCM GSA Add message.

### 8.2.3.2.2 Messages

Note that the message formats are defined in detail in 0.

*Key Request:* Request a TEK for this SAID. Sent by the CPE to the BS and authenticated with keyed message digest. The message authentication key used to do this, the MMP\_KEY, is derived from the AK.

*Key Reply:* Response from the BS carrying the two diversity sets of traffic keying material for this SAID. Sent by the BS to the CPE, it includes the SAID's TEKs, encrypted with a KEK derived from the AK or the GSAID's GTEK, encrypted with a. The Key Reply message is authenticated with a keyed message digest; the MMP\_KEY used to do this is key is derived from the AK.

*Key Reject:* Response from the BS to the CPE to indicate this SAID is no longer valid and no key will be sent. The Key Reject message is authenticated with a keyed message digest; the MMP\_KEY used to do this, is derived from the AK.

*TEK Invalid:* The BS sends this message to the CPE if it determines that the CPE encrypted an uplink PDU with an invalid TEK, i.e., an SAID's TEK key sequence number, contained within the received PDU's MAC Header, is out of the BS's range of known, valid sequence numbers for that SAID.

### 8.2.3.2.3 Events

*Stop:* Sent by the Authentication state machine to an active (non-START state) TEK state machine to terminate TEK state machine and remove the corresponding SAID's keying material from the CPE key table. See Figure 116.

*Authenticated:* Sent by the Authentication state machine to a non-active (START state) TEK state machine to notify TEK state machine of successful authentication. See Figure 115.

*Authentication Pending (Auth Pend):* Sent by the Authentication FSM to TEK FSM to place TEK FSM in a wait state while Authentication FSM completes reauthentication. See Figure 115.

*Authentication Complete (Auth Comp):* Sent by the Authentication state machine to a TEK state machine in the Operational Reauthenticate Wait or Rekey Reauthenticate Wait states to clear the wait state begun by the prior Authentication Pending event. See Figure 115.

*TEK Invalid:* This event is triggered by either a CPE's data packet decryption logic or by the receipt of a TEK Invalid message from the BS.

A CPE's data packet decryption logic triggers a TEK Invalid event if it recognizes a loss of TEK key synchronization between itself and the encrypting BS. For example, an SAID's TEK key sequence number, contained within the received downlink MAC PDU header, is out of the CPE's range of known sequence numbers for that SAID.

A BS sends a TEK Invalid message to the CPE, triggering a TEK Invalid event within the CPE, if the BS's decryption logic recognizes a loss of TEK key synchronization between itself and the CPE.

*Timeout:* A retry timer timeout. Generally, when either the *Operational Wait Timeout* expires while in the *Op Wait* state or when the *Rekey Wait Timeout* expires while in the *Rekey Wait* state. Whenever this happens, a counter tracking the current number of Key Request attempts is incremented.

*GTEK/TEK Refresh Timeout:* The TEK refresh timer timed out. This timer event signals the TEK state machine to issue a new Key Request in order to refresh its keying material. The refresh timer is set to fire a configurable duration of time (GTEK/TEK Grace Time) before the expiration of the newer TEK the CPE currently holds. This is configured via the BS to occur after the scheduled expiration of the older of the two TEKs.

*GKEK Updated:* This event is triggered when the CPE receives the new GKEK through the SCM GSA Add.

*TEK/GTEK Updated:* This event is triggered when the CPE receives the new TEK or GTEK and traffic keying material through the Key Reply message.

*Key Request Retry Exhaustion:* This event is triggered when the number of Key Request attempts after the *Timeout* event while in the "Op Wait" or "Rekey Wait" has been exhausted. When this even is triggered, the count of current number of Key Request attempts is reset.

#### 8.2.3.2.4 Parameters

All configuration parameter values take the default values from Table 272 or may be specified in Auth Reply message. Theses value shall be 4 octets long.

*Operational Wait Timeout:* Timeout period between sending of Key Request messages from the Op Wait state (see Table 272).

*Rekey Wait Timeout:* Timeout period between sending of Key Request messages from the Rekey Wait state (see Table 275).

*GTEK/TEK Grace Time:* Time interval, in seconds, before the estimated expiration of a GTEK/TEK that the CPE starts rekeying for a new GTEK/TEK. GTEK/TEK Grace Time takes the default value from Table 275 or may be specified in a configuration setting within the Auth Reply message and is the same across all SAIDs (see Table 275).

*Max # Key Request Attempts:* Maximum number times a CPE is allowed to attempt Key Request transaction while in the *Op Wait* or *Rekey Wait* states.

*Current # Key Request Attempts:* Current count of attempts to complete a Key Request transaction.

#### 8.2.3.2.5 Actions

Actions taken in association with state transitions are listed by <event> (<rcvd message>) → <state>:

1-B Op Wait (*Stop*) → Start

- a) Clear Key Request retry timer
- b) Terminate TEK FSM

1-C Op Reauth Wait (*Stop*) → Start

- a) Terminate TEK FSM

1-D Operational (*Stop*) → Start

- a) Clear TEK refresh timer, which is timer set to go off “GTEK/TEK Grace Time” seconds prior to the TEK’s scheduled expiration time
- b) Terminate TEK FSM
- c) Remove SAID keying material from key table

1-E Rekey Wait (*Stop*) → Start

- a) Clear Key Request retry timer
- b) Terminate TEK FSM
- c) Remove SAID keying material from key table

1-F Rekey Reauth Wait (*Stop*) → Start

- a) Terminate TEK FSM
- b) Remove SAID keying material from key table

2-A Start (*Authenticated*) → Op Wait

- a) Send Key Request message to BS
- b) Set Key Request retry timer to Operational Wait Timeout

3-B Op Wait (*Auth Pend*) → Op Reauth Wait

- a) Clear Key Request retry timer

3-E Rekey Wait (*Auth Pend*) → Rekey Reauth Wait

- a) Clear Key Request retry timer

4-C Op Reauth Wait (*Auth Comp*) → Op Wait

- a) Send Key Request message to BS
- b) Set Key Request retry timer to Operational Wait Timeout

4-F Rekey Reauth Wait (*Auth Comp*) → Rekey Wait

- a) Send Key Request message to BS
- b) Set Key Request retry timer to Rekey Wait Timeout

5-D Operational (*TEK Invalid*) → Rekey Wait

- a) Clear TEK refresh timer
- b) Send Key Request message to BS
- c) Set Key Request retry timer to Rekey Wait Timeout
- d) Remove SAID keying material from key table

6-B Op Wait (*Timeout*) → Op Wait

- a) Send Key Request message to BS
- b) Set Key Request retry timer to Operational Wait Timeout

6-E Rekey Wait (*Timeout*) → Rekey Wait

- a) Send Key Request message to BS
- b) Set Key Request retry timer to Rekey Wait Timeout

7-D Operational (*TEK Refresh Timeout or TEK Invalid message*) → Rekey Wait

- a) Send Key Request message to BS
- b) Set Key Request retry timer to Rekey Wait Timeout

8-G Multicast Rekey Interim Wait (*TEK Refresh Timeout*) → Rekey Wait

- a) Send Key Request message to BS
- b) Set Key Request retry timer to Rekey Wait Timeout

9-B Op Wait (*Key Reply*) → Operational

- a) Clear Key Request retry timer
- b) Process contents of Key Reply message and incorporate new keying material into key database
- c) Set the TEK refresh timer to go off “GTEK/TEK Grace Time” seconds prior to the newer key’s scheduled expiration

9-E Rekey Wait (*Key Reply*) → Operational

- a) Clear Key Request retry timer
- b) Process contents of Key Reply message and incorporate new keying material into key database
- c) Set the TEK refresh timer to go off “GTEK/TEK Grace Time” seconds prior to the newer key’s scheduled expiration

10-B Op Wait (*Key Reject*) → Start

- a) Clear Key Request retry timer
- b) Terminate TEK FSM

10-E Rekey Wait (*Key Reject*) → Start

- a) Clear Key Request retry timer
- b) Terminate TEK FSM
- c) Remove SAID keying material from key table

11-D Operational (*GKEK Updated*) → M&B Rekey Interim Wait

- a) Process contents of the received GSA Add message, and incorporate new GKEK into key database

12-G Operational (*GTEK Updated*) → M&B Rekey Interim Wait

- a) Process contents of the Key Reply message, and incorporate new traffic keying material into key database
- b) Set the GTEK refresh timer to go off “GTEK/TEK Grace Time” seconds prior to the key’s scheduled expiration.

13-B Op Wait (*Key Request Retry Exhaustion*) → Start

- a) Clear Key Request retry timer
- b) Clear count of current Key Request attempts
- c) Terminate TEK FSM
- d) Remove SAID keying material from key table

13-E Rekey Wait (*Key Request Retry Exhaustion*) → Start

- a) Clear Key Request retry timer
- b) Clear count of current Key Request attempts
- c) Terminate TEK FSM
- d) Remove SAID keying material from key table

#### 8.2.4 Key derivation

The SCM key hierarchy defines what keys are present in the system and how the keys are generated. IEEE 802.22 systems shall use either EAP-TLS or EAP-TTLS EAP-based, authentication schemes. The keys used to protect management message integrity and transport the TEKs are derived from source key material

generated by the authentication process. The EAP authentication process yields the Pairwise Master Key (PMK). All SCM key derivations are based on the Dot22KDF algorithm as defined in 8.2.4.7.

#### **8.2.4.1 AK derivation**

The AK will be derived by the BS and the CPE from the PMK, when the EAP-based authentication procedure has concluded.

After the authentication procedure has been performed, the CPE and BS will both possess the PMK. The derivation of the AK is based on the following:

$$\text{AK} = \text{Dot22KDF}(\text{PMK}, \text{CPE MAC Address} \mid \text{BSID} \mid \text{"AK"}, 160)$$

#### **8.2.4.2 KEK derivation**

The KEK is derived directly from the AK. It is used to encrypt the TEKs, GKEK and all other keys sent by the BS to the CPE in Key Reply message.

#### **8.2.4.3 GKEK derivation**

There are two methods for GKEK generation. If 0x05 is among the cryptographic suites (see Table 193) that is selected for a particular GSA, then GKEK is randomly generated at the BS or a network entity (for example, an ASA server) and transmitted to the CPE encrypted with the KEK. If 0x06 is among the cryptographic suites (see Table 193), then a pre-arranged operator specific method can be used to drive GKEK derivation. When using the operator specific method, the KEK is used to transport the keying material or any other data the operator specific method requires for GKEK generation. There is one GKEK per Group Security Association. GKEK is used to encrypt the GTEKs sent in the Key Reply message by the BS to the CPEs in the same multicast group.

#### **8.2.4.4 Traffic encryption key (TEK)**

The TEK is generated as a random number in the BS and is encrypted using the corresponding TEK encryption algorithm (e.g., AES key wrap [IETF RFC 5649] for SAs with TEK encryption algorithm identifier in the cryptographic suite is equal to 0x01–0x04), keyed with the KEK and transferred between BS and CPE in the TEK exchange.

#### **8.2.4.5 Group traffic encryption key (GTEK)**

The GTEK is used to encrypt data packets of the multicast management service and it is shared among all CPEs that belong to the multicast group. There are two GTEKs per GSA. Just as with TEKs, GTEKs will have overlapping lifetimes. Regardless of the cryptographic suite selected for GTEK generation (e.g., 0x05 or 0x06), the GTEK is encrypted using same algorithms applied to encryption for TEK and transmitted to the CPE in broadcast or unicast messages.

#### **8.2.4.6 Management Message Protection key and KEK derivation**

##### **8.2.4.6.1 MMP\_PN management**

The CPE shall maintain a MMP\_PN counter for each AK. The BS is assumed to maintain a MMP\_PN counter for each AK context as well. This is done to keep the MMP\_PN value synchronized with the corresponding counter at the CPE. The value of this counter maintained by the CPE is denoted as MMP\_PN<sub>C</sub> and the value maintained by the BS is denoted as MMP\_PN<sub>B</sub>.

#### **8.2.4.6.1.1 Maintenance of MMP\_PN<sub>C</sub> by the CPE**

Upon successful completion of the SCM initial authentication or reauthentication, and establishment of a new AK, the CPE shall instantiate a new MMP\_PN counter and set its value to 1. The CPE shall initiate reauthentication before the MMP\_PN<sub>C</sub> expires, e.g., reaches the half of the counter space (0x7FFFFF). The AK Lifetime (see 8.3.1.1) shall not be set to a value less than the expected amount of time required to for the MMP\_PN to be exhausted. The CPE shall manage a separate MMP\_PN<sub>C</sub> counter for every active AK context. Specifically, during reauthentication, but before the activation of the new AK, the old MMP\_PN<sub>C</sub> (corresponding to the old AK) shall be used signing and/or encryption of MAC control messages, while the new MMP\_PN<sub>C</sub> shall be used for signing and/or encrypting of SCM Key Request messages. If CPE should lose its AK context, then CPE shall restart the authentication process.

The CPE may optionally check to see if the MMP\_PN<sub>C</sub> is synchronized by adding the “MMP\_PN” and “Ciphertext ICV” IEs (see 7.7.5) to the RNG-REQ. The “Ciphertext ICV” is calculated over the RNG-REQ message (excluding the MMP\_PN IE), according the process defined in 8.4.2.1.2. The MMP\_PN value that is sent in the IE shall be the MMP\_PN for the active AK context. If the MMP\_PN<sub>C</sub> does not match (see 8.2.4.6.1.2) MMP\_PN<sub>B</sub>, then the CPE shall be instructed reauthenticate by sending the RNG-CMD with Ranging Status set to “Reauthenticate”.

#### **8.2.4.6.1.2 Processing of MMP\_PN<sub>B</sub> by the BS**

The BS may possess one or more AK contexts associated with the CPE, each of which includes the value of MMP\_PN<sub>B</sub>. This value shall be maintained as specified in subsequent paragraphs of this subclause.

Upon successful completion of the SCM initial Authentication and Reauthentication, and establishment of a new AK context, the BS shall set MMP\_PN<sub>B</sub> of the corresponding newly instantiated AK context to 1. The BS shall manage a separate MMP\_PN<sub>B</sub> for every AK context it is maintaining. Specifically, during reauthentication, but before the activation of the new AK, the old MMP\_PN<sub>B</sub> (corresponding to the old AK context) shall be used for signing and/or encryption of MAC control messages, while the new MMP\_PN<sub>B</sub> shall be used for signing and/or encrypting of SCM Key Reply messages.

During periodic ranging, the CPE can optionally transmit the RNG-REQ containing the MMP\_PN parameter using the “MMP\_PN” and “Ciphertext ICV” (see 7.7.6). If this is done, the BS shall compare the received MMP\_PN value, which is MMP\_PN<sub>C</sub>, with MMP\_PN<sub>B</sub> (i.e., the value of MMP\_PN counter maintained by the BS for the corresponding AK context). If MMP\_PN<sub>C</sub> < MMP\_PN<sub>B</sub>, the BS shall process the message as being invalid and send a RNG-CMD message requesting the CPE to reauthenticate. This can happen when either the BS or CPE loses the AK context.

#### **8.2.4.6.2 Derivation of Management Message Protection (MMP) keys and KEKs**

MMP keys are used to encrypt and sign management messages in order to validate the authenticity of the messages as well as provide confidentiality for the contents of these messages.

There is a single key for US and DS messages.

The MMP\_KEY and KEK are derived as follows:

$$\text{MMP\_PREKEY} \mid \text{KEK} = \text{Dot22KDF(AK, CPE MAC Address} \mid \text{BSID} \mid \text{"MMP\_KEY+KEK", 256}$$

$$\text{MMP\_KEY} = \text{AES}_{\text{MMP\_PREKEY}}(\text{MMP\_PN})$$

For a fixed CPE, the MMP\_PN shall be set to 0 in the derivation of the MMP\_KEY at the BS and the CPE. Specifically, the preprocessed value of MMP\_PREKEY is treated as the Cipher Key of the Advanced Encryption Standard (AES) algorithm AES128 [FIPS197]. The MMP\_PN is treated as the Input Block Plain Text of this algorithm. The AES128 algorithm is executed once. The Output Block Cipher Text of

this algorithm is treated as the resulting MMP\_KEY. When MMP\_PN is used as an input of AES128 algorithm, 104 zero bits are pre-padded before the 24-bit MMP\_PN where the MMP\_PN is regarded as most-significant-bit first order.

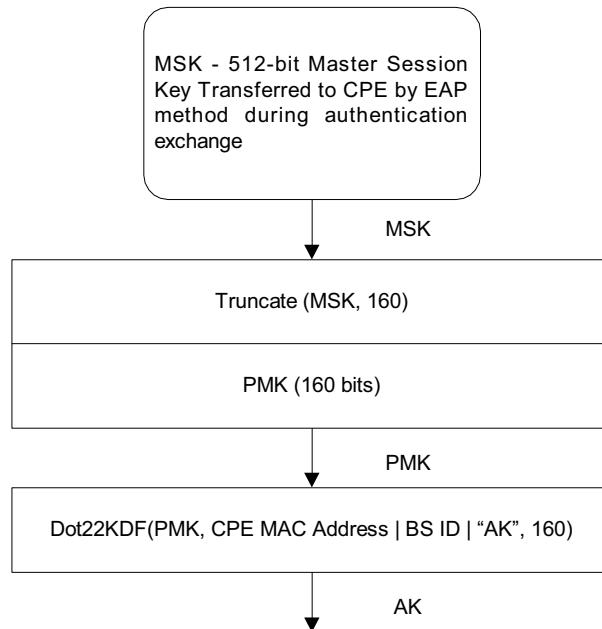
#### 8.2.4.7 Key Derivation function

The Dot22KDF algorithm is a CTR mode construction that may be used to derive an arbitrary amount of keying material from source keying material.

```
Dot22KDF(key, astring, keylength)
{
    result = null;
    Kin = Truncate (key, 128);
    for (i = 0; i < ceil((keylength-1)/128); i++) {
        result = result | AESKin(i | astring | keylength | result);
    }
    return Truncate (result, keylength);
}
```

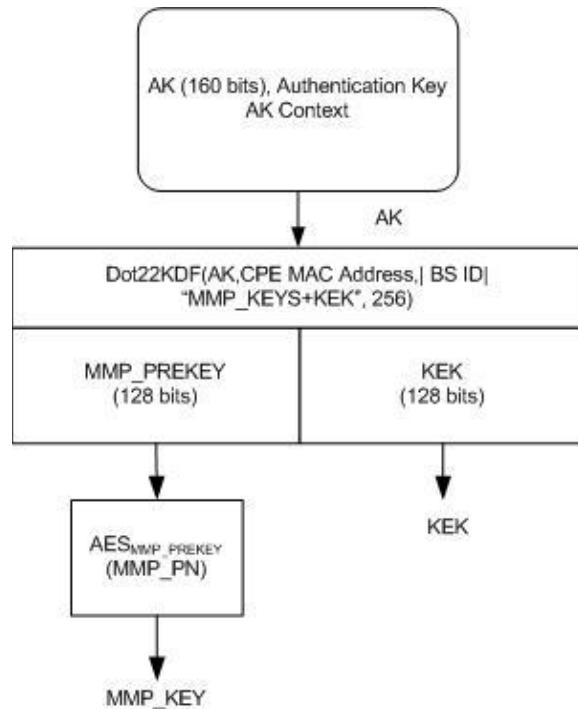
#### 8.2.5 Key hierarchy

Figure 116 outlines the process to calculate the AK when the EAP-based authentication process has taken place.



**Figure 116 — AK from PMK**

Figure 117 outlines the unicast key hierarchy starting from the AK.



**Figure 117 — MMP/KEK derivation from AK**

### 8.2.6 Maintenance of AK

The BS and CPE maintain cached PMK and AK as follows:

- 1) *PMK Maintenance:* Successful completion of the SCM EAP-based Authentication and establishment of a new PMK causes the activation of all the AK associated with the new PMK on the CPE. The Authenticator (e.g., AAA) shall delete the old PMK and any AKs that are associated with the old PMK for that CPE. During reauthentication, the procedures defined in 8.3 for switching AKs shall govern when the old PMK context is to be deleted.
- 2) *AK Maintenance:* If the packet counter belonging to MMP key reaches its maximum value, the associated AK becomes permanently deactivated. If protection of user traffic is not enabled (see 8.2.2.7 and 8.4.1), then new AK becomes active immediately after the old one expires. If protection of user transport traffic is enabled (see 8.2.2.7 and 8.4.1), then old AK and MMP\_Key shall be used to protect management messages, while the new AK (MMP\_Key and KEK derived from new AK) is used to complete the SCM Key-Request/Reply handshake for establishing keys for either the Primary or Secondary SA. Once the old AK expires, the MMP\_Key and KEK associated with the new AK are used for protection of subsequent management message and SCM Key-Request/Reply handshakes. The BS and CPE shall maintain the context of an AK (counters, timers, etc.) as long as they both retain the AK. The AK switching process is described in 8.3.

### 8.2.7 Security associations

Keying material is held within associations. There are three types of association: the security associations (SA) that maintain keying material for unicast connections; group security associations (GSA) that hold keying material for multicast groups; and the Null SA. If CPE and BS decide “No protection” as their only cryptographic suite, the Null SAID shall be used as the target SAID field in DSA-REQ/RSP messages.

### **8.2.7.1 Null security association**

The Null SA is the default SA that shall be established when the CPE enters the network. This security association contains keying material (e.g., MMP\_Key) that is used to protect unicast management connections. Unicast transport connections are mapped to this SA when the “No protection” cryptographic suite is selected for operation on the CPE. The contents of an SA are as follows:

- The SAID (a 16-bit identifier for the SA) = 0x0000. The SAID shall be unique within a BS.
- The KEK, a 128-bit key encryption key, derived from the AK.
- MMP Key, for encryption of US and DS management traffic
- MMP\_PN, 24 bit packet numbers for use by link cipher to protect US and DS management messages
- RxMMP\_PN, 24-bit receive sequence counter, for use by link cipher to protect US and DS management messages

### **8.2.7.2 Unicast security associations**

A security association contains keying material that is used to protect unicast connections. The contents of an SA are as follows:

- The SAID, a 16-bit identifier for the SA. The SAID shall be unique within a BS.
- Unicast SA type, either Primary or Secondary,
- TEK0 and TEK1, 128-bit traffic encryption keys, generated within the BS and transferred from the BS to the CPE using a secure key exchange.
- The TEK Lifetimes TEK0 and TEK1, a key aging lifetime value.
- PN0 and PN1, 24-bit packet numbers for use by the link cipher.
- RxPN0 and RxPN1, 24-bit receive sequence counter, for use by the link cipher.

### **8.2.7.3 Group security association**

The Group Security Association (GSA) contains keying material used to secure multicast transmissions. These are defined separately from SAs since GSA offer a lower security bound than unicast security associations, since keying material is shared between all members of the group, allowing any member of the group to forge traffic as if it came from any other member of the group.

The contents of a GSA are as follows:

- The SAID (GSAID), a 16-bit identifier for the GSA. The SAID shall be unique within the BS
- The Group Key Encryption Key (GKEK). Serves the same function as a KEK but for a GSA.
- The Group Traffic Encryption Key (GTEK). Served the same function as an SA TEK but for a GSA.
- GTEK0 and GTEK1, 128-bit traffic encryption keys.
- The GTEK Lifetimes for GTEK0 and GTEK1, a key aging lifetime value.
- GPN0 and GPN1, 24-bit packet numbers for use by the link cipher.
- RxGPN0 and RxGPN1, 24-bit receive sequence counter, for use by the link cipher.

## 8.2.8 Security context

The security context is a set of parameters linked to a key in each hierarchy that defines the scope while the key usage is considered to be secure. Examples of these parameters are key lifetime and counters ensuring the same encryption will not be used more than once. When the context of the key expires, a new key should be obtained to continue working.

The purpose of this subclause is to define the context that belongs to each key, how it is obtained and the scope of its usage.

The context described in 8.2.8.1 to 8.2.8.3, shall only be maintained if either one of two conditions are met. One, the BS and CPE have detected that they are no longer connected to each other. Two, the CPE detects that it has moved. If the CPE is being asked to shutdown or it is attempting affiliation with another BS, it shall stop any current state machines, remove any SAs, as well as delete any security context prior to affiliation with a new BS.

### 8.2.8.1 AK context

The AK key has two phases of lifetime: the first begins at AK creation and the second begins after validation by the SCM Key-Request/Reply handshake.

Hence, when the PKM is created, it is created with a specific lifetime.

If the (current) cached AK and associated context is lost either by the BS or the CPE, now new TEKs can be transported to the CPE using the KEK derived from that AK. Reauthentication shall be required to establish a new PKM, which allows for a new AK to be derived. From the AK, the MMP\_KEY and KEK are derived. The MMP\_KEY is used to protect management messages, while the KEK is to be used to transport new TEKs to the CPE.

The AK context is described in Table 190.

**Table 190 — AK Context in SCM**

Parameter	Size (bits)	Usage
AK	160	The authentication key, calculated as defined in 7.2.2.2.3.
AK Lifetime	32	This is the time this key is valid; it is calculated AK lifetime = PMK lifetime = Authentication Grace Time. When this expires, reauthentication is needed.
AK Sequence Number	4	The sequence number of the PMK from which this AK is derived.
KEK	128	Used to encrypt transport keys from the BS to the CPE.
MMP_KEY	128	The key which is used for signing and/or encrypting DS/US management messages.
MMP_PN	24	Used to avoid DS/US replay attack on management connection. When this expires reauthentication is needed.

### 8.2.8.2 GKEK context

The GKEK is the head of the group key hierarchy. There is a separate GKEK for each group (each GSA).

This key is randomly generated by the BS and transferred to the CPE encrypted with KEK. It is used to encrypt group TEKs (GTEK) when broadcasting them to all CPEs. The GKEK context is described in Table 191.

**Table 191 — GKEK context**

Parameter	Size (bits)	Usage
GKEK	128	Used to encrypt transport keys from the BS to the CPE.
GKEK Sequence Number	4	The sequence number of the GKEK. The new GKEK sequence number shall be one greater than the preceding GKEK sequence number.
GKEK Lifetime	32	This is the time this key is valid; prior to expiration a new GKEK should be obtained.
GTEK0	128	Older of two keys used to sign and/or encrypt multicast/broadcast management and data traffic messages.
GTEK1	128	Newer of two keys used to sign and/or encrypt multicast/broadcast management and data traffic messages.
GPN0	24	Packet number counter associate with older of two keys used to sign and/or encrypt multicast/broadcast management and data traffic messages. Used to avoid DS/US replay attack on multicast/broadcast connection. When this expires re-keying is needed.
GPN1	24	Packet number counter associate with older of two keys used to sign and/or encrypt multicast/broadcast management and data traffic messages. Used to avoid DS/US replay attack on multicast/broadcast connection. When this expires re-keying is needed.

### 8.2.8.3 PMK context

The PMK context includes all parameters associated with the PMK. This context is created when EAP-based Authentication completes.

The PMK context is described in Table 192.

**Table 192 — PMK Context**

Parameter	Size (bits)	Usage
PMK	160	A key yielded from EAP-based authentication
PMK Sequence Number	4	PMK sequence number, when the EAP-based authentication is achieved and a key is generated. The MSB 2 bits are the sequence counter, and the least significant bits are set to 0.

## 8.3 Key usage

### 8.3.1 BS key usage

The BS is responsible for maintaining keying information for all SAs. The SCM protocol defined in this specification describes a mechanism for synchronizing this keying information between a BS and its client CPE.

#### 8.3.1.1 AK lifetime

At initial network entry, if the security is enabled during the basic capabilities negotiation, the authentication procedure shall be initiated. The authentication procedure activates a new AK. This AK shall remain active until it expires according to its predefined *Authentication Grace Time*, a BS system

configuration parameter. In SCM, AK lifetime is determined the PAK lifetime or by the expiration of the MMP\_PN.

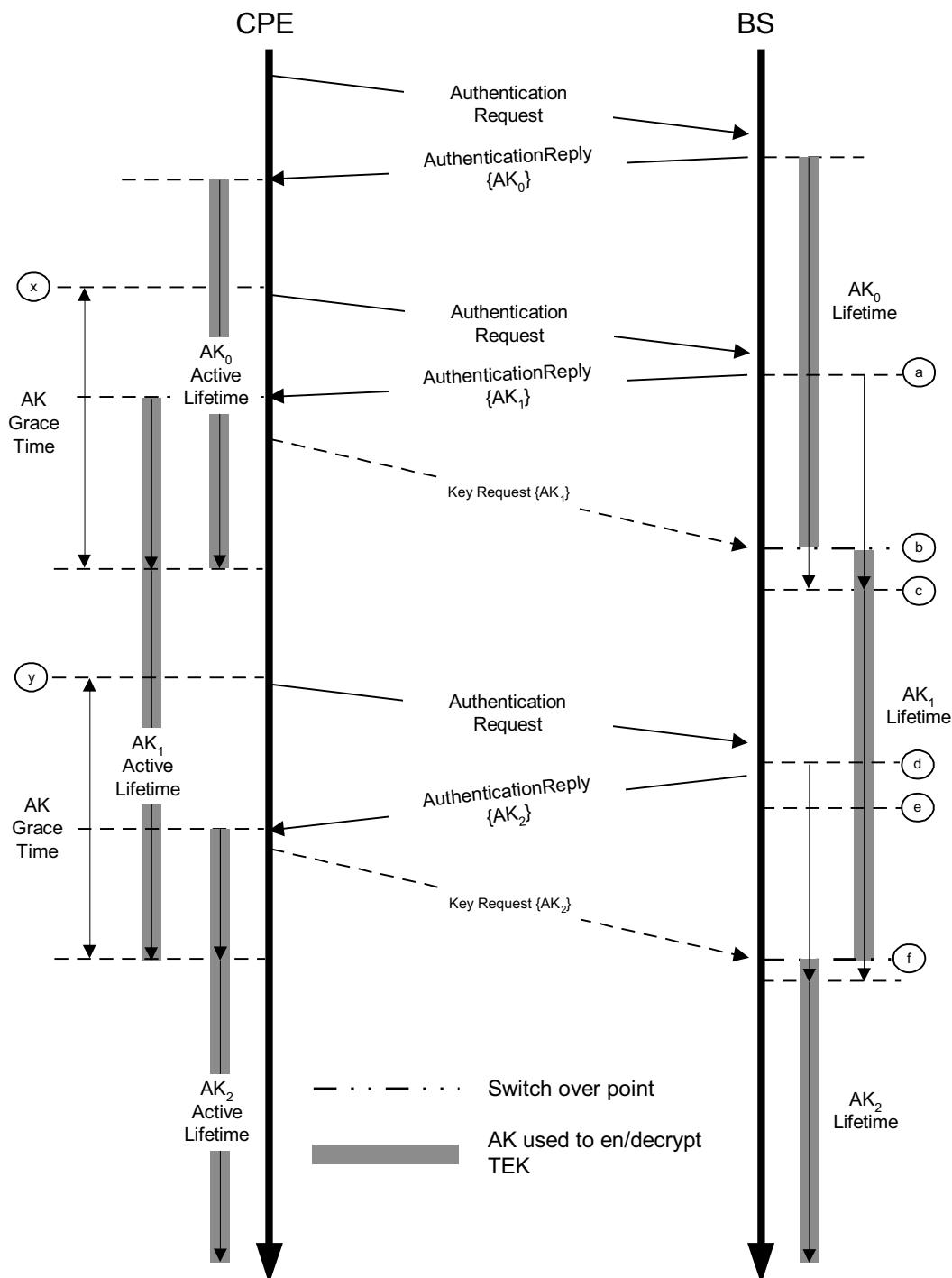
A CPE will initiate reauthentication before the expiration of its current AK. This leads the CPE to have two active sets of keying material. If a CPE fails to reauthenticate before the expiration of its current AK, the BS shall hold no active AKs for the CPE and shall consider the CPE *unauthenticated*. A BS shall remove from its keying tables all TEKs associated with an unauthenticated CPEs SA.

### 8.3.1.2 AK transition period on BS

The BS shall always be prepared to start reauthentication upon request. The BS shall be able to support two simultaneously active AKs for each client CPE. The BS has two active AKs during an AK transition period; the two active keys have overlapping lifetimes.

In SCM, an AK transition period begins when the BS receives an SCM EAP-Transfer or EAP-Start message from a CPE to start reauthentication and the BS has a single active AK for that CPE. In response to this request for reauthentication, the BS activates a second AK [see point (a) and (d) in Figure 118], which shall have a key sequence number one greater (modulo 16) than that of the existing AK and shall be sent back to the requesting CPE in an SCM EAP-Transfer message during reauthentication. The BS shall set the active lifetime of this second AK to be the remaining lifetime of the first AK [between points (a) and (c) in Figure 118], plus the predefined *AK Lifetime*; thus, the second, “newer” key shall remain active for one *AK Lifetime* beyond the expiration of the first, “older” key.

As long as the BS is in the midst of a CPE AK transition period, and thus is holding two active AKs for that CPE, it shall respond to the SCM EAP-Transfer messages with the newer of the two active keys. Once the older key expires, an SCM EAP-Transfer transmission sent to start reauthentication shall trigger the activation of a new AK, and the start of a new key transition period indicated at point (b) in Figure 118.



**Figure 118 — AK management in BS and CPE**

#### 8.3.1.3 BS usage of AK

The BS shall make use of keys derived from the CPE's AK for the following purposes:

- a) Verify MAC-Digests and decrypt (see 8.4) of SCM Key Request messages as well as all other non-SCM related management messages received from CPE
- b) Calculate MAC-Digests and encrypt (see 8.4) for SCM Key Reply messages as well as other non-SCM related management messages sent to CPE
- c) Encrypting TEK when it is sent to CPE in the Key Reply message

The MMP\_KEY is used to verify MAC Digests and decrypt (see 8.4) of SCM Key Request messages as well as other non-SCM related management messages received from CPE. The PN used in this operation is MMP\_PN (see 8.2.4.6.1.2). When a CPE issues an SCM Key Request message, it shall include the AK Sequence Number, to indicate that it is using the newer of the two AKs that it is assigned.

The MMP\_KEY is used to verify MAC Digests and decrypt (see 8.4) of SCM Key Reply messages as well as other non-SCM related management messages sent to the CPE. The PN used in this operation is MMP\_PN (see 8.2.4.6.1.1). If the BS has been informed by the CPE that the Key Request issued by the CPE was issued with the newer AK, then BS shall use the MMP\_KEY derived from the new AK and initialize MMP\_PN associated with the new AK to 0. If the BS has no knowledge that the CPE is using the new AK, then it will use the MMP\_KEY derived from the old AK and use the current value of MMP\_PN associated with the older AK. The CPE indicates which AK is being used by including the AK Sequence Number of that AK in the Key Request message.

Prior to expiration of the MMP\_PN, when half the key space ( $2^{23}$ ) has been used up, the CPE conduct reauthentication.

#### **8.3.1.4 TEK/GTEK lifetime**

The BS maintains two, active TEKs per SA or GTEKs per GSA. Both TEKs/GTEKs will have overlapping lifetimes. *TEK/GTEK Lifetime* is a system parameter that determines the length of time for which the TEK/GTEK is valid. *TEK/GTEK Lifetime* is only invalidated when the PN associated with that TEK is about to expire. The *TEK/GTEK Lifetime* is communicated to the CPE, along with both generations of TEKs, from the BS in the SCM Key Reply message.

In the generic MAC header (GMH), the usage of the newer TEK/GTEK is indicated in the value of the EKS field. For the newer TEK/GTEK, the EKS field is 1 greater (modulo 4) than that of the older TEK/GTEK.

#### **8.3.1.5 BS usage of TEK and GTEK**

Two generations of TEKs shall be maintained per SA, and two generations of GTEKs shall be maintained per GSA. Transitioning between both generations of TEKs/GTEKs and how they are used are dependent on whether or not the TEK/GTEK is used for DS or US traffic.

The BS transitions from using the older generation to the newer generation (for each of its SAs) based on the following rules:

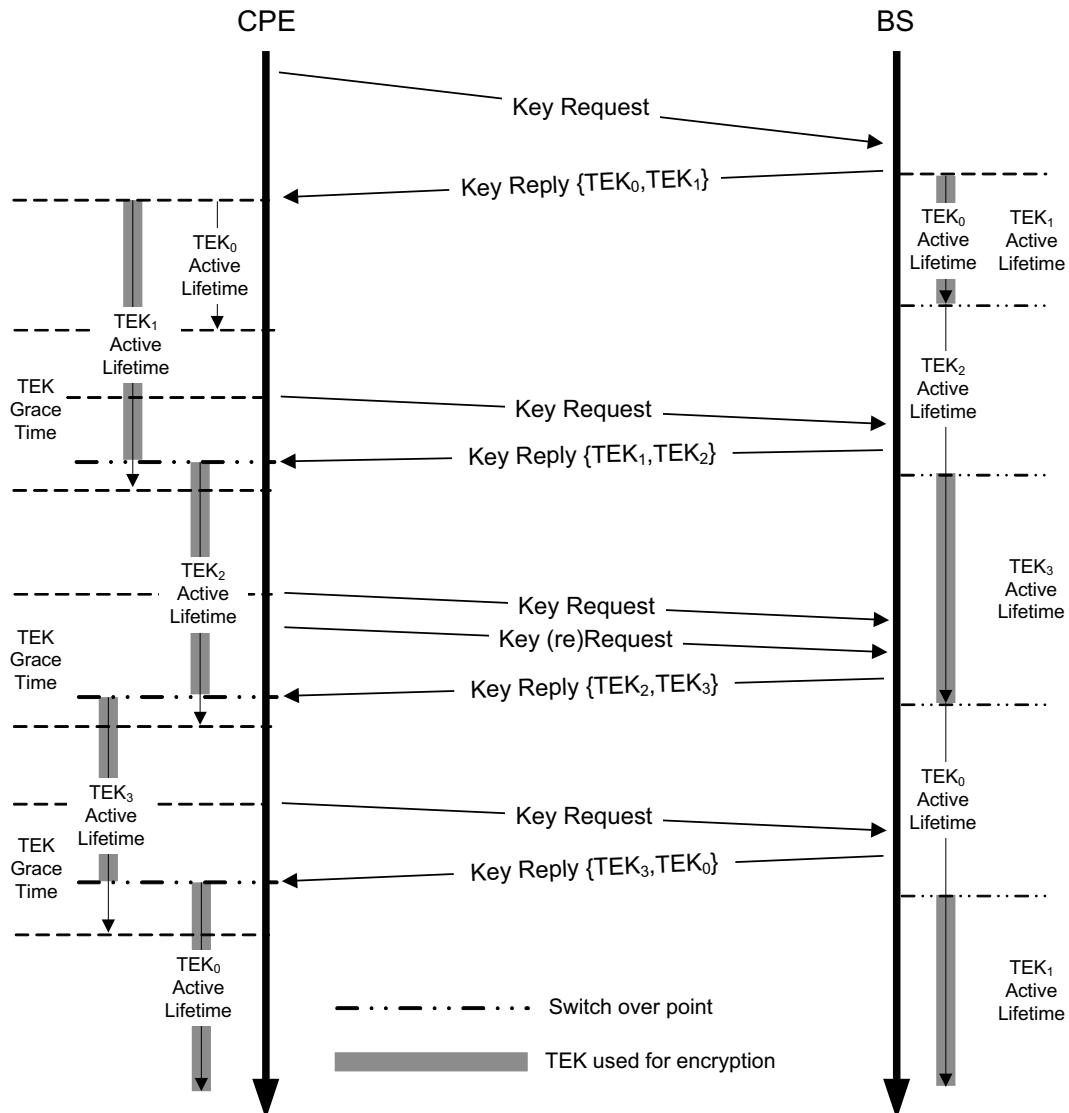
- a) At the expiration of the older TEK/GTEK, the BS shall immediately transition to using the newer TEK/GTEK for encryption.
- b) The transitional period for the encrypting US traffic begins when the BS issues the newer TEK/GTEK to the CPE in the SCM Key Reply message and concludes that the older TEK/GTEK has expired (i.e., its PN has expired).

The BS makes use of both generations of TEKs/GTEKs, based on the following rules:

- a) BS shall use the older TEK/GTEK for encrypting DS traffic.
- b) BS shall be able to decrypt US traffic using either of the two TEK.

It is the responsibility of the CPE to update its keys in a timely fashion; the BS shall transition to a new DS encryption key regardless of whether a client CPE has retrieved a copy of that TEK/GTEK.

Note that the BS encrypts with a given TEK/GTEK for only the second half of that TEK's total lifetime (see Figure 119). The BS is able, however, to decrypt with a TEK/GTEK for the TEKs/GTEKs entire lifetime.



**Figure 119 — TEK Management in BS and CPE**

### 8.3.2 CPE Key Usage

CPEs shall maintain an active AK and stay authenticated with the BS. This requires the CPE to initiate reauthentication periodically. Upon completing authentication and reauthentication, the CPE shall also be responsible for maintaining active keying material (e.g., TEKs) for encrypting DS and US traffic.

#### 8.3.2.1 CPE reauthentication

AKs have a limited lifetime and shall be periodically refreshed. The Authentication state machine (see Figure 114) manages the scheduling of reauthentication attempts for refreshing AKs. In SCM EAP-based authentication, the CPE refreshes its AK by issuing a SCM EAP-Request message.

In SCM, a CPE's Authentication state machine schedules the beginning of reauthentication a configurable duration of time, the *Authentication Grace Time*, [see points (x) and (y) in Figure 118], before the CPE's latest AK is scheduled to expire. The *Authentication Grace Time* is configured to provide a CPE with an authentication retry period that is sufficiently long to allow for system delays and provide adequate time for the CPE to successfully complete an Authentication exchange before the expiration of its most current AK. The *Authentication Grace Time* should be set at a value that does not expire for the MMP\_PN expires.

Note that the BS does not require knowledge of the *Authentication Grace Time*. The BS, however, shall track the lifetimes of its AKs and shall deactivate a key once it has expired.

#### 8.3.2.2 CPE usage of AK

A CPE shall use the MMP\_KEY/KEK derived from the newer of the two AKs it has when calculating MAC Digests and encryption of SCM Key Request, and other SCM-related messages. A CPE shall use the MMP\_KEY derived from the older of the two AKs to protect non-SCM related management messages that are transmitted to the BS.

The CPE shall be capable of using the MMP\_KEY/KEK derived from the newer one of its AKs to verify and decrypt SCM Key Reply, SCM TEK Invalid, as well as other SCM-related messages. A CPE shall use the MMP\_KEY derived from the older of the two AKs to protect non-SCM related management messages that are received from the BS.

#### 8.3.2.3 CPE usage of TEK and GTEK

Through operation of its TEK state machines, a CPE shall maintain two, successive sets of keying material for encrypting traffic per SA. The CPE schedules requests for a new set of traffic keying material, based a configurable amount of time, the *TEK/GTEK Lifetime* [see points (x) and (y) in Figure 118], before the CPE's latest TEK is scheduled to expire.

For each SA for which the CPE is configured, the CPE

- Shall use the newer of its two TEKs to encrypt US traffic
- Shall be able to decrypt DS traffic encrypted with either of the TEKs.

The left-hand side of Figure 118 illustrates the CPE's maintenance and usage of an SA's TEK, where the shaded portion of a TEK's lifetime indicates the time period during which that TEK shall be used to encrypt MAC PDU payloads.

GTEKs shall be treated in the same manner as TEKs, with regard to how they are managed (see Figure 118).

## 8.4 Cryptographic methods

This subclause specifies the cryptographic algorithms and key sizes used by the SCM protocol. All CPE and BS implementations shall support the method of packet data encryption and authentication defined in 8.4.2, using the cryptographic suites specified in 8.4.1.

All inputs to key derivation and other supporting functions shall be byte aligned. Furthermore, each byte shall be in canonical form as defined in IEEE Std 802-2001 where the leftmost bit in each byte is the most significant bit and the rightmost bit is the least significant bit.

### 8.4.1 Selection of Data Encryption and Authentication methods

Only one Data Encryption and Authentication algorithm is supported in IEEE 802.22, AES in GCM mode, therefore no specific configuration item is required to define the use of AES GCM. The parameters in Table 272) are associated with how AES GCM is to be applied in order to provide authentication and/or encryption for MAC PDU payloads. The cryptographic suite configuration is made up of selecting an Authentication method, and Encryption method, and a TEK Encryption method. Cryptographic suite configuration is negotiated during initial and reauthentication via the exchange of SCM EAP-Transfer messages (see 8.2.2.7).

Possible values for Authentication method are as follows:

- No Authentication
- Authentication for Unicast
- Authentication for Multicast

Possible values for Encryption method are as follows:

- No Encryption
- Encryption for Unicast
- Encryption for Multicast/Broadcast

Possible values for TEK/GTEK Encryption Method are as follows:

- AES-128 key wrap of TEK/GTEK using KEK/GKEK (IETF RFC 5649)

The cryptographic suite list is defined in Table 193 is a 1-byte construct defined in the following table:

**Table 193 — Cryptographic suite**

Value	Cryptographic suite
0x00	No Protection (No Authentication, No Encryption)
0x01	Authentication only for Unicast, AES-128 key wrap of TEK using KEK
0x02	Authentication and Encryption for Unicast, AES-128 key wrap of TEK using KEK
0x03	Authentication only for Multicast, AES-128 key wrap of GTEK with GKEK
0x04	Authentication and Encryption for Multicast, AES-128 key wrap of GTEK with GKEK
0x05	Encryption only for Unicast, AES-128 key wrap of TEK using KEK
0x06	BS random generation of GKEK and GTEK
0x07	Operator-specific function for GKEK and GTEK generation
0x08–0xFF	<i>Reserved</i>

In Table 272, a configuration parameter for the list of Cryptographic Suites supported will be transmitted to the AAA through the BS by the CPE in the SCM EAP-Start and/or EAP-Transfer messages.

## **8.4.2 Data Encryption and Authentication with AES GCM**

For all cryptographic suites (see Table 193) selected for operation during the Authentication, AES in GCM (NIST Special Publication 800-38D and FIPS 197) mode is used to provide authentication and/or encryption of MAC PDUs.

### **8.4.2.1 PDU format**

#### **8.4.2.1.1 Packet number**

The MAC PDU payload shall be prefixed with a 3-byte PN (Packet Number). The PN shall be encoded in the MAC PDU least significant byte first. The PN shall not be encrypted.

The PN associated with an SA shall be set to 1 when the SA is established and when a new TEK is installed. Upon completion of initial authentication or reauthentication and after the MMP\_KEY has been derived has been derived, the MMP\_PN is set to 1. After each PDU transmission, the PN and MMP\_PN shall be incremented by 1.

When admitting a CPE to an existing multicast/broadcast group, the BS will take the current value of the PN related to the newest generation of material for that GSA, and increment by 1 when establishing. The maximum number of CPEs that can be admitted to a multicast/broadcast group simultaneously is one half the PN\_WINDOW\_SIZE (see 8.4.2.3).

On DS connections, the PN shall be XORed with 0x800000 prior to encryption and transmission. This effectively splits the PN space into two ranges for DS (0x000000–0x7FFFFF) and DU (0x800001–0xFFFFFFF); thereby avoiding collision of PN values when using a single PN for DS and DU. On DS connections, the PN shall be used without such modification.

Any tuple value of {PN, KEY} shall not be used more than once for the purposes of transmitting data. This measure is known a protection against replay attacks.

A new TEK shall be requested and transferred before the PN on either the CPE or BS reaches 0x7FFFFFFF. If the PN in either the CPE or BS reaches 0x7FFFFFFF without new keys being installed, transport communications on that SA shall be halted until new TEKs are installed. In the case of the MMP\_KEY, if MMP\_PN expires, then current AK is invalidated and shall start Reauthentication.

#### **8.4.2.1.2 PDU format—Authentication only**

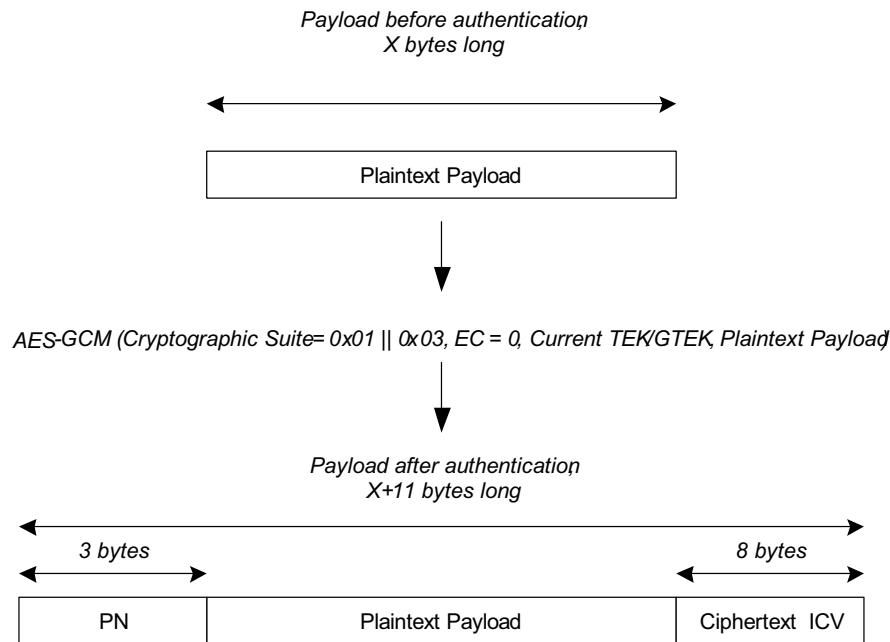
The ciphersuites allow for authentication and/or encryption of MAC PDUs. If suites 0x01 or 0x03 is assigned to the SA, then only authentication is provided for any MAC PDUs transmitted on service flows that are mapped to these SAs.

The AES in GCM protocol is applied in the following manner:

- 1) The Plaintext Payload is processed, generating an Integrity Check Value (ICV) that is 8 bytes long.
- 2) Only the ICV is encrypted using the active TEK/GTEK, generating the Ciphertext ICV.
- 3) The Authenticated PDU is formed by appending the Ciphertext ICV to the Plaintext Payload form the authenticated PDU.

This requires the EC bit in the GMH to be set to 0. If EC bit is not set to 0, the PDU shall be discarded, as this would indicate a conflict between the configured cryptographic suite and how it is being applied.

Figure 119 illustrates how MAC PDUs are processed and formatted when suite 0x01 or 0x03 is configured and the EC bit in GMH is set to 0. The Ciphertext ICV is transmitted so that byte index 0 (as enumerated in NIST Special Publication 800-38D) is transmitted first and byte index 7 is transmitted last (i.e., LSB first).



**Figure 120 — Authentication-only PDU format**

#### 8.4.2.1.3 PDU format—Authentication and encryption

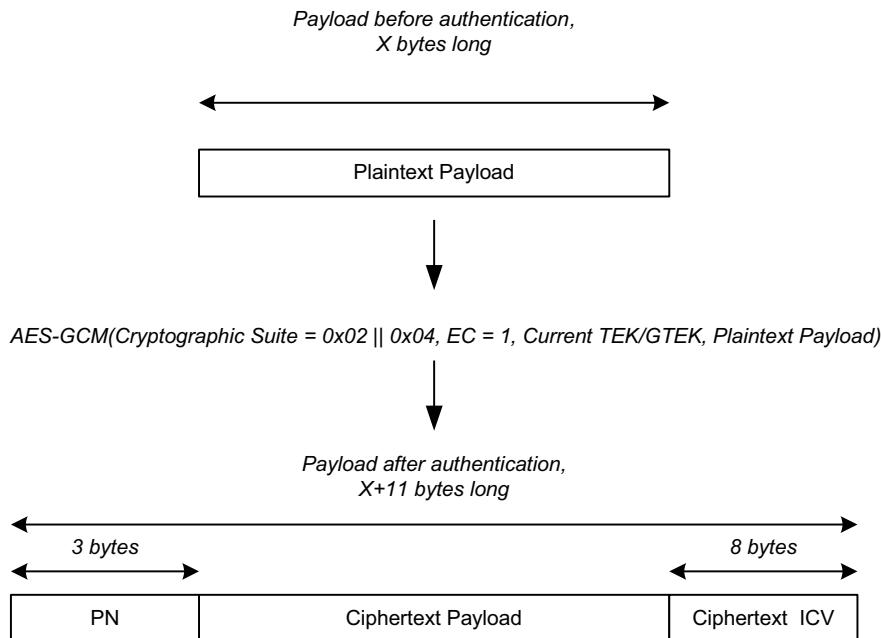
The ciphersuites allow for authentication and/or encryption of MAC PDUs. If the suites 0x02 or 0x04 is assigned to the SA, then authentication and encryption is provided for any MAC PDUs transmitted on service flows that are mapped to these SAs.

The AES in GCM protocol is applied in the following manner:

- 1) The Plaintext Payload is processed, generating an Integrity Check Value (ICV) that is 8 bytes long.
- 2) Then the ICV is encrypted using the active TEK/GTEK, generating the Ciphertext ICV.
- 3) Then the Plaintext Payload is then encrypted with AES using the active TEK/GTEK, generating a Ciphertext Payload.
- 4) The encrypted PDU is formed by appending the Ciphertext ICV to the Ciphertext Payload.

This requires the EC bit in the GMH to be set to 1. If EC bit is not set to 1, the PDU shall be discarded, as this would indicate a conflict between the configured cryptographic suite and how it is being applied.

Figure 120 illustrates how MAC PDUs are processed and formatted when suite 0x02 or 0x04 is configured and the EC bit in GMH is set to 1. The Ciphertext ICV is transmitted so that byte index 0 (as enumerated in NIST Special Publication 800-38D) is transmitted first and byte index 7 is transmitted last (i.e., LSB first).



**Figure 121 — Authenticated + encrypted PDU format**

#### 8.4.2.1.4 PDU format—Encryption only

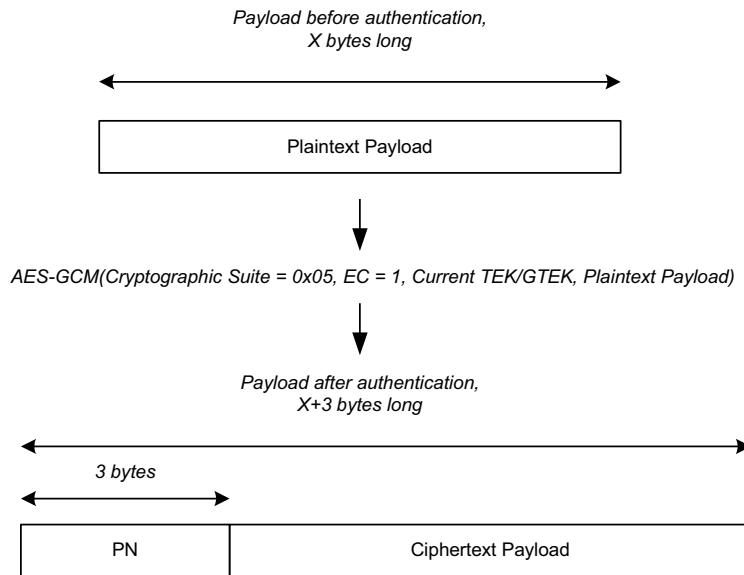
If the 0x05 ciphersuite is assigned to an SA, then MAC PDUs associated with service flows mapped to this SA shall only be protected by encryption and no other cipher suites can be mapped to this SA.

The AES in GCM protocol is applied in the following manner:

- 1) Processing of the Plaintext Payload is processed, generating the Integrity Check Value (ICV), and encrypting the ICV to generate the Ciphertext ICV is skipped.
- 2) Then the Plaintext Payload is then encrypted with AES using the active TEK/GTEK, generating a Ciphertext Payload.
- 3) The encrypted PDU is formed from the Ciphertext Payload.

This requires the EC bit in the GMH to be set to 1. If the EC bit is not set to 1, the PDU shall be discarded, as this would indicate a conflict between the configured cryptographic suite and how it is being applied.

Figure 122 illustrates how MAC PDUs are processed and formatted when suite 0x05 is configured and the EC bit in GMH is set to 1.



**Figure 122 — Encryption-only PDU format**

#### 8.4.2.2 GCM algorithm constraints

The GCM specification (NIST SP 800-38D) defines specific values for several parameters.

The additional authenticated data (AAD) to be used in the GCM process shall be the GMH.

$T$  represents the ICV (otherwise known as Message Authentication Code, MAC). This value, as stated in 8.4.2.1, shall be 64 bits (8 octets) long.

Consistent with the GCM specification, the  $IV$  or Initialization Vector is used to initialize the Authenticated Encryption function of GCM. The  $IV$  shall be 128 bits (16 octets) long and shall be constructed according to the procedure defined Section 8.2.1 of NIST Special Publication 800-38D. The  $IV$  is described in Figure 123.

The  $IV$  shall be 15 bytes long as shown in Figure 123. Bytes 0 through 3 shall be set to the first 4 bytes of the generic MAC header (thus excluding the HCS). The HCS of the generic MAC header is not included in the  $IV$  since it is redundant. Bytes 4 through 12 are reserved and shall be set to 0x0000000000000000. Bytes 13 through 15 shall be set to the value of the PN. The PN bytes shall be ordered so that byte 13 shall take the least significant byte and byte 15 shall take the most significant byte.

Field	Fixed Field				Invocation Field	
Byte	0	3	4	12	13	15
Data	GMH	<i>Reserved</i>			PN	
Contents	GMH (without HCS)	0x0000000000000000			PN field from Payload	

**Figure 123 — IV construction**

Consistent with the GCM specification, pre-counter block  $J_0$  is generated using the equations defined in Section 7 of NIST Special Publication 800-38D.

Consistent with the NIST GCM specification, the counter blocks  $CB_j$  are formatted as shown in Section 6.5 of NIST Special Publication 800-38D.

#### 8.4.2.3 Receive processing rules

On receipt of a PDU the receiving CPE or BS shall decrypt and authenticate the PDU consistent with the NIST GCM specification configured as specified in 8.4.2.2.

Packets that are found to be not authentic shall be discarded.

Receiving BS or CPEs shall maintain a record of the highest value PN and MMP\_PN received for each SA. The receiver shall maintain a PN window whose size is specified by the PN\_WINDOW\_SIZE parameter for SAs and management connections as defined in Table 272.

Any received PDU with a PN lower than the beginning of the PN window shall be discarded as a replay attempt. The receiver shall track PNs within the PN window. Any PN that is received more than once shall be discarded as a replay attempt. Upon reception of a PN, which is greater than the end of the PN window, the PN window shall be advanced to cover this PN.

#### 8.4.3 Requirements for EAP-TLS/TTLS

IEEE 802.22 devices shall use EAP-TLS or EAP-TTLS to support device authentication. The IEEE 802.22 BSs shall use EAP-based techniques for the authentication of the database service. Implementation of authentication services (e.g., key agreement and digital signature processed) based on EAP-TLS or EAP-TTLS shall conform to the specifications as defined in the following IETF RFCs:

- IETF RFC 5246
- IETF RFC 5216
- IETF RFC 5281
- IETF RFC 4492

Note that implementation of IETF RFC 5246 may include updates/extension to TLS as defined in IETF RFC 5746 [B39] and IETF RFC 5878 [B42].

### 8.5 Certificate profile

This standard mandates use of EAP-TLS or EAP-TTLS as the authentication mechanism. The certificate profile defined in this subclause provides a description of the credentials to be used for device authentication of IEEE 802.22 networks. This certificate profile is also used to develop credentials for database service access.

#### 8.5.1 Certificate format

This subclause describes the X.509 Version 3 certificate format and certificate extensions used in IEEE 802.22-compliant CPEs. The X.509 Version 3 format is defined in IETF RFC 2459. ASN.1 encoding of algorithm identifiers are also further described in IETF RFC 3279 (as updated by RFC 4055 [B34], RFC 5480 [B38], 5756 [B40], and RFC 5758 [B41]) and IETF RFC 5280. The basic X.509 Version 3 certificate format is retained from the reference system. Table 194 highlights the fields of an X.509v3 certificate.

**Table 194 — Fields of X.509 Version 3 Certificate**

<b>X.509 Version 3 Field</b>	<b>Description</b>
tbsCertificate.version	Indicates X.509 certificate version. Always set to 3.
tbsCertificate.serialNumber	Unique integer the issuing CA assigns to the certificate.
tbsCertificate.signature	Object identifier (OID) and optional parameters defining algorithm used to sign the certificate. This field shall contain the same algorithm identifier as the signatureAlgorithm field.
tbsCertificate.issuer	Distinguished Name of the CA that issued the certificate.
tbsCertificate.validity	Specifies when the certificate becomes active and when it expires.
tbsCertificate.subject	Distinguished Name identifying the entity whose public key is certified in the subject public key information field.
tbsCertificate.subjectPublicKeyInfo	Field contains the public key material (public key and parameters) and the identifier of the algorithm with which the key is used.
tbsCertificate.issuerUniqueID	Optional field to allow reuse of issuer names over time.
tbsCertificate.subjectUnique ID	Optional field to allow reuse of subject names over time.
tbsCertificate.extensions	The extension data.
signatureAlgorithm	OID and optional parameters defining algorithm used to sign the certificate. This field shall contain the same algorithm identifier as the signature field in tbsCertificate.
signatureValue	Digital signature computed upon the ASN.1 DER encoded tbsCertificate.

All certificates described in this specification shall be based on RSA or ECC. With RSA, the RSA signature algorithm SHA-256 is used as the one-way hash function. The RSA signature algorithm is described in PKCS #1 (IETF RFC 2437); SHA-256 is described in FIPS 180-3.

For ECC certificates elliptic curve domain parameters can be generated according to procedures defined in Section A.3 of ANSI X9.62-2005. Example parameters sets of parameters can be found in FIPS 186-3 and ANSI X9.63-2001.

#### **8.5.1.1 tbsCertificate.validity.notBefore and tbsCertificate.validity.notAfter**

CPE certificates shall not be renewable and shall thus have a validity period greater than the operational lifetime of the CPE. A Manufacturer/Service Provider CA certificate's validity period should exceed that of the CPE certificates it issues. The validity period of a CPE certificate shall begin with the date of generation of the device's certificate; the validity period should extend out to at least 10 years after that manufacturing date. Validity periods shall be encoded as UTC Time. UTC Time values shall be expressed Greenwich Mean Time (Zulu) and shall include seconds (i.e., times are YYMMDDHHMMSSZ), even where the number of seconds is zero.

#### **8.5.1.2 tbsCertificate.serialNumber**

Serial numbers for CPE certificates signed by a particular issuer shall be assigned by the manufacturer in increasing order. Thus, if the tbsCertificate.validity.notBefore field of one certificate is greater than the tbsCertificate.validity.notBefore field of another certificate, then the serial number of the first certificate shall be greater than the serial number of the second certificate.

#### **8.5.1.3 tbsCertificate.signature and signatureAlgorithm**

Certificates can be signed with the RSA or ECDSA (ANSI X9.62-2005) algorithms. ECDSA is the elliptic curve analog of the DSA signature algorithm. The following two subclauses define OIDs that represent values for tbsCertificate.signature and signatureAlgorithm fields of the X.509v3 certificate to describe each algorithm.

#### **8.5.1.3.1 RSA signature & signatureAlgorithm**

The RSA signature algorithm (PKCS #1, IETF RFC 2437), which makes use of SHA-256 is described in FIPS 180-3) as the one-way hash algorithm. The ASN.1 OID used to describe the RSA signature algorithm using SHA-256 is as follows:

```
sha-256WithRSAEncryption OBJECT IDENTIFIER ::= {  

    iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
```

The calculation and encoding of the signature value is described in PKCS #1 (IETF RFC 2313) specification. The signature value is calculated over the rest of ASN.1 encoded certificate, then inserted in the signatureValue field of the certificate.

#### **8.5.1.3.2 ECC signature & signatureAlgorithm**

ECDSA itself is identified by OIDs arranged in the following manner:

```
ansi-X9-62 OBJECT IDENTIFIER ::= {  

    iso(1) member-body(2) us(840) 10045 }
```

```
id-ecSigType OBJECT IDENTIFIER ::= {  

    ansi-X9-62 signatures(4) }
```

ECDSA also uses SHA-256 as the one-way hash function. The ASN.1 OID used to describe the ECDSA signature algorithm using SHA-256 is as follows:

```
ecdsa-with-SHA-256 OBJECT IDENTIFIER ::= { iso(1) member-body(2)  

    us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1  

    }
```

The calculation and encoding of the signature value is described in ANSI X9.62-2005. This process outputs two values (*r* and *s*). The signature value is calculated over the rest of ASN.1 encoded certificate, then inserted in the signatureValue field of the certificate using the following ASN.1 encoded data structure:

```
Ecdsa-Sig-Value ::= SEQUENCE {  

    r INTEGER,  

    s INTEGER }
```

When the ephemeral public key  $R:=(x_1,y_1):=kG$  that is generated during the ECDSA signature generation algorithm has an odd valued “y-” coordinate “ $y_1$ ,” the ECDSA signature component “*s*” SHALL be changed towards the integer “-*s*” (modulo *n*), where “*n*” is the prime order of the cyclic subgroup of the elliptic curve in question. Note that this extra post-processing step can be executed by any party and that using accelerated methods for signature verification is (of course) entirely optional.

#### **8.5.1.4 tbsCertificate.issuer and tbsCertificate.subject**

X.509 Names are SEQUENCES of RelativeDistinguishedNames, which are in turn SETs of AttributeTypeAndValue. AttributeTypeAndValue is a SEQUENCE of an AttributeType (an OBJECT IDENTIFIER) and an AttributeValue. The value of the countryName attribute shall be a two-character PrintableString, chosen from ISO 3166 [B44]; all other AttributeValues shall be encoded as either T.61/TeletexString or PrintableString character strings. The PrintableString encoding shall be used if the character string contains only characters from the PrintableString set. Specifically:

```
abcdefghijklmnopqrstuvwxyz  

ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

0123456789  
'()+,.-/:=? and space

The T.61/TeletexString shall be used if the character string contains other characters. The following OIDs are needed for defining issuer and subject Names in SCM certificates:

```
id-at OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) ds(5) 4}
id-at-commonName OBJECT IDENTIFIER ::= {id-at 3}
id-at-countryName OBJECT IDENTIFIER ::= {id-at 6}
id-at-localityName OBJECT IDENTIFIER ::= {id-at 7}
id-at-stateOrProvinceName OBJECT IDENTIFIER ::= {id-at 8}
id-at-organizationName OBJECT IDENTIFIER ::= {id-at 10}
id-at-organizationalUnitName OBJECT IDENTIFIER ::= {id-at 11}
```

The following subclauses describe the attributes that comprise the subject Name forms for each type of SCM certificate. Note that the issuer name form is the same as the subject of the issuing certificate. Additional attribute values that are present but unspecified in the following forms should not cause a device to reject the certificate.

#### **8.5.1.4.1 Manufacturer/ServiceProvider certificate**

```
countryName=<Country of Manufacturer/ServiceProvider>
[stateOrProvinceName=<state/province>]
[localityName=<City>]
organizationName=<Company Name>
organizationalUnitName=WirelessRAN
[organizationalUnitName=<Manufacturing Location>]
commonName=<Company Name> <Certification Authority>
```

The countryName, organizationName, and commonName attributes shall be included and shall have the values shown. The organizationalUnitName having the value “WirelessRAN” shall be included. The organizationalUnitName representing manufacturing location should be included. If included, it shall be preceded by the organizationalUnitName having value “WirelessRAN.” The stateOrProvinceName and localityName may be included. Other attributes are not allowed and shall not be included.

#### **8.5.1.4.2 CPE certificate**

```
countryName=<Country of Manufacturer/ServiceProvider>
organizationName=<Company Name>
organizationalUnitName=<manufacturing location>
commonName=<MAC Address>
commonName=<Device Id>
commonName=<Serial Number>
```

The “Device Id” and “Serial Number” shall be formatted as alpha-numeric strings with 17 and 12 characters respectively.

The MAC address shall be the CPE’s MAC address. It is expressed as six pairs of hexadecimal digits 20 separated by colons (:), e.g., “C4:2C:03:32:B2:A1”. The Alpha HEX characters (A–F) shall be expressed as 21 uppercase letters.

The organizationalUnitName in a CPE certificate, which describes the modem’s manufacturing location, should be the same as the organizationalUnitName in the issuer Name describing a manufacturing location.

The countryName, organizationName, organizationalUnitName, and commonName attributes shall be included. Other attributes are not allowed and shall not be included.

#### **8.5.1.4.3 BS certificate**

```
countryName=<Country of Operation>
organizationName=< Name of Infrastructure Operator>
organizationalUnitName=<WirelessRAN>
commonName=<MAC Address>
commonName=<Serial Number>
commonName=<FCC Id>
```

The “Serial Number” and “FCC Id” shall be formatted as alpha-numeric strings.

The MAC address shall be the BS's MAC address. It is expressed as six pairs of hexadecimal digits 20 separated by colons (:), e.g., “C4:2C:03:32:B2:A1.” The Alpha HEX characters (A–F) shall be expressed as 21 uppercase letters.

#### **8.5.1.5 tbsCertificate.subjectPublicKeyInfo**

The tbsCertificate.subjectPublicKeyInfo field contains the public key and the public key algorithm identifier. The following two subclauses describe OIDs used to encode this information for RSA public keys (8.5.1.5.1) and ECDSA/ECDH public keys (8.5.1.5.2).

##### **8.5.1.5.1 RSA public keys**

The OID that identify RSA encryption for a certificate are defined as follows:

```
pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
                                rsadsi(113549) pkcs(1) 1 }
```

```
rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1 }
```

The OID that identifies RSA public keys in a certificate is defined as follows:

```
RSA PublicKey ::= SEQUENCE {
    modulus      INTEGER, -- n
    publicExponent  INTEGER } -- e
```

##### **8.5.1.5.2 ECDSA/ECDH public keys**

ECDH (ANSI X9.63-2001) is the elliptic curve analog of Diffie-Hellman agreement. The OIDs and parameters used to encode information are similar for ECDSA signatures and ECDH encryption, and arranged in the following manner:

```
ansi-X9-62 OBJECT IDENTIFIER :=
{ iso(1) member-body(2) us(840) 10045 }
```

```
id-public-key-type OBJECT IDENTIFIER ::= { ansi-X9.62 2 }
```

```
id-ecPublicKey OBJECT IDENTIFIER ::= { id-publicKeyType 1 }
```

Each elliptic curve public key is associated with a set of elliptic curve parameters. The OIDs that define the elliptic curve parameters are arranged as follows:

```
EcpkParameters ::= CHOICE {
    ecParameters ECParameters,
    namedCurve OBJECT IDENTIFIER,
    implicitlyCA NULL }
```

If ecParameters are inherited from the certificate authority, then the implicitlyCA value is included in EcpkParameters and is set to NULL. ecParameters and its components are defined as follows:

```
ECParameters ::= SEQUENCE {
    version ECPVer, -- version is always 1
    fieldID FieldID, -- identifies the finite field over
                      -- which the curve is defined
    curve Curve, -- coefficients a and b of the
                  -- elliptic curve
    base ECPoint, -- specifies the base point P
                  -- on the elliptic curve
    order INTEGER, -- the order n of the base point
    cofactor INTEGER OPTIONAL -- The integer h = #E(Fq)/n
}
```

ECPVer ::= INTEGER {ecpVer1(1)}

```
Curve ::= SEQUENCE {
    a FieldElement,
    b FieldElement,
    seed BIT STRING OPTIONAL }
```

FieldElement ::= OCTET STRING

ECPoint ::= OCTET STRING

ECPoint represents the base point of an elliptic curve and can take on two forms, compressed and uncompressed (defined in ANSI X9.62-2005). For certificates the encoding of ECPoint shall be supported by the uncompressed form. The compressed form may (optionally) be used instead.

The elliptic curve domain parameters can be generated according to procedures defined in Section A.3 of ANSI X9.62-2005. Example parameters sets of parameters can be found in FIPS 186-3 and ANSI X9.63-2001.

#### **8.5.1.6 tbsCertificate.issuerUniqueID and tbsCertificate.subjectUniqueID**

The issuerUniqueID and subjectUniqueID fields shall be omitted for all of the SCM's certificate types.

#### **8.5.1.7 tbsCertificate.extensions**

##### **8.5.1.7.1 CPE certificates**

CPE certificates may contain noncritical extensions; they shall not contain critical extensions. If the KeyUsage extension is present, the keyAgreement and keyEncipherment bits shall be turned on, keyCertSign and cRLSign bits shall be turned off, and all other bits should be turned off.

### **8.5.1.7.2 BS certificates**

Manufacturer/ServiceProvider certificates may contain the Basic Constraints extension. If included, the Basic Constraints extension may appear as a critical extension or as a noncritical extension. Manufacturer/ServiceProvider certificates may contain noncritical extensions; they shall not contain critical extensions other than, possibly, the Basic Constraints extension. If the KeyUsage extension is present in a Manufacturer/ServiceProvider certificate, the keyCertSign bit shall be turned on and all other bits should be turned off.

### **8.5.1.8 signatureValue**

In all three SCM certificate types, the signatureValue can contain either the RSA (with SHA-256) or ECDSA signature computed over the ASN.1 DER encoded tbsCertificate. The ASN.1 DER encoded tbsCertificate is used as input to the RSA signature function. The resulting signature value is ASN.1 encoded as a bit string and included in the Certificate's signatureValue field.

## **8.5.2 Certificate storage and management**

### **8.5.2.1 Certificate storage and management in CPE**

Manufacturer/ServiceProvider-issued CPE certificates shall be stored in (e.g., pre-installed) CPE permanent, write-once memory. CPEs that have pre-installed RSA private/public key pairs shall also have factory-installed CPE certificates. CPEs that rely on internal algorithms to generate an RSA key pair shall support a mechanism for installing a manufacturer-issued CPE certificate following key generation. The CA certificate of the Manufacturer/ServiceProvider CA that signed the CPE certificate shall be embedded into the CPE software. If a manufacturer issues CPE certificates with multiple Manufacturer/ServiceProvider CA certificates, the CPE software shall include ALL of that manufacturer's CA certificates. The specific Manufacturer/ServiceProvider CA certificate installed by the CPE shall be that identifying the issuer of that modem's CPE certificate.

### **8.5.2.2 Certificate storage and management in the BS**

SCM employs digital certificates to allow BSs to verify the binding between an identity (encoded in an X.509 digital certificate's subject names) and its public key for both a CPE and a database service. The BS does this by validating the CPE or database service certificate's certification path or chain. Validating the chain means verifying the Manufacturer/ServiceProvider CA Certificate through some means.

## 8.6 Security sublayer 2—Security mechanisms for the cognitive functions

Unlike other standards where devices operate in the licensed spectrum, cognitive radio based WRANs need to operate in the unlicensed spectrum or *White spaces* as secondary occupiers of the spectrum. Mechanisms have been defined in various clauses of IEEE Std 802.22 to protect the incumbents who are the primary occupiers of the spectrum (spectrum sensing, geolocation, spectrum management, spectrum etiquette etc.). This subclause provides further details on how to protect the incumbents as well as the IEEE 802.22 systems against various types of Denial of Service (DoS) attacks targeted at the cognitive functions of the IEEE 802.22 systems. As a result, the security sublayer 2 has been introduced in the *cognitive plane* of the IEEE 802.22 entity. The *cognitive plane* consists of a Spectrum Sensing Function (SSF), a Geolocation Function and a SM at the BS or the Spectrum Automaton at the CPE.

Figure 4 (a) shows the IEEE 802.22 Protocol Reference Model (PRM) with its Cognitive Plane functions containing security sublayer 2 at the BS. Figure 4 (b) shows the IEEE 802.22 PRM with its Cognitive Plane functions containing security sublayer 2 at the CPE. Details on the PRM itself can be found in 5.1.

*Organization*—Subclause 8.6 defines detailed attributes and mechanisms that IEEE 802.22 systems are required to provide for securing and protecting the cognitive functions. Some cognitive plane security related mechanisms are an integral part of other cognitive functions required for the IEEE 802.22 system implementation such as Spectrum Sensing Function, geolocation, spectrum manager, Spectrum Automaton, Management Plane procedures and functions etc. Since these functions are described in clauses other than 8, Subclause 8.6 briefly describes the required security features and provides references as to where in IEEE 802.22 mechanisms or the messaging for the same can be found. These security mechanisms are related to availability, authentication, authorization, identification, integrity, confidentiality, and privacy. Subclause 8.6.1 describes distributed sensing, and decision making to enhance security for WRAN systems and the incumbents. The information fusion and decision making mechanism are explained in greater detail in Clause 10 on Cognitive Radio Capability. The theoretical background for collaborative sensing and decision making is provided in Annex E related to Collaborative Sensing and Decision Making to Provide Protection against the Spurious Signals. Some other security mechanisms related to the cognitive capability are also defined in greater detail in this subclause. Subclause 8.6.2 is related to the CBP Authentication Mechanisms and 8.6.3 is related to the IEEE 802.22.1 Wireless Microphone Beacon Authentication.

Some of the basic security functions of this layer and the remediation measures required to protect these functions are described in Annex F.

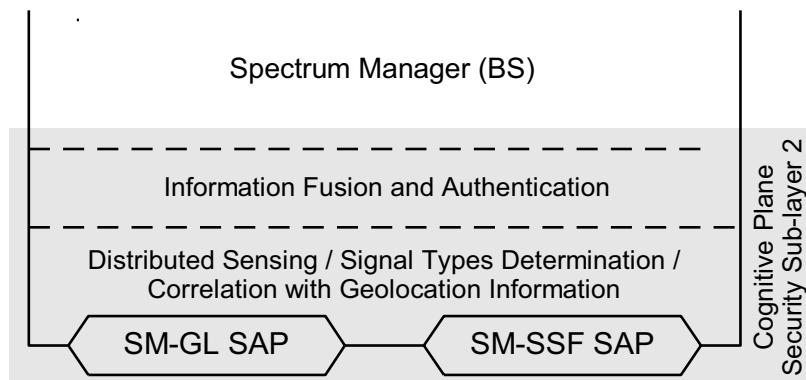


Figure 124 — Security sublayer 2 at the Cognitive Plane

## 8.6.1 Signal type determination, distributed sensing, and policy enforcement

### 8.6.1.1 General

The essential functions of the security sublayer 2 at the cognitive plane shall be to provide protection for the incumbents as well as protection to the IEEE 802.22 systems against DoS attacks of various types. Figure 124 shows the security sublayer architecture for the Cognitive Plane. This security sublayer is responsible for distributed spectrum sensing, signal type determination, correlation with geolocation information from various sensors (CPEs) located in the network and policy enforcement. This information from various sensors shall be combined in a certain way which is referred to as information fusion followed by policy enforcement. These steps enable the IEEE 802.22 systems to provide protection against some types of DoS attacks. Since this functionality is essentially a part of the Spectrum Manager (SM), the signal type determination, information fusion, and policies are defined in Clause 10; however a brief description is provided in 8.6.1.2 and 8.6.1.3.

### 8.6.1.2 Signal type determination

The IEEE 802.22 systems shall have the capability to determine the signal types that have been detected as an outcome of spectrum sensing. The signal type determination is dependent on the regulatory domain requirements and has been specified in Clause 10 and Annex A. In some regulatory domains, the signal type determination through the use of spectrum sensing may be necessary since it determines the radio transmission behavioral control using various policies and procedures.

### 8.6.1.3 Distributed sensing mechanisms

Distributed spectrum sensing is a scheme wherein *more than one* Radio Frequency (RF) sensors are used to sense the spectrum. This local sensing information shall be made available at the BS that makes a decision on whether to make opportunistic usage of the spectrum.

Annex E shows some comparisons of distributed spectrum sensing and information fusion to improve security in a network consisting of cognitive radios such as the one being considered for IEEE 802.22 systems. In Annex E, various rules are considered for information fusion where it has been shown that rather than using simple OR or AND type rules, *Voting based rules* provide flexibility and accuracy needed to provide security protection in cognitive radio systems. However, in certain regulatory domains such as the US, only ‘OR’ rule based distributed sensing is allowed wherein even if one sensor detects and determines the signal type, the policies defined in Clause 10 for such a detected signal need to be enforced.

Distributed sensing may take into account the knowledge on the geographic location of the specific sensing devices providing sensing reports. Sensing related information exchange for distributed sensing scheme may utilize available interfaces and data structures (IEEE Std 1900.6 [B16]). The correlation of the reports of the sensing devices that may have sent an urgent coexistence situation (UCS) message to the BS and their respective geographic location may provide means to identify the characteristics of the sensed signal. This may improve the decision making to determine the presence of an incumbent and its type versus presence of other devices based on their expected extent of coverage.

In the case of DTV detection, there will be larger area where the sensors will detect the presence of the signal. In the case of a wireless microphone, the detection will be over a limited area. This is also true in the case of the detection of an IEEE 802.22.1 beacon. This information is useful in determining the signal type and, in the case of an IEEE 802.22.1 beacon, it reduces the need to rely on the full PPDU decoding.

Since all the information may be available at the BS, based on what is allowed in the regulatory domain requirements, it will be up to the manufacturers to implement various levels of complexity in fusing the sensing reports and the geographic location of the sensing devices to come up with a reliable assessment of the presence of incumbents, that is true positives, while minimizing the probability of false positives.

Incumbents shall be protected in all cases and in case of doubt; action shall be taken to avoid interference to incumbents. More advanced data fusion and decision processes may have the advantage of avoiding false positives and false alarms and therefore reducing cases where WRAN systems would have to change frequency while it is not necessary.

Distributed sensing will help provide protection to the primary users of the spectrum since the probability of missed detection reduces with the number of sensors. Signal type determination and distributed sensing provides protection to the WRAN systems of the spectrum against DoS attacks. Distributed sensing helps to protect the WRAN systems against DoS attacks since it is easy to fool one sensor into believing the state of the spectrum, however, it is difficult to fool many sensors located in proximal, but disparate geographical locations. However, the data fusion rule for the distributed sensing shall be used in accordance with the specified regulatory domain requirements. (See Annex A.)

#### **8.6.1.4 Policy enforcement and radio transmission behavior control**

The IEEE 802.22 SM shall control the radio transmission behavior of the BS and the CPEs via policy sets as defined in 10.2.5.

#### **8.6.2 CBP Authentication mechanisms**

This subclause discusses a method to provide protection over CBP bursts. The CBP authentication works through direct transmissions of CBPs between BSs over-the-air, through CPEs in overlap areas that will just blindly relay the received CBP burst, or via a network backhaul mechanism. This method provides authentication and integrity protection for CBPs by using certificates to facilitate calculation of a signature over the CBPs. The calculation of the signature does not hide, modify or transform the data in anyway. This signature is then added to the CBPs as an IE. CBP bursts that include the signature IE can be decoded and processed by BSs that do not support the CBP protection mechanism. If the receiving BS supports the CBP protection, and has the key that can be used to verify the signature, the signature verification process is started. If verification is successful the CBP burst is processed, if verification fails the CBP burst is dropped.

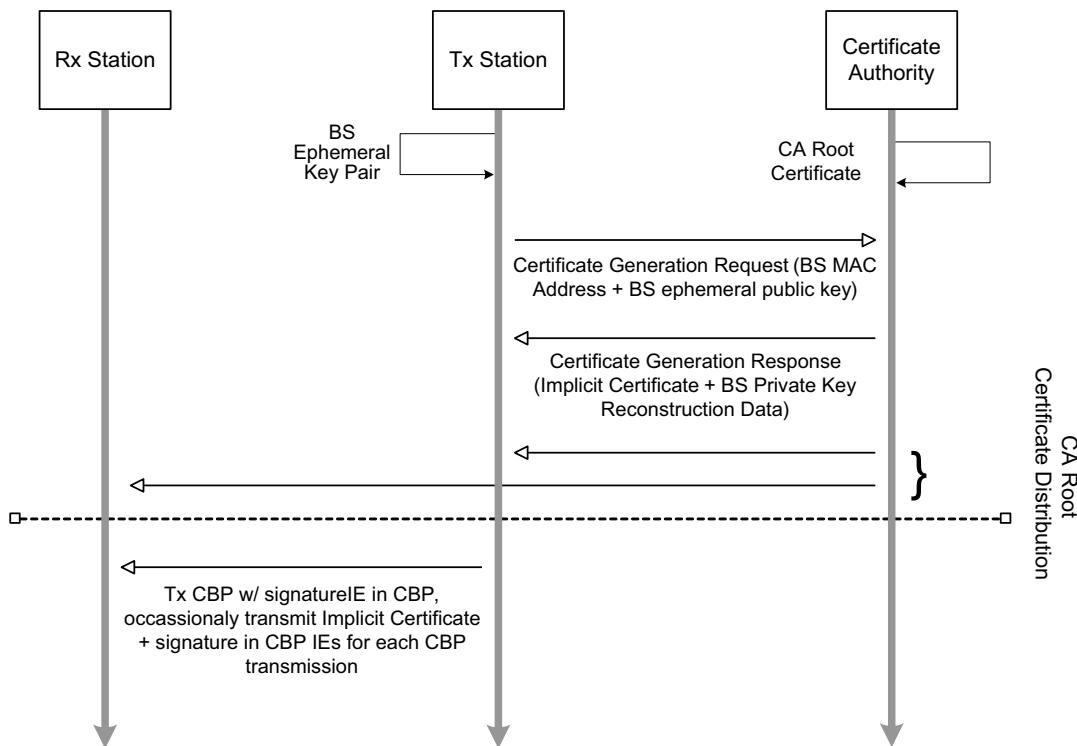
This method was derived from the method used to protect beacon messages transmitted by low powered, licensed devices operating in television broadcast bands as defined in the current IEEE Std 802.22.1-2010. The receiving station (CPE or BS) uses the certificate information to verify the signature. CBP Protection can be provided using one of two options. Figure 125 and Figure 126 describe the process by which certificates used in CBP Protection are distributed for each option. Subclauses 8.6.2.1 to 8.6.2.5 describe the options in detail. A process by which BSs can exchange their implicit certificates is described in 8.6.2.6.

CBP Authentication relies on certificates based on the Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV) as defined in SEC 4. Traditional certificates bind the identity of the device to a public key and a signature. The implicit certificate scheme defines a more compact certificate by binding the identity to public reconstruction data. The tuple of the “device identity || public reconstruction data || certificate authority public key” is fed into a know function to generate a public key for the device.

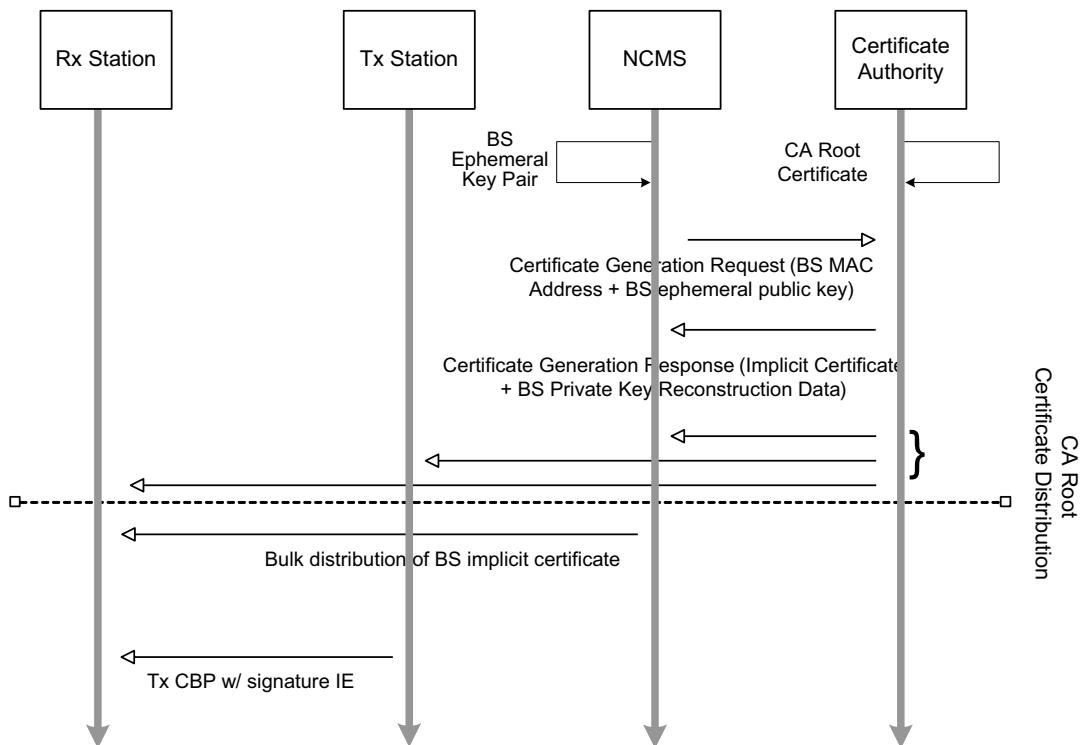
CBP Authentication makes use of implicit certificates given their smaller size and faster processing advantages. Given these advantages, it must be noted that there is one drawback. Any set of random data for the public reconstruction data and the certificate authority public key can be used with a device identity to generate a public key. This can be mitigated in one of two ways. First, if a device can provide knowledge of the private key that is bound to the reconstructed public key, it assures that the certificate authority has bound that public reconstruction data to that device’s identity. Second, if a malicious user makes use of random data to generate a public key, it is not feasible to recompute the associated private key.

The organization of this subclause is as follows:

- 8.6.2.1: Process for executing CBP Authentication Mode 1
- 8.6.2.2: Process for executing CBP Authentication Mode 2
- 8.6.2.3: Describes the format of implicit certificates and Signature IEs that are in CBP bursts
- 8.6.2.4: Prerequisites for and execution of certificate generation/verification processes
- 8.6.2.5: Prerequisites for and execution of Signature generation/verification processes
- 8.6.2.6: BS implicit certificate Exchange



**Figure 125 — CBP Authentication Mechanisms for Mode 1**



**Figure 126 — CBP Authentication Mechanisms for Mode 2**

#### 8.6.2.1 CBP Protection Mode 1

Mode 1 of CBP Protection entails transmission of BS ECC implicit certificates in CBP bursts on a regular basis, and inclusion of the signatures to be transmitted every CBP bursts. The format of the BS certificate and signature data is described in 8.6.2.3. Option 1 is executed in the following manner:

- 1) The BS uses the procedure in 8.6.2.4 to obtain an implicit certificate for the BS.
- 2) BS adds its implicit certificate to CBP as an IE. This may happen only via a periodic broadcast or during a certificate request/response (CERT-REQ/RSP, see 8.6.2.6).
- 3) BS implicit certificate private key is used directly to calculate an ECSSR-PV signature over the CBP burst data (see 8.6.2.5.2).
- 4) Receiving station receives a CBP burst with certificate and signature IEs. If the receiving station already has cached the implicit certificate from a transmitting station, it can skip ahead to verifying the signature. The receiving station then validates the BS implicit certificate's public key, Key Validity Date (Not Before), and Key Validity Time Period fields (see 8.6.2.4.3). If this validation fails, the receiving station drops the CBP. If successful, the receiving stations attempts to verify the signature (see 8.6.2.5.3). If this fails, receiving station will drop the CBP.

#### 8.6.2.2 CBP Protection Mode 2

Mode 2 of CBP Protection entails pre-distribution of BS ECC implicit certificates to receiving station. This can be done when the CPE is activated, or via NCMS (for periodic certificate updates). BS calculates the signature value in the same manner as described in steps 3 of the execution of Mode 1. The format of the of the BS certificate data that is pre-distributed the signature are defined in 8.6.2.3. Mode 2 is executed in the following manner:

- 5) The operator (via the NCMS) uses the procedures defined in 8.6.2.4.2 to obtain an implicit certificate and private key reconstruction data for each BS under its control. Each BS receives its own implicit certificate and private key reconstruction data. The NCMS verifies each BSs implicit certificate public key, Key Validity Date (Not Before), and Key Validity Time Period fields.
- 6) The operator (via the NCMS) then distributes implicit certificates of BSs to each BS that it controls in the network.
- 7) BS implicit certificate private key is used directly to calculate an ECSSR-PV signature over the CBP burst data (see 8.6.2.5.2).
- 8) Receiving station receives a CBP burst with the Signature IEs. The receiving station attempts to verify the Signature (see 8.6.2.5.3). If this fails, receiving station will drop the CBP.

### 8.6.2.3 CBP Protection Certificate and Signature structures

The following subclauses describe the structures of the certificate and signature information. For either mode, the Certificate Authority's root certificate (CARC) in Table 197 is exchanged only between the BS or operator NCMS, and the Certificate authority itself. For Mode 1, BS implicit certificates (BSIC) are exchanged between BS (via an IE in CBP burst) in order to facilitate CBP authentication. For Mode 2, the BS IC is not transmitted over the air. For either mode, the signature structure is included in an IE whenever a CBP burst is transmitted. The certificate and signature structures defined in this subclause are encoded as IEs that are defined in 7.6.1.3.1.7).

**Table 195 — Mode 1 and Mode 2 BS Implicit Certificate (BSIC)**

Item	Size	Description
CA ID	8 bits	ID of CA that issued implicit certificate to BS
Key ID	9 bits	Identifier of public key associated with certificate as assigned by CA. This identifier is generated by the Certification Authority (CA) when the certificate is created.
Key Validity Date (Not Before)	31 bits	Derived from ZDA NMEA 0183 string (each letter represents a digit encoded by different number of bits): <ul style="list-style-type: none"> <li>— X: year= 2010+X, X is 6 bits</li> <li>— M: month, e.g., 01–12, total is 4 bits</li> <li>— D: day, e.g., 01–31, total 5 bits</li> <li>— H: hour, e.g., 00–23, total 5 bits</li> <li>— m: minute, e.g., 00–59, total 6 bits</li> <li>— s: seconds, assumed to be 00, not actually encoded</li> <li>— zZ: hours off of GMT; z is 1 bit ± indication, 2nd Z is number hours 1–13 4 bits, total 5 bits</li> </ul>
Key Validity Time Period	7 bits	Amount of time in 6 month increments that the certificate is valid.

Item	Size	Description
Version	5 bit	00000: ECQV implicit certificates, ECSSR-PV signature scheme, K-233 EC Domain parameters in compressed form and 233-bit keys 00001: ECQV implicit certificates, ECSSR-PV signature scheme, B-233 EC Domain parameters in compressed form and 233-bit keys 00010: ECQV implicit certificates, ECSSR-PV signature scheme, sect233k1 EC Domain parameters in compressed form and 233-bit keys 00011: ECQV implicit certificates, ECSSR-PV signature scheme, sect233r1 EC Domain parameters in compressed form and 233-bit keys 00100–11111: reserved
Padding	4 bits	All bit shall be set to 0.
BS Public Key Reconstruction Data	31 byte	Key data used to reconstruct public key: — 31 bytes for 233 bit ECC keys

**Table 196 — Mode 1 and Mode 2 Signature structure**

Item	Size	Description
Key ID	9 bits	Identifier of the key associated with the BS implicit certificate used to generate the signature. This identifier is generated by the Certification Authority (CA) when the certificate is created.
Time Stamp	44 bits	Derived from ZDA NMEA 0183 string (each letter represents a digit encoded by different number of bits): — X: year= 2010+X, X is 6 bits — M: month, e.g., 01–12, total is 4 bits — D: day, e.g., 01–31, total 5 bits — H: hour, e.g., 00–23, total 5 bits — m: minute, e.g., 00–59, total 6 bits — ss: seconds, 00–59, 6 bits — .ss: 10 ms boundary, .000–.99, 7 bits — zZ: hours off of GMT; z is 1bit ± indication, 2nd Z is number hours 1–13 4 bits, total 5 bits
Version	5 bit	00000: ECQV implicit certificates, ECSSR-PV signature scheme, K-233 EC Domain parameters in compressed form and 233-bit keys 00001: ECQV implicit certificates, ECSSR-PV signature scheme, B-233 EC Domain parameters in compressed form and 233-bit keys 00010: ECQV implicit certificates, ECSSR-PV signature scheme, sect233k1 EC Domain parameters in compressed form and 233-bit keys 00011: ECQV implicit certificates, ECSSR-PV signature scheme, sect233r1 EC Domain parameters in compressed form and 233-bit keys 00100–11111: reserved
Padding	6 bits	All bits shall be set to 0.

Item	Size	Description
Signature	Variable	Output of signature process. This includes the <i>RecoverableMessage</i> part ( <i>C</i> ) and the Signature Data ( <i>d</i> ) as described in The signature process is detailed in 8.6.2.5.2. The signature calculated over the entire CBP MAC PDU. If Version==00000 or 00010, Size= 43 bytes If Version==00001 or 00011, Size= 44 bytes

**Table 197 — CA Root Certificate (CARC)**

Item	Size	Description
CA ID	8 bits	Unique identifier of the CA
Key ID	9 bits	Identifier of CA Root certificate as assigned by CA
Key Validity Date (Not Before)	31 bits	Derived from ZDA NMEA 0183 string (each letter represents a digit encoded by different number of bits): — X: year=2010 + X, X is 6 bits — M: month, e.g., 01–12, total is 4 bits — D: day, e.g., 01–31, total 5 bits — H: hour, e.g., 00–23, total 5 bits — m: minute, e.g., 00–59, total 6 bits — s: seconds, assumed to be 00, not actually encoded — zZ: hours off of GMT; z is 1bit ± indication, 2nd Z is number hours 1–13 4 bits, total 5 bits
Key Validity Time Period	7 bits	Amount of time in 6-month increments, that the certificate is valid.
Version	5 bit	00000: ECQV implicit certificates, ECSSR-PV signature scheme, K233 EC Domain parameters in compressed form & 233 bit keys 00001: ECQV implicit certificates, ECSSR-PV signature scheme, B-233 EC Domain parameters in compressed form & 233 bit keys 00010: ECQV implicit certificates, ECSSR-PV signature scheme, sect233k1 EC Domain parameters in compressed form & 233 bit keys 00011: ECQV implicit certificates, ECSSR-PV signature scheme, sect233r1 EC Domain parameters in compressed form & 233 bit keys 00100–11111: Reserved
EC Domain Parameters	4 bits	form0x0: Parameters for K-233 in [FIPS 186-3] 0x1: Parameters for B-233 in [FIPS 186-3] 0x2: Parameters for sect233k1 in SEC2 [B64] 0x3: Parameters for sect233r1 in SEC2 [B64] 0x4–0xF: Reserved
CA Public Key Reconstruction Data	31 bytes	Data used to reconstruct CA public key

#### 8.6.2.4 ECQV implicit certificate generation, processing, and validation requirements

Certificate generation requirements, as well the certificate validation and generation processes shall follow the process as described in Section 2.2, 2.3, and 2.4 of SEC 4.

#### **8.6.2.4.1 ECQV certificate generation requirements**

- 1) Infrastructure as described in Figure 125 for certificate generation and distribution
- 2) Recommended EC domain parameters to be used shall be for binary fields on either 223-bit random or Koblitz curves. Example domain parameters can be found in:
  - i) K-233 or B-233 elliptic curves defined in [FIPS 186-3],
  - ii) sect233k1 and sect233r1 curves defined in SEC2 [B64]
  - iii) In the EC domain parameters, elliptic curve points shall be represented in compressed form
- 3) BS shall be identified by its 48bit MAC Address
- 4) ‘to-be-signed certificate data’, IU construction is as follows:
  - For BSIC:  $I_U = I_U \parallel BEU$ , where  $I_U = \text{KeyID} \parallel \text{BS MAC Address} \parallel \text{CA ID} \parallel \text{Key Validity Date (Not Before)} \parallel \text{Key Validity Date (Not After)} \parallel \text{Version}$ , and  $BEU = \text{BS Public Key Reconstruction Data}$ ;
  - For CARC:  $CARC = I_U \parallel BEU$ , where  $I_U = \text{KeyID} \parallel \text{BS MAC Address} \parallel \text{CA ID} \parallel \text{Key Validity Date (Not Before)} \parallel \text{Key Validity Date (Not After)} \parallel \text{Version} \parallel \text{EC Domain Parameters}$ , and  $BEU = \text{CA Public Key Reconstruction Data}$
  - NOTE — BS MAC Address comes from the BS, the operator NCMS, or the SCH data in the CBP burst respectively. The Key ID, Key Validity Date (Not Before) and Key Validity Time Period are assigned by the CA and are contained in the Implicit Certificate.
- 3) The CA shall have a public-key pair that selected from the EC domain parameters in Requirement 2 and bound to the CA ID. Entities shall have access to the CA implicit certificate (with the CA’s public key reconstruction data), but no the private key associated with the implicit certificate.
- 4) SHA-256 shall be used as a *Hash* function.
- 5) If each operator is allowed to maintain its own BS implicit certificates (i.e., act as its own Certificate Authority)
  - Operator will register its Certificate Authority ID when registering its Operator ID. Mechanism by registration is executed is outside the scope of the standard.
  - Operators may share their own CA Root certificate with other operators that have BSs that border or overlap with BSs in their own network. The mechanism for CA Root Certificate sharing is outside the scope of the standard.

#### **8.6.2.4.2 ECQV Certificate generation process**

- 1) In order to start certificate generation process (see Figure 125) a request from the BS (for Mode 1, or on behalf of BS (by the NCMS) for Mode 2, shall be made to CA. Along with the request an ephemeral public key is transmitted to the CA. (Step 1 of Section 2.4.1 of SEC 4.)
  - This process requires that an ‘ephemeral’ key pair using established ECC domain parameters. ECC domain parameters used for ‘ephemeral’ key pair generation shall be the same parameters used by CA for its own certificate and BS implicit certificate generation. An ephemeral key pair generated for this step shall never be re-used.
- 2) The CA processes this request according to the procedures outline in Section 2.4.2 of SEC 4.
  - This process requires that CA generate its own ‘ephemeral’ key pair using established ECC domain parameters. ECC domain parameters used for ‘ephemeral’ key pair

generation shall be the same parameters it uses for its own certificate and BS implicit certificate generation. An ephemeral key pair shall never be reused.

- 3) The BS or operator NCMS receives a response from the CA and proceeds with the generation of the implicit certificate according to the steps 2–12 in Section 2.4.1 of SEC 4.

#### **8.6.2.4.3 ECQV Implicit Certificate Validation requirements**

- 1) Whether certificate information for a BS is received in Certificate IE or is distributed through the NCMS, a BS received that certificate shall validate it or obtain proof of validation from the NCMS.
  - BS or NCMS operator may check a CA's CRL during installation and validation of other BSs implicit certificates
- 2) The Certificate/License authority shall have its own certificate with its own EC key pair, that is generated from the EC domain parameters that are selected
- 3) ECC domain parameters that CA uses for generation of its own certificate must be same as parameters used for BS implicit certificates and ‘ephemeral’ key pair generation
- 4) The CA certificate and its associated KeyId shall be delivered to BS through NCMS, and stored in a MIB entry, which happens offline and not part of WRAN operation
- 5) Certificates for all CA's and a CA's associated ECC domain parameters shall be shared between operator's and distributed to all BSs within an operator's network. The mechanism by which this is done is outside the scope of the standard.

#### **8.6.2.4.4 ECQV Implicit Certificate Validation process**

- 1) BS implicit certificates are validated according to the procedure defined in Section 2.3.1 of SEC 4. This implies checking the validity of the implicit certificate's public key, as well as the Key Validity Date (Not Before) and Key Validity Time Period fields of the certificate.
- 2) If a certificate fails validation when received in a Certificate IE of a CBP burst, the CBP burst shall be dropped. In this case the operator may either continue to attempt coexistence operation with the transmitter of the CBP burst (in the future) or discontinue coexistence operation with the transmitter of the CBP burst.
- 3) If a certificate fails validation during installing on a BS, then the certificate shall not be installed on that BS.
  - BS or NCMS operator may check a CA's CRL during installation and validation of other BSs implicit certificates. Procedures describing the maintenance of a CRL for implicit certificates are out of the scope of the standard.

#### **8.6.2.5 Signature generation, processing, and validation requirements**

##### **8.6.2.5.1 Signature generation requirements**

- 1) The ECSSR-PV signature scheme that is used to generate the signature, is based on the same scheme as used calculate signatures for the wireless microphone beacon (IEEE 802.22.1-2010). Requirements for the Elliptic Curve Signature Scheme with Recovery, Pinstov-Vanstone (ECSSR-PV) as applied to wireless microphone beacon authentication are defined in 7.5.4.1 of IEEE Std 802.22.1-2010. ECSSR-PV requirements for CBP authentication differ in the following manner:

- i) EMSR2 shall be used as the message encoding method
  - ii) The *padLen* parameter for the EMSR2 encoding method shall be 14 octets
  - iii) The message representative of the *RecoverableMessage* (*C*) portion of the output of the signature in step 4 of 8.6.2.5.2, is an octet string of the octet ‘E0’ repeated *padLen* times (e.g., “E0 E0 E0”).
  - iv) ECSP-NR2/PV, ECSP-PV, ECVP-PV shall be used as the pre-signature, signature, and verification primitives respectively to be used in the application of the ECSSR-PV scheme
- 2) Prior to applying the ECSSR-PV signature scheme that is used to generate a signature, a BS transmitting the message shall use the Private Key Reconstruction Data (*s*) to reconstruct the private key associated with its BS implicit certificate. This is done according to the process as defined in section 2.4.1 of SEC 4.
  - 3) Prior to applying the ECSSR-PV signature scheme to verify a signature in a received CBP MAC PDU, a BS that receives messages shall use the Public Key Reconstruction Data (*BEU*, see 8.6.2.4.1) to reconstruct the public key of each BS implicit certificate that it has installed.
  - 4) The transmitting BS uses system clock (synchronized to GPS), to get time (to millisecond) for “Time” field of Signature IE.

#### 8.6.2.5.2 Signature generation process

- 1) The *M<sub>1</sub>* input into the signature process shall be an empty, null string.
- 2) The *M<sub>2</sub>* input into the signature process shall be constructed as follows:
  - i)  $M_2 = \text{CBP MAC PDU header} \parallel \text{CBP IE}_1 \parallel \text{CBP IE}_2 \dots \parallel \text{CBP IE}_n \parallel \text{EID} \parallel \text{KID} \parallel \text{Timestamp} \parallel V$
  - ii) CBP IE<sub>1</sub> – CBP IE<sub>n</sub> refer to the CBP IEs to be included in CBP
  - iii) EID refers to the Element ID field of the Signature IE, which is equal to 0x06
  - iv) KID refers to the 9-bit Key ID field of the Signature IE
  - v) V refers to the 5-bit Version field of the Signature IE
- 3) The ECSSR-PV signature scheme is applied (see 10.5.2 of IEEE 1363a-2004 [B12]), using the private key of the BS implicit certificate to generate *RecoverableMessage* Portion (*C*) and the Signature part (*d*) of the ‘to-be-sent signature data’, ‘to-be-sent signature data’ = *C* || *d*.
- 4) The ‘to-be-sent signature data’ value is inserted into the Signature field of the Signature IE, prior to transmission of the CBP burst.

#### 8.6.2.5.3 Signature verification process

- 1) The *M<sub>1</sub>* input into the ECSSR-PV scheme is an empty, null string.
- 2) The *M<sub>2</sub>* input into the ECSSR-PV scheme are derived from the fields in the received CBP burst as described in step 2) in 8.6.2.5.2.
- 3) Execute the ECSSR-PV signature verification process (see 10.5.3 of IEEE 1363a-2004 [B12]), using the public key associated with the BS implicit certificate of the BS that transmitted the CBP burst [see requirement 3) in 8.6.2.5.1].
  - i) If signature verification succeeds, the CBP burst is then processed.
  - ii) If not, then the CBP burst is dropped. BS may attempt to re-acquire CBPs from the transmitting BS or may discontinue coexistence operation with the transmitting BS.

### 8.6.2.6 BS Implicit Certificate Exchange

CBP Authentication Mode 1 requires that BSs exchange their implicit certificates in order to facilitate verification of CBP transmissions. CBP Protection Mode 2 allows for pre-distribution of CA Root and BS Implicit certificates between all BSs within an operator's network. This would be accomplished using the NCMS. This may not be possible when BSs from different operators border/overlap with each other. This subclause defines a certificate exchange process to handle this case which allows BSs to share their implicit certificates via CBP transmission during SCWs.

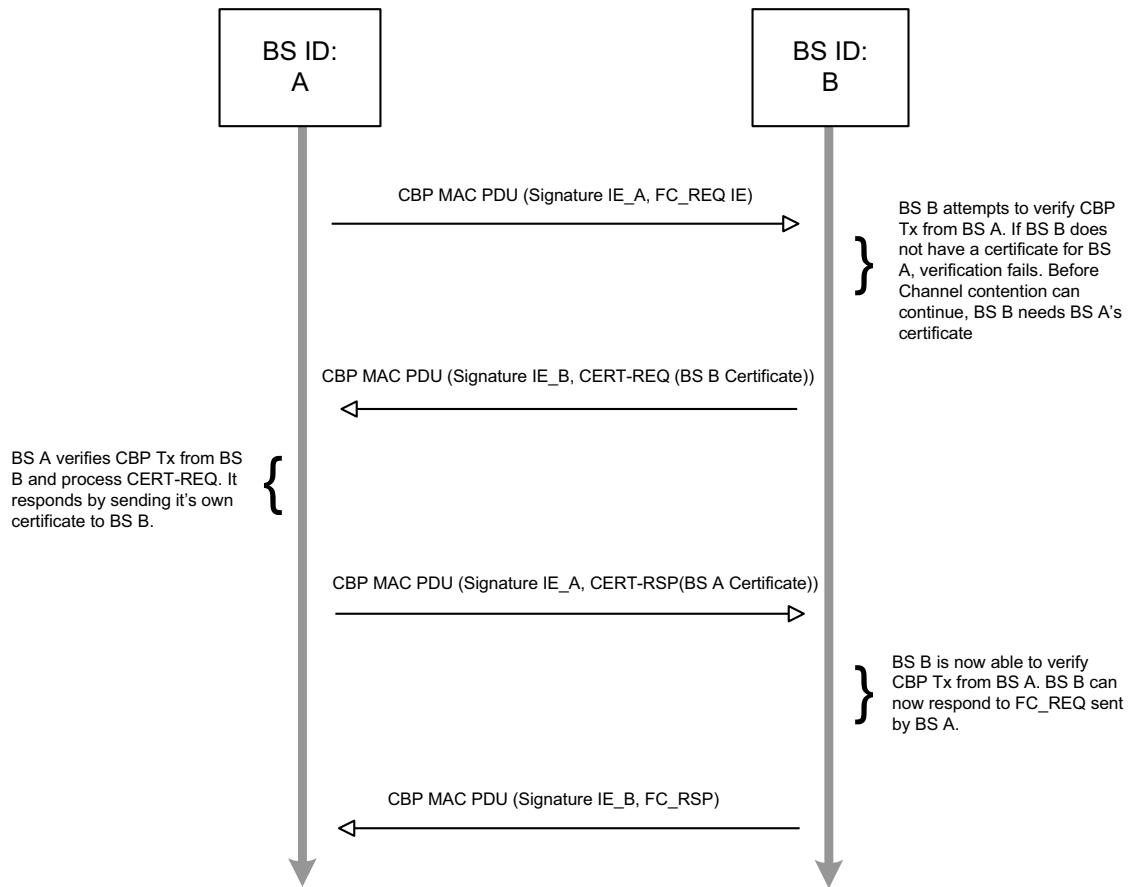
If there is a single CA, then the CA Root certificate and single set of EC domain parameters are available to all operators. If each operator is allowed to sign/create their own certificates, then operators shall make available their CA Root Certificate and EC domain parameters available to other operators.

If a BS receives a CBP from a BS, for whom it does not have the BS implicit certificate, it cannot verify the signature in the 2nd symbol (1st data symbol) of CBP and must drop the CBP packet. Upon doing this the BS (Certificate Requestor) will initiate a Certificate Request directed towards the source BS (Certificate Responder) of the unverifiable CBP. The Certificate Requestor BS does this by adding a CERT-REQ IE (see 7.6.1.3.1.7.2), with its own BS implicit certificate, as an IE in the CBP MAC PDU.

When the Certificate Responder receives a CBP with a CERT-REQ IE from a Certificate Requestor it verifies the certificate and Signature data in the Signature IE of the CBP MAC PDU. If both BSs are under the same CA then the Certificate Responder already has the CA Root certificate and EC domain parameters it needs to verify the BS implicit certificate from Certificate Requestor. If they are not, e.g., each operator has its own CA or CAs exist on a regional basis, than the Certificate Responder shall use a mechanism to request the CA Root certificate and EC domain parameters of another CA. This mechanism shall be provided. The definition of this mechanism is outside the scope of the standard.

After verifying the Certificate Requestor's certificate and signature over CBP in which CERT-REQ IE was received, the Certificate Responder initiates a Certificate Response directed towards the Certificate Requestor. The Certificate Responder does this by adding a CERT-RSP IE (see 7.6.1.3.1.7.3), with its own BS implicit certificate to the CBP MAC PDU.

When Certificate Requestor receives the CBP with the Certificate Response, it verifies it in the same manner that Certificate Responder verifies the Certificate Request. After this, any pending self-coexistence signaling (e.g., Channel Contention) can proceed. Figure 127 illustrates the BS Implicit Certificate Exchange. For certificate exchange between BSs operating in the same area, the requester makes use of an optimally selected CPE for reliable CBP burst transmission. If the destination BS does not respond, the certificate requestor assumes that the destination BS does not support self-coexistence and normal operation will continue.



**Figure 127 — BS Implicit Certificate Exchange**

### 8.6.3 IEEE 802.22.1 Beacon Authentication

The Beacon, as defined in IEEE 802.22.1 standard, is used to afford protection to devices that fall under FCC Part 74 in the US from harmful interference from license-exempt devices in the television bands. Authentication information has been added to the beacon to allow IEEE 802.22 BSs to verify the authenticity of the transmission of the beacon. Without this verification, it may be possible for a rogue device/operator to send out an illegitimate beacon in an effort to cause the receiver of the beacon to vacate that particular channel.

D.8.2 defines 10 modes for sensing and decoding the IEEE 802.22.1 beacon. Sensing Types 1-8 are not adequate for sensing and decoding enough of the IEEE 802.22.1 Beacon Frame to provide the receiving device with the information to authenticate the IEEE 802.22.1 beacon. To authenticate the beacon, Sensing Types 9 and 10 shall be used.

If Sensing Type 9 (see D.8.2.9) is used, then MSF1 and MSF2 of the IEEE 802.22.1 beacon frame is captured and decoded. If the CRC verification on both MSF1 and MSF2 passes, the CPE relays the payloads to the BS. The signature calculated over the IEEE 802.22.1 beacon frame is contained with the Signature field of MSF2. To verify the signature, the public key of the certificate used to generate the signature is required. In this case, the certificate and public key shall be obtained by the BS via some off-line method (see 5.6.1 and 7.5.5, IEEE Std 802.22.1-2010) and installed at the IEEE 802.22 BS via a MIB.

If Sensing Type 10 (see D.8.2.10) is used, then MSF1, MSF2, and MSF3 of the IEEE 802.22.1 beacon frame is captured and decoded. If the CRC verification on all three MSFs passes, the CPE relays the payloads to the BS. With this method the receiving device has all of the information it needs to verify the signature.

The process for verifying the signature in the IEEE 802.22.1 beacon frame is detailed in 7.5.4 of IEEE Std 802.22.1-2010. If the signature is processed, and verified as being authentic, the receiving device has knowledge that the originator of the beacon is an authentic PPD as defined by IEEE Std 802.22.1-2010. Under this circumstance, the IEEE 802.22 device must vacate the channel after following the procedures as defined by the policy in Clause 10. If the signature is not verified as being authentic, then no action is taken (see policy 3b in Table 234).

## 8.7 CPE privacy

CPE SID and MAC Address are sent in the clear during the Ranging procedure. This can allow malicious users to track an individual CPE in the network, which is both a security concern and may (in some regulatory domains) violate laws regarding privacy of user information.

The following process details a procedure that can be used to ensure user privacy:

- a) Upon receiving the CDMA Allocation IE, CPE transmits the RNG-REQ with its MAC Address on the Initial Ranging connection.
  - 1) The BS receives the RNG-REQ, and transmits the RNG-RSP to the intended CPE using the MAC Address received in the RNG-REQ. The RNG-RSP shall contain a “temporary” SID selected from the pool of unused multicast SIDs.
  - 2) The “temporary” SID is then used by the BS and CPE to conduct the basic capability exchange (CBC-REQ/RSP).
  - 3) The BS or CPE transmits the SCM EAP-Start and EAP-Transfer messages on the “temporary” SID until authentication is complete.
  - 4) The “temporary” SID is used to setup the keying on the CPE via SCM Key-Request/Reply messages.
  - 5) The registration process is initiated when the CPE transmits the REG-REQ to the BS. When the BS responds with the REG-RSP, it shall include the Permanent SID IE (see 7.7.7.3.4.12), to assign the “permanent” SID to the CPE

The CPE and BS “hold” onto the temporary SID until the CPE completes the REG-REQ/RSP. Until then no other CPE can enter the network utilizing the same temporary SID. Use of this procedure is optional and at the discretion of the operator.

## 9. PHY

This clause specifies the basic technologies for the standardization of the physical (PHY) layer for WRAN systems. The specification is for a system that uses vacant channels to provide wireless communication over a distance of up to 100 km, the propagation time over the first 30 km range being absorbed by the TTG at the PHY layer and the propagation time beyond 30 km being absorbed by proper MAC packet scheduling at the BS, as well as time buffers before and after the opportunistic bursts (ranging, BW request, and UCS notification) and before and after the CBP burst.

The system reference frequency is the center frequency of the channel in which the transmitter and the receiver equipment operates. Annex A lists the frequencies corresponding to the channels used for WRAN operation in various regulatory domains.

The PHY specification is based on an orthogonal frequency division multiple access (OFDMA) scheme where information to (downstream) or from (upstream) multiple CPEs are modulated on orthogonal subcarriers using Inverse Fourier Transforms. The main system parameters are provided in Table 198.

**Table 198 — System parameters for WRAN**

Parameters	Specification	Remark
Frequency range	54~862 MHz <sup>a</sup>	
Channel bandwidth	6, 7, or 8 MHz	According to regulatory domain (see Annex A).
Data rate	4.54 to 22.69 Mbit/s	See Table 202
Spectral Efficiency	0.76 to 3.78 bit/(s·Hz)	See Table 202
Payload modulation	QPSK, 16-QAM, 64-QAM	BPSK used for preambles, pilots and CDMA codes.
Transmit EIRP	4W maximum for CPEs. 4W maximum for BS's in the USA regulatory domain.	Maximum EIRP for BS's may vary in other regulatory domains.
Multiple Access	OFDMA	
FFT Size ( $N_{FFT}$ )	2048	
Cyclic Prefix Modes	1/4, 1/8, 1/16, 1/32	
Duplex	TDD	

<sup>a</sup> Frequency range allocated to the Television Broadcasting Service in various parts of the world.  
See Annex A for further details.

The following subclauses provide details on the various aspects of the PHY specifications.

### 9.1 Symbol description

#### 9.1.1 OFDM symbol mathematical representation

The RF signal transmitted during any OFDM symbol duration can be represented mathematically as follows:

$$s(t) = \operatorname{Re} \left\{ e^{j2\pi f_c t} \sum_{\substack{k=-N_T/2 \\ k \neq 0}}^{N_T/2} c_k e^{j2\pi k \Delta f (t - T_{CP})} \right\} \quad (1)$$

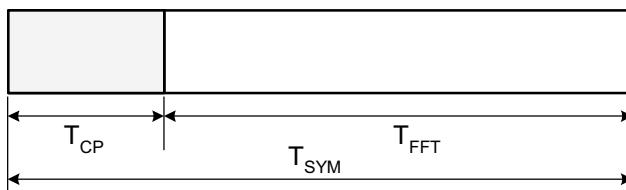
where

$t$	is the time elapsed since the beginning of the current symbol, with $0 < t < T_{SYM}$
$T_{SYM}$	is the symbol duration, including cyclic prefix duration
$Re(\cdot)$	real part of the signal
$f_c$	is the carrier frequency
$c_k$	is a complex number; the data to be transmitted on the subcarrier whose frequency offset index is $k$ , during the current symbol. It specifies a point in a QAM constellation.
$\Delta f$	is the subcarrier frequency spacing
$T_{CP}$	is the time duration of cyclic prefix
$N_T$	is the number of used subcarriers (not including DC subcarrier)

### 9.1.1.1 Time domain description

The time-domain signal is generated by taking the inverse Fourier transform of the length  $N_{FFT}$  vector. The vector is formed by taking the constellation mapper output and inserting pilot and guard tones. At the receiver, the time domain signal is transformed to the frequency domain representation by using a Fourier transform.

Let  $T_{FFT}$  represent the time duration of the IFFT output signal. The OFDM symbol is formed by inserting a cyclic prefix of time duration  $T_{CP}$  (shown in Figure 128), resulting in a symbol duration of  $T_{SYM} = T_{FFT} + T_{CP}$ .



**Figure 128 — OFDM symbol format**

The specific values for  $T_{FFT}$ ,  $T_{CP}$  and  $T_{SYM}$  are given in 9.1.2. The BS determines these parameters and conveys the  $T_{CP}$  to  $T_{FFT}$  ratio to the CPEs using the SCH (see Table 1).

The time at which the FFT window starts within the symbol period for reception at the CPE is determined by the local synchronization strategy to minimize inter-symbol interference due to pre- and post-echoes and any synchronization error, and is implementation dependent.

### 9.1.1.2 Frequency domain description

In the frequency domain, an OFDM symbol is defined in terms of its subcarriers. The subcarriers are classified as: 1) data subcarriers, 2) pilot subcarriers, 3) guard and Null (including DC) subcarriers. The classification is based on the functionality of the subcarriers. The DS and US may have different allocations of subcarriers. The total number of subcarriers is determined by the FFT/IFFT size. The pilot subcarriers are distributed across the bandwidth. The exact location of the pilot and data subcarriers and the symbol's subchannel allocation is determined by the particular configuration used. All the remaining guard/Null subcarriers carry no energy and are located at the center frequency of the channel (DC subcarrier) and at both edges of the channel (guard subcarriers).

## 9.1.2 Symbol parameters

### 9.1.2.1 Subcarrier spacing

The BS and CPEs shall use the 2048 FFT mode with the subcarriers spacing specified in Table 199.

The subcarrier spacing,  $\Delta f$ , is dependent on the bandwidth of the channel (6 MHz, 7 MHz, or 8 MHz). Table 199 shows the subcarrier spacing and the corresponding FFT/IFFT period ( $T_{FFT}$ ) values for the different channel bandwidth options.

**Table 199 — Subcarrier spacing and FFT/IFFT period values for different bandwidth options based on sampling frequency equivalent to 8/7 channel bandwidth**

	6 MHz based channels	7 MHz based channels	8 MHz based channels
<b>Basic sampling frequency, <math>F_S</math> (MHz)</b>	6.856	8	9.136
<b>Inter-carrier spacing, <math>\Delta f</math> (Hz) = <math>F_S/2048</math></b>	3347.656...	3906.25	4460.938...
<b>FFT/IFFT period, <math>T_{FFT}</math> (μs)=<math>1/\Delta f</math></b>	298.716...	256	224.168...
<b>Time Unit (ns) <math>TU=T_{FFT}/2048</math></b>	145.858...	125	109.457...

### 9.1.2.2 Symbol duration for different cyclic prefix modes

The cyclic prefix duration  $T_{CP}$  could be one of the following derived values:  $T_{FFT}/32$ ,  $T_{FFT}/16$ ,  $T_{FFT}/8$ , and  $T_{FFT}/4$ . The OFDM symbol duration for different values of cyclic prefix is given in Table 200.

**Table 200 — Symbol duration for different cyclic prefixes and bandwidth options**

		$CP = T_{FFT}/32$	$CP = T_{FFT}/16$	$CP = T_{FFT}/8$	$CP = T_{FFT}/4$
$T_{SYM} = T_{FFT} + T_{CP}$ (μs)	<b>6 MHz</b>	308.051...	317.386...	336.056...	373.396...
	<b>7 MHz</b>	264	272	288	320
	<b>8 MHz</b>	231.173...	238.179...	252.189...	280.210...

### 9.1.2.3 Transmission parameters

Table 201 shows the different parameters and their values for the three bandwidths.

**Table 201 — OFDM parameters for the three channel bandwidths**

TV channel bandwidth (MHz)	6	7	8
Total number of subcarriers, $N_{FFT}$	2048		
Number of guard subcarriers, $N_G$ (L, DC, R)	368 (184, 1, 183)		
Number of used subcarriers, $N_T = N_D + N_P$	1680		
Number of data subcarriers, $N_D$	1440		
Number of pilot subcarriers, $N_P$	240		

## 9.2 Data rates

Table 202 defines the different PHY modulation and encoding modes with their associated parameters along with an example of the resulting gross data rates in the case of the 6 MHz channel bandwidth.

**Table 202 — PHY Modes and their related modulations, coding rates  
and data rates for  $T_{CP} = T_{FFT}/16$**

PHY Mode	Modulation	Coding Rate	Data rate (Mb/s)	Spectral Efficiency <sup>5</sup> (for 6 MHz bandwidth)
1 <sup>1</sup>	BPSK	Uncoded	6 <sup>6</sup>	6 <sup>6</sup>
2 <sup>2</sup>	QPSK	1/2 Repetition: 4	6 <sup>6</sup>	6 <sup>6</sup>
3 <sup>3</sup>	QPSK	1/2 Repetition: 3	6 <sup>6</sup>	6 <sup>6</sup>
4 <sup>4</sup>	QPSK	1/2 Repetition: 2	6 <sup>6</sup>	6 <sup>6</sup>
5	QPSK	1/2	4.54	0.76
6	QPSK	2/3	6.05	1.01
7	QPSK	3/4	6.81	1.13
8	QPSK	5/6	7.56	1.26
9	16-QAM	1/2	9.08	1.51
10	16-QAM	2/3	12.10	2.02
11	16-QAM	3/4	13.61	2.27
12	16-QAM	5/6	15.13	2.52
13	64-QAM	1/2	13.61	2.27
14	64-QAM	2/3	18.15	3.03
15	64-QAM	3/4	20.42	3.40
16	64-QAM	5/6	22.69	3.78

NOTE 1: Mode 1 is only used for CDMA opportunistic bursts.

NOTE 2: Mode 2 is only used for SCH packet transmission.

NOTE 3: Mode 3 is only used for CBP transmission.

NOTE 4: Mode 4 is only used for FCH transmission.

NOTE 5: Spectral efficiency informative values are calculated assuming continuous stream of 1440 data subcarriers for the given modulation and FEC modes (i.e., assuming no TTG, RTG and superframe and frame headers).

NOTE 6: These modes are for control signal transmissions and there is no need to specify data rate or spectral efficiency.

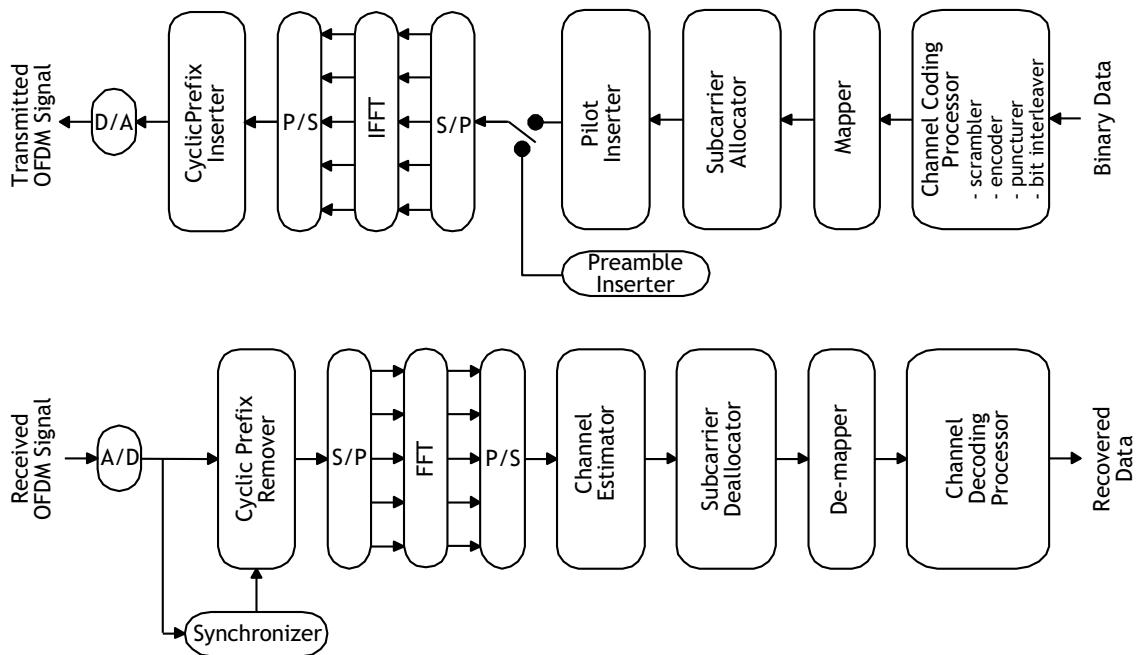
### 9.3 Functional block diagram applicable to the PHY layer

The functional block diagram of the transmitter and receiver for the PHY layer is shown in Figure 129. This subclause describes the general processing of the WRAN baseband signal. The binary data intended for transmission is supplied to the PHY layer from the MAC layer. This input is sent to a channel coding processor which includes a data scrambler, encoder, puncturer (except for LDPC and SBTC) as specified in 9.7, and a bit interleaver specified in 9.6.5. The interleaved data is mapped to data constellations as described in 9.8 according to the modulation schemes specified as shown in Table 202. The subcarrier allocator assigns the data constellations to the corresponding subchannels according to the subcarrier allocation methods described in 9.6.3 and 9.6.4.

A frame may have its first OFDM symbol occupied by the frame preamble or have its first and second OFDM symbols occupied by the superframe preamble and the frame preamble as specified in 9.4.1. The pilot subcarriers are transmitted at fixed positions in the frequency domain within each OFDM data symbol as specified in 9.6.1. Preambles and pilots can support the synchronization, channel estimation and tracking process. In the frequency-domain, an OFDM symbol contains the data, pilot, and null subcarriers, as defined in Table 201. The resultant stream of constellations is subsequently input to an inverse Discrete Fourier Transform after a serial-to-parallel conversion. The inverse Fast Fourier Transform (IFFT) is the expected means of performing the inverse Discrete Fourier Transform. In order to prevent inter-symbol interference (ISI) eventually caused by the channel delay spread, the OFDM symbol is extended by a cyclic prefix that contains the same waveform as the corresponding ending part of the symbol. Finally, the OFDM signal is transferred to the RF transmission modules via a digital-to-analog converter.

The OFDM receiver roughly implements the same operations as performed by the transmitter but in reverse order. In addition to the data processing, synchronization and channel estimation must be performed at the receiver.

The CBP packet can also be generated through the same process as that used for the data transmission. The only difference is in the subcarrier allocator and the preamble and pilot inserters. The subcarrier allocation of CBP data is similar to a spreading process because each QPSK symbol is transmitted on three different spread subcarriers. The CBP packet subcarrier allocation, preamble and pilot patterns are described in 9.5.



**Figure 129 — Transmitter and receiver block diagram for the OFDMA PHY**

## 9.4 Superframe and frame structures

The basic superframe structure and frame structure are shown in Figure 10, Figure 11, and Figure 12. See 7.3 and 7.3.2 for a full description of the superframe and frame structures.

The superframe shall consist of 16 frames of 10 ms each. Each frame contains a preamble, header, and data bursts.

For both normal and self-coexistence operational modes, in the first allocated frame, the first symbol shall be the superframe preamble, followed by a frame preamble symbol. The third symbol shall be the SCH, and the fourth symbol shall contain the FCH and, when needed, DS-MAP, US-MAP, DCD and UCD, and data bursts if there is some room left. The SCH is transmitted to provide protection to incumbents through the scheduling of quiet periods and self-coexistence through the mapping of the frames belonging to the appropriate WRAN cell, and so on (see 7.3). The FCH specifies the length of the first MAP that will immediately follow the FCH. The first frame allocated to a BS in a superframe shall contain two fewer symbols than normal frames to keep the length to 10 ms.

The other allocated frames of the superframe shall contain successively a frame preamble, the FCH and the DS-MAP, US-MAP, DCD, and UCD messages when needed, and the data bursts.

In each frame, a TTG shall be inserted between the downstream and upstream bursts to allow the CPE to switch between the receive mode and transmit mode and to absorb the signal propagation time for a distance of up to 30 km (note that the propagation time for CPEs beyond this distance will be accommodated by proper scheduling of the downstream bursts and upstream grants). A RTG shall be inserted at the end of each frame to allow the BS to switch between its receiving mode and transmit mode (see Figure 13 in 7.4). The values indicated in Table 203 for the TTG and RTG shall be used for the specified cyclic prefixes and channel bandwidth options.

**Table 203 — WRAN frame parameters**

Cyclic Prefix	Number of symbols per frame <sup>1</sup>	Transmit-receive turnaround gap <sup>2</sup> (TTG)	Receive-transmit turnaround gap <sup>3</sup> (RTG)
BW	6 MHz 7 MHz 8 MHz	6 MHz 7 MHz 8 MHz	6 MHz 7 MHz 8 MHz
1/4	24	1439 TU	561 TU
	28	1680 TU	1520 TU
	32	1918 TU	2402 TU
1/8	26	1439 TU	2097 TU
	31	1680 TU	1776 TU
	36	1918 TU	1378 TU
1/16	28	1439 TU	1073 TU
	33	1680 TU	1392 TU
	38	1918 TU	1634 TU
1/32	29	1439 TU	753 TU
	34	1680 TU	1392 TU
	39	1918 TU	1954 TU

NOTE 1—Indicates the DS/US payload symbols only. Here, one frame preamble symbol and one header symbol carrying the FCH, DS/US-MAP and DCD/UCD are assumed. Different values may apply when the frame carries more header symbols using 1/4 cyclic prefix such as the superframe preamble and SCH.

NOTE 2—Example of TTG set to absorb the propagation delay for up to 30 km and a CPE turnaround time of 10 µs. For larger distances, proper scheduling at the BS will allow for absorption of longer propagation delay.

NOTE 3—Portion of symbol left over to arrive at the 10 ms frame period.

#### 9.4.1 Preamble

##### 9.4.1.1 Preamble definition

Two types of frequency domain sequences are defined in order to facilitate burst detection, synchronization and channel estimation at a WRAN receiver.

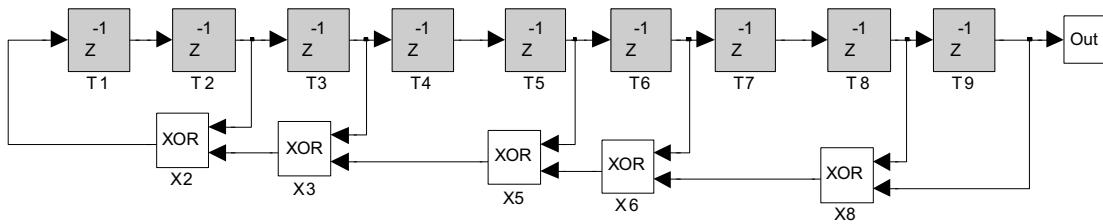
- 1) Short Training Sequence (STS): This sequence is made of 512 bits producing a binary bipolar sequence (+1, -1) applied to every 4<sup>th</sup> subcarrier of an OFDM symbol. Thus, in the time domain, this will result in 4 repetitions of a 512-sample sequence for each OFDM symbol modulated by the STS.
- 2) Long Training Sequence (LTS): This sequence is made of 1024 bits producing a binary bipolar sequence (+1, -1) applied to every 2<sup>nd</sup> subcarrier of an OFDM symbol. Thus, in the time domain, this will result in 2 repetitions of a 1024-sample sequence for each OFDM symbol modulated by the LTS.

The STS is used to form the superframe and CBP preambles while the LTS is used to form the frame preamble. Each sequence element is associated with one OFDM subcarrier (BPSK modulated) in the frequency domain. The sequence element values (+1, -1) are generated in an algorithmic way to provide for low peak-to-average-power-ratio (PAPR).

These sequences shall be generated by the method described in the 9.4.1.1.1 and 9.4.1.1.2.

###### 9.4.1.1.1 Generation of STS

First, a periodic sequence  $P_{REF}^{ST}$  with a period of 512 is generated using a pseudo-noise (PN) sequence generator with the following polynomial:  $X^9 + X^8 + X^6 + X^5 + X^3 + X^2 + 1$ . Figure 130 depicts an implementation of this PN sequence generator using a Linear Feedback Shift Register.

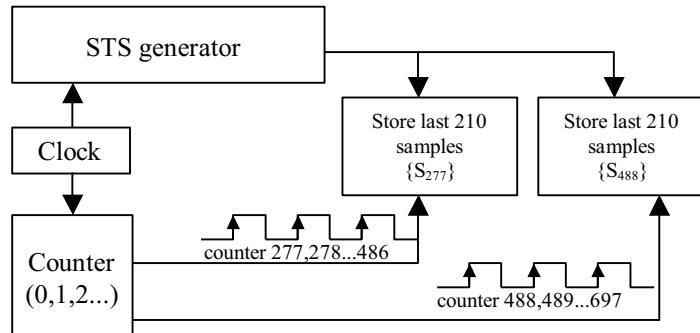


**Figure 130 — Structure of a Linear Feedback Shift Register implementation for the given STS polynomial**

The STS sequence generator is initialized to a value of 1 1111 1111. The resultant  $P_{REF}^{ST}$  sequence of 511 samples (using BPSK mapping as shown in Figure 153) is given as follows:

$$P_{REF}^{ST}(0:510) = \{1, 1, 1, 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, -1, 1, -1, 1, \dots, -1, -1, -1, -1, -1, -1, 1, 1, -1, -1, -1, -1, -1, -1, -1, 1, -1\}$$

Second, define  $S_{277}(0:209) = P_{REF}^{ST}(277:486)$ . The elements of sequence  $\{S_{277}\}$  may be obtained by clocking the STS generator, without resetting it, 487 times consecutively, and storing only the last 210 samples (out of the BPSK modulator, see Figure 130). Moreover, define  $S_{488}(0:209) = P_{REF}^{ST}(488:697)$ . The elements of sequence  $\{S_{488}\}$  may be obtained by continuing to clock the STS generator, without resetting it, for an extra 211 clocks, after  $S_{277}$  has been stored. The last 210 samples form the elements of  $S_{488}$  taken from the BPSK modulator. Therefore, a total of 698 clocks are necessary to obtain one pair of sequences  $\{S_{277}, S_{488}\}$  (see Figure 131).



**Figure 131 — Scheme for the generation of sequences  $\{S_{277}, S_{488}\}$**

After resetting the clock, the first 210 symbols of these sequences are as follows:

$$S_{277}(0:209) = \{1, 1, -1, -1, -1, 1, -1, 1, 1, -1, 1, 1, 1, 1, -1, -1, 1, 1, \dots, 1, 1, -1, 1, -1, -1, -1, -1, 1, 1, -1, 1, -1, -1, -1, -1, -1\}, \text{ and}$$

$$S_{488}(0:209) = \{-1, -1, 1, -1, -1, -1, -1, -1, -1, 1, 1, 1, -1, -1, -1, -1, -1, \dots, -1, -1, -1, -1, -1, -1, 1, -1, 1, -1, -1, -1, -1\}$$

For illustration only, consider that after resetting the STS generator, the pair of sequences  $\{S_{277}, S_{488}\}$  can be represented in Hexadecimal format where the elements with amplitude value of  $-1$  are mapped to bit0 (bit zero) and the elements with value of  $+1$  are mapped to bit1 (bit one). These sequences can therefore be represented in hex format after appending 2 dummy zero bits at the end (bit ordering from left to right) as follows:

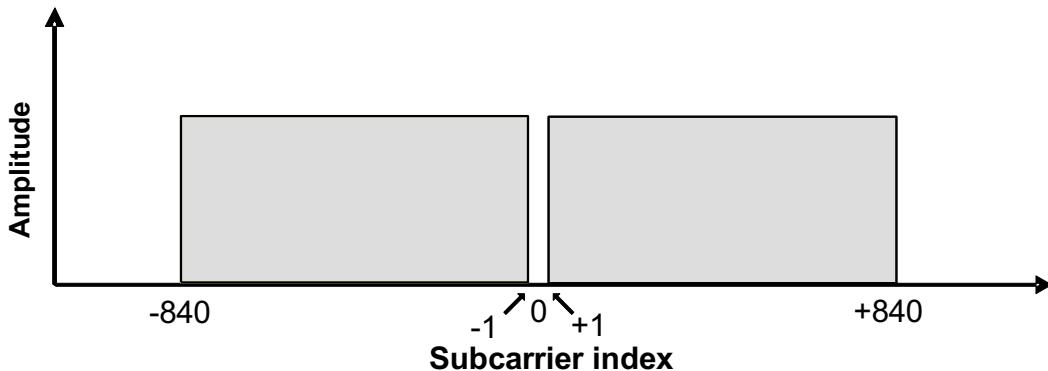
$$\{S_{277}\}_{hex} = C56F36BB65B724B8E5E8D6137C4AF1942307BF5AB264770B41B00$$

{S<sub>488</sub>hex} = 203805FF2AB99A227875F4D4ECE9163C851F3D4530C410FC15030

The coefficients of the 2048 frequency elements to be presented at the input of the inverse DFT are then formed from the above two sequences using the following equation where  $N_T$  represents the number of used subcarriers (see Table 201):

$$P_{ST}(k) = \begin{cases} \sqrt{\frac{N_T}{420}} S_{277} \left( \frac{k+840}{4} \right), & -840 \leq k \leq -4, k \bmod 4 = 0 \\ \sqrt{\frac{N_T}{420}} S_{488} \left( \frac{k-4}{4} \right), & 4 \leq k \leq 840, k \bmod 4 = 0 \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

and results in the short training sequence (STS) as shown below:



**Figure 132 — Subcarrier numbering scheme**

$$P_{ST}(-1024:-841) = \{0, 0, 0, 0, 0, \dots, 0, 0, 0, 0, 0, 0\}$$

$$P_{ST}(-840:-1) = \sqrt{\frac{N_T}{420}} \{1, 0, 0, 0, 0, 1, 0, 0, 0, -1, 0, 0, 0, -1, 0, 0, 0, -1, 0, 0, 0, \dots, -1, 0, 0, 0, -1, 0, 0, 0, -1, 0, 0, 0, -1, 0, 0, 0, -1, 0, 0, 0\}$$

$$P_{ST}(0) = 0$$

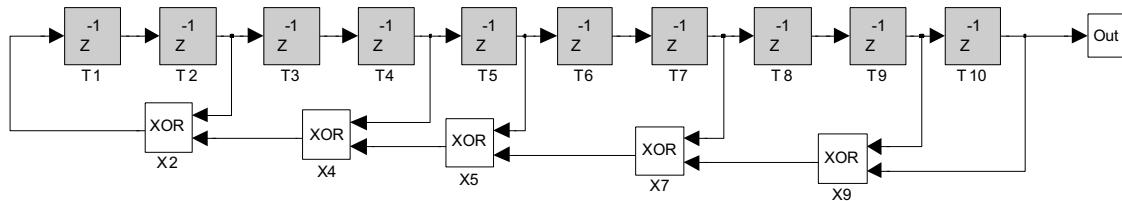
$$P_{ST}(1:840) = \sqrt{\frac{N_T}{420}} \{0, 0, 0, -1, 0, 0, 0, -1, 0, 0, 0, 1, 0, 0, 0, -1, 0, 0, 0, \dots, 0, 0, 0, -1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, -1, 0, 0, 0, 0, -1\}$$

$$P_{ST}(841:1023) = \{0, 0, 0, 0, 0, \dots, 0, 0, 0, 0, 0, 0\}$$

Taking the inverse DFT of the above sequence will generate 4 repetitions of a 512-sample sequence in the time domain. The factor  $\sqrt{\frac{N_r}{420}}$  is used to normalize the signal energy, where  $N_r$  represents the number of used subcarriers.

#### 9.4.1.1.2 Generation of LTS

First, a periodic sequence  $P_{REF}^{LT}$  with a period of 1024 is generated using a pseudo-noise (PN) sequence generator with a polynomial of  $X^{10} + X^9 + X^7 + X^5 + X^4 + X^2 + 1$ . Figure 133 depicts an implementation of this PN sequence generator using a Linear Feedback Shift Register.



**Figure 133 — Structure of a Linear Feedback Shift Register implementation for the given LTS polynomial**

The LTS sequence generator is initialized to a value of 11 1111 1111. The resultant  $P_{REF}^{LT}$  sequence of 1023 samples (using BPSK mapping) is given as follows:

$$P_{REF}^{LT}(0:1022) = \{1, 1, 1, 1, 1, 1, 1, 1, 1, 1, -1, -1, 1, 1, 1, -1, 1, 1, -1, 1, 1, 1, \dots, 1, -1, 1, 1, -1, -1, 1, -1, -1, -1, 1, 1, -1, -1, -1, 1, 1, -1, -1\}$$

Second, define  $S_{536}(0:419) = P_{REF}^{LT}(536:955)$  and  $S_{115}(0:419) = P_{REF}^{LT}(115:534)$  respectively. The first 420 binary values of these sequences are as follows:

$$\begin{aligned} S_{536}(0:419) &= \{1, 1, 1, 1, -1, -1, 1, 1, 1, -1, -1, 1, -1, -1, -1, 1, 1, -1, \dots, 1, -1, -1, 1, -1, -1, 1, 1, \\ &\quad 1, -1, -1, -1, 1, 1, -1, 1, 1, 1, 1, 1\}, \text{ and} \\ S_{115}(0:419) &= \{1, -1, 1, -1, 1, -1, -1, -1, 1, 1, 1, -1, 1, 1, 1, 1, 1, 1, \dots, 1, 1, -1, 1, -1, 1, 1, 1, -1, 1, \\ &\quad 1, -1, -1, 1, -1, -1, 1, 1, 1\} \end{aligned}$$

For illustration only, consider that after resetting the LTS generator, the pair of sequences  $\{S_{536}, S_{115}\}$  can be represented in Hexadecimal format where the elements with amplitude value of -1 are mapped to bit0 (bit zero) and the elements with value of +1 are mapped to bit1 (bit one). These sequences can therefore be represented in hex format (bit ordering from left to right) as follows:

```
{S536hex}=
F1C4677539900F45F5E42A3418663A12B8F6C1081350487D8D55D344BACF02CD9C9BCD68C4932A
67D2AC0473878B1F970A2A938DF
{S115hex}=
A877F40C94889D20B91E7FB49616CB714A17845A62EE00A795947CC27EFBB3E32F5B7E0FE2607
056F6669D872C8A0376E8ED764F
```

The coefficients of the 2048 frequency elements to be presented at the input of the inverse DFT are then formed from the above two sequences using the following equation where  $N_T$  represents the number of used subcarriers:

$$P_{LT}(k) = \begin{cases} \sqrt{\frac{N_T}{840}} S_{536}\left(\frac{k+840}{2}\right), & -840 \leq k \leq -2, k \bmod 2 = 0 \\ \sqrt{\frac{N_T}{840}} S_{115}\left(\frac{k-2}{2}\right), & 2 \leq k \leq 840, k \bmod 2 = 0 \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

and results in the long training (LT) sequence as shown below:

$$P_{LT}(-1024:-841) = \{0, 0, 0, 0, 0, \dots, 0, 0, 0, 0, 0\}$$

$$P_{LT}(-840:-1) = \sqrt{\frac{N_t}{840}} \{1, 0, -1, 0, 1, 0, -1, 0, 1, 0, -1, 0, -1, 0, -1, 0, -1, 0, 1, 0, \dots, 1, 0, -1, 0, -1, 0, 1, 0, -1, 0, -1, 0, 1, 0, 1, 0, 1, 0\}$$

$$P_{LT}(0) = 0$$

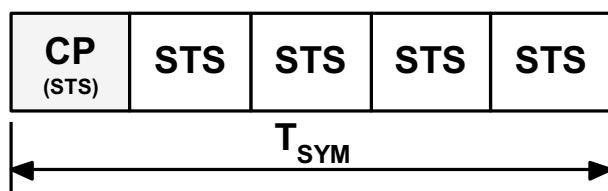
$$P_{LT}(1:840) = \sqrt{\frac{N_T}{840}} \{0, 1, 0, 1, 0, 1, 0, 1, 0, -1, 0, -1, 0, -1, 0, 1, 0, 1, 0, \dots, 0, -1, 0, -1, 0, 1, 0, 1, 0, -1, 0, 1, 0, 1, 0, 1, 0, 1\}$$

$$P_{LT}(841:1023) = \{0, 0, 0, 0, 0, \dots, 0, 0, 0, 0, 0\}$$

Taking the inverse DFT of  $P_{LT}$  will result in 2 repetitions of a 1024-sample vector in the time domain. The factor  $\sqrt{\frac{N_T}{840}}$  is used to normalize the signal energy, where  $N_T$  represents the number of used subcarriers.

#### 9.4.1.2 Superframe preamble

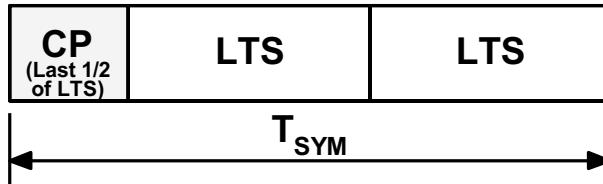
The superframe preamble is used by the receiver for frequency and time synchronization. The format of the superframe preamble is shown in Figure 134. The superframe preamble shall be 1 OFDM symbol in duration and shall consist of 4 repetitions of the STS in the time domain preceded by a cyclic prefix of length  $1/4$  ( $T_{CP} = 1/4 T_{FFT}$ ) which shall also consist of an STS.



**Figure 134 — Superframe preamble format using the short training sequence**

#### 9.4.1.3 Frame preamble

The format of the frame preamble is shown in Figure 135. The frame preamble shall use the  $T_{CP} = 1/4 T_{FFT}$  which shall consist of the second half of the LTS.

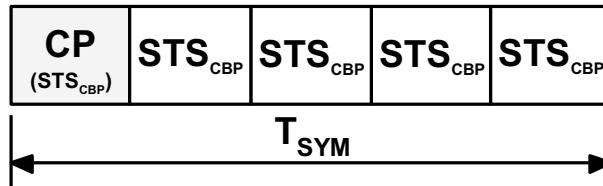


**Figure 135 — Frame preamble format using LTS**

#### 9.4.1.4 CBP preamble

The CBP preamble shall have a duration of 1 OFDM symbol and it shall be composed of five short training sequences ( $STS_{CBP}$ ). The  $STS_{CBP}$  is generated as described in 9.4.1.1.1 with  $S_{233}(0:209) = P_{REF}^{ST}(233:442)$  and  $S_{22}(0:209) = P_{REF}^{ST}(22:231)$ . These shifts generate a preamble that has low cross-correlation with the superframe preamble. The sequences  $S_{233}(0:209)$  and  $S_{22}(0:209)$  are the first 210 bits of the following sequences in hex format (bit order from left to right):

$S_{233}(0:209) = 2939C5D0D3EC56F36BB65B724B8E5E8D6137C4AF1942307BF5AB0$   
 $S_{22}(0:209) = 33444F0EBE9A9D9D22C790A3E7A8A618821F82A067F754B31BBD8$



**Figure 136 — CBP preamble format using a short training sequence**

The coefficients of the 2048 frequency elements to be presented at the input of the inverse DFT are then formed from the above two sequences using the following equation where  $N_T$  represents the number of used subcarriers (see Table 201):

$$P_{ST}(k) = \begin{cases} \sqrt{\frac{N_T}{420}} S_{233}\left(\frac{k+840}{4}\right), & -840 \leq k \leq -4, k \bmod 4 = 0 \\ \sqrt{\frac{N_T}{420}} S_{22}\left(\frac{k-4}{4}\right), & 4 \leq k \leq 840, k \bmod 4 = 0 \\ 0 & \text{otherwise} \end{cases} \quad (4)$$

and results in the short training sequence ( $STS_{CBP}$ ) as shown below:

$$P_{ST}(-1024:-841) = \{0, 0, 0, 0, 0, \dots, 0, 0, 0, 0, 0\}$$

$$P_{ST}(-840:-1) = \sqrt{\frac{N_T}{420}} \{-1, 0, 0, 0, -1, 0, 0, 0, 1, 0, 0, 0, -1, 0, 0, 0, 1, 0, 0, 0, \dots, 1, 0, 0, 0, -1, 0, 0, 0, -1, 0, 0, 0, -1, 0, 0, 0, -1, 0, 0, 0\}$$

$$P_{ST}(0) = 0$$

$$P_{ST}(1:840) = \sqrt{\frac{N_T}{420}} \{0, 0, 0, -1, 0, 0, 0, -1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, \dots, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, -1, 0, 0, -1, 0, 0, 0, -1\}$$

$$P_{ST}(841:1023) = \{0, 0, 0, 0, 0, \dots, 0, 0, 0, 0, 0\}$$

Taking the inverse DFT of the above sequence will generate 4 repetitions of a 512-sample sequence in the time domain. The factor  $\sqrt{\frac{N_T}{420}}$  is used to normalize the signal energy, where NT represents the number of used subcarriers.

#### 9.4.2 Control header and MAP definitions

##### 9.4.2.1 Superframe Control header (SCH)

The field definitions of the SCH are provided in 7.5.1. The length shall be one OFDM symbol.

The SCH shall be transmitted using the PHY mode 2 (see Table 202) and  $T_{CP} = 1/4T_{FFT}$ . The SCH shall be decoded by all the CPEs associated with that BS (or in the region of that BS).

The SCH is transmitted over all 60 subchannels using all 1440 data subcarriers. The 240 pilot subcarrier indices of the SCH shall be:  $\{-840, -833, -826, \dots, -21, -14, -7, 1, 8, 15, \dots, 820, 827, 834\}$  for the first symbol of the frame (i.e., the FCH symbol or the SCH of the first frame of the superframe belonging to the WRAN cell). The pilot pattern is defined in 9.6.1. The rest of the active subcarriers are then designated as data subcarriers.

The length of the SCH is 45 bytes and is encoded by a rate: 1/2 convolutional coder to give 720 coded bits. These coded bits are then interleaved according to Table 206. The output of the interleaver is mapped to 360 QPSK symbols,  $D_1$  to  $D_{360}$ . These 360 symbols are then mapped to the 1440 data carriers, skipping the pilot subcarriers, as follows:

$$\begin{aligned} D_1:D_6 &= S_{-839}:S_{-834} = S_{-419}:S_{-414} = S_2:S_7 = S_{422}S_{427} \\ D_7:D_{12} &= S_{-832}:S_{-827} = S_{-412}:S_{-407} = S_9:S_{14} = S_{429}S_{434} \\ D_{13}:D_{18} &= S_{-825}:S_{-820} = S_{-405}:S_{-400} = S_{16}:S_{21} = S_{436}:S_{441} \\ \dots \\ D_{355}:D_{360} &= S_{-426}:S_{-421} = S_{-6}:S_{-1} = S_{415}:S_{420} = S_{835}:S_{840} \end{aligned}$$

$S_k$  represents the symbol on  $k^{\text{th}}$  data subcarrier. Thus each data symbol  $D_k$  is spread over four data subcarriers for added robustness.

##### 9.4.2.2 Frame control header (FCH)

The frame control header is transmitted as part of the downstream PDU in the DS subframe. The length of the FCH shall be 3 bytes and contain information as specified in 7.5.2. The FCH shall be sent in the first subchannel of the symbol immediately following the frame preamble symbol except when it is the first frame of a superframe belonging to a specific BS where this symbol will follow the SCH. This second symbol of the frame carrying the FCH shall use a cyclic prefix  $T_{CP}=1/4 T_{FFT}$ .

The FCH shall be encoded using the binary convolutional channel coding specified in 9.7.2.1.1. The FCH shall be transmitted using the PHY mode 5 listed in Table 202. The 15-bit randomizer is initialized using the 15 LSBs of the BS ID. The BS ID is transmitted as part of the SCH and is thus available to the CPEs for

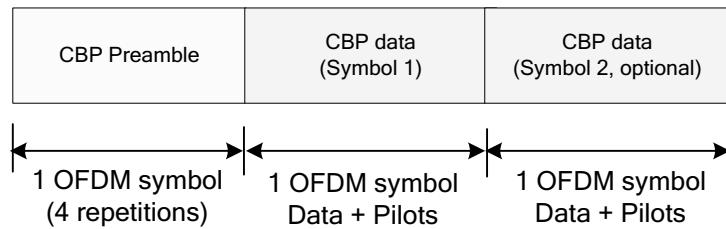
decoding. The 24 FCH bits are encoded and mapped onto 24 data subcarriers (note that the subcarrier allocation for FCH is as defined in 9.6.2). In order to increase the robustness of the FCH, as signaled in the SCH, the encoded and mapped FCH data may be transmitted using the PHY mode 4 listed in Table 202. The FCH then occupies the first two OFDM slots.

#### 9.4.2.3 DS-MAP, US-MAP, DCD, and UCD

The length of the DS-MAP PDU is variable and is defined in the FCH (7.5.2). Note that if the DS-MAP PDU is not present, this length will be that of the US-MAP PDU. This PDU shall be encoded using the binary convolutional channel coding specified in 9.7.2.1.1 and transmitted using the PHY mode 5 listed in Table 202 in the logical subchannel immediately following the FCH. If the DS-MAP is present, the length of the US-MAP, DCD and UCD, when present, shall be specified at the beginning of the DS-MAP in that order. The number of subchannels required to transmit these fields shall be determined by their respective lengths in number of OFDM slots. These fields shall be transmitted using PHY mode 5. If this number exceeds the number of subchannels allocated per symbol, the transmission of these PDUs will continue in the next symbol starting with the first logical subchannel. The unused subchannels in the last symbol of the frame header shall be used for DS transmissions.

### 9.5 CBP packet format

The format of the CBP packet is shown in Figure 137. The CBP packet consists of a preamble portion and a data portion. The CBP preamble is one OFDM symbol in duration and is generated as described in 9.4.1.4. The CBP data portion can be either one or two OFDM symbols in duration. The length field in the first symbol enables a receiver to determine the presence or absence of the second data symbol.



**Figure 137 — CBP packet format**

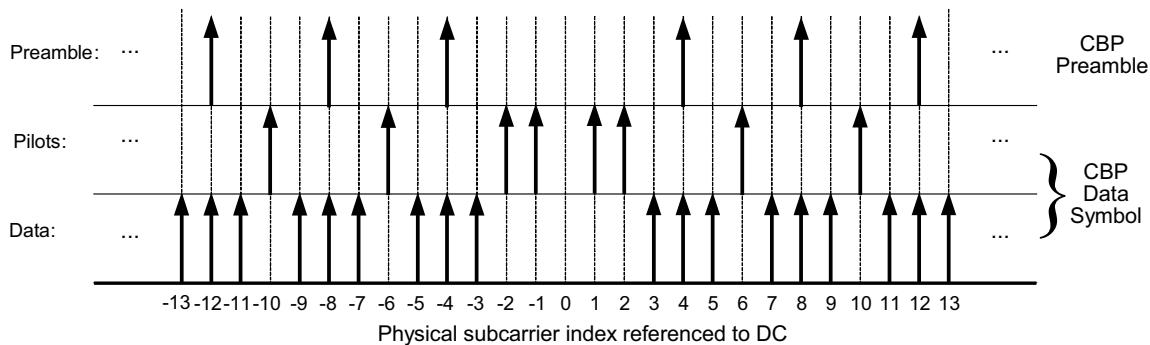
The CBP preamble consists of four repetitions of a short training sequence. A receiver may use the first two short training sequences in this field for acquisition and AGC setting and the next two short training sequences for frequency offset estimation. The CBP data symbols consist of the data and the pilot subcarriers. From the 1680 used subcarriers, 426 subcarriers are designated as pilot subcarriers and the remaining 1254 subcarriers are designated as data subcarriers.

The location of the non-zero subcarriers in the CBP preamble and the location of pilot and data subcarriers in the CBP data symbols are given below and shown pictorially in Figure 138.

*Location of non-zero subcarriers in the CBP preamble symbol:* (-840, -836, -832, -828, ..., -12, -8, -4, 4, 8, 12, 16, ..., 832, 836, 840)

*Location of 426 pilot subcarriers in the data portion:* (-840, -839, -838, -834, -830, -826, ..., -10, -6, -2, -1, 1, 2, 6, 10, ..., 830, 834, 838, 839, 840)

*Location of 1254 data subcarriers in the data portion:* (-837, -836, -835), (-833, -832, -831), (-829, -828, -827), ..., (-9, -8, -7), (-5, -4, -3), (3, 4, 5), (7, 8, 9), (11, 12, 13), ... (831, 832, 833), (835, 836, 837).

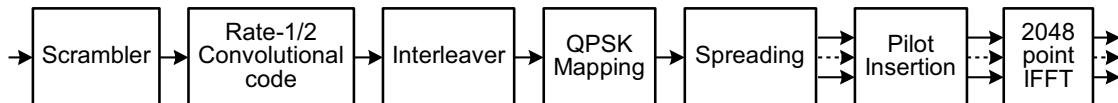


**Figure 138 — Subcarrier definition for CBP preamble and data symbols**

The pilot signals in the CBP packet shall be BPSK modulated, as described in 9.8.2, by a pseudo random binary sequence to avoid the generation of spectral line frequencies. The polynomial for the PRBS generator shall be the same as that used for the data scrambler, as defined in 9.7.1. The PRBS generator shall be initialized by the same seed value, 0 1 1 0 1 1 1 0 0 0 1 0 1 0 1, starting with the MSB on the left. The first 426 bits of the sequence shall be used for pilot modulation in the first OFDMA symbol, while the next 426 bits shall be used for pilot modulation in the second OFDMA symbol. The first OFDMA symbol starts after the preamble in every CBP packet.

### 9.5.1 Encoding of CBP data

Figure 139 shows a simplified block diagram of the CBP data encoder and mapper.



**Figure 139 — Encoding steps for CBP data**

The CBP payload is first processed by the scrambler, which is functionally the same as the data scrambler (see 9.7.1). The scrambler shall be initialized for each CBP payload with the same initialization vector as for the PSDU data (see 9.7.1). The scrambled CBP payload is divided into blocks of 418 bits before encoding and mapping. Unlike for a data burst, OFDM slot concatenation (see 9.7.2.1.3) is not used for the CBP payload. Each block of 418 bits shall be first encoded using a rate: 1/2 convolutional code (see 9.7.2.1.1) with tail biting resulting in 836 encoded bits. To do this, the convolutional coder has to be initialized with the last 6 bits of each block to be encoded. After interleaving of the encoded bits by a bit interleaver with interleaving size of 836 bits (see 9.6.5), the bits are then mapped using the QPSK constellation (see Figure 150), resulting in 418 QPSK symbols. Each of these QPSK symbols is transmitted on three subcarriers in order to provide additional frequency diversity. The spreading function is described by the following equation:

$$\begin{bmatrix} S_i \\ S_{i+418} \\ S_{i+836} \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \begin{bmatrix} D_i \\ D_{i+418} \\ D_{i+836} \end{bmatrix} \quad i = 0, 1, 2, \dots, 417 \quad (5)$$

Where  $D_i$  represents the  $i^{\text{th}}$  QPSK symbol and  $S_k$  represents the symbol on the  $k^{\text{th}}$  data subcarrier. The 1254 spread symbols are inserted in their corresponding locations as described above. This will result in symbol  $S_0$  being inserted in frequency bin -837, symbol  $S_1$  in frequency bin -836, symbol  $S_2$  in frequency bin -835, symbol  $S_3$  in frequency bin -833, etc. The 426 pilot symbols are then inserted in their designated

frequency bins. The resultant vector is then transformed into the time domain using an IFFT module. The length of cyclic prefix for the CBP packet symbols is  $T_{CP} = 1/4 T_{FFT}$ .

A WRAN receiver can combine the pilot subcarriers of the CBP data symbols with those of the preamble symbols to perform better interpolation to derive channel estimates. These channel estimates can then be used to equalize the CBP data symbols. The receiver can also use maximal ratio combining (MRC) to de-spread the data symbols. The use of soft-decision Viterbi decoding is recommended.

## 9.6 OFDM subcarrier allocation

Among the 2048 subcarriers in each OFDM symbol, 384 subcarriers are null subcarriers (left guard band, right guard band and DC subcarriers) with 0 amplitude and 0 phase. The remaining 1680 subcarriers, which are partitioned into 60 subchannels, are for pilot and data. A subchannel is composed of 28 subcarriers (24 data and 4 pilot subcarriers). A subchannel is the basic unit used for subcarrier allocation in both downstream and upstream.

In the downstream, the 240 pilot values are allocated first. A sequence of 1440 complex data values generated by the constellation mapper is interleaved using the Turbo-Like Interleaving (TLI) algorithm described in 9.6.2. These interleaved values are then allocated to the 1440 data subcarriers.

In the upstream, the first six logical subchannels, which are usually reserved for opportunistic or scheduled control signaling, use a set of regularly spaced subcarriers with physical mapping as specified in 9.6.4. The US-MAP may also assign up to 10 additional subchannels for such opportunistic signaling (see Table 35). Among the remaining subchannels, the subchannels allocated to a CPE are assigned with pilot values and data from the constellation mapper. Other subchannels are assigned with 0 amplitude and 0 phase at the CPE. The 1512 assigned values are interleaved using the TLI algorithm described in 9.6.2. These interleaved values are then allocated to the 1512 remaining subcarriers.

### 9.6.1 Pilot pattern

The pilot insertion pattern is shown in Figure 140. The pilot pattern shall be repeated every 7 OFDM symbols and 7 subcarriers in the time and frequency domains, respectively. The pilot pattern is always the same, independent of the channel bandwidth. The pilot pattern shall also be the same for the downstream and upstream. In the downstream, the pilots do not participate in the interleaving procedure, and the physical representation of the pilots in the time and frequency domains follows the same pattern as shown in Figure 140 except for the subcarrier index. The following physical pilot indices,  $P_k$ , after the last frame preamble in every downstream subframe, shall be used instead of the logical indices 0, 1, ..., 6.

$$P_k = -840 + 7k + \text{pilot\_subcarrier\_offset} + \text{DC\_flag} \quad k = 0, 1, 2, \dots, 239 \quad (6)$$

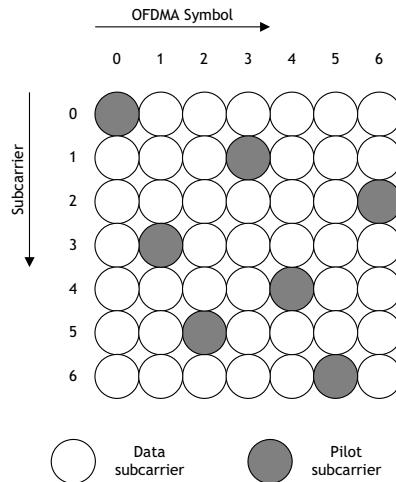
where:

$k$  is the running subcarrier index from 0 to 239

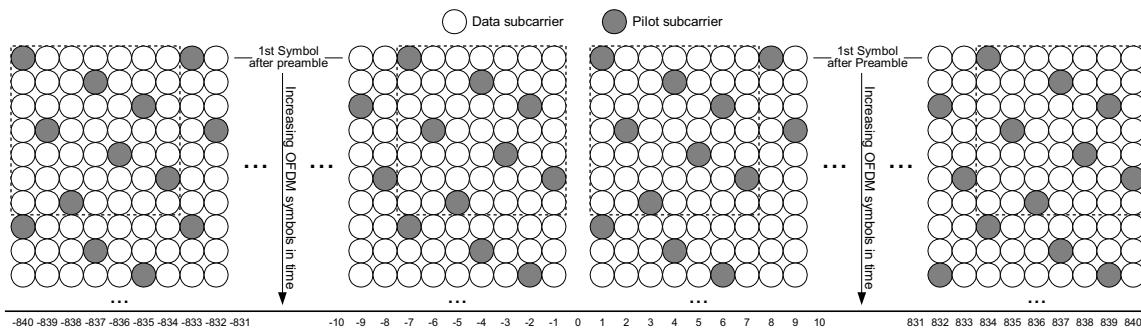
$\text{pilot\_subcarrier\_offset}$  is the subcarrier offset to control the beginning of first pilot subcarrier within each OFDM symbol. The  $\text{pilot\_subcarrier\_offset}$  is 0, 3, 5, 1, 4, 6, and 2 for  $(\text{OFDMA\_symbol\_index mod } 7) = 0, 1, 2, 3, 4, 5$ , and 6, respectively. The OFDMA symbol of index 0 should be the first OFDMA symbol in every downstream or upstream subframes.

$\text{DC\_flag}$  is used to count the DC subcarrier in the calculation of pilot subcarrier index. When  $k$  is equal or larger than 120, the value is set to 1.

In the upstream, the pilots participate in the interleaving procedure, they will not have the same spacing after the interleaving process, and their physical representation will be different from Figure 140. These pilot subcarriers should be used by both BS and CPE for robust channel estimation and tracking against frequency offset and phase noise. Note that the pattern described in this subclause does not apply to the CBP packet.



**Figure 140 — Repetition unit of the pilot pattern**  
(in the logical domain before interleaving)



**Figure 141 — Physical location of the downstream pilot subcarriers**

In both downstream and upstream, the pilot subcarriers shall be BPSK modulated, as described in 9.8.2, by a pseudo random binary sequence to avoid the generation of line spectral frequencies. The polynomial for the PRBS generator shall be the same as that used for the data scrambler, as defined in 9.7.1. The PRBS generator shall be initialized by the same seed value, 0 1 1 0 1 1 1 0 0 0 1 0 1 0 1, starting with the MSB on the left. The first 240 bits of the sequence shall be used for pilot modulation in the first OFDM symbol, while the next 240 bits shall be used for pilot modulation in the second OFDM symbol, and so on. The first OFDM symbol starts after the frame preamble in every downstream subframe, while the first OFDMA symbol starts from the initial OFDMA symbol in every upstream burst.

### 9.6.2 Turbo-Like Interleaving (TLI) algorithm

The TLI algorithm uses four parameters  $K$ ,  $p$ ,  $q$ , and  $j$  to generate a permutation rule  $L(k)$ .  $K$  is the interleaving block size,  $p$  and  $q$  are integers, and  $j$  specifies the number of iterative calculations in the algorithm.

For both subcarrier interleaving and bit interleaving, an input sequence is interleaved to generate an output sequence. After the interleaving, the value at index  $L(k)$  in the input sequence is relocated to index  $k$  in the output sequence. In other words, index  $L(k)$  in the input sequence corresponds to index  $k$  ( $k = 0, \dots, K-1$ ) in the output sequence.

Let  $I_{p,q,K}^{(0)}(k) = k$  denote the initial index pattern, i.e., the index pattern of the input sequence. The algorithm iteratively updates the index pattern. At the output of iteration  $m$ , the index pattern can be calculated as

$$I_{p,q,K}^{(m)} = \left[ K - p + k + q \cdot p \cdot \left[ -k - p \cdot I_{p,q,K}^{(m-1)}(k) \right] \bmod K \right] \bmod K. \quad (7)$$

After  $j$  iterations, the  $j^{\text{th}}$  iteration output index pattern is used as the permutation rule:  $L(k) = I_{p,q,K}^{(j)}(k)$ .

The performance of  $L(k)$  is characterized by the interleaving spreading depth  $\Delta L(\Delta k)$ . For any indices  $k$  and  $k+\Delta k$  in the output sequence,  $\Delta L(\Delta k)$  represents the minimum distance between the corresponding indices  $L(k)$  and  $L(k+\Delta k)$  in the input sequence.  $\Delta L(\Delta k)$  can be calculated as:

$$\Delta L(\Delta k) = \min_{0 \leq k \leq K-1} |L(k + \Delta k) - L(k)| \quad (8)$$

The interleaving parameters  $\{p, q, j\}$  have been set to maximize the interleaving spreading depth  $\Delta L(\Delta k)$  for small values of  $\Delta k$ .

### 9.6.3 Downstream subcarrier allocation

For each symbol in the downstream, every 4 pilot values and every 24 complex data from the constellation mapper are assigned to a subchannel. For example, subchannel 1 is constituted of pilot values at indices 0, ..., 3 and complex data values at indices 0, ..., 23; subchannel 2 is constituted of pilot values at indices 4, ..., 7 and complex data values at indices 24, ..., 47.

The pilot values shall be directly allocated (without interleaving) to pilot subcarriers following the pilot pattern defined in 9.6.1. A sequence of 1440 complex data from the constellation mapper shall first be interleaved, and then the interleaved data sequence shall be allocated to the data subcarriers sequentially.

The permutation rule  $L(k)$  used for the interleaving shall be determined using the TLI algorithm described in 9.6.2 with the parameters  $\{K, p, q, j\} = \{1440, 32, 2, 3\}$  (as specified in Table 206). Index  $L(k)$  in the constellation mapper output data sequence shall correspond to index  $k$  in the interleaved data sequence. For illustration, Table 204 shows the relationship between the constellation mapper output sequence and the interleaved sequence for subchannels 1, 2 and 3. In the table, the constellation mapper output sequence is the input; the interleaved sequence is the output.

**Table 204 —Interleaving patterns for subchannels 1, 2, and 3 in the downstream**

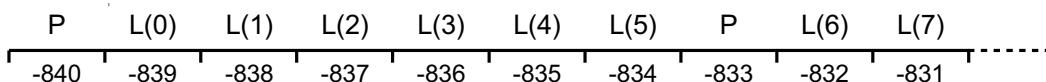
Subchannel 1		Subchannel 2		Subchannel 3	
Input index	Output index	Input index	Output index	Input index	Output index
0	673	24	985	48	985
1	386	25	698	49	698
2	99	26	411	50	411

Subchannel 1		Subchannel 2		Subchannel 3	
Input index	Output index	Input index	Output index	Input index	Output index
3	1252	27	124	51	124
4	965	28	1277	52	1277
5	678	29	990	53	990
6	391	30	703	54	703
7	104	31	416	55	416
8	1257	32	129	56	129
9	970	33	1282	57	1282
10	683	34	995	58	995
11	396	35	708	59	708
12	109	36	421	60	421
13	1262	37	134	61	134
14	975	38	1287	62	1287
15	688	39	1000	63	1000
16	401	40	713	64	713
17	114	41	426	65	426
18	1267	42	139	66	139
19	980	43	1292	67	1292
20	693	44	1005	68	1005
21	406	45	718	69	718
22	119	46	431	70	431
23	1272	47	144	71	144

The subcarrier allocation in the downstream is performed using the following procedure:

- All null subcarriers are first allocated.
- The pilot values are allocated to the pilot subcarriers following the pilot pattern described in 9.6.1.
- $K=1440$  complex values from the constellation mapper are interleaved using the TLI algorithm with parameters  $\{K,p,q,j\}=\{1440,32,2,3\}$ .
- The interleaved data sequence is allocated sequentially to the remaining subcarriers.

Figure 142 shows an example allocation for the first OFDM symbol in a burst, where P is a pilot subcarrier, and L(x) represents an index in the constellation mapper output data sequence.



**Figure 142 — Example allocation for the first OFDMA symbol in a burst**

#### 9.6.4 Upstream Subcarrier allocation

In the upstream, the first six subchannels, which are usually reserved for opportunistic or scheduled control signaling (i.e., Ranging/BW request/UCS notification bursts, see 9.9.3), use the pre-determined regular subcarrier indices specified below. When these subchannels are not used for control signaling, they can be used for data. In such case, the pilot subcarriers are logically allocated as shown in Figure 140. The remaining regularly spaced subcarriers are then sequentially assigned with data values from the constellation mapper.

All the subcarriers in the subchannels not assigned to the CPE shall be assigned 0 amplitude and 0 phase at the CPE. For each subchannel assigned to the CPE, 4 associated pilot values shall be assigned and 24 complex data from the constellation mapper shall be assigned following the pattern specified in 9.6.1.

Among the 240 pilot values, every 4 pilot values are associated with a subchannel. For example, pilot values at indices 0, ..., 3 are associated with subchannel 1, pilot values at indices 4, ..., 7 are associated with subchannel 2, and so on. However, if a subchannel is used for CDMA opportunistic signaling, its pilot values normally associated with this subchannel are not used. Every 24 complex data values from the constellation mapper are assigned to a subchannel. The assignment follows the pattern specified in 9.6.1.

Within each subchannel assigned to the CPE, the 4 pilot values shall be inserted following the pilot pattern described in 9.6.1. Then complex data values shall be sequentially allocated to the remaining 24 logical subcarriers.

While the logical subcarriers in the six first subchannels are allocated to regularly spaced physical subcarriers after interleaving among these 168 subcarriers as indicated in Table 206, interleaving shall be performed on the subcarriers in the remaining 54 subchannels, that is for the remaining 1512 subcarriers as indicated in Table 206. The interleaved sequence shall be allocated sequentially to the 1512 remaining physical subcarriers in the symbol. In other words, each subchannel is mapped to a group of 28 physical subcarriers following the interleaving scheme described below.

The permutation rule L(k) used for interleaving shall be determined using the TLI algorithm described in 9.6.2 with the parameters {K,p,q,j}={1512,2,5,5} (as specified in Table 206). Index L(k) in the interleaver input sequence shall correspond to index k in the interleaver output sequence. Table 205 shows the relationship between the interleaver input sequence and the interleaver output sequence for subchannels 7 and 8 with the pilot allocation shown for the first symbol of the upstream subframe. In the table,  $P_i$  represents the  $i^{\text{th}}$  pilot value,  $D_{j,k}$  represents the  $k^{\text{th}}$  data value in the group of 24 data values (obtained from the constellation mapper) allocated to subchannel j.

**Table 205 — Example of interleaving patterns in the upstream for the first symbol of the interleaved subchannels 7 and 8**

Subchannel 7			Subchannel 8		
Input index	Value	Output index	Input index	Value	Output index
0	$P_0$	479	28	$P_4$	171
1	$D_{3,0}$	90	29	$D_{4,0}$	1294
2	$D_{3,1}$	1213	30	$D_{4,1}$	905
3	$D_{3,2}$	824	31	$D_{4,2}$	516
4	$D_{3,3}$	435	32	$D_{4,3}$	127
5	$D_{3,4}$	46	33	$D_{4,4}$	1250
6	$D_{3,5}$	1169	34	$D_{4,5}$	861
7	$P_1$	780	35	$P_5$	472
8	$D_{3,6}$	391	36	$D_{4,6}$	83
9	$D_{3,7}$	2	37	$D_{4,7}$	1206
10	$D_{3,8}$	1125	38	$D_{4,8}$	817
11	$D_{3,9}$	736	39	$D_{4,9}$	428
12	$D_{3,10}$	347	40	$D_{4,10}$	39
13	$D_{3,11}$	1470	41	$D_{4,11}$	1162
14	$P_2$	1081	42	$P_6$	773
15	$D_{3,12}$	692	43	$D_{4,12}$	384
16	$D_{3,13}$	303	44	$D_{4,13}$	1507
17	$D_{3,14}$	1426	45	$D_{4,14}$	1118

Subchannel 7			Subchannel 8		
Input index	Value	Output index	Input index	Value	Output index
18	$D_{3,15}$	1037	46	$D_{4,15}$	729
19	$D_{3,16}$	648	47	$D_{4,16}$	340
20	$D_{3,17}$	259	48	$D_{4,17}$	1463
21	$P_3$	1382	49	$P_7$	1074
22	$D_{3,18}$	993	50	$D_{4,18}$	685
23	$D_{3,19}$	604	51	$D_{4,19}$	296
24	$D_{3,20}$	215	52	$D_{4,20}$	1419
25	$D_{3,21}$	1338	53	$D_{4,21}$	1030
26	$D_{3,22}$	949	54	$D_{4,22}$	641
27	$D_{3,23}$	560	55	$D_{4,23}$	252

The subcarrier allocation in the upstream shall be performed using the following procedure:

- 1) All null subcarriers and the DC subcarrier are first allocated with 0 amplitude and 0 phase.
- 2) The 168 subcarriers of the six first subchannels, which are usually reserved for “Ranging/BW requests/UCS notification,” are allocated using the following subcarrier indices:  $\{-840, -830, -820, \dots, -20, -10, 10, 20, \dots, 820, 830, 840\}$ . In the case where the US-MAP indicates that any of these six first subchannels are assigned to the CPE for data transmission, the pilot subcarriers are logically allocated as shown in 9.6.1 as a function of the symbol order in the upstream subframe. The remaining regularly spaced subcarriers are then sequentially assigned with data values from the constellation mapper.
- 3) For each subchannel allocated to the CPE among the remaining 54 subchannels, the 4 associated pilot values are logically inserted following the pilot pattern described in 9.6.1 as a function of the symbol order in the upstream subframe. Complex data values from the constellation mapper are then sequentially allocated to the remaining 24 logical subcarriers. Note that in the upstream, a CPE is assigned 7 or more symbols that can span one or more subchannels, and data values are inserted into the same subchannel on a symbol by symbol basis (over all assigned symbols) before the next subchannel is used. If the US-MAP indicates that more than 6 subchannels are assigned for “Ranging/BW request/UCS notification,” the logical subcarriers for these subchannels shall be allocated accordingly.
- 4) All the subcarriers of the remaining subchannels are allocated with 0 amplitude and 0 phase.
- 5) The 168 logical subcarriers assigned to the first 6 subchannels are interleaved using the TLI algorithm with parameters  $\{K,p,q,j\}=\{168,4,2,2\}$ .
- 6) The 1512 assigned logical subcarriers are interleaved using the TLI algorithm with parameters  $\{K,p,q,j\}=\{1512,2,5,5\}$ .
- 7) The interleaved sequence is allocated sequentially to the remaining 1512 subcarriers.

**Table 206 —Interleaving parameters for the downstream and upstream subcarrier mapping allocation**

	Interleaving depth	Interleaving parameters		
<b>DS</b>	K	p	q	j
	1440	32	2	3
<b>US</b>	K	p	q	j
	1512	2	5	5
	K	p	q	j
	168	4	2	2
<b>SCH</b>	K	p	q	j
	720	12	2	1
<b>CBP burst</b>	K	p	q	j
	836	22	2	2

### 9.6.5 Bit interleaving

The Turbo-Like Interleaving algorithm described in 9.6.2 shall be used to interleave the data bits at the output of the channel coding procedure to generate an interleaved bit sequence. The index L(k) in the bit sequence at the output of the channel coding procedure shall correspond to the index k in the interleaved bit sequence.

Table 207 provides the supported block sizes, sets of interleaving parameters {p,q,j} as well as informative indication on the interleaving spreading depth  $\Delta L(\Delta k)$  for some  $\Delta k$  values.

**Table 207 — Interleaving pattern description**

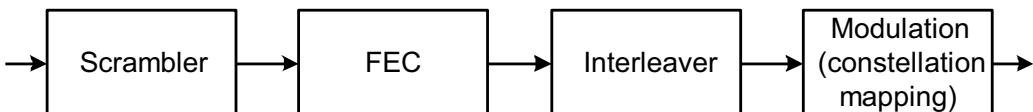
Coded block	Interleaver parameters		
	p	q	j
48	16	2	2
96	3	2	3
144	6	2	3
192	3	2	3
240	6	2	3
288	3	2	3
336	16	2	3
384	6	2	3
432	18	2	1

Coded block	Interleaver parameters		
	p	q	j
480	16	2	3
528	6	2	3
576	36	2	1
672	3	2	2
720	12	2	1
768	3	2	3
836	22	2	2
864	48	2	1
960	6	2	3
1008	36	2	1
1056	16	2	3
1152	36	2	1
1248	3	2	2
1344	6	2	3
1440	40	2	2
1536	6	2	3
1632	3	2	3
1680	40	2	2
1728	36	2	1
1824	48	2	1
1920	48	2	1
2016	16	2	3
2112	16	2	3
2208	3	2	3
2304	16	2	3

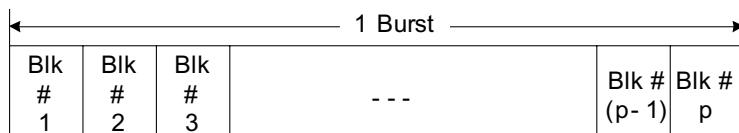
## 9.7 Channel coding

Channel coding includes data scrambling, binary convolutional coding or advanced coding, puncturing in the case of BCC and CTC, bit interleaving and constellation mapping. Figure 143 shows the mandatory channel coding process. The channel coder processes the control headers and the PSDU portion of the PPDU. The channel coder shall not process the preamble part of the PPDU.

For the purpose of channel coding, each data burst is further subdivided into data blocks as shown in Figure 144. Each block of encoded data will be mapped and transmitted on one or more OFDM slots.



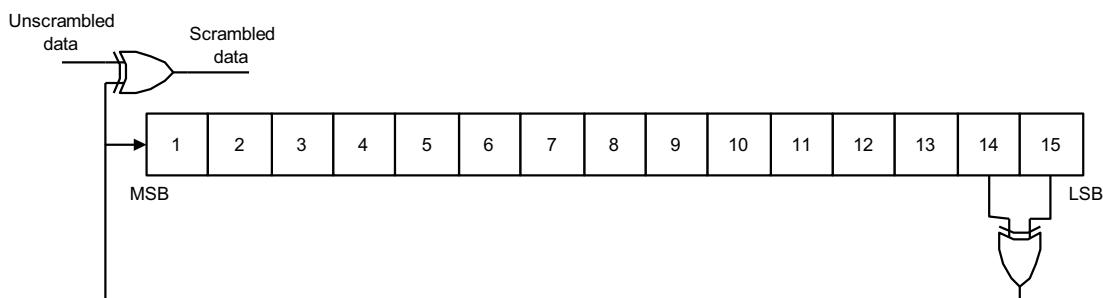
**Figure 143 — Channel coding process**



**Figure 144 — Partitioning of a data burst into data blocks**

### 9.7.1 Data scrambling

The PSDU data is first processed by the data scrambler using a pseudo random binary sequence (PRBS) generator. The PRBS generator polynomial is  $1 + X^{14} + X^{15}$  and is shown in Figure 145. The preamble and the control header fields of the PPDU shall not be scrambled. The data scrambler is initialized on each burst with 011011100010101, starting with the MSB on the left. The generation of the initialization vector for control headers is described in 9.4.2. The pad bits, if present, shall be scrambled.



**Figure 145 — Pseudo random binary sequence generator for data scrambler**

### 9.7.2 Forward Error Correction (FEC)

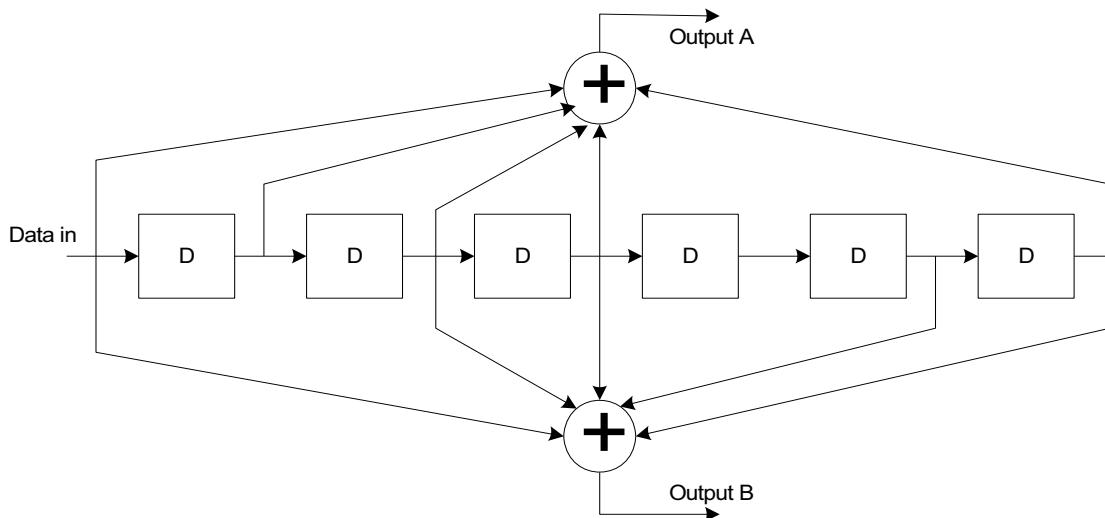
The binary convolutional code is mandatory and there are three additional optional modes.

#### 9.7.2.1 Binary Convolutional code (BCC) mode (mandatory)

##### 9.7.2.1.1 Binary convolutional coding

The data burst is encoded using a rate: 1/2 binary convolutional encoder. The constraint length of this coder is equal to 7 and its generator polynomials are 171<sub>o</sub> and 133<sub>o</sub> for outputs A and B respectively. Figure 146 is a graphical description of the generator polynomials. Output A and output B represent the first and second output bits respectively of this encoder.

The convolutional coder shall be initialized at the beginning of the control headers and at the beginning of each PSDU data block. Tail biting shall be used with both control headers and the PSDU data. This implies that for the case of control headers, the encoder memory is initialized with the last 6 bits in the headers and for the case of PSDU data, the encoder memory is initialized with the last 6 bits in each PSDU data burst.



**Figure 146 — Rate: 1/2 convolutional coder with generator polynomials 171o, 133o**  
(The delay element represents a delay of 1 bit.)

#### 9.7.2.1.2 Puncturing

Different coding rates can be obtained by puncturing the output of the convolutional coder. Table 208 shows the different rates that can be derived from the output of the rate: 1/2 convolutional coder and the associated puncturing patterns.

Decoding by using Viterbi algorithm is recommended. At the receiver, zeros are inserted in the locations of the punctured bits before the Viterbi decoder.

**Table 208 — Puncturing and bit-insertion for the different coding rates**

Code rate	1/2	2/3	3/4	5/6
<b>Convolutional coder output</b>	A <sub>1</sub> B <sub>1</sub>	A <sub>1</sub> B <sub>1</sub> A <sub>2</sub> B <sub>2</sub>	A <sub>1</sub> B <sub>1</sub> A <sub>2</sub> B <sub>2</sub> A <sub>3</sub> B <sub>3</sub>	A <sub>1</sub> B <sub>1</sub> A <sub>2</sub> B <sub>2</sub> A <sub>3</sub> B <sub>3</sub> A <sub>4</sub> B <sub>4</sub> A <sub>5</sub> B <sub>5</sub>
<b>Puncturer output/bit-inserter input</b>	A <sub>1</sub> B <sub>1</sub>	A <sub>1</sub> B <sub>1</sub> B <sub>2</sub>	A <sub>1</sub> B <sub>1</sub> B <sub>2</sub> A <sub>3</sub>	A <sub>1</sub> B <sub>1</sub> B <sub>2</sub> A <sub>3</sub> B <sub>4</sub> A <sub>5</sub>
<b>Decoder input</b>	A <sub>1</sub> B <sub>1</sub>	A <sub>1</sub> B <sub>1</sub> 0B <sub>2</sub>	A <sub>1</sub> B <sub>1</sub> 0B <sub>2</sub> A <sub>3</sub> 0	A <sub>1</sub> B <sub>1</sub> 0B <sub>2</sub> A <sub>3</sub> 00B <sub>4</sub> A <sub>5</sub> 0

#### 9.7.2.1.3 OFDM slot concatenation

The encoding block size shall depend on the number of OFDM slots allocated and the modulation specified for the current transmission. Concatenation of a number of OFDM slots shall be performed in order to allow for transmission of larger blocks of coding where it is possible, with the limitation of not exceeding the largest block size for the corresponding modulation and coding. Table 209 specifies the concatenation index for different modulations and coding.

For any modulation and coding, the following parameters are defined:

- j: index dependent on the modulation level and FEC rate
- n: number of allocated OFDM slots
- k: floor (n / j)
- m: n mod j

Table 210 shows the rules used for OFDM slot concatenation.

**Table 209 — Concatenation index for different modulations and coding**

Modulation and Rate	j
QPSK 1/2	12
QPSK 2/3	9
QPSK 3/4	8
QPSK 5/6	7
16-QAM 1/2	6
16-QAM 2/3	4
16-QAM 3/4	4
16-QAM 5/6	3
64-QAM 1/2	4
64-QAM 2/3	3
64-QAM 3/4	2
64-QAM 5/6	2

**Table 210 — OFDM slot concatenation rule**

Number of OFDM slots	Concatenated slots
$n \leq j$	1 block of n slots
$n > j$	If ( $n \bmod j = 0$ ) k blocks of j slots else ( $k-1$ ) blocks of j slots 1 block of $\text{ceil}((m+j)/2)$ slots 1 block of $\text{floor}((m+j)/2)$ slots

Table 211 defines the basic sizes of the useful data payloads (in bytes) to be encoded in relation with the selected modulation type, encoding rate, and concatenation rule.

**Table 211 — Useful data payload in bytes for an FEC block**

QPSK				16-QAM				64-QAM			
R=1/2	R=2/3	R=3/4	R=5/6	R=1/2	R=2/3	R=3/4	R=5/6	R=1/2	R=2/3	R=3/4	R=5/6
3											
	4										
		5									
6				6							
	8				8						
9		9				9		9			
			10				10				
12	12			12					12		
15			15							15	
	16				16						
18		18		18		18		18			
	20		20				20				
21											
24	24			24	24				24		
			25								
27		27				27		27		27	
	28										

QPSK				16-QAM				64-QAM			
R=1/2	R=2/3	R=3/4	R=5/6	R=1/2	R=2/3	R=3/4	R=5/6	R=1/2	R=2/3	R=3/4	R=5/6
30			30	30			30				30
	32				32						
33											
			35								
36	36	36		36		36		36	36		

### 9.7.2.2 Duo-binary convolutional Turbo code (CTC) mode (optional)

#### 9.7.2.2.1 Duo-binary convolutional turbo coding

The Duo-binary Turbo Code is illustrated in Figure 147. It uses a Circular Recursive Systematic Convolutional (CRSC) Code as component codes, with double-binary input.

The bits of the data to be encoded are alternately fed to inputs A and B, starting with the MSB of the first byte being fed to A. The encoding system is fed by blocks of k bits or N couples ( $k=2 \times N$ ). N is a multiple of 4 (k is a multiple of 8).

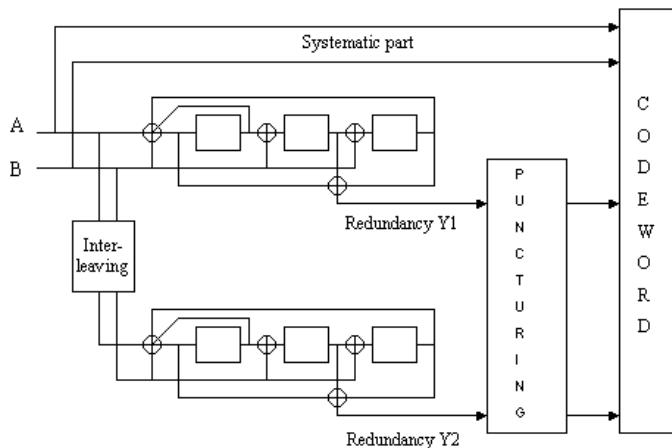


Figure 147 — Duo-binary convolutional turbo code: Encoding scheme

The polynomials, which shall be used for the connections, are described in octal and symbolic notations as follows:

- For the feedback branch: 15 (in octal), equivalently  $1+D+D^3$  (in symbolic notation)
- For the Y1 and Y2 parity bits, 13, equivalently  $1+D^2+D^3$

The input A shall be connected to tap “1” of the shift register and the input “B” shall be connected to the input taps “1,” D, and  $D^2$ .

This first encoding is called C1 encoding. After initialization by the circulation state  $S_{c_1}$ , the encoder shall be fed by the sequence in the natural order with incremental address  $i = 0, \dots, N-1$ .

This second encoding is called C2 encoding. After initialization by the circulation state  $S_{c_2}$ , the encoder shall be fed by the interleaved sequence with incremental address  $j = 0, \dots, N-1$ .

The permuting function that gives the natural address  $i$  of the considered couple, when reading it at place  $j$  for the second encoding, is given in 9.7.2.2.2.

### 9.7.2.2.2 CTC interleaver

In the CTC interleaver, the permutation shall be done on two levels:

- The first one inside the couples (**level 1**)
- The second one between couples (**level 2**)

The permutation is described in the following algorithm.

- Set the permutation parameters  $P_0$ ,  $P_1$ ,  $P_2$  and  $P_3$ . These parameters depend on the size of the sequence to be encoded. Table 212 gives the block size, code rates, and code parameters for the different modulation and coding schemes. Optimized code parameters are given for data block sizes up to 240 bytes.
- $j = 0, \dots, N-1$ .
- **level 1**
  - if  $j \bmod 2 = 0$ , let  $(A,B) = (B,A)$  (invert the couple)
- **level 2**
  - if  $j \bmod 4 = 0$ , then  $P = 0$ ;
  - if  $j \bmod 4 = 1$ , then  $P = N/2 + P_1$ ;
  - if  $j \bmod 4 = 2$ , then  $P = P_2$ ;
  - if  $j \bmod 4 = 3$ , then  $P = N/2 + P_3$ .
  - $i = P_0:j + P + 1 \bmod N$

**Table 212 — Code parameters for the different modulation and coding schemes**

Data block size (byte)	Encoded data block size (bytes)								N	P0	P1	P2	P3						
	QPSK		16-QAM		64-QAM														
	1/2	3/4	1/2	3/4	1/2	2/3	3/4	5/6											
6	12	—	—	—	—	—	—	—	24	5	0	0	0	0					
9	—	12	—	—	—	—	—	—	36	11	18	0	18	0					
12	24	—	24	—	—	—	—	—	48	13	24	0	24	0					
18	36	24	—	24	36	—	—	—	72	11	6	0	6	0					
20	—	—	—	—	—	—	—	—	80	13	4	40	20	0					
24	48	—	48	—	—	36	—	—	96	7	48	24	72	0					
27	—	36	—	—	—	—	36	—	108	11	54	56	2	0					
30	60	—	—	—	—	—	—	36	120	13	60	0	60	0					
36	72	48	72	48	72	—	—	—	144	17	74	72	2	0					
41	—	—	—	—	—	—	—	—	164	19	18	20	122	0					
45	—	60	—	—	—	—	—	—	180	11	90	0	90	0					
48	96	—	96	—	—	72	—	—	192	11	96	48	144	0					
54	108	72	—	72	108	—	72	—	216	13	108	0	108	0					
60	120	—	120	—	—	—	—	72	240	13	120	60	180	0					
66	132	—	—	—	—	—	—	—	264	23	2	160	30	0					
72	144	96	144	96	144	108	—	—	288	23	50	188	50	0					
78	156	—	—	—	—	—	—	—	312	23	102	64	38	0					

Data block size (byte)	Encoded data block size (bytes)								N	P0	P1	P2	P3					
	QPSK		16-QAM		64-QAM													
	1/2	3/4	1/2	3/4	1/2	2/3	3/4	5/6										
81	—	108	—	—	—	—	108	—	324	11	172	164	16					
83	—	—	—	—	—	—	—	—	332	23	96	160	32					
90	180	120	—	120	180	—	—	108	360	29	56	0	68					
96	192	—	192	—	—	144	—	—	384	29	68	140	56					
99	—	132	—	—	—	—	—	—	396	29	36	128	76					
102	204	—	—	—	—	—	—	—	408	29	124	204	40					
108	216	144	216	144	216	—	144	—	432	13	0	4	8					
114	228	—	—	—	—	—	—	—	456	31	100	224	104					
117	—	156	—	—	—	—	—	—	468	31	98	220	98					
120	240	—	240	—	—	180	—	144	480	31	52	240	52					
132	264	—	264	—	—	—	—	—	528	31	24	36	104					
135	—	180	—	—	—	—	180	—	540	31	42	248	34					
138	276	—	—	—	—	—	—	—	552	35	14	136	6					
144	288	192	288	192	288	216	—	—	576	31	42	232	18					
150	300	—	—	—	—	—	—	180	600	37	20	152	0					
153	—	204	—	—	—	—	—	—	612	37	6	164	14					
156	312	—	312	—	—	—	—	—	624	37	312	156	468					
162	324	216	—	216	324	—	216	—	648	37	62	160	34					
171	—	228	—	—	—	—	—	—	684	37	108	136	8					
174	348	—	—	—	—	—	—	—	696	37	0	128	12					
180	360	240	360	240	360	—	—	216	720	37	92	100	68					
186	372	—	—	—	—	—	—	—	744	37	54	196	50					
192	384	—	384	—	—	288	—	—	768	19	384	216	600					
198	396	264	—	264	396	—	—	—	792	41	0	228	24					
204	408	—	408	—	—	—	—	—	816	37	408	204	612					
207	—	276	—	—	—	—	—	—	828	41	136	288	192					
216	432	288	432	288	432	324	288	—	864	19	2	16	6					
222	444	—	—	—	—	—	—	—	888	43	10	220	18					
225	—	300	—	—	—	—	—	—	900	43	8	56	20					
228	456	—	456	—	—	—	—	—	912	43	96	8	124					
234	468	312	—	312	468	—	—	—	936	43	120	140	124					
240	480	—	480	—	—	360	—	288	960	43	52	120	28					

### 9.7.2.2.3 Determination of the circulation states

The state of the encoder is denoted  $S$  ( $0 \leq S \leq 7$ ) with  $S = 4 \cdot s_1 + 2 \cdot s_2 + s_3$  (see Table 213). The circulation states  $S_{c_1}$  and  $S_{c_2}$  shall be determined by the following operations:

- Initialize the encoder with state 0. Encode the sequence in the natural order for the determination of  $S_{c_1}$  or in the interleaved order for the determination of  $S_{c_2}$  (without producing redundancy). In both cases, the final state of the encoder is denoted  $S_{N-1}^0$ .

- According to the length  $N$  of the sequence, the following correspondence shall be used to find  $S_{c_1}$  and  $S_{c_2}$  (see Table 213).

**Table 213 — Circulation state correspondence table**

$S_{N-1}^0$ $N \bmod 7$	0	1	2	3	4	5	6	7
1	Sc=0	Sc=6	Sc=4	Sc=2	Sc=7	Sc=1	Sc=3	Sc=5
2	Sc=0	Sc=3	Sc=7	Sc=4	Sc=5	Sc=6	Sc=2	Sc=1
3	Sc=0	Sc=5	Sc=3	Sc=6	Sc=2	Sc=7	Sc=1	Sc=4
4	Sc=0	Sc=4	Sc=1	Sc=5	Sc=6	Sc=2	Sc=7	Sc=3
5	Sc=0	Sc=2	Sc=5	Sc=7	Sc=1	Sc=3	Sc=4	Sc=6
6	Sc=0	Sc=7	Sc=6	Sc=1	Sc=3	Sc=4	Sc=5	Sc=2

#### 9.7.2.2.4 Code rate and puncturing

Four code rates are defined to match those defined for the convolution code:  $R = 1/2, 2/3, 3/4$  and  $5/6$ . These rates shall be achieved through selectively deleting or puncturing the parity bits. The puncturing pattern defined in Table 214 shall be applied to the outputs of both codes C1 and C2 (in parallel). The puncturing algorithm holds even when the number of couples is not a multiple of 10, for rate:  $5/6$ , or a multiple of 12 for rates:  $1/2, 2/3$ , and  $3/4$ . This is illustrated more specifically in the following example. A two-byte input (16 bits) to the encoder would produce 16 redundancy bits, 8 bits from Y1, and 8 bits from Y2 (refer to Figure 147). These two sets of 8 bits are punctured separately. Using a rate of  $3/4$  puncturing vector would yield 2 sets of 3 bits, totaling 6 redundancy bits. Thus the output would be  $16 + 6 = 22$  coded bits. Using a rate:  $5/6$ , the puncturing vector would yield two sets of 2 bits, totaling in 4 redundancy bits. Thus the output would be  $16 + 4 = 20$  coded bits.

**Table 214 — Puncturing patterns for turbo codes (“1”= keep, “0”= puncture)**

Code Rate	Puncturing vector
1/2	$Y = [1 \ 1 \ 1 \ 1 \ 1 \ 1]$
2/3	$Y = [1 \ 0 \ 1 \ 0 \ 1 \ 0]$
3/4	$Y = [1 \ 0 \ 0 \ 1 \ 0 \ 0]$
5/6	$Y = [1 \ 0 \ 0 \ 0 \ 0]$

#### 9.7.2.2.5 Block concatenation

The concatenation scheme of the CTC blocks is defined to allow data block sizes of up to 240 bytes. The rules to be used with the concatenation scheme are defined fully in Table 215, Table 216, and Table 217. This is used for OFDM subchannelization with QPSK, 16-QAM and 64-QAM. Table 217 defines shortening and puncturing patterns needed for supporting block sizes with a multiplicative factor of 7. Table 217 shall be used when the number of allocated OFDM slots,  $n$ , corresponds to transmitted blocks of size 336, 672, 1008, 1344, 1680, and 2016 bits.

**Table 215 — CTC Encoding subchannel concatenation**

Modulation and rate	j	L
QPSK, rate: 1/2	j = 80	L=1
QPSK, rate: 3/4	j = 52	L=1
16-QAM, rate: 1/2	j = 40	L=2
16-QAM, rate: 3/4	j = 26	L=2
64-QAM, rate: 1/2	j = 26	L=3
64-QAM, rate: 2/3	j = 20	L=3
64-QAM, rate: 3/4	j = 16	L=3
64-QAM, rate: 5/6	j = 16	L=3

**Table 216 — Block fitting for n (number OFDM slots) equal to a multiple of 7**

Rate	Trans mitted (bits)	Ideal Data Size (bits)	Ideal Data Size (bytes)	Supporte d block size (bytes)	Input size to encoder (bits)	Data Payload (bits)	After encoder (bits)	Shorte ned (bits)	Padding (bits)	Punctu ring (bits)	Data Payload (bytes)
1/2	<b>336</b>	168	21	20	160	160	320	0	16	0	20
2/3	<b>336</b>	224	28	27	216	216	324	0	12	0	27
3/4	<b>336</b>	252	31.5	31	248	248	332	0	4	0	31
5/6	<b>336</b>	280	35	36	288	280	346	8	0	2	35
1/2	<b>672</b>	336	42	41	328	328	656	0	16	0	41
2/3	<b>672</b>	448	56	55	440	440	660	0	12	0	55
3/4	<b>672</b>	504	63	64	512	504	684	8	0	4	63
5/6	<b>672</b>	560	70	69	552	552	664	0	8	0	69
1/2	<b>1008</b>	504	63	64	512	504	1024	8	0	8	63
2/3	<b>1008</b>	672	84	83	664	664	996	0	12	0	83
3/4	<b>1008</b>	756	94.5	96	768	752	1024	16	0	0	94
5/6	<b>1008</b>	840	105	106	848	840	1018	8	0	2	105
1/2	<b>1344</b>	672	84	83	664	664	1328	0	16	0	83
2/3	<b>1344</b>	896	112	110	880	880	1320	0	24	0	110
3/4	<b>1344</b>	1008	126	128	1024	1008	1366	16	0	6	126
5/6	<b>1344</b>	1120	140	138	1104	1104	1326	0	18	0	138
1/2	<b>1680</b>	840	105	106	848	840	1696	8	0	8	105
2/3	<b>1680</b>	1120	140	138	1104	1104	1656	0	24	0	138
3/4	<b>1680</b>	1260	157.5	156	1248	1248	1664	0	16	0	156
5/6	<b>1680</b>	1400	175	174	1392	1392	1672	0	8	0	174
1/2	<b>2016</b>	1008	126	128	1024	1008	2048	16	0	16	126
2/3	<b>2016</b>	1344	168	171	1368	1344	2052	24	0	12	168
3/4	<b>2016</b>	1512	189	190	1520	1512	2028	8	0	4	189
5/6	<b>2016</b>	1680	210	212	1696	1680	2036	16	0	4	210

**Table 217 — Subchannel concatenation rule for CTC**

Number of OFDM slots	Subchannels concatenated
$n \leq j$ AND $n \bmod 7 \neq 0$	1 block of $n$ slots
$n \leq j$ AND $n \bmod 7 = 0$ , AND $n > 42/L$	1 block of $4n/7$ slots 1 block of $3n/7$ slots
$n > j$	If ( $n \bmod j = 0$ ) $q$ blocks of $j$ slots else ( $q-1$ ) blocks of $j$ slots 1 block of $L_{b1}$ slots 1 block of $L_{b2}$ slots Where: $q = n \bmod j$ $L_{b1} = \text{ceil}((n-(q-1);j)/2)$ $L_{b2} = \text{floor}((n-(q-1);j)/2)$ If ( $L_{b1} \bmod 7 = 0$ ) or ( $L_{b2} \bmod 7 = 0$ ) $L_{b1} = L_{b1} + 1$ ; $L_{b2} = L_{b2} - 1$

### 9.7.2.3 Low-density parity check codes (LDPC) mode (optional)

#### 9.7.2.3.1 Code description

The LDPC code is based on a set of fundamental LDPC codes. Each of the fundamental codes is a systematic linear block code. Using the methods described in 9.7.2.3.2, the fundamental codes can accommodate various code rates and packet sizes.

Each LDPC code in the set of LDPC codes is defined by a parity-check matrix  $\mathbf{H}$  of size  $m$ -by- $n$ , where  $n$  is the length of the code and  $m$  is the number of parity check bits in the code. The number of systematic bits is  $k = n - m$ .

The matrix  $\mathbf{H}$  is defined as

$$\mathbf{H} = \begin{bmatrix} \mathbf{P}_{0,0} & \mathbf{P}_{0,1} & \mathbf{P}_{0,2} & \cdots & \mathbf{P}_{0,n_b-2} & \mathbf{P}_{0,n_b-1} \\ \mathbf{P}_{1,0} & \mathbf{P}_{1,1} & \mathbf{P}_{1,2} & \cdots & \mathbf{P}_{1,n_b-2} & \mathbf{P}_{1,n_b-1} \\ \mathbf{P}_{2,0} & \mathbf{P}_{2,1} & \mathbf{P}_{2,2} & \cdots & \mathbf{P}_{2,n_b-2} & \mathbf{P}_{2,n_b-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ \mathbf{P}_{m_b-1,0} & \mathbf{P}_{m_b-1,1} & \mathbf{P}_{m_b-1,2} & \cdots & \mathbf{P}_{m_b-1,n_b-2} & \mathbf{P}_{m_b-1,n_b-1} \end{bmatrix} = \mathbf{P}^{H_b}$$

where  $\mathbf{P}_{ij}$  is one of a set of  $z$ -by- $z$  permutation matrices or a  $z$ -by- $z$  zero matrix. The matrix  $\mathbf{H}$  is expanded from a binary base matrix  $\mathbf{H}_b$  of size  $m_b$ -by- $n_b$ , where  $n = z \times n_b$  and  $m = z \times m_b$ , with integer  $z \geq 1$ . The base matrix is expanded by replacing each 1 in the base matrix with a  $z$ -by- $z$  permutation matrix, and each 0 with a  $z$ -by- $z$  zero matrix. The base matrix size  $n_b$  is equal to 24.

The permutations used are circular right shifts, and the set of permutation matrices contains the  $z \times z$  identity matrix and circular right shifted versions of the identity matrix. Because each permutation matrix is specified by a single circular right shift, the binary base matrix information and permutation replacement information can be combined into a single compact model matrix  $\mathbf{H}_{bm}$ . The model matrix  $\mathbf{H}_{bm}$  has the same size as the binary base matrix  $\mathbf{H}_b$ , with each binary entry  $(i,j)$  of the base matrix  $\mathbf{H}_b$  replaced to create the model matrix  $\mathbf{H}_{bm}$ . Each 0 in  $\mathbf{H}_b$  is replaced by a blank or negative value (e.g., by -1) to denote a  $z \times z$  all-zero matrix, and each 1 in  $\mathbf{H}_b$  is replaced by a circular shift size  $p(i,j) \geq 0$ . The model matrix  $\mathbf{H}_{bm}$  can then be directly expanded to  $\mathbf{H}$ .

$\mathbf{H}_b$  is partitioned into two sections, where  $\mathbf{H}_{b1}$  corresponds to the systematic bits and  $\mathbf{H}_{b2}$  corresponds to the parity-check bits, such that  $\mathbf{H}_b = \left[ \begin{array}{c|c} (\mathbf{H}_{b1})_{m_b \times k_b} & (\mathbf{H}_{b2})_{m_b \times m_b} \end{array} \right]$ .

Section  $\mathbf{H}_{b2}$  is further partitioned into two sections, where vector  $\mathbf{h}_b$  has odd weight, and  $\mathbf{H}'_{b2}$  has a dual-diagonal structure with matrix elements at row  $i$ , column  $j$  equal to 1 for  $i=j$ , 1 for  $i=j+1$ , and 0 elsewhere:

$$\mathbf{H}_{b2} = \left[ \mathbf{h}_b \mid \mathbf{H}'_{b2} \right] = \left[ \begin{array}{c|ccc} h_b(0) & 1 & & \\ h_b(1) & 1 & 1 & \mathbf{0} \\ \cdot & 1 & \ddots & \\ \cdot & \ddots & \ddots & 1 \\ \cdot & \mathbf{0} & 1 & 1 \\ h_b(m_b-1) & & & 1 \end{array} \right]. \quad (8)$$

The base matrix has  $h_b(0) = 1$ ,  $h_b(m_b-1) = 1$ , and a third value  $h_b(j)$ ,  $0 < j < (m_b - 1)$  equals to 1. The base matrix structure avoids having columns with multiple weights of value 1 in the expanded matrix.

In particular, the non-zero sub-matrices are circularly right shifted by a particular circular shift value. Each “1” in  $\mathbf{H}'_{b2}$  is assigned a shift size of 0, and is replaced by a  $z \times z$  identity matrix when expanding to  $\mathbf{H}$ . The two 1s located at the top and the bottom of  $\mathbf{h}_b$  are assigned shift sizes equal to 0, and the third 1 in the middle of  $\mathbf{h}_b$  is given an unpaired shift size greater than 0.

A base model matrix is defined for the largest code length ( $n = 2304$ ) of each code rate. The set of shifts  $\{p(i,j)\}$  in the base model matrix are used to determine the shift sizes for all other code lengths of the same code rate. Each base model matrix has  $n_b = 24$  columns, and the expansion factor  $z_f$  is equal to  $n/24$  for code length  $n$ . Here  $f$  is the index of the code lengths for a given code rate,  $f = 0, 1, 2, \dots, 20$ . For code length  $n = 2304$  the expansion factor is designated  $z_0 = 96$ .

For each code rate, the shift sizes  $\{p(f, i, j)\}$  for a code size corresponding to expansion factor  $z_f$  are derived from  $\{p(i,j)\}$  by scaling  $p(i,j)$  proportionally,

$$p(f, i, j) = \begin{cases} p(i, j), & p(i, j) \leq 0 \\ \frac{p(i, j)z_f}{z_0}, & p(i, j) > 0 \end{cases}, \quad (9)$$

where  $\lfloor x \rfloor$  denotes the flooring function which gives the nearest integer towards  $-\infty$ .

Rate 1/2 code:

```

-1 94 73 -1 -1 -1 -1 1 55 83 -1 -1 7 0 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1
-1 27 -1 -1 -1 22 79 9 -1 -1 12 -1 0 0 -1 -1 -1 -1 -1 -1 -1 -1 -1
-1 -1 -1 24 22 81 -1 33 -1 -1 -1 0 -1 -1 0 0 -1 -1 -1 -1 -1 -1 -1
61 -1 47 -1 -1 -1 -1 65 25 -1 -1 -1 -1 0 0 -1 -1 -1 -1 -1 -1 -1
-1 -1 39 -1 -1 -1 84 -1 -1 41 72 -1 -1 -1 -1 0 0 -1 -1 -1 -1 -1 -1
-1 -1 -1 -1 46 40 -1 82 -1 -1 -1 79 0 -1 -1 -1 0 0 -1 -1 -1 -1 -1
-1 -1 95 53 -1 -1 -1 -1 14 18 -1 -1 -1 -1 -1 0 0 -1 -1 -1 -1 -1 -1
-1 11 73 -1 -1 -1 2 -1 -1 47 -1 -1 -1 -1 -1 -1 0 0 -1 -1 -1 -1 -1
12 -1 -1 -1 83 24 -1 43 -1 -1 -1 51 -1 -1 -1 -1 -1 -1 0 0 -1 -1
-1 -1 -1 -1 94 -1 59 -1 -1 70 72 -1 -1 -1 -1 -1 -1 -1 0 0 -1
-1 -1 7 65 -1 -1 -1 -1 39 49 -1 -1 -1 -1 -1 -1 -1 -1 -1 0 0
43 -1 -1 -1 -1 66 -1 41 -1 -1 -1 26 7 -1 -1 -1 -1 -1 -1 -1 -1 -1 0

```

Note that the R=1/2 code is designed such that after a model matrix row permutation of [0, 2, 4, 11, 6, 8, 10, 1, 3, 5, 7, 9], consecutive rows do not intersect. This may be used to increase decoding throughput in some layered decoding architectures.

Rate 2/3 code:

```
2 -1 19 -1 47 -1 48 -1 36 -1 82 -1 47 -1 15 -1 95 0 -1 -1 -1 -1 -1  
-1 69 -1 88 -1 33 -1 3 -1 16 -1 37 -1 40 -1 48 -1 0 0 -1 -1 -1 -1  
10 -1 86 -1 62 -1 28 -1 85 -1 16 -1 34 -1 73 -1 -1 -1 0 0 -1 -1 -1  
-1 28 -1 32 -1 81 -1 27 -1 88 -1 5 -1 56 -1 37 -1 -1 -1 0 0 -1 -1 -1  
23 -1 29 -1 15 -1 30 -1 66 -1 24 -1 50 -1 62 -1 -1 -1 -1 0 0 -1 -1  
-1 30 -1 65 -1 54 -1 14 -1 0 -1 30 -1 74 -1 0 -1 -1 -1 -1 0 0 0 -1  
32 -1 0 -1 15 -1 56 -1 85 -1 5 -1 6 -1 52 -1 0 -1 -1 -1 -1 0 0  
-1 0 -1 47 -1 13 -1 61 -1 84 -1 55 -1 78 -1 41 95 -1 -1 -1 -1 -1 0
```

Note that the R=2/3 code is designed such that after a model matrix row permutation of [0, 3, 6, 1, 4, 7, 2, 5], consecutive rows do not intersect. This may be used to increase decoding throughput in some layered decoding architectures.

Rate 3/4 code:

```
6 38 3 93 -1 -1 -1 30 70 -1 86 -1 37 38 4 11 -1 46 48 0 -1 -1 -1 -1  
62 94 19 84 -1 92 78 -1 15 -1 -1 92 -1 45 24 32 30 -1 -1 0 0 -1 -1 -1  
71 -1 55 -1 12 66 45 79 -1 78 -1 -1 10 -1 22 55 70 82 -1 -1 0 0 -1 -1  
38 61 -1 66 9 73 47 64 -1 39 61 43 -1 -1 -1 -1 95 32 0 -1 -1 0 0 -1  
-1 -1 -1 -1 32 52 55 80 95 22 6 51 24 90 44 20 -1 -1 -1 -1 -1 0 0  
-1 63 31 88 20 -1 -1 -1 6 40 56 16 71 53 -1 -1 27 26 48 -1 -1 -1 -1 0
```

Rate 5/6 code:

```
1 25 55 -1 47 4 -1 91 84 8 86 52 82 33 5 0 36 20 4 77 80 0 -1 -1  
-1 6 -1 36 40 47 12 79 47 -1 41 21 12 71 14 72 0 44 49 0 0 0 0 -1  
51 81 83 4 67 -1 21 -1 31 24 91 61 81 9 86 78 60 88 67 15 -1 -1 0 0  
50 -1 50 15 -1 36 13 10 11 20 53 90 29 92 57 30 84 92 11 66 80 -1 -1 0
```

### 9.7.2.3.2 Code rate and block size adjustment

The LDPC code flexibly supports different block sizes for each code rate through the use of an expansion factor as shown in Table 218. Each base model matrix has  $n_b = 24$  columns and the expansion factor ( $z$  factor) is equal to  $n/3$  for code length  $n$ . In each case, the number of information bits is equal to the code rate times the coded length  $n$ .

**Table 218 — LDPC Encoded Block Sizes, Z factor and Code Rates**

$n$ encoded bits	Encoded bytes	$z$ factor	$k$ (data bytes)				Number of OFDM slots		
			R=1/2	R=2/3	R=3/4	R=5/6	QPSK	16-QAM	64-QAM
384	48	16	24	32	36	40	8	4	—
480	60	20	30	40	45	50	10	5	—
576	72	24	36	48	54	60	12	6	4
672	84	28	42	56	63	70	14	7	—
768	96	32	48	64	72	80	16	8	—

<b><i>n</i> encoded bits</b>	<b>Encoded bytes</b>	<b><i>z</i> factor</b>	<b><i>k</i> (data bytes)</b>				<b>Number of OFDM slots</b>		
			<b>R=1/2</b>	<b>R=2/3</b>	<b>R=3/4</b>	<b>R=5/6</b>	<b>QPSK</b>	<b>16-QAM</b>	<b>64-QAM</b>
864	108	36	54	72	81	90	18	9	6
960	120	40	60	80	90	100	20	10	—
1056	132	44	66	88	99	110	22	11	—
1152	144	48	72	96	108	120	24	12	8
1248	156	52	78	104	117	130	26	13	—
1344	168	56	84	112	126	140	28	14	—
1440	180	60	90	120	135	150	30	15	10
1536	192	64	96	128	144	160	32	16	—
1632	204	68	102	136	153	170	34	17	—
1728	216	72	108	144	162	180	36	18	12
1824	228	76	114	152	171	190	38	19	—
1920	240	80	120	160	180	200	40	20	—
2016	252	84	126	168	189	210	42	21	14
2112	264	88	132	176	198	220	44	22	—
2208	276	92	138	184	207	230	46	23	—
2304	288	96	144	192	216	240	48	24	16

### 9.7.2.3.3 Packet encoding

The encoding block size  $k$  shall depend on the number of OFDM slots allocated and the modulation specified for the current transmission. Concatenation of a number of OFDM slots shall be performed in order to make larger blocks of coding where it is possible, with the limitation of not exceeding the largest block under the same coding rate (the block defined by the 64-QAM modulation). Table 219 and Table 220 specify the concatenation of OFDM slots for different allocations and modulations.

For any modulation and FEC rate, given an allocation of  $N_{\text{slot}}$  OFDM slots, the following parameters can be defined:

- $j$ : modulation-dependent parameter
- $N_{\text{slot}}$ : number of allocated OFDM slots
- $F: \text{floor}(N_{\text{slot}}/j)$
- $M: N_{\text{slot}} \bmod j$

The parameter  $j$  for LDPC is determined as shown in Table 219:

**Table 219 — Parameter ‘j’ for LDPC**

<b><i>j</i></b>	<b>Modulation</b>
48	QPSK
24	16-QAM
16	64-QAM

**Table 220 — OFDM slot concatenation**

$N_{SLOT}$	<b>OFDM slots concatenated</b>
$N_{SLOT} \leq j$	1 block of $N_{SLOT}$ OFDM slots
$N_{SLOT} > j, M=0$	F blocks of $j$ OFDM slot
$N_{SLOT} > j, M>0$	(F – 1) blocks of $j$ OFDM slots 1 block of $\text{ceil}((M+j)/2)$ OFDM slots 1 block of $\text{floor}((M+j)/2)$ OFDM slots

Control information and packets that result in a codeword size  $n$  of less than 384 bits are encoded using BCC, with appropriate code rates and modulation orders, as described in 9.7.2.1.

#### 9.7.2.4 Shortened block turbo codes (SBTC) mode (optional)

The BTC is constructed by the product of two simple component codes, which are binary Hamming codes with a special design or parity check codes. Table 221 specifies the parity check matrix for the Hamming codes. Actually, all the columns of the parity check matrix for  $n = 7$  are the binary representation of integers 1 to 7 (the topmost part corresponds to the least-significant bit in the binary representation of an integer). Similarly, all the columns of the parity check matrix for  $n = 15, 31$  and  $63$  are the binary representation of integers 1 to 15, 1 to 31, and 1 to 63, respectively. Note that with this encoding scheme, the parity check bits are no longer located together at the end of the code word. In general, for a  $(2^m-1, 2^m-1-m)$  Hamming code with integer  $m$  larger than 2, the parity-check positions are located in columns numbered  $1, 2, 4 \dots 2^{m-1}$  of the parity check matrix. Both Hamming codes and extended Hamming codes may be used as component codes. To create extended Hamming codes, the overall even parity check bit is added at the end of each code word.

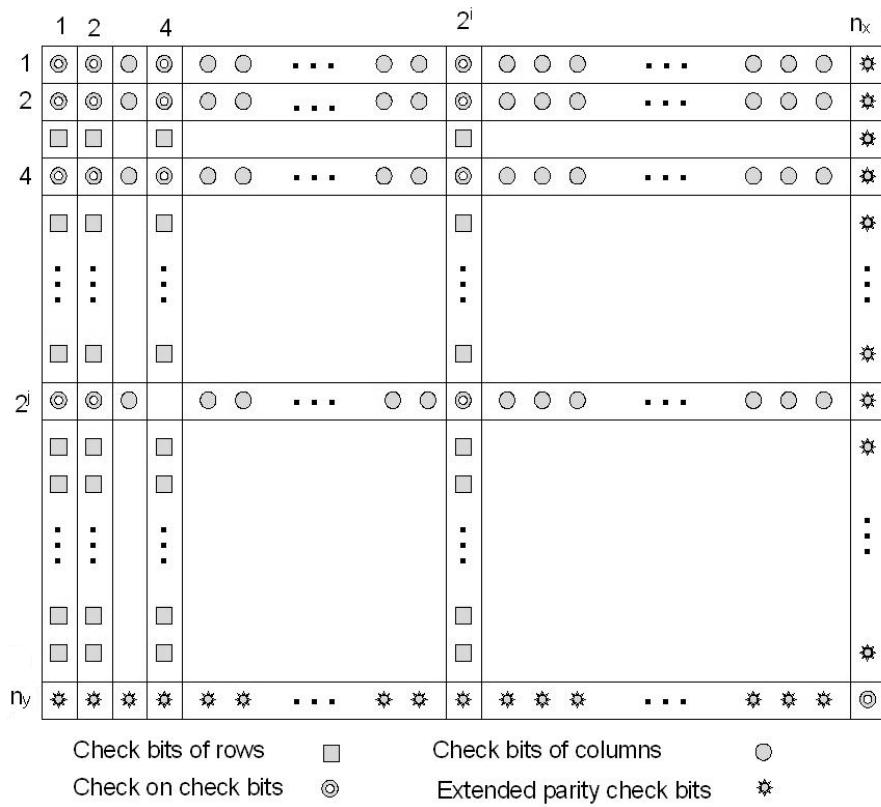
**Table 221 — Parity check matrix for the Hamming codes**

$n'$	$K'$	<b>Parity check matrix</b>
7	4	$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}_{3 \times 7}$
15	11	$\begin{bmatrix} 1 & 0 & 1 & \cdots & 1 & 0 & 1 \\ 0 & 1 & 1 & \cdots & 0 & 1 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 1 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 1 & 1 \end{bmatrix}_{4 \times 15}$
31	26	$\begin{bmatrix} 1 & 0 & 1 & \cdots & 1 & 0 & 1 \\ 0 & 1 & 1 & \cdots & 0 & 1 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 1 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 1 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 1 & 1 \end{bmatrix}_{5 \times 31}$

<b>n'</b>	<b>K'</b>	<b>Parity check matrix</b>
63	57	$\begin{bmatrix} 1 & 0 & 1 & \cdots & 1 & 0 & 1 \\ 0 & 1 & 1 & \cdots & 0 & 1 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 1 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 1 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 1 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 1 & 1 \end{bmatrix}_{6 \times 63}$

Several parameters are used to describe the BTC encoder.  $k_y$ ,  $n_y$  and  $k_x$ ,  $n_x$  are the number of information bits and codeword lengths for the vertical component code and the horizontal component code, respectively.  $I_x$ ,  $I_y$ , and  $D$ , as defined in Table 223, are used to construct the shortened BTC codes. With the aid of Figure 148, the procedure to construct BTC is listed as follows:

- Place  $(k_y, k_x)$  information bits in information area (the blank area in Figure 148). The information bits may be placed in columns with indexes from 1 to  $n_x - 1$ , except for columns  $2^i$  with  $i = 0, 1, 2, \dots, n_x - k_x - 2$  ( $n_x - k_x - 1$  parity check bits). Similarly, information bits may be located in rows with indexes 1 to  $n_y$  except for rows with indexes  $2^j$  with  $j = 0, 1, 2, \dots, n_y - k_y - 2$  ( $n_y - k_y - 1$  parity check bits).
- Compute the parity check bits of  $k_y$  rows using the corresponding parity check matrix in Table 221 and inserting them in the corresponding positions signed by  $\blacksquare$ .
- Compute the parity check bits of  $k_x$  columns using the corresponding parity check matrix in Table 221 and inserting them in the corresponding positions signed by  $\bullet$  and  $\circledcirc$ .
- Calculate and append the extended parity check bits to the corresponding rows and columns, if the component code of the row (or column) is an extended Hamming code.
- The overall block size of such a product code is  $n = n_x \times n_y$ , the total number of information bits  $k = k_x \times k_y$ , and the code rate is  $R = R_x \times R_y$ , where  $R_i = k_i/n_i$ ,  $i = x, y$ . The Hamming distance of the product code is  $d = d_x \times d_y$ . Data bit ordering for the composite BTC block is the first bit in the first row is the LSB and the last data bit in the last data row is the MSB.



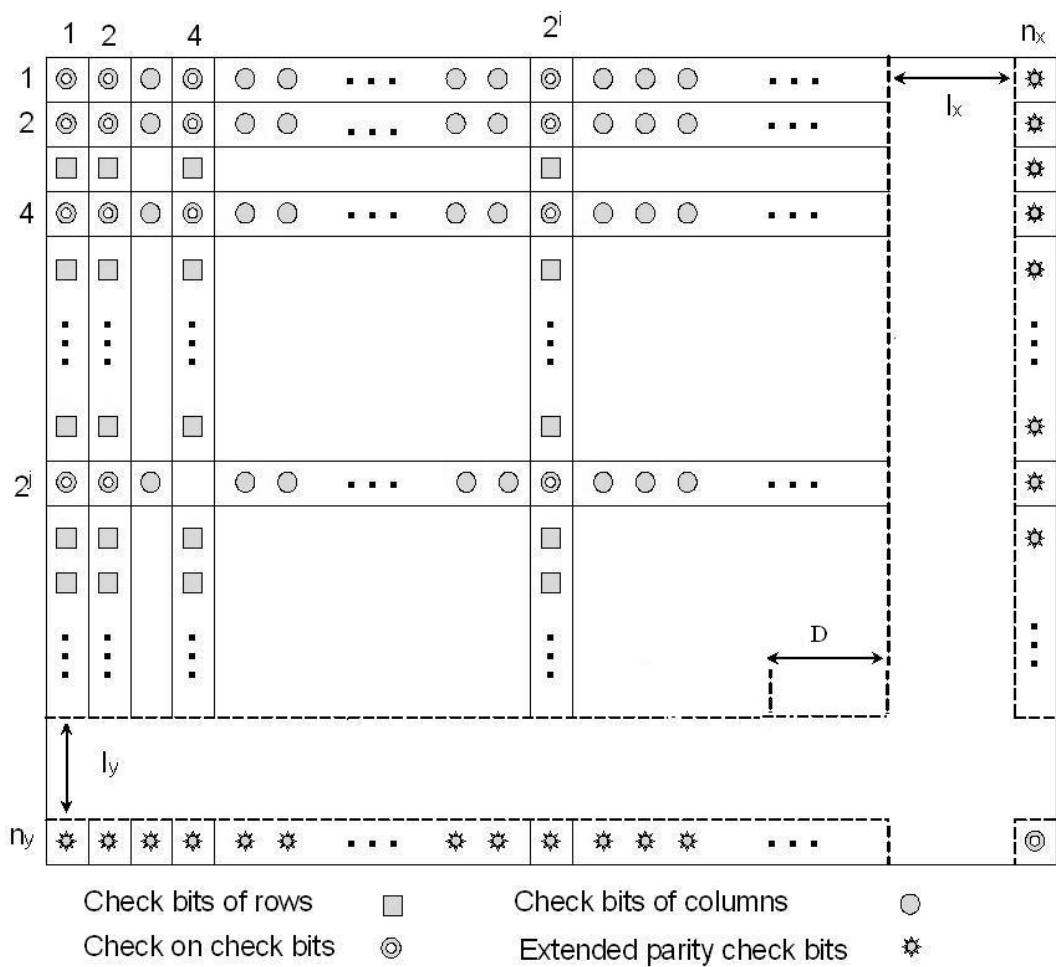
**Figure 148 — Block turbo code (BTC) structure**

Transmission of the block over the channel shall occur in a linear fashion, with all bits of the first row transmitted left to right followed by the second row, etc. To match a required packet size, BTC may be shortened by removing symbols from the BTC array. In the two-dimensional case, rows, columns, or parts thereof can be removed until the appropriate size is reached. There are two steps in the process of shortening product codes:

- Step 1) Remove  $I_x$  rows and  $I_y$  columns from the two-dimensional code. This is equivalent to shortening the component codes that make up the BTC.
- Step 2) Use if the size of data field of SBTC specified from Step (1) above is larger than the expected size. In this case, the D right LSBs are zero-filled by the encoder. After decoding at the receive end, the decoder shall strip off these unused bits and only the specified data payload is passed to the next higher level in the PHY. The same general method is used for shortening the last code word in a message where the available data bytes do not fill the available data bytes in a code block.

These two processes of code shortening are depicted in Figure 149. The new coded block length of the code is  $(n_x - I_x)(n_y - I_y)$ . The corresponding information length is given as  $(k_x - I_x)(k_y - I_y) - D$ . Consequently, the code rate is given by Equation (10).

$$R = \frac{(k_x - I_x)(k_y - I_y) - D}{(n_x - I_x)(n_y - I_y)} \quad (10)$$



**Figure 149 — Shortened BTC (SBTC) structure**

The basic sizes of the useful data payloads for different modulation types and encoding rates are displayed in Table 222. Table 223 gives the code parameters of SBTC for different data payload and coded block sizes.

**Table 222 — Useful data payload for one or multiple OFDM slots**

Modulation scheme	QPSK		16-QAM		64-QAM				Coded Bytes
	1/2	3/4	1/2	3/4	1/2	2/3	3/4	5/6	
Encoding Rate	3	—	—	—	—	—	—	—	6
Allowed Data (Bytes)	6	9	6	9	—	—	—	—	12
	9	—	—	—	9	12	—	15	18
	12	18	12	18	—	—	—	—	24
	15	—	—	—	—	—	—	—	30
	18	27	18	27	18	24	27	30	36
	21	—	—	—	—	—	—	—	42
	24	36	24	36	—	—	—	—	48

	27	—	—	—	27	36	—	45	54
30	45	30	45	—	—	—	—	—	60
33	—	—	—	—	—	—	—	—	66
36	54	36	54	36	48	54	60	72	

The encoding block size shall depend on the number of OFDM slots allocated and the modulation specified for the current transmission. Concatenation of a number of OFDM slots shall be performed in order to allow for transmission of larger blocks of coding where it is possible, with the limitation of not going beyond the largest block under the same coding rate. Table 224 specifies the concatenation of OFDM slots for different allocations and modulations. The parameters in Table 224 and Table 225 shall apply to the SBTC encoding scheme.

For any modulation and FEC rate, given an allocation of n OFDM slots, the following parameters are defined:

- j: parameter dependent on the modulation and FEC rates
- n: number of allocated OFDM slots
- k: floor (n/j)
- m: n mod j

The rules used for OFDM slot concatenation are showed in Table 224.

**Table 223 — Code parameters for different data payload coded block sizes**

Data Bytes	Coded Bytes	Constituent	Code parameters		
			I <sub>x</sub>	I <sub>y</sub>	D
3	6	(15,11)(8,7)	3	4	0
6	12	(16,11) (8,7)	4	0	1
9	12	(16,15) (16,15)	10	0	3
9	18	(16,11) (16,15)	4	4	5
12	18	(8,7) (64,63)	4	28	9
15	18	(16,15) (16,15)	7	0	0
12	24	(16,11) (16,15)	4	0	9
18	24	(8,7) (32,31)	2	0	11
15	30	(15,11) (31,26)	3	11	0
18	36	(15,11) (31,26)	3	7	8
24	36	(16,15) (32,26)	4	8	6
27	36	(8,7) (64,63)	2	16	19
30	36	(16,15) (32,31)	7	0	8
21	42	(7,4) (63,57)	0	15	0
24	48	(16,11) (32,26)	0	8	6

Data Bytes	Coded Bytes	Constituent	Code parameters		
			I <sub>x</sub>	I <sub>y</sub>	D
36	48	(16,15) (63,57)	8	15	6
27	54	(32,26) (32,26)	14	8	0
36	54	(32,31) (31,26)	8	13	11
45	54	(8,7) (64,63)	0	10	11
30	60	(32,26) (32,26)	2	16	0
45	60	(16,15) (32,26)	0	2	0
33	66	(32,26) (32,26)	8	10	24
36	72	(32,26) (32,26)	14	0	24
48	72	(16,11) (64,63)	0	28	1
54	72	(16,15) (64,57)	0	28	3
60	72	(16,15) (64,63)	7	0	24

**Table 224 — Subchannel concatenation rule**

Number of OFDM slots	OFDM slots concatenated	
n ≤ j	One block of n OFDM slots	
n > j	m = 0	k blocks of j OFDM slots
	m ≠ 0	(k-l) blocks of j OFDM slots One block of ceil ((m+j)/2 ) OFDM slots One block of floor ((m+j)/2 ) OFDM slots

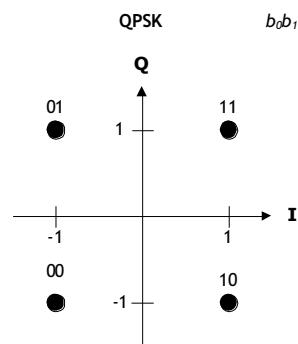
**Table 225 — Encoding OFDM slots concatenation for different allocations and modulations**

Modulation and rate	J
QPSK 1/2	12
QPSK 3/4	6
16-QAM 1/2	6
16-QAM 3/4	6
64-QAM 1/2	4
64-QAM 2/3	4
64-QAM 3/4	2
64-QAM 5/6	4

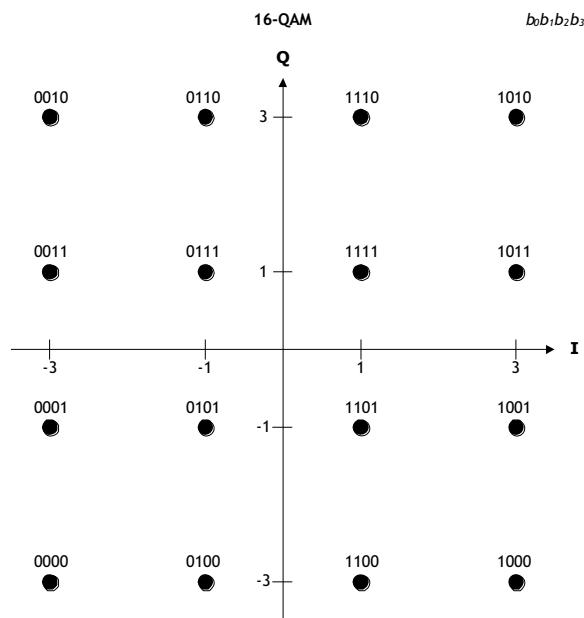
## 9.8 Constellation mapping and modulation

### 9.8.1 Data modulation

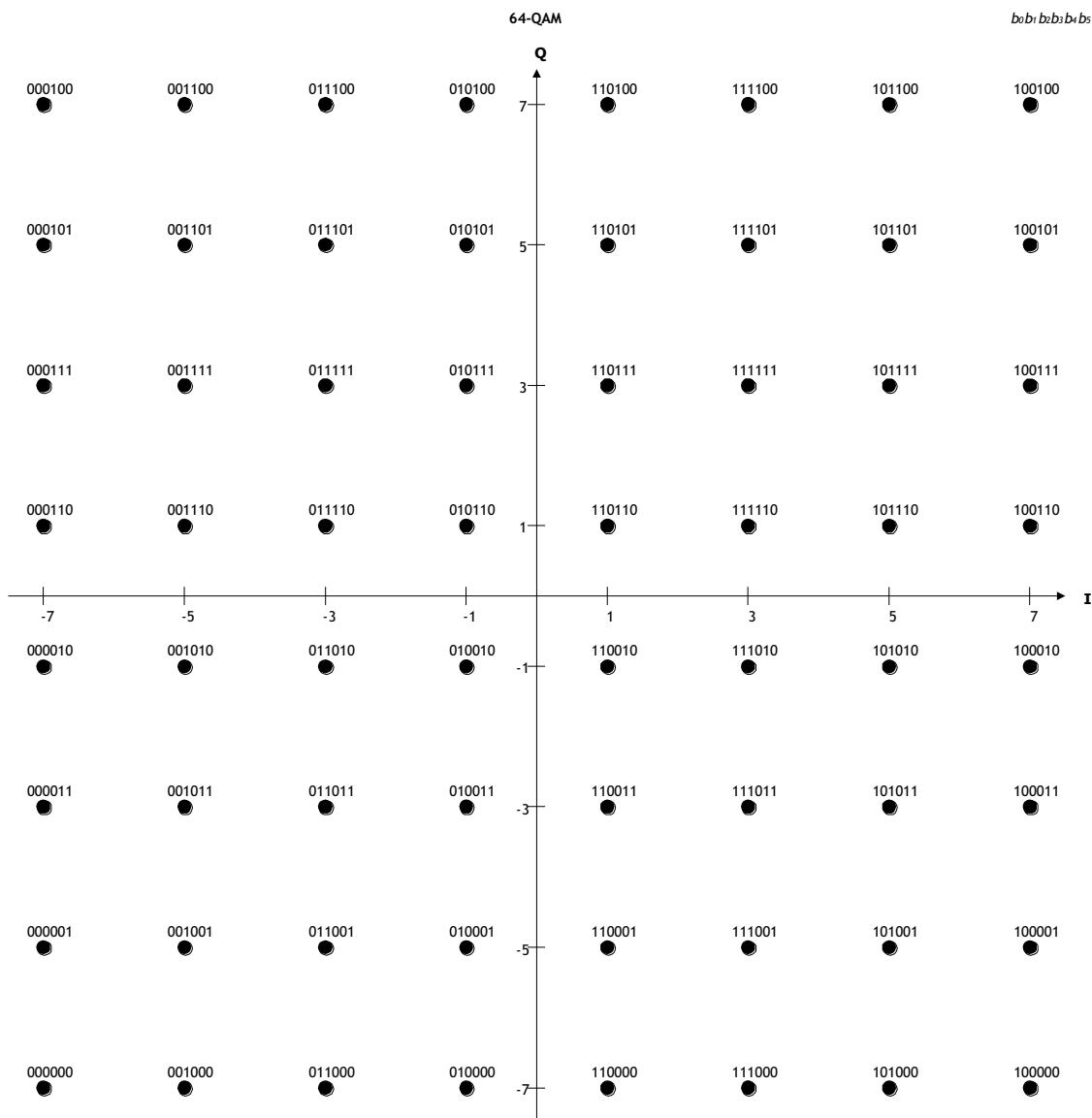
The output of the bit interleaver is entered serially to the constellation mapper. The input data to the mapper is first divided into groups of number of coded bits per carrier, i.e.,  $N_{CBPC}$  (see Table 226) bits and then converted into complex numbers representing QPSK, 16-QAM or 64-QAM constellation points. The mapping for QPSK, 16-QAM and 64-QAM is performed according to Gray-coding constellation mapping, as shown in Figure 150, Figure 151, and Figure 152, respectively where  $b_0$  represents the most significant modulation bit for all constellations.



**Figure 150 — Gray mapping for QPSK**



**Figure 151 — Gray mapping for 16-QAM**



**Figure 152 — Gray mapping for 64-QAM**

The complex value number is scaled by a modulation dependent normalization factor  $K_{\text{MOD}}$ . Table 226 shows the  $K_{\text{MOD}}$  values for the different modulation types defined in this subclause. The number of coded bits per slot ( $N_{\text{CBPS}}$ ) and the number of data bits per slot for the different modulation constellation and coding rate combinations are summarized in Table 227. Note that an OFDM slot corresponds to one OFDM symbol by one subchannel).

**Table 226 — Number of coded bit per carrier and normalization factor for different modulation constellations**

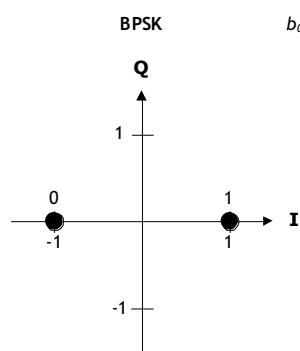
Modulation Type	N <sub>CBPC</sub>	K <sub>MOD</sub>
QPSK	2	1/√2
16-QAM	4	1/√10
64-QAM	6	1/√42

**Table 227 — Number of coded bits per OFDM slot (N<sub>CBPS</sub>) and corresponding number of data bits for different modulation constellation and coding rate combinations**

Constellation type	Coding rate	N <sub>CBPS</sub>	Corresponding number of data bits
QPSK	1/2	48	24
QPSK	2/3	48	32
QPSK	3/4	48	36
QPSK	5/6	48	40
16-QAM	1/2	96	48
16-QAM	2/3	96	64
16-QAM	3/4	96	72
16-QAM	5/6	96	80
64-QAM	½	144	72
64-QAM	2/3	144	96
64-QAM	3/4	144	108
64-QAM	5/6	144	120

### 9.8.2 Pilot modulation

The pilot subcarriers shall be modulated according to the BPSK modulation, as shown in Figure 153. In the BPSK modulation, the modulation-dependent normalization factor, K<sub>MOD</sub>, is 1.



**Figure 153 — BPSK constellation bit encoding**

## 9.9 Control mechanisms

### 9.9.1 Downstream synchronization

A downstream synchronization process shall be performed by each CPE. All the CPEs shall be synchronized with the BS.

The superframe and frame preambles may be used to perform the downstream synchronization. This process shall provide a CPE with sufficient time and frequency accuracy (i.e., to synchronize the CPE's local clock to the reference clock at the BS) to allow it to correctly receive DS information from the BS. Such DS information includes, among other things, the timing of the next upstream transmission opportunities for the CPE.

### 9.9.2 Upstream synchronization

Upstream synchronization shall be achieved through initial ranging and periodic ranging processes. The initial ranging transmission burst is specified in 9.9.3.1.2. The periodic ranging transmission burst is specified in 9.9.3.1.3. Upstream synchronization shall ensure that all US transmissions are received at the BS with which the CPEs are associated within  $\pm 25\%$  of the shortest cyclic prefix as given in Table 198, i.e.,  $\pm 2.333 \mu s$  or  $\pm 16$  sampling periods.

### 9.9.3 Opportunistic upstream bursts

Some transmission capacity shall be reserved in the upstream subframe, when needed, for CDMA ranging, CDMA or contention-based BW request, and CDMA or contention-based UCS notification. In the time domain, capacity shall be assigned over the width of the upstream subframe. In the frequency domain, the transmitted signal shall consist in the first six subchannels using the regularly spaced subcarrier pattern described in 9.6.4, which is optimized for the terrestrial-based geolocation ranging (see 10.5.2), and up to 10 additional subchannels using the regular upstream subcarrier interleaving scheme described in 9.6.4. The group of 168 regularly spaced subcarriers constituting the first six subchannels and the additional subchannels mentioned above are collectively called the ranging channel.

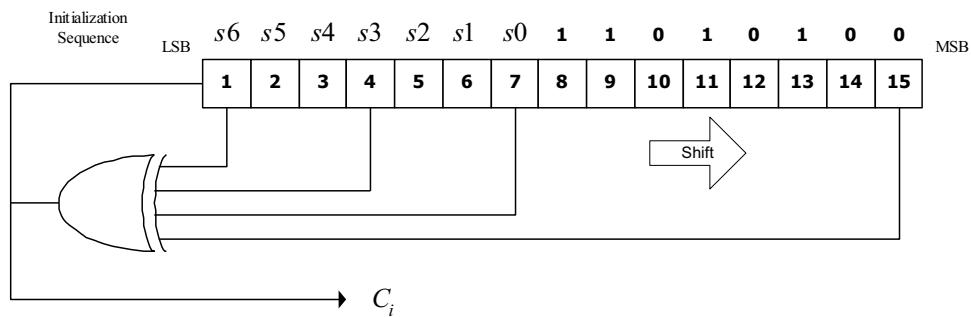
#### 9.9.3.1 CDMA bursts

The number of subchannels for the ranging channel and the number of symbols for each transmission (CDMA initial ranging, CDMA periodic ranging, CDMA BW request and CDMA UCS notification) are specified in the US-MAP\_IE Table 35

CPEs are allowed to collide on the ranging channel. To still provide reliable transmission, each CPE randomly chooses one ranging code from the subgroup of specified binary codes that is defined in 9.9.3.1.1. These codes are then BPSK modulated onto the subcarriers in the ranging channel. The length of these binary codes is the same as the number of subcarriers in the ranging channel.

##### 9.9.3.1.1 CDMA codes

The binary codes shall be the pseudo-noise codes produced by the PRBS generator described in Figure 154, which illustrates the following polynomial generator:  $1 + x^1 + x^4 + x^7 + x^{15}$ . The PRBS generator shall be initialized by the seed  $b_{15}...b_1 = 0,0,1,0,1,0,1,1,s_0,s_1,s_2,s_3,s_4,s_5,s_6$  where  $s_6$  is the LSB of the PRBS seed, and  $s_6:s_0$  are the least significant 7 bits of the  $BS\_ID$ , where  $s_6$  is the LSB of the  $BS\_ID$  (see Table 1).



**Figure 154 — PRBS generator for ranging code generation**

The binary ranging codes shall be subsequences of the pseudo-noise sequence appearing at its output  $C_i$ . The length of each ranging code is  $N_{code}$  bits, which is defined by the number of subchannels on the US\_MAP\_IE and shall always be multiple of 28 to satisfy the number of subcarriers per subchannel. These bits are used to modulate the subcarriers in the ranging channel and are mapped to the subcarriers in increasing frequency order of the logical subcarriers, such that the lowest indexed bit modulates the subcarrier with the lowest subcarrier index and the highest indexed bit modulates the subcarrier with the highest index.

For example, the first  $N_{code}$  bit code block is obtained by clocking the PN generator as specified, with  $BS\_ID = 0$ , the first code shall be 00110000010001... The next code block is produced by taking the output of the  $(N_{code} + 1)^{th}$  to  $(2 \times N_{code})^{th}$  clock of the PRBS generator, etc.

Each BS uses a subset of these codes. Let “p” point within the array of code blocks, each code block being  $N_{code}$  bits long. For example, if  $p = 200$  and  $N_{code} = 28$ , the code block 200 located from bits 5600 to 5627 will be used. A set of variables called S, N, M, L and I shall be sent from the BS to the CPE to indicate the beginning code block in the code stream. For example, if  $S = 202$ , we will start using the code block  $p=202$ , namely bits 5656 to 5683. The code blocks to be used shall be consecutive. Starting from code block S, the first N code blocks shall be used for initial ranging. The next M code blocks shall be used for periodic ranging. The next L code blocks shall be used for BW-request. The next I code blocks shall be used for UCS notification. The end of the bit structure shall be truncated to align with the last complete code block. If the end of the last complete block is reached in the process, the bit usage will continue by wrapping to code block 0.

The BS shall separate colliding codes and extract timing (ranging) and power information by using a correlation function. The time (ranging) and power measurements shall be used by the system to compensate for the various BS-CPE-BS propagation distances. In the process of CPE code detection, the BS will also get the Channel Impulse Response (CIR) for the transmission link from the specific CPE. The precise timing offset shall be estimated by terrestrial ranging (see 10.5.2).

### 9.9.3.1.2 Initial-ranging transmission

The initial ranging transmission shall be used by all CPEs to synchronize to the system when attempting to associate. The initial ranging transmission will be used for detecting and adjusting the timing offset and adjusting the transmission EIRP level. The initial-ranging transmission is performed using three consecutive symbols starting, as indicated in the US-MAP for the CPE, on the first symbol after the TTG. To allow for absorption of the signal propagation delay for the forward and return paths from a CPE located at a distance of up to a maximum of 100 km, 2 more buffer symbols are needed at the BS for this initial ranging burst to avoid spilling onto other signals received from synchronized CPEs. The window for the initial-ranging transmission shall therefore always occupy the first 5 OFDM symbols of the upstream subframe.

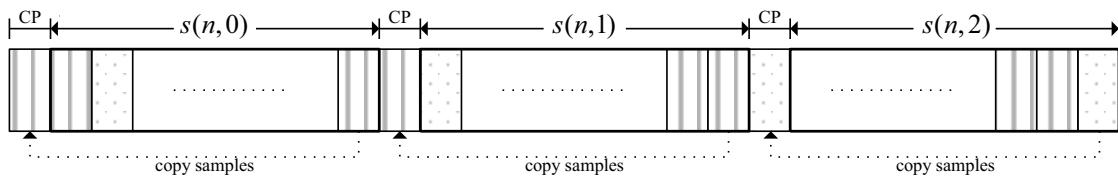
The same ranging code shall be repeated on the ranging channel of these three OFDM symbols and this code shall be BPSK modulated with phase rotation according to the symbol index and the subcarrier index in order to maintain the phase continuity between two contiguous symbols after the CP is inserted in front of each OFDM symbol. These symbols shall be generated according to Equation (11). A time-domain illustration of the three consecutive symbols used for the initial-ranging transmission is shown in Figure 155.

$$s(n,l) = \sum_{k=0}^{N_{FFT}-1} \left[ b_k \cdot e^{j2\pi \frac{k \cdot l \cdot N_{CP}}{N_{FFT}}} \right] \cdot e^{j2\pi \frac{k \cdot n}{N_{FFT}}} = \sum_{k=0}^{N_{FFT}-1} b_k \cdot e^{j2\pi \frac{k \cdot (n+l \cdot N_{CP})}{N_{FFT}}}, \quad (11)$$

$$b_k = \begin{cases} 2 \cdot \left( \frac{1}{2} - C_i \right), & i = i+1, k \in R \\ 0 & , k \notin R \end{cases}$$

where

- $s(n,l)$  is the  $l^{\text{th}}$  OFDM symbol for initial ranging with the sample index  $n$ .  $l$  is  $[0,1,2]$ .
- $k$  is the subcarrier index in the channel
- $C_i$  is the ranging code defined in 9.9.3.1.1.  $i = [0 \sim N_{code}-1]$  where  $N_{code}$  is the length of the CDMA code
- $R$  is the set of index of subcarriers within the ranging subchannel
- $N_{FFT}$  is the size of 2K FFT, 2048
- $N_{CP}$  is the size of the cyclic prefix

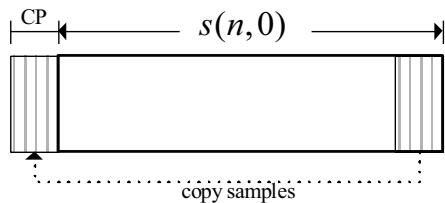


**Figure 155 — Initial-ranging transmission using three consecutive OFDM symbols**

#### 9.9.3.1.3 CDMA periodic-ranging, BW-request, and UCS notification transmission

Periodic-ranging transmissions shall be sent periodically by CPEs identified by the BS for system periodic ranging. Bandwidth-request transmissions shall be for requesting upstream allocations from the BS. UCS notification transmissions shall be used for reporting detection of an incumbent. These transmissions shall be sent only by CPEs that have already associated with the base station. To perform periodic-ranging, bandwidth-request or UCS notification transmission, the CPE can send a transmission in the following manner.

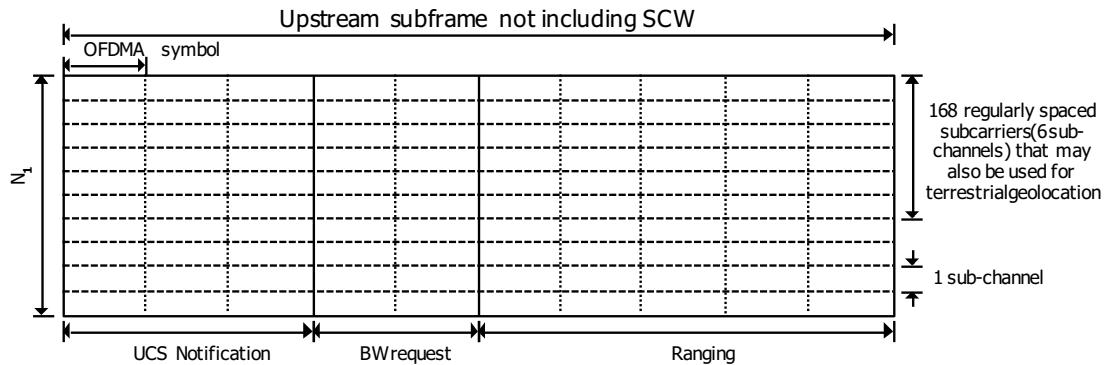
Modulate one ranging code on the ranging channel for a period of one OFDM symbol. Ranging channels shall be dynamically allocated by the MAC layer at the BS and indicated by the number of subchannels in the US-MAP\_IE (see Table 35). A time domain illustration of the periodic-ranging, bandwidth-request or UCS notification transmission is shown in Figure 156, where  $s(n,0)$  follows Equation (11) in 9.9.3.1.2 for  $l = 0$ .



**Figure 156 — Periodic-ranging/Bandwidth-request/UCS notification transmission**

#### 9.9.3.1.4 Ranging, BW request, and UCS notification opportunity windows

The opportunity window for each type of CDMA burst shall be assigned to some or all of the first six subchannels containing the 168 regularly spaced subcarriers normally used for terrestrial geolocation ranging and to a number of additional subchannels if needed, over the entire upstream subframe. Initial ranging, periodic ranging, BW-request, and UCS notification CDMA bursts, if present, shall be allocated to a number of symbols in successive portions of the total opportunity window as indicated by the US\_MAP\_IE (see Table 35) and illustrated in Figure 157.  $N_1$  denotes the number of subchannels over which concatenated initial ranging, periodic ranging, BW-request and UCS notification codes will be transmitted. The initial ranging, when scheduled, shall occupy the first 5 symbols of the ranging window. These symbols should be excluded from the scheduling of the other opportunity windows. It is assumed that, except for the initial ranging, the CDMA bursts will be transmitted by the CPEs such that they arrive at the BS with the proper timing within the cyclic prefix.



**Figure 157 — Example of Ranging/BW request/UCS notification opportunities windows**

#### 9.9.3.2 Contention-based BW Request and UCS notification

The contention-based BW Request and UCS notification opportunity window shall be assigned to some or all of the first six subchannels containing the 168 regularly spaced subcarriers that are normally used for terrestrial geolocation ranging and to a number of additional subchannels if needed, over the entire upstream subframe as specified in Table 35. In order to avoid excessive number of collisions, each contention-based burst will be transmitted with a random back-off uniformly selected within the range specified in Table 30. The allowed size for these contention-based bursts is specified by the BS in its US-MAP (see Table 31).

## 9.9.4 Power control

The WRAN system standard shall support Transmit Power Control (TPC) on a link-by-link basis to allow a reduction of the transmit EIRP at the CPEs to the lowest levels possible to minimize interference to incumbents while still maintaining the fastest possible reliable connection. CPE transmit EIRP is also controlled by the coarse ranging process (see 7.14.2.8.2) to minimize the dynamic range between carriers received at the base station from the near and far CPEs.

### 9.9.4.1 Transmit Power control boundaries and EIRP limits

The transmitter shall support monotonic power level control over a range of at least 60 dB, with a resolution (step size) of 0.5 dB. The EIRP accuracy shall be  $\pm 1.5$  dB when the level is at least 10 dB below the maximum regulatory power limit and  $\pm 0.5$  dB elsewhere.

A compliant implementation shall limit the device's maximum operating EIRP by 0.5 dB from the maximum allowed EIRP obtained from the database service or from the regulated EIRP limit (see Annex A) to assure that the regulated EIRP and power constraints are not exceeded.

The relationship between the transmitted EIRP and the conducted power going to the antenna will be established at the device with the knowledge of the maximum antenna gain for each channel on which the device can operate.

$EIRP_{MAX} (\text{dBm}) = \text{maximum transmit power } (\text{dBm}) + \text{maximum antenna gain for the specified channel } (\text{dBi}).$

Such antenna gain shall be available under the following requirements:

- Non-integrated antennas shall be required to store their maximum directional gain, in dBi, for each channel and report values in response of the device request (see 10.7.6).
- CPEs employing non-integrated antennas shall query their antenna for the maximum gain per channel at start-up as part of the self-test prior to association using the M-ANTENNA-INFORMATION primitive structure described in 10.7.6.3.
- In the case of an antenna integrated to the CPE, indicated by using the M-ANTENNA-INTEGRATED primitive structure described in 10.7.6.1, the maximum antenna gain per channel shall be recorded in the CPE by the manufacturer.

The conservative assumption is made that there is 0 dB loss due to antenna coupling and cable loss between the CPE and its antenna. Such losses should be minimized in practice to allow the CPE to reach the maximum EIRP (e.g., 4 W), which would be reduced by the amount of these losses since the BS will not go beyond this maximum assuming that there is 0 dB coupling and cable loss.

### 9.9.4.2 Transmit Power Control mechanism

A power control algorithm shall be supported for the US channel with both an initialization procedure through initial ranging and a periodic adjustment procedure to be carried out without loss of data. The BS shall be capable of providing accurate power measurements of the received burst signal. This value shall then be compared against a reference level, and the resulting EIRP level per subcarrier to be used by the CPE shall be fed back to the CPE through the RNG-CMD MAC message (see 7.7.6). The power control algorithm shall support EIRP adjustment as required (due to propagation loss and power fluctuations) at rates of up to 6 dB/s. The CPE shall adjust its transmit EIRP in response to a TPC command in the next scheduled upstream burst following receipt of the command. The power control algorithm at the BS shall take into account the various SNR requirements resulting from the different burst profiles while preventing violation of the emission masks (see 9.13) and maximum EIRP levels (see Annex A).

A transmitting CPE shall maintain the same transmitted EIRP density (EIRP per OFDMA subcarrier) regardless of the number of subchannels assigned, unless the maximum allowable total EIRP level (EIRP per subcarrier multiplied by the number of subcarriers used at any particular time) is reached. In other words, when the number of active subchannels allocated to a user is reduced, the total transmitted EIRP shall be reduced proportionally by the CPE, without additional power control messages (i.e., the gain of the RF transmission path is kept constant). When the number of subchannels is increased, the total transmitted EIRP shall also be increased proportionally. However, the transmitted EIRP level shall not exceed the maximum allowable EIRP level in an entire channel as dictated by regulatory requirements (see Annex A). The CPE shall interpret power control messages as the required transmitted EIRP density (EIRP per OFDMA subcarrier) as described above.

To maintain at the BS a received power density (received signal strength level (RSSL) per subcarrier) consistent with the modulation and FEC rate used by each CPE, the BS may change the EIRP density transmitted by the CPE, through the RNG-CMD message (see 7.7.6), as well as the CPE-assigned modulation and FEC rate. There are, however, situations where the CPE should automatically update its transmitted EIRP density without being explicitly instructed by the BS. This happens when the CPE transmits in the region marked by UIUC = 2 to 7 (see Table 36). In all these situations, the CPE shall use a new transmitted EIRP density value set according to Equation (12) (in dBm).

$$\begin{aligned} P_{tmp} &= P_{last} + (CNR_{new} - CNR_{last}) + Offset \\ P_{Tot} &= P_{tmp} + 10 \cdot \log(N_{new}) \\ P_{new} &= \begin{cases} P_{tmp} & \text{if } P_{Tot} \leq P_{Max} \\ P_{Max} - 10 \cdot \log(N_{new}) & \text{if } P_{Tot} > P_{Max} \end{cases} \end{aligned} \quad (12)$$

where

- $P_{Max}$  is the maximum allowable transmitted EIRP on the current operating channel
- $P_{tmp}$  is the temporary transmitted EIRP density (per subcarrier)
- $P_{Tot}$  is the temporary total transmitted EIRP
- $CNR_{new}$  is the normalized CNR of new modulation/FEC rate instructed by the UIUC
- $CNR_{last}$  is the normalized CNR of the last used modulation/FEC rate
- $P_{range}$  is the EIRP density (per subcarrier) indicated by the BS by the RNG-CMD MAC message
- $P_{last}$  is the  $P_{range}$  specified by the RNG-CMD MAC message for the last used modulation/FEC rate
- $P_{new}$  is the EIRP density (per subcarrier) to be used for the current burst transmission

Note that the “normalized CNR” corresponds to the subcarrier power over the noise power present in the subcarrier nominal bandwidth that corresponds numerically to the subcarrier spacing as indicated in Table 199, expressed in dB. In other words, the “normalized CNR” corresponds to the subcarrier power density over the noise power density expressed in dB.

In all other situations, the CPE shall use the EIRP density value set according to Equation (13) (in dBm).

$$P_{new} = P_{range} \quad (13)$$

This resulting value  $P_{new}$  is updated based on the value  $P_{range}$  transmitted regularly to the CPE by the BS through the RNG-CMD MAC message (see 7.7.6) to keep the TPC of the RF link up-to-date. The CPE shall be calibrated by the manufacturer so that the actual EIRP density per subcarrier transmitted by the CPE corresponds to the level indicated by the  $P_{range}$  variable resulting from the RNG-CMD message (within 0.5 dB). The default normalized CNR values per modulation for the binary convolutional code (BCC), except for the CDMA code, are given in Table 228. These values may be overridden by the BS by using a dedicated UCD message (see Table 33). The second column is the default value and third column is informative and indicative of the modulation performance in a multipath channel.

**Table 228 — Normalized CNR per modulation for BER=  $2 \times 10^{-4}$** 

Modulation—FEC rate	Normalized CNR (dB)	
	AWGN (default)	Multipath channel <sup>20</sup>
CDMA code	1.2	5
QPSK, rate: 1/2	4.3	8.1
QPSK, rate: 2/3	6.1	11.6
QPSK, rate: 3/4	7.1	14.0
QPSK, rate: 5/6	8.1	17.8
16-QAM, rate: 1/2	10.2	14.8
16-QAM, rate: 2/3	12.4	20.3
16-QAM, rate: 3/4	13.5	24.6
16-QAM, rate: 5/6	14.8	28.6
64-QAM, rate: 1/2	15.6	20.5
64-QAM, rate: 2/3	18.3	26.2
64-QAM, rate: 3/4	19.7	31.8
64-QAM, rate: 5/6	20.9	40.4

The CPE shall report, at registration, the maximum EIRP that it can achieve in the case of the transmission of a full multiplex (60 subchannels) while still meeting the required RF mask (see 9.13) and other performance limits set by the manufacturer. The maximum EIRP achievable at the CPE (see 7.7.11.3.2.1) may be reported in the CBC-REQ MAC message (see 7.7.11.1). This parameter may be used by the BS to determine the maximum EIRP density per subcarrier achievable as a function of the number of used subchannels allocated to the CPE for its upstream burst, noting that the PAPR tends to increase with the number of transmitted subcarriers in the burst. This parameter may also be used by the BS for optimal assignment of coding schemes and modulations and also for optimal allocation of subchannels. These algorithms are vendor-specific.

For the periodic ranging, once a CPE sends a periodic ranging code and fails to receive a RNG-CMD (7.7.6), the CPE may adjust its EIRP for the transmission of subsequent periodic ranging codes up to  $EIRP_{IR\_MAX}$  (7.14.2.8.1).

## 9.10 Network synchronization

For multiple WRAN cells implementation, it is required that all BSs be time synchronized within a tolerance of  $\pm 8$  TU (equivalent to  $1.167\ \mu s$  for 6 MHz,  $1\ \mu s$  for 7 MHz BW and  $0.875\ \mu s$  for 8 MHz BW). It should be noted that any filtering at the output of the OFDM modulator to help meeting the rejection required by the RF mask (see 9.13) will create temporal dispersion that will consume part of the cyclic prefix capability provided for alleviating channel time spreading.

In the event of a loss of synchronization with the common clock or with nearby WRAN BSs, the BS shall continue to operate and shall automatically resynchronize through the synchronization process described in 7.23.

For multiple WRAN cells implementation, frequency references derived from a common timing reference shall be used to control the frequency accuracy of Base-Stations as specified in 7.23, provided that they meet the frequency accuracy requirements of 9.11. This applies during normal operation and during loss of timing reference.

<sup>20</sup> The multipath channel used for the calculations is defined on 6 paths as follows: excess delay: -3, 0, 2, 4, 7 and 11  $\mu s$ ; relative amplitude: -6, 0, -7, -22, -16, and -20 dB; the phase for each path is random. The delay, amplitude and phase are assumed to be constant over the period of one symbol.

## 9.11 Frequency Control requirements

At the BS, the transmitted center frequency and the symbol clock frequency shall be derived from the same reference oscillator. At the BS, the reference frequency tolerance shall be better than  $\pm 2$  ppm.

At the CPE, the transmitted center frequency and the symbol clock frequency shall be derived from the same reference oscillator. Thereby, the transmit center frequency shall be synchronized and locked to the frequency transmitted from the BS with a maximum tolerance of 2% of the subcarrier spacing.

During the synchronization period, the CPE shall acquire frequency synchronization within the specified tolerance before attempting any upstream transmission. During normal operation, the CPE shall track the frequency changes and shall defer any transmission if synchronization is lost.

## 9.12 Antenna

### 9.12.1 Antenna reference patterns

#### 9.12.1.1 CPE transmit/receive antenna reference pattern

The WRAN transmit/receive antenna at the CPE shall meet the reference antenna pattern depicted in Figure 158. The backlobe rejection level of 17 dB shall be met for all elevation angles in the range of  $\pm 20$  degrees from the horizontal plane. This pattern was developed assuming a typical antenna gain of 12 dBi and is described by Equation (14):

$$\text{Maximum relative gain (dB)} = \begin{cases} 10 \cdot \log_{10}(\cos^4 \theta), & |\theta| \leq 68^\circ \\ -17, & 68^\circ < |\theta| < 180^\circ \end{cases} \quad (\text{main lobe}) \quad (14)$$

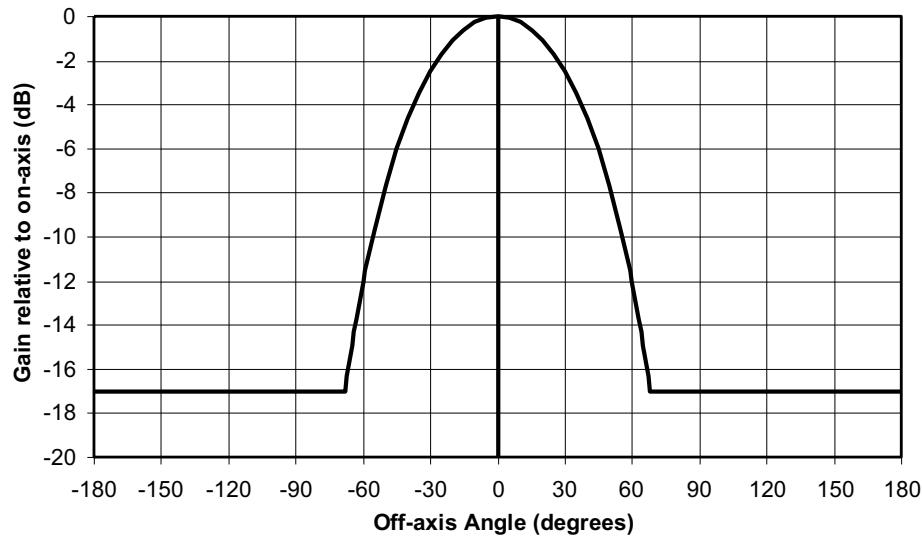


Figure 158 — CPE TX/RX reference antenna pattern

In the case where the WRAN transmit and receive functions of the CPE use separate antennas, the gain of these antennas shall track within 0.5 dB of each other in all azimuths of the main lobe. Outside the main lobe, both antennas shall meet the specified front-to-back ratio.

### 9.12.1.2 Sensing antenna reference pattern

The gain of the sensing antenna in the horizontal azimuthal plane shall be equivalent to an omni-directional antenna. The deviation from this nominal gain shall be no worse than  $-1$  dB. Such maximum deviation from this nominal gain should be kept over  $\pm 20$  degrees in the vertical pattern in all azimuths.

### 9.12.1.3 BS transmit/receive antennas

The BS shall use the same antenna for transmission and reception. This allows the assumption of reciprocal transmit and receive path used in the equations in this Standard for the calculation of the power levels.

## 9.12.2 Antenna interface

### 9.12.2.1 TRU/AU physical interface

The IEEE 802.22 BS and CPE may be implemented as separate TRUs and AUs or integrated into a single unit. In the case where they are separate units, the TRU and the AU shall have a coaxial interface to convey the radio signals to be transmitted and received by the antenna as well as ancillary signals to be transferred between the TRU and AU such as data, clock and power supply.

An integrated unit is defined as one where removal or disconnection of the RF antenna or GPS antenna shall only be possible through tampering with the unit in such a way as to trigger the tamper proof mechanisms (see Clause 11). Any other implementation will result in separate CPE and AUs to which the following specification shall apply.

When implemented as separate units, interfaces shall exist on both the AU and the TRU. The transceiver unit shall be connected to the AU via a 50-ohm coaxial cable. The AU shall consist of the antenna and, where required, the integrated GPS receiver. The TRU interface shall be a female “N” type connector. The AU interface shall be a female “N” type connector. The coaxial cable shall have a male Standard or Corrugated type “N” connector at both the TRU and the AU ends. The length of the coaxial cable shall be less than 50 meters for cables fitted with Standard type “N” connectors and be less than 250 meters for cables fitted with corrugated type “N” connectors. These connectors shall comply with MIL-PRF-39012E with Amendment 1 and MIL-STD-348. Table 229 summarizes the technical requirements for the “N” connectors and Figure 159 illustrates typical TRU and AU interfaces and the coaxial cable linking them.

**Table 229 —Type “N” connector requirements**

Impedance	50 $\Omega$
Frequency range	0–11 GHz
Voltage rating	1500 volts peak
VSWR	1.35 maximum over 0–11 GHz
Dielectric withstanding voltage	2500 volts rms
Insulation resistance	5000 M $\Omega$ minimum
Center contact resistance	1.0 m $\Omega$
Outer contact resistance	0.2 m $\Omega$
RF leakage	–90 dB minimum at 3 GHz
Insertion loss	0.15 dB maximum at 10 GHz
Mating	5/8-24 threaded coupling MIL-STD-348
Weatherproof	All connectors exposed to outside conditions shall be weatherproof



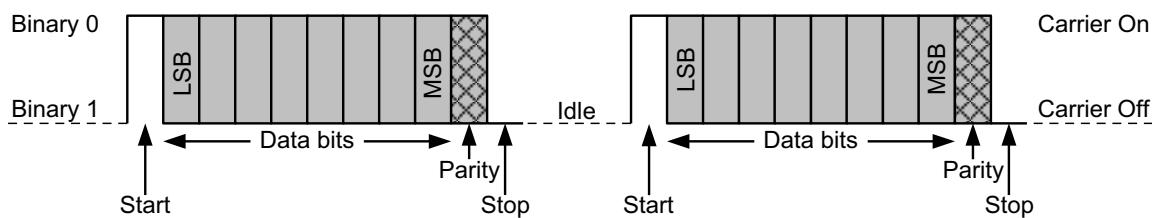
**Figure 159 — RF interface between an IEEE 802.22 transceiver and its antenna**

The TRU and AU interfaces and the coaxial cable linking them shall convey the following multiplex of signal components:

- 1) TX-RF: the transmit RF signal generated by the TRU. The AU shall not change the frequency or amplify this signal.
- 2) RX-RF: the RF signal received over the air by the AU. The AU shall not change the frequency of this signal.
- 3) COAX-DC: a temporary DC power applied by the TRU. When applied, its voltage shall be maintained at  $5 \pm 0.25$  Volts and it shall support any DC load up to  $0.5 \pm 0.1$  Ampere. If the DC load present on the “N” connector is below 10 ohms, the TRU shall remove the COAX-DC signal and report the “short detected” event. The AU may use this DC as power supply and shall not present a load of more than 0.4 Ampere at any time.
- 4) UP-LINK: signaling generated by the TRU, superimposed to the COAX-DC and destined for the AU. The UP-LINK shall consist of a binary signal encoded as a  $2.0 \pm 0.01$  MHz amplitude-switched carrier. This carrier shall have an amplitude of  $0.3 \pm 0.03$  Vpk-pk to represent a binary 0 and an amplitude of  $0.03 \pm .03$  V to represent a binary 1.
- 5) DN-LINK: signaling generated by the AU, superimposed to the COAX-DC and destined for the TRU. The DN-LINK shall consist of a binary signal encoded as a  $1.0 \pm 0.005$  MHz amplitude switched carrier. This carrier shall have an amplitude of  $0.3 \pm 0.03$  Vpk-pk to represent a binary 0 and an amplitude of  $0.03 \pm 0.03$  V to represent a binary 1.

The TRU shall apply and maintain COAX-DC at least 0.5 second before applying the UP-LINK signal. The AU shall be ready to receive the UP-LINK signal and transmit the DN-LINK signal within 0.4 second after the application of COAX-DC.

When data is transmitted on either UP-LINK or DN-LINK, the rate of transmission shall be 9600 bits per second. The asynchronous data communication method used for the UP-LINK and DN-LINK shall consist of a bit-by-bit transmission on the physical channel. The information shall be broken into 8-bit data words. Each data word, starting with the least significant bit, shall be preceded by one start bit (binary 0), augmented with one parity bit generated from the 8-bit data word with even parity, and followed by one stop bit (binary 1). When the transmission link is idle, it shall be at binary state 1. Figure 160 illustrates the structure of the bit stream for two successively transmitted octets.



**Figure 160 — Structure of the UP-LINK and DN-LINK bit stream**

### 9.12.2.2 TRU/AU messaging interface

The following message codes shall be used to signal communication between the TRU and AU:

Instructions are formatted as follows: 1 byte of opcode followed by data or control code bytes.

**TRU-HELLO:**

- I. This message shall be sent if the TRU has not received an AU-HELLO message within 4 seconds after applying power to the AU.
- II. Purpose: for the TRU to initiate handshaking with the AU to verify that the AU is available for query. If the AU does not respond within 4 seconds after this message transmission, the TRU shall declare the antenna non-operational and abort its operation.
- III. Format:
  - a) Opcode: 0x0000
  - b) Data: none

**AU-HELLO:**

- I. Sent by the AU upon power-on or in response to the TRU-HELLO message.
- II. Purpose: for the AU to announce that it is available for query. The AU shall respond within 4 seconds after the transmission of the TRU-HELLO message,
- III. Format:
  - a) Opcode: 0x1YYY, where YYY is the amount of data (antenna model and antenna gain) that is stored in the AU (maximum length= 2k octets).
  - b) Data: none

**AU-REQ:**

- I. Sent by the TRU after setup of serial communication and indication of AU availability (i.e., after reception of AU-HELLO).
- II. Purpose: for the TRU to request transfer of antenna information from the AU.
- III. Format:
  - a) Opcode: 0x2000
  - b) Data: none

**AU-RSP:**

- I. Sent by the AU after receiving an AU-REQ from the TRU.
- II. Purpose: for the AU to transfer the antenna model and gain information.
- III. Format:
  - a) Opcode: 0x3YYY, where 0xYYY is the length of the data string that is to be sent to the TRU (maximum length= 2k octets).
  - b) Data: string of octets that contains the antenna model and gain information according to the format specified below (2k octets maximum). Once received, this string of octets shall be parsed by the TRU and stored in the appropriate MIBs (see 7.7.7.3.4.8 and 7.7.7.3.4.9).

**GPS-REQ:**

- I. Sent by the TRU after setup of serial communication and indication of AU availability (i.e., after reception of AU-HELLO)
- II. Purpose: for the TRU to request delivery of geolocation data from the GPS receiver.
- III. Format:
  - a) Opcode: 0x4YYY, where 0xYYY is the length of the data string that is to be relayed transparently to the GPS receiver (maximum length = 2k octets).
  - b) Data: Character string to be relayed transparently to the GPS receiver.

**GPS-RSP:**

- I. Sent by the AU after receiving data from the GPS receiver.

II. Purpose: forwarding the NMEA string received from the GPS receiver to the TRU.

III. Format:

- a) Opcode: 0x5YYY, where 0xYYY is the length of the data string that is being relayed transparently to the TRU.
- b) Data: Character string received from the GPS receiver (2k octets maximum).

#### 9.12.2.3 AU antenna information mapping

Table 230 presents the mapping of the information to be stored at the AU. It is defined by segments that contain the type of information (3 octets), the length of the segment (1 octet), and the information, followed by a CRC-16 to protect the information contained in the segment during transmission.

**Table 230 — Example of data segments stored at the AU (to be read vertically)**

MDL	USA	GBR	—
Length 0xYY	Length 56=0x38	Length 55=0x37	Length 0xYY
—	Gain <sub>2</sub>	Gain <sub>21</sub>	—
—	Gain <sub>3</sub>	Gain <sub>22</sub>	—
—	—	—	—
—	—	—	—
—	—	—	—
—	—	Gain <sub>68</sub>	—
—	Gain <sub>50</sub>	Gain <sub>69</sub>	CRC-16
CRC-16	Gain <sub>51</sub>	CRC-16	
	CRC-16		

Each data segment shall begin with a 3 ASCII characters long code contained in the following 3 octets:

- MDL: Antenna model segment. These 3 first octets are followed by one octet indicating the length of data to follow before the closing 2 CRC octets. The data shall contain the antenna model and serial number stored in a character string assigned by the AU manufacturer.
- USA, GBR, etc.: Regulatory domain ISO 3166 [B44] code included as the first 3 octets followed by one octet indicating the length of data to follow before the closing 2 CRC octets. The data portion shall contain one octet per channel indicating the on-axis gain of the antenna at the center frequency. The channels correspond to those listed in Annex A and are ordered the same way as shown in Annex A (see Table A.17 for the USA and Table A.18 for European countries). Additional segments can be added for further regulatory domains up to 2k octets.
- Gain<sub>n</sub>: Maximum on-axis antenna gain in the specific channel in 0.25 dB units ranging from -22.0 dB<sub>i</sub> (0x01) to 41.0 dB<sub>i</sub> (0xFD). Code 0x00 shall be assigned to channels for which the antenna is not intended to be used. Code 0x01 shall also be used for antenna gain smaller than -22.0 dB<sub>i</sub>. Code 0xFE shall be used for antenna gain higher than 41.0 dB<sub>i</sub>. Code 0xFF is not allowed. (See Table 58, 7.7.7.3.4.9).

#### 9.13 RF mask

IEEE 802.22 devices shall comply with the RF mask specified for the appropriate regulatory domain as indicated in Annex A. Where such requirements have not been specified, the IEEE 802.22 devices shall meet at least one of the RF masks included in Annex A. The power spectrum density (PSD) measurement shall be done over a measurement bandwidth of 100 kHz and a video bandwidth of 100 kHz with an average detector.

In order to meet the various RF masks specified in Annex A, there may be a need to shape the transmission signal with either filtering in the frequency domain or windowing in the time domain. This is implementation dependent.

## 9.14 Receiver requirements

### 9.14.1 Receiver minimum sensitivity

The receiver minimum sensitivity level,  $R_{SS}$ , is defined as the minimum power, measured at the antenna port, at which the bit error rate performance is equal to the required limit. The equation is given as follows:

$$R_{SS} (\text{dBm}) = \text{Reference Thermal Noise Density Level} + \text{Noise Figure} + \text{Effective Channel Bandwidth} + \text{Required Signal-to-Noise Ratio} + \text{Receiver Implementation Margin} + \text{Interference Allowance}$$

where

Reference Thermal Noise Density Level = Boltzman Constant +  $10 \times \log(\text{Reference Noise Temperature})$   
with Boltzman Constant =  $-138.6 \text{ dB(mW/(K} \times \text{MHz}))$  and Reference Noise Temperature = 290 K (degrees Kelvin)

Noise Figure = 3 dB for the base station and 6 dB for the CPE

Effective Channel Bandwidth =  $10 \log (\text{Signal Bandwidth (MHz)})$  with Signal Bandwidth values as in Table 201)

Required Signal-to-Noise Ratio = the Reference Normalized SNR as shown in Table 228 for a BER performance of  $2 \times 10^{-4}$  where the values include 1.1 dB, 1.3 dB, and 1.5 dB decoder implementation margins for QPSK, 16-QAM, and 64-QAM modulations respectively

Receiver Implementation Margin = 1.9 dB and 2.1 dB for BS and CPE respectively, accounting for the coupling loss, pre-amplification filter loss, assuming that a low-noise pre-amplifier is located at the antenna

Interference Allowance = 1 dB for either BS or CPE to cover for the impact of local interference at the receiver

The base station and CPE minimum receiver sensitivity for the three channel bandwidths shall at least meet the values given in Table 231.

**Table 231 — Minimum receiver sensitivity requirement for QPSK rate: 1/2 at BER=  $2 \times 10^{-4}$**

TV channel bandwidth (MHz)	6	7	8
Base station receiver sensitivity (dBm)	-94.5	-93.8	-93.2
CPE receiver sensitivity (dBm)	-91.3	-90.6	-90.0

### 9.14.2 Receiver selectivity

The receiver selectivity is a measure of the ability of the receiver to reject signals from adjacent channels, while receiving a wanted signal on the selected frequency. It is defined as the ratio of the selected channel signal power to the power of the signal in the adjacent channel, subject to the target BER of  $2 \times 10^{-4}$ .

For IEEE 802.22 WRAN systems, the minimum receiver selectivity shall be

$$D/U_{adj} = 50.7 \text{ dB} \quad \text{for the most robust modulation: QPSK, rate: } 1/2$$

corresponding to the 55 dBr (72.5 dBc) rejection in the first adjacent channel of a transmitted WRAN signal (consistent with what is specified in the FCC R&O 08-260).

#### **9.14.3 Receiver tolerance to interference overload**

The receiver tolerance to interference overload (also known as the receiver blocking level or maximum input level) refers to the effect of strong RF signals in channels other than the channel of interest and its two adjacent channels on the ability of the receiver to decode a wanted signal in the selected channel.

The receiver tolerance to interference overload (i.e., maximum input level) for both the base station and CPE shall be –8 dBm.

## 10. Cognitive radio capability

### 10.1 General

This clause describes the cognitive radio capabilities supported by IEEE Std 802.22, which are required to meet regulatory requirements for protection of incumbents as well as to provide for efficient operation of IEEE 802.22 networks. The cognitive radio capabilities include: BS's SM, Spectrum Sensing Automaton (SSA), Access to the database services, Channel set management, Policy (Table 234 and Annex A), CPE Registration and Tracking, Spectrum Sensing services, and Geolocation services.

IEEE 802.22 devices shall employ cognitive radio capability, which shall enable them to make decisions about their radio operating behavior based on information from various sources such as sensing, geolocation and the database service, policy, etc. The information should be obtained through communication with the database service, or through direct sensing for incumbents on channels that would be impacted by operation of the IEEE 802.22 device, or both. The information may also be the result of rules governing the particular regulatory domain where the device intends to operate (e.g., certain channels may be "off limits" because they were allocated for some other specific use). This clause defines the IEEE 802.22 functional entities, information elements, and procedures related to obtaining and managing this information.

If a database service is present in the domain where the IEEE 802.22 device would operate, the IEEE 802.22 device shall retrieve appropriate spectrum availability information based on the geographic coordinates of its intended operating location from the database service, as described by procedures defined in this clause.

An IEEE 802.22 device shall also sense for the presence of incumbents in areas where the IEEE 802.22 device intends to operate, both prior to, and during operation. This includes sensing the prospective channels of operation as well as any other channels that might be subjected to harmful interference as a result of the operation of the IEEE 802.22 device. Signals that the IEEE 802.22 device shall sense are as follows:

- Television Broadcasts
- Wireless Microphone transmissions
- Transmissions from protecting devices, such as the IEEE 802.22.1 Wireless Beacon
- Other incumbent devices such as medical telemetry devices that may need to be protected in the local regulatory domain (see footnote 20, page 8 of the FCC R&O 08-260)

The IEEE 802.22 systems shall select their operating, backup, candidate channel sets based on the procedures that are described in 10.2.3. The IEEE 802.22 transmission shall be controlled by various policies that are defined in 10.2.5 related to the SM Policies. The SM operation is described in detail in 10.2.

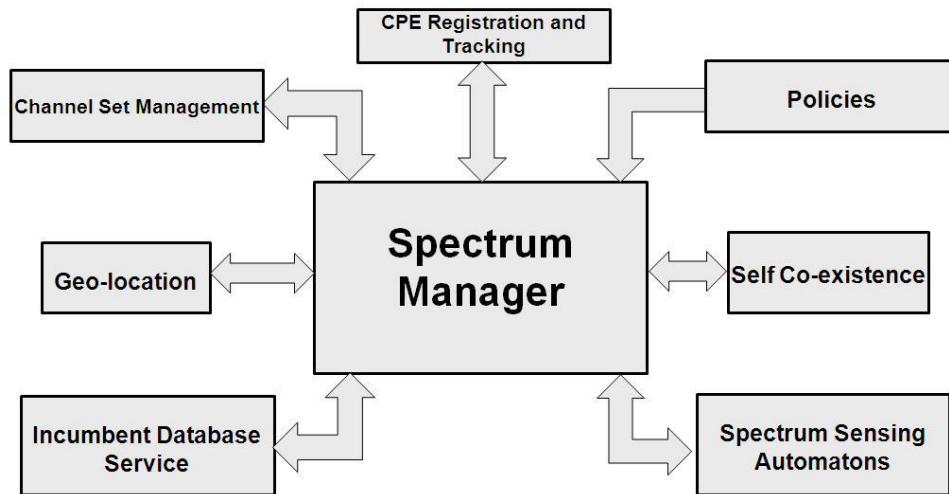
Note that IEEE 802.22 devices must also sense for other IEEE 802.22 systems that may be present and operating in their area. If such systems are discovered, the devices shall follow the self-coexistence procedures defined in 7.20.

The organization of this clause is as follows: 10.2 describes the Spectrum Manager operation; 10.3 describes the Spectrum Sensing Automaton; 10.4 describes the Spectrum Sensing Function; 10.5 describes the Geolocation; 10.6 describes the database service, and finally 10.7 describes primitives and messaging associated with the cognitive functions

## 10.2 Spectrum Manager operation

### 10.2.1 General

The SM, as shown in the IEEE 802.22 reference model (Figure 4), shall be part of the cognitive plane and shall always be present at the IEEE 802.22 BS. The SM is responsible for the most important tasks, such as maintaining spectrum availability information, channel selection, channel management, scheduling spectrum sensing operation, access to the database, enforcing IEEE 802.22 and regulatory domain policies, and enabling self-coexistence, etc. The detailed operation of the SM is described in 10.2.



**Figure 161 — IEEE 802.22 spectrum manager and logical interfaces**

All the IEEE 802.22 devices (BS and CPEs) shall also have an entity called the Spectrum Sensing Automaton (SSA). The SSA interfaces to the Spectrum Sensing Function (SSF) and executes the commands from the SM to enable spectrum sensing. The detailed operation of the SSA is described in 10.3. This subclause (10.2) describes the SM functionalities.

The SM is a central part of the WRAN BS, which shall be responsible for ensuring protection of incumbents and efficient spectrum utilization while complying with regulatory policies. For that, the SM centralizes all the decisions within the WRAN cell with respect to spectrum availability and utilization. In summary, the key functions of the SM are the following:

- Maintain spectrum availability Information
- Channel classification and selection
- Association control
- Channel set management
- Accessing the database service
- Scheduling quiet periods for spectrum sensing
- Enforcing IEEE 802.22 and regulatory domain policies
- Making channel move decisions for one or more CPEs or the entire cell
- Self-coexistence with other WRANs, etc.

These functions are described in the following clauses. It is important to note that this standard does not specify any particular SM implementation, but instead, it describes the mandatory behavior for any SM implementation in order to provide for proper protection of incumbents, compliance with regulatory domain policies, and interoperability among different WRAN implementations.

The SM shall determine the requirements for the rate of SCWs to ensure sufficient self-coexistence information exchange capacity and shall work with the data scheduler to influence the amount of data going to a CPE so that it has sufficient time to clear enough backup channels during its idle time.

### 10.2.2 Maintain spectrum availability information

The SM shall maintain the status of the spectrum (i.e., channels) available for WRAN operation at its location within a regulatory domain according to the policies and rules established for that domain (e.g., regulatory rules established by the FCC in the US for use of channels). The SM shall obtain information on the channel status with respect to the presence of incumbents and other WRANs in the area, and it shall use this information as input for its decisions with respect to channel selection, channel state management and self-coexistence mechanisms.

To maintain the status of the channels available for operation, the SM shall be able to aggregate information from at least the following sources:

- 1) **Database service:** The SM shall access an incumbent database through the higher layers. The SM shall be responsible for accessing the database service in the regulatory domains that mandate the presence of such a database. The database service is a service officially operated under the rules of the local regulatory authority that provides a list of available channels and possibly the maximum EIRP allowable on these channels based on queries containing the geolocation of the WRAN devices. In the regulatory domains that do not mandate such database service, a database of available channels shall be provided by the operator.
- 2) **Geolocation:** The SM shall be able to access geolocation information available at the BS to identify its own location, and it shall also be able to obtain location information from all CPEs associated with the BS or that are requesting association with the BS.
- 3) **Spectrum sensing:** The SM shall interface with the Spectrum Sensing Automatons located within the BS and the CPEs. The SM shall use the MAC and PHY layer functionalities and management frames to control and coordinate spectrum sensing within the WRAN cell. The SM shall trigger the requests for the SSAs located within the BS and the CPEs to perform sensing and collect sensing reports. The SM shall combine the local sensing results with the results collected from CPEs.

The SM shall define the status of the channels with respect to the presence of incumbents by combining geolocation information, information from incumbent databases, and spectrum sensing results. In order for IEEE 802.22 systems to operate, the BS shall maintain communication with a database service containing location dependent available channels if it exists. When operating in a regulatory domain that does not require a database service, all channels are initially assumed to be available. In this case, the SM shall define the status of the available channels based on spectrum sensing.

The channel availability information shall be defined during the network initialization and it shall be periodically updated during the network operation.

For example, Annex A specifies the US regulatory requirements for acquiring a channel (i.e., out-of-band sensing for IEEE 802.22 systems), and for in-service monitoring (i.e., in-band sensing for IEEE 802.22 systems). The actual values for these timings will depend on the regulatory domains and the specific values shall be obtained by the CPE through the MIBs at the time of initialization based on the regulatory classes defined in Table A.13.

### 10.2.3 Channel classification and selection

The SM shall assign the operating channel to the MAC/PHY modules in the WRAN. The SM shall also define the backup channel(s) and their corresponding priorities. The rest of the channels that are potentially available for operation, but that are not selected as the operating channel or as backup channel(s), may be classified as candidate, occupied or disallowed channel(s). The channels may be classified using the following categories:

**Available:** channels available for consideration for potential WRAN operation at a given location according to the database service. Channels not deemed available by the database service are precluded for use by WRANs.

Available channels are further classified into one of the following categories:

- **Disallowed:** Channels that are precluded from use by the operator due to operational or local regulatory constraints.
- **Operating:** The current channel used for communication between BS and CPEs within a WRAN cell. The operating channel shall be sensed at least every 2 seconds for the signal types as required by a particular regulatory domain. The operating channel shall also be sensed every 2 seconds for the IEEE 802.22.1 wireless beacon in the regulatory domains where the operation of such a beacon is allowed.
- **Backup:** Channels that have been cleared to immediately become the operating channel in case the WRAN needs to switch to another channel. The BS may maintain multiple backup channels at any given time and shall order them according to their relative priorities. Backup channels shall be sensed for incumbent detection at least once every 6 seconds. A channel can stay in the backup channel list as long as no incumbent is found on this channel towards which harmful interference could be produced by the WRAN transmission.
- **Candidate:** Channels that are candidates to become a backup channel. These are channels that the BS may request the CPEs to sense to evaluate the possibility of elevating them to a backup channel status. Although sensing of candidate channels could be infrequent, before a candidate channel is elevated to backup channel, it must be sensed as incumbent-free at least every 6 seconds for no less than 30 seconds. If the first channel in the list can be confirmed to be clear of any incumbent operation towards which harmful interference could be produced by the WRAN transmission within the required time period, the base station can move it to the backup list if needed. The constitution of the candidate channel list relies on the extra time that the CPEs will have to do sensing beyond what is required to clear the backup channel list.
- **Protected:** Channels in which incumbent or the WRAN operation has been detected through sensing. Protected channels may be moved to the candidate channel set in the event that the incumbent or the WRAN systems have vacated the channel. Information from the database service or sensing may be used for this purpose. A protected channel may also become a backup channel, but before a protected channel is elevated to backup channel status, it must be sensed as incumbent-free at least every 6 seconds for no less than 30 seconds. The SM should, when possible, determine the type of signals occupying every protected channel (see 10.2.5).
- **Unclassified:** channels that have not been sensed. These channels may be sensed according to the SM implementation. Once an unclassified channel has been sensed, it may be re-classified as protected or candidate channel depending on the sensing results.

For the above channel set as defined: “Disallowed,” “Operating,” “Backup,” “Candidate,” “Protected,” and “Unclassified,” all the states in the set are exclusive to each other, i.e., a channel cannot belong to more than one state at a time. However, because of the WRAN self-coexistence mechanism, an operating channel for one WRAN system can also be the operating channel of another WRAN system (“self-coexistence”) or belong to its backup or candidate list as explained in 10.2.3.1.

The specific algorithms for selecting the operating channel and defining how the backup and candidate channels are prioritized is outside the scope of this standard as long as these implementations meet the

sensing requirements. However, any implementation of these algorithms shall use as input current channel availability information (as described in 10.2.2). Furthermore, other criteria may also be taken into account by the implementation, such as traffic requirements, location information, and self-coexistence with neighboring WRANs.

#### 10.2.3.1 Transition diagrams for channel sets

Each channel on the available channel list that is returned from the database service (see 10.7) belongs to one of the possible channel states by the SM. At the end of the quiet period, depending on the activity of incumbent users and channel quality<sup>21</sup> each channel may transit to other states as shown by the state transition diagram in Figure 162. The transition diagram consists of 5 states and 9 events. The 5 states are described in 10.2.3. Note that these states are classified using spectrum sensing results obtained during WRAN initialization and operation. Therefore, disallowed and unavailable channels are omitted in this state transition diagram because those channels are classified by operator or database service. Possible Events for each state transition are described as follows:

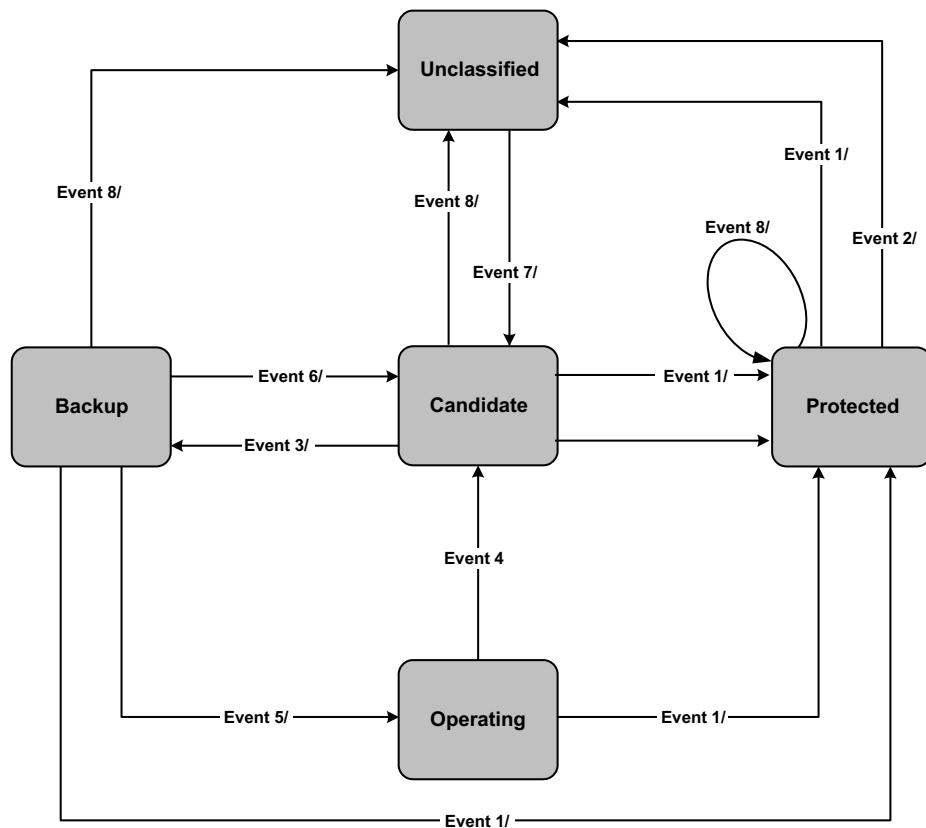
- Event 1: The channel in the operating, backup or candidate set becomes a member of the protected set as an incumbent is detected using spectrum sensing.
- Event 2: No incumbent service has been detected on the channel.
- Event 3: No incumbent has been detected on this channel and the timing requirements for sensing as per the definition of the backup channel are satisfied by all CPEs reporting to the BS. (Furthermore, a prioritization among the back up channels can be made based on the measured channel quality.).
- Event 4: The channel is released due to the termination of WRAN usage.
- Event 5: The channel becomes Operating by its new allocation to the WRAN service.
- Event 6: The timing requirements for sensing are not satisfied as required by the definition of the backup channel by one or more CPEs. (Furthermore, a prioritization among the candidate channels can be made based on the measured channel quality.)
- Event 7: Once an Unclassified channel has been sensed by all active CPEs, it can be re-classified as a Candidate channel by the SM if no incumbent service has been detected and reported within the predefined time duration
- Event 8: If the channel is not sensed within the timing requirements as specified in IEEE Std 802.22 or according to the regulatory domain requirements, the channel becomes Unclassified. However if the channel is in the Protected state and it has not been sensed as required, it shall remain in the Protected state. (Note that a channel has to be sensed by all active CPEs within the pre-defined time duration and the results reported to the BS to not be considered as Unclassified.)

The following legend applies to the transition diagram depicted in Figure 162.

- a) Ovals indicate the state of the channel (the channel set to which it belongs)
- b) Transition lines (i.e., channel state transition) are labeled as Event / Action. Actions triggered by the events for this figure are the state transitions themselves, and so they have been omitted in this diagram.
- c) The detailed explanation for each transition Event is given above.

---

<sup>18</sup> Channel quality refers to a compounded qualitative assessment of the likelihood of the channel to be occupied by an incumbent, the occupancy pattern, the number of CPEs that would be affected by the incumbent and the level of interference-plus-noise in the channel. This assessment has to do with the implementation of the spectrum manager and does not need to be standardized.



**Figure 162 — Channel set transition diagram**

The channel set transition matrix is also presented in Table 250. Each row specifies the state transition due to each event. Each column specifies state transition due to the events in each row for a particular current state.

A shaded cell within the transition matrix implies that either the specific event cannot or should not occur within that state. And if the event does occur, the SM shall ignore it. For example, the Candidate channel cannot transition to Operating channel directly.

**Table 232 — Channel Set Transition Matrix**

<i>State Events \ State</i>	<i>Unclassified</i>	<i>Candidate</i>	<i>Backup</i>	<i>Operating</i>	<i>Protected</i>
<i>Event 1</i>	Protected	Protected	Protected	Protected	
<i>Event 2</i>					Unclassified
<i>Event 3</i>		Backup			
<i>Event 4</i>				Candidate	
<i>Event 5</i>			Operating		
<i>Event 6</i>			Candidate		
<i>Event 7</i>	Candidate				
<i>Event 8</i>		Unclassified	Unclassified		Unclassified

### 10.2.3.2 Backup and Candidate Channel Prioritization using spectrum etiquette

The channel selection at a cell obeys the spectrum etiquette rule so that the chosen channel does not interfere, or interferes with a minimum number of channels to be used by its neighbor cells. Without cooperation, the frequency selection in a cell may lead to one or more BS not having enough channels. For example, the available channel sets at BS1, BS2 and BS3 are {1, 3}, {1, 2, 3} and {1, 2, 3} respectively. If BS2 decides to use channel {1} and BS3 decides to use channel {3}, BS1 would have no channel to use. The cooperation also minimizes the channel collision probability when multiple cells switch their operational channels by avoiding using the same backup channel set.

The channel-selection decision of each cell follows the flowchart in Figure 102. The terms of central cell and neighbor cells are relative concepts. Beside the definition of channel sets as in 10.2.3, the following additional channel sets are defined in spectrum etiquette operation:

- WRAN occupied Channel Set: channels that are operating channels of the discovered neighboring WRAN cell.
- Neighbor WRAN Backup Channel Set: channels that are within the backup channel sets of the discovered neighboring WRAN cells. This channel set is built by listening to SCH/CBPs of the discovered neighboring cells carrying the backup channel information.
- Local Priority Set 1: = (Backup Channel Set U Candidate Channel Set) \ (WRAN-Occupied Channel Set U Neighbor WRAN Backup Channel Set)
- Local Priority Set 2: = (Backup Channel Set U Candidate Channel Set) \ (WRAN-Occupied Channel Set)
- Local Priority Set 3: = (WRAN-Occupied Channel Set)

Note that

- Symbols U,  $\cap$ , and \ are set operation of union, intersection, and exclusion, respectively.
- Local Priority Sets 1~3 is local information, which is not shared with neighbor cells.

The spectrum etiquette is triggered by the following events:

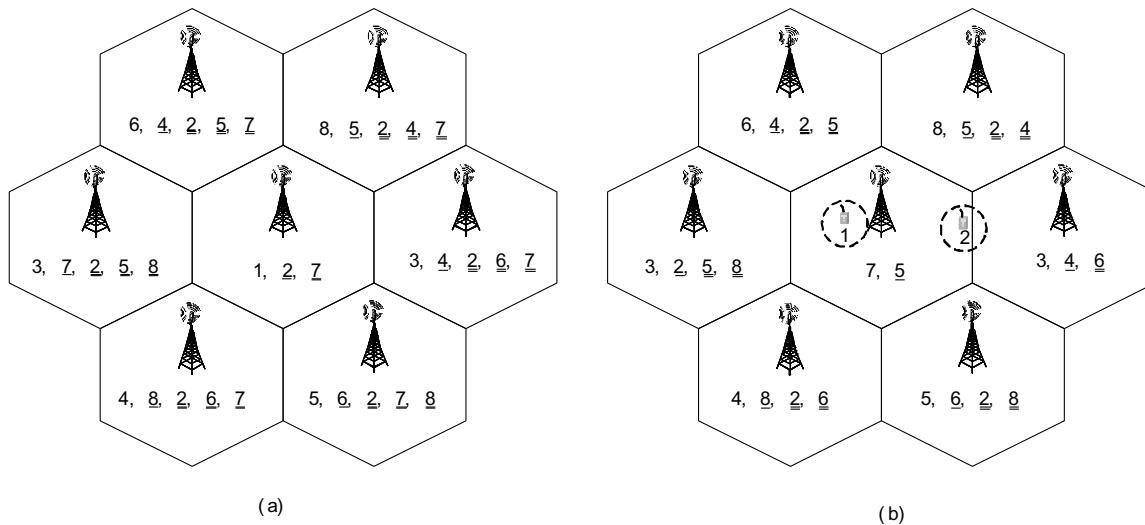
- Incumbent discovery
- Neighbor WRAN cells' discovery/update
- Operating channel switch demand (e.g., due to interference)
- Contention request received from neighbor WRAN cells

The procedure of WRAN spectrum etiquette is depicted in Figure 102 and explained in the following item. Note that the triggering event is defined in the previous paragraph.

- 1) The SM builds/updates channel sets as described in 7.22.1 and 10.2.3, either by receiving indication from the geolocation database, or spectrum awareness of incumbents and WRANs. The neighboring WRAN occupied channel set and neighboring WRAN backup channel set are built/updated accordingly.
- 2) Update backup channel set by choosing one or several channels from Local Priority Set 1; if Local Priority Set 1 is empty, update backup channel set by choosing one or several channels from Local Priority Set 2 that are backup channels by the least number of neighbor cells; (if several channels are backup channels of the same number of neighbor cells, the present cell shall choose from those channels randomly.) if Local Priority Set 2 is also empty, choose one or several channel from Local Priority Set 3, which are operating channels by the least number of neighbor cells; (if several channels are operating channels of the same number of neighbor cells, the present cell shall choose from those channels randomly.)

- 3) If switching operating channel is necessary or demanded by higher layer indication (due to incumbent discovery in the operating channel, significant detected interference in the operating channel, or preferable channel quality of a backup channel, etc.), promote the first backup channel to operating channel; go to step 2) to update backup channel set;
- 4) If the new operating channel is also an operating channel of a neighbor cell, initialize the self-coexistence contention procedure as described in 7.20.3.2.
- 5) Update the neighbor cells with new operating and backup channel sets via SCH/CBP.

The spectrum etiquette procedure is further illustrated using the example in Figure 163. The central cell has six neighbor cells. The central cell has one operating channel #1, one backup channel #2 (underlined), and one candidate channel #3 (double underlined). The channel sets information for the neighbor cells are accordingly noted as in Figure 163 (a). In Figure 163 (b), two incumbents appear in the central cell on the operating and backup channel, and thus the central cell is forced to change both its operating and backup channel. The spectrum etiquette is triggered. The former candidate channel #7 is promoted to operating channel, and channel #5 is promoted to backup channel, which is only used by one neighbor cell as the operating channel. All the neighbor cells perform spectrum etiquette after receiving the channel set update information from the central cell accordingly, and the resultant channel sets for each cell are illustrated in Figure 163 (b) and Table 233. If another incumbent appears in the central cell on channel #7, the central cell will have to use channel #5 as the operating channel and start contention-based self-coexistence with its neighbor cell. The SM may use information on the performance on the CPE antenna to prioritize the list of candidate channels (see 7.7.7.3.4.9).



**Figure 163 — Illustration of the procedure of spectrum etiquette**

**Table 233 — Illustration of the spectrum etiquette procedure**

Central cell status	Before	Upon incumbent appearance	After spectrum etiquette
Operating Channel Set	1	‡	7
Backup Channel Set	2	‡	5
Candidate Channel Set	7	3,4,5,6,7,8	∅
WRAN-Occupied Channel Set	3,4,5,6,8	3,4,5,6,8	3,4,5,6,8
Neighbor Backup Channel Set	4,5,6,7,8	3,4,5,6,7,8	4,5,6,7,8
Local Priority Set 1:	2	‡	∅
Local Priority Set 2:	2,7	‡,7	∅
Local Priority Set 3:	3,4,5,6,8	‡,3,4,5,6,7,8	3,4,5,6,8

#### 10.2.4 Association control

Association is defined as the process by which the CPE completes the registration with the BS. When CPEs request association with a WRAN BS (see CPE initialization procedure described in 7.14.2), the SM is responsible for granting or denying association rights to the requesting CPEs. For that, the SM shall consider location information, and basic and registered capabilities of each requesting CPE. The SM shall access the database service, to obtain the list of available channels and corresponding maximum EIRP limits at the CPE's location, and based on the received information, the SM shall decide whether to grant association rights to the CPE in its current operating channel and indicate the maximum transmit EIRP allowed for the CPE. It is the responsibility of the SM to granting association rights to the requesting CPE while avoiding harmful interference to incumbents. The SM shall make a decision on CPE association during the CPE registration process (REG-REQ) if it is satisfied that the specifications and capabilities of the CPE are within the tolerable limits for it to join the network.

#### 10.2.5 Spectrum Manager policies

The SM shall be responsible for enforcing the IEEE 802.22 policies within the cell in order to guarantee the required protection of incumbents while supporting QoS for the WRAN users. The SM shall adhere to the policies as specified in Table 234.

Each of the policy in Table 234 is identified using a Policy ID, the event that triggers the policy, the event description and the corresponding action.

Policies with enumeration 1 are related to the events initiated from the database service but not from a locally generated operator database in case the local regulatory domain does not specify the use of such an incumbent database. For the purposes of the IEEE 802.22 operation, a database containing location dependent available channels shall always exist. The SM shall be responsible for accessing the database service in the regulatory domains that mandate the presence of such a database service. In the regulatory domains that do not mandate a database service, a database of available channels shall be provided by the operator. When operating in a regulatory domain that does not require a database service, all channels are initially assumed to be available.

Policies with enumeration 2 are related to an event that a TV signal is detected.

Policies with enumeration 3 are related to an event that a wireless microphone signal or the IEEE 802.22.1 beacon signal is detected.

Remaining policies are a combination of these earlier events or related to whether an IEEE 802.22 device is allowed to transmit under certain conditions.

The actions shall include:

- Switch the entire cell to a new operating channel
- Direct a single CPE or a group of CPEs to a different operating channel when possible
- Terminate operation in a given channel for a single CPE, a group of CPEs or the entire cell

The SM shall use one of the channel management mechanisms defined in 10.2.3.

Each channel management action may be triggered by one or more events. For instance, the action of switching channels for the entire cell may be triggered by the detection of an incumbent on the operating channel, by degradation of the QoS due to interference, or traffic load in the current channel.

Although different trigger events may be supported depending on the implementation, the trigger events and corresponding channel management actions shall be executed as described in Table 234 to provide protection of incumbents or as required by regulatory policies applicable within the regulatory domain.

Note that the value for timer Tch\_move (i.e., T44, see Table 276) used in Table 234 is to be found in Annex A for the various Regulatory domains where the WRAN operation takes place (see A.3.2). The default value of Tch\_move shall be 2 seconds.

**Table 234 — Spectrum Manager policies**

Policy ID	IEEE 802.22 component involved	Event trigger	Event description	Action
1a	BS	DB S	If the SM is directed by the database service that the current operating channel is no longer available for the BS (see 10.7.1.6).	Set the Flag <i>Initiate_Channel_Move</i> to '1'. Initiate a channel switch of the entire cell to a new operating channel within ( <i>Tch_move</i> – 0.5) seconds from the time when the database service informed the SM. The new operating channel should be the highest priority backup channel. The timer <i>Tch_move</i> (i.e., T44) is to be found in Annex A for the various Regulatory domains where the WRAN operation takes place. The default value of the <i>Tch_move</i> shall be 2 seconds.
1b	CPE	DBS	If the SM is directed by the database service that the current operating channel is no longer available for some of the CPEs (see 10.7.1.6).	<p><b>Option 1:</b> Set the Flag <i>Initiate_Channel_Move</i> to '1'. Initiate a channel switch of the entire cell to a new operating channel within (<i>Tch_move</i> – 0.5) seconds from the time when the database service informed the SM. The new operating channel should be the highest priority backup channel. The default value of the <i>Tch_move</i> shall be 2 seconds.</p> <p><b>Option 2:</b> Disassociate the CPEs that are not allowed to operate on the current channel within (<i>Tch_move</i> – 0.5) seconds from the time when the database service informed the SM and continue normal operation with the other CPEs. A DREG-CMD with Action Code = 0x04 (7.7.12), aimed at dropping their association on the current operating channel, shall be sent to these CPEs so that they no longer wait for an allocation in the US-MAP and/or transmit an opportunistic BW request UCS or Ranging request. Optionally, the BS may signal the affected CPEs to move to a particular channel using the DREG-CMD with Action Code = 0x00, in order to re-associate with another BS and continue their operation. The default value of the <i>Tch_move</i> shall be 2 seconds.</p>
1c	BS	DBS	If the SM obtains information from the database service that indicates the current operating channel will become unavailable for the BS at a specific time in the future (see 10.7.1.6 and 10.7.2.3).	<p><b>Option 1:</b> Set the Flag <i>Initiate_Channel_Move</i> to '1'. Initiate a channel switch of the entire cell to a new operating channel no later than (<i>Tch_move</i> – 0.5) seconds after the time specified by the database service. The new operating channel should be the highest priority backup channel. The default value of the <i>Tch_move</i> shall be 2 seconds.</p> <p><b>Option 2:</b> Disassociate the CPEs that are not allowed to operate on the current channel within (<i>Tch_move</i> – 0.5) seconds after the time specified by the database service and continue normal operation with the other CPEs. A DREG-CMD with Action Code = 0x04 (7.7.12) aimed at dropping their association on the current operating channel shall be sent to these CPEs so that they no longer wait for an allocation in the US-MAP and/or transmit an opportunistic BW request UCS or Ranging request. Optionally, the BS may signal the affected CPEs to move to a particular channel using the DREG-CMD with Action Code = 0x00, in order to re-associate with another BS and continue their operation. The default value of the <i>Tch_move</i> shall be 2 seconds.</p>

1d	CPE	DBS	If the SM obtains information from the database service that indicates the current operating channel will become unavailable for some of the CPEs at a specific time in the future (see 10.7.1.6 and 10.7.2.3).	<p><b>Option 1:</b> Schedule a channel switch for the entire cell to a new operating channel at least 0.5 seconds before the expected time (as obtained from the database service) at which its current channel will become unavailable, by setting the Flag Initiate_Channel_Move to '1'. The new operating channel should be the highest priority backup channel.</p> <p><b>Option 2:</b> If the channel is going to be unavailable for a period of time less than the CPE_Registration_Timer (7.14.2.1.1), then temporarily dis-associate and disable the CPEs that are not allowed to operate on the current channel within (Tch_move - 0.5) seconds from the time when the database service informed the SM and continue normal operation with the other CPEs. A DREG-CMD with Action Code = 0x01 shall be sent to the CPEs (see 7.7.12), so that the CPEs affected will shutdown their transmission and only listen on the channel. Later, the BS may signal the affected CPEs to move to return to normal operation on that channel using the DREG-CMD with Action Code = 0x03 in order to re-associate with another BS and continue their operation. If the period of unavailability is greater than the CPE_Registration_Timer, than the timer will expire and the CPE shall attempt re-association on the next available channel. The default value of the Tch_move shall be 2 seconds.</p>
1e	BS	DBS	Where a database service exists for the regulatory domain of operation (see Annex A), if such a service becomes unavailable for greater than T45 specified in Annex A, Table A.16 for that domain (default value for T45 shall be 1 hour) (see 10.7.1.2).	The BS shall de-register its associated CPEs and terminate its own operation until the database service becomes available.
1f	CPE	DBS	Where a database service exists for the regulatory domain of operation (see Annex A), and if a new CPE is trying to register (see 10.7.1.4 and 10.7.1.6).	Do not allow the CPE to register to the network until the channel availability information is available.

			<p>If the signal detected on the operating channel or either of its first adjacent channels is a TV signal through the BS spectrum sensing function or through a combination of sensing results from multiple CPEs.</p> <p><sup>1</sup> Detection threshold is to be found in Annex A for the various Regulatory domains where the WRAN operation takes place.</p>	<p>Note the information about the detection of TV signal and make it available according to the local regulatory requirements.</p> <p>Does the local regulatory domain require to vacate the channel on confirmation of the presence of a TV signal?</p> <p>No further action</p> <p>Set the Flag Initiate_Channel_Move to '1'. Initiate a channel switch of the entire cell to a new operating channel within (Tch_move - 0.5) seconds from the time when the TV signal was detected. The new operating channel should be the highest priority backup channel. The value for Tch_move is to be found in Annex B for the various Regulatory domains where the WRAN operation takes place. The default value of the Tch_move shall be 2 seconds.</p>
2	BSCPE	Signal detected		

<p>If the signal detected on the operating channel is a wireless microphone signal through the BS spectrum sensing function or through the sensing results from a CPE or a combination of multiple CPEs.<sup>2</sup></p> <p>2. The following action should apply to any of the nodes (BS or CPE) that detected the wireless microphone signal.</p> <p><b>NOTE</b>— The variable microphone protection radius (MPR) is defined in Annex A for the various Regulatory domains where the WRAN operation takes place. The default value of the MPR shall be 4 km.</p>	<p>Note the information about the detection of wireless microphone signal and make it available according to the local regulatory requirements.</p> <pre> graph TD     A{Clearance radius exists for W-microphone} -- No --&gt; B[Set the Flag Initiate_Channel_Move to '1']     A -- Yes --&gt; C{Can the location of the wireless microphone be determined?}     C -- No --&gt; B     C -- Yes --&gt; D{BS within the clearance radius of the wireless mike?}     D -- No --&gt; B     D -- Yes --&gt; E[Set the Flag Initiate_Channel_Move to '1']   </pre>
---	--

<p><b>3b</b></p> <p><b>BSCPE</b></p> <p><b>Signal detected</b></p> <p>If the signal detected on the operating channel is an IEEE 802.22.1 wireless microphone beacon signal.<sup>1</sup></p> <p>The following action should apply to any of the nodes (BS or CPE) that detected the IEEE 802.22.1 wireless microphone beacon signal.</p> <p><b>NOTE</b>—The variable Microphone_Protection_Radius (MPR) is defined in Annex A for the various Regulatory domains where the WRAN operation takes place. The default value for MPR shall be 4 km.</p>	<p>Note the information about the detection of wireless microphone beacon signal and make it available according to the local regulatory requirements.</p> <pre> graph TD     A[Can the location of the microphone beacon be determined?] -- No --&gt; B[BS within the protected radius of the wireless mikes?]     A -- Yes --&gt; C[Complete cell move]     B -- No --&gt; D[Complete cell move]     B -- Yes --&gt; E[BS skips the beacon authentication step. Set the Flag Initiate_Channel_Move to '1' and initiate the switching of the entire cell to a new operating channel within (Tch_move - 0.5) seconds of the time when the beacon was detected. The new operating channel shall be the highest priority backup channel.]     E --&gt; F[Option I (No Authentication): BS skips the beacon authentication step. Set the Flag Initiate_Channel_Move to '1' and initiate the switching of the entire cell to a new operating channel within (Tch_move - 0.5) seconds of the time when the beacon was detected. The new operating channel shall be the highest priority backup channel.]     F --&gt; G[Option II (Authentication): A (Tch_move - 0.5) second timer is set. BS shall authenticate the beacon by scheduling quiet periods within (Tch_move - 0.5) seconds, ask the CPEs to capture the required portion of the 802.22.1 payload and decode the MSF1, MSF2, and/or MSF3 fields as found sufficient by the operator. If the IEEE 802.22.1 beacon is found to be authentic or (Tch_move - 0.5) seconds timer expires, then the BS shall initiate the switching of the entire cell to a new operating channel which should be the highest priority backup channel. If the beacon is found to be non-authentic, no action is taken. The default value of Tch_move shall be 2 seconds.]     G --&gt; H[Specific CPEs cease to operate or move]   </pre> <p><b>Option I (No Authentication)</b>: BS skips the beacon authentication step and dis-associates the CPEs that are within less than MPR from the wireless microphone operation within (Tch_move - 0.5) seconds from the time when the IEEE 802.22.1 signal was detected and continue normal operation with other CPEs. A DREG-CMD with Action Code = 0x04 shall be sent to these CPEs before dropping their association so that the CPEs no longer wait for an allocation in the US-MAP and/or transmit an opportunistic BW request, UCS notification or Ranging request. Optionally, the BS may signal the next channel to go to for the dis-associated CPEs in the DREG-CMD with Action Code = 0x00 before shutting down the communication. The default value of Tch_move shall be 2 seconds.</p>
---	---

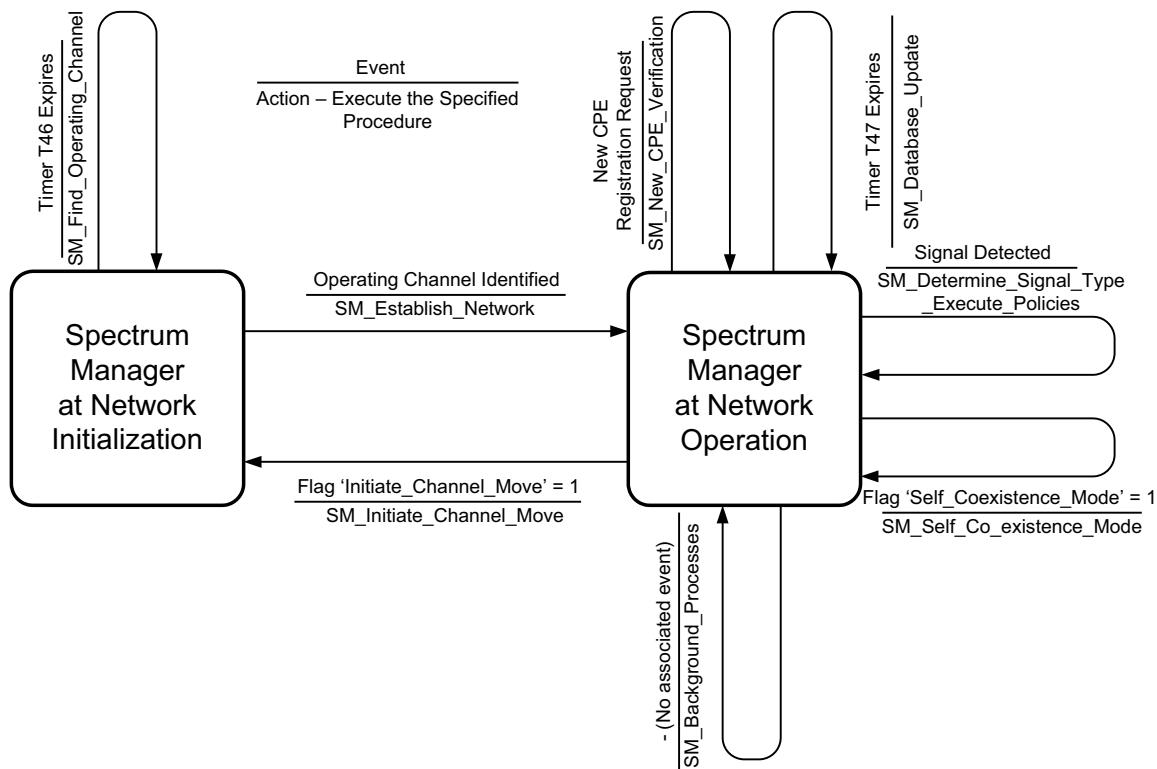
			<b>Option II (Authentication):</b> A (Tch_move – 0.5) second timer is set. BS shall authenticate the beacon by scheduling quiet periods within (Tch_move – 0.5) seconds, ask the CPEs to capture the required portion of the IEEE 802.22.1 payload and decode the MSF1, MSF2, and/or MSF3 fields as found sufficient by the operator. If the IEEE 802.22.1 beacon is found to be authentic or (Tch_move – 0.5) seconds timer expires then the BS shall dis-associate the CPEs that are within MPR from the wireless microphone operation within (Tch_move – 0.5) seconds from the time when the 802.22.1 signal was detected and continue normal operation with the other CPEs. A DREG-CMD with Action Code = 0x04 shall be sent to these CPEs before dropping their association so that the CPEs no longer wait for an allocation in the US-MAP and/or transmit an opportunistic BW request, UCS or Ranging request. Optionally, the BS may signal the next channel to go to for the dis-associated CPEs in the DREG-CMD with Action Code 0x00 before shutting down the communication. If the beacon is found to be non-authentic, no action is taken. The default value of Tch_move shall be 2 seconds.
4	BS/CPE	DBS or Signal detected	If there is no backup channel available AND (if the database service indicates that the current operating channel is not available or the signal detected on the operating channel is a wireless microphone or an IEEE 802.22.1 signal, or, in case of a TV signal, the signal is detected on the operating or any of its first adjacent channels) (see 10.7.1.6 and 10.7.4.3).  5
5	CPE	Signal detected	If before the CPE has registered with a BS on the same channel, the signal detected on the operating channel is a wireless microphone or an IEEE 802.22.1 signal, or, in case of a TV signal, the signal is detected on the operating or any of its first adjacent channels.  6
6	CPE	Signal detected	If the signal detected on the operating channel is a wireless microphone or an IEEE 802.22.1 signal, or, in case of a TV signal, the signal is detected on the operating or any of its first adjacent channels and the CPE has already registered with the BS.
7a	BS/CPE	DBS or Signal detected	If the SM confirms the presence of any other device that is granted protection in the regulatory domain (see Annex A).  7b
7b	BS/CPE	Signal detected	No action is to be taken.

8	CPE	Geolocation	BS has determined that the position of the CPE has changed by greater than that specified by the local regulations (see Annex A) (default 50 m radius).	BS shall request the CPE to geolocate and report its position to verify the change in location. If the location is confirmed to have changed, the BS shall immediately obtain a new list of available channels from the database service based on the new location of the CPE. The CPE shall abide by the EIRP limit specified by the database service or, if not available, abide by the regulatory requirements specified in Annex A. If the service for the affected CPE on the current operating channel at the new location is prohibited or if the device type is fixed as specified in Annex A, then the BS shall de-register the CPE using DREG-CMD with Action Code = 0x04.
---	-----	-------------	---	--

## 10.2.6 Spectrum Manager operation

The SM, as shown in the IEEE 802.22 reference model (Figure 4), shall be part of the cognitive plane and shall always be present at the IEEE 802.22 BS. The SM is responsible for important tasks, such as maintaining spectrum availability information, channel selection, channel management, scheduling spectrum sensing operation, access to the database, enforcing IEEE 802.22 and regulatory domain policies, enabling self-coexistence, etc. The detailed operation of the SM state machine and procedures is described in the following subclauses.

### 10.2.6.1 Spectrum Manager state machine



**Figure 164 — Spectrum Manager state machine**

Figure 164 describes the SM state machine diagram. The SM has two states of operation, namely, the SM at Network Initialization, and the SM at Network Operation.

The Timer T46 in the State SM at Network Initialization shall be initially set to a default value of 20 ms. However; the value of this timer shall be configurable in accordance with the other regulatory domain requirements as specified in the Annex A.

During the Network Initialization state, the primary responsibility of the SM shall be to find the operating channel.

Once the Timer T46 expires, the SM shall execute the Procedure SM\_Find\_Operating\_Channel. The various tasks involved in order to find an operating channel have been illustrated in Figure 165.

In case, the SM at this stage already has an exclusive backup channel to operate on, the SM shall choose the operating channel based on spectrum etiquette as described in 10.2.3.2. The SM shall then execute the Procedure `SM_Establish_Network` in the Normal Mode and move to the State Spectrum Manager at Network Operation. This may happen when the SM was operating on some other channel before where it had already computed its backup channels, and now it is in a transition after it has initiated a channel move.

In case, no exclusive backup channels are available, the procedure to find an operating channel shall consist of accessing the database service to obtain a list of available channels, discovering neighboring IEEE 802.22 systems, synchronizing and scheduling quiet periods, initiating sensing for the primary user signals and exploring the possibility to convert some of the available channel to an operating channel once the conditions in 10.2.3 have been met. In selecting the new operating channel from the list of available channels, consideration should be given to the relative performance of the BS receive antenna at these various available channels for best operation.

#### **10.2.6.2 Procedure SM\_Find\_Operating\_Channel**

The SM shall make sure that the database service is available within T45. If this is not the case, then it shall execute Policy 1e. Timer T45 as specified in Procedure `SM_Find_Operating_Channel` indicates the longest time that a WRAN service can operate in the un-licensed band without access to the database service. The timer values may be initially set to the United States regulatory domain, however they shall be configurable in accordance with the other regulatory domain requirements as specified in Annex A.

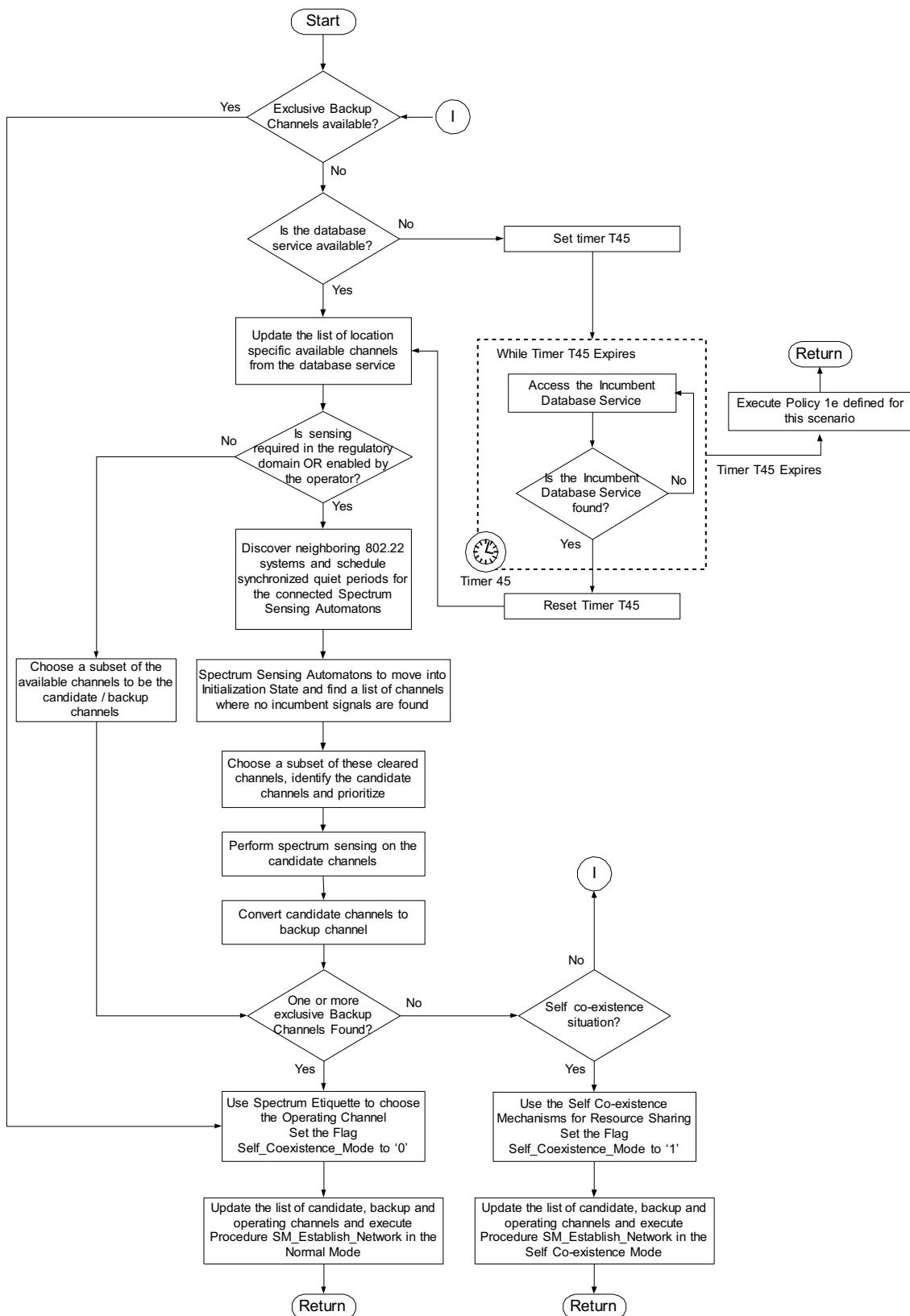
The SM shall take into consideration the database service information, to find a list of available channels. The SM shall then synchronize its quiet periods to other IEEE 802.22 systems, schedule its own quiet periods and convey the quiet period information to the Spectrum Sensing Automatons through a SCH or an appropriate MAC message. The SSA shall move into the ‘Initialization State’ as described in 10.3.2. Based on the sensing information, the Spectrum Sensing Automatons shall provide the SM with a list of candidate channels as a subset of the available channels. The SM shall schedule further quiet periods to convert the list of candidate channels to backup channels.

A candidate channel shall become a backup channel and a backup channel shall become an operating channel based on the state transition diagram as specified in 10.2.3.

In case one or more exclusive backup channels are available, the SM shall choose an operating channel using spectrum etiquette as described in 10.2.3.2. The SM may also use information on the performance on the CPE antenna to prioritize the list of candidate channels (see 7.7.7.3.4.9). The SM shall set the Flag `Self_Coexistence_Mode` to ‘0’, execute the Procedure `SM_Establish_Network` and move to the State Spectrum Manager at Network Operation.

As soon as the SM moves to the State Network Operation, it shall set the Timer  $T_{\text{Refresh\_Database\_Info}}$ . The default value for the Timer  $T_{\text{Refresh\_Database\_Info}}$  shall be 1 hour; however, the value for this timer shall be configurable in accordance with the other regulatory domain requirements as specified in the Annex A.

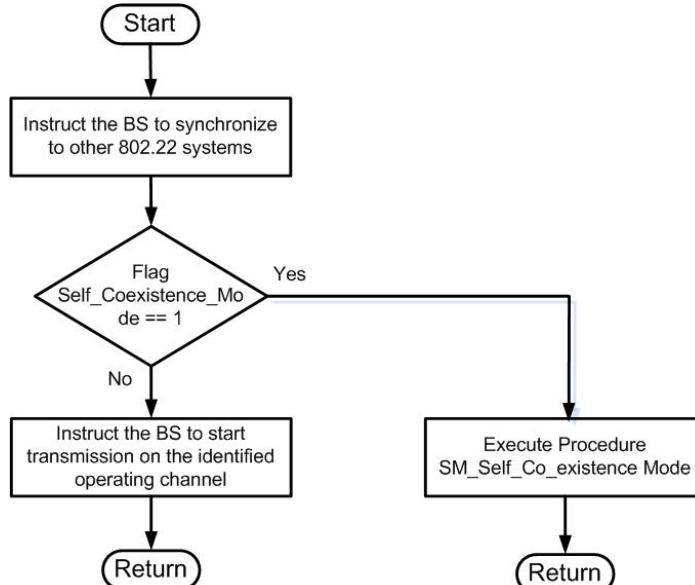
In case no exclusive backup channels are found, the SM shall execute Procedure `SM_Establish_Network` in the Co-existence Mode. In this case, the SM shall set the Flag `Self_Coexistence_Mode` to ‘1’, execute the Procedure `SM_Establish_Network` and move to the State Spectrum Manager at Network Operation.



**Figure 165 — Procedure find operating channel**

### 10.2.6.3 Procedure SM\_Establish\_Network

The Procedure SM\_Establish\_Network has been illustrated in Figure 166. Initially, the SM shall instruct the BS to synchronize to other IEEE 802.22 systems. If it is the Normal Mode of operation (Flag Self\_Coexistence\_Mode is ‘0’), the BS shall start transmission on the identified operating channel and wait for the CPEs to join the network. The CPE initialization operation and registration operation has been described in 7.14.2 and 7.14.2.11, respectively.



**Figure 166 — Procedure Establish\_Network**

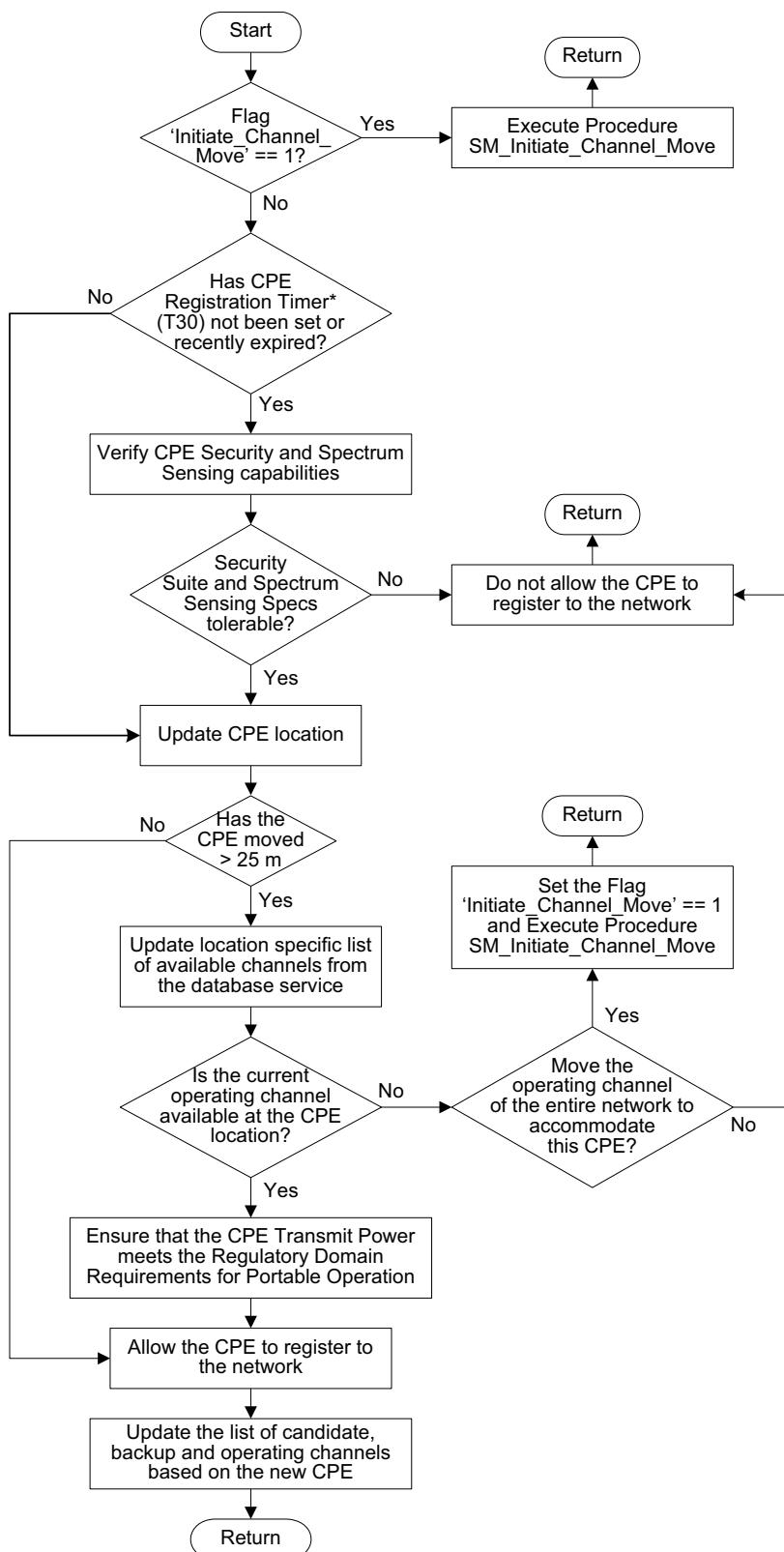
In the Self Co-existence Mode of operation, the BS shall execute Procedure SM\_Self\_Coexistence\_Mode which is described below.

### 10.2.6.4 Procedure SM\_CPE\_Registration\_and\_Tracking

For each new CPE that has never before registered with the BS and that makes the registration request to the BS, the SM shall access the database service to verify if the current operating channel is available at the CPE location. In addition, the SM shall verify the security suite that the CPE supports and its spectrum sensing capabilities are within tolerable limits. If the SM finds that the current occupied channel is not available at the CPE location, or the CPE capabilities are less than required, it shall choose to prevent the CPE from registering to the network. The SM shall also track the location of each CPE. Policy 8 in 10.2.5 specifies the action to be taken in case the location of any CPE has changed.

The SM may also make a decision that in order to accommodate one or more such CPEs; it may need to move to another operating channel. In this case, the SM shall set the Flag Initiate\_Channel\_Move to ‘1’ and execute the Procedure SM\_Initiate\_Channel\_Move. Figure 167 illustrates the SM operation during Procedure SM\_CPE\_Registration\_and\_Tracking.

Note that the CPE registration messaging contains the location information as a NMEA string. The BS also tracks the CPE location by requesting CPE re-registration based on the expiration of timer T30 (see 7.14.2.11), for which the value can be configured for fixed or portable operation (see 7.7.7.3.5).

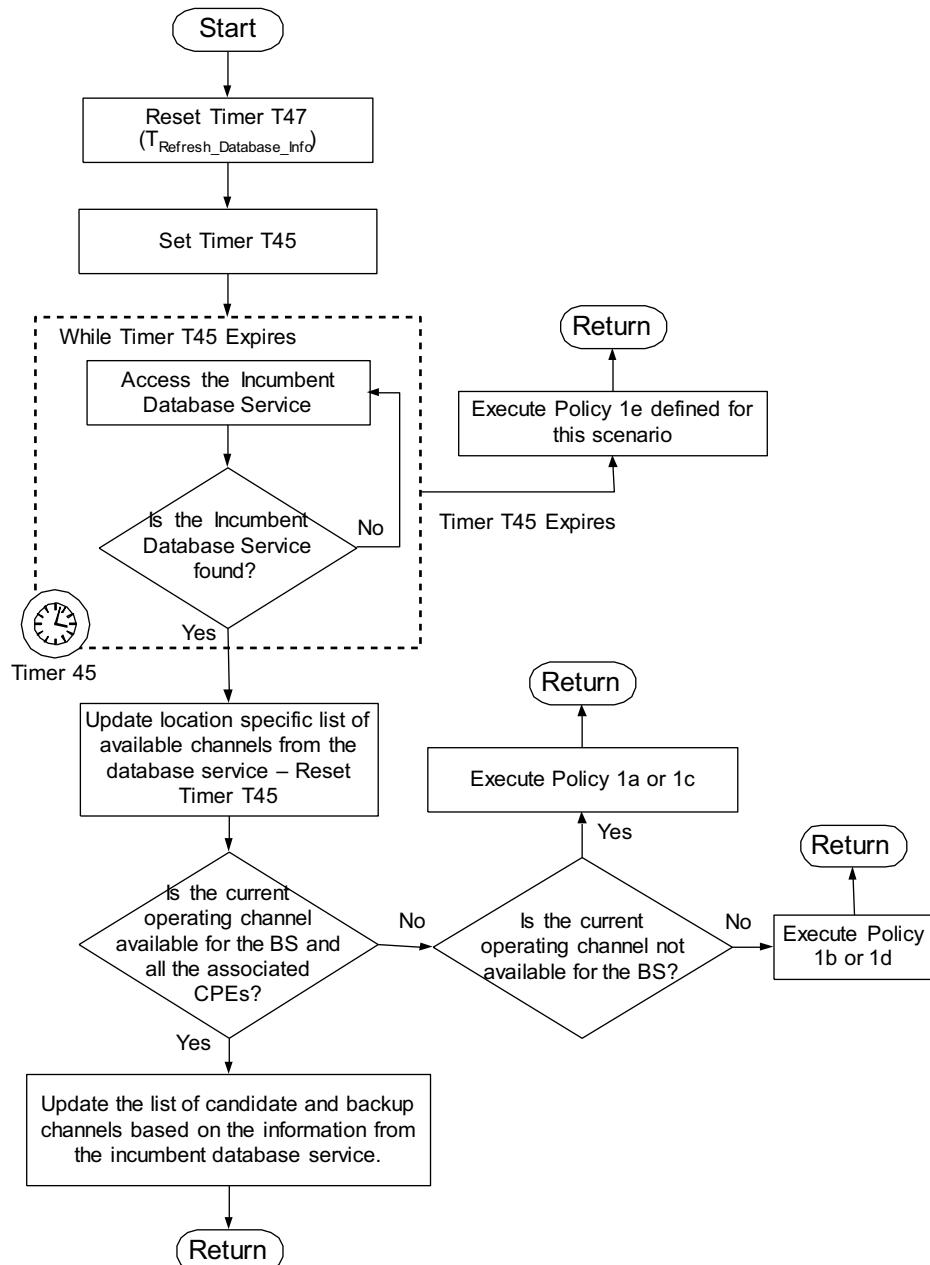


**Figure 167 — Procedure SM\_CPE\_Registration\_and\_Tracking**

### 10.2.6.5 Procedure SM\_Database\_Update

In the event that the Timer  $T_{\text{Refresh\_Database\_Info}}$  expires, the SM shall execute Procedure SM\_Database\_Update as illustrated in Figure 168. During this procedure, the SM shall verify that the current operating channel is available for itself and all its CPEs. If the current operating channel is available for the BS and all its associated CPEs, the BS shall continue the operation on the existing operating channel.

If the current operating channel is not available for the BS or one or more of its CPEs, the SM shall execute the policies as specified in the Spectrum Manager policies in 10.2.5 and as shown in Figure 168. The SM shall also update the candidate and backup channel list based on the new information.



**Figure 168 — Procedure SM\_Database\_Update**

#### 10.2.6.6 Procedure SM\_Determine\_Signal\_Type\_Execute\_Policies

If the SM is notified that a signal is detected through the SSAs of the BS or one or more of its CPEs, the SM shall execute Procedure SM\_Determine\_Signal\_Type\_Execute\_Policies. The Procedure SM\_Determine\_Signal\_Type\_Execute\_Policies is illustrated in Figure 169. If a signal is detected, but its signal type cannot be determined, the SM shall schedule additional quiet periods for a larger spectrum sensing integration time. Based on the type of signal that is detected, the SM shall execute policies as specified in the Spectrum Manager policies in 10.2.5.

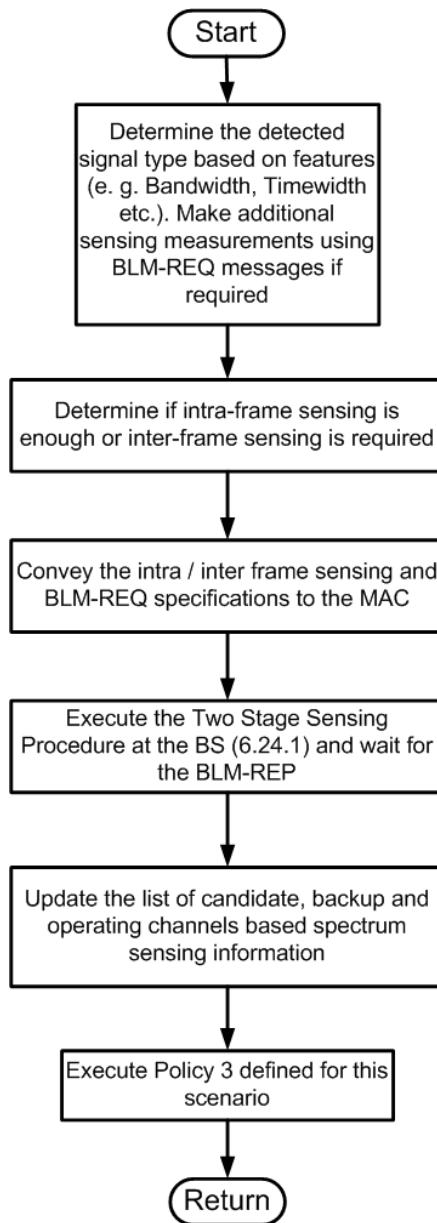
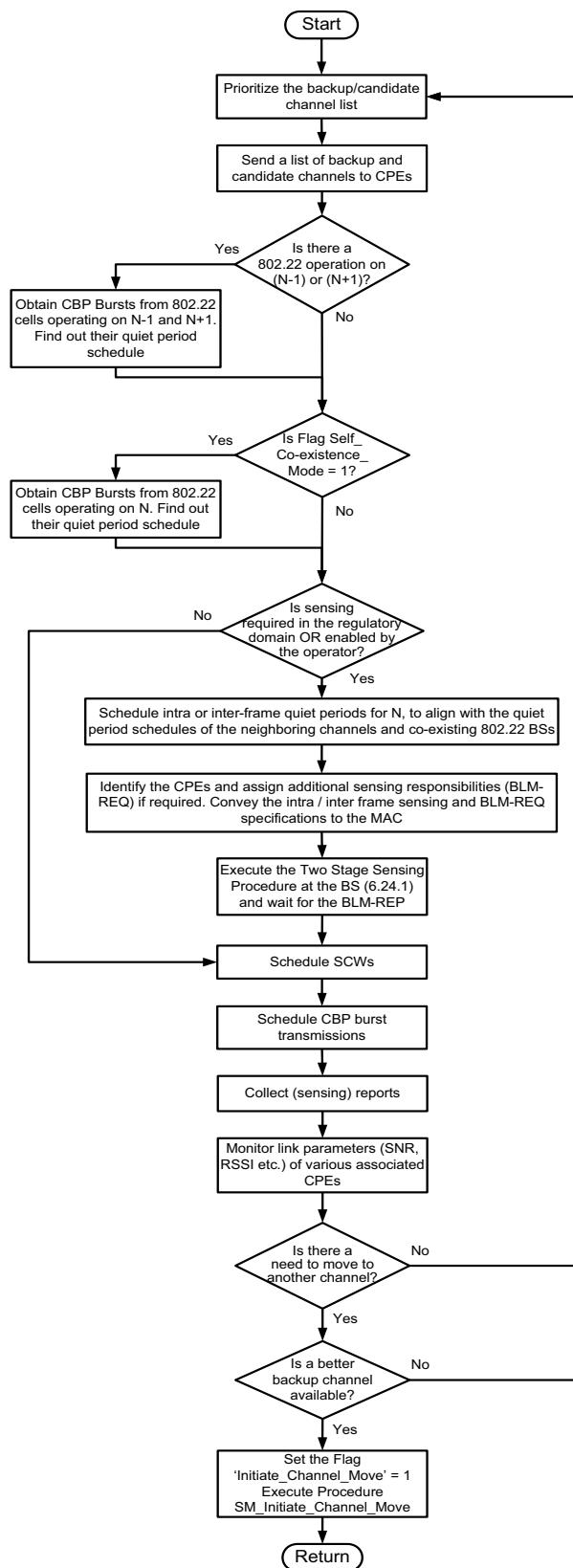


Figure 169 — Procedure SM\_Determine\_Signal\_Type\_Execute\_Policies

#### **10.2.6.7 Procedure SM\_Background\_Processes**

SM shall constantly run the Procedure SM\_Background\_Processes. In this procedure, the SM shall be responsible for prioritizing the list of backup/candidate channels, scheduling the quiet periods, assigning the sensing responsibilities to the corresponding SSAs, scheduling the CBP transmissions, scheduling the Self Co-existence Windows (SCWs) collecting the spectrum sensing reports (through BLM-REP), maintaining the channel state information, monitoring the link quality of various CPEs, and deciding if channel move is needed. The prioritization of the backup/candidate channel list shall be based on information from the database service, spectrum sensing information, spectrum etiquette and the information on the CPE antenna gain as a function of frequency. The SM operation during Procedure SM\_Background\_Processes has been illustrated in Figure 170.



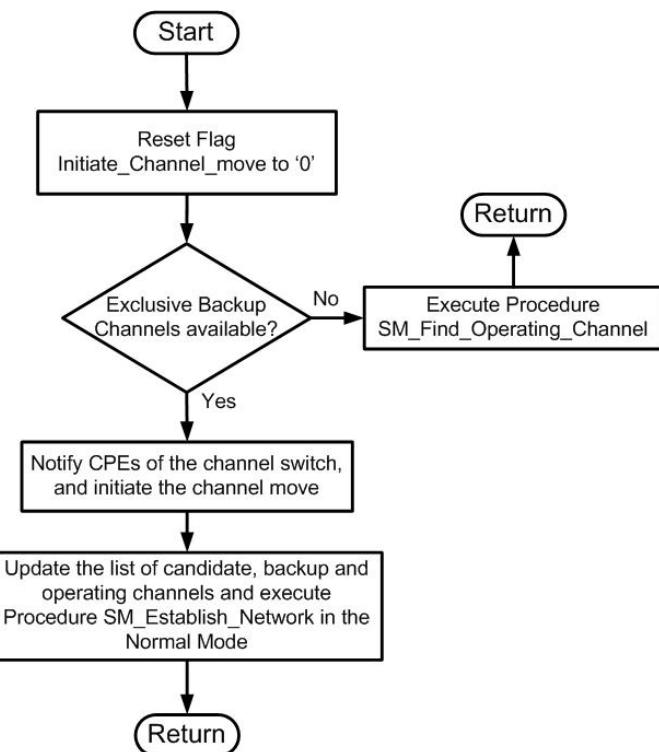
**Figure 170 — Procedure SM\_Background\_Processes**

#### **10.2.6.8 Procedure SM\_Initiate\_Channel\_Move**

In case the SM finds that there is a need to move to another channel, the SM shall set the Flag Initiate\_Channel\_Move to ‘1’.

If the Flag Initiate\_Channel\_Move is set to ‘1’, then the SM shall execute Procedure SM\_Initiate\_Channel\_Move. Procedure SM\_Initiate\_Channel\_Move has been illustrated in Figure 171. During the execution of this procedure the SM shall reset the Flag Initiate\_Channel\_Move to ‘0’. If exclusive backup channels are available, the SM shall update the list of operating, candidate and backup channels, and execute Procedure SM\_Establish\_Network.

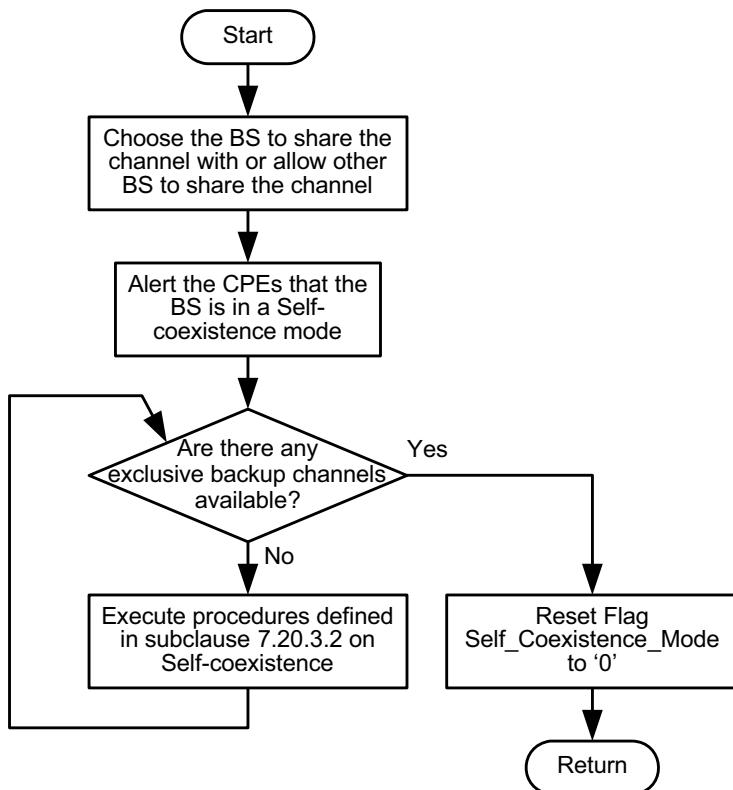
In case no exclusive backup channels are available, the SM shall execute Procedure SM\_Find\_Operating\_Channel.



**Figure 171 — Procedure SM\_Initiate\_Channel\_Move**

#### **10.2.6.9 Procedure SM\_Self\_Coexistence\_Mode**

If the Flag Self\_Coexistence\_Mode is set to ‘1’, then the SM shall execute Procedure SM\_Self\_Coexistence\_Mode as illustrated in Figure 172. During the Procedure SM\_Self\_Coexistence\_Mode, the SM shall choose a BS to share the channel with, or allow another BS to share its own channel, alert the CPEs that the BS is in the self-coexistence mode via the SCH, and assist the BS in executing procedures that are defined in 7.20.3.2 on self co-existence mechanisms. In case an exclusive backup channel becomes available, the SM shall reset the Flag Self\_Coexistence\_Mode to ‘0’.



**Figure 172 — Procedure SM\_Self\_Coexistence\_Mode**

### 10.3 Spectrum Sensing Automaton (SSA)

All the IEEE 802.22 devices (BS and CPEs) shall also have an entity called the Spectrum Sensing Automaton (SSA). The SSA interfaces to the Spectrum Sensing Function (SSF) and executes the commands from the SM to enable spectrum sensing. The BS normally controls the sensing behavior of the SSA. However, the SSA shall control its sensing behavior locally under the following six conditions:

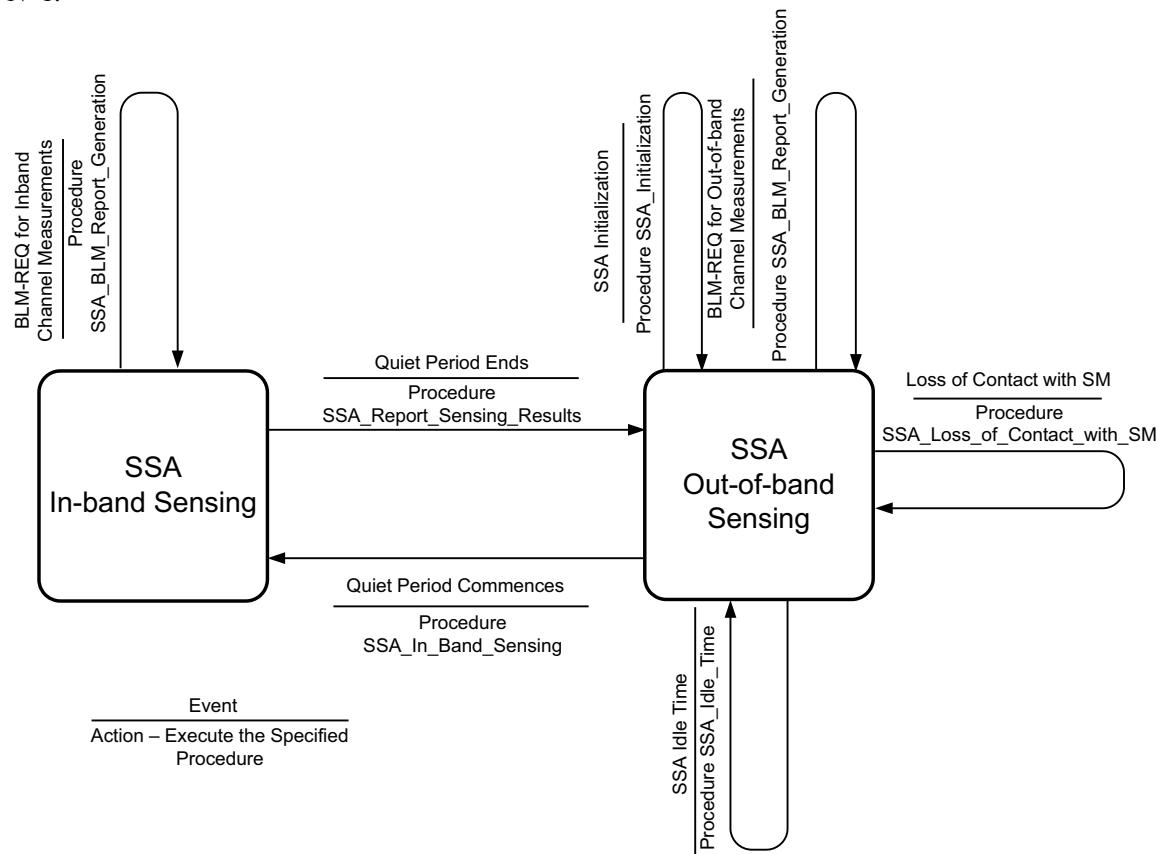
- 1) At the initial turn-on of the BS before it starts to transmit any signal
- 2) at initial turn-on of the CPE before association is established with the base station
- 3) During the quiet periods defined by the SM and signaled by the BS through the SCH for in-band sensing
- 4) During out-of-band sensing at the BS when the base station is not transmitting
- 5) During idle time at the CPE when the base station has not attributed any specific task to the CPE sensing signal path through the BLM-REQ message, see 7.7.18.1, when the CPE does not transmit or, if the WRAN operation and RF sensing use the same tuner, when the CPE does not transmit or receive
- 6) When the CPE loses contact with its base station.

The functionality of the SSA for these six specific cases, and embodied in the local sensing automaton, is covered by the normative behavioral models described in the following subclauses.

### 10.3.1 SSA state machine operation

The SSA state machine operation is shown in Figure 173. The SSA state machine consists of two states—SSA In-band Sensing and SSA Out-of-band Sensing. During the SSA Out-of-band Sensing state, the SSA may execute any of the three procedures as described in 10.3.2, 10.3.4, and 10.3.5, based on the event that may have occurred.

During the SM scheduled in-band quiet periods, the SSA shall control in-band sensing on channels N and  $N \pm 1$ .



**Figure 173 — Spectrum Sensing Automaton state machine operation**

### 10.3.2 Procedure SSA\_Initialization

The functionality of the SSA local autonomous spectrum sensing process, when the BS is initially switched on or when the CPE is initialized before association with the base station, is described below and depicted in Figure 174 and Figure 174 respectively. This process is part of the more general BS and CPE initialization process described in 7.14.1 and 7.14.2 respectively. At initial turn-on and self-test, the SSA shall sweep a specific channel, a specified range of channels or all the channels that are likely to be impacted by the WRAN device operating on a given channel depending on pre-set information at the BS or CPE, or directions from the higher layers at the BS or CPE. If all channels of a range of operation need to be sensed, one additional channel at both ends of the range shall be sensed to cover the adjacent channel case unless this goes beyond the extent of the relevant TV band.

For each channel, an RSSI measurement<sup>22</sup> shall be performed on the WRAN signal path and attempt shall be made to capture a WRAN superframe header or a CBP burst. If an SCH is captured and the level of the RF signal on the WRAN signal path is sufficiently high (see Table 247), attempt shall be made to acquire the frame header, the broadcast PDUs sent by the BS to advertise the WRAN service for BS and CPE initialization and the list of channels prohibited from incumbent operation obtained from the base station by the IPC-UPD management MAC message. If an SCH can be acquired but the signal level is insufficient or a CBP burst can be acquired but cannot be decoded, the presence of a WRAN signal shall be recorded along with the channel number and the measured RSSI. If an SCH or a CBP burst cannot be detected, RF signal sensing and signal classification shall be carried out to determine the presence of broadcast incumbents and their signal type. The result of the measurement and the signal classification shall be provided to the SM at the BS or stored at the CPE locally so that it can later be sent to the base station when association is established or later on upon request from the BS.

The channel shall then be incremented and the above initial sensing shall be repeated. The order in which the channels are to be sensed will be implementation dependent. Note that the list of channels prohibited from incumbent operation acquired from the SM through the IPC-UPD message can be used to skip sensing on these channels.

Note that when a BS initializes, it is primarily interested in identifying an empty channel where it can establish its service. When a CPE initializes, it is primarily interested in identifying operational WRAN channels with which it can associate. These two goals are not completely compatible and this is why two partly different SSA initialization processes shall exist at the BS and CPE (see Figure 174 and Figure 175).

In the case of the BS SSA initialization, if there is at least one available channel ( $N_0$ ), a selection shall be made and a second round of spectrum sensing shall then take place on the adjacent channels ( $N_0 \pm 1$ ) of the selected channel. Attempt to acquire an SCH or CBP burst shall be made on the WRAN signal path to determine the timing of the quiet periods of an eventual WRAN signal on these two adjacent channels. If a WRAN signal is detected, RF signal sensing and signal classification shall then be carried out on the channel ( $N_0 + 1$  or  $N_0 - 1$  or both) through the sensing path during the identified quiet periods to verify the presence and the identity of the incumbent service underneath the WRAN operation. In such case, a new available channel will need to be selected. If no incumbent signal is detected underneath the WRAN operation in the adjacent channels, then the BS can proceed with the next step in its initialization process (see 7.14.1).

If there is no channel available, the BS shall either abort its initialization process or initiate a self-coexistence process on a selected channel with the already existing WRAN operation (see 7.20.3.2).

In the case of the SSA initialization, if there is no WRAN channel that can be used at the location of the CPE, its initialization shall be aborted. Depending on the CPE implementation, the information obtained from the various WRAN base stations may be presented to the local interface of the CPE so that it could ultimately be displayed on a local screen to allow for an informed selection among available local WRAN networks available in the area at the CPE (similar to the Access Point selection in Wi-Fi). Local algorithms could also be implemented in the CPE to automate the process for choosing the WRAN network.

A second round of spectrum sensing shall then take place on the selected channel ( $N_0$ ) and its adjacent channels ( $N_0 \pm 1$ ). Since, by definition, a WRAN service is present on the selected channel, the WRAN signal path shall acquire the SCH or the CBP burst through the WRAN signal path to determine the timing of the quiet periods in this channel. RF signal sensing and signal classification shall then be carried out on channel  $N_0$  by the sensing path during the quiet periods to verify the presence and, in this case, attempt to

---

<sup>22</sup> See footnote 20 page 8 of the FCC R&O 08-260. The RSSI measurements will generate more useful information than a simple signal detection and classification. When sufficiently high-level signals are present, the signal classification schemes developed for low signal levels may be replaced by simpler, faster, and more effective signal classification schemes. Such fast incumbent signal classification schemes will be implementation dependent.

identify the incumbent service underneath the WRAN operation at the specific CPE location. The findings shall be recorded locally.

The sensing process shall then proceed to sense the two adjacent channels during the quiet periods by sensing the presence of an incumbent signal and classifying its type. The findings shall be recorded locally and if incumbents are found in these channels, the selected channel shall be removed from the list of available WRAN services and the updated list shall be presented to the higher layers at the CPE for the selection of another WRAN service. If no more WRAN service exists at the CPE, its initialization shall be aborted. However, if a WRAN service exists and no incumbent is present in the three channels ( $N_0$  and  $N_0 \pm 1$ ), the CPE initialization process shall continue as described in 7.14.2.

In the case of the CPE initialization, if the authorization is refused by the currently selected base station, the currently selected channel shall be removed from the list of available WRAN services (entry “A” in Figure 174) and this list shall be presented to the higher layers at the CPE for a new channel selection to be made. Then, the next round of sensing process shall be repeated with the sensing of the newly selected channel ( $N_0$ ) and its adjacent channels ( $N_0 \pm 1$ ) as described above. If no incumbent is present in the three channels, the CPE initialization process shall continue as described in 7.14.2.

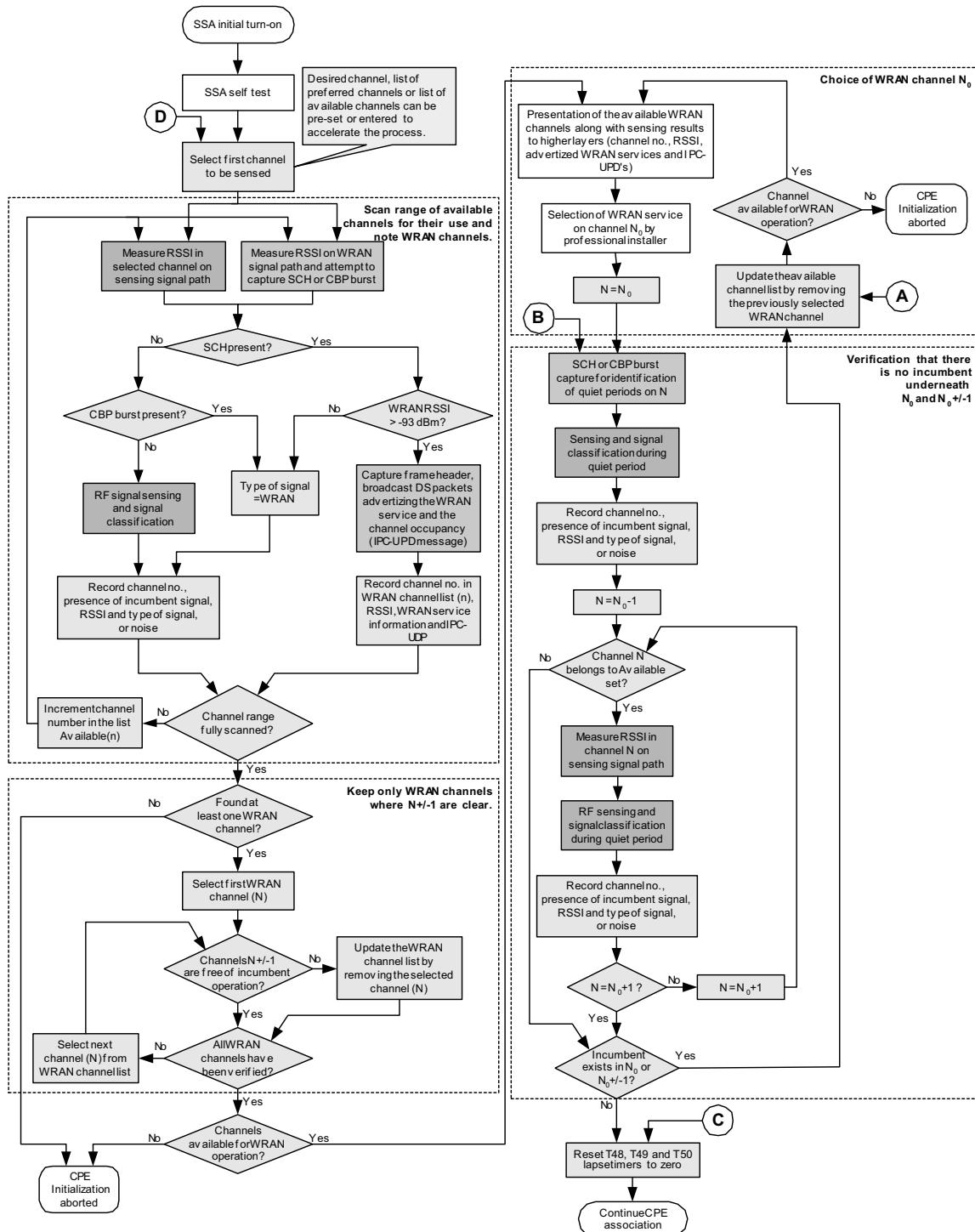


Figure 174 — Flow diagram Procedure SSA\_Initialization at the BS

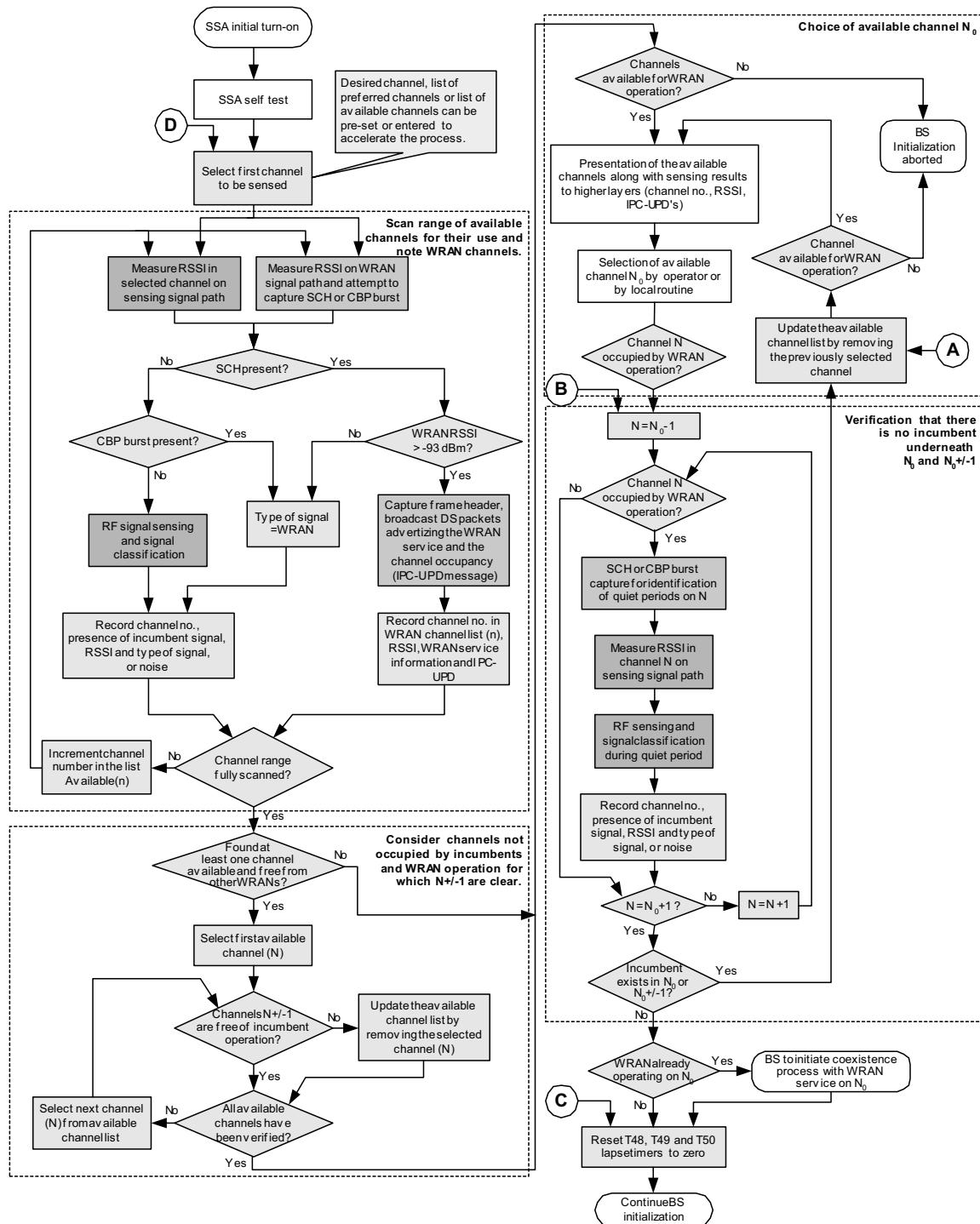


Figure 175 — Flow diagram Procedure SSA\_Initialization at the CPE

### 10.3.3 Procedure SSA\_In-band\_Sensing

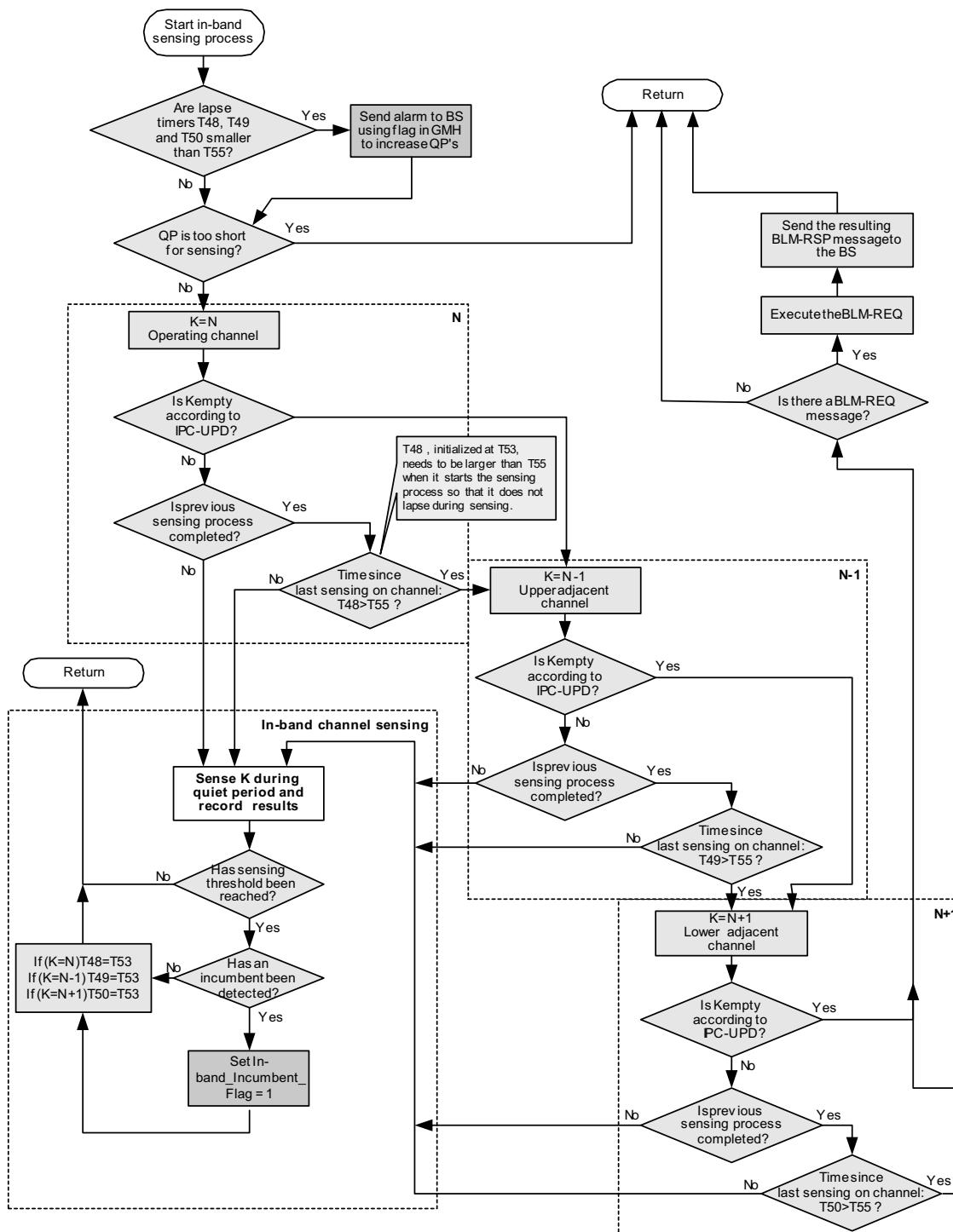
The SM at the BS is responsible for scheduling the in-band (channels N and N±1) quiet periods. The SSA shall autonomously utilize those quiet periods to perform in-band spectrum sensing and report the results of incumbent discovery to the SM.

Once a Quiet period is scheduled by the SM and signaled by the SCH to the CPE, the CPE will first verify if the sensing timers have lapsed since the last sensing on channels N or N±1 (i.e., lapse timers > T53, see Figure 176). An urgent MAC message contained in the GMH (see QPA bit in Table 4) will be sent to the BS to ask the SM to increase its scheduling of the quiet periods. Then, the SSA will verify that this quiet period is sufficiently long to initiate in-band sensing. This length will depend on the local capability of the sensor at the CPE. Depending on the sensing technology used, sensing may need to be done in a ‘contiguous’ fashion to reach the required sensing threshold or with integration over a number of sensing instances of smaller length to be able to reach the required sensing threshold. If the quiet period that is scheduled is shorter than required, the SSA will have to skip sensing for that specific period. (Note that other CPEs that require less time to carry out sensing shall proceed with their sensing.)

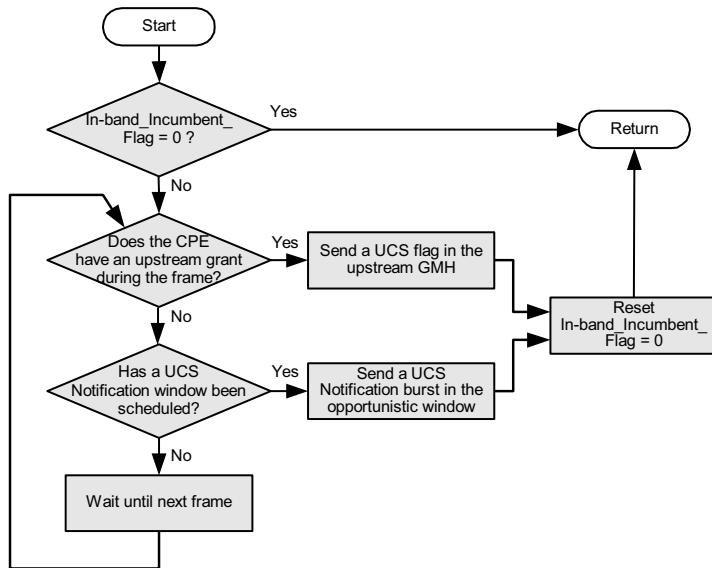
If the sensing period is sufficiently long, the SSA shall undertake the sensing on N and N±1 where needed. Once the quiet period is over, the in-band sensing shall be put on hold. At the start of the next scheduled quiet period, the SSA shall resume its in-band sensing activity by verifying the time lapsed since the last sensing on each of the N, N+1, and N–1 channels and initiate new sensing when the time lapsed since the last sensing gets close to the maximum period between sensing. As a result, if an incumbent is discovered, the SSA shall either use the UCS flag in the header of its next upstream PDU (see 7.6.1.1) to signal the presence of the incumbent in the channel or, if no bandwidth has been granted in the current upstream subframe but an opportunistic UCS notification window has been scheduled (either CDMA or contention-based, see 7.7.4.1.1), it shall send a UCS notification to the BS as illustrated in Figure 177. If neither of the conditions exists, the SSA shall then wait to report on the next frames when the opportunity is given.

At the start of every scheduled quiet period, the SSA shall verify whether channel N has been identified as prohibited from incumbent operation in the IPC-UPD message (i.e., it has been indicated to the CPE that there is no incumbent in this channel). If it is the case, sensing on N can be skipped. If not, it shall then verify that the sensing on the operating channel has been completed, and if not, it shall proceed to complete it. If it has been completed, it will verify the time lapsed since the last completion and compare it to the repetition period required by the local regulator ( $T_{INsens}$ , T53, see Table 272 and Annex A) less a safety margin corresponding to the time to carry out this sensing ( $T_{sensin}$ , T55 see Table 276). If this lapse time is larger than specified, the CPE shall re-initiate its sensing on the operational channel. Otherwise, the SSA shall skip to N+1 and repeat the verification process, and then skip to N–1 and repeat the same process.

Once this is done and that N, N+1, and N–1 have been cleared, the remaining scheduled quiet periods can be used to perform the in-band sensing process as specified by the BLM-REQ message until the clearance period for any of N, N+1, or N–1 has lapsed, in such case, the above process is repeated.



**Figure 176 — Procedure SSA\_In-band\_Sensing**



**Figure 177 — Flow diagram for Procedure SSA\_Report\_In-band\_Sensing\_Results**

#### 10.3.4 Procedure SSA\_Idle\_Time SSA operation during CPE idle time

In addition to being able to carry out the in-band sensing process and any higher priority sensing requests coming from the base station through the specific MAC messages described in the BLM-REQ message (see 7.7.18.1), the SSA shall have the necessary local routines to autonomously sense the channels in its backup/candidate channel list in the proper order of priority during its idle time. This process is described below and depicted in Figure 178.

The SSA shall begin its autonomous sensing operation by sensing the first channel in the backup/candidate channel list. If the last sensing has been carried out less than T54 seconds earlier (see Table 276), the sensing on this channel can be skipped. The next channel is then selected in the order of the backup/candidate channel list. The SSA shall try to go as deep as possible in the backup/candidate channel list given the amount of idle time provided for local sensing.

A measure of the depth reached by the local out-of-band sensing process shall be kept at the BS and at each CPE to keep track of the number of channels that the SSA has been able to ‘clear’, i.e., verify that there is no incumbent on the channel and its two adjacent channels within the valid clearance period (T54 as specified in Table 276 and in Annex A for the various regulatory domains), between any interruption from the base station. After any interruption, the automaton shall restart its out-of-band sensing process with the first backup channel and the depth will track the number of channels that can be ‘cleared’ within the valid clearance period. Due to the nature of the algorithm, this process will be directed to any channel reaching the end of its period of validity (T54) in order of priority from the first backup channel through the backup list and the candidate list.

Sensing through the WRAN signal path will be interrupted and the WRAN signal path will be re-tuned to the operating channel ‘ $N_0$ ’ during the following intervals:

- Superframe headers
- Frame headers for the frames assigned to the base station to which the CPE is associated in a self-coexistence situation
- Downstream frame at the BS

- CPE receiving data during the DS subframe as signaled by the DS-MAP
- CPE transmitting data during the US subframe as signaled by the US-MAP
- CPE transmitting data during the opportunistic ranging/UCS notification/BW request window
- CPE monitoring activity as requested by the base station for CBP packet capture
- CPE transmitting activity as requested by the base station for CBP packet transmission

For each channel ‘N’ for which the  $T_{OUTsens}$  (T54) validity period has lapsed,<sup>23</sup> the SSA shall measure the RSSI on this channel ‘N’ through its sensing path as well as through its WRAN signal path and attempt to capture the SCH or CBP burst of a WRAN transmission on that channel. If the SCH or CBP information can be decoded, the SSA will sense channels N, N–1, and N+1 during the appropriate quiet periods and record the channel number, the RSSI, the signal type (or noise if none is found) and the time at which the sensing took place.

If there is no WRAN operation on the channel being sensed or the signal level is too low to decode the SCH or CBP burst, the sensing process shall verify whether there is WRAN operation on the two adjacent channels by trying to capture the SCH or the CBP burst to be able to schedule its sensing during the quiet intervals of these WRAN operations. If no WRAN operation is found on channels N and N±1, sensing on channel is N is then carried out with no consideration for quiet periods. Since signal sensing has to be done on the adjacent channels, if no WRAN operation can be detected on N and N±1, the sensing process shall verify whether there is WRAN operation on N±2 to be able to sense N±1 during the quiet intervals of N±2 because of possible adjacent channel leakage that could mask the presence of incumbents on N±1.<sup>24</sup> Sensing on N–1 and N+1 will then be carried out at any time or during quiet periods depending on whether WRAN operation is found in N–2 or N+2 respectively.

As a result, the SSA shall send a warning to the SM at the base station directly if at the BS or using the BLM-RSP message with the “Unavailable Backup Channel” IE, as illustrated in Figure 179, to be sent during the bandwidth allocation assigned to the CPE in the US-MAP or using the opportunistic BW Request mechanism to allow sending this MAC message in a later frame if an incumbent appears on one of the backup channels. Furthermore, if the depth reached by the SSA at the time of an interruption is less than the depth of the backup list, the SSA shall advise the SM directly if located at the BS or using the BLM-RSP message with the “Backup channel list clearance depth” IE, as illustrated in Figure 180, to be sent during the US bandwidth allocation assigned to the CPE in the US-MAP or using the opportunistic BW Request mechanism to allow sending this MAC message in a later frame to warn the BS. Otherwise, the SSA shall be prepared to provide the information on its current sensing depth in a solicited mode directly to the SM if located at the BS or with the BLM-RSP message with the IE “Backup/candidate channel list clearance depth” upon reception of the normal BLM-REQ MAC message whenever the base station requests it. This information collected by the base station from all SSAs will be used to adjust the size of the backup channel list. The base station will be responsible for reserving sufficient idle time in the scheduling of the data traffic towards each of its CPEs to allow them the time to verify the availability of the backup channels and some extra candidate channels if possible.

---

<sup>23</sup> A time buffer T60 representing the time to carry out one typical round of out-of-band sensing, as depicted in Figure 178, should be removed from the T54 requirement to avoid that this time requirement lapses during the sensing process (see Table 276).

<sup>24</sup> It is assumed that the quiet periods will be aligned among WRAN cells operating on channels N, N±1, and N±2 in the same area.

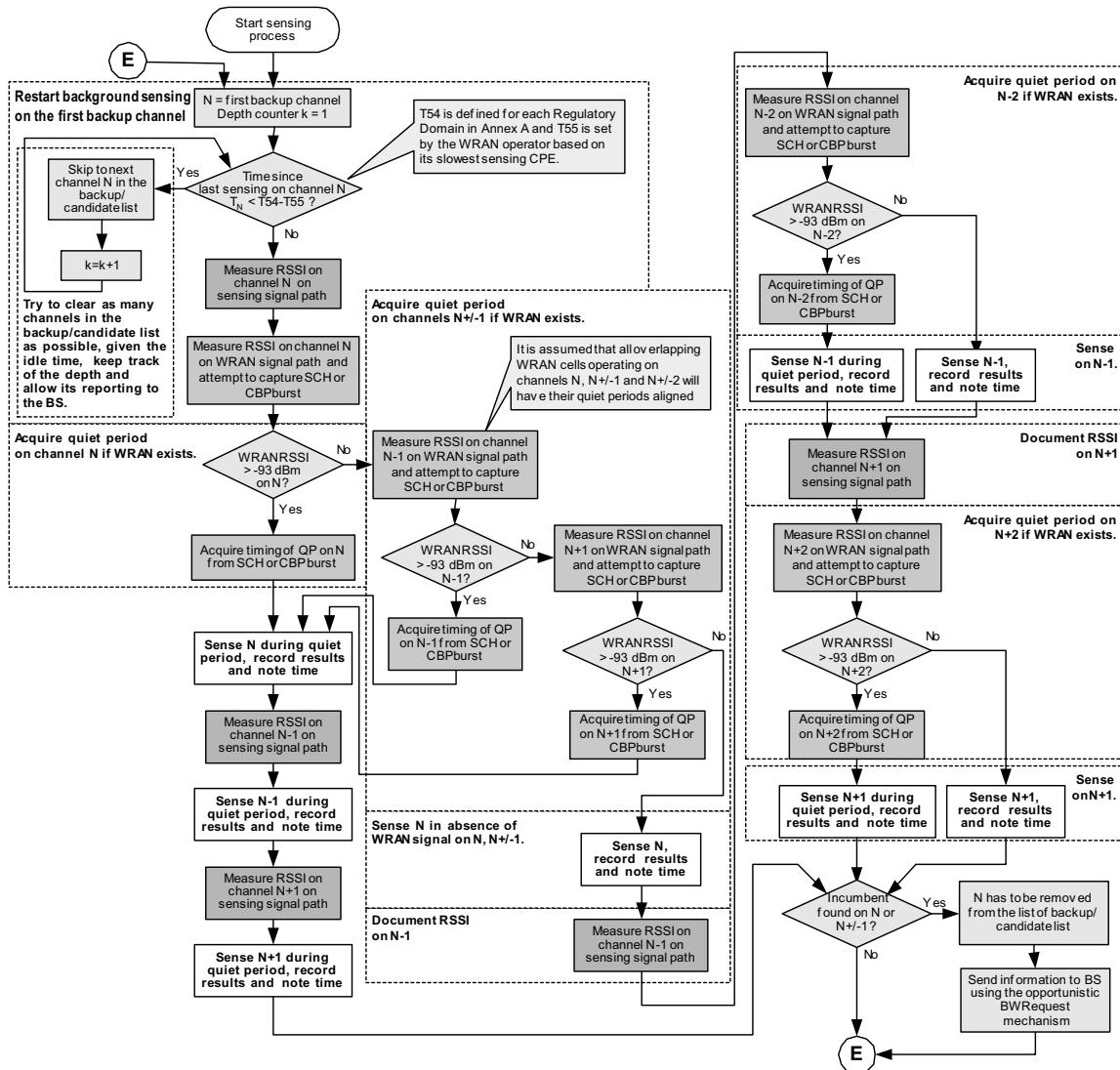
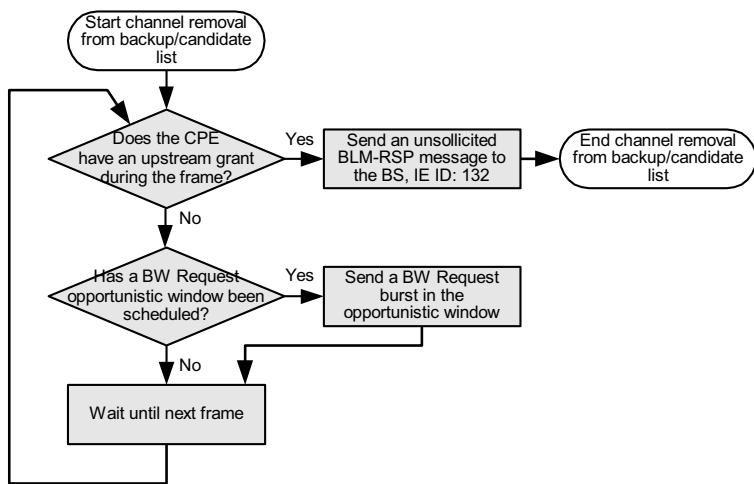
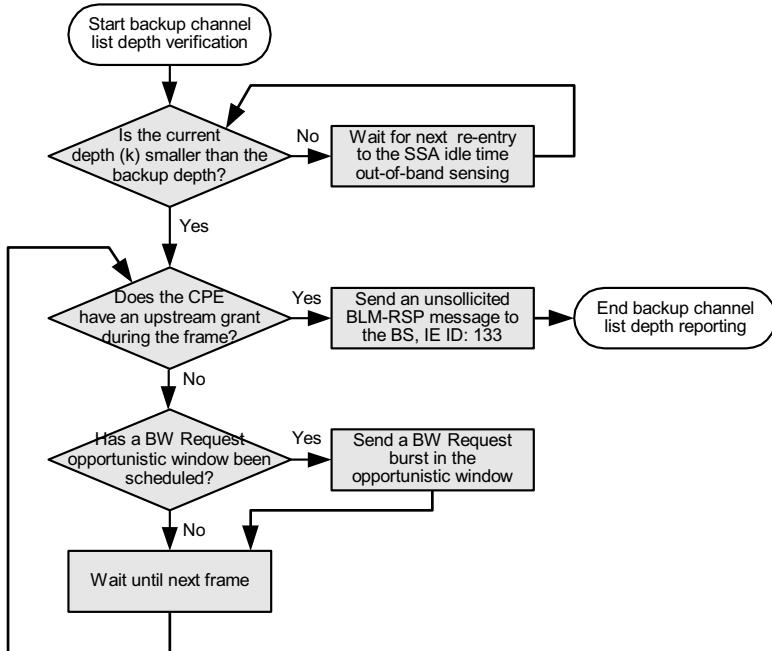


Figure 178 — Flow diagram for CPE sensing during idle time



**Figure 179 — Flow diagram for Procedure SSA\_Report\_Unavailable\_Backup\_Channel**



**Figure 180 — Flow diagram for Procedure SSA\_Report\_Backup\_Channel\_List Dept**

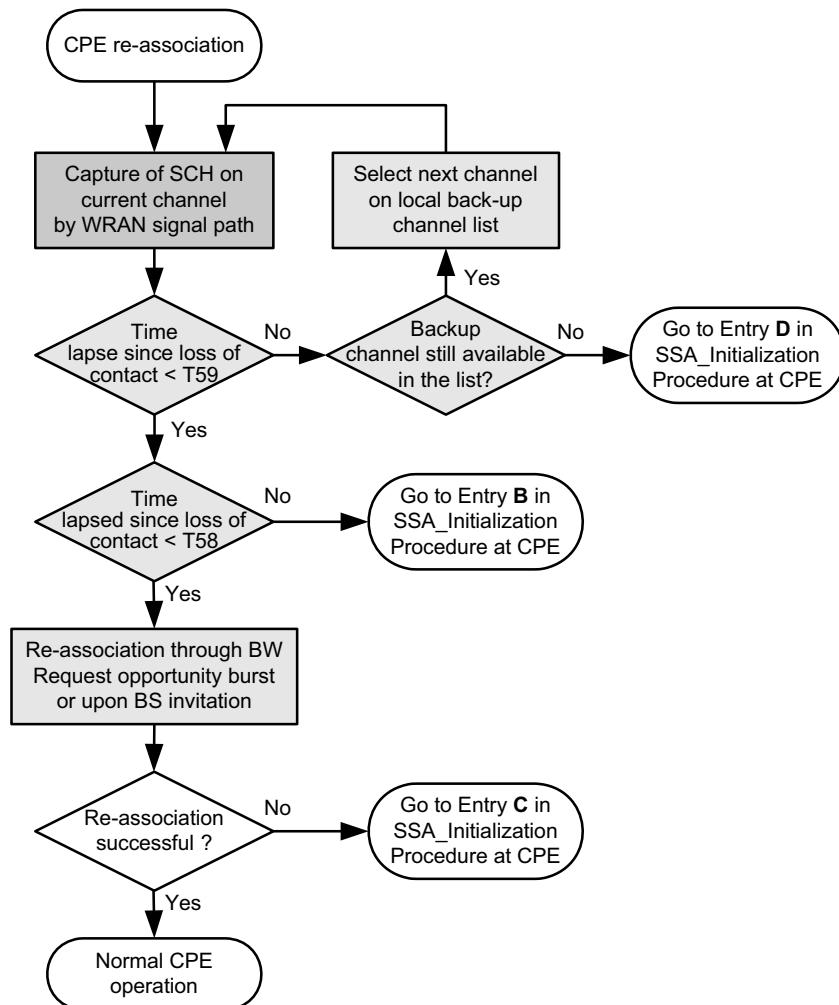
### 10.3.5 Loss of contact with the BS

If the CPE loses contact with its base station, the SSA local intelligence shall make sure that a reasonable number of attempts are made to reconnect with the base station, while avoiding potential interference to licensed incumbents. The functionality of the SSA located at the CPE is summarized below for the loss of contact with the base station and is depicted in Figure 181.

The SSA shall first identify whether or not a WRAN signal is still present on the selected channel by trying to capture the superframe header (SCH). If successful within the value set of the Lost\_SCH Timer (T58) (e.g., 2 s maximum), attempts to re-associate shall be made through the BW Request opportunistic burst or upon specific invitation by the BS. If this does not work, the re-association shall start from an earlier stage with the CDMA ranging burst (entry ‘C’ in Figure 174). If re-association cannot be achieved within this time, then the CPE shall execute the second round of initial sensing for the co-channel and first adjacent channels cases to protect any broadcast incumbent that may have appeared in the affected channels since the loss of connection with the base station (entry ‘B’ in Figure 174).

If the WRAN signal is found to be no longer present in the channel for longer than the value set for the Timer TWait\_channel\_switch (T58 and/or T59), then the CPE shall select the next channel in its back-up list and try to capture the SCH to synchronize with the base station on this new channel. If a scheduled channel switch is performed with proper contact with the BS and done within the value set for the timer T59, re-association shall be made through the BW Request opportunistic burst or upon specific invitation by the BS, or through the earlier stage of the CDMA ranging burst (entry ‘C’ in Figure 174).

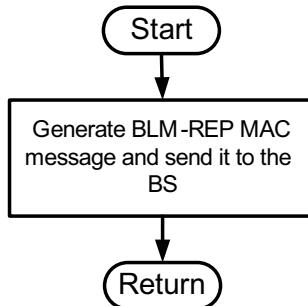
If the SCH capture on the new channel is not successful, then the CPE shall select the next channel on its backup list and repeat the process until a successful superframe capture is achieved. If re-association on all the valid channels in the backup list has failed, the CPE shall restart its entire initialization process (entry ‘D’ in Figure 174).



**Figure 181 — Flow diagram for Procedure SSA\_Loss\_of\_Contact\_with\_SM**

### 10.3.6 Procedure SSA\_BLM\_Report\_Generation

Procedure SSA\_BLM\_Report\_Generation is executed in response to an in-band or out-of-band Bulk Measurement request (BLM-REQ). The Procedure SSA\_BLM\_Report\_Generation is as shown in Figure 182.



**Figure 182 — Flow diagram for Procedure SSA\_BLM\_Report\_Generation**

### 10.3.7 Example of sensing information representation at the SSA

Once association has been achieved, the base station may request the SSA to send the complete results of the initial sensing or any update thereof at anytime directly to the SM if located at the BS or using the appropriate BLM-REQ PDU if located at the CPE. The SSAE will therefore need to keep the latest information stored by the sensing process in its local registers at all times. Table 235 gives an example of a possible representation of the information that needs to be stored locally. The SSA shall be capable of reporting the information from all rows of the table except for the two last rows that contain information obtained from the base station.

**Table 235 — Example of sensing registers at the CPE**

Channel number	...	25	26	27	28	29	30	...
Time of last sensing								
Time of last positive								
Sensing path RSSI								
WRAN path RSSI								
Signal type								
WRAN service advertisement								
Sensing path RSSI under WRAN								
Signal type under WRAN								
List of incumbent prohibited channels from BS (IPC-UPD)								

## 10.4 Spectrum sensing

Spectrum sensing is the process of observing the RF spectrum of a television channel to determine its occupancy (by either incumbents or other WRANs).

The base station and all CPEs shall implement the Spectrum Sensing Function (SSF).

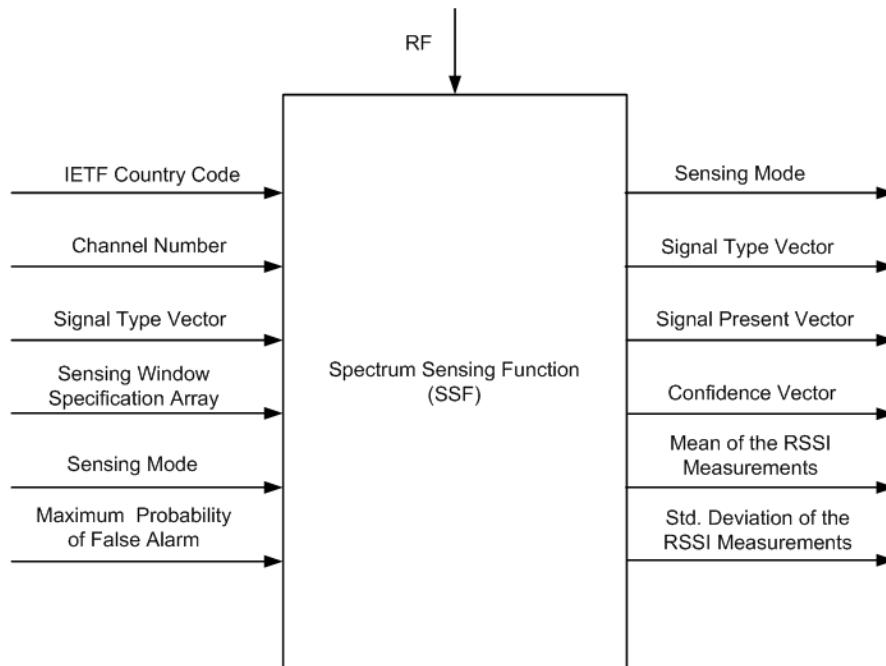
The SSF shall be driven by the SSA. The SSF shall observe the RF spectrum of a television channel and shall report the results of that observation to the SM (at the BS) via its associated SSA. The Spectrum Sensing Function (SSF) is described in 10.4.1. The primitives for the SSF are described in 10.7.

### 10.4.1 Spectrum Sensing Function (SSF)

The Spectrum Sensing Function observes the RF spectrum of a television channel for a set of signal types and reports the results of this observation. The spectrum sensing function is implemented in both the base station and the CPEs. There are MAC management frames that allow the base station to control the operation of the spectrum sensing function within each of the CPEs. Figure 183 illustrates the inputs and outputs of the spectrum sensing function.

The inputs to the spectrum sensing function come from the SM via SSA. The inputs to the spectrum sensing function are described in 10.4.1.1. The outputs from the spectrum sensing function are returned to the SM via SSA. The outputs of the spectrum sensing function are described in 10.4.1.2. The behavior of the spectrum sensing function is described in 10.4.1.3.

Some of the possible sensing techniques that can be used to realize the spectrum sensing function are described in Annex C. The use of any specific sensing technique is optional, as long as the inputs, outputs and behavior meet the specification of this subclause.



**Figure 183 —Spectrum sensing function**

### 10.4.1.1 SSF inputs

A summary of the spectrum sensing inputs is given in Table 236.

**Table 236 —Spectrum Sensing Function input signals**

Input name	Input description	Length (bits)	Values
RF	Radio Frequency signal from the sensing antenna	N/A	N/A
ISO 3166 Country Code	Regulatory domain of operation	24	ASCII Characters—e.g., USA represents United States of America
Channel Number	The channel number that is to be sensed by the SSF	8	0–255
Channel Bandwidth	The bandwidth of the channel to be sensed by the SSF	4	0000 = 6 MHz 0001 = 7 MHz 0010 = 8 MHz 0011–111 = Reserved
Signal Type Array	An array indicating the signal types for which the SSF is to sense	32	Described in Table 237
Sensing Window Specification Array	An array of sensing window specifications. Each SFS specifies the details of the sensing window for a given signal type being sensed	$N \times 32$ , where N is the number of signal types enumerated in Signal Type Array. The 24 bits cover the NumSensingPeriods, SensingPeriodDuration & SensingPeriodInterval.	Ranges for values given in Table 238: Bits 0–7: NumSensingPeriodsBits 8–17: SensingPeriodDurationBits 18–31: SensingPeriodInterval
Sensing Mode	The sensing mode specifies which SSF outputs are valid and in some cases it specifies the behavior of the SSF	2 bits	Sensing modes specified in Table 239
Maximum Probability of False Alarm)	In sensing modes 0 and 1 this value specifies the maximum probability of false alarm for each sensing mode decision in the signal present array	8 bits	Maximum Probability of False Alarm—0x00 indicates ‘0’ and 0x01 indicates ‘0.001’, and 0xFF = 0.255

The RF input is connected via an RF stage to the WRAN sensing antenna.

The ISO 3166 country code defines the regulatory domain of operation. For example, the ISO 3166 country code ‘USA’ corresponds to the regulatory domain of the United States of America.

The channel number is the relative television channel number that the SSF is to sense. The center frequency for each channel number and the exact mapping between the relative channel number and the absolute channel number are given in Annex A.

The channel bandwidth is the bandwidth of the television channel that the SSF is to sense.

The signal type array (STA) indicates which signal types that are to be sensed for by the SSF. The array is a one-dimensional array of length  $STALength$ , indexed from 0 to  $STALength - 1$ . The STA is a binary array whose elements are either zero or 1. The  $i^{\text{th}}$  element in the array specifies whether the SSF is to sense for  $i^{\text{th}}$  signal type. The mapping of STA index to signal type is given in Table 237.

The value of  $STALength$  is 32 and can be represented using 4 octets.

**Table 237 — Signal type array indices**

STA Index	Signal type
0	Undetermined
1	IEEE 802.22 WRAN
2	ATSC
3	DVB-T
4	ISDB-T
5	NTSC
6	PAL
7	SECAM
8	Wireless Microphone
9	IEEE 802.22.1 Sync Burst
10	IEEE 802.22.1 PPDU MFS1
11	IEEE 802.22.1 PPDU MSF2
12	IEEE 802.22.1 PPDU MSF3
13–32	<i>Reserved</i>

A one in index zero of the STA indicates sensing for any signal type, with no distinction between signal types. A one in index one of the STA indicates the SSF should sense for an IEEE 802.22 WRAN.

As an example, if the STA is given as follows:

$$\text{STA} = (0010111000000000\dots00)$$

Then the SSF shall sense for an IEEE 802.22.1 Sync Burst, an ATSC signal, and NTSC signal and a wireless microphone. Table A.11 specifies that, depending upon the regulatory domain of operation, some STA indices in the STA shall be set at all times.

The sensing window specification array (SWSA) is a two-dimensional array of length STA Length  $N \times 32$ . Each row of the SWSA is a sensing window specification (SWS). If the  $i^{\text{th}}$  element of the STA is one (1) then the  $i^{\text{th}}$  row of the SWSA shall be set to a valid sensing window specification. If the  $i^{\text{th}}$  row of the STA is set to zero (0) then the  $i^{\text{th}}$  row of the SWSA does not need to be set to a valid SWS since it will be ignored by the SSF.

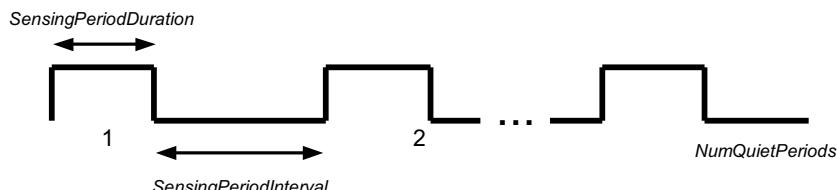
A sensing window specification (SWS) consists of three parameters. These three parameters specify the window of time over which the SSF shall sense for specified signal type. Figure 184 illustrates a sensing window.

A sensing window consists of *NumSensingPeriods* number of sensing periods. The minimum number of sensing periods is one and the maximum number is 255. This maximum number is based on the need to avoid that a rogue BS could bring down other co-existing co-channel BSs in the area by excessive scheduling of quiet periods.

Each sensing period is of duration *SensingPeriodDuration* symbols and adjacent sensing periods are separated by *SensingPeriodInterval* symbols as shown in Figure 184.

The parameters in a sensing window specification are given in Table 238. Such sensing window can occupy a portion of a quiet period, an entire quiet period or multiple quiet periods.

The details on how quiet periods are scheduled are found in 7.5.1.



**Figure 184 — Sensing window**

**Table 238 — Bounds of sensing window specifications**

Parameter Name	Range	Units	Value
<i>NumSensingPeriods</i>	0 to 255	integer	Comes from SM or SSA Default = 1, values from 128 to 255 are reserved
<i>SensingPeriodDuration</i>	0 to 1023	symbols	Comes from SM or SSA Default = 16 symbols
<i>SensingPeriodInterval</i>	0 to 2047	frames	Comes from SM or SSA Default = 200 frames

Quiet periods are scheduled by the MAC layer. Quiet periods can be scheduled using the SCH as described in 7.5.1. Also, quiet periods can be scheduled using the channel quiet request message, as described in 7.7.17.3. A general discussion on quiet periods can found in 7.21

The aggregate of all quiet period durations within which a spectrum sensing technique meets the required detection threshold for any signal type specified in Table 237 shall not exceed 200 ms. The processing latency to detect any signal shall not exceed 2 seconds.

The sensing mode specifies which outputs of the SSF are valid and in some cases the behavior of the SSF. Table 239 summarizes the valid SSF outputs for each of the sensing modes. The table also includes a description of each sensing mode.

**Table 239 — Summary of the sensing modes**

Sensing mode	Valid SSF outputs	Description
0	Signal Present Array	For each signal type the SSF generates a binary decision as to whether the signal is present in the television channel
1	Signal Present Array Confidence Array	Same as sensing mode 0 with the addition of a confidence metric for binary decision
2	Mean and standard deviation of the measured RSSI	For each signal type the SSF generates an estimate of the mean and standard deviation for up to 255 instantaneous RSSI measurements on a specified channel (see 0)

Sensing Mode 0 is mandatory at the BS and the CPE if sensing is required (see Annex A).

Sensing Mode 1 is optional at the BS and the CPE if sensing is required (see Annex A).

Sensing Mode 2 is optional at the BS and the CPE if sensing is required (see Annex A).

The maximum probability of false alarm input specifies the behavior of the elements of the signal present array when no signal is present on the RF input. The details of the behavior of the SSF, and its dependence on this input parameter, are given in 10.4.1.3.

### 10.4.1.2 SSF outputs

The sensing mode and the signal type array are passed through the SSF. These parameters indicate which of the other SSF outputs are valid and hence are useful for subsequent processing. The MAC messages for specifying the sensing measurement report structure are covered in 7.7.18. There is a general description of sensing measurement reporting in 7.19.4.

The signal present array is a one-dimensional array of length *STALength*. Each element in the array is a signal present decision. Each decision can take on three possible values, which are given in Table 240. The  $i^{\text{th}}$  signal present decision corresponds to the  $i^{\text{th}}$  signal type as listed in Table 237.

**Table 240 — Values of the signal present decision**

Value of signal present decision	Length (bits)	Value of signal present decision	Description
<i>TRUE</i>	8	0xFF	SSF decided that the signal is present in the channel
<i>FALSE</i>	8	0x00	SSF decided that the signal is not present in the channel
<i>NODECISION</i>	8	0x7F	The SSF makes no decision regarding the presence of the signal in the channel. This is the output when the SSF was not instructed to sense for the signal type.

The confidence array is a one-dimensional array of confidence metrics. The  $i^{\text{th}}$  confidence metric indicates the confidence in the  $i^{\text{th}}$  signal present decision. A confidence metric varies between a minimum of zero (0x00) indicating no confidence in the signal present decision and a maximum of 255 (0xFF) indicating total confidence in the signal present decision. The range of a confidence metric is given in Table 241 and shall be represented by an 8-bit variable. The Variable Confidence Metric at the present time shall always assume a value of 0x00 or 0xFF, and all other values are reserved.

**Table 241 — Range of a confidence metric**

Limit	Value	Description
Minimum confidence metric	0x00	No confidence in signal present decision
Maximum confidence metric	10xFF	Total confidence in signal present decision

The RSSI measurement results are stored in a one-dimensional array of up to M instantaneous measurement results at the SSF for a channel. The integration time to acquire each RSSI measurement shall be set to a default 2 ms. The representation of the multiple RSSI estimates at the SSF is given in Table 242 for an 8-bit resolution.

**Table 242 — RSSI measurements**

Limit	Length (bits)	Value	Units	Description
RSSI	$M \times 8$	Signed Integer	dBm	Up to M RSSI measurements. M can be as large as 255. These RSSI shall be measured in dBm and shall be normalized for a 0 dBi antenna gain and 0 dB coupling and cable loss. Signed in units of dBm in 0.5 dB steps ranging from -104 dBm (encoded 0x00) to +23.5 dBm (encoded 0xFF). Values outside this range shall be assigned the closest extreme.

When the SM requests a number of repeated measurements through the BLM-REQ MAC message (see 7.7.18.1), the SSF shall calculate the mean for the M values acquired in the RSSI one-dimensional array. The standard deviation for these M values shall also be calculated and will represent the dynamic aspect of the RSSI during the M measurements. The range of the mean and the standard deviation of the RSSI measurements that will be reported by the SSF in the BLM-RSP MAC message (see 7.7.18.3.1.1) is given in Table 243.

**Table 243 — Range of the mean and standard deviation of a field strength estimate error**

Parameter	Length (bits)	Value	Units	Description
RSSI	8	Signed Integer	dBm	Mean of the M RSSI measurements. Signed in units of dBm in 0.5 dB steps ranging from -104 dBm (encoded 0x00) to +23.5 dBm (encoded 0xFF). Values outside this range shall be assigned the closest extreme.
Standard Deviation	8	Integer	dB	Standard Deviation of the M RSSI measurements. Expressed in units of dB in 0.1 dB steps ranging from 0.0 dB (encoded 0x00) to +25.5 dB (encoded 0xFF). Values beyond +25.5 dB shall be encoded as 0xFF.

#### 10.4.1.3 SSF behavior

In this clause, all references to signal power shall refer to the signal power in dBm measured at the input of the sensing receiver.

##### 10.4.1.3.1 Sensing Mode 0

When the sensing mode is set to zero (0) the only valid SSF outputs are listed in Table 244.

**Table 244 — Valid outputs in Sensing Mode 0**

Sensing Mode
Signal Type Array
Signal Present Array

The values of Sensing Mode and Signal Type Array shall be the same as their input values.

In sensing mode zero, if the  $i^{\text{th}}$  element of the signal type array is zero then the  $i^{\text{th}}$  element of the SPA shall be set to *NODECISION*.

**Table 245 — Example of SPA for Sensing Mode Zero with STA(i) set to 0**

Sensing mode	STA Index $i$	Signal type	STA(i)	SPA(i)
0	0	Undetermined	0	<i>NODECISION</i>
0	1	IEEE 802.22 WRAN	0	<i>NODECISION</i>
0	2	ATSC	0	<i>NODECISION</i>
0	3	DVB-T	0	<i>NODECISION</i>
0	4	ISDB-T	0	<i>NODECISION</i>
0	5	NTSC		
0	6	PAL		
0	7	SECAM		
0	8	Wireless microphone	0	<i>NODECISION</i>
0	9	IEEE 802.22.1 Sync Burst	0	<i>NODECISION</i>
0	10	IEEE 802.22.1 PPDU MSF1	0	<i>NODECISION</i>

Sensing mode	STA Index <i>i</i>	Signal type	STA(i)	SPA(i)
0	11	IEEE 802.22.1 PPDU MSF2	0	<i>NODECISION</i>
0	12	IEEE 802.22.1 PPDU MFS3	0	<i>NODECISION</i>
0	13–32	<i>Reserved</i>		

In sensing mode zero if the  $i^{\text{th}}$  element of the signal type array is set to one and there is no signal present at the sensing antenna then the  $i^{\text{th}}$  element of the SPA shall be FALSE with probability greater than or equal to 1-MPFA, where MPFA is the maximum probability of false alarm for that signal as specified in the regulatory domain requirements, Annex A. The  $i^{\text{th}}$  element of the SPA shall be set to TRUE with probability less than or equal to MPFA. The regulatory domain requirements for various signal types, the minimum detection and maximum false alarm probabilities (MPFA) at specified signal power thresholds is provided in Annex A.

The behavior of the SSF in sensing mode 0 with the  $i^{\text{th}}$  element of STA set to one and with no signal present at the sensing antenna is summarized in Table 246.

**Table 246 — Example of SPA for Sensing Mode Zero with STA (i) set to 1 with no signal present**

Sensing mode	STA Index <i>i</i>	Signal type	STA(i)	SPA(i)
0	0	Undetermined	1	FALSE
0	1	IEEE 802.22 WRAN	1	FALSE
0	2	ATSC	1	FALSE
0	3	DVB-T	1	FALSE
0	4	ISDB-T	1	FALSE
0	5	NTSC	1	FALSE
0	6	PAL	1	FALSE
0	7	SECAM	1	FALSE
0	8	Wireless Microphone	1	FALSE
0	9	IEEE 802.22.1 Sync Burst	1	FALSE
0	10	IEEE 802.22.1 PPDU MSF1	1	FALSE
0	11	IEEE 802.22.1 PPDU MSF2	1	FALSE
0	12	IEEE 802.22.1 PPDU MSF3	1	FALSE
	13–32	<i>Reserved</i>		

In sensing mode zero with the  $i^{\text{th}}$  element of the STA set to one and if the signal is present in the channel at the specified signal power level given in Table 247, the  $i^{\text{th}}$  output of the SPA shall be TRUE with probability as specified for that signal type in that regulatory domain. The regulatory domain requirements for various signal types, the minimum detection and maximum false alarm probabilities at specified signal power thresholds is provided in Annex A.

The behavior of the SSF output SPA is specified in Table 247.

**Table 247 — Summary of SSF Outputs for Sensing Mode Zero**

Sensing Mode	STA Index <i>i</i>	Signal Type	STA(i)	Signal Power <sup>25</sup> (dBm)	SPA(i)
0	0	Undetermined	1	-90 <sup>26</sup>	TRUE
0	1	IEEE 802.22 WRAN	1	-93	TRUE
0	2	ATSC	1	-114	TRUE
0	3	DVB-T	1	Not available	TRUE
0	4	ISDB-T	1	Not available	TRUE
0	5	NTSC	1	-114	TRUE
0	6	PAL	1	Not available	TRUE
0	7	SECAM	1	Not available	TRUE
0	68	Wireless Microphone	1	-114	TRUE
0	9	IEEE 802.22.1 Sync Burst	1	-116	TRUE
0	10	IEEE 802.22.1 PPDU MSF1	1	-116	TRUE
0	11	IEEE 802.22.1 PPDU MSF2	1	-116	TRUE
0	12	IEEE 802.22.1 PPDU MSF3	1	-123	TRUE

#### 10.4.1.3.2 Sensing Mode 1

When the sensing mode is set to one, the only valid SSF outputs are listed in Table 248.

**Table 248 — Valid outputs in Sensing Mode 1**

Sensing Mode
Signal Type Array
Signal Present Array
Confidence Array

The values of sensing mode, signal type array and signal present array shall be the same as in Sensing Mode 0.

If the *i*<sup>th</sup> element of the signal type array is set to zero then the *i*<sup>th</sup> element of the confidence array is set to 0.

If the *i*<sup>th</sup> element of the signal type array is set to one then the *i*<sup>th</sup> element of the confidence array is a confidence metric indicating the confidence the SSF has in the *i*<sup>th</sup> element of the signal present array. A confidence metric is a measure of the confidence of a decision. The range of a confidence metric is given in Table 241.

#### 10.4.1.3.3 Sensing Mode 2

When the sensing mode is set to two the only valid SSF outputs are listed in Table 249.

---

<sup>25</sup> This power level is based on the assumption of a 0 dBi sensing antenna gain, 0 dB connector and cable loss, VSWR = 1:1. Note that, in order to account for the possible desensitization of the sensing detector by distant WRAN operation where the signal level at the CPE location is too low to allow detection of the SCH to identify its quiet period scheduling, a 3 dB increase in detector sensitivity or RF front-end performance may be needed.

<sup>26</sup> Assumed sensing RF front-end Noise Figure = 10 dB.

**Table 249 — Valid outputs in Sensing Mode 2**

Sensing Mode
Signal Type Array
Mean of the RSSI Measurements
Standard Deviation of the RSSI Measurements

The values of sensing mode and signal type array are the same as their input values.

The output consists of the mean resulting from M instantaneous RSSI measurements for a particular channel, where M can be as large as 255. The integration time to acquire each RSSI measurement shall be set to a default 2 ms.

The output also consists of the standard deviation calculated from the M instantaneous RSSI measurements and it represents the dynamic nature of the channel over M RSSI measurements.

#### 10.4.2 Special SSF considerations for the IEEE 802.22.1 beacon

The IEEE 802.22.1 beacon has been developed with the goal of allowing detection within a reasonable time window that allows IEEE 802.22 systems to attempt to provide tolerable QoS. The beacon has been designed such that the synch burst and index can be acquired within 5.1 ms, including the slippage due to the asynchronous capture of the burst. When types of signals such as DTV and analog TV need to be sensed, proper sensing schemes should be used to allow detection at the required sensing threshold within the same sensing window. The IEEE 802.22.1 beacon can also provide additional information such as the location of the beacon (MSF1), the beacon signature (MSF2) and its authentication (MSF3) with correspondingly larger sensing periods. See Table D.2.

The WRAN shall take the action of vacating a channel on which a valid IEEE 802.22.1 beacon signal has been received. Reception of the beacon is defined as either detection or demodulation of the beacon signal.

Acceptable methods to comply with detection of the beacon include energy detection, baud rate detection, correlation to the spreading sequence, or synchronization and determination of start-of-frame from the index. Other methods also exist. The WRAN must cease operation on a channel on which a beacon is detected unless the WRAN operator chooses to demodulate the beacon and perform further verification and validation of the received beacon signal. Performing demodulation of the beacon signal increases confidence that a received beacon signal is legitimate. The degree to which demodulation is performed is also at the discretion of the WRAN operator but if validity is detected at the point at which the WRAN chooses to stop further investigation of the demodulated beacon, it must protect the incumbent. It shall be at the discretion of the WRAN operator to determine the degree to which sequential steps are taken to validate the beacon. It can, therefore, make a decision after reception of MSF1 should it choose to do so. It may further choose to receive MSF1 combined with MSF2, and, if absolute confirmation is desired, MSF3. A determination of validity may be assessed at each step.

Demodulation of MSF1 allows the WRAN operator to acquire location and other pertinent information pertaining to the device protected by the beacon signal. The WRAN can, therefore, determine the best method to protect the incumbent device. This may include vacating the channel, reduction of power in the azimuth of the protected incumbent or moving a portion of its CPEs to a second channel. Other methods of protection also exist. Demodulation of the beacon information may, therefore, impact the WRAN operator and a BS's ability to schedule traffic in an optimal manner. In these cases, the QoS for a portion of the WRAN clients may not be satisfied while adequately protecting the incumbent.

Finally, if the WRAN operator is suspicious of the validity of a beacon signal, it may verify the signature and certificate of the beacon utilizing the data received in MSF2 and MSF3. MSF2 contains the signature

and MSF3 contains the public key certificate. In general, MSF3 demodulation is not required as the certificate is generally available over the internet. See Annex D for more details.

Beacon information to be reported depends on the sensing mode. There are 2 sensing modes: nominal (sync/index only) and beacon frame (MSF content).

- a) Nominal sensing mode: this is the 5.1 ms quiet period used to sense for the beacon sync frame. The sync frame contains the 15-bit sync word, a (15,7) BCH-encoded index, and 2 reserved bits.
  - Sync word above threshold (needs only one bit)
  - BCH-encoded index passes error correction (needs only one bit)
  - Decoded index (needs only 5 bits for the 31 unique values including the index-0 inter-device communication period that is either all zeros if not aggregating or is opened up for RTS/ANP)
  - Total number of bits required is 7

**Table 250 — Rules for indicating successful detection of MSF1, MSF2, and MSF3**

Syntax	Size	Notes
Sync	1 bit	1 = sync found 0 = sync absent <i>If sync absent, remaining values except reserved bits are ‘don’t care’ and are set to 0.</i>
Index Status (only if “sync found”)	1 bit	1 = passed decoding 0 = failed decoding
Index Value	5 bits	Binary value of the index
Other Detection Methods	1 bit	Correlation on spreading sequence or energy detection above threshold 1 = above threshold 0 = below threshold

- b) Beacon frame sensing mode: this mode is only activated for IEEE 802.22 devices that have reported a positive response from the nominal sensing mode. That is, the Sync was “sync found” and the Index Status was “passed decoding.” At this point there are several options:
  - 1) Capture MSF1 alone (no authentication) and find that it passes convolutional decoding and CRC. Report the MSF1 contents to the BS (requires 15 decoded bytes (the original 17 minus the 2 byte CRC) or 120 bits). If it did not pass CRC, it would not pass the information along but would report a failed CRC. Depending on whether the BS received a successful MSF1 decoding from another CPE, it might change the channel or schedule another long quiet period to try again to get a successful MSF1 decoding.
  - 2) Capture MSF1 and MSF2 where BS has access to certificates via backhaul. Report the relevant MSF1 content (15 bytes = 120 bits) and the signature portion of MSF2 (44 bytes = 352 bits) for a total of 59 bytes = 472 bits. If both CRC1 and CRC2 failed, it would not pass the information along but would report the failed CRCs. If MSF2 failed but MSF1 passed CRC, the CPE could at least report MSF1 (15 bytes) if requested by the BS. If MSF1 failed but MSF2 passed CRC, there is no useful information to report (0 bytes). Depending on whether the BS received a successful MSF1 + MSF2 decoding from another CPE, it might change the channel or schedule another long quiet period to try again to get a successful MSF1 + MSF2 decoding.
    - Optionally, a BS could collect a successful MSF1 from one CPE and a successful MSF2 from a different CPE. So, if one CPE reports only MSF1 passed and another CPE reports only MSF2 passed, the BS could request the appropriate information be passed from the respective CPEs, rather than schedule another long quiet period. This is sort of a spatial diversity.

- 3) Capture MSF1, MSF2 and MSF3 where the BS does not have backhaul access to the certificates. All CRCs need to be passed to be able to perform an authentication. If MSF1 passes but MSF2 and MSF3 fail, at least MSF1's contents could be sent if the BS requests.
- Again, optionally a BS could collect a successful MSF1 from one CPE, a successful MSF2 from another CPE, and a successful MSF3 from yet another CPE, or it could accept multiple subframes from a single CPE, i.e., if CPE<sub>1</sub> has successful MSF1 and MSF3 decoding and CPE<sub>2</sub> has successful MSF2 decoding, the BS could use the two subframes from CPE<sub>1</sub> and the single subframe from CPE 2.

A multi-frame handshaking transfer can be used here. First, depending on the mode, the CPEs report which subframes were successfully decoded. Then, from its collection of CPEs, the BS can examine which ones can provide the successful subframes and assemble its collective superframe from the constituent parts. Then CPEs transmit the relevant portions of the subframes as requested. There need to be different downlink messages to do all of this as well.

**Table 251 — Rules for indicating successful decoding of MSF1, MSF2 and MSF3**

Syntax	Size	Notes
CRC1 status	1 bit	1 = passed 0 = failed Used for all modes
CRC2 status	1 bit	1 = passed 0 = failed Used for modes b, c and d.
CRC3 status	1 bit	1 = passed 0 = failed Used for modes c and d.
Sync/index status	1 bit	1 = frame aligned 0 = frame misaligned Based on observed index words, the device did not capture the required portion of the superframe.
<i>Reserved</i>	2 bits	

Based on this initial response from a CPE, the BS might request it to send a second message with the relevant portions of the MAC subframes as shown in 7.7.18.3.1.8.

## 10.5 Geolocation

Two modes of geolocation can be used with IEEE Std 802.22. Satellite-based geolocation is mandatory. Terrestrial-based geolocation assisted by the CDMA ranging, superframe preamble, frame preamble and the coexistence beacon protocol is also described in the paragraphs that follow. The geolocation technology shall detect if any device in the network moves by a distance greater than the values specified in Table A.9 in Annex A. In such case, the BS and CPE shall follow the local regulations and shall obtain the new list of available channels from the database service based on the new location of the device.

### 10.5.1 Satellite-based Geolocation

The BS shall use its satellite-based geolocation capability to determine the latitude and longitude of its transmitting antenna within a radius of 50 m. The BS may also use the altitude information derived from the satellite-based geolocation capability.<sup>27</sup>

Each CPE shall use its satellite-based geolocation technology to determine the latitude and longitude of its antenna within a radius of 50 m. Each CPE may also use its altitude above mean sea level. Each CPE shall provide its geolocation coordinates using the NMEA strings to the BS during the registration process. The WRAN system shall use the NMEA strings provided by each CPE's satellite-based geolocation subsystem to determine the location of the CPEs.

The satellite-based geolocation antenna shall be co-located (i.e.,  $\leq 1$  m separation) with the transmit and sensing antennas.

Lock to satellite-based geolocation system is not necessary to continue operation. However, the device shall cease operation if T30 expires after losing the lock. If movement is detected, the CPE shall be de-registered via the DREG-CMD with code 0x01. CPE transmission can be re-enabled with the code 0x03 if new coordinates can be obtained. If new coordinates cannot be obtained, the CPE can be shut down by a DREG-CMD with code 0x04 or be forced to reinitialize on the current operating channel via a DREG-CMD with code 0x05.

### 10.5.2 Terrestrially-based geolocation

IEEE Std 802.22 has been designed to support terrestrially-based geolocation capability by providing all the necessary PHY and MAC tools to make it possible. Terrestrially-based geolocation can be achieved in a two-step process. First, the range between the BS and a number of its CPEs involved in the process is determined with sufficient high accuracy. Second, in order to establish the geolocation of a CPE through triangulation, the precise distances between the CPE to be geolocated and a number of reference CPEs belonging to the same cell are determined. The goal of this process is to allow an entity called the geolocator to build a precise graphic representation of the geographic location of the CPEs that form a cell under the control of the BS. This is achieved using the capabilities of the coherent multicarrier modulation inherent to the OFDM/OFDMA technique used by IEEE Std 802.22 as explained in Annex B.

The IEEE 802.22 operational conditions under which the terrestrial geolocation can be achieved with sufficient accuracy conditions are described in 10.5.2.1 and the schemes, including the actual MAC messaging, to carry out the BS-to-CPE and CPE-to-CPE ‘fine’ ranging are detailed in 10.5.2.2 and 10.5.2.3. Once the necessary timing information has been acquired through these specific schemes, a geolocation process for which an example is given in 10.5.2.4 and 10.5.2.5 can be applied to obtain the new geolocation of a CPE. Annex B gives additional details on the scientific approach to support the terrestrial geolocation process based on the properties of the coherent multicarrier modulation technique used in IEEE Std 802.22, allowing the reader to better understand this terrestrial geolocation process.

#### 10.5.2.1 Conditions to carry out precise ranging

It is first assumed that the WRAN cell is operating normally and that all the CPEs are synchronized in frequency and time to the BS on the downstream within the tolerance specified in 9.11 through the normal acquisition of the super-frame and frame preambles as described in 9.9.1. It is also assumed that the transmit frequency at the CPEs will be synchronized and locked to the frequency transmitted from the BS within the tolerance specified in 9.11 and that proper upstream time synchronization is achieved through initial ranging and periodic ranging processes as described in 9.9.3. Note that these ranging processes, based on TU increments (i.e., nominal sampling period, see Table 199) are called ‘coarse’ ranging

<sup>27</sup> The 50 m limit comes from the FCC R&O. No current requirement exists on the accuracy of the antenna height.

processes for the purpose of this subclause as opposed to the more accurate ‘fine’ ranging processes needed to carry out terrestrial geolocation as described in the paragraphs that follow.

As part of the ‘coarse’ ranging process, the BS keeps an indication of the absolute timing advance required at the CPE in integer number of TUs to compensate for the signal propagation delay on both downstream and upstream RF paths as specified in Table 44. Such absolute timing advance is referenced to a zero value when the CPE is co-located with the BS and will increase as the distance between the BS and the CPE increases. This timing advance can therefore readily be used as a coarse indication of the range between the BS and the CPE. This parameter will be used in the ‘fine’ ranging processes described below.

The ‘fine’ ranging processes will need to work with accuracy in the range of nanoseconds and the various amounts of residual delay present in different CPEs will need to be taken into account. Such residual delay may vary from one CPE model to another as well as from one antenna setup to another in the case where the antenna is not integrated to the CPE. Such residual delay will need to be measured by the manufacturer with an accuracy of at least  $\pm 30$  ns as specified in 7.7.7.3.4.10. This CPE residual delay will be declared during the CPE registration process through the REG-REQ MAC message (see 7.7.7.3.4.10).

The normal time unit used by IEEE Std 802.22 in its time synchronization and ‘coarse’ ranging is the sampling period or Time Unit (TU, see Table 199). Better time accuracy will be needed to carry out the ‘fine’ ranging described in 10.5.2.2 and the use of a sort of “vernier”<sup>28</sup> comes in handy. This “vernier” will allow an improvement of some two orders of magnitude in timing accuracy through the use of the phase correlation between the orthogonal carriers of the OFDM modulation.

### 10.5.2.2 BS-to-CPE fine ranging

If the ‘fine’ BS-to-CPE ranging process is to take place, the following procedure shall be used to provide the necessary information to the terrestrial geolocation process described in 10.5.2.4 and 10.5.2.5:

- 1) The BS transmits a RNG-CMD MAC message (see 7.7.6) to the specific CPE to re-range (ranging status = 011) and starts its counter T52 at the exact time when the downstream burst leaves the BS (i.e., at the start of the frame preamble). The T52 increments in TUs at the BS.
- 2) The BS keeps in memory (Range\_map) the symbol number scheduled in the US-MAP (see 7.7.4) for the RNG-REQ message (UIUC = 6).
- 3) The BS notes the size of the TTG in TUs for the given channel bandwidth and the cyclic prefix used in the frame (see Table 200).
- 4) The CPE acquires the values of the amplitude and phase rotation (or I&Q values) of the received subcarriers sent during the frame preamble in the downstream, removes the STS encoding and keeps the resulting information locally as the vector ‘Vernier<sub>1</sub>’. Optionally, this amplitude and phase information can also include the results of the pilot carrier tracking taking place during the downstream subframe to increase accuracy.
- 5) The CPE stores this amplitude and phase rotation information, i.e., ‘Vernier<sub>1</sub>’, in a local register (1680x2 bytes) and reports it to the BS when requested by the BLM-REQ message (see 7.7.18.3.1.10).

---

<sup>28</sup> Vernier: A vernier scale is an additional scale which allows a measurement to be read more precisely than directly reading a uniformly divided measurement scale (from: [http://en.wikipedia.org/wiki/Vernier\\_scale](http://en.wikipedia.org/wiki/Vernier_scale)).

- 6) The BS can then arrange for this data to be processed to precisely determine the time of arrival of the key multipath (usually the first) relative to the synchronization time at the CPE (which is recovered by the preamble correlator). The precise time of arrival of the downstream burst (in ns) relative to the timing of the CPE clock (incremented in TU's) can then be deduced from the values contained in 'Vernier<sub>1</sub>'. Unlike the process to gather the basic timing information described in this subclause, the calculations to accomplish this signal processing are beyond the scope of the standard and belong to the geolocation process for which a simple example is presented in 10.5.2.4 and 10.5.2.5. Note that the amplitude and phase rotation of the subcarriers recovered from the decoded frame preamble actually represent the frequency domain of the channel impulse response. Note also that typical OFDM demodulation processes readily use this information to correct the constellations in amplitude and phase at the output of the FFT for proper data decoding.
- 7) The CPE responds to the RNG-CMD MAC message by sending a RNG-REQ CDMA message in the time slot allocated in the US-MAP (UIUC = 6).
- 8) At the time of arrival of the CDMA ranging burst from the CPE, the BS stops the T52 timer precisely at the time of the first sampling period belonging to the CDMA burst.
- 9) The BS acquires the values of the amplitude and phase rotation (or I&Q values) of the 168 regularly spaced subcarriers (see 9.6.4) from the output of the FFT and removes the CDMA signature. These corrected values, which constitute 'Vernier<sub>2</sub>' (168x2 bytes), are stored at the BS and sent to the geolocator for processing.

#### **10.5.2.3 CPE-to-CPE fine ranging**

Inter-CPE communication is possible by the means of the CBP bursts (7.20.1) transmitted during the SCW (Table 35, UIUC = 0 and 1). These bursts can be used for self-coexistence between adjacent and overlapping WRAN cells, for device identification as may be required by local regulation and for carrying out the CPE-to-CPE 'fine' ranging process described in this subclause.

If the 'fine' CPE-to-CPE ranging process is to take place, the following procedure shall be used to provide the necessary information to the terrestrial geolocation process described in 10.5.2.4 and 10.5.2.5:

- 1) The BS starts the process by signaling in the US-MAP the presence of an active mode SCW at the end of the frame for the CPE that needs to be ranged (see Table 35, UIUC = 0).
- 2) The BS indicates the Timing Advance that it wants this CPE to use for its CBP burst so that this burst is received within the cyclic prefix at the nearby reference CPEs unlike the RNG-CMD Timing Advance, which is adjusted so that the CPE burst is received within the cyclic prefix at the BS. The BS can also adjust the EIRP Density Level for sufficient local coverage noting that the CBP burst may be transmitted through the antenna backlobe and received by another CPE through its antenna backlobe depending on the geometry of the RF path.
- 3) The BS signals the presence of a passive mode SCW at the end of the frame for the reference CPEs that have been selected to carry out this 'fine' CPE-to-CPE ranging process. This is done at the BS by including IE's with UIUC = 1 addressing each reference CPE to be used for 'fine' CPE to CPE ranging in the US-MAP (see Table 35).
- 4) The BS indicates that the channel to be listen to during the SCW is the operating channel and the BS specifies that the reference CPEs are to use the synchronization mode = 0 so that the CBP burst capture is done synchronously with the internal frequency and time synchronization of each reference CPE that are locked to the BS (see Table 35, UIUC = 1).

- 5) The BS uses the same frame to carry out the ‘fine’ CPE-to-CPE ranging process between the CPE to be geolocated and the reference CPEs as that used for the BS-to-CPE ‘fine’ ranging process with its reference CPEs as well as with the CPE to be geolocated as described in 10.5.2.2. Note that the adjacent frames can also be used if frequency and time synchronization slippage between these consecutive frames is tightly controlled.
- 6) The CPE in active mode transmits its CBP burst with the specified Timing Advance relative to the start of the fourth symbol before the end of the frame and the specified EIRP Density Level for proper RF path propagation margin (see Table 35) and it should contain, at least, the CBP Identification IE (see 7.6.1.3.1.6) to confirm that the burst comes from the right CPE.
- 7) Each reference CPE signaled by the BS to be in SCW passive mode during this frame captures the CBP burst using its own internal synchronization locked to the BS (i.e., Synchronization Mode = 0, see Table 35) and acquires the amplitude and phase rotation (or I&Q values) of the subcarriers contained in the CBP preamble. Optionally, this amplitude and phase information can also include the results of the pilot carrier tracking taking place during the CBP burst decoding to increase accuracy. This information constitutes the vector ‘Vernier<sub>3</sub>’, and is stored in a local register (840x2 or 1680x2 bytes).
- 8) The BS then queries the values contained in ‘Vernier<sub>3</sub>’ from each reference CPE and arrange for this data to be processed by the terrestrial geolocation process.

#### **10.5.2.4 Terrestrial geolocation process**

The terrestrial geolocation process is responsible for managing the WRAN device ‘fine’ ranging process and collecting, through the MAC messages between the BS and its CPEs, all the information necessary to carry out the calculations required to geolocate a CPE.

When the terrestrial geolocation process needs to locate a CPE, it determines which reference CPEs will be used for this purpose using existing geolocation information and its own criteria. The BS as well as a minimum of two reference CPEs, for which the location has already been determined through either surveying, satellite-based initial geolocation or by having pre-applied the current triangulation method based on other reference devices, are needed to carry out the new geolocation process. The terrestrial geolocation process signals to the BS the CPEs that it has selected to carry out the process and the BS initiates the necessary signaling process with these reference CPEs and the new CPE to be located and, once done, transfers the collected information to the terrestrial geolocation process. Triangulation calculations can then be carried out on the resulting device-to-device distances to find the location of the new CPE. All the signaling required takes place within the WRAN cell.

The BS establishes the precise distance to each of the reference CPEs as well as to the new CPE using the BS-to-CPE ranging process described in 10.5.2.2. This multiple ‘fine’ ranging process is conducted in parallel with the CPE-to-CPE ranging process to establish the distance between the new CPE and each reference CPE involved using the ranging process described in 10.5.2.3. It is assumed that the terrestrial geolocation process already knows the absolute location of the BS and of the reference CPEs and the BS only needs to gather the information that it has acquired from these various BS-to-CPE and CPE-to-CPE ranging processes.

Using all this information, the terrestrial geolocation process computes the location of the new CPE and returns a NMEA longitude-latitude string.

#### **10.5.2.5 Geolocation calculations**

Once the terrestrial geolocation process has acquired all the information generated by the ‘fine’ BS-to-CPE ranging process described in 10.5.2.2, the calculations to determine the precise BS-to-CPE propagation time and propagation distance can be carried out as follows:

BS-to-CPE Propagation time = T52 - (Range\_map+TTG) - CPE residual delay + Vernier<sub>1</sub> + Vernier<sub>2</sub>

BS-to-CPE Propagation distance =  $c \times$  Propagation time / 2

Furthermore, the various propagation distances between the BS and the reference CPEs and the CPE to be geolocated will be augmented with the information on the propagation distances obtained from the ‘fine’ CPE-to-CPE ranging process between the CPE to be geolocated and each of these reference CPEs and calculated as follows based on the Vernier<sub>3</sub> acquired in 10.5.2.3:

CPE<sub>1</sub>-to-CPE<sub>2</sub> Propagation time = -PT<sub>1</sub> + TA<sub>CBP</sub> + (PT<sub>2</sub> - CPE<sub>2</sub> residual delay) + Vernier<sub>3</sub>

where:

PT<sub>1</sub>: propagation time between the BS and CPE<sub>1</sub> as calculated by the previous equation for BS-to-CPE

PT<sub>2</sub>: propagation time between the BS and CPE<sub>2</sub> as calculated by the previous equation for BS-to-CPE

TA<sub>CBP</sub>: Timing Advance of the CBP burst [see step 2) of 10.5.2.3]

(Note that the geolocation process will have to pre-adjust TA<sub>CBP</sub> depending on the distance between the two CPE to be geolocated and the reference CPEs so that the delays measured by Vernier<sub>3</sub> fall within the symbol cyclic prefix (e.g., 74.68 μs corresponding to 22.4 km).

CPE<sub>1</sub>-to-CPE<sub>2</sub> Propagation distance = c × Propagation time / 2

Once these BS-to-CPE and CPE-to-CPE distances have been found, triangulation calculations can be carried out to come up with the precise position of the CPE to be geolocated.

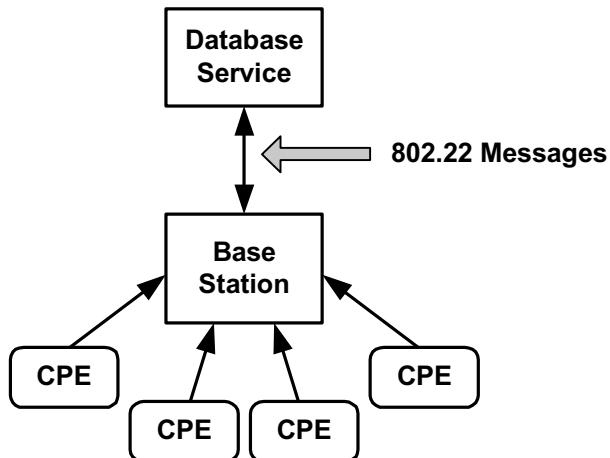
The accuracy of the process will be limited first by the accuracy of the CPE residual delays reported at registration by each CPE involved through the RNG-REQ MAC message, which is specified to be  $\pm 30$  ns in 7.7.7.3.4.10. It will also be limited by potential multipath contained in the channel impulse response received at each CPE. If complex multipath is experienced, it is possible that the right impulse that reflects the correct propagation distance may be hidden and/or diffused by other multipaths due to reflections on the RF channel. Low SNR resulting from blockage or distant reference CPEs may also impact the accuracy. However, accuracy can be improved in building redundancy in the process by using more reference CPEs. This would help in selecting the reference CPEs that provide the cleanest channels among those used for the ranging process. This choice will be made by the terrestrial geolocation process since it can have access to the channel impulse response at each reception point as the time domain representation of the different ‘Vernier’ vectors. More accuracy in the triangulation calculations can also be obtained by using more reference CPEs in these calculations.

## 10.6 Database service

### 10.6.1 System model for the database access

The system model that has been assumed all along in the development of IEEE Std 802.22 is a point-to-multipoint model for extending broadband access to less populated rural areas where more available channels can be found. In this model, the base station (BS) is assumed to control all RF parameters of its associated customer premises equipment (CPE) (frequency, EIRP, modulation, etc.) in a “master-slave” relationship so that the responsibility of protecting the TV broadcast incumbents is fully carried by the Wireless Regional Area Network (WRAN) operator. When this model was applied to an interface to the

database service proposed in the FCC R&O 08-260, the initial finding made by the IEEE 802.22 Working Group was that this interface is to take place entirely between the database service and the BS rather than with its individual CPEs. The system architecture and interface to the database services that the IEEE 802.22 Working Group has developed is depicted in Figure 185.



**Figure 185 — Structure of the IEEE 802.22 WRAN access to the database service**

#### 10.6.2 Database service access

The BS will initially enlist with the database service as a fixed device.<sup>29</sup> It will also enlist all its associated CPEs with their geographic location, device identification, etc. as obtained at association on a real time basis since its association may depend on the response from the database service. On an ongoing basis, the BS will then query the database (at least once every 24 hours) using the M-DB-AVAILABLE-CHANNEL-REQUEST message so that it can retrieve the channel information. Furthermore, the database service could send any update relevant to the BS operation through ‘push’ internet technology since the network address of the base station is provided as part of the messages. Such ‘push’ technology would allow for a better reaction time than the 24 hours minimum access time currently specified while keeping the database traffic to a minimum.

#### 10.6.3 Security for these messages

Security on the messages exchanged between the base station and the database service will be critical for the proper operation of the systems to allow authentication of the database service provider as well as the WRAN system querying the service. Security will also be necessary to avoid the message exchange being altered on the backhaul connection. The network will only support SSL on the link between the database service and the BS to provide transport layer security. The IEEE 802.22 network shall use the same authentication protocols for device and database service authentication and for interacting with the database (i.e., EAP-TLS or EAP-TTLS, see 8.4.3) as those specified for device authentication in Clause 8. All database service primitives are exchanged between the CPE/BS and the database service via Attribute Value Pairs of EAP messaging. The formatting of said messages shall conform to the authentication service (e.g., RADIUS/RFC 2865 [B26] or DIAMETER/RFC 3588 [B1]) that the database service employs.

---

<sup>29</sup> For the purpose of this document, the base station is assumed to be the operator’s contact point for the database service.

## 10.7 Primitives for cognitive radio capabilities

### 10.7.1 Database service primitives

The following list of messages, present in IEEE Std 802.22, defines the necessary messaging to support access to the database service by the BS. The format described in 10.7.1.1 to 10.7.1.8 shall be used for the messages sent directly to the database service as well as those received directly from the database service. Some parameters in the following primitives are variable-length character strings. The length of these parameters is given in terms of the number of characters in those strings. The total size of those parameters is the number of characters (the length) multiplied by the size of each character. For ASCII character sets, each character is 1 octet. For Unicode character sets, each character is 2 octets. Note that all variable-length character strings shall be null terminated.

#### 10.7.1.1 M-DB-AVAILABLE-REQUEST

**M-DB-AVAILABLE-REQUEST:** Message that allows the BS to verify that it is connected to the database service in order to receive channel availability and maximum allowed EIRP updates.

Name	Type	Length	Description
Base station-ID Length	Integer	2 bytes	Length of Base station-ID field (number of characters)
Base station-ID	Character String	Variable	In US, this is FCC-ID
Serial Number Length	Integer	2 bytes	Length of Serial Number field (number of characters)
Serial Number	Character String	Variable	
Database Service URL Length	Integer	2 bytes	Length of database service URL field (number of characters). This is used to set the Locator for the Database service
Database Service URL	Character String	Variable	A fully qualified URL starting with, http:// or https://
Base Station Database Service Access URL Length	Integer	2 bytes	Length of Base Station Database Service URL filed (number of characters)
Base Station Database Service Access URL	Character String	Variable	A fully qualified URL. This is used to set the Locator for the Base Station Access by the Database Service
Base Station Management URL Length	Integer	2 bytes	Length of Base Station Management URL field (number of characters)
Base Station Management URL	Character String	Variable	A fully qualified URL. This is used to set the Locator for the BS Management Service
Timestamp Length	Integer	2 bytes	Length of Timestamp field (number of characters)
Timestamp	Character String	NMEA 0183 \$ZDA string	Timestamp of the present request at time of transmission and as encoded in the \$ZDA substring of the NMEA 0183 string

#### 10.7.1.2 M-DB-AVAILABLE-CONFIRM

**M-DB-AVAILABLE-CONFIRM:** Message that allows the database service to confirm that the BS is still connected to the database service.

Name	Type	Length	Description
Base station-ID Length	Integer	2 bytes	Length of Base station-ID field (number of characters)
Base station-ID	Character String	Variable	In US, this is FCC-ID
Serial Number Length	Integer	2 bytes	Length of Serial Number field (number of characters)
Serial Number	Character String	Variable	
Timestamp Length	Integer	2 bytes	Length of Timestamp field (number of characters)
Timestamp	Character String	NMEA 0183 \$ZDA string	Copied from the timestamp in the M-DB-AVAILABLE-REQUEST

#### 10.7.1.3 M-DEVICE-ENLISTMENT-REQUEST

**M-DEVICE-ENLISTMENT-REQUEST:** Message that allows the BS to enlist with the database service a device that has joined its WRAN network.<sup>30</sup>

Name	Type	Length	Description
Device Type	Integer	1 byte	The value identifies the type of device obtained as part of its process to associate 0x00 = Fixed base station 0x01 = Fixed CPE 0x02 = Personal/portable mode 0x03–0xFF = Reserved
Device-ID Length	Integer	2 bytes	Length of Device-ID field (number of characters)
Device-ID	Character String	Variable	In US, this is FCC-ID
Serial Number Length	Integer	2 bytes	Length of Serial Number field (number of characters)
Serial Number	Character String	Variable	
Proxy Device-ID Length	Integer	2 bytes	Length of Proxy Device-ID field (number of characters)
Proxy Device-ID	Character String	Variable	This element is the device ID for the device (most likely the controlling BS) that is acting as the proxy to the database service. (In US, this is the FCC-ID.)
Proxy Serial Number Length	Integer	2 bytes	Length of Proxy Serial Number field (number of characters)
Proxy Serial Number	Character String	Variable	This element is the serial number for the device (most likely the controlling BS) that is acting as the proxy to the database service.
Location Data String Length	Integer	2 bytes	Length of Location Data String field (number of characters)
Location Data String	Character String	NMEA 0183	The value identifies the location of the device (latitude, longitude).
Responsible Party Name Length	Integer	2 bytes	Length of Responsible Party Name field (number of characters)
Responsible Party Name	Character String	Variable	
Antenna height	Integer	1 byte	Antenna height above ground level in meters.
If (Device Type = 0x00 or 0x01) {			

<sup>30</sup> Note that this interface allows enlistment of TVBD devices (beyond IEEE 802.22 BS and CPE) that may not need to be formally “registered” as required by the FCC R&O 08-260 for potential broader capability and applicability of the database service.

Name	Type	Length	Description
Contact Name Length	Integer	2 bytes	Length of Contact Name field (number of characters)
Contact Name	Character String	Variable	
Contact Physical Address Length	Integer	2 bytes	Length of Contact Physical Address field (number of characters)
Contact Physical Address	Character String	Variable	
Contact Email Address Length	Integer	2 bytes	Length of Contact Email Address field (number of characters)
Contact Email Address	Character String	Variable	
Contact Telephone Number Length	Integer	2 bytes	Length of Contact Telephone Number field (number of characters)
Contact Telephone Number	Character String	Variable	
}			
Base Station Database Service Access URL Length	Integer	2 bytes	Length of Base Station Database Service URL field (number of characters)
Base Station Database Service Access URL	Character String	Variable	A fully qualified URL. This is used to set the Locator for the Base Station Access by the Database Service.
Database Service URL Length	Integer	2 bytes	Length of Database Service URL field (number of characters)
Database Service URL	Character String	Variable	A fully qualified URL starting with, http:// or https://
If (wraniIfDatabaseService BSAntennaInformation SupportedMib) {			
Antenna information	Character String	72 bytes	Antenna directionality information of the device in dB relative to the main lobe maximum gain for every 5 degree azimuth clockwise starting from the direction of the maximum antenna gain expressed in unit of 0.25 dB over the range -63.75 dB (encoded 0x00) to 0 dB (0xFF). (to allow the database calculation of the channel availability and the maximum allowed EIRP values at the registering location <sup>31</sup> )
Antenna azimuth	Integer	2 bytes	Antenna azimuth in degrees, clockwise from true North
}			
}			
Timestamp Length	Integer	2 bytes	Length of Timestamp field (number of characters)
Timestamp	Character String	NMEA 0183 \$ZDA string	Timestamp of the present request at time of transmission and as encoded in the \$ZDA substring of the NMEA 0183 string

#### 10.7.1.4 M-DEVICE-ENLISTMENT-CONFIRM

**M-DEVICE-ENLISTMENT-CONFIRM:** Message that allows the database service to confirm to the BS that the new device has been successfully registered.

<sup>31</sup> Antenna directionality will represent the antenna gain pattern in the horizontal plane in dB referred to the gain of its main lobe and it is assumed that the database service will use its knowledge of the geolocation of the base station and the device being enlisted to calculate the azimuth of the device antenna main lobe for interference calculations in the case of base station and CPE operation. Omnidirectional antennas shall be assumed as the default.

Name	Type	Length	Description
Device-ID Length	Integer	2 bytes	Length of Device-ID field (number of characters)
Device-ID	Character String	Variable	In US, this is FCC-ID
Serial Number Length	Integer	2 bytes	Length of Serial Number field (number of characters)
Serial Number	Character String	Variable	
Timestamp Length	Integer	2 bytes	Length of Timestamp field (number of characters)
Timestamp	Character String	NMEA 0183 \$ZDA string	Copied from the timestamp in the M-DB-AVAILABLE-REQUEST

#### 10.7.1.5 M-DB-AVAILABLE-CHANNEL-REQUEST

**M-DB-AVAILABLE-CHANNEL-REQUEST:** Message that allows the BS to request a list of available channels and maximum allowed EIRP per channel from the database service for the specified type of device at the particular location.

Name	Type	Length	Description
Device Type	Integer	1 byte	The value identifies the type of device at the geolocation registering 0x00 = Fixed base station 0x01 = Fixed CPE 0x02 = Personal/portable mode 0x03–0xFF = Reserved
Device-ID Length	Integer	2 bytes	Length of Device-ID field (number of characters)
Device-ID	Character String	Variable	In US, this is FCC-ID
Serial Number Length	Integer	2 bytes	Length of Serial Number field (number of characters)
Serial Number	Character String	Variable	
Location Data String Length	Integer	2 bytes	Length of Location Data String field (number of characters)
Location Data String	Character String	NMEA 0183 Character String	The value identifies the location of the device (latitude, longitude) <sup>32</sup>
Timestamp Length	Integer	2 bytes	Length of Timestamp field (number of characters)
Timestamp	Character String	NMEA 0183 \$ZDA string	Timestamp of the present request at time of transmission and as encoded in the \$ZDA substring of the NMEA 0183 string

#### 10.7.1.6 M-DB-AVAILABLE-CHANNEL-INDICATION

**M-DB-AVAILABLE-CHANNEL-INDICATION:** Message that is used to return to the BS the list of available channels as provided by the database service in the form of channel, maximum allowed EIRP, and availability schedule.

---

<sup>32</sup> See footnote 3.

Name	Type	Length	Description
Device-ID Length	Integer	2 bytes	Length of Device-ID field (number of characters)
Device-ID	Character String	Variable	In US, this is FCC-ID
Serial Number Length	Integer	2 bytes	Length of Serial Number field (number of characters)
Serial number	Character String	Variable	
Number of Channels Available	Integer	1 byte	
{ If( Number of Channels Available > 0)			If the number of channels is equal to 0, this means that the device cannot operate.
For ( $i=1; i \leq$ Number of Channels Available; $i++$ ) { Channel_Number Max_Allowed_EIR (dBm) Availability schedule } }	Vector of $2 \times N$ bytes and a number of pairs of NMEA 0183 \$ZDA strings	Variable	List of available channel numbers and corresponding maximum allowed EIRP expressed in dBm over the range -64 dBm (encoded 0x00) to +63.5 dBm (encoded 0xFF) as well as the availability schedule (start and stop date/time) for each channel in Universal date and time system
Status Message	Character String	Variable	Various status messages coming from the database service (e.g., unapproved device flag)
Timestamp Length	Integer	2 bytes	Length of Timestamp field (number of characters)
Timestamp	Character String	NMEA 0183 \$ZDA string	Copied from the timestamp in the M-DB-AVAILABLE-CHANNEL-REQUEST

#### 10.7.1.7 M-DB-DELIST-REQUEST

**M-DB-DELIST-REQUEST:** Message that allows the BS to request the database service to remove the enlistment of a device that was associated with that base station.

Name	Type	Length	Description
Device-ID Length	Integer	2 bytes	Length of Device-ID field (number of characters)
Device-ID	Character String	Variable	In US, this is FCC-ID
Serial Number Length	Integer	2 bytes	Length of Serial Number field (number of characters)
Serial Number	Character String	Variable	
Responsible Party Name Length	Integer	2 bytes	Length of Responsible Party Name field (number of characters)
Responsible Party Name	Character String	Variable	
Location Data String Length	Integer	2 bytes	Length of Location Data String
Location Data String	Char	NMEA 0183 Character string	The value identifies the location of the device (latitude, longitude) <sup>33</sup>

---

<sup>33</sup> See footnote 3.

### 10.7.1.8 M-DB-DELIST-CONFIRM

**M-DB-DELIST-CONFIRM:** Message that is used to inform the BS whether its request to remove the enlistment of a device that was associated with that base station was successfully received and executed by the database service.

Name	Type	Length	Description
Device-ID	Character String	Variable	In US, this is FCC-ID
Serial Number	Character String	Variable	
Responsible Party Name	Character String	Variable	
Location Data String Length	Integer	2 bytes	Length of Location Data String field (number of characters)
Location Data String	Character String	NMEA 0183 Character string	The value identifies the location of the device (latitude, longitude)

### 10.7.2 BS configuration and monitoring primitives

The BS SM occasionally sends the available channel list to its higher layers for additional channel classification. The available channel list can be presented to its higher layers to have channels classified as disallowed. The classification of an operating channel by the BS is also performed by its higher layers. The M-SAP is an interface that provides a means of exchange information between the SM and the higher layers in the BS. Table 252 summarizes the primitives supported by the SM to pass the available channel list and to receive disallowed channel classifications and the selected operating channel through the M-SAP interface. The primitives are discussed in the subclauses referenced in the table.

**Table 252 — Available channel list primitives supported by the M-SAP**

Name	Request	Indication	Confirm
M-AVAIL-TV-CH-REPORT	10.7.2.1		10.7.2.2
M-DISALLOWED-TV-CHS		10.7.2.3	
M-OPERATING-TV-CH		10.7.2.4	

#### 10.7.2.1 M-AVAIL-TV-CH-REPORT.request

The M-AVAIL-TV-CH-REPORT.request primitive is sent by the BS SM to request the higher layers for a selection of an operating channel based on the available channel list information provided this primitive. Table 253 specifies the parameters for the M-AVAIL-TV-CH-REPORT.request primitive.

**Table 253 — M-AVAIL-TV-CH-REPORT.request parameters**

Name	Type	Valid range	Description
For ( $i = 1; i \leq$ Number of Channels Available; $i++$ ) { Channel_Number Maximum Allowed EIRP }	List of available channels and their Maximum Allowed EIRP		List of available channels and corresponding Maximum Allowed EIRP
Mode			The expected response from the higher layers 0 = Test 1 = Request for disallowed channel classification 2 = Request for selection of operating channel

#### 10.7.2.1.1 When generated

The M-AVAIL-TV-CH-REPORT.request primitive is generated by the BS SM and issued to the higher layers either (depending on the mode) to request disallowed channel classification or selection of an operating channel during BS initialization as described in 7.14.1.

#### 10.7.2.1.2 Effect on receipt

When the higher layers receive the M-AVAIL-TV-CH-REPORT.request primitive, they generate an M-AVAIL-TV-CH-REPORT.confirm primitive to notify the SM if the request was successfully received.

#### 10.7.2.2 M-AVAIL-TV-CH-REPORT.confirm

The M-WRAN-SERVICE-REPORT.confirm primitive allows the higher layers to inform the SM if the receipt of the available channel list was successful. Table 254 specifies the parameters for the M-AVAIL-TV-CH-REPORT.confirm primitive.

**Table 254 — M-WRAN-SERVICE-REPORT.confirm parameters**

Name	Type	Valid range	Description
Status	Enumeration	SUCCESS, INVALID_REQUEST	The value indicates whether the request to select a WRAN service was successfully generated.

#### 10.7.2.2.1 When generated

The M-AVAIL-TV-CH-REPORT.confirm primitive is generated by the higher layers and issued to its MIB when an M-AVAIL-TV-CH-REPORT.request primitive is received to indicate whether the available channel list was successfully generated.

#### 10.7.2.2.2 Effect on receipt

When the SM of a CPE receives the M-AVAIL-TV-CH-REPORT.confirm primitive and depending on the mode, it expects the higher layers either to return nothing, an M-DISALLOWED-TV-CHS.indication primitive with classified disallowed channels, or an M-OPERATING-TV-CH.indication with the selected channel.

### 10.7.2.3 M-DISALLOWED-TV-CHS.indication

The M-DISALLOWED-TV-CHS.indication primitive is used by the higher layers to return the disallowed channels on the available channel list to the SM per its request. Table 255 specifies the parameters for the M-DISALLOWED-TV-CHS.indication primitive.

**Table 255 — M-DISALLOWED-TV-CHS.indication parameters**

Name	Type	Valid range	Description
For ( $i = 1; i \leq$ Number of Channels Disallowed; $i++$ ) { Channel_Number }	List of disallowed channels		List of disallowed channels.

#### 10.7.2.3.1 When generated

The M-DISALLOWED-TV-CHS.indication primitive is generated by the higher layers and issued to the MIB to indicate the disallowed channels from the available channel list.

#### 10.7.2.3.2 Effect on receipt

When the SM receives the M-DISALLOWED-TV-CHS.indication it will identify whether the response to its request for the higher layers to classify channels as disallowed from the available channel list was successfully received by the higher layers, in which case, the SM will obtain the classified disallowed channels and the BS will continue to the following steps of initialization and perform detection, described in 7.14.1.6. If the response is not successful, the SM may decide to issue another request.

### 10.7.2.4 M-OPERATING-TV-CH.indication

The M-OPERATING-TV-CH.indication primitive is used by the higher layers to return the selected operating channel on the available channel list to the SM per its request. Table 256 specifies the parameters for the M-OPERATING-TV-CH.indication primitive.

**Table 256 — M-OPERATING-TV-CH.indication parameters**

Name	Type	Valid range	Description
Channel_Number	The selected operating channel	0–80	The selected operating channel

#### 10.7.2.4.1 When generated

The M-OPERATING-TV-CH.indication primitive is generated by the higher layers and issued to the MIB to indicate the selected operating channel from the available channel list.

#### 10.7.2.4.2 Effect on receipt

When the SM receives the M-OPERATING-TV-CH.indication it will identify whether the response to its request for the higher layers to select the operating channel from the available channel list was successfully received by the higher layers, in which case, the SM will obtain the selected operating channel and the BS

will continue to commence operation on the selected channel. If the response is not successful the SM may decide to issue another request.

### 10.7.3 CPE reports the resulting available WRAN services list

The selection of WRAN service by the CPE is performed by its higher layers. The M-SAP is an interface that provides a means of exchange information between the SA and the higher layers. Table 257 summarizes the primitives supported by the SM to pass the available WRAN services list and the selected WRAN service through the M-SAP interface. The primitives are discussed in the subclauses referenced in the table.

**Table 257 — Available WRAN services list primitives supported by the M-SAP**

Name	Request	Indication	Confirm
M-WRAN-SERVICE-REPORT	10.7.3.1		10.7.3.2
M-WRAN-SERVICE-RESPONSE		10.7.3.3	

#### 10.7.3.1 M-WRAN-SERVICE-REPORT.request

The M-WRAN-SERVICE-REPORT.request primitive is sent by the CPE SA to request the higher layers for a selection of a WRAN service based on the available WRAN service list information provided this primitive. Table 258 specifies the parameters for the M-WRAN-SERVICE-REPORT.request primitive.

**Table 258 — M-WRAN-SERVICE-REPORT.request parameters**

Name	Type	Valid range	Description
For ( $i = 1; i \leq$ Number of Channels Available; $i++$ ) { WRAN service Channel_Number RSSI }	List of available WRAN services, the channel, and the received signal strength		List of available WRAN services, corresponding channel, and received signal strength.

##### 10.7.3.1.1 When generated

The M-WRAN-SERVICE-REPORT.request primitive is generated by the CPE SA and issued to the higher layers to request a selection of a WRAN service during CPE initialization as described in 7.14.2.5.

##### 10.7.3.1.2 Effect on receipt

When the higher layers receive the M-WRAN-SERVICE-REPORT.request primitive, it generates an M-WRAN-SERVICE-REPORT.confirm primitive to notify the SM if the request was successfully received.

#### 10.7.3.2 M-WRAN-SERVICE-REPORT.confirm

The M-WRAN-SERVICE-REPORT.confirm primitive allows the higher layers to inform the SA if the request to select an available WRAN service was successful. Table 259 specifies the parameters for the M-WRAN-SERVICE-REPORT.confirm primitive.

**Table 259 — M-WRAN-SERVICE-REPORT.confirm parameters**

Name	Type	Valid range	Description
Status	Enumeration	SUCCESS, INVALID_REQUEST	The value indicates whether the request to select a WRAN service was successfully generated.

#### 10.7.3.2.1 When generated

The M-WRAN-SERVICE-REPORT.confirm primitive is generated by the higher layers and issued to the MIB when an M-WRAN-SERVICE-REPORT.request primitive is received to indicate whether the request to select a WRAN service was successfully generated.

#### 10.7.3.2.2 Effect on receipt

When the SA of a CPE receives the M-WRAN-SERVICE-REPORT.confirm primitive, it expects the higher layers to return an M-WRAN-SERVICE-RESPONSE.indication primitive with a selected WRAN service.

#### 10.7.3.3 M-WRAN-SERVICE-RESPONSE.indication

The M-WRAN-SERVICE-RESPONSE.indication primitive is used by the higher layers to return a selected WRAN channel from the available WRAN service list to the SA per its request. Table 260 specifies the parameters for the M-WRAN-SERVICE-RESPONSE.indication primitive.

**Table 260 — M-WRAN-SERVICE-RESPONSE.indication parameters**

Name	Type	Valid range	Description
Selected Channel Number	Integer	0–80	The value identifies the selected channel of the WRAN service.

#### 10.7.3.3.1 When generated

The M-WRAN-SERVICE-RESPONSE.indication primitive is generated by the higher layers and issued to the MIB to indicate the selected channel from the available WRAN service list.

#### 10.7.3.3.2 Effect on receipt

When the SA receives the M-WRAN-SERVICE-RESPONSE.indication it will identify whether the response to its request for the higher layers to select a channel from the available WRAN service list was successfully received by the higher layers, in which case, the SA will obtain the selected channel and CPE will continue to the following steps of initialization. If the response is not successful the SA may decide to issue another query.

### 10.7.4 Spectrum Sensing Services

The IEEE 802.22 PHY layer shall provide local spectrum sensing services through its SSF accessed through the SM-SSF-SAP. Table 261 summarizes the spectrum sensing primitives supported through the SM-SSF-SAP interface. The primitives are discussed in the subclauses referenced in the table.

**Table 261 — Spectrum Sensing Primitives supported by the SM-SSF-SAP**

Name	Request	Indication	Confirm
SM-SSF-SAP-CHANNEL-SENSING	10.7.4.1		10.7.4.2
SM-SSF-SAP-SENSING-RESULTS		10.7.4.3	

#### 10.7.4.1 SM-SSF-SAP-CHANNEL-SENSING.request

The SM-SSF-SAP-CHANNEL-SENSING.request primitive allows the SM to request the local PHY SSF unit to perform spectrum sensing. Table 262 specifies the parameters for the SM-SSF-SAP-CHANNEL-SENSING.request primitive.

**Table 262 — SM-SSF-SAP-CHANNEL-SENSING.request parameters**

Name	Type	Length (bits)	Value / Description
ISO 3166 Country Code	ASCII	24 bits	See Annex A
Channel Number	Integer	8 bits	The channel number that is to be sensed by the SSF. Range as specified in Table 236.
Channel Bandwidth	Integer	4 bits	The bandwidth of the channel to be sensed by the SSF. Values as specified in Table 236.
Sensing Mode	Integer	2 bits	The sensing mode specifies which SSF outputs are valid as specified in Table 239.
Signal Type Array	Array	32 bits	An array indicating which signal types the SSF is to sense for as specified in Table 237.
Sensing Window Specification Array	Array	$N \times 32$	$N$ is the number of signal types enumerated (that are equal to ‘1’) in the Signal Type Array. Sensing window specifications as given in Table 245 and Table 246. Each element in the Sensing Window Specification consists of: NumSensingPeriods SensingPeriodDuration SensingPeriodInterval
Maximum Probability of False Alarm Array	Array	$N \times 8$	$N$ is the number of signal types enumerated (that are equal to ‘1’) in the Signal Type Array. This value is valid only for sensing modes 0 and 1. Each element specifies the maximum probability of false alarm for the corresponding signal type decision in the sensing present Array. Maximum Probability of False Alarm – 0x00 indicates ‘0’ and 0x01 indicates ‘0.001, and 0xFF = 0.255 (see Table 236).

##### 10.7.4.1.1 When generated

The SM-SSF-SAP-CHANNEL-SENSING.request primitive is generated by the SM and issued to the SSF to request the local PHY SSF to perform spectrum sensing.

##### 10.7.4.1.2 Effect on receipt

When the SSF receives the SM-SSF-SAP-CHANNEL-SENSING.request primitive, it requests the local PHY SSF to perform spectrum sensing.

On receipt of the SM-SSF-SAP-CHANNEL-SENSING.request the SSF shall issue a SM-SSF-SAP-CHANNEL-SENSING.confirm primitive to the SM with a status value.

#### 10.7.4.2 SM-SSF-SAP-CHANNEL-SENSING.confirm

The SM-SSF-SAP-CHANNEL-SENSING.confirm primitive is used to inform the SM whether its request to the local PHY SSF was successfully generated by the SM. Table 263 specifies the parameters for the SM-SSF-SAP-CHANNEL-SENSING.confirm primitive.

**Table 263 — SM-SSF-SAP-CHANNEL-SENSING.confirm parameters**

Name	Type	Length (bits)	Value / Description
ISO 3166 Country Code	ASCII	16 bits	
Channel Number	Integer	8 bits	The channel number that is to be sensed by the SSF. Range is specified in Table 236.
Sensing Mode	Integer	2 bits	The sensing mode specifies which SSF outputs are valid as specified in Table 239.
Status	Enumeration	2 bits	00: INVALID_REQUEST 01: INVALID_SIGNAL_TYPES 10: Reserved 11: SUCCESS The value indicates whether the sensing request was successfully generated.
Invalid Signal Type Array	Array	32 bits	An array indicating that signal types the SSF will not be able to sense as specified in Table 237. This attribute is valid only if the Status = INVALID_SIGNAL_TYPES

##### 10.7.4.2.1 When generated

The SM-SSF-SAP-CHANNEL-SENSING.confirm primitive is generated by the SSF and issued to its SM to indicate whether the received SM-SSF-SAP-CHANNEL-SENSING.request was valid and whether the SSF is able to perform sensing for the signal types as requested. If the SSF is able to perform the sensing in the requested sensing mode and with the requested probability of false alarm for all types of signals requested, the Status code shall be set to SUCCESS. If the SSF does not support the requested sensing mode, the status value should be INVALID\_REQUEST. If one or more of the signal types in the request is not valid or the SSF does not have the capability to sensing a requested signal type, the status code should be set to INVALID\_SIGNAL\_TYPE and the corresponding invalid signal types shall be indicated in the Invalid Signal Type Array.

##### 10.7.4.2.2 Effect on receipt

When the SM receives the SM-SSF-SAP-CHANNEL-SENSING.confirm primitive, it will identify whether its request to the local PHY SSF was successfully received by the SSF. The status parameter indicates the appropriate error code from 7.7.24 in case the request is invalid.

#### 10.7.4.3 SM-SSF-SAP-SENSING-RESULTS.indication

The SM-SSF-SAP-SENSING-RESULTS.indication primitive is used to inform the SM when the results of a previously issued request to the local PHY SSF were successfully generated by the SSF. Table 264 specifies the parameters for the SM-SSF-SAP-SENSING-RESULTS.indication primitive.

**Table 264 — SM-SSF-SAP-SENSING-RESULTS.indication parameters**

Name	Type	Length (bits)	Value / Description
ISO 3166 Country Code	ASCII	16 bits	
Channel Number	Integer	8 bits	The channel number that is to be sensed by the SSF. Range as specified in Table 236.
Sensing Mode	Integer	2 bits	The sensing mode specifies which SSF outputs are valid as specified in Table 239.
Signal Type Array	Array	32 bits	An array indicating which signal types the SSF is to sense as specified in Table 237.
Signal Present Array	Array	$N \times 2$	$N$ is the number of signal types enumerated (that are equal to '1') in the Signal Type Array. Each element in the Array is a signal present decision. Each decision can take on three possible values, as given in Table 240.
Confidence Array	Array	$N \times 8$	Confidence array is only valid for Sensing Mode 2. Each element in the confidence Array is a confidence metric for the sensing result for the corresponding signal type as defined in Table 240.  0x00: No confidence 0x01 to 0xFE: Reserved 0xFF: Full confidence
RSSI Measurements	Integer	8 bits	RSSI Measurement is only valid for Sensing Mode 3.  Each RSSI measurement result is a signed integer number encoded with 8 bits (see Table 240). BS can ask the CPE for up to 255 measurements of the RSSI. In such case, each RSSI measurement will represent the mean of the multiple measurement results.
RSSI Standard Deviation	Integer	8 bits	RSSI Measurement is only valid for Sensing Mode 3. BS can ask the CPE for up to 255 measurements of the RSSI. In such case, this parameter represents the result of the standard deviation calculation done on these multiple RSSI measurements results.

#### 10.7.4.3.1 When generated

The SM-SSF-SAP-SENSING-RESULTS.indication primitive is generated by the SSF and issued to the SM to indicate the results of a previously issued request to the local PHY SSF have been generated.

#### 10.7.4.3.2 Effect on receipt

When the SM receives the SM-SSF-SAP-SENSING-RESULTS.indication it will obtain the sensing results to its request to the local PHY SSF.

### 10.7.5 Geolocation services

The PHY layer provides local geolocation services through its satellite-based location acquisition unit to the SM/SSA through the SM-GL-SAP. Table 265 summarizes the geolocation primitives supported through the SM-GL-SAP interface. The primitives are discussed in the subclauses referenced in the table.

**Table 265 — Geolocation Primitives supported by the SM-GL-SAP**

Name	Request	Indication	Confirm
SM-GL-SAP-GEOLOCATION	10.7.5.1		10.7.5.2
SM-GL-SAP-GEOLOCATION-RESULTS		10.7.5.3	

#### 10.7.5.1 SM-GL-SAP-GEOLOCATION.request

The SM-GL-SAP-GEOLOCATION.request primitive allows the SM to request the local PHY geolocation unit to perform geolocation. Table 266 specifies the parameters for the SM-GL-SAP-GEOLOCATION.request primitive.

**Table 266 — SM-GL-SAP-GEOLOCATION.request parameters**

Name	Type	Valid range	Description
NMEA Sentence Request	String	(length 6 octets)	NMEA 0183 ASCII string (e.g., \$GPGGA)

##### 10.7.5.1.1 When generated

The SM-GL-SAP-GEOLOCATION.request primitive is generated by the SM and issued to its SSF to request the local PHY geolocation service to perform geolocation.

##### 10.7.5.1.2 Effect on receipt

When the Geolocation receives the SM-GL-SAP-GEOLOCATION.request primitive, it requests the local PHY geolocation service to perform geolocation.

On receipt of the SM-GL-SAP-GEOLOCATION.request the Geolocation shall issue a SM-GL-SAP-GEOLOCATION.confirm primitive to the SM with a status value.

#### 10.7.5.2 SM-GL-SAP-GEOLOCATION.confirm

The SM-GL-SAP-GEOLOCATION.confirm primitive is used to inform the SM whether its request to the local PHY geolocation service was successfully generated by the Geolocation. Table 267 specifies the parameters for the SM-GL-SAP-GEOLOCATION.confirm primitive.

**Table 267 — SM-GL-SAP-GEOLOCATION.confirm parameters**

Name	Type	Valid range	Description
Status	Enumeration	SUCCESS, INVALID_REQUEST	The value indicates whether the requested query was successfully generated.

##### 10.7.5.2.1 When generated

The SM-GL-SAP-GEOLOCATION.confirm primitive is generated by the Geolocation and issued to its SM to indicate whether the received SM-GL-SAP-GEOLOCATION.request was valid, in which case the Geolocation acquires the requested NMEA sentence from the local PHY geolocation service.

#### **10.7.5.2.2 Effect on receipt**

When the SM receives the SM-GL-SAP-GEOLOCATION.confirm primitive, it will identify whether its request to the local PHY geolocation service was successfully received by the Geolocation. The status parameter indicates the appropriate error code from 7.7.24 in case the local PHY geolocation service was not available.

#### **10.7.5.3 SM-GL-SAP-GEOLOCATION-RESULTS.indication**

The SM-GL-SAP-GEOLOCATION-RESULTS.indication primitive is used to inform the SM when a response to a previously issued request to the local PHY geolocation service was successfully received by the Geolocation. Table 268 specifies the parameters for the SM-GL-SAP-GEOLOCATION-RESULTS.indication primitive.

**Table 268 — SM-GL-SAP-GEOLOCATION-RESULTS.indication parameters**

Name	Type	Valid range	Description
Length	Integer	0–128	Length of the location data string in octets (0 to 128 characters)
Location Data String	Char	NMEA string	NMEA 0183 ASCII string

#### **10.7.5.3.1 When generated**

The SM-GL-SAP-GEOLOCATION-RESULTS.indication primitive shall be generated by the Geolocation and issued to the SM to indicate the reception of a response to a query previously issued to the local PHY geolocation service.

#### **10.7.5.3.2 Effect on receipt**

When the SM receives the SM-GL-SAP-GEOLOCATION-RESULTS.indication it shall identify whether the response to its request to the local PHY service was successfully received by the Geolocation, in which case, the SM will obtain NMEA string containing the latitude and longitude information. If the response is not successful the SM may decide to issue another request.

### **10.7.6 Antenna primitives**

Essential antenna information is provided to the MAC by the antenna through the M-SAP. The M-SAP is an interface that provides a means of exchanging information between the SM at the BS MAC and the SSA at the CPE MAC and their respective antenna. Table 269 summarizes the primitives supported by the MAC to access antenna information through the M-SAP interface. The primitives are discussed in the subclauses referenced in the table.

**Table 269 — Antenna primitives supported by the M-SAP**

Name	Request	Indication	Confirm	Response
M-ANTENNA-INTEGRATED	10.7.6.1		10.7.6.2	
M-ANTENNA- INFORMATION	10.7.6.3			10.7.6.4

### **10.7.6.1 M-ANTENNA-INTEGRATED.request**

The M-ANTENNA-INTEGRATED.request primitive allows the MAC to identify whether the device's antenna is integrated or non-integrated through the M-SAP in order to know whether it is required to get antenna gain information for calculation of EIRP. The M-ANTENNA-INTEGRATED.request primitive has no attributes.

#### **10.7.6.1.1 When generated**

The M-ANTENNA-INTEGRATED.request primitive shall be generated by the MAC and issued to its antenna to identify whether its antenna is integrated or non-integrated.

#### **10.7.6.1.2 Effect on receipt**

When the antenna receives the M-ANTENNA-INTEGRATED.request primitive, the antenna shall generate an M-ANTENNA-INTEGRATED.confirm primitive to indicate whether the antenna is integrated or non-integrated.

### **10.7.6.2 M-ANTENNA-INTEGRATED.confirm**

The M-ANTENNA-INTEGRATED.confirm primitive allows the antenna to inform the MAC whether it is integrated or non-integrated through the M-SAP. Table 270 specifies the parameters for the M-ANTENNA-INTEGRATED.confirm primitive.

**Table 270 — M-ANTENNA-INTEGRATED.confirm parameters**

Name	Type	Valid range	Description
Antenna Type	Integer	0–1	The value indicates whether the antenna is integrated or non-integrated. 0 = integrated antenna 1 = non-integrated antenna

#### **10.7.6.2.1 When generated**

The M-ANTENNA-INTEGRATED.confirm primitive shall be generated by the antenna and issued to its MAC when an M-ANTENNA-INTEGRATED.request primitive is received to indicate whether the antenna is integrated or non-integrated through the M-SAP.

#### **10.7.6.2.2 Effect on receipt**

When the MAC receives the M-ANTENNA-INTEGRATED.confirm primitive, the SM at the BS and the SSA at the CPE shall identify whether the antenna is integrated or non-integrated.

### **10.7.6.3 M-ANTENNA-INFORMATION.request**

The M-ANTENNA-INFORMATION.request primitive allows the MAC to request antenna information from the antenna. The M-ANTENNA-INFORMATION.request primitive has no attributes.

#### 10.7.6.3.1 When generated

The M-ANTENNA-INFORMATION.request primitive shall be generated by the SM of a BS or the SSA of the CPE and issued to their respective antenna for antenna information.

#### 10.7.6.3.2 Effect on receipt

When the antenna receives the M-ANTENNA-INFORMATION.request primitive, the antenna shall generate an M-ANTENNA-INFORMATION.response containing information that describes the attributes of the antenna.

#### 10.7.6.4 M-ANTENNA-INFORMATION.response

The M-ANTENNA-INFORMATION.response primitive is used to respond to the MAC request with antenna information. Table 271 specifies the parameters for the M-ANTENNA-INFORMATION.response primitive.

**Table 271 — M-ANTENNA-INFORMATION.response parameters**

Name	Type	Valid range	Description
For ( $i = 1$ ; $i \leq$ Number of Channels; $i++$ ) { Channel_Number Maximum Gain }	List channels and max gain per channel		List Channel Numbers and corresponding maximum gain (dBi).

#### 10.7.6.4.1 When generated

The M-ANTENNA-INFORMATION.response primitive shall be generated by the antenna and issued to the MAC to respond with information about the antenna.

#### 10.7.6.4.2 Effect on receipt

When the MAC receives the M-ANTENNA-INFORMATION.response, MAC shall store the maximum gain (dBi) for each channel so that the device can convert from transmit power to EIRP.

## 11. Configuration

Tamper-proof mechanisms shall be implemented to prevent unauthorized modification to firmware and/or functionalities (e.g., MAC address, SM/SSA functionality, database service communication, RF sensing, DFS, TPC, tuning) that would allow device or network operation to violate either the specifications of IEEE Std 802.22 or the requirements of the local regulations. Any attempt to load unapproved firmware into an IEEE 802.22 device shall render it inoperable. Measures for both local and remote attestation of authorized and approved hardware and software running on an IEEE 802.22 device shall be implemented. Implementation of the Trusting Computing Group's Trusted Platform Module (TPM) Main Specification Level 2 Version 1.2 (Revision 103) [see TPM references in Clause 2] shall be used to bind the hardware and software running on IEEE 802.22 devices to a cryptographic key.

When a CPE detects that the information on the antenna model and serial number has changed (see 9.12.2) after a request from the BS for this information (REG-REQ/RSP, see 7.7.7.3.4.9), the CPE shall re-initialize.

## 12. Parameters and connection management

### 12.1 Parameters, timers, message IEs

This subclause defines bounds for various parameters, timers, and message/IE fields that are specified throughout the standard.

#### 12.1.1 MAC (dynamic service flow, multicast, ARQ, capability, and bandwidth management)

**Table 272 — MAC parameters, timers, message IEs**

Entity/ Scope	Name	Reference	Min value	Default value	Max value
CPE, BS	DSx Request Retries	Number of Timeout Retries on DSA/DSC/DSD Requests	—	3	—
CPE, BS	DSx Response Retries	Number of Timeout Retries on DSA/DSC/DSD Responses	—	3	—
CPE	T6	Wait for registration response	—	—	3 s
CPE, BS	T7	Wait for DSA/DSC/DSD Response timeout	—	—	1 s
CPE, BS	T8	Wait for DSA/DSC Acknowledge timeout	—	—	300 ms
BS	T9	Registration Timeout, the time allowed between the BS sending a RNG-CMD (success) to a CPE, and receiving a CBC-REQ from that same CPE	300 ms	300 ms	—
CPE, BS	T10	Wait for Transaction End timeout	—	—	3 s
BS	T13	The time allowed for an CPE, following receipt of a REG-RSP message to send a TFTP-CPLT message to the BS	15 min	15 min	—
CPE	T14	Wait for DSx-RSP/DSX-RVD Timeout	—	—	200 ms
BS	T15	Wait for MCA-RSP	20 ms	20 ms	—
CPE	T16	Wait for bandwidth request grant	10 ms	—	Service QoS dependent
CPE	T18	Wait for CBC-RSP timeout	—	5 ms	<< T9
CPE, BS	T22	Wait for ARQ-Reset	—	—	0.5 s
CPE	T26	Wait for TFTP-RSP	10 ms	10 ms	200 ms
BS	T27 as idle timer	Maximum time between unicast grants to CPE when BS believes CPE upstream transmission quality is <i>good enough</i>	CPE Ranging Response Processing Time	—	—
BS	T27 as active timer	Maximum time between unicast grants to CPE when BS believes CPE upstream transmission quality is <i>not good enough</i>	CPE Ranging Response Processing Time	—	—
BS	T28	Time allowed for the BS to complete the transmission of the backup/candidate channel list to its CPEs after initial registration by a new CPE, including the database service query	—	60 s	—

<b>Entity/ Scope</b>	<b>Name</b>	<b>Reference</b>	<b>Min value</b>	<b>Default value</b>	<b>Max value</b>
CPE	CBC Request Retries	Number of retries on CBC Request	3	3	16
	DSx Flow Control	Maximum # of ongoing dynamic service flow (DSx) transactions that are ongoing	1	4	Infinite
	MCA Flow Control	Maximum # of ongoing multicast group assignment (MCA-REQ/RSP) transactions	1	—	Infinite
	Max # of multicast groups	Maximum # of multicast groups the BS supports in a cell	1	—	511
BS, CPE	T30	CPE registration Timer (see 7.7.7.3.4 and 7.14.2.11)	160 ms	40.8 s	10,485.6 s
BS, CPE	ARQ_BSN_MODULUS	Number of unique BSN values	—	2^10	—
BS, CPE	ARQ_WINDOW_SIZE	Max # of un-acknowledged ARQ blocks at a given time	—	—	$\leq (ARQ\_BSN\_MODULUS)/2$
BS, CPE	ARQ_BLOC_K_LIFETIME	Max time interval an ARQ block shall be managed by the Tx ARQ state machine	10 $\mu$ s	—	655.36 ms
BS, CPE	ARQ_RETRY_TIMEOUT (TRANSMITTER_DELAY/RECEIVER_DELAY)	Minimum time interval a transmitter shall wait before retransmission of a unacknowledged block	10 $\mu$ s	—	655.36 ms
BS, CPE	ARQ_SYNC_LOSS_TIMEROUT	Max amount of time ARQ_TX_WINDOW_START or ARQ_RX_WINDOW_START shall be allowed to remain at the same value before declaring a loss of synchronization of the sender and receiver state machines for an ongoing transfer.	10 $\mu$ s	—	655.36 ms
BS, CPE	ARQ_RX_PURGE_TIMEOUT	Time interval the receiver shall wait after successful reception of a block that does not result in advancement of ARQ_RX_WINDOW_START, before advancing ARQ_RX_WINDOW_START	10 $\mu$ s	—	655.36ms
BS, CPE	ARQ_BLOC_K_SIZE	Size of ARQ block that SDU is fragmented into	1 octet	—	2040 octet
BS	Max CPE Transmit EIRP	Maximum CPE Transmit EIRP as negotiated during registration	-64 dBm	—	+63.5 dBm
CPE	Registration Request Retries	Number of retries on registration requests	1	—	3
CPE	Request Retries	Number of retries on bandwidth allocation requests	16	—	—

### 12.1.2 PHY (initialization, operation, and DS/US synchronization)

**Table 273 — PHY parameters, timers, message IEs**

<b>Entity/ Scope</b>	<b>Name</b>	<b>Reference</b>	<b>Min value</b>	<b>Default value</b>	<b>Max value</b>
BS	DCD Interval	Time between transmission of DCD messages	—	—	10 s
BS	UCD Interval	Time between transmission of UCD messages	—	—	10 s
BS	UCD Transition	The time the BS shall wait after repeating a UCD message with an incremented Configuration Change Count before issuing a US-MAP message referring to Upstream_Burst_Profiles defined in that UCD message	2 MAC frames	—	—
BS	DCD Transition	The time the BS shall wait after repeating a DCD message with an incremented Configuration Change Count before issuing a DS-MAP message referring to Downstream_Burst_Profiles defined in that DCD message	2 MAC frames	—	—
BS	Initial Ranging Interval	Time between Initial Ranging opportunities assigned by the BS	—	—	2 s
BS	CLK-CMP Interval	Time between the clock compare measurements used for the generation of CLK-CMP messages	50 ms	50 ms	50 ms
CPE	Lost DS-MAP Interval (T56)	Time since last received DS-MAP message before downstream synchronization is considered lost	—	—	600 ms
CPE	Lost US-MAP Interval (T57)	Time since last received US-MAP message before upstream synchronization is considered lost	—	—	600 ms
CPE	Lost SCH (T58)	Number of SCH that can be lost until synchronization is considered lost	—	—	15
CPE	CDMA Ranging Retries	Number of retries on CDMA Ranging Requests	1	—	4
CPE, BS	Invited Ranging Retries	Number of retries on inviting Ranging Requests	16	—	—
BS	US-MAP Process Time	Time provided between arrival of the last bit of a US-MAP at a CPE and effectiveness of that map	5 symbols	—	—
BS	CPE Ranging Response Processing Time	Time allowed for a CPE following receipt of a ranging response before it is expected to reply to an invited ranging request	10 ms	—	—
CPE	T1	Wait for DCD timeout	—	—	$5 \times$ DCD interval maximum value
CPE	T2	Wait for broadcast ranging timeout	—	—	$5 \times$ ranging interval
CPE	T3	Ranging Response reception timeout following the transmission of a Ranging Request	—	200 ms	200 ms

<b>Entity/ Scope</b>	<b>Name</b>	<b>Reference</b>	<b>Min value</b>	<b>Default value</b>	<b>Max value</b>
CPE	T4	Wait for unicast ranging opportunity. If the pending-until-complete field was used earlier by this CPE, then the value of that field shall be added to this interval.	1 s	30 min (fixed) 10 min. (portable)	30 min
BS	T5	Wait for Upstream Channel Change response	—	—	2 s
CPE	T12	Wait for UCD descriptor	—	—	5 × UCD Interval maximum value
CPE	T20	Time the CPE searches for preambles on a given channel	2 MAC frames	—	—
CPE	T21	Time the CPE searches for DS-MAP on a given channel	—	—	10 s
BS	EIRP <sub>BS</sub>	EIRP of BS (DS)	-64 dBm	—	63.5 dBm
BS	TTG	Transmit/Receive Transition Gap	105 µs	210 µs	333 µs
BS	DIUC Mandatory Exit Threshold	CINR at or below which this DIUC can no longer be used and where change to a more robust DIUC is required.	-64 dB	—	+63.5 dB
BS	DIUC Mandatory Entry Threshold	The minimum CINR required to start using this DIUC when changing from a more robust DIUC is required	-64 dB	—	+63.5 dB
BS	Boosting	Boosting applied to a DS allocation	-12 dB	0 dB	+9 dB
BS, CPE	BW Request Backoff Start	Initial size of BW Request opportunity used by CPEs to contend to send BW requests to BS	0	—	15
BS, CPE	BW Request Backoff End	Final size of BW Request opportunity used by CPEs to contend to send BW requests to BS	1	—	15
BS, CPE	UCS notification Backoff Start	Initial backoff window size in units of UCS notification opportunity used by CPEs to contend to send UCS notifications to BS.	0	—	15
BS, CPE	UCS notification Backoff End	Final size of UCS notification opportunity used by CPEs to contend to send UCS notification to BS	1	—	15
BS, CPE	Contention-based reservation Timeout	Number of US-MAPs to receive before contention-based reservation is attempted again for the same connection	1	—	255
BS, CPE	BW Request opportunity size	Size (in OFDM slots) of PHY bursts, that a CPE may use to format and transmit a bandwidth request message in a contention request opportunity.	1	—	255
BS, CPE	UCS notification request opportunity size	Size (in OFDM slots) of PHY bursts that a CPE may use to transmit a UCS notification.	1	—	255
BS, CPE	# of initial ranging codes	Number of initial ranging CDMA codes (N)	1	—	255
BS, CPE	# of periodic ranging codes	Number of periodic ranging CDMA codes (M)	1	—	255
BS, CPE	# of bandwidth request codes	Number of bandwidth request CDMA codes (L)	1	—	255

<b>Entity/ Scope</b>	<b>Name</b>	<b>Reference</b>	<b>Min value</b>	<b>Default value</b>	<b>Max value</b>
BS, CPE	# of UCS notification codes	Number of UCS notification CDMA codes (I)	1	—	255
BS, CPE	Start of CDMA codes group	Indicates the starting number, S, of the group of codes used for the US	0	See 6.10.3	255
BS, CPE	EIRP Density Level	EIRP Transmitted per subcarrier	-104 dBm	—	+23.5 dBm
BS, CPE	EIRP Control	EIRP per subcarrier that the CPE should apply to correct its current transmission EIRP	-104 dBm	—	+23.5 dBm
BS	EIRP Per subcarrier	EIRP transmitted per subcarrier	-104 dBm	—	+23.5 dBm

### 12.1.3 Coexistence

**Table 274 — Coexistence parameters, timers, message IEs**

<b>Entity/ Scope</b>	<b>Name</b>	<b>Reference</b>	<b>Min value</b>	<b>Default value</b>	<b>Max value</b>
BS	Tse (T33)	Time between transmission of the broadcast message of the operating backup and candidate channel sets for the purpose of spectrum etiquette.	—	—	60 s
BS	T32	Wait for the Frame Contention Response message	1 superframe	—	32 superframes
BS	FCW	Frame Contention Window: number of superframes during which a BS (FC_DST) accumulates the frame contention requests before reacting to it and responding to the FC_SRC's.	0 superframe	—	16 superframes
BS	SCWBackoff Max	Integer denoting the maximum superframes for the SCW backoff window	—	—	—
BS	Frame_Cont ention_Min	Number of frames not available for contention at a BS in a coexistence situation	0	2	8
BS	FCN_range	Exponent in base 2 defining the extent of the range of the random number FCN	4	—	16
BS	SF_release	Number of super-frame after which the BS releases the frames won by another BS through frame contention	—	5	—
CPE	T <sub>CBP</sub> (T34)	The minimum time between transmissions of a CBP packet carrying its MAC address for identification by nearby CPEs and BSs for coexistence purpose, as well as by spectrum monitoring systems to identify potential interference situations. Timing value may depend on the regulatory domain where the WRAN system operates (see Annex A)	8 s	—	15 min
BS	SCWBackoff Timer (T35)	Backoff timer that controls exiting or continuation of Frame contention procedure	—	—	SCWBacko ff_Max

### 12.1.4 Security

**Table 275 — Security parameters, timers, message IEs**

Entity/ Scope	Name	Reference	Min value	Default value	Max value
CPE	EAP Authentication Timer (T36)	Timeout period between sending SCM EAP-Start or EAP-Transfer (8.2.2.5)	2 s	10 s	30 s
CPE	Authentication Grace Timer (T37)	Amount of time after authentication is complete that must pass before reauthentication is complete (8.2.2.5)	5 min (300 s)	10 min (600 s)	35 days (3,024,000 s)
CPE	Max #of Authentication Attempts	Maximum # of Times a CPE is allowed to attempt EAP Authentication (8.2.2.5)	1 s	5 s	10 s
CPE	Operational Wait Timeout (T38)	Timeout period between sending of Key Request messages from the Op Wait state (8.2.3.2.4)	1 s	1 s	10 s
CPE	Rekey Wait Timeout (T39)	Timeout period between sending of Key Request messages from the Rekey Wait state (8.2.3.2.4)	1 s	1 s	10 s
CPE	GTEK/TEK Grace Time (T40)	Time interval, in seconds before the estimated expiration of a GTEK/TEK (8.2.3.2.4)	5 min (300 s)	1 h (3600 s)	3.5 days (302,400 s)
BS	AK Lifetime	Lifetime BS assigns to new AK	1 day (86,400 s)	7 days (604,800 s)	70 days (6,048,000 s)
BS	TEK Lifetime	Lifetime BS assigns to new TEK	30 min (1800 s)	12 h (43,200 s)	7 days (604,800 s)
BS, CPE	SCM Flow Control	The maximum number of concurrent SCM transactions	0 (Default: unlimited # of transactions)	—	255
BS, CPE	Number of Supported security associations	The maximum number of supported security associations	2	—	2+m where m is the number of multicast groups
BS, CPE	PN_WINDOW_SIZE	Window that defines the acceptable PNs for received PDUs that are to be processed by encryption/decryption process	16	—	512
BS	T17	Time allowed for CPE to complete CPE Authorization and Key Exchange	5 min	5 min	—

### 12.1.5 Cognitive radio capabilities (SM, SSA, incumbent protection, QP management )

**Table 276 — Cognitive radio capability parameters, timers, message IEs**

Entity/ Scope	Name	Reference	Min value	Default value	Max value
CPE	T19	Time DS-channel remains unusable	—	—	—
CPE	T29	Wait for BLM-ACK timeout	10 ms	—	300 ms
BS	T31	Wait for BLM-REP timeout	1 MAC Frame	—	—
CPE	BLM-REP Retries	Number of retries allowed for sending BLM-REP	—	3	—
BS, CPE	Channel Availability Check Time	The time during which a channel SHALL be checked for the presence of licensed incumbent signals having a level above the Incumbent Detection Threshold prior to the commencement of WRAN operation in that channel, and in the case of TV, a related channel at an EIRP level that can affect the measured channel.	—	30 s	—
BS, CPE	Non-Occupancy Period	The required period during which WRAN device transmissions SHALL NOT occur in a given channel because of the detected presence of an incumbent signal in that channel above the Incumbent Detection Threshold or, in the case of TV, above a given EIRP level.	10 min	—	—
BS, CPE	Channel Detection Time	The maximum time taken by a WRAN device to detect a licensed incumbent signal above the Incumbent Detection Threshold within a given channel during normal WRAN operation.	—	≤ 2 s to ≥ 90% Probability of Detection with a False Alarm rate of ≤ 10%	—
BS, CPE	Channel Setup Time	The window of time that may be taken by a WRAN CPE to transmit control information to a WRAN base station in order to establish operation with that base station at the prescribed power, or in the case of TV, at or below the allowable EIRP within a given channel.	—	2 s	—
BS, CPE	Channel Opening Transmission Time (Aggregate transmission time)	The aggregate duration of control transmissions by WRAN devices during the Channel Setup Time, which starts at the end of the Channel Availability Check Time.	—	100 ms	—
BS, CPE	Channel Move Time (In-service monitoring)	The time taken by a WRAN system to cease all interfering transmissions on the current channel upon detection of a licensed incumbent signal above the relevant Incumbent Detection Threshold or, in the case TV, to alternatively reduce its EIRP to that which is allowable within a given channel upon detection of a TV signal in the same or a related channel	—	2 s	—
BS, CPE	Channel Closing Transmission	The aggregate duration of control transmissions by the WRAN devices during the Channel Move/EIRP Reduction Time, which starts upon	—	100 ms	—

<b>Entity/ Scope</b>	<b>Name</b>	<b>Reference</b>	<b>Min value</b>	<b>Default value</b>	<b>Max value</b>
	Time (Aggregate transmission time)	detection of a licensed incumbent signal above the relevant Incumbent Detection Threshold			
BS, CPE	Channel Number	The channel number which is to be sensed by the SSF (10.4)	0	—	255
BS, CPE	Channel Bandwidth	The bandwidth of the channel to be sensed by the SSF (10.4)	—	6/7/8 MHz (depending on regulatory domain)	—
BS, CPE	Maximum Probability of false alarm	In sensing modes 0 and 1 this value specifies the maximum probability of false alarm for each sensing mode decision in the signal present array	0.0	—	0.255
BS, CPE	NumSensing Periods	Number of sensing periods field in a Sensing Window Specification Array entry	0	1	127
BS, CPE	SensingPerio dDuration	Duration of sensing period field (in units of OFDM symbols) in a Sensing Window Specification Array entry	0	16	1023
BS, CPE	SensingPerio dInterval	Periodicity of Sensing period field in a Sensing Window Specification Array entry	0	200	2047
BS, CPE	Sensing Window Specification Array	Array containing Sensing Window specification for each signal type enumerated in Signal Type Array	$1 \times \text{sizeof}(\text{NumSensingPeriods+SensingPeriodDuration+SensingPeriodInterval})$	—	$32 \times \text{sizeof}(\text{NumSensingPeriods+SensingPeriodDuration+SensingPeriodInterval})$
BS, CPE	Signal Type Array	Bitmap that indicates which signal types are to be sensed for in a given regulatory domain	—	Set on a regulatory domain- by-domain basis (see <a href="#">Annex A</a> , <a href="#">Table A.11</a> )	—
BS, CPE	Sensing Mode	The sensing mode a CPE supports. Negotiated during CPE initialization. Various modes are described in Table 238.	—	No Sensing	—
BS, CPE	Signal Present Decision	Indication of whether or not a signal of a specific type has been detected. All unused values are reserved	0x00 (Absent)	0x7F (No Decision could be made)	0xFF (Signal Present)
BS, CPE	Confidence Metric	Confidence with which sensing can determine the signal type	0x00 (No Confidence)	—	0xFF (Full confidence)
BS, CPE	Mean RSSI	Mean of M RSSI measurements	-104 dBm	—	+23.5 dBm
BS, CPE	Standard Deviation of RSSI	Standard deviation of the M RSSI measurements	+0.0 dB	—	+25.5 dB
BS, CPE	RSSI_detecti on_threshold	Energy detection threshold indicating the presence of an incumbent, other WRAN system, or interference	-120 dBm	—	-10 dBm
BS, CPE	Microphone protection radius	Radius of the contour within which the WRAN system cannot operate due to potential interference with the microphone	0.1 km	—	100 km

<b>Entity/ Scope</b>	<b>Name</b>	<b>Reference</b>	<b>Min value</b>	<b>Default value</b>	<b>Max value</b>
BS, CPE	T <sub>Candidate_Chann el_Refresh (T41)</sub>	Maximum time interval allowed before sensing is performed on the candidate channel to ensure that no incumbents are detected.	1 s	6 s	10 s
BS, CPE	T <sub>Backup_Channel _Refresh (T42)</sub>	Maximum time interval allowed before sensing is performed on the backup channel to ensure that no incumbents are detected.	1 s	6 s	10 s
BS, CPE	T <sub>Candidate_to_Ba ckup_Transition (T43)</sub>	Minimum time duration without detection of any incumbent for a candidate channel to transition to the backup channel.	1 s	30 s	100 s
BS, CPE	T <sub>Ch_Move (T44)</sub>	Maximum time to ensure that the channel move information is successfully conveyed to all the associated CPEs and BS (self-coexistence mode).	1 s	—	10 s
BS, CPE	T <sub>No_DB (T45)</sub>	Maximum WRAN operation time without access to the incumbent database service	0.1 hr	—	72 hrs
BS	T <sub>Wait_Before_Ch annel_Move (T46)</sub>	Waiting time before which the BS moves to the first backup channel. This is used to make sure that all the CPEs are ready to move to the backup channel before BS switches operation to this backup channel.	1 frame	—	256x16 frames
CPE	T <sub>Wait_Before_Ch annel_Move (T59)</sub>	Waiting time before which the CPE moves to its backup channels if it no longer hears from its BS. This is used to make sure that the CPE waits long enough after its UCS notification so that the BS has had time to move to a backup channel, if it decided to do so.	1 frame	—	256x16 frames
BS, CPE	T <sub>Refresh_Databas e_Info (T47)</sub>	The prescribed time by the WRAN operator to refresh the incumbent database service.	0.1 hr	—	72 hrs
BS, CPE	T <sub>Clear_N (T48)</sub>	Lapser Timer keeps track of whether the Operating Channel N has been cleared using spectrum sensing	0.1 s	—	60 s
BS, CPE	T <sub>Clear_N-1 (T49)</sub>	Lapser Timer keeps track of whether the Adjacent Channel N-1 has been cleared using spectrum sensing	0.1 s	—	60 s
BS, CPE	T <sub>Clear_N+1 (T50)</sub>	Lapser Timer keeps track of whether the Adjacent Channel N+1 has been cleared using spectrum sensing	0.1 s	—	60 s
BS, CPE	T <sub>Loss_of_BS_Con tact (T51)</sub>	Initiated when the CPE loses contact with the BS	1 s	—	600 s
BS, CPE	T <sub>Range1 (T52)</sub>	Used for terrestrial geolocation. Initiated when the downstream burst leaves the BS (i.e., at the start of the frame preamble).	1 TU	—	1000 TU
BS, CPE	T <sub>INsens (T53)</sub>	The parameter T <sub>INsens</sub> is used to verify that in-band sensing has been done within the required In-service monitoring period. The T <sub>INsens</sub> parameter is driven by the regulatory domain requirements. See Annex A.	0.1 s	—	60 s
BS, CPE	T <sub>OUTsens (T54)</sub>	The parameter T <sub>OUTsens</sub> is used to verify that out-of-band sensing has been done within the required “Acquiring a channel monitoring period” specified in Table A.13 (30 s in the US). This value would be used to either initialize a “lapse timer” for each channel in the backup/candidate list at each CPE so that it is compared to T <sub>sens</sub>	0.1 s	—	60 s
BS, CPE	T <sub>sensin (T55)</sub>	T <sub>sensin</sub> parameter corresponds to the maximum length of time required to carry out the sensing	1 ms	—	160 ms

Entity/ Scope	Name	Reference	Min value	Default value	Max value
		process on an in-band channel (N, N-1, or N+1). Manufacturers need to specify the sensing time required to detect the specified signals with required accuracy (see Figure 176).			
CPE	T <sub>sensout</sub> (T60)	T <sub>sensout</sub> parameter corresponds to the maximum length of time required to carry out an out-of-band sensing process for a specified channel N (i.e., N, N-1, and N+1). Manufacturers need to specify the sensing time required to detect the specified signals out-of-band with required accuracy (see Figure 178).	20 ms		160 ms
BS, CPE	ISO 3166 Country Code	3 character, ASCII string denoting the regulatory domain of operation (e.g., “USA” is for United States of America)	—	3 characters	—
BS, CPE	TA <sub>CBP</sub>	Timing Advance of the CBP burst (see step 2 of 10.5.2.3). Note that the geolocation process will have to pre-adjust TA <sub>CBP</sub> depending on the distance between the two CPE to be geolocated and the reference CPEs so that the delays measured by Vernier <sub>3</sub> fall within the symbol cyclic prefix (e.g., 74.68 μs corresponding to 22.4 km).	-1024 TU	—	+1024 TU

## 12.2 Well-known CIDs

Connections assigned to CPEs and multicast groups in an IEEE 802.22 network are identified by two items, the station ID (SID) and flow ID (FID). A connection identifier (CID) can be constructed from the tuple of SID and FID (CID = SID | FID). The SID makes up the 9 MSB of the CID, while the FID makes up the 3 LSB of the CID. Figure 186 shows the relationship between SIDs and FIDs, with respect to CIDs.

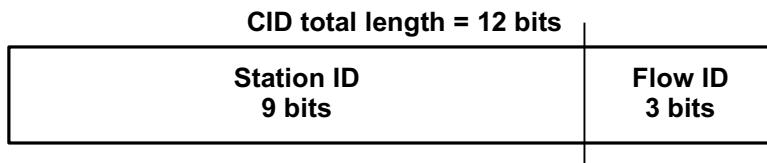


Figure 186 — Relationship between CID, SID, and FID

CPEs operating under a particular BS are uniquely identified by a Station Identifier (SID). The SID is a 9-bit value, allowing for a maximum of up to 512 stations operating under the control of a BS. The number of unicast stations (e.g., individual CPEs) and multicast stations (e.g., multicast groups) is controlled by the operator. A SID is reserved for IEEE 802.22 broadcast and initial ranging communications. SIDs are shall be handled as described in Table 277.

**Table 277 — Station ID allocation**

<b>SID</b>	<b>Value</b>	<b>Description</b>
Cell	0x000	Cell-wide SID reserved for broadcast and initial ranging
Unicast	0x001 – m	SID for individual CPEs
Multicast	m+1 – 0x200	SID for multicast groups

Traffic flows for a station are identified by the flow ID (FID). The FID is a 3-bit value, allowing for a maximum of up to 8 flows assigned to a particular SID. Table 278 to Table 280 show how FIDs shall be used for the Cell, Unicast, and Multicast SIDs.

**Table 278 — Flow ID allocation for Cell SID**

<b>FID</b>	<b>Value</b>	<b>Description</b>
Broadcast	000	Traffic on broadcast connection mapped to the Broadcast Flow assigned to Cell SID
Initial Ranging	001	Traffic on initial ranging connection mapped to the Initial Ranging Flow assigned to Cell SID
<i>Reserved</i>	010–111	<i>Reserved for future use</i>

**Table 279 — Flow ID allocation for Unicast SID**

<b>FID</b>	<b>Value</b>	<b>Description</b>
Basic	000	Traffic on basic connection mapped to the Basic Flow assigned to CPE
Primary Management	001	Traffic on primary management connection mapped to Primary Management Flow assigned to CPE
BE	010	Data sent on unicast transport connection using the BE scheduling class mapped to BE Flow
nrtPS	011	Data sent on unicast transport connection using the nrtPS scheduling class mapped to nrtPS Flow
rtPS	100	Data sent on unicast transport connection using the rtPS scheduling class mapped to the rtPS Flow
UGS	101	Data sent on unicast transport connection using the UGS scheduling class mapped to the UGS Flow
<i>Reserved</i>	110	<i>Flow ID reserved for future use</i>
Secondary Management	111	Traffic on secondary management connection mapped to Secondary Management Flow assigned to CPE

**Table 280 — Station ID allocation**

<b>FID</b>	<b>Value</b>	<b>Description</b>
Multicast Polling	000	Traffic on multicast bandwidth request polling sent on the Multicast Polling Flow assigned to multicast SID (group)
Multicast Management	001	Traffic on multicast management sent on the Multicast Management Flow assigned to multicast SID (group)
BE	010	Data sent on multicast transport connection using the BE scheduling class mapped to BE Flow assigned to multicast SID (group)
nrtPS	011	Data sent on multicast transport connection using the nrtPS scheduling class mapped to nrtPS Flow assigned to multicast SID (group)
rtPS	100	Data sent on multicast transport connection using the rtPS scheduling class mapped to the rtPS Flow assigned to multicast SID (group)
UGS	101	Data sent on multicast transport connection using the UGS scheduling class mapped to the UGS Flow assigned to

FID	Value	Description
		multicast SID (group)
<i>Reserved</i>	110–111	<i>Flow ID reserved for future use</i>

From Figure 186 and Table 277 to Table 280 it is possible to construct CIDs for various system connections. The following is an example list of system connections and how they are constructed from SIDs and FIDs.

- Basic CID = Unicast SID | Basic FID
- Broadcast CID = Cell SID | Broadcast FID
- Initial Ranging CID = Cell SID | Initial Ranging FID
- Unicast Transport CID using UGS = Unicast SID | UGS FID
- Multicast manage CID = Multicast SID | Multicast Management FID

This approach to CID management is taken to allow for a reduction of overhead by signaling just the SID in the DS/US-MAP allocation for a station, then identifying particular connections by the FID that is then carried in the GMH of individual MAC PDUs within a station’s allocation.

### 12.3 ARQ parameters

**Table 281 — ARQ parameters**

Entity	Name	Description	Length (octets)	Value
BS, CPE	ARQ_BSN_MODULUS	7.9.3.1	2	$2^{10}$
BS, CPE	ARQ_WINDOW_SIZE	7.9.3.2	2	See Table 92, 7.7.8.9.17.2
BS, CPE	ARQ_BLOCK_LIFETIME	7.9.3.3	2	See Table 94, 7.7.8.9.17.4
BS, CPE	ARQ_RETRY_TIMEOUT	7.9.3.4	2	See Table 93, 7.7.8.9.17.3
BS, CPE	ARQ_SYNC_LOSS_TIMEOUT	7.9.3.5	2	See Table 95, 7.7.8.9.17.5
BS, CPE	ARQ_PURGE_TIMEOUT	7.9.3.6	2	See Table 97, Table 97
BS, CPE	ARQ_BLOCK_SIZE	7.9.3.7	2	See Table 98, 7.7.8.9.17.8

## 13. MIB structure

The definition of managed objects in this standard is expressed in Structure of Management Information Version 2 (SMIV2). It supports a management protocol agnostic approach, including SNMP.

The basic MIB objects are the following:

- wranDevMib: Basic MIB for BS/CPE device management. Can be used to track software versioning of BS/CPE HW/SW and what SNMP traps can be configured on those devices
- wranIfBsMib: Basic MIB for BS-related MIB objects related to providing fixed AND portable service.
- wranIfBsSfMgmt: Basic MIB for managing items related to Service Flow configuration, instantiation, and management
- wranIfCpeMib: Basic MIB for CPE-related MIB objects related to operation of fixed AND portable CPEs
- wranIfSmMib: Basic MIB for SM related MIB objects
- wranIfSsaMib: Basic MIB for Spectrum Automaton related MIB objects
- wranIfDatabaseServiceMib: Basic MIB for Database Service access related MIB objects

### 13.1 MIB description

#### 13.1.1 wranDevMib

wranDevMib details objects that will be managed by the SNMP agent in the BS and CPE. This MIB element is broken down into the following MIB groups:

- wranDevBsObjects: MIB objects to be implemented by the SNMP agent in BS
- wranDevCpeObjects: MIB objects to be implemented by the SNMP agent in CPE
- wranDevCommonObjects: MIB objects to be implemented by the SNMP agent in BS/CPE
- wranDevMibConformance: MIB objects related to conformance

##### 13.1.1.1 wranDevBsObjects

wranDevBsObjects is broken down into the following two items:

- wranDevBsSoftwareUpgradeTable: contains objects related to BS SW upgrade
- wranDevBsNotification: managed objects related to SNMP traps on BS

###### 13.1.1.1.1 wranDevBsSoftwareUpgradeTable

This table defines objects associated with BS software configuration. It may have one or more entry, although only one software configuration shall be active at any given time. Each entry is defined by a compound attribute, wranDevBsSoftwareUpgradeEntry.

### **13.1.1.1.1.1 wranDevBsSoftwareUpgradeEntry**

Each entry in the wranDevBsSoftwareUpgradeTable is made up of the following items:

#### **13.1.1.1.1.1.1 wranDevBsDeviceIndex**

Index of entry in the table.

#### **13.1.1.1.1.1.2 wranDevBsVendorId**

This value identifies the managed BS vendor to which SW upgrade was applied.

#### **13.1.1.1.1.1.3 wranDevBsHwId**

Version of HW to which SW upgrade is applied.

#### **13.1.1.1.1.1.4 wranDevBsCurrentSwVersion**

Version of SW currently running on the BS. This value is set by the vendor specified by the Vendor ID. The SW version and HW ID (wranDevBsHwId) should be a unique tuple. After the downloaded software is activated, the value in this object shall be replaced with the version in wranDevBsDownloadSwVersion.

#### **13.1.1.1.1.1.5 wranDevBsDownloadSwVersion**

Version of the SW to be downloaded. This value is set by the vendor specified by the Vendor ID. The SW version and HW ID (wranDevBsHwId) should be a unique tuple. This should be initialized before software is downloaded or activated.

#### **13.1.1.1.1.1.6 wranDevBsUpgradeFileName**

Fully qualified path name that points to the location of SW version that is to be downloaded/activated.

#### **13.1.1.1.1.1.7 wranDevBsSoftwareUpgradeAdminState**

This value can take on two states. When set to *Download*, the software listed by wranDevBsDownloadSwVersion will be downloaded. When set to *Activate*, the software recently downloaded will be activated. The *Download* and *Activate* procedures are vendor specific operations that are not defined in this standard.

#### **13.1.1.1.1.1.8 wranDevBsDowloadSwProgress**

This value shows the progress of the SW download highlighted by wranDevBsDownloadSwVersion, encoded as the percentage of the download successfully completed.

### **13.1.1.1.1.9 wranDevBsSoftwareUpgradeTimeStamp**

This value is a timestamp to indicate when the last SW downloads or activation took place.

### **13.1.1.1.2 wranDevBsNotification**

This group of objects relates to SNMP traps on the BS. There is a control element that enables/disables the traps and whether or not a trap is sent when an event is logged.

#### **13.1.1.1.2.1 wranDevBsTrapControl**

Defines control elements for traps.

##### **13.1.1.1.2.1.1 wranDevBsTrapPrefix**

This object groups all of the notification objects for the BS. It is defined to be compatible with SNMPv1, following Section 8.5 and 8.6 of IETF RFC 2758.

##### **13.1.1.1.2.1.2 wranDevBsTrapControlRegister**

This is a 2-bit bitmap that enables the two BS traps that are available:

wranDevBsEventTrapControl, wranDevBsLogBuffExceedThresholdTrapControl.

##### **13.1.1.1.2.2 wranDevBsEventTrapControl**

This trap is sent when an event is logged into the event table, wranDevCmnEventTable.

##### **13.1.1.1.2.2.1 wranDevBsLogBuffExceedThresholdTrap**

This trap is sent when the size of the event log buffer is greater than the configured threshold.

### **13.1.1.2 wranDevCpeObjects**

wranDevCpeObjects are broken down into the following elements:

- wranDevCpeConfigFileEncodingTable: Related to configuration information about the CPE
- wranDevCpeNotification: Related to SNMP traps that are particular to the CPE

#### **13.1.1.2.1 wranDevCpeConfigFileEncodingTable**

This table defines objects associated with CPE software configuration. This table may only have one entry, defined by a compound attribute, wranDevCpeConfigFileEncodingEntry.

### **13.1.1.2.1.1.1 wranDevCpeConfigFileEncodingEntry**

The single entry in the `wranDevCpeConfigFileEncodingTable` is made up of the following items:

#### **13.1.1.2.1.1.1.1 wranDevCpeDeviceIndex**

Index of entry in the table, defaults to 0.

#### **13.1.1.2.1.1.1.2 wranDevCpeMicConfigSetting**

This value contains the MIC (Message Integrity Code) calculated for the CPE configuration file.

#### **13.1.1.2.1.1.1.3 wranDevCpeVendorId**

This value identifies the vendor of the managed CPE to which a configuration file upgrade is to be applied.

#### **13.1.1.2.1.1.1.4 wranDevCpeHwId**

This value identifies the hardware version of the CPE which the configuration file upgrade is to be applied.

#### **13.1.1.2.1.1.1.5 wranDevCpeConfigFileVersion**

Version of the configuration file to be downloaded. This value is set by the vendor specified by the Vendor ID. The SW version and HW ID (`wranDevCpeHwId`) should be a unique tuple. This should be initialized before software is downloaded or activated.

#### **13.1.1.2.1.1.1.6 wranDevCpeUpgradeFileName**

Fully qualified path name that points to the location of configuration file that is to be downloaded.

#### **13.1.1.2.1.1.1.7 wranDevCpeSwTftpServer**

IP address of the TFTP server on which the new configuration file resides.

#### **13.1.1.2.1.1.1.8 wranDevCpeTftpServerTimeStamp**

The time the configuration file was sent in seconds, as defined by IETF RFC 868.

### **13.1.1.2.2 wranDevCpeNotification**

This group of objects relates to SNMP traps on the BS. There is a control element that enables/disables the traps and whether or not a trap is sent when an event is logged.

### **13.1.1.2.2.1 wranDevCpeTrapControl**

Defines control elements for traps.

#### **13.1.1.2.2.1.1 wranDevCpeTrapPrefix**

This object groups all of the notification objects for the BS. It is defined to be compatible with SNMPv1, following Section 8.5 and 8.6 of IETF RFC 2758.

#### **13.1.1.2.2.1.2 wranDevCpeTrapControlRegister**

This is a 2-bit, bitmap that enables the two BS traps that are available:  
`wranDevCpeEventTrapControl`, `wranDevBsLogBuffExceedThresholdTrapControl`.

#### **13.1.1.2.2.2 wranDevCpeEventTrapControl**

This trap is sent when an event is logged into the event table, `wranDevCmnEventTable`.

#### **13.1.1.2.2.2.1 wranDevBsLogBuffExceedThresholdTrap**

This trap is sent when the size of the event log buffer is greater than the configured threshold.

### **13.1.1.3 wranDevCommonObjects**

This object contains the following managed elements that are common to CPE and BS:

- `wranDevCmnEventLog`: Contains managed objects related to the Event Log
- `wranDevCmnSnmpAgent`: Contains managed objects related to SNMP agent configuration
- `wranDevCmnDeviceConfig`: Contains common managed objects related to device configuration

#### **13.1.1.3.1 wranDevCmnEventLog**

Event Log is a compound attribute made up of the following:

- `wranDevCmnEventLogConfigTable`: Configuration of parameters for Event Log operation
- `wranDevCmnEventTable`: Defines events that are supported by the CPE and BS
- `wranDevCmnEventLogTable`: Used to store local Events that shall reside in non-volatile memory

#### **13.1.1.3.1.1 wranDevCmnEventLogConfigTable**

Each entry stores the Event Log configuration for a device. Each entry is defined as `wranDevCmnEventLogConfigEntry`.

**13.1.1.3.1.1.1 wranDevCmnEventLogConfigEntry**

This object is a compound object that Event Log configuration for a particular device, indicated by wranDevCmnDeviceIndex.

**13.1.1.3.1.1.2 wranDevCmnDeviceIndex**

Index value that identifies a BS or CPE entry in the wranDevCmnEventLogConfigTable.

**13.1.1.3.1.1.3 wranDevCmnEventLogEntryLimit**

Maximum number of entries in wranDevCmnEventLogConfigTable. If this value is changed while entries exist in the wranDevCmnEventLogTable, old entries will be discarded until limit is reached.

**13.1.1.3.1.1.4 wranDevCmnEventLogLifeTimeLimit**

A value of 0 means that an entry is kept indefinitely. Any other value, it is the maximum time an entry can exist in wranDevCmnEventLogTable. If this value is changed while entries exist in wranDevCmnEventLogTable, entries older than this limit will be discarded.

**13.1.1.3.1.1.5 wranDevCmnEventLogEntryLimitPerEventId**

The number of log entries that can be logged per event.

**13.1.1.3.1.1.6 wranDevCmnEventLogSeverityThreshold**

Minimum severity level of an event that can be logged into the Event Log.

**13.1.1.3.1.1.7 wranDevCmnEventLogWrapAroundBuffEnable**

Indication of whether or not the Event Log can wrap around when full or is emptied when full.

**13.1.1.3.1.1.8 wranDevCmnEventLogLatestEvent**

Index of latest event in Event Log.

**13.1.1.3.1.1.9 wranDevCmnEventLogPersistenceSupported**

Indication of whether or not Event Log is to persist through power cycle or reset of device.

**13.1.1.3.1.1.10 wranDevCmnEventLogResidualBuffThreshold**

Threshold ratio of used capacity for Event Log to total capacity of Event Log, that when reached a TRAP is issued.

### **13.1.1.3.1.2 wranDevCmnEventTable**

This compound object defines the types of events that are supported by a BS or CPE. Each event is defined by wranDevCmnEventEntry.

#### **13.1.1.3.1.2.1 wranDevCmnEventEntry**

This object defines the parameters of an event entry into the wranDevCmnEventTable. Each entry is indexed by wranDevCmnDeviceIndex and wranDevCmnEventIdentifier.

##### **13.1.1.3.1.2.1.1 wranDevCmnEventIdentifier**

Event Identifier encoded as a numeric value.

##### **13.1.1.3.1.2.1.2 wranDevCmnEventDescription**

Description of the event in the form of a SnmpAdminString.

##### **13.1.1.3.1.2.1.3 wranDevCmnEventSeverity**

The severity of the event as assigned by the device. The Severity assigned to an event is configurable by the system.

##### **13.1.1.3.1.2.1.4 wranDevCmnEventNotification**

Notification will be made when event occurs.

##### **13.1.1.3.1.2.1.5 wranDevCmnEventNotificationOid**

This is the object identifier of a notification object. If wranDevCmnEventNotification is true, a trap identified by the OID will be reported.

### **13.1.1.3.1.3 wranDevCmnEventLogTable**

This is the log table that stores local events as they happen. This table shall reside in non-volatile memory that may persist after power cycle or reset of the device. The maximum number of entries in this table is determined by the wranDevCmnEventLogEntryLimit. If it is setup as a wrap-around log, then the oldest entry will be removed to make room for the newest entry. If it is not setup as a wrap-around log, then the log will be flushed. Multiple entries are stored in the table. Each entry is defined by wranDevCmnEventLogEntry.

### **13.1.1.3.1.3.1 wranDevCmnEventEntry**

Each entry in the Event Log table is made up of several parameters.

#### **13.1.1.3.1.3.1.1 wranDevCmnEventId**

A counter used to index entries in the Event Log. When it reaches the maximum value, it will either wrap-around if configured to wrap-around or the log will be flushed if it is not configured to wrap-around.

#### **13.1.1.3.1.3.1.2 wranDevCmnEventLoggedTime**

The time that the entry was placed into the Event Log. If this event happened just before the last initialization of the management system, then this value is set to 0.

#### **13.1.1.3.1.3.1.3 wranDevCmnEventLogDescription**

The Description of the event.

#### **13.1.1.3.1.3.1.4 wranDevCmnEventLogSeverity**

The severity of the recorded event.

### **13.1.1.3.2 wranDevCmnSnmpAgent**

This compound object deals with the common objects related to SNMP agent configuration.

#### **13.1.1.3.2.1 wranDevCmnSnmpV1V2TrapDestTable**

This compound object deals with the configuration items of the SNMP agent. Each configuration item is represented by a wranDevCmnSnmpV1V2TrapDestEntry.

#### **13.1.1.3.2.1.1 wranDevCmnSnmpV1V2TrapDestEntry**

This compound object contains the parameters that identify the destination of an SNMP trap.

#### **13.1.1.3.2.1.1.1 wranDevCmnSnmpV1V2TrapDestIndex**

Identifies the trap in the table. This parameter shall have a maximum value of 8.

#### **13.1.1.3.2.1.1.2 wranDevCmnSnmpV1V2TrapDestIpAddrType**

Type of IP address stored in wranDevCmnSnmpV1V2TrapDestIpAddr.

### **13.1.1.3.2.1.1.3 wranDevCmnSntpV1V2TrapDestIpAddr**

SNMP manager's IP address that is configured as a destination for traps.

### **13.1.1.3.2.1.1.4 wranDevCmnSntpV1V2TrapDestPort**

Port number of SNMP manager application configured as a trap destination.

### **13.1.1.3.2.1.1.5 wranDevCmnSntpV1V2TrapDestRowStatus**

This object is used to make sure that any write operation to multiple columns is treated as an atomic operation.

## **13.1.1.3.3 wranDevCmnDeviceConfig**

This compound attribute contains the following:

- wranDevCmnResetDevice: Object that is used to reset the device
- wranDevMibConformance: MIB objects that are required for conformance

### **13.1.1.3.3.1 wranDevCmnResetDevice**

There are two actions defined for the object. When set to *actionResetDeviceNoAction*, no action is taken. When set to *actionResetDevice*, the device will reset itself.

### **13.1.1.3.3.2 wranDevMibConformance**

This object helps define which MIB groups are necessary to meet conformance and what MIB objects are part of each group.

#### **13.1.1.3.3.2.1 wranDevMibBsGroup**

This MIB group is mandatory. It is made up of wranDevBsTrapControlRegister.

#### **13.1.1.3.3.2.2 wranDevMibBsSwUpgradeGroup**

This MIB group is optional. It is a compound object made up of the following:

wranDevBsVendorId, wranDevBsHwId, wranDevBsCurrentSwVersion,  
wranDevBsDownloadSwVersion, wranDevBsUpgradeFileName,  
wranDevBsSoftwareUpgradeAdminState, wranDevBsDownloadSwProgress,  
wranDevBsSoftwareUpgradeTimeStamp.

It contains the values of the most recent/current entry in wranDevBsSoftwareUpgradeTable.

#### **13.1.1.3.3.2.3 wranDevMibCpeGroup**

This MIB group is mandatory. It is a compound object made up of the following:  
wranDevCpeMicConfigSetting, wranDevBsVendorId, wranDevCpeHwId,  
wranDevCpeSwVersion, wranDevCpeUpgradeFileName, wranDevCpeSwTftpServer,  
wranDevCpeTftpServerTimeStamp, wranDevCpeTrapControlRegister.  
It contains the values of the most recent/current entry in wranDevCpeConfigFileEncodingTable  
for a particular CPE.

#### **13.1.1.3.3.2.4 wranDevMibCmnGroup**

This MIB group is mandatory. It is a compound object made up of the following:  
wranDevCmnSnmpV1V2TrapDestIpAddrType, wranDevCmnSnmpV1V2TrapDestIpAddr,  
wranDevCmnSnmpV1V2TrapDestPort, wranDevCmnSnmpV1V2TrapDestRowStatus,  
wranDevCmnResetDevice, wranDevCmnDeviceIndex,  
wranDevCmnEventLogEntryLimit, wranDevCmnEventLogLifeTimeLimit,  
wranDevCmnEventLogEntryLimitPerEventId,  
wranDevCmnEventLogSeverityThreshold,  
wranDevCmnEventLogWrapAroundBuffEnable, wranDevCmnEventLogLatestEvent,  
wranDevCmnEventLogPersistenceSupported,  
wranDevCmnEventLogResidualBuffThreshold, wranDevCmnEventDescription,  
wranDevCmnEventSeverity, wranDevCmnEventNotification,  
wranDevCmnEventNotificationOid, wranDevCmnEventId,  
wranDevCmnEventLoggedTime, wranDevCmnEventLogDescription,  
wranDevCmnEventLogSeverity.  
It contains the values of the most recent/current entry in wranDevCmnSnmpV1V2TrapDestTable and  
wranDevCmnEventLogTable.

#### **13.1.1.3.3.2.5 wranDevMibBsNotificationGroup**

This MIB group is optional. It is a compound object that contains wranDevBsEventTrap,  
wranDevBsLogBuffExceedThresholdTrap.

#### **13.1.1.3.3.2.6 wranDevMibCpeNotificationGroup**

This MIB group is optional. It is a compound object that contains wranDevCpeEventTrap,  
wranDevCpeLogBuffExceedThresholdTrap.

### **13.1.2 wranIfBsMib**

This MIB represent core MIB functionality that all base stations shall support. It is based on the FCAPS reference model, which is comprised of MIBs relating to management of the following items: *Fault*, *Configuration*, *Accounting*, *Performance*, and *Security*. The following list defines MIBs that compose wranIfBsMib:

- wranIfBsFm: Fault management
- wranIfBsCm: Configuration management
- wranIfBsAm: Accounting management

- `wranIfBsPm`: Performance management/measurement
- `wranIfBsScm`: Security management

### **13.1.2.1 `wranIfBsFm`**

Exceptions and fault events can be reported by using the traps defined in this MIB. `wranIfBsFm` is made up of the following MIBs: `wranIfBsTrapControlRegister`, `wranIfBsCpeNotificationObjectsTable`, and `wranIfBsThresholdConfigTable`.

#### **13.1.2.1.1 `wranIfBsTrapControlRegister`**

This MIB is a bitmap that is used to disable/enable the following BS:

`traps:wranIfBsCpeDynamicServiceFailNotification`,  
`wranIfBsCpeRssiStatusChangeNotification`,  
`wranIfBsCpeEIRPStatusChangeNotification`,  
`wranIfBsCpeRegisterNotification`, `wranIfBsCpeScmFailNotification`,  
`wranIfBsCpeStartupStatusChangeNotification`, `wranIfBsThroughputMetricsNotification`,  
`wranIfBsNetworkEntryMetricsNotification`,  
`wranIfBsPacketErrorRateChangeNotification`,  
`wranIfBsUserMetricsChangeNotification`,  
`wranIfBsCoexistenceStatusNotification`,  
`wranIfBsCpeCbpReceptionNotification`,  
`wranIfBsCpeWiMicBeaconMSF1Notification`,  
`wranIfBsCpeWiMicBeaconMSF12Notification`,  
`wranIfBsCpeWiMicBeaconMSF123Notification`,  
`wranIfBsInterFrameSensingStatusNotification`,  
`wranIfBsMeasurementStatusNotification`.  
 Enable of a trap indicates that the trap will be recorded in  
`wranIfBsCpeNotificationObjectsTable`.

#### **13.1.2.1.2 `wranIfBsCpeNotificationObjectsTable`**

This table contains objects that represent notifications reported in CPE fault traps. The table is made up of one more entries.

##### **13.1.2.1.2.1 `wranIfBsCpeNotificationObjectsEntry`**

This MIB is a compound object that represents an entry in the MIB object `wranIfBsCpeNotificationsObjectsTable`.

###### **13.1.2.1.2.1.1 `wranIfBsCpeNotificationMacAddr`**

The MAC address of the CPE reporting the notification.

###### **13.1.2.1.2.1.2 `wranIfBsCpeStartupStatusChange`**

This object that is used to indicate the status of a CPE as it proceeds through the network entry and initialization procedures.

### **13.1.2.1.2.1.3 wranIfBsDynamicServiceFailTrap**

This object indicates the reason for failure if a dynamic service flow command failed and the SFID of that service flow.

### **13.1.2.1.2.1.4 wranIfBsCpeRssiStatus**

This object is an indication of what type of RSSI alarm (see 13.1.2.1.3) has recently been triggered.

### **13.1.2.1.2.1.5 wranIfBsCpeEirpStatus**

This object is an indication of what type of EIRP alarm (see 13.1.2.1.3) has recently been triggered.

### **13.1.2.1.2.1.6 wranIfBsCpeRegisterStatus**

This object is an indication of the status of CPE registration.

### **13.1.2.1.2.1.7 wranIfBsCpeScmFail**

This object contains the status of the CPE registration.

### **13.1.2.1.2.1.8 wranIfBsPacketErrorRateChange**

The recent change in Packet Error rate metrics.

### **13.1.2.1.2.1.9 wranIfBsUserMetricsChange**

The recent change in User metrics.

### **13.1.2.1.2.1.10 wranIfBsCoexistenceStatus**

Indication when cell moves between normal operation and coexistence operation.

### **13.1.2.1.2.1.11 wranIfBsCpeCbpReception**

This object would contain the contents of a recently received and decoded CBP.

### **13.1.2.1.2.1.12 wranIfBsCpeWiMicBeaconMSF1**

This object would contain the contents of a recently received and decoded MSF1 of a wireless microphone beacon.

### **13.1.2.1.2.1.13 wranIfBsCpeWiMicBeaconMSF12**

This object would contain the contents of a recently received and decoded MSF1+MSF2 of a wireless microphone beacon.

### **13.1.2.1.2.1.14 wranIfBsCpeWiMicBeaconMSF123**

This object would contain the contents of a recently received and decoded MSF1+MSF2+MSF3 of a wireless microphone beacon.

### **13.1.2.1.2.1.15 wranIfBsMeasurementStatus**

Indication when sensing measurement report has been received.

### **13.1.2.1.2.1.16 wranIfBsInterFrameSensingStatus**

Indication when Inter-frame sensing configuration has been changed.

### **13.1.2.1.2.1.17 wranIfBsIntraFrameSensingStatus**

Indication when Intra-frame sensing configuration has been changed.

## **13.1.2.1.3 wranIfBsThresholdConfigTable**

This MIB provides a table that allows the setting to thresholds that can be used to detect the crossing of RSSI and EIRP thresholds. Each table is made up of entries for low and high thresholds for RSSI and EIRP.

### **13.1.2.1.3.1 wranIfBsThresholdConfigEntry**

This MIB provides entries into the wranIfBsThresholdConfigTable.

#### **13.1.2.1.3.1.1 wranIfBsRssiLowThreshold**

Low threshold for generating an RSSI alarm.

#### **13.1.2.1.3.1.2 wranIfBsRssiHighThreshold**

High threshold for generating an RSSI alarm.

#### **13.1.2.1.3.1.3 wranIfBsEirpLowThreshold**

Low threshold for generating an EIRP alarm.

### **13.1.2.1.3.1.4 wranIfBsEirpHighThreshold**

High threshold for generating an EIRP alarm.

### **13.1.2.2 wranIfBsCm**

This MIB contains various objects related to Configuration Management.

#### **13.1.2.2.1 wranIfBsCpeRngCapabilityReqTable**

This object provides a table containing the ranging configuration requested by the CPE in the RNG-REQ during network entry. Each table is made up of multiple entries, one for each CPE that has sent a RNG-REQ, which is defined by wranIfBsCpeRngCapabilityReqEntry.

##### **13.1.2.2.1.1 wranIfBsCpeRngCapabilityReqEntry**

This object is a compound object that contains the ranging parameters transmitted in RNG-REQ by the CPE during network entry.

###### **13.1.2.2.1.1.1 wranIfBsCpeMacAddress**

The MAC address of the CPE that has attempted ranging with the BS.

###### **13.1.2.2.1.1.2 wranIfMmpPn**

Current value of MMP\_PN that CPE is using if authenticated ranging (see 8.2.4.6.1.2) is used.

###### **13.1.2.2.1.1.3 wranIfCiphertextIcv**

Calculated value of Ciphertext ICV, calculated over RNG-REQ is authenticated ranging (see 8.2.4.6.1.2).

###### **13.1.2.2.1.1.4 wranIfRngAnomaly**

Indication of any error condition detected by CPE during ranging process.

#### **13.1.2.2.2 wranIfBsCpeRngCapabilityCmdTable**

This object provides a table containing the ranging configuration the BS is specifying for CPE in the RNG-CMD during network entry. Each table is made up of multiple entries, one for each CPE that a RNG-CMD is sent to, that are defined by wranIfBsCpeRngCapabilityRspEntry.

### **13.1.2.2.2.1 wranIfBsCpeRngCapabilityCmdEntry**

This object is a compound object that contains the ranging parameters selected for the CPE by the BS and transmitted in RNG-CMD by the BS to CPE during network entry.

#### **13.1.2.2.2.1.1 wranIfBsCpeMacAddress**

MAC Address of CPE that the RNG-CMD is sent to. This is used to fill in MAC Address field of RNG-CMD, when RNG-CMD is sent in response to initial ranging.

#### **13.1.2.2.2.1.2 wranIfBsCpeStationId**

Station ID of CPE that RNG-CMD is sent to. This is used to fill in MAC Address field of RNG-CMD, when RNG-CMD is sent in response to initial ranging.

#### **13.1.2.2.2.1.3 wranIfTimingAdvance**

Timing advance parameter to Table 44.

#### **13.1.2.2.2.1.4 wranIfEirpPerSubcarrier**

EIRP per transmitted subcarrier parameter for the RNG-CMD in Table 44.

#### **13.1.2.2.2.1.5 wranIfOffsetFreqAdjust**

Offset frequency adjustment parameter of RNG-CMD in Table 44.

#### **13.1.2.2.2.1.6 wranIfRangingStatus**

Ranging status field of the RNG-CMD in Table 44.

#### **13.1.2.2.2.1.7 wranIfActionSuperFrameNum**

The Action Superframe Number field of the RNG-CMD in Table 44.

#### **13.1.2.2.2.1.8 wranIfCdmaCode**

The CDMA Code field of the RNG-CMD in Table 44.

#### **13.1.2.2.2.1.9 wranIfTxOpportunityOffset**

The Transmission Opportunity Offset field of the RNG-CMD in Table 44.

### **13.1.2.2.3 wranIfBsCpeBasicCapabilityReqTable**

This object provides a table containing the basic capability information of CPEs that have requested configuration from the BS in the CBC-REQ. Each table is made up of multiple entries, one for each CPE that has transmitted the CBC-REQ, that are defined by `wranIfBsCpeBasicCapabilityReqEntry`.

#### **13.1.2.2.3.1 wranIfBsCPEBasicCapabilityReqEntry**

This object is a compound object that contains the requested configuration of basic capabilities by a CPE during network entry.

##### **13.1.2.2.3.1.1 wranIfBsCpeBasicCapabilityReqEntryIndex**

A unique index for the entry in this table.

##### **13.1.2.2.3.1.2 wranIfBsCpeBasicCapabilityReqNumAttempts**

The current number of attempts that a CPE has attempted basic capability configuration during network entry. This item gets set to 0 upon successful completion of registration process and a CPE is admitted into the network. This item gets incremented every time a CPE attempts basic capability configuration, but is unsuccessful. If this value reaches the limit set by `wranIfBsMaxNumCbcReqAttempts`, then BS shall re-attempt network entry.

##### **13.1.2.2.3.1.3 wranIfBsCpeMacAddress**

The MAC address of the CPE attempting basic capability configuration.

##### **13.1.2.2.3.1.4 wranIfBsCpeStationId**

The Station ID of the CPE attempting basic capability configuration.

##### **13.1.2.2.3.1.5 wranIfMacPduTxandConstruction**

An integer value that indicates the methods for transmission and construction of MAC PDUs that the CPE supports. This reflects the setting of the IE defined in 7.7.11.3.1.

##### **13.1.2.2.3.1.6 wranIfMaxCpeTxEirp**

An integer value, encoded in hexadecimal, that indicates the maximum EIRP for which the CPE is configured. This reflects the setting of the IE defined in 7.7.11.3.2.1.

##### **13.1.2.2.3.1.7 wranIfCpeDemodulator**

A bit map that encodes the DIUCs that the CPE supports. This reflects the setting of the IE defined in 7.7.11.3.2.2.1.

### **13.1.2.2.3.1.8 wranIfCpeModulator**

A bit map that encodes the UIUCs that the CPE supports. This reflects the setting of the IE defined in 7.7.11.3.2.2.2.

### **13.1.2.2.3.1.9 wranIfCpeScmVersionSupport**

Indicator of the version of the SCM protocol that the CPE supports. This reflects the setting of the IE defined in 7.7.11.3.3.1.

### **13.1.2.2.3.1.10 wranIfCpePnWindowSize**

Size of PN\_WINDOW (see 8.4) that is used to protect against replay attacks. This reflects the setting of the IE defined in 7.7.11.3.3.2.

### **13.1.2.2.3.1.11 wranIfCpeScmFlowControl**

Maximum number of ongoing SCM transactions that the CPE can support. This reflects the setting of the IE defined in 7.7.11.3.3.3.

## **13.1.2.2.4 wranIfBsCpeBasicCapabilityRspTable**

This object provides a table containing the basic capability information BS has configured for CPEs BS in the CBC-RSP. Each table is made up of multiple entries, one for each CPE that has transmitted the CBC-RSP, that are defined by wranIfBsCpeBasicCapabilityRspEntry.

### **13.1.2.2.4.1 wranIfBsCpeBasicCapabilityRspEntry**

This object is a compound object that contains the configuration of basic capabilities BS has selected for a CPE during network entry. This table reflects the current configuration of a CPE's basic capabilities.

NOTE—The relevant objects that make up this entry are described in 13.1.2.2.3.1.1 to 13.1.2.2.3.1.11. All items defined for the entry will need to move to the beginning of the ASN.1 formatting of wranIfBsMib.

## **13.1.2.2.5 wranIfBsCpeRegCapabilityReqTable**

This object provides a table containing the capability information for which a CPE has requested confirmation from the BS during REG-REQ. Each table is made up of multiple entries, one for each CPE, that are defined by wranIfBsCpeRegCapabilityRegEntry.

### **13.1.2.2.5.1 wranIfBsCpeRegCapabilityReqEntry**

This object is a compound object that contains the capabilities information for which a CPE has requested confirmation from the BS, e.g., through sending a REG-REQ to the BS.

**13.1.2.2.5.1.1 wranIfBsRegisteredCpeMacAddress**

MAC address of the CPE that is currently registered with the BS. This object uniquely identifies the entry associated with a particular CPE's configured capabilities.

**13.1.2.2.5.1.2 wranIfBsRegisteredCpeRegReqNumAttempts**

The current number of attempts that a CPE has made for network entry. This item gets set to 0 upon successful completion of registration process and a CPE is admitted into the network. This item gets incremented every time a CPE attempts registration, but is unsuccessful. If this value reaches the limit set by wranIfBsMaxNumRegReqAttempts, then BS shall send a DREG-CMD to CPE.

**13.1.2.2.5.1.3 wranIfNmeaLocString**

NMEA location string of the CPE in REG-REQ (see 7.7.7.3.1).

**13.1.2.2.5.1.4 wranIfIcsConfig**

Indication in REG-REQ/RSP of how the provider will operate the CPE on an ongoing basis; either with the Ethernet CS only, the IP CS, or both (see 7.7.7.3.2).

**13.1.2.2.5.1.5 wranIfIpVersion**

What version of the IP protocol (either v4 or v6) indicated in REG-REQ/RSP that the CPE supports (see 7.7.7.3.3).

**13.1.2.2.5.1.6 wranIfIpRohcSupport**

Indication in REG-REQ/RSP on whether or not the CPE supports IP Robust Header Compression (ROHC), see 7.7.7.3.4.1.

**13.1.2.2.5.1.7 wranIfArqSupport**

ARQ Support IE of REG-REQ/RSP in 7.7.7.3.4.2.

**13.1.2.2.5.1.8 wranIf2ndMgmtArqWindowSize**

Secondary Management flow — ARQ Window Size IE of REG-REQ/RSP defined in 7.7.8.9.17.2.

**13.1.2.2.5.1.9 wranIf2ndMgmtArqRetryTxDelay**

Secondary Management flow — Transmitter Delay component of ARQ Retry Timeout IE of REG-REQ/RSP defined in 7.7.8.9.17.3.

### **13.1.2.2.5.1.10 wranIf2ndMgmtArqRetryRxDelay**

Secondary Management flow — Receiver Delay component of ARQ Retry Timeout IE of REG-REQ/RSP defined in 7.7.8.9.17.3.

### **13.1.2.2.5.1.11 wranIf2ndMgmtArqBlockLifetime**

Secondary Management flow — ARQ Block Lifetime IE of REG-REQ/RSP defined in 7.7.8.9.17.4.

### **13.1.2.2.5.1.12 wranIf2ndMgmtArqSyncLossTimeout**

Secondary Management flow — ARQ Sync Loss Timeout IE of REG-REQ/RSP defined in 7.7.8.9.17.5.

### **13.1.2.2.5.1.13 wranIf2ndMgmtArqDeliverInOrder**

Secondary Management flow — ARQ Deliver In Order IE of REG-REQ/RSP defined in 7.7.8.9.17.6.

### **13.1.2.2.5.1.14 wranIf2ndMgmtArqRxPurgeTimeout**

Secondary Management flow — ARQ Rx Purge Timeout IE of REG-REQ/RSP defined in 7.7.8.9.17.7.

### **13.1.2.2.5.1.15 wranIf2ndMgmtArqBlockSize**

Secondary Management flow — ARQ Block Size IE of REG-REQ/RSP defined in 7.7.8.9.17.8.

### **13.1.2.2.5.1.16 wranIfDsxFlowControl**

DSx Flow Control IE of REG-REQ/RSP in 7.7.7.3.4.4.

### **13.1.2.2.5.1.17 wranIfMcaFlowControl**

MCA Flow Control IE of REG-REQ/RSP in 7.7.7.3.4.5.

### **13.1.2.2.5.1.18 wranIfMaxNumMcastGroups**

Maximum Number of Multicast Groups IE of REG-REQ/RSP in 7.7.7.3.4.6.

### **13.1.2.2.5.1.19 wranIfSensModeSupportArray**

Value for the “Sensing Mode Support Array” of the Measurement Support IE in REG-REQ/RSP in 7.7.7.3.4.7. If the value of this parameter is set to “No Sensing” then wranIfBsCpeMeasurementSupportReqTable will not be stored for the CPE.

**13.1.2.2.5.1.20 wranIfAntennaModel**

Manufacturer Specific Antenna Model IE of REG-REQ in 7.7.7.3.4.8.

**13.1.2.2.5.1.21 wranIfCpeResidualDelay**

CPE Residual Delay IE of REG-REQ in 7.7.7.3.4.10.

**13.1.2.2.5.1.22 wranIfSecMgmtIpAllocationMethod**

Method for allocating IP Addresses on Secondary Management Connection IE of REG-REQ/RSP in 7.7.7.3.4.11.

**13.1.2.2.5.1.23 wranIfCpeOperationalCapability**

CPE Operation Capability IE of REG-REQ in 7.7.7.3.4.13.

**13.1.2.2.5.1.24 wranIfCpeRegistrationTimer**

CPE Registration Timer IE of REG-REQ/RSP in 7.7.7.3.5.

**13.1.2.2.6 wranIfBsCpeMeasurementSupportReqTable**

A compound object representing the Measurement Support IE of REG-REQ/RSP in 7.7.7.3.4.7. It is made up of multiple entries, one for each signal type for which sensing is supported. Each entry is defined by wranIfBsCpeMeasurementSupportReqEntry. Entries for a CPE are only present if the value for wranIfSensModeSupportArray is anything other than “No Sensing.”

**13.1.2.2.6.1 wranIfBsCpeMeasurementSupportReqEntry**

A compound object representing entries of Measurement Support IE of REG-REQ in 7.7.7.3.4.7. It is made up of multiple objects. A CPE will have one entry for each Signal Type in the Signal Type Array of the Measurement Support IE.

**13.1.2.2.6.1.1 wranIfMeasurementSupportEntryIndex**

A unique index for every entry in wranIfBsCpeMeasurementSupportReqTable.

**13.1.2.2.6.1.2 wranIfBsCpeRegisteredMacAddress**

MAC address of CPE. This corresponds to an entry in wranIfBsCpeRegistrationReqTable for a registered CPE.

### **13.1.2.2.6.1.3 wranIfMeasurementSignalType**

Signal type that measurement configuration this entry pertains to (see Table 237).

### **13.1.2.2.6.1.4 wranIfMeasurementThreshold**

Signed number that signifies the sensitivity threshold for the signal type.

### **13.1.2.2.6.1.5 wranIfMeasurementPd**

Probability of detection (PD) for the signal type.

### **13.1.2.2.6.1.6 wranIfMeasurementMpfa**

Maximum Probability of False Alarm for the signal type.

### **13.1.2.2.6.1.7 wranIfMeasurementRecNumSensPeriods**

Recommended number of sensing periods required to sense the signal type.

### **13.1.2.2.6.1.8 wranIfMeasurementRecSensPeriodDuration**

Recommended duration of sensing periods, units of symbols.

### **13.1.2.2.6.1.9 wranIfMeasurementRecSensPeriodInterval**

Recommended length for the sensing period interval, units of integer number of frames.

## **13.1.2.2.7 wranIfBsCpeRegCapabilityRspTable**

This object provides a table containing the capability information that a BS has configured for a CPE in REG-RSP. Each table is made up of multiple entries, one for each CPE, that are defined by wranIfBsCpeRegCapabilityRspEntry.

### **13.1.2.2.7.1 wranIfBsCpeRegCapabilityRspEntry**

This object is a compound object that contains the capabilities information that a BS has configured for a CPE.

NOTE 1—As with CBC-RSP, the entries will contain the objects that have scope in both REG-REQ and REG-RSP object types as the REG-REQ objects, e.g., this entry will be made of the objects in 13.1.2.2.5.1.1-13.1.2.2.15.1.1.24.

NOTE 2—In addition to having the objects in 13.1.2.2.5.1.1 through 13.1.2.2.5.1.24, this compound object will have an object containing the permanent station Id when CPE privacy (see 8.7) is being used.

### **13.1.2.2.7.1.25 wranIfPermanentSid**

Permanent station ID assigned to CPE, when CPE is entering the network under the CPE Privacy method (see 8.7). The format of this IE shall be as defined in 7.7.7.3.4.12.

### **13.1.2.2.8 wranIfBsCpeMeasurementSupportRspTable**

A compound object representing the Measurement Support IE of REG-REQ/RSP in 7.7.7.3.4.7. It is made up of multiple entries, one for each signal type that sensing supports. Each entry is defined by wranIfBsCpeMeasurementSupportRspEntry.

#### **13.1.2.2.8.1 wranIfBsCpeMeasurementSupportRspEntry**

A compound object representing entries of Measurement Support IE of REG-RSP in 7.7.7.3.4.7. It is made up of multiple objects. A CPE will have one entry for each Signal Type in the Signal Type Array of the Measurement Support IE. Entries for a CPE are only present if the value for wranIfSensModeSupportArray is anything other than “No Sensing.”

NOTE— This will contain the same objects types, e.g., this entry will be made of the objects in 13.1.2.2.6.1.1 through 13.1.2.2.6.1.9.

### **13.1.2.2.9 wranIfBsCpeAntennaGainTable**

At the CPE, this object represents a compound object representing entries of the CPE Antenna Gain IE (7.7.7.3.4.9), that carries a CPE’s antenna gain when a CPE transmits a REG-REQ to the BS. At the BS, this object is a compound object that represents the entries for its own transmit antenna gain as well as the antenna gain information for each CPE that sent a CPE Antenna Gain IE in a REG-REQ (and has successfully completed registration). This object is a table that is made up of multiple entries, each defined by wranIfBsCpeAntennaGainEntry.

#### **13.1.2.2.9.1 wranIfBsCpeAntennaGainEntry**

A compound object representing the on-axis gain (in dB) for each channel on which the CPE’s or BS’s antenna is capable of operating.

##### **13.1.2.2.9.1.1 wranIfBsCpeMacAddress**

MAC address of the device.

##### **13.1.2.2.9.1.2 wranIfTvChannel**

TV Channel number.

##### **13.1.2.2.9.1.3 wranIfOnAxisGain**

Maximum gain in the specified TV channel.

### **13.1.2.2.10 wranIfBsCapabilitiesConfigTable**

This table is analogous to the wranIfBsCpeBasicCapabilityRspTable and wranIfBsCpeRegCapabilityRspTable, except there is only one entry in this table. This MIB provides default values for the capabilities that the BS uses to evaluate the REG-REQ and REG-REQ from CPE. These default values could be defined on a per-regulatory domain basis (see Annex B) to comply with regulations defined by various regulatory bodies. This is a compound object that contains all the entries specified in wranIfBsCpeBasicCapabilityRspEntry and wranIfBsCpeRegCapabilityRspEntry.

#### **13.1.2.2.10.1 wranIfBsCapabilitiesConfigEntry**

This object represents an entry into wranIfBsCapabilitiesConfigTable. Items in this object comprise of the IEs as defined for the CBC-REQ/RSP and REG-REQ/RSP messages as well as a limit on the maximum number of CBC-REQ/RSP attempts [REG-REQ/RSP attempts (wranIfBsMaxNumRegReqAttempts)].

##### **13.1.2.2.10.1.1 wranIfBsMaxNumRegReqAttempts**

This object represents the default limit of maximum number of attempts a CPE can make to register itself. When this limit is reached, the BS shall send a DREG-CMD to the CPE to tell it to shutdown. The default for this limit is 5.

##### **13.1.2.2.10.1.2 wranIfBsMaxNumCbcReqAttempt**

This object represents the default limit of maximum number of attempts a CPE can make to configure basic capabilities itself. The default for this limit is 5.

NOTE—The remaining objects in wranIfBsCapabilitiesConfigEntry will be made of the objects described in 13.1.2.2.3.1.1 through 13.1.2.2.3.1.8 and 13.1.2.2.5.1.1 through 13.1.2.2.5.1.23.

##### **13.1.2.2.10.1.3 wranIfBsDsxReqRetries**

Maximum number of timeout retries for DSx-REQ messages.

##### **13.1.2.2.10.1.4 wranIfBsDsxRspRetires**

Maximum number of timeout retries for DSx-RSP messages.

##### **13.1.2.2.10.1.5 wranIfBsT7**

Wait for DSx-RSP timeout.

**13.1.2.2.10.1.6 wranIfBsT8**

Wait for DSA/DSC-RSP timeout.

**13.1.2.2.10.1.7 wranIfBsT10**

Wait for Transaction End timeout.

**13.1.2.2.10.1.8 wranIfBsT13**

Time allowed for a CPE, following receipt of a REG-RSP to send a TFTP-CPLT message to the BS.

**13.1.2.2.10.1.9 wranIfBsT15**

Wait for MCA-RSP.

**13.1.2.2.10.1.10 wranIfBsT22**

Wait for ARQ-Reset.

**13.1.2.2.10.1.11 wranIfBsT27Idle**

Maximum time between unicast grants to CPE when BS believe CPE transmission quality is good enough.

**13.1.2.2.10.1.12 wranIfBsT27Active**

Maximum time between unicast grants to CPE when BS believes CPE transmission quality is not good enough.

**13.1.2.2.10.1.13 wranIfBsT28**

Time allowed for BS to complete the transmission of the backup/candidate channel list to its CPEs after initial registration by a new CPE, including the database service query.

**13.1.2.2.10.1.14 wranIfBsDSxFlowControl**

Maximum number of ongoing dynamic service flow (DSx-REQ/RSP) transactions.

**13.1.2.2.10.1.15 wranIfBsMcaFlowControl**

Maximum number of ongoing multicast group assignment (MCA-REQ/RSP) transactions.

**13.1.2.2.10.1.16 wranIfBsMaxMcastGroups**

Maximum number of multicast groups the BS supports in a cell.

### **13.1.2.2.10.1.17 wranIfBsT30**

CPE Registration timer as set by REG-REQ IE (see 7.7.7.3.5 and 7.14.2.11).

### **13.1.2.2.10.1.18 wranIfBs2ndMgmtArqWindowSize**

Maximum number of unacknowledged ARQ blocks at a given time that BS applies on secondary management flows.

### **13.1.2.2.10.1.19 wranIfBs2ndMgmtArqRetryTxDelay**

Transmitter delay as applied by BS to ARQ on Secondary Management flow.

### **13.1.2.2.10.1.20 wranIfBs2ndMgmtArqRetryRxDelay**

Receiver Delay as applied by BS to ARQ on Secondary Management flow.

### **13.1.2.2.10.1.21 wranIfBs2ndMgmtArqBlockLifetime**

ARQ Block Lifetime as applied by BS to ARQ on Secondary Management flow.

### **13.1.2.2.10.1.22 wranIfBs2ndMgmtArqSyncLossTimeout**

ARQ Sync Loss Timeout as applied by BS to ARQ on Secondary Management flow.

### **13.1.2.2.10.1.23 wranIfBs2ndMgmtArqDeliverInOrder**

ARQ Deliver In Order specification that BS applies to ARQ on Secondary Management flow.

### **13.1.2.2.10.1.24 wranIfBs2ndMgmtArqRxPurgeTimeout**

ARQ Rx Purge Timeout that BS applies to ARQ on Secondary Management flow.

### **13.1.2.2.10.1.25 wranIfBs2ndMgmtArqBlockSize**

ARQ Block Size that BS applies to ARQ on Secondary Management flow.

### **13.1.2.2.10.1.26 wranIfBsMaxCpeTxEirp**

Maximum CPE Transmit EIRP as negotiated during registration.

**13.1.2.2.10.1.27 wranIfBsT36**

Default value for EAP Authentication Timer.

**13.1.2.2.10.1.28 wranIfBsT37**

Default value for Authentication Grace Timer.

**13.1.2.2.10.1.29 wranIfBsMaxNumAuthAttempts**

Default value for the maximum number of times a CPE may attempt authentication.

**13.1.2.2.10.1.30 wranIfBsT38**

Default value for Operational Wait Timeout.

**13.1.2.2.10.1.31 wranIfBsT39**

Default value for Rekey Wait Timeout.

**13.1.2.2.10.1.32 wranIfBsAkLifetime**

Default lifetime BS assigns to a new AK.

**13.1.2.2.10.1.33 wranIfBsTekLifetime**

Default lifetime BS assigns to a new TEK.

**13.1.2.2.10.1.34 wranIfBsScmFlowControl**

Default value for the maximum number of ongoing SCM transactions.

**13.1.2.2.10.1.35 wranIfBsNumSupportedSAs**

Maximum number of SAs a CPE can support.

**13.1.2.2.10.1.36 wranIfBsPnWindowSize**

Size of PN\_WINDOW (see 8.4) used to protect against replay attacks.

**13.1.2.2.10.1.37 wranIfBsT17**

Time allowed for CPE to complete authentication and key exchange.

### **13.1.2.2.11 wranIfBsMeasurementSupportTable**

A compound object representing default values that a BS uses to select configuration of the measurement capabilities (via the Measurement Support IE of REG-RSP in 7.7.7.3.4.7). It is made up of multiple entries. Each entry defines the default measurement configuration for each signal type for which sensing is supported. Each entry is defined by `wranIfMeasurementSupportEntry`.

#### **13.1.2.2.11.1 wranIfBsMeasurementSupportEntry**

A compound object representing entries of `wranIfBsMeasurementSupportTable` that will be used to evaluate and select configuration of the Measurement Support IE of REG-RSP in 7.7.7.3.4.7. It is made up of multiple objects. There will have one entry for each Signal Type that corresponds to Signal Type Array of the Measurement Support IE.

NOTE—This object is made up of the objects in 13.1.2.2.6.1.1 through 13.1.2.2.6.1.9. The values that these objects are set up in this table will be based on recommendations in Annex A.

### **13.1.2.2.12 wranIfBsActionsTable**

This object provides a table that stores actions that can be configured to have BS direct a CPE to act upon receiving unsolicited MAC management messages such as RNG-CMD and DREG-CMD. Each table is made up of an entry for each action directed to a particular CPE. Each entry is defined by `wranIfBsActionsEntry`.

#### **13.1.2.2.12.1 wranIfBsActionsEntry**

This object is a compound object that contains actions that are requested for a particular CPE. A BS may skip directing the CPE to execute a particular action based on the current state of the CPE. Only one action is executable at a given time.

##### **13.1.2.2.12.1.1 wranIfBsCpeActionsMacAddress**

This uniquely identifies the CPE that is the target of the action by the CPE's MAC address.

##### **13.1.2.2.12.1.2 wranIfBsCpeActionsRangeCpe**

When set, the BS will send an unsolicited RNG-CMD to a CPE with the Ranging Status field set to 'abort' without any new parameter or the Ranging Status field set to 'abort' with a new set of parameters. No action is to be taken if this object is read.

##### **13.1.2.2.12.1.3 wranIfBsCpeActionsDeRegCpe**

When set to an Action Code value as defined in Table 115, the BS will send a DREG-CMD to the CPE with that Action Code. No action is to be taken if this object is read or an invalid Action Code is specified.

### **13.1.2.2.12.1.4 wranIfBsCpeActionsStatus**

This object contains the status of the write operation for a component of the wranIfBsCpeActionsEntry to make sure the write operation has been executed properly.

### **13.1.2.2.13wranIfBsCpeMulticastConfigTable**

This table contains the configuration of multicast groups and what CPEs are assigned to them. Each table is made up of multiple entries, defined by wranIfBsCpeMulticastEntry. A CPE may have multiple entries in this table, one for each multicast group that it belongs to. Entries will be deleted for a CPE whenever a CPE is asked to leave a multicast group.

#### **13.1.2.2.13.1 wranIfBsCpeMulticastEntry**

This object is a compound object that contains information about the configuration of a CPE's multicast group membership configuration.

##### **13.1.2.2.13.1.1 wranIfBsCpeMacAddress**

This object refers to a CPE's MAC address. It is used to uniquely index the multicast group configuration for a particular CPE in wranIfBsCpeMulticastConfigTable, along with wranIfBsCpeMulticastCid.

##### **13.1.2.2.13.1.2 wranIfBsMulticastSid**

This object refers to the multicast SID that is assigned to a multicast group.

##### **13.1.2.2.13.1.3 wranIfBsMulticastPeriodicAllocationParameterM**

This object defines the 'm' value (see Table 103) that is used to calculate the periodic allocation for multicast transmission.

##### **13.1.2.2.13.1.4 wranIfBsMulticastPeriodicAllocationParameterK**

This object defines the 'k' value (see Table 103) that is used to calculate the periodic allocation for multicast transmission.

##### **13.1.2.2.13.1.5 wranIfBsMulticastPeriodicAllocationParameterN**

This object defines the 'n' value (see Table 103) that is used to calculate the periodic allocation for multicast transmission.

### **13.1.2.2.14wranIfBsCoexistenceConfigTable**

This table contains the configuration items related to self-coexistence operation and CBP transmission. It is made up of one entry represents the default values for self-coexistence operation and CBP transmission.

#### **13.1.2.2.14.1 wranIfBsCoexistenceConfigEntry**

This object represents a single entry that is in wranIfBsCoexistenceConfigTable.

##### **13.1.2.2.14.1.1 wranIfBsT34**

This governs how often (in seconds) the Device Identification IE is transmitted in a CBP burst. Default value is 300 s.

##### **13.1.2.2.14.1.2 wranIfBsT33**

Time between transmissions of CBP bursts with backup/candidate channel list information (see 7.6.1.3.1.1) to facilitate spectrum etiquette.

##### **13.1.2.2.14.1.3 wranIfBsT32**

Wait for Frame Contention Response (FC-RSP) message.

##### **13.1.2.2.14.1.4 wranIfBsFcw**

Frame contention window, the number of superframes that a contention destination accumulates frame contention requests before responding to them.

##### **13.1.2.2.14.1.5 wranIfBsScwBackoffMax**

Maximum number of superframes for the SCW backoff window.

##### **13.1.2.2.14.1.6 wranIfBsFcMin**

Number of frames not available for contention at the BS.

##### **13.1.2.2.14.1.7 wranIfBsFcnRange**

Exponent, base 2, defining the range of random numbers for the FCN.

**13.1.2.2.14.1.8 wranIfBsSfRel**

Number of superframes after which a BS releases the frames won by another BS through frame contention.

**13.1.2.2.14.1.9 wranIfBsT35**

SCW Backoff Timer, timer controlling continuation or exiting of Frame Contention Procedure.

**13.1.2.2.15wranIfBsPhy**

This MIB object contains managed objects related to the PHY configuration. All objects described are related to the OFDMA PHY that is supported.

**13.1.2.2.15.1 wranIfBsOfdmaPhyUsChannelTable**

This object provides a table to describe attributes of upstream channels. It is a compound object that is made up of multiple entries, each described by `wranIfBsOfdmaPhyUsChannelTableEntry`.

**13.1.2.2.15.1.1 wranIfBsOfdmaPhyUsChannelTableEntry**

This object is a compound object that represents an entry for the BS upstream channel.

**13.1.2.2.15.1.1.1 wranIfBsOfdmaCtBasedResvTimeout**

The number of US-MAPs to receive before contention-based reservation is attempted again for the same connection.

**13.1.2.2.15.1.1.2 wranIfBsOfdmaUsCenterFrequency**

Upstream center frequency in kHz.

**13.1.2.2.15.1.1.3 wranIfBsOfdmaUsRadioResource**

Indicates the average percentage (ratio) of non-assigned US radio resource to total usable US radio resources.

**13.1.2.2.15.1.1.4 wranIfBsOfdmaUsConfigChangeCount**

Current UCD change count.

**13.1.2.2.15.1.1.5 wranIfBsOfdmaUsUcsNotificationCodes**

Number of CDMA codes for UCS Notification.

### **13.1.2.2.15.1.1.6 wranIfBsOfdmaUsInitRngCodes**

Number of CDMA codes for initial ranging.

### **13.1.2.2.15.1.1.7 wranIfBsOfdmaUsPeriodicRngCodes**

Number of CDMA codes for periodic ranging.

### **13.1.2.2.15.1.1.8 wranIfBsOfdmaUsBWReqCodes**

Number of CDMA codes for bandwidth requests.

### **13.1.2.2.15.1.1.9 wranIfBsOfdmaUsPeriodicRngBackoffStart**

Represented as a power of 2, initial size of backoff window used for periodic ranging contention.

### **13.1.2.2.15.1.1.10 wranIfBsOfdmaUsPeriodicRngBackoffEnd**

Represented as a power of 2, final size of backoff window used for periodic ranging contention.

### **13.1.2.2.15.1.1.11 wranIfBsOfdmaUsStartofCodes**

Includes first code in block of codes to be used, known as S. The total set of codes ranges from S to  
 $(wranIfBsOfdmaUsInitRngCodes + wranIfBsOfdmaUsPeriodicRngCodes +$   
 $wranIfBsOfdmaUsBWReqCodes + wranIfBsOfdmaUsUcsNotificationCodes) \bmod 256$ .

### **13.1.2.2.15.1.1.12 wranIfBsOfdmaUsNormalizedCnrOverride**

This is a list of numbers, encoded by a nibble and interpreted by a signed integer. The nibbles are defined in 9.9.4.2. The number encoded by each nibble represents the difference in normalized CNR relative to the previous one.

### **13.1.2.2.15.1.1.13 wranIfBsOfdmaUsNormalizedCnrValue**

A signed integer that corresponds to the normalized CNR value in the previous line.

### **13.1.2.2.15.1.1.14 wranIfBsOfdmaUsCpeUpPowerAdjStep**

CPE-specific up power offset adjustment step.

### **13.1.2.2.15.1.1.15 wranIfBsOfdmaUsInitialRangingInterval**

Number of frames between initial ranging interval allocation.

### **13.1.2.2.15.1.1.16 wranIfBsOfdmaUsTxPowerReport**

Tx Power report.

### **13.1.2.2.15.1.1.17 wranIfBsOfdmaUsUcsNotificationBackoffStart**

Expressed as a power of 2, initial backoff window size for UCS notification contention.

### **13.1.2.2.15.1.1.18 wranIfBsOfdmaUsUcsNotificationBackoffEnd**

Expressed as a power of 2, final backoff window size for UCS notification contention.

### **13.1.2.2.15.1.1.19 wranIfBsOfdmaUsInitialRngBackoffStart**

Expressed as a power of 2, initial backoff window size for initial ranging contention.

### **13.1.2.2.15.1.1.20 wranIfBsOfdmaUsInitialRngBackoffEnd**

Expressed as a power of 2, final backoff window size for initial ranging contention.

### **13.1.2.2.15.1.1.21 wranIfBsOfdmaUsBwRequestBackoffStart**

Expressed as a power of 2, initial backoff window for contention-based BW requests.

### **13.1.2.2.15.1.1.22 wranIfBsOfdmaUsBwRequestBackoffEnd**

Expressed as a power of 2, the final backoff window size for contention-based BW requests.

### **13.1.2.2.15.1.1.23 wranIfBsOfdmaUsRelPwrOffsetMacMgmtBurst**

Relative to normal traffic bursts, the power offset used for US MAC management message transmission.

### **13.1.2.2.15.1.1.24 wranIfBsOfdmaUsInitialTxTiming**

Initial timing reference for US transmissions.

### **13.1.2.2.15.1.1.25 wranIfBsOfdmaUsRangingRegion**

US ranging region definition.

### **13.1.2.2.15.1.1.26 wranIfBsOfdmaUsUcdInterval**

Time between transmission of UCD messages.

### **13.1.2.2.15.1.1.27 wranIfBsOfdmaUsUcdTransition**

Time BS shall wait after repeating a UCD message with an incremented Configuration Change Count before issuing a US-MAP message referring to Upstream\_Burst\_Profiles defined in that UCD message.

### **13.1.2.2.15.1.1.28 wranIfBsOfdmaUsClkCmpInterval**

Time between the clock compare measurements used for the generation of CLK-CMP messages.

### **13.1.2.2.15.1.1.29 wranIfBsOfdmaUsT57**

Lost US-MAP interval, time since last received US-MAP message before upstream synchronization is considered lost (used on the CPE).

### **13.1.2.2.15.1.1.30 wranIfBsOfdmaT58**

Number of SCH that can be lost until synchronization is considered lost.

### **13.1.2.2.15.1.1.31 wranIfBsOfdmaUsCdmaRngRetries**

Number of retries on CDMA RNG-REQs.

### **13.1.2.2.15.1.1.32 wranIfBsOfdmaUsInvRngReq**

Number of retries on inviting RNG-REQs.

### **13.1.2.2.15.1.1.33 wranIfBsOfdmaUsMapProcTime**

Time provided between arrival of the last bit of a US-MAP at a CPE and the effectiveness of that map.

### **13.1.2.2.15.1.1.34 wranIfBsOfdmaUsT3**

RNG-CMD reception timeout following the transmission of a RNG-REQ.

### **13.1.2.2.15.1.1.35 wranIfBsOfdmaUsT4**

Time to wait for unicast ranging opportunity.

### **13.1.2.2.15.1.1.36 wranIfBsOfdmaUsT5**

Time to wait for Upstream Channel Change response.

### **13.1.2.2.15.1.1.37 wranIfBsOfdmaUsT12**

Wait for UCD descriptor.

## **13.1.2.2.15.2 wranIfBsOfdmaPhyDsChannelTable**

This object provides a table to describe attributes of downstream channels. It is a compound object that is made up of multiple entries, each described by `wranIfBsOfdmaPhyDsChannelTableEntry`.

### **13.1.2.2.15.2.1 wranIfBsOfdmaPhyDsChannelTableEntry**

This object is a compound object that represents an entry for the BS downstream channel.

#### **13.1.2.2.15.2.1.1 wranIfBsOfdmaDsEirp**

The equivalent isotropic radiated power of the base station, which is computed for a simple single-antenna transmitter.

#### **13.1.2.2.15.2.1.2 wranIfBsOfdmaDsChannelNumber**

Current operating channel.

#### **13.1.2.2.15.2.1.3 wranIfBsOfdmaDsPhyMaxEirp**

Initial ranging maximum EIRP, at BS in units of 1 dBm.

#### **13.1.2.2.15.2.1.4 wranIfBsOfdmaDsCenterFreq**

DS center frequency in kHz.

#### **13.1.2.2.15.2.1.5 wranIfBsOfdmaDsBsId**

Base Station ID.

#### **13.1.2.2.15.2.1.6 wranIfBsOfdmaDsMacVersion**

The MAC version to which the BS is conformant.

**13.1.2.2.15.2.1.7 wranIfBsOfdmaDsCyclicPrefix**

Ratio of CP time to useful symbol time; possible values are 1/4, 1/8, 1/16, 1/32.

**13.1.2.2.15.2.1.8 wranIfBsOfdmaDsRadioResource**

Average ratio of non-assigned DS radio resources to total usable DS radio resources.

**13.1.2.2.15.2.1.9 wranIfBsOfdmaDsHysteresisMargin**

When the CINR of a neighbor BS is larger than the sum of the CINR of the current serving BS and the hysteresis margin for the time-to-trigger duration, than the neighbor BS is included in the list of possible target BS with which to attempt initial network entry.

**13.1.2.2.15.2.1.10 wranIfBsOfdmaDsCellType**

This object identifies classes of BSs that can be used by CPE when selecting with which cell to attempt network entry.

**13.1.2.2.15.2.1.11 wranIfBsOfdmaDsConfigChangeCount**

Current BS DCD configuration change count.

**13.1.2.2.15.2.1.12 wranIfBsOfdmaDsPowerControlMode**

Defines the default power control information to CPE.

**13.1.2.2.15.2.1.13 wranIfBsOfdmaDsFrameDuration**

Duration of the frame.

**13.1.2.2.15.2.1.14 wranIfBsOfdmaDsRssiCinrAvgParameter**

Bits 0–3 of default RSSI and CINR averaging parameter.

**13.1.2.2.15.2.1.15 wranIfBsOfdmaDsThresholdAddBsServiceSet**

Threshold used by CPE to add a neighbor BS to the list of available WRAN service.

**13.1.2.2.15.2.1.16 wranIfBsOfdmaDsThresholdDelBsServiceSet**

Threshold used by CPE to delete a neighbor BS to the diversity set.

### **13.1.2.2.15.2.1.17 wranIfBsOfdmaDsDcdInterval**

Time between transmission of DCD messages.

### **13.1.2.2.15.2.1.18 wranIfBsOfdmaDsDcdTransition**

Time BS shall wait after repeating a DCD message with an incremented Configuration Change Count before issuing a DS-MAP message referring to Downstream\_Burst\_Profiles defined in that DCD message.

### **13.1.2.2.15.2.1.19 wranIfBsOfdmaDsT56**

Time since last received DS-MAP message before downstream synchronization is considered lost.

### **13.1.2.2.15.2.1.20 wranIfBsOfdmaDsT1**

Wait for DCD timeout.

### **13.1.2.2.15.2.1.21 wranIfBsOfdmaDsT2**

Wait for broadcast ranging timeout.

### **13.1.2.2.15.2.1.22 wranIfBsOfdmaDsT20**

Time CPE searches for preambles on a given channel.

### **13.1.2.2.15.2.1.23 wranIfBsOfdmaDsT21**

Time the CPE searches for a DS-MAP on a given channel.

### **13.1.2.2.15.2.1.24 wranIfBsOfdmaDsTtg**

Transmit/Receive Transition Gap.

## **13.1.2.2.15.3 wranIfBsOfdmaUcdBurstProfileTable**

This table contains the UCD burst profile configurations for each upstream channel. Each entry in the table is represented by wranIfBsOfdmaUcdBurstProfileEntry.

### **13.1.2.2.15.3.1 wranIfBsOfdmaUcdBurstProfileEntry**

This is a compound object that defines each entry in wranIfBsOfdmaUcdBurstProfileTable.

**13.1.2.2.15.3.1.1 wranIfBsOfdmaUcdUiucIndex**

The UIUC that indicates the upstream burst profile in the UCD message.

**13.1.2.2.15.3.1.2 wranIfBsOfdmaUcdFecCodeType**

Modulation and FEC for upstream.

**13.1.2.2.15.3.1.3 wranIfBsOfdmaUcdUiucExitThreshold**

CINR at or below which this UIUC can no longer be used where change to a more robust UIUC is required.

**13.1.2.2.15.3.1.4 wranIfBsOfdmaUcdUiucEntryThreshold**

Minimum CINR required to starting using this UIUC when changing from a more robust UIUC is required.

**13.1.2.2.15.3.1.5 wranIfBsOfdmaUcdRangingDataRatio**

Difference in power from burst UCD and power to be used for CDMA ranging in units of 1 dB.

**13.1.2.2.15.4 wranIfBsOfdmaDcdBurstProfileTable**

This table provides configuration for each DCD burst profile. It is made up of multiple entries defined by wranIfBsOfdmaDcdBurstProfileEntry.

**13.1.2.2.15.4.1 wranIfBsOfdmaDcdBurstProfileEntry**

This is a compound object that defines each entry in wranIfBsOfdmaDcdBurstProfileTable.

**13.1.2.2.15.4.1.1 wranIfBsOfdmaDcdDiucIndex**

The DIUC of the DS burst profile in the DCD message.

**13.1.2.2.15.4.1.2 wranIfBsOfdmaDcdFecCodeType**

Modulation and FEC for downstream.

**13.1.2.2.15.4.1.3 wranIfBsOfdmaDcdDiucExitThreshold**

CINR at or below which this DIUC can no longer be used where change to a more robust DIUC is required.

**13.1.2.2.15.4.1.4 wranIfBsOfdmaDcdDiucEntryThreshold**

Minimum CINR required to starting using this DIUC when changing from a more robust DIUC is required.

### **13.1.2.2.15.5 wranIfBsOfdmaDsRegionTable**

This table provides the configuration of the DS subframe. It is made up of entries defined by wranIfBsOfdmaDsRegionEntry.

#### **13.1.2.2.15.5.1 wranIfBsOfdmaDsRegionEntry**

This is a compound object that describes each entry in wranIfBsOfdmaDsRegionTable.

##### **13.1.2.2.15.5.1.1 wranIfBsOfdmaDsRegionIndex**

Index DS region in table.

##### **13.1.2.2.15.5.1.2 wranIfBsOfdmaDsDuration**

Number of OFDMA slots linearly allocated to a DS burst region.

### **13.1.2.2.15.6 wranIfBsOfdmaUsRegionTable**

This table provides the configuration of the US subframe. It is made up of entries defined by wranIfBsOfdmaUsRegionEntry.

#### **13.1.2.2.15.6.1 wranIfBsOfdmaUsRegionEntry**

This is a compound object that describes each entry in wranIfUsOfdmaDsRegionTable.

##### **13.1.2.2.15.6.1.1 wranIfBsOfdmaUsRegionIndex**

Index US region in table.

##### **13.1.2.2.15.6.1.2 wranIfBsOfdmaUsDuration**

Number of OFDMA slots linearly allocated to a US burst region.

### **13.1.2.3 wranIfBsAm**

This MIB group contains various objects related to Accounting Management.

### **13.1.2.3.1 wranIfBsOtaUsageDataRecordTable**

This object contains usage entries that track the number of octets/packets transmitted or received over the air interface. Records may be transferred to an external database, such as an AAA server, after which they can be deleted from this table. Each entry is defined by wranIfBsOtaUsageDataRecordEntry.

#### **13.1.2.3.1.1 wranIfBsOtaUsageDataRecordEntry**

This object is a compound object that identifies entries in the wranIfBsOtausageDataRecordTable.

##### **13.1.2.3.1.1.1 wranIfBsSid**

A 9-bit Station ID that identifies the station that is carrying traffic.

##### **13.1.2.3.1.1.2 wranIfBsFid**

A 3-bit flow ID that identifies the specific flow assigned to a station that is carrying traffic. For data traffic this identifies the FID that is mapped to a SFID (i.e., wranIfBsServiceFlowId).

##### **13.1.2.3.1.1.3 wranIfBsSessionId**

An identifier for a session. A session is a segment in time when a service flow is active. Multiple sessions can be created during the service flow activation time to allow the BS to track usage during periods when the service flow configuration (e.g., QoS) is changing.

##### **13.1.2.3.1.1.4 wranIfBsServiceFlowId**

32-bit identifier of the service flow. This value is set to 0, when wranIfBsFid is a basic, primary management, secondary management for unicast SIDs (single CPEs), as well as multicast management and polling FID of multicast SID (group of CPEs).

##### **13.1.2.3.1.1.5 wranIfBsMacSduCount**

Counter of the number of MAC SDUs transmitted on a FID. If the FID represents a basic, primary/secondary management, or multicast management CID, then this deals with traffic transmitted on both the DS and US.

##### **13.1.2.3.1.1.6 wranIfBsOctetCount**

Counter of the number of MAC SDUs/messages that have been transmitted and received over the air interface.

##### **13.1.2.3.1.1.7 wranIfBsSessionStartTime**

Date and time a session was established.

### **13.1.2.3.1.1.8 wranIfBsSessionEndTime**

Date and time a session was ended.

### **13.1.2.3.1.1.9 wranIfBsOtaQoSProfileIndex**

This index points to entry in QoS Profile table that defines the QoS parameter set used in the session.

## **13.1.2.4 wranIfBsPm**

This MIB group contains objects related to Performance Management. The following tables are provided in this MIB:

- wranIfBsPmConfigurationTable: Provides configuration determining which tables are enabled.
- wranIfBsRssiCinrMetricsTable: Help track metrics related to measurement of CPE upstream signal by BS and BS downstream signal by CPE.
- wranIfBsStartupMetricsTable: Help track non-timing metrics related to network entry and re-entry.
- wranIfBsThroughputMetricsTable: Help track metrics related to peak/average data rate.
- wranIfBsNetworkEntryMetricsTable: Help track timing metrics related to network entry and re-entry.
- wranIfBsPacketErrorRateTable: Help track metrics related to packet error rate measurements.
- wranIfBsUserMetricsTable: Help track metrics related to current status of CPEs in the cell.
- wranIfBsServiceFlowMetricsTable: Helps track metrics related to service flows.
- wranIfBsArqMetricsTable: Helps track the performance of ARQ.
- wranIfBsAuthenticationMetricsTable: Table helps track the number of authentication/encryption errors that occur.
- wranIfBsCoexistenceStatusTable: Table helps track the status of ongoing coexistence (e.g., Frame Contention) transaction.
- wranIfBsCoexistenceSourceTable: Table helps track what neighbor BSs are attempting a coexistence (Frame Contention) transaction with a particular source BS.
- wranIfBsCoexistenceResourceListTable: Table helps track what resources neighboring WRANs are making use of. This includes the Backup/Candidate channel lists, DS/US splits, SCW schedule.
- wranIfBsCoexistenceCurrentConfigTable: Table helps keep track of current (frame) allocation allowed to winner of recent winner, and the release time.

### **13.1.2.4.1 wranIfBsPmConfigurationTable**

The configuration of statistics capture and measurement is captured in this table. There is one entry in this table for each BS sector. The entries are defined by wranIfBsPmConfigurationEntry.

#### **13.1.2.4.1.1.1 wranIfBsPmConfigurationEntry**

This object is a compound object that represents an entry in wranIfBsPmConfigurationTable.

##### **13.1.2.4.1.1.1.1 wranIfBsGranularityInterval**

Data rate statistics captured in wranIfBsDataRateStatisticsTable are measured over the time interval this object specifies.

##### **13.1.2.4.1.1.1.2 wranIfBsCountersReportInterval**

This MIB determines the interval in which traps in wranIfBsTrapControlRegister related to performance measurement are reported to the NCMS.

##### **13.1.2.4.1.1.1.3 wranIfBsPmMeasurementBitmap**

This MIB object is a bitmap indicating which of the measurement tables are enabled or disabled.

#### **13.1.2.4.2 wranIfBsRssiCinrMetricsTable**

This MIB object contains a table that records BS upstream measurement of a CPE's transmissions, as well as CPE measurement of BS downstream signal. The data is stored as a histogram. This table is made up of entries defined by wranIfBsRssiCinrMetricsEntry. Each entry is uniquely identified by the CPE's MAC address and the index of the entry in the histogram.

##### **13.1.2.4.2.1 wranIfBsRssiCinrMetricsEntry**

This is a compound object made up objects that represent an entry in wranIfBsRssiCinrMetricsTable.

###### **13.1.2.4.2.1.1 wranIfBsCpeMacAddress**

MAC Address of the CPE.

###### **13.1.2.4.2.1.2 wranIfBsCpeHistogramIndex**

Index in histogram to which the entry pertains.

###### **13.1.2.4.2.1.3 wranIfBsChannelDirection**

Direction of channel, whether DS or US, on which the measurement was done.

###### **13.1.2.4.2.1.4 wranIfBsChannelNumber**

Channel number on which the measurement was done.

#### **13.1.2.4.2.1.5 wranIfBsStartFrame**

Frame number in which the measurement was conducted.

#### **13.1.2.4.2.1.6 wranIfBsMeasurementDuration**

Duration of measurement period in units of symbol period.

#### **13.1.2.4.2.1.7 wranIfBsSignalReportType**

This object indicates what type of signal was detected during the measurement that is recorded in this entry.

#### **13.1.2.4.2.1.8 wranIfBsMeanCinrReport**

Mean CINR report.

#### **13.1.2.4.2.1.9 wranIfBsMeanRssiReport**

Mean RSSI report.

#### **13.1.2.4.2.1.10 wranIfBsStdDevCinrReport**

Standard Deviation CINR report.

#### **13.1.2.4.2.1.11 wranIfBsStdDevRssiReport**

Standard Deviation RSSI report.

### **13.1.2.4.3 wranIfBsStartupMetricsTable**

This MIB provides a table to track how CPEs perform during initial network entry and re-entry. This table is made of entries, defined by wranIfBsStartupMetricsEntry. There is one entry for each sector of the BS.

#### **13.1.2.4.3.1 wranIfBsStartupMetricsEntry**

This object is a compound object that defines entries in wranIfBsStartupMetricsTable.

##### **13.1.2.4.3.1.1 wranIfBsNumAuthAttempt**

A counter for the number of CPE authentication attempts.

#### **13.1.2.4.3.1.2 wranIfBsNumAuthSuccess**

A counter for the number of successful authentication handshake completions.

#### **13.1.2.4.3.1.3 wranIfBsAuthSuccessRate**

Success rate of authentication attempts:  $wranIfBsAuthSuccessRate = 100 \times (wranIfBsNumAuthSuccess / wranIfBsNumAuthAttempt)$ .

#### **13.1.2.4.3.1.4 wranIfBsNumRangingAttempt**

Number of CPE ranging requests received.

#### **13.1.2.4.3.1.5 wranIfBsNumRangingSuccess**

Number of CPE ranging responses sent.

#### **13.1.2.4.3.1.6 wranIfBsRangingSuccessRate**

Success rate of ranging attempts:  $wranIfBsRangingSuccessRate = 100 \times (wranIfBsNumRangingSuccess / wranIfBsNumRangingAttempt)$ .

### **13.1.2.4.4 wranIfBsThroughputMetricsTable**

This MIB object provides a table to record peak/average data rate. This table is made up of multiple entries, one for each sector of a BS. Each entry is defined by `wranIfBsThroughputMetricsEntry`.

#### **13.1.2.4.4.1 wranIfBsThroughputMetricsEntry**

This object is a compound object that contains an entry in `wranIfBsThroughputMetricsTable`.

##### **13.1.2.4.4.1.1 wranIfBsAvgDsUserThroughput**

This records the average user throughput in the DS. This is a function of the number of octets of MAC SDUs transmitted by the BS to CPEs over time.

##### **13.1.2.4.4.1.2 wranIfBsAvgUsUserThroughput**

This records the average user throughput in the US. This is a function of the number of octets of MAC SDUs transmitted by CPEs to the BS over time.

##### **13.1.2.4.4.1.3 wranIfBsAvgDsMacThroughput**

This records the average MAC throughput in the DS. This is a function of the number of octets of MAC PDUs transmitted by the BS to CPEs over time.

#### **13.1.2.4.4.1.4 wranIfBsAvgUsMacThroughput**

This records the average MAC throughput in the US. This is a function of the number of octets of MAC PDUs transmitted by the CPEs to the BS over time.

#### **13.1.2.4.4.1.5 wranIfBsAvgDsPhyThroughput**

This records the average PHY throughput in the DS. This is a function of the number of burst octets (e.g., MAC PDU + PHYoverhead) transmitted by the BS to CPEs over time.

#### **13.1.2.4.4.1.6 wranIfBsAvgUsPhyThroughput**

This records the average PHY throughput in the US. This is a function of the number of octets of (e.g., MAC PDU + PHYoverhead) transmitted by the CPEs to the BS over time.

#### **13.1.2.4.4.1.7 wranIfBsPeakDsUserThroughput**

This records the Peak user throughput in the DS. This is the maximum of a function representing the number of octets of MAC SDUs transmitted by the BS to CPEs over time.

#### **13.1.2.4.4.1.8 wranIfBsPeakUsUserThroughput**

This records the peak user throughput in the US. This is a maximum of a function of the number of octets of MAC SDUs transmitted by CPEs to the BS over time.

#### **13.1.2.4.4.1.9 wranIfBsPeakDsMacThroughput**

This records the peak MAC throughput in the DS. This is a maximum of a function of the number of octets of MAC PDUs transmitted by the BS to CPEs over time.

#### **13.1.2.4.4.1.10 wranIfBsPeakUsMacThroughput**

This records the peak MAC throughput in the US. This is a maximum of a function of the number of octets of MAC PDUs transmitted by the CPEs to the BS over time.

#### **13.1.2.4.4.1.11 wranIfBsPeakDsPhyThroughput**

This records the peak PHY throughput in the DS. This is a maximum of the function of the number of burst octets (e.g., MAC PDU + PHYoverhead) transmitted by the BS to CPEs over time.

#### **13.1.2.4.4.1.12 wranIfBsAvgUsPhyThroughput**

This records the peak PHY throughput in the US. This is a maximum of the function of the number of octets of (e.g., MAC PDU + PHYoverhead) transmitted by the CPEs to the BS over time.

#### **13.1.2.4.4.1.13 wranIfBsAvgDsCellEdgeThroughput**

This records the average MAC throughput in the DS transmitted with the most robust MCS. This is a function of the number of octets of MAC PDUs transmitted by the BS to CPEs over time using QPSK.

#### **13.1.2.4.4.1.14 wranIfBsAvgUsCellEdgeThroughput**

This records the average MAC throughput in the US transmitted with the most robust MCS. This is a function of the number of octets of MAC PDUs transmitted by CPEs to the BS over time using QPSK.

#### **13.1.2.4.4.1.15 wranIfBsNumThroughputMeasurements**

This tracks the number of throughput measurements.

### **13.1.2.4.5 wranIfBsNetworkEntryMetricsTable**

This MIB provides a table that contains latency (time) for network entry and network re-entry. Network entry time is measured as the time in between receiving the first RNG-REQ from a CPE until the CPE has received the REG-RSP. Network re-entry process is governed by policies in the Policy Table 234. This could require execution of the entire network re-entry process if the CPE is forced to re-initialize itself or it could only require execution of the CPE initialization procedure through the ranging process (see 7.14.2). There is one entry in the table for each BS sector. Each entry is defined by wranIfBsNetworkEntryMetricsEntry.

#### **13.1.2.4.5.1 wranIfBsNetworkEntryMetricsEntry**

This object is a compound object that represents an entry in wranIfBsNetworkEntryMetricsTable.

##### **13.1.2.4.5.1.1 wranIfBsAvgNetworkEntryLatency**

Average network entry latency, measured in seconds.

##### **13.1.2.4.5.1.2 wranIfBsMaxNetworkEntryLatency**

Maximum network entry latency, measured in seconds.

##### **13.1.2.4.5.1.3 wranIfBsAvgNetworkReEntryLatency**

Average network re-entry latency, measured in seconds.

##### **13.1.2.4.5.1.4 wranIfBsMaxNetworkReEntryLatency**

Maximum network re-entry latency, measured in seconds.

### **13.1.2.4.5.1.5 wranIfBsNumNetworkEntryAttempts**

Number of network entry attempts.

### **13.1.2.4.5.1.6 wranIfBsNumNetworkReEntryAttempts**

Number of network re-entry attempts.

## **13.1.2.4.6 wranIfBsPacketErrorRateTable**

This MIB object contains information about packet error rate measurements. The table is made up of multiple entries, one for each BS sector. Each entry is defined by wranIfBsPacketErrorRateEntry.

### **13.1.2.4.6.1 wranIfBsPacketErrorRateEntry**

This object is a compound object that defines an entry in wranIfBsPacketErrorRateTable.

#### **13.1.2.4.6.1.1 wranIfBsDsPacketsSent**

Total number of MAC SDUs that the BS has sent.

#### **13.1.2.4.6.1.2 wranIfBsDsPacketsErrored**

Total number of MAC SDUs, including ARQ blocks, that have not been acknowledged.

#### **13.1.2.4.6.1.3 wranIfBsDsPacketErrorRate**

wranIfBsDsPacketErrorRate = (wranIfBsDsPacketsErrored /  
wranIfBsDsPacketsSent) × 10000000, in units of 1e-7.

#### **13.1.2.4.6.1.4 wranIfBsUsPacketsReceived**

Total number of MAC SDUs that the BS has received.

#### **13.1.2.4.6.1.5 wranIfBsUsPacketsErrored**

Total number of MAC SDUs with CRC errors and/or ARQ blocks that required re-transmission that has been received by the BS.

### **13.1.2.4.6.1.6 wranIfBsUsPacketErrorRate**

wranIfBsUsPacketErrorRate = (wranIfBsUsPacketsErrored / wranIfBsUsPacketsReceived) × 10000000, in units of 1e-7.

### **13.1.2.4.7 wranIfBsUserMetricsTable**

This MIB object provides a table to track the current status of users in the cell. There is one row for each BS sector. Each entry is defined by `wranIfBsUserMetricsEntry`.

#### **13.1.2.4.7.1 wranIfBsUserMetricsEntry**

This object is a compound object that defines a row in `wranIfBsUserMetricsTable`.

##### **13.1.2.4.7.1.1 wranIfBsNumActiveUsers**

Total number of users that have CIDs with active SFs on them.

##### **13.1.2.4.7.1.2 wranIfBsNumTotalUsers**

Total number of users that have completed the registration (REG-REQ/RSP) process.

##### **13.1.2.4.7.1.3 wranIfBsNumTimeoutUsers**

Total number of users that are in Timeout.

### **13.1.2.4.8 wranIfBsServiceFlowMetricsTable**

This MIB object provides a table to track metrics related to service flows. This table is made up of multiple entries, one entry for each BS sector. Each entry is defined by `wranIfBsServiceFlowMetricsEntry`.

#### **13.1.2.4.8.1 wranIfBsServiceFlowMetricsEntry**

This object is a compound object that represents an entry in `wranIfBsServiceFlowMetricsTable`.

##### **13.1.2.4.8.1.1 wranIfBsNumDsaReq**

Number of DSA-REQ counted during reporting period.

##### **13.1.2.4.8.1.2 wranIfBsNumDsaReqSuccess**

Number of successful SF activations counted during reporting period. A successful activation of a SF is noted when a BS receives a DSA-RSP with a successful confirmation in response to a particular DSA-REQ.

#### **13.1.2.4.8.1.3 wranIfBsNumDsaSuccessRate**

wranIfBsNumDsaSuccessRate = ( wranIfBsNumDsaReqSuccess / wranIfBsNumDsaReq )  
 $\times 100.$

#### **13.1.2.4.8.1.4 wranIfBsNumDscReq**

Number of DSC-REQ BS sent during reporting period.

#### **13.1.2.4.8.1.5 wranIfBsNumDscReqSuccess**

Number of successful SF modifications counted during reporting period. A successful modification of a SF is noted when a BS receives a DSC-RSP with a successful confirmation in response to a particular DSC-REQ.

#### **13.1.2.4.8.1.6 wranIfBsNumDscSuccessRate**

wranIfBsNumDscSuccessRate = ( wranIfBsNumDscReqSuccess / wranIfBsNumDscReq )  
 $\times 100.$

#### **13.1.2.4.8.1.7 wranIfBsNumDsdReq**

Number of DSD-REQ BS sent during reporting period.

#### **13.1.2.4.8.1.8 wranIfBsNumDsdReqSuccess**

Number of successful SF deletions counted during reporting period. A successful deletion of a SF is noted when a BS receives a DSD-RSP with a successful confirmation in response to a particular DSD-REQ.

#### **13.1.2.4.8.1.9 wranIfBsNumDsdSuccessRate**

wranIfBsNumDsdSuccessRate = ( wranIfBsNumDsdReqSuccess / wranIfBsNumDsdReq )  
 $\times 100.$

#### **13.1.2.4.8.1.10 wranIfBsMaxActiveServiceFlow**

Maximum number of service flows active during reporting period.

#### **13.1.2.4.8.1.11 wranIfBsAvgActiveServiceFlow**

Average number of service flows active during reporting period.

**13.1.2.4.8.1.12 wranIfBsMaxProvisionedServiceFlow**

Maximum number of pre-provisioned service flows active during reporting period.

**13.1.2.4.8.1.13 wranIfBsAvgProvisionedServiceFlow**

Average number of pre-provisioned service flows active during reporting period.

**13.1.2.4.8.1.14 wranIfBsMaxDsServiceFlow**

Maximum number of DS service flows active during reporting period.

**13.1.2.4.8.1.15 wranIfBsMaxUsServiceFlow**

Maximum number of US service flows active during reporting period.

**13.1.2.4.8.1.16 wranIfBsAvgDsServiceFlow**

Average number of DS service flows active during reporting period.

**13.1.2.4.8.1.17 wranIfBsAvgUsServiceFlow**

Average number of US service flows active during reporting period.

**13.1.2.4.8.1.18 wranIfBsNumSfidAllocated**

Number of SFIDs allocated during reporting period.

**13.1.2.4.9 wranIfBsArqMetricsTable**

This MIB provides a table to track performance of ARQ. This table is made up of multiple entries, one for each BS sector. Each entry is defined by wranIfBsArqMetricsEntry.

**13.1.2.4.9.1 wranIfBsArqMetricsEntry**

This object is a compound object that provides a definition of entries in wranIfBsArqMetricsTable.

**13.1.2.4.9.1.1 wranIfBsDsNumArqBlocks**

Total number of ARQ blocks, including retransmissions, that the BS has sent during reporting period.

**13.1.2.4.9.1.2 wranIfBsDsNumArqBlocksDropped**

Total number of ARQ blocks that were dropped, due to unsuccessful attempts at retransmission.

#### **13.1.2.4.9.1.3 wranIfBsDsArqBlockErrorRate**

$wranIfBsDsArqBlockErrorRate = (wranIfBsDsNumArqBlocksDropped / wranIfBsDsNumArqBlocks) \times 10000000$ , in units of 1e-7.

#### **13.1.2.4.9.1.4 wranIfBsDsNumArqBlockRetransmissions**

Total number of ARQ blocks that were retransmitted.

#### **13.1.2.4.9.1.5 wranIfBsDsArqBlockEfficiency**

$wranIfBsDsArqBlockEfficiency = (wranIfBsDsNumArqBlockRetransmissions / wranIfBsDsNumArqBlocks) \times 10000000$ , in units of 1e-7.

#### **13.1.2.4.9.1.6 wranIfBsUsNumArqBlocks**

Total number of ARQ blocks, including retransmissions, that the BS has received during reporting period.

#### **13.1.2.4.9.1.7 wranIfBsUsNumArqBlockRetransmissions**

Total number of ARQ blocks that were retransmitted by CPE during reporting period.

#### **13.1.2.4.9.1.8 wranIfBsDsArqBlockEfficiency**

$wranIfBsUsArqBlockEfficiency = (wranIfBsUsNumArqBlockRetransmissions / wranIfBsUsNumArqBlocks) \times 10000000$ , in units of 1e-7.

### **13.1.2.4.10 wranIfBsAuthenticationMetricsTable**

This MIB provides a table to track the number of authentication/encryption errors that occur. This information can be used to detect if an active attack on the system is occurring. This table is made up of multiple entries, one for each BS sector. Each entry is defined by wranIfBsAuthenticationMetricsEntry.

#### **13.1.2.4.10.1 wranIfBsAuthenticationMetricsEntry**

This object is a compound object that defines an entry in wranIfBsAuthenticationMetricsTable.

##### **13.1.2.4.10.1.1 wranIfBsMangmentAuthenticationErrors**

A counter that gets incremented every time a management message from the CPE cannot be properly authenticated.

#### **13.1.2.4.10.1.2 wranIfBsDataAuthenticationErrors**

A counter that gets incremented every time a data message from the CPE can not be properly authenticated.

#### **13.1.2.4.10.1.3 wranIfBsWiMicAuthenticationErrors**

A counter that gets incremented every time a wireless microphone beacon (MSF1+MSF2+MSF3) cannot be properly authenticated.

#### **13.1.2.4.10.1.4 wranIfBsCbpAuthenticationErrors**

A counter that gets incremented every time a CBP from a neighboring WRAN cannot be properly authenticated.

### **13.1.2.4.11 wranIfBsCoexistenceStatusTable**

This MIB provides a table to track the ongoing coexistence (Frame Contention) transactions. This table is made up of multiple entries, one for each ongoing transaction. Each entry is defined by wranIfBsCoexistenceStatusEntry. If a Frame Contention Destination receives a FC-REQ from a source on a channel for which it already has a message from, then the existing entry is updated

#### **13.1.2.4.11.1 wranIfBsCoexistenceStatusEntry**

This object is a compound object that defines an entry in wranIfBsCoexistenceStatusTable.

##### **13.1.2.4.11.1.1 wranIfBsContentionChannel**

Channel # on which FC-REQ was received (i.e., channel that is being contented for).

##### **13.1.2.4.11.1.2 wranIfBsFrameContentionSourceID**

BS ID (MAC Address) of the transmitter of a FC-REQ message in a CBP burst. This is pulled from the SCH data in the CBP MAC PDU header pulled from the CBP burst containing the FC-REQ.

##### **13.1.2.4.11.1.3 wranIfBsFrameContentionSeqNum**

Sequence # field of the received FC-REQ message.

##### **13.1.2.4.11.1.4 wranIfBsFrameContentionNumber**

Value of the Frame Contention Number (FCN) in the FC-REQ.

#### **13.1.2.4.11.1.5 wranIfBsContentionReqFrameIndexVector**

Bitmap index of data frames within a superframe that a Frame Contention Source is requesting, to be scheduled in the next superframe after the current one.

#### **13.1.2.4.12wranIfBsCoexistenceSourceTable**

This MIB provides a table to track what neighbor BSs are attempting a coexistence (Frame Contention) transaction with a particular BS or have communicated other information (e.g., Backup/Candidate channel list) via CBP. Each entry is defined by `wranIfBsCoexistenceSourceEntry`.

##### **13.1.2.4.12.1 wranIfBsCoexistenceSourceEntry**

This object is a compound object that defines an entry in `wranIfBsCoexistenceSourceTable`. When a CBP is received from a neighboring WRAN that already has an entry in the table, the existing entry is updated.

###### **13.1.2.4.12.1.1 wranIfBsMacAddress**

BS ID of the BS that sent the CBP burst; obtained from SCH data in CBP MAC PDU header (see Table 1 and Table 9).

###### **13.1.2.4.12.1.2 wranIfBsSchDataIndex**

SCH Data Index field of CBP MAC PDU header. It indicates the length of and an indication of what SCH fields comprise the `wranIfBsSchData` in this table.

###### **13.1.2.4.12.1.3 wranIfBsSchData**

SCH Data from CBP MAC PDU header. The length of this field is governed by `wranIfBsSchDataIndex`.

#### **13.1.2.4.13wranIfBsCoexistenceResourceListTable**

This MIB provides a table to track the resources being used by neighboring WRANs. This includes the Backup/Candidate Lists being transmitted by neighboring WRANs, as well as the DS/US split. This table is made up of multiple entries, defined by `wranIfBsChannelListEntry`. A BS may keep an entry in this table for its own settings.

##### **13.1.2.4.13.1 wranIfBsCoexistenceResourceListEntry**

This object is a compound object that defines an entry in `wranIfBsChannelListTable`. When a CBP is received from a neighboring WRAN that already has an entry in the table, the existing entry is updated.

#### **13.1.2.4.13.1.1 wranIfBsMacAddress**

BS ID of the BS that sent the CBP burst, obtained from SCH data in CBP MAC PDU header (see Table 1 and Table 9).

#### **13.1.2.4.13.1.2 wranIfBsSelfCoexistenceCapacityIndicator**

Field within SCH Data field within CBP MAC PDU header that indicates what coexistence capabilities a BS supports. If this field is 0000, the remaining fields of this entry are null.

#### **13.1.2.4.13.1.3 wranIfBsNumBackupCandidateChannels**

Number of backup and candidate channels in the wranIfBsBackupCandidateChannelList.

#### **13.1.2.4.13.1.4 wranIfBsNumBackupChannels**

Number of backup channels in wranIfBsBackupCandidateChannelList.

#### **13.1.2.4.13.1.5 wranIfBsBackupCandidateChannelList**

This object is a vector, of the length = 8 bits × wranIfBsNumBackupCandidateChannels, that contains the backup/candidate channel list received in a CBP burst from a neighbor WRAN.

#### **13.1.2.4.13.1.6 wranIfBsCurrentDSUSSplit**

Current US/DS split indicated in SCH data of CBP MAC PDU header received from neighbor WRAN.

#### **13.1.2.4.13.1.7 wranIfBsClaimedDSUSSplit**

Claimed US/DS split indicated in SCH data of CBP MAC PDU header received from neighbor WRAN.

#### **13.1.2.4.13.1.8 wranIfBsDSUSChangeOffset**

DS/US Change Offset indicated in SCH data of CBP MAC PDU header received from neighbor WRAN.

#### **13.1.2.4.13.1.9 wranIfBsFrameAllocationMap**

Indicate which frames in a superframe are allocated to the neighbor WRAN BS.

#### **13.1.2.4.13.1.10 wranIfBsScwCycleLength**

SCW Cycle Length being applied by neighbor WRAN.

#### **13.1.2.4.13.1.11 wranIfBsScwCycleOffset**

SCW Cycle Offset being applied by neighbor WRAN.

#### **13.1.2.4.13.1.12 wranIfBsScwCycleFrameBitmap**

DS/US Change Offset indicated in SCH data of CBP MAC PDU header received from neighbor WRAN.

#### **13.1.2.4.14 wranIfBsCoexistenceCurrentConfigTable**

This MIB provides a table to track what frame allocation has been awarded to a frame contention winner, and when the awarded resource will be released. It is made up of multiple entries, one for each channel that frame contention procedure was executed on, as defined in `wranIfBsCoexistenceCurrentConfigEntry`. When a frame contention winner is selected, the corresponding entries in `wranIfCoexistenceStatusTable` are removed.

##### **13.1.2.4.14.1 wranIfBsCoexistenceCurrentConfigEntry**

This object is a compound object that defines an entry in `wranIfBsCoexistenceCurrentConfigTable` when a frame contention winner is selected and entry into this table is filled. When frames are reclaimed, the corresponding entry in this table is removed.

###### **13.1.2.4.14.1.1 wranIfBsContentionChannel**

Channel # on which the frame contention was executed.

###### **13.1.2.4.14.1.2 wranIfBsFrameContentionSourceID**

BS ID of frame contention source that has won contention

###### **13.1.2.4.14.1.3 wranIfBsAwardedSeqNum**

Sequence number of the frame contention winner from the FC-REQ message.

###### **13.1.2.4.14.1.4 wranIfBsContentionRspFrameIndexVector**

Sequence number of the frame contention winner from the FC-REQ message.

###### **13.1.2.4.14.1.5 wranIfBsContentionRspFrameReleaseTime**

Starting from the next superframe, the number of superframes after which the TV channel shall be released by the frame contention destination.

### **13.1.2.5 wranIfBsScm**

This MIB group has objects related to Security Management. The following tables are included in this MIB object:

- **wranIfBsScmCapabilityConfiguration**: Contains information on what cryptographic suite capabilities are supported on the BS.
- **wranIfBsCpeCapabilityConfigTable**: Contains information on what cryptographic suite capabilities are supported on CPEs.
- **wranIfBsScmAuthConfigTable**: Contains information on configuration of SCM attributes, e.g., timers and constants defined in Clause 8.
- **wranIfBsCpeScmAuthStatusTable**: Contains information related to the current status of CPE authentication.
- **wranIfBsCpeScmSaConfigTable**: Contains information related to attributes of SAs that are configured on CPEs.
- **wranIfBsCpeTekRefreshTable**: Contains information related to ongoing SCM Key-Request/Reply transactions.
- **wranIfBsCBPAuthCACertTable**: Contains CA root certificates used in CBP Authentication
- **wranIfBsCBPAuthBsImplicitCertTable**: Contains BS implicit certificates used in CBP Authentication
- **wranIfBsWiMicAuthCertTable**: Contains implicit certificates contained in MSF3 of captured wireless microphone beacons.

#### **13.1.2.5.1 wranIfBsScmCapabilityConfiguration**

This MIB provides a bitmap that describes the cryptographic suites that the BS supports. The list of suites is provided in Table 193.

#### **13.1.2.5.2 wranIfBsCpeScmCapabilityConfigTable**

This MIB provides a table that provides a listing for the security capabilities for each CPE. Each CPE stores this Table. At the BS, this table is made up of multiple entries, one for each CPE. Entries on the BS Table do not contain the **wranIfBsCpeEapTlsTtlsCredential** object. Each entry is defined by **wranIfBsCpeScmCapabilityConfigEntry**. The list of capabilities is listed in Table 193.

#### **13.1.2.5.2.1 wranIfBsCpeScmCapabilityConfigEntry**

This object is a compound object that provides the definition of the entries **wranIfBsCpeScmCapabilityConfigTable**.

##### **13.1.2.5.2.1.1 wranIfBsCpeMacAddress**

The MAC address of the CPE.

### **13.1.2.5.2.1.2 wranIfBsCpeScmCapabilityConfiguration**

This MIB provides a bitmap that describes the cryptographic suites that the CPE supports. The list of suites is provided in Table 193.

### **13.1.2.5.3 wranIfBsScmAuthConfigTable**

This MIB provides a table that provides the configuration of the SCM attributes (e.g., timers and other items relating to the authentication process). This table is made up of one entry, defined by wranIfBsScmAuthConfigEntry.

#### **13.1.2.5.3.1 wranIfBsScmAuthConfigEntry**

This object is a compound object that defines an entry in wranIfBsScmAuthConfigTable.

##### **13.1.2.5.3.1.1 wranIfBsT36**

EAP Authentication Timer, T36.

##### **13.1.2.5.3.1.2 wranIfBsT37**

Authentication Grace Timer, T37.

##### **13.1.2.5.3.1.3 wranIfBsMaxNumAuthAttempts**

Maximum # of Authentication Attempts.

##### **13.1.2.5.3.1.4 wranIfBsT38**

Operational Wait Timeout, T38.

##### **13.1.2.5.3.1.5 wranIfBsT39**

Rekey Wait Timeout, T39.

##### **13.1.2.5.3.1.6 wranIfBsT40**

GTEK/TEK Grace time, T40.

##### **13.1.2.5.3.1.7 wranIfBsAkLifetime**

Lifetime BS assigns to new AK.

### **13.1.2.5.3.1.8 wranIfBsTekLifetime**

Lifetime BS assigns to new TEK.

### **13.1.2.5.3.1.9 wranIfBsMaxNumSa**

Maximum number of SAs for which a CPE can be configured.

### **13.1.2.5.3.1.10 wranIfBsT17**

Time for the CPE to complete authentication and key exchange.

## **13.1.2.5.4 wranIfBsCpeScmAuthStatusTable**

This object provides a table that stores information regarding the current state of the CPE's authentication state machine. This table is stored on each CPE and made up of one entry, defined by wranIfBsCpeScmAuthStatusEntry.

### **13.1.2.5.4.1 wranIfBsCpeScmAuthStatusEntry**

This object is a compound object that defines an entry in wranIfBsCpeScmAuthStatusTable.

#### **13.1.2.5.4.1.1 wranIfBsCpeScmAuthStatus**

State of CPE's authentication state machine (see 8.2.2.1) that CPE is in.

#### **13.1.2.5.4.1.2 wranIfBsCpeScmAuthRecentEvent**

Indication of the most recent event (see 8.2.2.4) that has occurred in the ASM.

#### **13.1.2.5.4.1.3 wranIfBsCpeScmNumAuthAttempts**

Current # of EAP authentication attempts.

#### **13.1.2.5.4.1.4 wranIfBsCpeScmAuthRecentMsg**

Contents of most recent authentication message, either EAP-Start or EAP-Transfer.

#### **13.1.2.5.4.1.5 wranIfBsCpeScmAuthEapAuthTimerExpiration**

Indication of when EAP Authentication timer for pending EAP-Start or EAP-Transfer message is to expire.

#### **13.1.2.5.4.1.6 wranIfBsCpeScmAuthGraceTimer1**

Indication of when Authentication Grace timer for the current (active) AK will expire.

#### **13.1.2.5.4.1.7 wranIfBsCpeScmAuthGraceTimer2**

Indication of when Authentication Grace timer for second generation (non-active) AK will expire.

#### **13.1.2.5.4.1.8 wranIfBsCpeScmAk1Lifetime**

Remaining lifetime for current (active) AK will expire.

#### **13.1.2.5.4.1.9 wranIfBsCpeScmAk2Lifetime**

Remaining lifetime for second generation (non-active) AK will expire.

#### **13.1.2.5.4.1.10 wranIfBsCpeScmConfigRequest**

Contents of SCM configuration request (see Table 187) sent by CPE, upon initial authentication or reauthentication, to AAA server.

#### **13.1.2.5.4.1.11 wranIfBsCpeScmConfigReply**

Contents of SCM configuration reply (see Table 188) sent by AAA server, upon confirmation of initial authentication or reauthentication, to CPE.

### **13.1.2.5 wranIfBsCpeScmSaConfigTable**

This object provides a table that provides the configuration of the SA attributes that are related to SAs configured on each CPE. This table is maintained on each CPE as well as on the BS. On the BS, this table represents the configuration of SAs for all CPEs under its control. This table is made up of one entry for each SA that a CPE supports. Each entry is defined by `wranIfBsCpeScmSaConfigEntry`.

#### **13.1.2.5.5.1 wranIfBsCpeScmaConfigEntry**

This object is a compound object that defines an entry in `wranIfBsCpeScmSaConfigTable`.

##### **13.1.2.5.5.1.1 wranIfBsCpeMacAddress**

MAC address of the CPE.

##### **13.1.2.5.5.1.2 wranIfBsCpeSaid**

SAID of SA to which this entry refers.

**13.1.2.5.5.1.3 wranIfBsCpeSaType**

Type of SA, either Null, Primary, Secondary, or Group.

**13.1.2.5.5.1.4 wranIfBsCpeCryptoSuiteCapability**

This MIB provides a bitmap that describes the cryptographic suites that the CPE supports for this particular SA. The complete list of suites is provided in Table 193.

**13.1.2.5.5.1.5 wranIfBsCpeTekN-1SequenceNumber**

The EKS value for the current (active) generation of the two TEKs that are configured for this SA.

**13.1.2.5.5.1.6 wranIfBsCpeTekN-1Lifetime**

The lifetime, in units of time (e.g., seconds), for the current (active) generation of the two TEKs that are configured for this SA.

**13.1.2.5.5.1.7 wranIfBsCpeTekN-1Pn**

Current value of the PN counter for the current (active) generation of the two TEKs that are configured for this SA.

**13.1.2.5.5.1.8 wranIfBsCpeTekN-1ExpireTime**

Time at which current (active) generation of the two TEKS configured for an SA will expire. This time is calculated as a function of the Reception Time of Key Reply with TEK N-1 + TEK N-1 Lifetime.

**13.1.2.5.5.1.9 wranIfBsCpeTekNSequenceNumber**

The EKS value for the second (non-active) generation of the two TEKs that are configured for this SA.

**13.1.2.5.5.1.10 wranIfBsCpeTekNLifetime**

The lifetime, in units of time (e.g., seconds), for the second (non-active) generation of the two TEKs that are configured for this SA.

**13.1.2.5.5.1.11 wranIfBsCpeTekNPn**

Current value of the PN counter for the second (non-active) generation of the two TEKs that are configured for this SA.

### **13.1.2.5.5.1.12 wranIfBsCpeTekNExpireTime**

Time at which second (non-active) generation of the two TEKS configured for an SA will expire. This time is calculated as a function of the Reception Time of Key Reply with TEK N + TEK N Lifetime.

### **13.1.2.5.6 wranIfBsCpeTekRefreshTable**

This MIB object provides a table to track information related to ongoing Key-Request transactions. This table has one entry for each current SCM Key-Request transaction. Each entry is defined by wranIfBsCpeTekRefreshEntry.

#### **13.1.2.5.6.1 wranIfBsCpeTekRefreshEntry**

This object is a compound object that provides a definition for entries in wranIfBsCpeTekRefreshTable.

##### **13.1.2.5.6.1.1 wranIfBsCpeScmReqId**

Value of SCM Identifier field of SCM REQ that carried the corresponding Key-Request message.

##### **13.1.2.5.6.1.2 wranIfBsCpeScmKeyReqKeySeqNum**

Key Sequence Number of Key-Sequence message.

##### **13.1.2.5.6.1.3 wranIfBsCpeScmKeyReqSaid**

SAID for which keys are being requested.

##### **13.1.2.5.6.1.4 wranIfBsCpeScmKeyReqGroupKeyIndicator**

Indicator of whether or not Key-Request was for a GSA or not.

##### **13.1.2.5.6.1.5 wranIfBsCpeScmKeyReqCpeRandom**

Random number generated by CPE and sent in the Key-Request.

### **13.1.2.5.7 wranIfBsCBPAuthCACertTable**

This object provides a table to CA root certificates (see 8.6.2.3) used to validate CBP BS implicit certificates. There will be one entry for each CA for which a root certificate is installed. Each entry is defined by wranIfBsCBPAuthCACertEntry.

### **13.1.2.5.7.1 wranIfBsCBPAuthCACertEntry**

This object is a compound object that provides a definition for entries in wranIfBsCBPAuthCACertTable.

#### **13.1.2.5.7.1.1 wranIfBsCBPAuthCACertCAID**

CA ID, identifier of CA in CA root certificate.

#### **13.1.2.5.7.1.2 wranIfBsCBPAuthCACertKeyID**

Key ID, identifier of assigned to public key reconstruction data in CA root certificate.

#### **13.1.2.5.7.1.3 wranIfBsCBPAuthCACertKeyValidityDate**

Key Validity Date (Not Before), date/time at which CA root certificate becomes valid.

#### **13.1.2.5.7.1.4 wranIfBsCBPAuthCACertKeyValidityTimePeriod**

Key Validity Time Period, length of time from Key Validity Date (Not Before) in which CA root certificate is valid.

#### **13.1.2.5.7.1.5 wranIfBsCBPAuthCACertVersion**

Version of CBP Authentication being applied that the CA root certificate supports.

#### **13.1.2.5.7.1.6 wranIfBsCBPAuthCACertECDomainParameters**

Elliptic Curve domain parameters that the CA uses.

#### **13.1.2.5.7.1.7 wranIfBsCBPAuthCACertCAPubKrd**

Public Key Reconstruction Data that can be used to generate the public key associated with CA root certificate.

#### **13.1.2.5.7.1.8 wranIfBsCBPAuthCACertCAPubK**

Public Key reconstructed from wranIfBsCBPAuthCACertCAPubKrd associated with CA root certificate.

### **13.1.2.5.8 wranIfBsCBPAuthBslImplicitCertTable**

This object provides a table to store BS implicit certificates for neighbor WRANs that make use of CBP authentication. There will be one entry for each BS whose implicit certificate is installed

(via this object) on the BS or received by CERT-REQ/RSP. Each entry is defined by wranIfBsCBPAuthBsImplicitCertEntry.

#### **13.1.2.5.8.1 wranIfBsCBPAuthBsImplicitCertEntry**

This object is a compound object that provides a definition for entries in wranIfBsCBPAuthBsImplicitCertTable.

##### **13.1.2.5.8.1.1 wranIfBsCBPAuthBsImplicitCertBsID**

BS ID (MAC Address) of BS that implicit certificate belongs to.

##### **13.1.2.5.8.1.2 wranIfBsCBPAuthBsImplicitCertCAID**

CA ID, identifier of CA in BS implicit certificate.

##### **13.1.2.5.8.1.3 wranIfBsCBPAuthBsImplicitCertKeyID**

Key ID, identifier of assigned to public key reconstruction data in BS implicit certificate.

##### **13.1.2.5.8.1.4 wranIfBsCBPAuthBsImplicitCertKeyValidityDate**

Key Validity Date (Not Before), date/time at which BS implicit certificate becomes valid.

##### **13.1.2.5.8.1.5 wranIfBsCBPAuthBsImplicitCertKeyValidityTimePeriod**

Key Validity Time Period, length of time from Key Validity Date (Not Before) in which BS implicit certificate is valid.

##### **13.1.2.5.8.1.6 wranIfBsCBPAuthBsImplicitCertVersion**

Version of CBP Authentication being applied that the BS implicit certificate supports.

##### **13.1.2.5.8.1.7 wranIfBsCBPAuthBsImplicitCertPubKrd**

Public Key Reconstruction Data that can be used to generate the public key associated with BS implicit certificate.

##### **13.1.2.5.8.1.8 wranIfBsCBPAuthBsImplicitCertPubK**

Public Key reconstructed from wranIfBsCBPAuthBsImplicitCertPubKrd that can be used to generate the public key associated with BS implicit certificate.

### **13.1.2.5.8.1.9 wranIfBsCBPAuthBsImplicitCertPrKrd**

Private Key Reconstruction Data associated with a BS's implicit certificate. This field is only applicable for the entry into 13.1.2.5.8 pertaining a BS's own implicit certificate Private Key Reconstruction Data, and not any other BSs. A BS may keep an entry for its own implicit certificate in this object. In this case, wranIfBsCBPAuthBsImplicitCertPrKrd and wranIfBsCBPAuthBsImplicitCertPrK are only applicable to a BS's own entry and shall be null for all other BS's implicit certificate entries.

### **13.1.2.5.8.1.10 wranIfBsCBPAuthBsImplicitCertPrK**

Private Key reconstructed from wranIfBsCBPAuthBsImplicitCertPrKrd associated with a BS's implicit certificate. This field is only applicable for the entry into 13.1.2.5.8 pertaining a BS's own implicit certificate Private Key, and not any other BSs.

## **13.1.2.5.9 wranIfBsWiMicAuthCertTable**

This object provides a table to store wireless microphone implicit certificates contained in MSF3 of decoded wireless microphone beacons. This table is made up of multiple entries, one defined for each unique wireless microphone beacon implicit certificate. Each entry is defined by wranIfBsWiMicAuthCertEntry. Entries are added to this table when a wireless microphone beacon (MSF1+MSF2+MSF3) has been successfully received and decode.

### **13.1.2.5.9.1 wranIfBsWiMicAuthCertEntry**

This object is a compound object that provides a definition for entries in wranIfBsWiMicAuthCertTable.

#### **13.1.2.5.9.1.1 wranIfBsWiMicAuthSrcAddress**

Source Address from MSF1 of received wireless microphone beacon. It is stored as a 48-bit IEEE conformant MAC address that identifies the beaconing device associated with the implicit certificate.

#### **13.1.2.5.9.1.2 wranIfBsWiMicAuthImplicitCert**

Wireless microphone beacon implicit certificate obtained from MSF3 of received wireless microphone beacon. Format of implicit certificate is defined in 7.5.5 of IEEE Std 802.22.1-2010.

## **13.1.3 wranIfBsSfMgmt**

This MIB group provides objects for managing service flows in the network.

Classification rules to be defined by the operator shall be downloadable to the BS and CPEs in a uniform and standardized format. The resulting behavior of a given classification rule shall be standardized and implementation independent. This shall be done by the MIB.

In this MIB group the following tables are defined:

- **wranIfBsProvSfTable**: Contains information about service flows provisioned by the NCMS.
- **wranIfBsScTable**: Contains the QoS parameter set for service flows defined for the supported service classes.
- **wranIfBsSfTable**: Contains information about dynamic service flows that are created/torn-down on-the-fly.
- **wranIfBsProvClassifierRuleTable**: Contains information about classifier rules as applied to service flows provisioned by the NCMS.
- **wranIfBsClassifierRuleTable**: Contains information about classifier rules as applied to service flows applied to dynamic service flows.

### **13.1.3.1 wranIfBsProvSfTable**

This MIB object defines the profiles for services that are provisioned by the NCMS. Services flow that are provisioned for a particular CPE are tied to that CPE via that CPE's MAC Address. This table is made up of multiple entries, each specific to a particular provisioned service flow. Each entry is defined by **wranIfBsProvSfEntry**.

The QoS parameters for provisioned service flows are mapped to information in **wranIfBsScTable**. Classification rules for provisioned service flows are defined in **wranIfBsProvClassifierRuleTable**.

#### **13.1.3.1.1 wranIfBsProvSfEntry**

This object is a compound object that defines an entry in **wranIfBsProvSfTable**.

##### **13.1.3.1.1.1 wranIfBsCpeProvMacAddress**

MAC address of the CPE for which the service flow is provisioned.

##### **13.1.3.1.1.2 wranIfBsSfId**

Unique identifier for the SF that is provisioned between a BS and a particular CPE.

##### **13.1.3.1.1.3 wranIfBsSfDirection**

Indication of whether or not the SF is an US SF or a DS SF.

##### **13.1.3.1.1.4 wranIfBsScIndex**

Index into a **wranIfBsScTable** entry that indicates the QoS parameter set for this service flow.

##### **13.1.3.1.1.5 wranIfBsCsSpecification**

Indication of which convergence sublayer has been used to encapsulate the higher-layer SDU.

### **13.1.3.1.1.6 wranIfBsProvSfStatus**

Indication of whether or not the provisioned service flow is currently active or not.

### **13.1.3.1.1.7 wranIfBsProvSfProvisioningTime**

If currently active (see 13.1.3.1.1.6), the time at which the service flow was provisioned.

## **13.1.3.2 wranIfBsScTable**

This MIB object provides a table that describes attributes of service flows, such as the QoS parameter set. This table is made up of multiple entries, one for each service class. Each entry is defined by wranIfBsScEntry.

### **13.1.3.2.1 wranIfBsScEntry**

This object is a compound object that defines an entry in wranIfBsScTable.

#### **13.1.3.2.1.1 wranIfBsScIndex**

Index value to uniquely identify an entry into wranIfBsScTable.

#### **13.1.3.2.1.2 wranIfBsQosServiceClassName**

Defines the name of the service class associated with this entry.

#### **13.1.3.2.1.3 wranIfBsQosTrafficPriority**

Priority of service flow. For US, the BS uses this to determine order in which to process BW requests and CPE uses this to determine order for making bandwidth requests.

#### **13.1.3.2.1.4 wranIfBsQosMaxSustainedRate**

Peak information/data rate of SDUs carried by the service flow, defined in units of bits per second.

#### **13.1.3.2.1.5 wranIfBsQosTrafficSize**

If fixed-length SDUs (see 13.1.3.2.1.9) are enabled, this represents the size of SDU assigned to the service flow. If variable-length SDUs (see 13.1.3.2.1.19) are enabled, this represents the average size of SDU assigned to the service flow.

#### **13.1.3.2.1.6 wranIfBsQosMinReservedRate**

Minimum required information/date rate of SDUs carried by the service flow, defined in units of bits per second.

#### **13.1.3.2.1.7 wranIfBsQosToleratedJitter**

The maximum jitter (variation in delay) that can be suffered by the traffic assigned to the service flow.

#### **13.1.3.2.1.8 wranIfBsQosMaxLatency**

The maximum delay that can be suffered by traffic assigned to the service flow.

#### **13.1.3.2.1.9 wranIfBsQosEnableVariableLengthSdus**

Setting this object allows to enable/disable use of variable-length SDUs. Default is to allow use of variable-length SDUs.

#### **13.1.3.2.1.10 wranIfBsQosSchedulingType**

The scheduling type, e.g., BE, nrtPS, rtPS, or UGS. Default is BE.

#### **13.1.3.2.1.11 wranIfBsQosArqEnable**

Setting this object enables/disables ARQ for a service flow. Default is that ARQ is enabled.

#### **13.1.3.2.1.12 wranIfBsQosArqWindowSize**

Indication of the maximum number of unacknowledged fragments at any given time. Only valid if wranIfBsQosArqEnable is set.

#### **13.1.3.2.1.13 wranIfBsQosArqTxRetryTimeout**

Total time before timing out retransmissions of ARQ blocks. For BS, this should include time to compensate for scheduling and the propagation time for transmission.

#### **13.1.3.2.1.14 wranIfBsQosArqRxRetryTimeout**

Total time before timing out reception of ARQ block retransmission. For BS, this should include time to compensate for scheduling and the propagation time for transmission.

#### **13.1.3.2.1.15 wranIfBsQosArqBlockLifetime**

The maximum amount of time that an ARQ block can be held in the ARQ state machine before it is dropped.

### **13.1.3.2.1.16 wranIfBsQosArqSyncLossTimeout**

Timeout for determining that the transmitter and receiver state machines have become unsynchronized.

### **13.1.3.2.1.17 wranIfBsQosArqDeliverInOrderEnable**

Disable/enables ability to deliver ARQ blocks to higher layer at receiver in the same order they were transmitted by the transmitter.

### **13.1.3.2.1.18 wranIfBsQosArqRxPurgeTimeout**

How much the ARQ window is advanced after an ARQ fragment is received.

### **13.1.3.2.1.19 wranIfBsQosArqBlockSizeReq**

This object defines the value of the ARQ block size included in DSA-REQ and REG-REQ messages.

### **13.1.3.2.1.20 wranIfBsQosArqBlockSizeRsp**

This object defines the value of the ARQ block size included in DSA-RSP and REG-RSP messages.

### **13.1.3.2.1.21 wranIfBsQosReqTxPolicy**

This value is a bitmap that enables/disables the following capabilities for a service flow: Use of broadcast BW request for US, use of multicast BW request for US only, piggyback BW requests on data for US transmissions, enable/disable fragmentation, enable/disable packing, and use of CRC for MAC PDU.

### **13.1.3.2.1.22 wranIfBsCsSpecification**

The CS used for encapsulating SDUs for this service flow.

### **13.1.3.2.1.23 wranIfBsTargetSaid**

SAID of SA to which the service flow is being mapped.

### **13.1.3.2.1.24 wranIfBsFsnType**

Indication of the size of the fragment sequence number (FSN) window that is being used for the connection.

## **13.1.3.3 wranIfBsSfTable**

This MIB object provides a table that is used to manage service flows that are currently active between the BS and CPEs. This table is made up of multiple entries, one for each service flow mapped to a particular CPE. Each entry is defined by wranIfBsSfEntry.

### **13.1.3.3.1 wranIfBsSfEntry**

This object is a compound object that provides the definition of an entry into wranIfBsSfTable.

#### **13.1.3.3.1.1 wranIfBsSfSfid**

SFID of the service flow that is assigned to a particular CPE.

#### **13.1.3.3.1.2 wranIfBsSfCid**

CID (SID || FID) to which the service flow is mapped.

#### **13.1.3.3.1.3 wranIfBsSfDirection**

Direction of service flow: BS to CPE (DS), CPE to BS (US).

#### **13.1.3.3.1.4 wranIfBsSfState**

Current state of service flow. Service flow can be in one of four states: inactive, provisioned, admitted (service flow initiated but not received BW yet), or active (service flow initiated and there has been bandwidth assigned to use on service flow).

#### **13.1.3.3.1.5 wranIfBsSfPriority**

Priority of service flow. Priority is used in determining in which order BW requests shall be serviced.

#### **13.1.3.3.1.6 wranIfBsSfMaxSustainedRate**

Peak information/data rate of SDUs carried by the service flow, defined in units of bits per second.

#### **13.1.3.3.1.7 wranIfBsSfTrafficSize**

If fixed-length SDUs (see 13.1.3.2.1.9) are enabled, this represents the size of SDU assigned to the service flow. If variable-length SDUs (see 13.1.3.2.1.9) are enabled, this represents the average size of SDU assigned the service flow.

#### **13.1.3.3.1.8 wranIfBsSfMinReservedRate**

Minimum required information/date rate of SDUs carried by the service flow, defined in units of bits per second.

### **13.1.3.3.1.9 wranIfBsSfToleratedJitter**

The maximum jitter (variation in delay) that can be suffered by the traffic assigned to the service flow.

### **13.1.3.3.1.10 wranIfBsSfMaxLatency**

The maximum delay that can be suffered by traffic assigned to the service flow.

### **13.1.3.3.1.11 wranIfBsSfEnableVariableLengthSdus**

Setting this object allows to enable/disable use of variable-length SDUs. Default is to allow use of variable-length SDUs.

### **13.1.3.3.1.12 wranIfBsSfSchedulingType**

The scheduling type, e.g., BE, nrtPS, rtPS, or UGS. Default is BE.

### **13.1.3.3.1.13 wranIfBsSfArqEnable**

Setting this object enables/disables ARQ for a service flow. Default is that ARQ is enabled.

### **13.1.3.3.1.14 wranIfBsSfArqWindowSize**

Indication of the maximum number of unacknowledged fragments at any given time. Only valid if wranIfBsSfArqEnable is set.

### **13.1.3.3.1.15 wranIfBsSfArqTxRetryTimeout**

Total time before timing out retransmissions of ARQ blocks. For BS, this should include time to compensate for scheduling and the propagation time for transmission.

### **13.1.3.3.1.16 wranIfBsSfArqRxRetryTimeout**

Total time before timing out reception of ARQ block retransmission. For BS, this should include time to compensate for scheduling and the propagation time for transmission.

### **13.1.3.3.1.17 wranIfBsSfArqBlockLifetime**

The maximum amount of time that an ARQ block can be held in the ARQ state machine before it is dropped.

### **13.1.3.3.1.18 wranIfBsSfArqSyncLossTimeout**

Timeout for determining that transmitter and receiver state machines have become unsynchronized.

**13.1.3.3.1.19 wranIfBsSfArqDeliverInOrderEnable**

Disable/enables ability to deliver ARQ blocks to higher layer at receiver in the same order they were transmitted by the transmitter.

**13.1.3.3.1.20 wranIfBsSfArqRxPurgeTimeout**

How much the ARQ window is advanced after an ARQ fragment is received.

**13.1.3.3.1.21 wranIfBsSfArqBlockSizeReq**

This object defines the value of the ARQ block size included in DSA-REQ and REG-REQ messages.

**13.1.3.3.1.22 wranIfBsSfArqBlockSizeRsp**

This object defines the value of the ARQ block size included in DSA-RSP and REG-RSP messages.

**13.1.3.3.1.23 wranIfBsSfReqTxPolicy**

This value is a bitmap that enables/disables the following capabilities for a service flow: Use of broadcast BW request for US, use of multicast BW request for US only, piggyback BW requests on data for US transmissions, enable/disable fragmentation, enable/disable packing, use of CRC for MAC PDU.

**13.1.3.3.1.24 wranIfBsCsSpecification**

The CS used for encapsulating SDUs for this service flow.

**13.1.3.3.1.25 wranIfBsTargetSaid**

SAID of SA to which the service flow is being mapped.

**13.1.3.3.1.26 wranIfBsSfFsnType**

Indication of the size of the fragment sequence number (FSN) window that is being used for the connection.

**13.1.3.4 wranIfBsProvClassifierRuleTable**

This table contains classifier rules that are to be applied to service flows for CPEs that are provisioned by the NCMS. There are multiple entries in this table, one for each classifier rule. Each entry is defined by wranIfBsProvClassifierRuleEntry.

**13.1.3.4.1 wranIfBsProvClassifierRuleEntry**

This object is a compound object that provides the definition of entries in wranIfBsProvClassifierRuleTable.

#### **13.1.3.4.1.1 wranIfBsProvClsfRuleIndex**

Index to uniquely identify an entry in wranIfBsProvClassifierRuleTable.

#### **13.1.3.4.1.2 wranIfBsProvClsfRulePriority**

Priority of the classification rule. This determines the order in which classification rules are applied.

#### **13.1.3.4.1.3 wranIfBsProvClsfRuleIpProtocol**

Value of IP Protocol field. For IPv6 headers, this refers to the next header entry in the last header of the IP header list. The value of this field follows the “Protocol Numbers” specification defined by IANA.

#### **13.1.3.4.1.4 wranIfBsProvClsfRuleIpSrcAddr**

Source IP address from IP header.

#### **13.1.3.4.1.5 wranIfBsProvClsfRuleIpSrcMask**

IP address mask. IP src address (wranIfBsProvClsfRuleIpSrcAddr) is matched when output of applying (bitwise AND) this value to IP src address from IP packet.

#### **13.1.3.4.1.6 wranIfBsProvClsfRuleIpDestAddr**

Destination IP address from IP header.

#### **13.1.3.4.1.7 wranIfBsProvClsfRuleIpDestMask**

IP address mask. IP dest address (wranIfBsProvClsfRuleIpDestAddr) is matched when output of applying (bitwise AND) this value to IP dest address from IP packet.

#### **13.1.3.4.1.8 wranIfBsProvClsfRuleSrcPortStart**

Start (inclusive) of range of source ports that that packet will be compared against.

#### **13.1.3.4.1.9 wranIfBsProvClsfRuleSrcPortEnd**

End (inclusive) of range of source ports against which that packet will be compared.

#### **13.1.3.4.1.10 wranIfBsProvClsfRuleDestPortStart**

Start (inclusive) of range of destination ports that packet will be compared against.

#### **13.1.3.4.1.11 wranIfBsProvClifRuleDestPortEnd**

End (inclusive) of range of destination ports against which that packet will be compared.

#### **13.1.3.4.1.12 wranIfBsProvClifRuleDestMacAddr**

Destination MAC address to be matched against the destination MAC address in Ethernet header.

#### **13.1.3.4.1.13 wranIfBsProvClifRuleDestMacMask**

MAC address mask. A destination MAC address (`wranIfBsProvClifRuleDestMacAddr`) is matched when the destination MAC address from Ethernet header is applied (bitwise AND) with this mask.

#### **13.1.3.4.1.14 wranIfBsProvClifRuleSrcMacAddr**

Source MAC address to be matched against the source MAC address in Ethernet header.

#### **13.1.3.4.1.15 wranIfBsProvClifRuleDestMacMask**

MAC address mask. A source MAC address (`wranIfBsProvClifRuleSrcMacAddr`) is matched when the source MAC address from Ethernet header is applied (bitwise AND) with this mask.

#### **13.1.3.4.1.16 wranIfBsProvClifRuleEonetProtType**

Enable/disable use layer 3 protocol type in Ethernet frame, EtherType in DIX/SNAP based frames, DSAP in IEEE 802.3 frames, are used in Ethernet frame classification. If IEEE Std 802.1Q [B9] is supported, the EtherType value in the IEEE 802.1Q header is used.

#### **13.1.3.4.1.17 wranIfBsProvClifRuleEonetProtocol**

Ethernet protocol type value that is used for classification. This value will be processed based on what is set in `wranIfBsProvClifRuleEonetProtType`.

#### **13.1.3.4.1.18 wranIfBsProvClifRuleUserPriLow**

Low value (inclusive) in range of 3-bit user priority value. This field is part of 16 bit tag of an IEEE 802.1Q header. Only valid if IEEE Std 802.1Q [B9] is being used.

#### **13.1.3.4.1.19 wranIfBsProvClifRuleUserPriHigh**

High value (inclusive) in range of 3-bit user priority value. This field is part of a 16 bit tag of an IEEE 802.1Q header. Only valid if IEEE Std 802.1Q [B9] is being used.

#### **13.1.3.4.1.20 wranIfBsProvClsfRuleVlanId**

VLAN Id from Ethernet frame. Only valid if IEEE Std 802.1Q [B9] is being used.

#### **13.1.3.4.1.21 wranIfBsProvClsfRuleIpv6FlowLabel**

Flow label field from IPv6 header.

#### **13.1.3.4.1.22 wranIfBsProvClsfRuleIpTypeOfService**

The value to match the IP TOS octet from the IP header. The 6 MSBs are read in as the DSCP (IETF RFC 2474 [B24]).

#### **13.1.3.4.1.23 wranIfBsProvClsfRuleMap**

A bitmap that indicates which classification parameters are included in the classification rule.

#### **13.1.3.4.1.24 wranIfBsProvClsfRulePktCount**

Counter to indicate the number of packets classified by this rule.

### **13.1.3.5 wranIfBsClassifierRuleTable**

This MIB object provides a table to contain classification rules for service flows that are dynamically created/destroyed. There are multiple entries in this table, one for each classifier rule. Each entry is defined by wranIfBsClassifierRuleEntry.

#### **13.1.3.5.1 wranIfBsClassifierRuleEntry**

This object is a compound object that provides the definition of entries in wranIfBsClassifierRuleTable.

##### **13.1.3.5.1.1 wranIfBsClsfRuleIndex**

Index to uniquely identify an entry in wranIfBsClassifierRuleTable.

##### **13.1.3.5.1.2 wranIfBsClsfRulePriority**

Priority of the classification rule. This determines the order in which classification rules are applied.

##### **13.1.3.5.1.3 wranIfBsClsfRuleIpProtocol**

Value of IP Protocol field. For IPv6 headers, this refers to the next header entry in the last header of the IP header list. The value of this field follows the “Protocol Numbers” specification defined by IANA.

#### **13.1.3.5.1.4 wranIfBsClifRuleIpSrcAddr**

Source IP address from the IP header.

#### **13.1.3.5.1.5 wranIfBsClifRuleIpSrcMask**

IP address mask. IP src address (wranIfBsClifRuleIpSrcAddr) is matched when output of applying (bitwise AND) this value to IP src address from IP packet.

#### **13.1.3.5.1.6 wranIfBsClifRuleIpDestAddr**

Destination IP address from IP header.

#### **13.1.3.5.1.7 wranIfBsClifRuleIpDestMask**

IP address mask. IP dest address (wranIfBsClifRuleIpDestAddr) is matched when output of applying (bitwise AND) this value to IP dest address from IP packet.

#### **13.1.3.5.1.8 wranIfBsClifRuleSrcPortStart**

Start (inclusive) of range of source ports that that packet will be compared against.

#### **13.1.3.5.1.9 wranIfBsClifRuleSrcPortEnd**

End (inclusive) of range of source ports against which that packet will be compared.

#### **13.1.3.5.1.10 wranIfBsClifRuleDestPortStart**

Start (inclusive) of range of destination ports that that packet will be compared against.

#### **13.1.3.5.1.11 wranIfBsClifRuleDestPortEnd**

End (inclusive) of range of destination ports against which that packet will be compared.

#### **13.1.3.5.1.12 wranIfBsClifRuleDestMacAddr**

Destination MAC address to be matched against destination MAC address in Ethernet header.

#### **13.1.3.5.1.13 wranIfBsClifRuleDestMacMask**

MAC address mask. A destination MAC address (wranIfBsProvClifRuleDestMacAddr) is matched when the destination MAC address from Ethernet header is applied (bitwise AND) with this mask.

#### **13.1.3.5.1.14 wranIfBsClifRuleSrcMacAddr**

Source MAC address to be matched against source MAC address in Ethernet header.

#### **13.1.3.5.1.15 wranIfBsClifRuleDestMacMask**

MAC address mask. A source MAC address (`wranIfBsProvClifRuleSrcMacAddr`) is matched when the source MAC address from Ethernet header is applied (bitwise AND) with this mask.

#### **13.1.3.5.1.16 wranIfBsClifRuleEonetProtType**

Enable/disable use layer 3 protocol type in Ethernet frame, EtherType in DIX/SNAP based frames, DSAP in IEEE 802.3 frames, are used in Ethernet frame classification. If IEEE Std 802.1Q [B9] is supported, the EtherType value in the IEEE 802.1Q header is used.

#### **13.1.3.5.1.17 wranIfBsClifRuleEonetProtocol**

Ethernet protocol type value that is used for classification. This value will be processed based on what is set in `wranIfBsClifRuleEonetProtType`.

#### **13.1.3.5.1.18 wranIfBsClifRuleUserPriLow**

Low value (inclusive) in range of 3-bit user priority value. This field is part of 16-bit tag of an IEEE 802.1Q header. Only valid if IEEE Std 802.1Q is being used.

#### **13.1.3.5.1.19 wranIfBsClifRuleUserPriHigh**

High value (inclusive) in range of 3-bit user priority value. This field is part of a 16-bit tag of an IEEE 802.1Q header. Only valid if IEEE Std 802.1Q [B9] is being used.

#### **13.1.3.5.1.20 wranIfBsClifRuleVlanId**

VLAN Id from Ethernet frame. Only valid if IEEE Std 802.1Q [B9] is being used.

#### **13.1.3.5.1.21 wranIfBsClifRuleIpv6FlowLabel**

Flow label field from IPv6 header.

#### **13.1.3.5.1.22 wranIfBsClifRuleIpTypeOfService**

The value to match the IP TOS octet from IP header. The 6 MSBs are read in as the DSCP (IETF RFC 2474 [B24]).

### 13.1.3.5.1.23 wranIfBsClsfRuleMap

A bitmap that indicates which classification parameters are included in the classification rule.

### 13.1.3.5.1.24 wranIfBsClsfRulePktCount

Counter to indicate the number of packets classified by this rule.

## 13.1.4 wranIfCpeMib

This MIB defines objects used for managing CPEs. It is broken up into the following subclauses:

- wranIfCpeConfigurationTable: Definition of system parameters, timers, and constants related to CPE operation.
- wranIfCpeTrapControl: Enabling/disabling of traps and setting thresholds for certain events.
- wranIfCpeTrapDefinitions: Definition of traps and objects that can be reported by traps.

### 13.1.4.1 wranIfCpeConfigurationTable

This MIB provides a table that provides the values for system parameters. The parameters in this table are applied to all CPEs in the network; hence there is one entry in the table, defined by wranIfCpeConfigurationEntry.

#### 13.1.4.1.1 wranIfCpeConfigurationEntry

This object is a compound object that provides the definition of the (single) entry into wranIfCpeConfigurationTable.

##### 13.1.4.1.1.1 wranIfCpeLostDsMapInterval

Amount of time since reception of last DS-MAP before DS synchronization is considered lost.

##### 13.1.4.1.1.2 wranIfCpeLostUsMapInterval

Amount of time since reception of last US-MAP before US synchronization is considered lost.

##### 13.1.4.1.1.3 wranIfCpeContentionRangingRetries

Maximum number of retries allowed for contention-based ranging.

##### 13.1.4.1.1.4 wranIfCpeContentionBwRetries

Maximum number of retries allowed for contention-based bandwidth requests.

#### **13.1.4.1.1.5 wranIfCpeRegReqRetries**

Maximum number of retries allowed for registration requests.

#### **13.1.4.1.1.6 wranIfCpeTftpBackoffStart**

Initial value for TFTP backoff.

#### **13.1.4.1.1.7 wranIfCpeTftpBackoffEnd**

Last value for TFTP backoff.

#### **13.1.4.1.1.8 wranIfCpeTftpReqRetries**

Maximum number of retries allowed for attempting TFTP to get CPE configuration.

#### **13.1.4.1.1.9 wranIfCpeTftpDownloadRetries**

Maximum number of retries allowed for re-attempting TFTP (after a failed/corrupted download) to get CPE configuration.

#### **13.1.4.1.1.10 wranIfCpeTftpWait**

Time to wait before consecutive attempts to obtain configuration via TFTP.

#### **13.1.4.1.1.11 wranIfCpeToDRetries**

Maximum number of retries allowed for attempting to establish time of day.

#### **13.1.4.1.1.12 wranIfCpeToDRetryPeriod**

Amount of time to wait before retrying establishment of time of day after failed attempt.

#### **13.1.4.1.1.13 wranIfCpeCBCReqRetries**

Maximum number of retries allowed for sending SBC request.

#### **13.1.4.1.1.14 wranIfCpeTftpCpltRetries**

Maximum number of retries allowed for sending TFTP-CPLT message to BS.

**13.1.4.1.1.15 wranIfCpePowerCtrlProcTime**

Maximum time CPE is allowed to wait after receiving instruction to adjust power, before power adjustment is executed.

**13.1.4.1.1.16 wranIfCpeUsMapProcTime**

Time provided between arrival of last bit of US-MAP at a CPE and the effectiveness of that map in microseconds. For OFDMA, this is entire frame length.

**13.1.4.1.1.17 wranIfCpeRangRspProcTime**

Maximum time CPE is allowed to wait before applying corrections received in RNG-CMD.

**13.1.4.1.1.18 wranIfCpeInvitedRangRetries**

Maximum number of retries on invited ranging requests.

**13.1.4.1.1.19 wranIfCpeDSxReqRetries**

Maximum number of timeout retries on DSx-REQ.

**13.1.4.1.1.20 wranIfCpeDSxRspRetries**

Maximum number of timeout retries on DSx-RSP.

**13.1.4.2 wranIfCpeTrapControl**

wranIfCpeTrapControl is comprised of the following two MIBs that deal with SNMP traps:  
wranIfCpeTrapControlRegister and wranIfCpeThresholdConfigTable.

**13.1.4.2.1 wranIfCpeTrapControlRegister**

This MIB object is a bitmap that allows the following SNMP traps to be set for CPEs:  
wranIfCpeDhcpSuccess, wranIfCpeRssiStatusChange,  
wranIfCpeEirpStatusChange, wranIfCpeScmSilentState.

**13.1.4.2.2 wranIfCpeThresholdConfigTable**

This MIB provides a table that allows the setting of thresholds that can be used to detect the crossing of RSSI and EIRP thresholds. Each table is made up of entries for low and high thresholds for RSSI and EIRP.

**13.1.4.2.2.1 wranIfCpeThresholdConfigEntry**

This object is a compound object that provides definition of entries into wranIfCpeThresholdConfigTable.

**13.1.4.2.2.1.1 wranIfCpeRssiLowThreshold**

Low threshold for generating an RSSI alarm.

**13.1.4.2.2.1.2 wranIfCpeRssiHighThreshold**

High threshold for generating an RSSI alarm.

**13.1.4.2.2.1.3 wranIfCpeEirpLowThreshold**

Low threshold for generating an EIRP alarm.

**13.1.4.2.2.1.4 wranIfCpeEirpHighThreshold**

High threshold for generating an EIRP alarm.

**13.1.4.2.3 wranIfCpeNotificationObjectsTable**

This MIB provides a table to track notification objects that have been reported by traps on a particular CPE. There are multiple entries in this table, one for each CPE's trap. Each entry is defined by wranIfCpeNotificationObjectsEntry.

**13.1.4.2.3.1 wranIfCpeNotificationObjectsEntry**

This object is a compound object that contains the definition of an entry in wranIfCpeNotificationObjectsTable.

**13.1.4.2.3.1.1 wranIfCpeMacAddress**

MAC address of the CPE generating the trap.

**13.1.4.2.3.1.2 wranIfCpeRssiStatus**

An RSSI alarm is generated when RSSI is lower than wranIfCpeRssiLowThreshold or higher than wranIfCpeRssiHighThreshold.

**13.1.4.2.3.1.3 wranIfCpeEirpStatus**

An EIRP alarm is generated when EIRP is lower than wranIfCpeEirpLowThreshold or higher than wranIfCpeEirpHighThreshold.

### **13.1.5 wranIfSmMib**

This MIB group deals with objects related to the configuration, operation, and monitoring of the SM.

#### **13.1.5.1 wranIfSmConfigTable**

This MIB object represents a table that tracks what the default configuration of SM timers and constants. There is only one entry in this table, to define the default configuration of the SM. This entry is defined by wranIfSmConfigEntry.

##### **13.1.5.1.1 wranIfSmConfigEntry**

This object represents the entry in wranIfSmConfigTable.

###### **13.1.5.1.1.1 wranIfSmT31**

Wait for BLM-REP timeout.

###### **13.1.5.1.1.2 wranIfSmSsaChAvailabilityCheckTime**

Time during which a TV channel shall be checked for the presence of licensed incumbent signals having a level above the incumbent detection threshold prior to commencement of WRAN operation in the channel, and in the case of TV, a related channel at an EIRP level that can affect the measured TV channel.

###### **13.1.5.1.1.3 wranIfSmSsaNonOccupancyPeriod**

The required period during which WRAN device transmissions SHALL NOT occur in a given TV channel because of the detected presence of an incumbent signal in that channel above the Incumbent detection threshold, or in the case of TV, above a given EIRP level.

###### **13.1.5.1.1.4 wranIfSmSsaChannelDetectionTime**

Maximum time taken by a WRAN device to detect a licensed incumbent signal above the Incumbent Detection Threshold within a given TV channel during normal WRAN operation.

###### **13.1.5.1.1.5 wranIfSmSsaChannelSetupTime**

The window of time that may be taken by a WRAN CPE to transmit control information to a WRAN base station in order to establish operation with that base station at the prescribed power or, in the case of TV, at or below the allowable EIRP within a given TV channel.

#### **13.1.5.1.1.6 wranIfSmSsaChannelOpeningTxTime**

The aggregate duration of control transmissions by WRAN devices during the Channel Setup Time that starts at the end of the Channel Availability Check Time.

#### **13.1.5.1.1.7 wranIfSmSsaChannelMoveTime**

The time taken by WRAN system to cease all interfering transmissions on the current TV channel upon detection of a license incumbent signal above the relevant Incumbent Detection Threshold, or in the case of TV, to alternatively reduces its EIRP to which is allowable within a given TV channel upon detection of a TV signal in the same or a related channel.

#### **13.1.5.1.1.8 wranIfSmSsaChannelClosingTxTime**

The aggregate duration of control transmissions by the WRAN devices during the Channel Move/EIRP Reduction Time that starts upon detection of a licensed incumbent signal above the relevant Incumbent Detection Threshold.

#### **13.1.5.1.1.9 wranIfSmSsaMicProtectionRadius**

Radius of contour within which the WRAN system cannot operate due to potential interference with the microphone.

#### **13.1.5.1.1.10 wranIfSmSsaT41**

Maximum time interval allowed before sensing is performed on the candidate channel to ensure that no incumbents are detected.

#### **13.1.5.1.1.11 wranIfSmSsaT42**

Maximum time interval allowed before sensing is performed on the backup channel to ensure that no incumbents are detected.

#### **13.1.5.1.1.12 wranIfSmSsaT43**

Minimum time duration without detection of any incumbent for a candidate channel to transition to the backup channel.

#### **13.1.5.1.1.13 wranIfSmSsaT44**

Maximum time to ensure that the channel move information is successfully conveyed to all the associated CPEs and BS (self-coexistence mode).

#### **13.1.5.1.1.14 wranIfSmSsaT45**

Maximum WRAN operation time without access to the incumbent database service.

### **13.1.5.1.1.15 wranIfSmT46**

Waiting time before which the BS moves to the first backup channel. This is used to make sure that all the CPEs are ready to move to the backup channel before BS switches operation to this backup channel.

### **13.1.5.1.1.16 wranIfSmSsaT59**

Waiting time before which the CPE moves to its backup channels if it no longer hears from its BS. This is used to make sure that the CPE waits long enough after UCS Notification so that BS has had time to move to the backup channel, it decided to do so.

### **13.1.5.1.1.17 wranIfSmSsaT47**

The prescribed time by the WRAN operator to refresh the incumbent database service.

### **13.1.5.1.1.18 wranIfSmSsaT48**

Lapse timer keeps track of whether the Operating Channel N has been cleared using spectrum sensing.

### **13.1.5.1.1.19 wranIfSmSsaT49**

Lapse timer keeps track of whether the Adjacent Channel N–1 has been cleared using spectrum sensing.

### **13.1.5.1.1.20 wranIfSmSsaT50**

Lapse timer keeps track of whether the Adjacent Channel N+1 has been cleared using spectrum sensing.

### **13.1.5.1.1.21 wranIfSmSsaT51**

Initiated when SSA loses contact with the SM.

### **13.1.5.1.1.22 wranIfSmSsaT53**

The parameter  $T_{INsens}$  is used to verify that in-band sensing has been done within the required In-service monitoring period. The  $T_{INsens}$  parameter is driven by regulatory domain requirements (Annex A).

### **13.1.5.1.1.23 wranIfSmSsaT54**

The parameter  $T_{OUTsens}$  is used to verify that out-of-band sensing has been done within the required “Acquiring a channel monitoring period” specified in Annex A. This value would be used to initialize a lapse timer for each channel in the backup candidate channel list at each CPE so that it is compared to  $T_{sensout}$ .

### **13.1.5.1.1.24 wranIfSmSsaT55**

The T55 or  $T_{\text{sensin}}$  parameter corresponds to the maximum length of time required to carry out the sensing process on an in-band channel (see Figure 176). Manufacturers need to specify the sensing time required to detect the specified signals with required accuracy.

### **13.1.5.1.1.25 wranIfSmSsaT60**

The T60 or  $T_{\text{sensout}}$  parameter corresponds to the maximum length of time required to carry out the out-of-band sensing process to clear one channel (see Figure 178). Manufacturers need to specify the sensing time required to detect the specified signals with required accuracy for out-of-band sensing.

## **13.1.5.2 wranIfSmPendingBlmReqTable**

This MIB object represents a table that tracks the status of the execution of ongoing sensing requests (BLM-REQ). For each BLM-REQ there is a corresponding BLM-RSP to indicate that REQ message was received by the SSA. When an SSA is done with the sensing it will send a BLM-REP to the SM. This table keeps track of any BLM-REP messages that are pending transmission from the SSA. When a report is received a acknowledgement is sent to the SSA, and then the entry corresponding to the report and request will be cleared. This entry is defined by wranIfSmPendingBlmReqEntry.

### **13.1.5.2.1 wranIfSmPendingBlmReqEntry**

This object represents the entry in wranIfSmPendingBlmReqTable.

#### **13.1.5.2.1.1 wranIfSsaPendingBlmReqTransactionId**

Transaction ID of BLM-REQ.

#### **13.1.5.2.1.2 wranIfSmPendingBlmReqMsg**

Contents of BLM-REQ message pending a report.

#### **13.1.5.2.1.3 wranIfSmPendingBlmRspReceived**

Indication of whether or not BLM-RSP pertaining to BLM-REQ has been received from SSA.

#### **13.1.5.2.1.4 wranIfSmPendingBlmRspMulticastReceived**

If BLM-REQ was multicast, indication of whether or not BLM-RSP pertaining to BLM-REQ has been received from each SSA (CPE) in the multicast group.

#### **13.1.5.2.1.5 wranIfSmPendingBlmRepTimeout**

Indication of current value of T31 set for this BLM-REP.

### **13.1.5.2.1.6 wranIfSmPendingBlmRepReceived**

Indication of whether or not BLM-REP pertaining to BLM-REQ has been received from SSA.

### **13.1.5.2.1.7 wranIfSmPendingBlmRepMulticastReceived**

If BLM-REQ was multicast, indication of whether or not BLM-REP pertaining to BLM-REQ has been received from each SSA (CPE) in the multicast group.

### **13.1.5.2.1.8 wranIfSsaPendingBlmRepAck**

Indication of whether or not BLM-ACK, used to indicate sent to SSA(s) whether or not BLM-REP was received, is sent to SSA(s).

## **13.1.5.3 wranIfSmBlmRepTable**

This object contains BLM-REP messages received in response to BLM-REQ; it is made up of multiple entries, one for each BLM-REP that pertains to a BLM-REQ. Each entry is defined by wranIfSmBlmRepEntry.

### **13.1.5.3.1 wranIfSmBlmRepEntry**

This object represents the entry in wranIfSmBlmRepTable.

#### **13.1.5.3.1.1 wranIfSmBlmRepSid**

SID of CPE that sent the BLM-REP.

#### **13.1.5.3.1.2 wranIfSmBlmRepTransactionId**

Transaction ID of BLM-REP, it should match a transaction ID of an entry in wranIfSmPendingBlmReqTable.

#### **13.1.5.3.1.3 wranIfSmBlmRepMsg**

Contents of BLM-REP msg.

## **13.1.5.4 wranIfSmChClassificationStatusTable**

This MIB object represents a table that the status for channels that the SM is managing. It is made up multiple entries, one for each channel, as defined in wranIfSmChClassificationStatusEntry.

#### **13.1.5.4.1 wranIfSmChClassificationStatusEntry**

This object represents the entry in wranIfSmChClassificationStatusTable.

##### **13.1.5.4.1.1 wranIfSmManagedChannel**

Channel number of channel being managed.

##### **13.1.5.4.1.2 wranIfSmManagedChannelStatus**

The state of the channel as set by the states in the Channel Set Transition Diagram (Figure 162) or disallowed state (if channel is in IPC-UPD).

##### **13.1.5.4.1.3 wranIfSmManagedChannelRecentEvent**

Most recent event (see 10.2.3.1) that dictated a transition to the current state.

#### **13.1.5.5 wranIfSmSizeWranOccupiedChannelSet**

Number of channels in WRAN Occupied Channel Set.

#### **13.1.5.6 wranIfSmWranOccupiedChannelSet**

Vector of channels of length 8 bits  $\times$  wranIfSmSizeWranOccupiedChannelSet that indicate the channels that occupy the WRAN Occupied Channel Set used by the Spectrum Etiquette procedure (see 10.2.3.2).

#### **13.1.5.7 wranIfSmSizeNghbrWranBackupChannelSet**

Number of channels in Neighbor WRAN Backup Channel Set.

#### **13.1.5.8 wranIfSmNghbrWranOccupiedChannelSet**

Vector of channels of length 8 bits  $\times$  wranIfSmSizeNghbrWranBackupChannelSet that indicates the channels that occupy the Neighbor WRAN Backup Channel Set used by the Spectrum Etiquette procedure (see 9.2.3.2).

#### **13.1.5.9 wranIfSmSizeLocalPrioritySet1**

Number of channels in Local Priority Set 1.

### **13.1.5.10 wranIfSmLocalPrioritySet1**

Vector of channels of length 8 bits  $\times$  wranIfSmSizeLocalPrioritySet1 that indicate the channels that occupy the Local Priority Set 1 used by Spectrum Etiquette procedure (see 10.2.3.2).

### **13.1.5.11 wranIfSmSizeLocalPrioritySet2**

Number of channels in Local Priority Set 2.

### **13.1.5.12 wranIfSmLocalPrioritySet2**

Vector of channels of length 8 bits  $\times$  wranIfSmSizeLocalPrioritySet2 that indicate the channels that occupy the Local Priority Set 2 used by Spectrum Etiquette procedure (see 10.2.3.2).

### **13.1.5.13 wranIfSmSizeLocalPrioritySet3**

Number of channels in Local Priority Set 3, should be the same size as wranIfSmSizeWranOccupiedChannelSet.

### **13.1.5.14 wranIfSmLocalPrioritySet3**

Vector of channels of length 8 bits  $\times$  wranIfSmSizeLocalPrioritySet3 that indicate the channels that occupy the Local Priority Set 3 used by Spectrum Etiquette procedure (see 10.2.3.2). Should contain the same channel set as wranIfSmWranOccupiedChannelSet.

### **13.1.5.15 wranIfSmCurrentStatusTable**

This MIB object represents a table that records the current status of the SM. This includes the state the SM is in, the event that triggered a move into that state, as well as the current state of any relevant timers. There is one entry in this table defined in wranIfSmCurrentStatusEntry.

#### **13.1.5.15.1 wranIfSmCurrentStatusEntry**

This object represents the entry in wranIfSmCurrentStatusTable.

##### **13.1.5.15.1.1 wranIfSmCurrentState**

The state (see Figure 162) that the SM is in.

##### **13.1.5.15.1.2 wranIfSmRecentEvent**

Recent event that triggered a transition into the current state as given in 10.2.6.1.

### **13.1.5.15.1.3 wranIfSmRecentAction**

Recent action that was taken when transitioning into the current state as given in 10.2.6.1.

### **13.1.5.15.1.4 wranIfSmInitiateChannelMove**

Current value of ‘Initiate\_Channel\_Move’ flag.

### **13.1.5.15.1.5 wranIfSmSelfCoexistenceMode**

Current value of ‘Self\_Coexistence\_Mode’ flag.

### **13.1.5.15.1.6 wranIfSmCurrentOperatingChannel**

Current operating channel.

### **13.1.5.15.1.7 wranIfSmRecentSignalType**

Type of signal recently detected.

### **13.1.5.15.1.8 wranIfSmCurrentT47**

Current value of T47.

### **13.1.5.15.1.9 wranIfSmCurrentT46**

Current value of T46.

## **13.1.5.16 wranIfSmRegTrackingTable**

This MIB object represents a table that records the SM’s monitoring of CPE’s associated with the BS. It contains the location data string and current value of T30 for each CPE. There are multiple entries in this table (one for each CPE) defined in wranIfSmRegTrackingEntry.

### **13.1.5.16.1 wranIfSmRegTrackingEntry**

This object represents the entry in wranIfSmRegTrackingTable.

#### **13.1.5.16.1.1 wranIfSmRegTrackingCpeSid**

SID of CPE currently associated with BS.

### **13.1.5.16.1.2 wranIfSmRegTrackingCurrentT30**

Current value of CPE's T30, as known by SM.

### **13.1.5.16.1.3 wranIfSmRegTrackingLocStringSize**

Size of the location string in octets.

### **13.1.5.16.1.4 wranIfSmRegTrackingLocString**

CPE's location string.

## **13.1.6 wranIfSsaMib**

This MIB group deals with objects related to the configuration, operation, and monitoring of the Spectrum Automaton.

The automaton needs to be told what needs to be sensed in the given regulatory domain. This can be done through the MIB referring to the regulatory domain information from Annex A. The CPE also need to be told which type of incumbent requires urgent, less urgent and non-urgent reporting to the BS (see Table A.7). The background sensing done by the automaton shall be done under the MIB guidance.

### **13.1.6.1 wranIfSsaSensingCapTable**

This MIB object represents a table that stores the current sensing capabilities for a SSA under control of the SM. There is one entry in this table for a SSA, defined by `wranIfSsaSensingCapEntry`. This MIB is stored at the BS and CPE. These values are also stored in `wranIfBsRegisteredCpeTable` (see 10.4.2) at the BS, in an entry specific to this CPE.

#### **13.1.6.1.1 wranIfSsaSensingCapEntry**

This object represents the entry that stores a CPE's sensing capabilities.

##### **13.1.6.1.1.1 wranIfSsaSensingThreshold**

This object is the recommended sensing threshold that the CPE is capable of supporting. It is in units of dBm, encoded in a single, integer byte value that is assumed to be negative (e.g., 0x01 = -1 dBm, 0x72 = -114 dBm).

##### **13.1.6.1.1.2 wranIfSsaSensRecContigPeriodDuration**

This object is the recommended contiguous sensing period duration that the CPE is capable of supporting. It is in integer, in units of symbols. This value ranges from 0 to 1023, and is encoded in a 2-octet length value.

### **13.1.6.1.1.3 wranIfSsaSensRecNumPeriods**

This object is the recommended number of sensing periods that a CPE can support. It is an integer value, encoded in 1-octet length value.

### **13.1.6.1.1.4 wranIfSsaSensRecPeriodInterval**

This object is the recommended interval between sensing periods that a CPE can support. It is an integer value, in units of frames. It is encoded in a 2-octet length value.

## **13.1.6.2 wranIfSsaStatusTable**

This MIB object represents a table that tracks what the current state the SSA is in. There is only one entry in this table, to define the current state of the SSA, as well as any parameters of interest for current SSA procedures. This entry is defined by `wranIfSsaStatusEntry`.

### **13.1.6.2.1 wranIfSsaStatusEntry**

This object represents the entry in `wranIfSsaStatusTable`.

#### **13.1.6.2.1.1 wranIfSsaCurrentState**

The current state of the SSA is in (see 10.3.1, Figure 173), either “SSA In-band Sensing” or “SSA Out-of-band Sensing”.

#### **13.1.6.2.1.2 wranIfSsaRecentEvent**

The recent event that caused entry into the current state (see 10.3.1, Figure 173).

#### **13.1.6.2.1.3 wranIfSsaRecentAction**

The recent action, triggered by recent event, that was undertaken while entering into the current state (see 10.3.1, Figure 173).

#### **13.1.6.2.1.4 wranIfSsaIncProhibitedChannels**

Contents of most recent IPC-UPD message received from SM.

#### **13.1.6.2.1.5 wranIfSsaCurrentT48**

Current value of T48 at the SSA.

#### **13.1.6.2.1.6 wranIfSsaCurrentT49**

Current value of T49 at the SSA.

### **13.1.6.2.1.7 wranIfSsaCurrentT50**

Current value of T50 at the SSA.

### **13.1.6.2.1.8 wranIfSsaIntraFrameQpCycleLength**

Obtained from CHQ-REQ or SCH. Specified in number of superframes, it indicates the spacing between the superframes for which the intra-frame quiet period specification is valid. For example, if this field is set to 1, the Quiet Period Cycle repeats every superframe; if it is set to 2, the Quiet Period Cycle repeats every 2 superframes, etc. When = 0, no intra-frame quiet period is scheduled or the current intra-frame quiet period is canceled

### **13.1.6.2.1.9 wranIfSsaIntraFrameQpCycleOffset**

Obtained from CHQ-REQ or SCH. Valid only if intra-frame Sensing Cycle Length > 0. Used for in-band intra-frame sensing. Specified in number of superframes, it indicates the offset from this SCH transmission to the beginning of the first superframe in the current intra-frame sensing cycle.

### **13.1.6.2.1.10 wranIfSsaIntraFrameQpCycleFrameBitmap**

Obtained from CHQ-REQ or SCH. Valid only if Intra-frame Quiet Period Cycle Length > 0. Valid for each superframe identified by the Intra-frame Quiet Period Cycle Length, each bit in the bitmap corresponds to one frame within the superframe. If the bit is set to 0, no intra-frame quiet period shall be scheduled in the corresponding frame. If the bit is set to 1, an intra-frame quiet period shall be scheduled within the corresponding frame for the duration specified by Intra-frame Quiet period Duration.

### **13.1.6.2.1.11 wranIfSsaIntraFrameQpDuration**

Obtained from CHQ-REQ or SCH. Valid only if Intra-frame Quiet Period Cycle Length > 0. If this field is set to a value different from 0 (zero): it indicates the number of symbols starting from the end of the frame during which no transmission shall take place.

### **13.1.6.2.1.12 wranIfSsaInterFrameQpDuration**

Obtained from CHQ-REQ or SCH. Used for in-band inter-frame sensing, it indicates the duration of the next scheduled quiet period. When > 0, it indicates the number of frames starting from Inter-frame Quiet Period Offset that shall be used to perform inter-frame sensing. When == 0, it cancels the next scheduled quiet period for inter-frame sensing or indicates that no inter-frame sensing are currently scheduled.

### **13.1.6.2.1.13 wranIfSsaInterFrameQpOffset**

Obtained from CHQ-REQ or SCH. Used for in-band inter-frame sensing, it indicates the time span between the transmission of this information and the next scheduled quiet period for inter-frame sensing. Bit 11–4: index the superframe number, Bit 3–0: index the frame number when the next scheduled quiet period for inter-frame sensing will start.

### **13.1.6.3 wranIfSsaConfigTable**

This MIB object represents a table that tracks what the default configuration of SSA timers and constants. There is only one entry in this table, to define the default configuration of the SSA. This entry is defined by wranIfSsaConfigEntry.

#### **13.1.6.3.1 wranIfSsaConfigEntry**

This object represents the entry in wranIfSsaConfigTable.

##### **13.1.6.3.1.1 wranIfSsaT19**

Time DS-channel remains unusable.

##### **13.1.6.3.1.2 wranIfSsaT29**

Wait for BLM-ACK timeout.

##### **13.1.6.3.1.3 wranIfSsaMaxBlmRepRetries**

Maximum number of retry attempts allowed for sending BLM-REP.

##### **13.1.6.3.1.4 wranIfSmSsaChAvailabilityCheckTime**

Time during which a TV channel shall be checked for the presence of licensed incumbent signals having a level above the incumbent detection threshold prior to commencement of WRAN operation in the channel and, in the case of TV, a related channel at an EIRP level that can affect the measured TV channel.

##### **13.1.6.3.1.5 wranIfSmSsaNonOccupancyPeriod**

The required period during which WRAN device transmissions SHALL NOT occur in a given TV channel because of the detected presence of an incumbent signal in that channel above the Incumbent detection threshold or, in the case of TV, above a given EIRP level.

##### **13.1.6.3.1.6 wranIfSmSsaChannelDetectionTime**

Maximum time taken by a WRAN device to detect a licensed incumbent signal above the Incumbent Detection Threshold within a given TV channel during normal WRAN operation.

##### **13.1.6.3.1.7 wranIfSmSsaChannelSetupTime**

The window of time that may be taken by a WRAN CPE to transmit control information to a WRAN base station in order to establish operation with that base station at the prescribed power or, in the case of TV, at or below the allowable EIRP within a given TV channel.

#### **13.1.6.3.1.8 wranIfSmSsaChannelOpeningTxTime**

The aggregate duration of control transmissions by WRAN devices during the Channel Setup Time, which starts at the end of the Channel Availability Check Time.

#### **13.1.6.3.1.9 wranIfSmSsaChannelMoveTime**

The time taken by WRAN system to cease all interfering transmissions on the current TV channel upon detection of a license incumbent signal above the relevant Incumbent Detection Threshold or, in the case of TV, to alternatively reduces its EIRP to which is allowable within a given TV channel upon detection of a TV signal in the same or a related channel.

#### **13.1.6.3.1.10 wranIfSmSsaChannelClosingTxTime**

The aggregate duration of control transmissions by the WRAN devices during the Channel Move/EIRP Reduction Time, which starts upon detection of a licensed incumbent signal above the relevant Incumbent Detection Threshold.

#### **13.1.6.3.1.11 wranIfSmSsaMicProtectionRadius**

Radius of contour within which the WRAN system cannot operate due to potential interference with the microphone.

#### **13.1.6.3.1.12 wranIfSmSsaT41**

Maximum time interval allowed before sensing is performed on the candidate channel to ensure that no incumbents are detected.

#### **13.1.6.3.1.13 wranIfSmSsaT42**

Maximum time interval allowed before sensing is performed on the backup channel to ensure that no incumbents are detected.

#### **13.1.6.3.1.14 wranIfSmSsaT43**

Minimum time duration without detection of any incumbent for a candidate channel to transition to the backup channel.

#### **13.1.6.3.1.15 wranIfSmSsaT44**

Maximum time to ensure that the channel move information is successfully conveyed to all the associated CPEs and BS (self-coexistence mode).

**13.1.6.3.1.16 wranIfSmSsaT45**

Maximum WRAN operation time without access to the incumbent database service.

**13.1.6.3.1.17 wranIfSmSsaT59**

Waiting time before which the CPE moves to its backup channels if it no longer hears from its BS. This is used to make sure that the CPE waits long enough after UCS notification so that BS has had time to move to the backup channel, it decided to do so.

**13.1.6.3.1.18 wranIfSmSsaT47**

The prescribed time by the WRAN operator to refresh the incumbent database service.

**13.1.6.3.1.19 wranIfSmSsaT48**

Lapse timer keeps track of whether the Operating Channel N has been cleared using spectrum sensing.

**13.1.6.3.1.20 wranIfSmSsaT49**

Lapse timer keeps track of whether the Adjacent Channel N-1 has been cleared using spectrum sensing.

**13.1.6.3.1.21 wranIfSmSsaT50**

Lapse timer keeps track of whether the Adjacent Channel N+1 has been cleared using spectrum sensing.

**13.1.6.3.1.22 wranIfSmSsaT51**

Initiated when SSA loses contact with the SM.

**13.1.6.3.1.23 wranIfSmSsaT53**

The parameter  $T_{INsens}$  is used to verify that in-band sensing has been done within the required In-service monitoring period. The  $T_{INsens}$  parameter is driven by regulatory domain requirements (Annex A).

**13.1.6.3.1.24 wranIfSmSsaT54**

The parameter  $T_{OUTsens}$  is used to verify that out-of-band sensing has been done within the required “Acquiring a channel monitoring period” specified in Annex A. This value would be used to initialize a lapse timer for each channel in the backup candidate channel list at each CPE so that it compared to  $T_{sensout}$ .

### 13.1.6.3.1.25 wranIfSmSsaT55

The T55 or  $T_{\text{sensin}}$  parameter corresponds to the maximum length of time required to carry out the in-band sensing process (see Figure 176). Manufacturers need to specify the sensing time required to detect the specified signals with required accuracy for in-band sensing.

### 13.1.6.3.1.26 wranIfSmSsaT60

The T60 or  $T_{\text{sensout}}$  parameter corresponds to the maximum length of time required to carry out the out-of-band sensing process (see Figure 178). Manufacturers need to specify the sensing time required to detect the specified signals with required accuracy for out-of-band sensing.

## 13.1.6.4 wranIfSsaPendingBlmRepTable

This MIB object represents a table that tracks the status of the execution of ongoing reporting (BLM-REP) in response to BLM-REQs. For each BLM-REQ there is a corresponding BLM-RSP to indicate that REQ message was received by the SSA. When an SSA is done with the sensing, it will send a BLM-REP to the SM. This table keeps track of any BLM-REP messages that are pending acknowledgement from the SM. When a report sent in a response is acknowledged, then the entry corresponding to the report and request will be cleared. This entry is defined by wranIfSsaPendingBlmRepEntry.

### 13.1.6.4.1 wranIfSsaPendingBlmRepEntry

This object represents the entry in wranIfSsaPendingBlmRepTable.

#### 13.1.6.4.1.1 wranIfSsaPendingBlmReqTransactionId

Transaction ID for pending BLM-REQ.

#### 13.1.6.4.1.2 wranIfSsaPendingBlmReqMsg

Contents of pending BLM-REQ message.

#### 13.1.6.4.1.3 wranIfSsaPendingBlmRspSent

Indication of whether or not BLM-RSP pertaining to BLM-REQ has been sent.

#### 13.1.6.4.1.4 wranIfSsaPendingBlmRepGenerated

Indication of whether or not BLM-REP corresponding to BLM-REQ has been generated, i.e., sensing has been executed.

#### 13.1.6.4.1.5 wranIfSsaPendingBlmRepMsg

Contents of BLM-REP message that corresponds to the BLM-REQ.

#### **13.1.6.4.1.6 wranIfSsaPendingBlmRepSent**

Indication of whether or not BLM-REP pertaining to BLM-REQ has been sent.

#### **13.1.6.4.1.7 wranIfSsaPendingBlmRepAck**

Indication of whether or not BLM-REP pertaining to BLM-REQ has been acknowledged (via BLM-ACK).

#### **13.1.6.4.1.8 wranIfSsaPendingBlmRepNumTx**

Current number of times that BLM-REP has been resent.

### **13.1.6.5 wranIfSsaSensingRecordTable**

This object contains information the sensing status of each channel. It is made of multiple entries, one for each channel, as defined by `wranIfSsaSensingRecordEntry`.

#### **13.1.6.5.1 wranIfSsaSensingRecordEntry**

This object represents the entry in `wranIfSsaSensingRecordTable`.

##### **13.1.6.5.1.1 wranIfSsaSensingChannel**

Channel that sensing has been conducted on, or not conducted on if in IPC-UPD.

##### **13.1.6.5.1.2 wranIfSsaTimeLastSensing**

Last time that this channel was sensed.

##### **13.1.6.5.1.3 wranIfSsaTimeLastPositive**

Last time that signal was positively confirmed on this channel.

##### **13.1.6.5.1.4 wranIfSsaSensingPathRssi**

RSSI on sensing path.

##### **13.1.6.5.1.5 wranIfSsaWranPathRssi**

RSSI on WRAN signal path.

### **13.1.6.5.1.6 wranIfSsaSignalType**

Type of signal that was sensed on the channel.

### **13.1.6.5.1.7 wranIfSsaWranServiceAdvertisement**

If signal type was for WRAN, this indicates the BS ID of the captured SCH from neighbor WRAN.

### **13.1.6.5.1.8 wranIfSsaldcUpdIndication**

Indication if channel is on IPC-UPD.

## **13.1.6.6 wranIfSsaSsfMode0OutputTable**

This object contains the current output of SSF Mode 0 sensing. It is made up of multiple entries, one for each signal type that was sensed. Each entry is defined by `wranIfSsaSsfMode0OutputEntry`.

### **13.1.6.6.1 wranIfSsaSsfMode0OutputEntry**

This object represents the entry in `wranIfSsaSsfMode0OutputTable`.

#### **13.1.6.6.1.1 wranIfSsaSsfMode0SignalType**

Type of signal that was to be sensed .

#### **13.1.6.6.1.2 wranIfSsaSsfMode0SignalPresent**

Indication of whether or not a signal of signal type was detected.

## **13.1.6.7 wranIfSsaSsfMode1OutputTable**

This object contains the current output of SSF Mode 1 sensing. It is made up of multiple entries, one for each signal type that was sensed. Each entry is defined by `wranIfSsaSsfMode1OutputEntry`.

### **13.1.6.7.1 wranIfSsaSsfMode1OutputEntry**

This object represents the entry in `wranIfSsaSsfMode1OutputTable`.

#### **13.1.6.7.1.1 wranIfSsaSsfMode1SignalType**

Type of signal that was to be sensed.

### **13.1.6.7.1.2 wranIfSsaSsfMode1SignalPresent**

Indication of whether or not a signal of signal type was detected.

### **13.1.6.7.1.3 wranIfSsaSsfMode1SignalConfidence**

Confidence level in signal present decision.

## **13.1.6.8 wranIfSsaSsfMode2OutputTable**

This object contains the current output of SSF Mode 2 sensing. It is made up of multiple entries, one for each signal type that was sensed. Each entry is defined by `wranIfSsaSsfMode2OutputEntry`.

### **13.1.6.8.1 wranIfSsaSsfMode2OutputEntry**

This object represents the entry in `wranIfSsaSsfMode2OutputTable`.

#### **13.1.6.8.1.1 wranIfSsaSsfMode2SignalType**

Type of signal that was to be sensed.

#### **13.1.6.8.1.2 wranIfSsaSsfMode0SignalRssiMean**

Mean of RSSI signal measurements.

#### **13.1.6.8.1.3 wranIfSsaSsfMode0SignalStdDevRssi**

Std Dev of RSSI signal measurements.

## **13.1.6.9 wranIfSsaSsfWiMicMSF1Table**

This object contains the current output the payload of MSF1 of an IEEE 802.22.1 beacon on recently sensed channels. It is made up of multiple entries for each channel a MSF1 was sensed on. Each entry is defined by `wranIfSsaSsfWiMicMSF1Entry`.

### **13.1.6.9.1 wranIfSsaSsfWiMicMSF1Entry**

This object represents the entry in `wranIfSsaSsfWiMicMSF1Table`.

#### **13.1.6.9.1.1 wranIfSsaSsfWiMicMSF1Channel**

Channel number on which the wireless microphone beacon was captured.

**13.1.6.9.1.2 wranIfSsaSsfWiMicMSF1Payload**

Payload of MSF1, not including the CRC1 field.

**13.1.6.9.1.3 wranIfSsaSsfWiMicMSF1Crc1Status**

Indication of whether or not MSF1 passed verification of CRC1.

**13.1.6.10 wranIfSsaSsfWiMicMSF2Table**

This object contains the current output the payload of MSF2 of an IEEE 802.22.1 beacon on recently sensed channels. It is made up of multiple entries for each channel a MSF2 was sensed on. Each entry is defined by `wranIfSsaSsfWiMicMSF1Entry`.

**13.1.6.10.1 wranIfSsaSsfWiMicMSF2Entry**

This object represents the entry in `wranIfSsaSsfWiMicMSF2Table`.

**13.1.6.10.1.1 wranIfSsaSsfWiMicMSF2Channel**

Channel number on which wireless microphone beacon was captured.

**13.1.6.10.1.2 wranIfSsaSsfWiMicMSF2Payload**

Payload of MSF2, not including the CRC2 field.

**13.1.6.10.1.3 wranIfSsaSsfWiMicMSF2Crc2Status**

Indication of whether or not MSF2 passed verification of CRC2.

**13.1.6.11 wranIfSsaSsfWiMicMSF3Table**

This object contains the current output the payload of MSF3 of an IEEE 802.22.1 beacon on recently sensed channels. It is made up of multiple entries for each channel a MSF3 was sensed on. Each entry is defined by `wranIfSsaSsfWiMicMSF1Entry`.

**13.1.6.11.1 wranIfSsaSsfWiMicMSF3Entry**

This object represents the entry in `wranIfSsaSsfWiMicMSF3Table`.

**13.1.6.11.1.1 wranIfSsaSsfWiMicMSF3Channel**

Channel number on which wireless microphone beacon was captured.

### **13.1.6.11.1.2 wranIfSsaSsFWiMicMSF3Payload**

Payload of MSF3, not including the CRC3 field.

### **13.1.6.11.1.3 wranIfSsaSsFWiMicMSF3Crc3Status**

Indication of whether or not MSF3 passed verification of CRC3.

## **13.1.6.12 wranIfSsaGeolocationTable**

This object contains the current parameters and calculations being used by the Geolocation component of the SSA. It is made up of one entry to contain current values being used/calculated in the BS-to-CPE fine-ranging, CPE-to-CPE fine ranging, geolocation calculation outputs, and final geolocation string. It is made up of one entry, defined by `wranIfSsaGeoLocationEntry`.

### **13.1.6.12.1 wranIfSsaGeolocationEntry**

This object represents the entry in `wranIfSsaGeolocationTable`.

#### **13.1.6.12.1.1 wranIfSsaGeolocationVernier1**

$Vernier_1$ , recorded only at the CPE.

#### **13.1.6.12.1.2 wranIfSsaGeolocationVernier2**

$Vernier_2$ , recorded only at the BS.

#### **13.1.6.12.1.3 wranIfSsaGeolocationVernier3**

$Vernier_3$ , recorded only at the CPE.

#### **13.1.6.12.1.4 wranIfSsaGeolocationTRange1**

$T_{Range1}$ , also known as T52. Set by BS when downstream burst leaves the BS, i.e., at start of frame preamble.

#### **13.1.6.12.1.5 wranIfSsaGeolocationTACbp**

$TA_{CBP}$ , Timing advance for CBP burst used in ranging calculations.

### **13.1.7 wranIfDatabaseServiceMib**

This MIB group deals with objects related to the configuration of access to, as well as the interaction with the database service.

#### **13.1.7.1 wranIfBsMgmtInfoTable**

This object stores information regarding information on the BS management interface the DBS can access. It is made up of one entry, defined by `wranIfBsMgmtInfoEntry`.

##### **13.1.7.1.1 wranIfBsMgmtInfoEntry**

This object defines an entry in `wranIfBsMgmtInfoTable`.

###### **13.1.7.1.1.1 wranIfBsMgmtUrl**

Base Station Management URL (see 10.7.1.1).

###### **13.1.7.1.1.2 wranIfBsMgmtDeviceId**

BS FCC Device ID (see 10.7.1.1).

###### **13.1.7.1.1.3 wranIfBsMgmtSn**

BS serial number (see 10.7.1.1).

###### **13.1.7.1.1.4 wranIfBsMgmtLocation**

Location data string of BS.

###### **13.1.7.1.1.5 wranIfBsMgmtAntennaHeight**

Antenna height at the BS.

###### **13.1.7.1.1.6 wranIfBsMgmtContactName**

Contact Name for person(s) who has ownership of the BS.

###### **13.1.7.1.1.7 wranIfBsMgmtContactPhysAddress**

Physical address for contacting the owner of the BS.

**13.1.7.1.1.8 wranIfBsMgmtEmailAddress**

E-mail address for contacting the owner of the BS.

**13.1.7.1.1.9 wranIfBsMgmtPhoneNumber**

Telephone # for contacting the owner of the BS.

**13.1.7.2 wranIfBsDeviceEnlistmentTable**

This object stores information regarding information on devices entering the network that the BS has attempted to enlist/register with the database service. It is made up of multiple values, defined by wranIfBsDeviceEnlistmentEntry.

**13.1.7.2.1 wranIfBsDeviceEnlistmentEntry**

This object defines an entry in wranIfBsDeviceEnlistmentTable.

**13.1.7.2.1.1 wranIfBsDeviceEnlistmentConfirmed**

Has this enlistment been confirmed via receipt of M-DEVICE-ENLISTMENT-CONFIRM (see 10.7.1.4) from the database service?

**13.1.7.2.1.2 wranIfBsDeviceType**

Type of device being registered, fixed BS, fixed CPE, personal/portable.

**13.1.7.2.1.3 wranIfBsDeviceId**

Device ID for the device that is being enlisted/registered with the database service.

**13.1.7.2.1.4 wranIfBsDeviceSn**

Serial number of the device that is being enlisted/registered with the database service.

**13.1.7.2.1.5 wranIfBsDeviceLocation**

Location string of the device requesting enlistment.

**13.1.7.2.1.6 wranIfBsProxyDeviceId**

Device ID of proxy device BS may use to send queries to the database.

### **13.1.7.2.1.7 wranIfBsProxySn**

Serial number of proxy device BS may use to send queries to the database.

### **13.1.7.2.1.8 wranIfBsRespPartyName**

Name of the party responsible for the device enlistment/registration.

### **13.1.7.2.1.9 wranIfBsDeviceAntennaHeight**

Antenna height of the device being enlisted.

### **13.1.7.2.1.10 wranIfBsDeviceContactName**

Contact Name for person(s) who has ownership of the device, only pertinent of device type is fixed BS or CPE.

### **13.1.7.2.1.11 wranIfBsDeviceContactPhysAddress**

Physical address for contacting the owner of the BS; the only pertinent device types are fixed BS and fixed CPE.

### **13.1.7.2.1.12 wranIfBsDeviceEmailAddress**

E-mail address for contacting the owner of the BS; the only pertinent device types are fixed BS and fixed CPE.

### **13.1.7.2.1.13 wranIfBsDevicePhoneNumber**

Telephone number for contacting the owner of the BS, the only pertinent device types are fixed BS and fixed CPE.

### **13.1.7.2.1.14 wranIfBsDeviceAntennaInformation**

Antenna information of device; only applicable if transmission of antenna information is supported by the database service.

### **13.1.7.2.1.15 wranIfBsDeviceAntennaAzimuth**

Antenna azimuth of device; only applicable if transmission of antenna information is supported by the database service.

### **13.1.7.2.1.16 wranIfBsDeviceConfirmationMsgTime**

Timestamp of transmission for M-DEVICE-ENLISTMENT-REQUEST.

## **13.1.7.3 wranIfDbsChannelIndicationTable**

This object stores information what channels have been indicated as available and their EIRP limit at a given location for a particular device. It is made up of multiple entries, one each for the tuple of location||channel||EIRP||DeviceID. Each entry is defined by wranIfDbsChannelIndicationEntry.

### **13.1.7.3.1 wranIfDbsChannelIndicationEntry**

Compound object that defines an entry in wranIfDbsChannelIndicationTable.

#### **13.1.7.3.1.1 wranIfBsDeviceId**

Device ID of device for which the channel is indicated as available.

#### **13.1.7.3.1.2 wranIfBsDeviceSn**

Serial number of device for which the channel is indicated as available.

#### **13.1.7.3.1.3 wranIfBsDeviceChannelNumber**

Channel number for which availability is indicated.

#### **13.1.7.3.1.4 wranIfBsDeviceMaxAllowedEirp**

Maximum allowed EIRP on the channel.

#### **13.1.7.3.1.5 wranIfBsDeviceLocation**

Location string of device requesting that the channel availability is indicated.

#### **13.1.7.3.1.6 wranIfBsDeviceDbsIndex**

Index of entry in wranIfDbsAccessTable that corresponds to the database service that provided this channel indication.

#### **13.1.7.4 wranIfDbsAccessTable**

This object stores information regarding access information for accessing a database service. There is more than one entry in this table, one for each database service that is available. Each entry is defined by wranIfDbsAccessEntry.

##### **13.1.7.4.1 wranIfDbsAccessEntry**

A compound object that stores entries in wranIfDbsAccessTable.

###### **13.1.7.4.1.1 wranIfDbsAccessEntryIndex**

Index of entry in this table.

###### **13.1.7.4.1.2 wranIfDbsAccessUrl**

URL used to access database service.

###### **13.1.7.4.1.3 wranIfDbsAccessCredentialType**

Indication of the type of credential to be used when authenticating access and transfer of information to the database service.

###### **13.1.7.4.1.4 wranIfDbsAccessCredential**

Credential BS or proxy device used to authenticate access to the database service, e.g., password, certificate.

###### **13.1.7.4.1.5 wranIfDbsAccessLastTxTime**

Time indication of the last transmission of a message to the database service.

###### **13.1.7.4.1.6 wranIfDbsAccessLastRxTime**

Time indication of the last reception of a message from the database service.

###### **13.1.7.4.1.7 wranIfDbsAccessAntennaInfoRequired**

Indication of whether or not antenna info is required to be transmitted to database service.

## Annex A

(normative)

### IEEE 802.22 regulatory domains and regulatory classes requirements

This annex describes the various technical parameters and specifications required by the various regulatory domains for operation of the IEEE Std 802.22 in the TV bands.

#### A.1 Regulatory domains, regulatory classes, and professional installation

Table A.1 specifies the regulatory domains and licensing regime where the IEEE 802.22 systems are planned to be authorized to operate in the TV bands.

**Table A.1—Regulatory domains**

Geographic area	Regulatory domain ISO 3166 (3 Bytes)	Licensing regime	Approval authority
United States	USA	Unlicensed	FCC
Canada	CAN	Licensed	IC
United Kingdom	GBR	—	OFCOM
—	—	—	—

Table A.2 specifies the authorized regulatory classes under their respective regulatory domains.

**Table A.2—Regulatory classes**

Regulatory domain	Regulatory class and profile	
	Fixed	Personal portable
USA	Stationary fixed	Mode I & II <sup>a</sup>
CAN	Stationary fixed	N/A
—	—	—

<sup>a</sup>The behavioral limits sets for Modes I and II are defined in the FCC Report and Order. However, IEEE Std 802.22 will only operate in portable nomadic Mode II.

Table A.3 specifies the requirement for professional installation of the WRAN BS and CPEs.

**Table A.3—Professional installation requirement**

Regulatory domain	Type of terminal		Definition of professional installer
	BS	CPE	
USA	Professionally installed	Professionally installed	A professional installer is a competent individual or team of individuals with experience in installing radio communications equipment and who normally provides service on a fee basis—such an individual or team can generally be expected to be capable of ascertaining the geographic coordinates of a site and entering them into the device for communication to a database.
CAN	Professionally installed	N/A	Same as for USA.
—	—	—	—

## A.2 Radio performance requirements

### A.2.1 Transmit power limits and EIRP requirements

Table A.4 specifies the transmitted EIRP levels authorized by the various regulatory domains for the different regulatory classes described in Table A.2.

**Table A.4—Transmit power level by regulatory domain and classes**

Regulatory domain	Regulatory class	Maximum BS EIR /Maximum antenna height	Maximum CPE EIRP/Maximum antenna height	Polarization
USA	Stationary fixed	4 W / 30 m AGL, <sup>a</sup> 76 m GHAAT <sup>b</sup>	4 W / 30 m AGL, 76 m GHAAT	Any
USA	Personal Portable (Modes I & II)	100 mW / N/A	100 mW / N/A	Any
CAN	Stationary fixed	500 W / ≤ 60 m AHAAT <sup>c</sup> 250 W / ≤ 90 m AHAAT 125 W / ≤ 120 m AHAAT 66 W / ≤ 180 m AHAAT 33 W / ≤ 240 m AHAAT 4 W / ≤ 500 m AHAAT	4 W / 10 m AGL	Vertical
—	—	—	—	—

<sup>a</sup> AGL: Above ground level

<sup>b</sup> GHAAT: Ground height above average terrain

<sup>c</sup> AHAAT: Antenna height above average terrain

### A.2.2 Transmit spectrum mask requirements

Table A.5 specifies the transmit spectrum mask requirements authorized by the various regulatory domains for the different regulatory classes described in Table A.2. Table A.5 refers to the appropriate figure (Figure A.1 and Figure A.2), which illustrate the various RF Masks applicable to the IEEE 802.22 systems. The power spectrum density (PSD) measurement shall be done over a measurement bandwidth of 100 kHz and a video bandwidth of 100 kHz with an average detector.

**Table A.5—Transmit spectrum mask requirements**

Regulatory domain	Regulatory class	Transmit spectrum mask	Description
USA	Stationary fixed	First adjacent channel  Beyond the outer edge of the first adjacent channel  (See Figure A.1)	55 dB below the highest power in a 6 MHz operating channel in 100 kHz bandwidth  Comply with FCC section 15.209(a)
USA	Portable Mode II	First adjacent channel  Beyond the outer edge of the first adjacent channel  (See Figure A.1)	55 dB below the highest power in a 6 MHz operating channel in 100 kHz bandwidth  Comply with FCC section 15.209(a)

Regulatory domain	Regulatory class	Transmit spectrum mask	Description
CAN	Stationary fixed( $\Delta f$ is referenced to the edge of the operating channel, Measurement bandwidth is 100 kHz, levels are expressed in dBc, relative to the total power in the operating channel)	$0.05 \leq \Delta f \leq 6$ $6 \leq \Delta f \leq 12$ $12 \leq \Delta f \leq 18$ $\Delta f > 18$ AND within <i>54–72 MHz, 76–88 MHz, 174–216 MHz, 470–608 MHz and 614–698 MHz</i>  <i>Outside the above cases (See Figure A.2)</i>	$44.9 + 1.1 \times (\Delta f)^{1.6}$ $37.8 + 4.4 \times \Delta f$ $70.2 + 1.7 \times \Delta f$  100.8  BS: $43 + 10 \times \log(P \text{ in Watts})$ CPE: Comply with Table 2 of RSS-210 [B43]
—	—	—	—

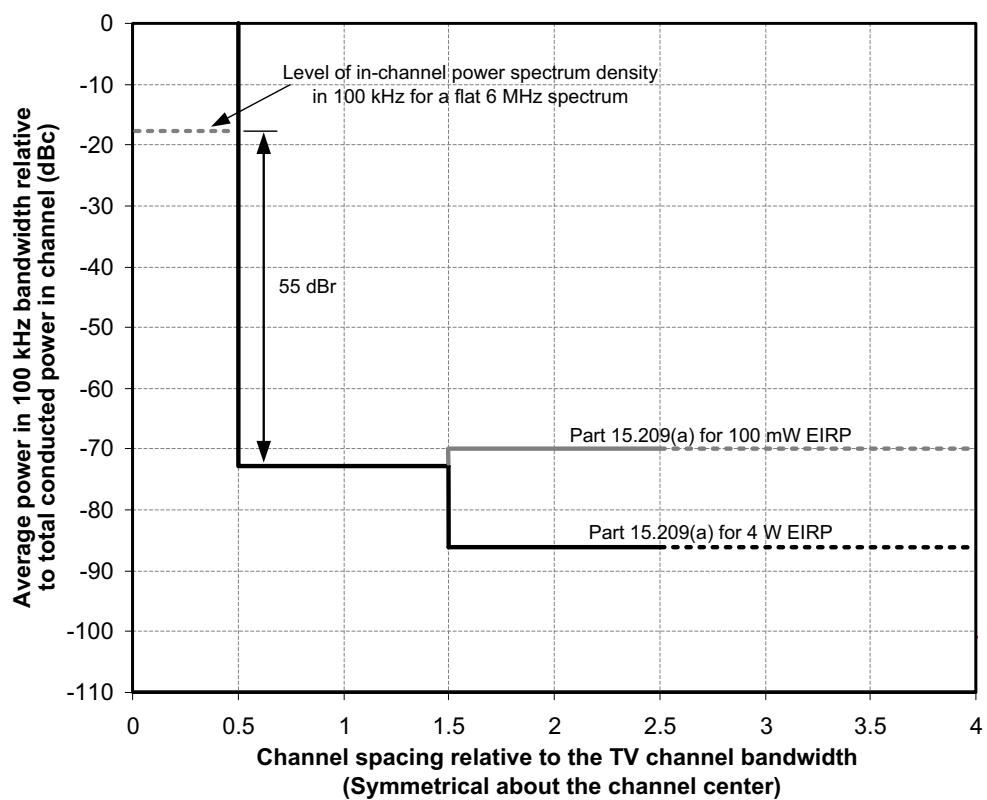
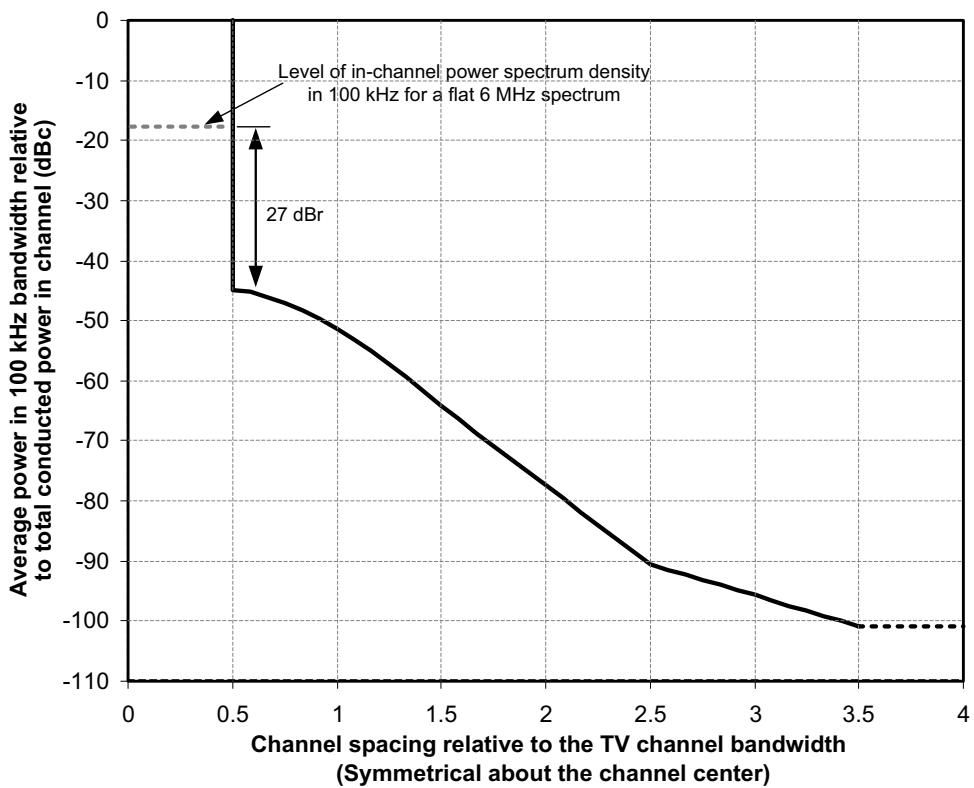


Figure A.1—IEEE 802.22 WRAN transmission RF mask for the USA



**Figure A.2—IEEE 802.22 WRAN transmission RF Mask for Canada**

### A.3 Channel availability and sensing requirements

#### A.3.1 Channel Availability requirements

Table A.6 specifies the channels that are not available inside the protected contour of a television station operating on channel “N” for the various regulatory domains.

**Table A.6—Channel availability requirements**

Regulatory domain	Regulatory class	Unavailable channels
USA	Stationary fixed	N N±1
USA	Portable (Modes I & II) (above 40 mW)	N N±1
USA	Portable (Modes I & II) (below 40 mW)	N
CAN	Stationary fixed	N N±1 N±2
—	—	—

### A.3.2 Channel move timing requirements

Table A.7 identifies channel move timing specifications authorized for various regulatory domains.

**Table A.7—Channel move timing specifications**

Regulatory domain	Regulatory class	Channel Move Time (T44) once incumbent signal is detected (seconds)
USA	Stationary fixed	2
USA	Portable (Mode I & II)	2
CAN	Stationary fixed	N/A
—	—	—

### A.3.3 Microphone protection radius

Table A.8 specifies the minimum distance from which a WRAN device can operate from a wireless microphone operation.

**Table A.8—Microphone protection radius**

Regulatory domain	Regulatory class	Microphone protection radius (MPR)
USA	Stationary fixed	1 km
USA	Portable (Mode I & II)	1 km
CAN	Stationary fixed	—
—	—	—

### A.3.4 Minimum distance for new geolocation

Table A.9 specifies the minimum WRAN device displacement beyond which a new query to the database service is required.

**Table A.9—WRAN device location accuracy and distance threshold**

Regulatory domain	Location accuracy	Confidence level	Distance threshold for portable devices
USA	100 m 300 m	67% 95%	50 m
CAN	—	—	—
—	—	—	—

Table A.10 gives the wireless microphone protection radius for the various regulatory domains.

**Table A.10—Microphone protection radius**

Regulatory domain	Regulatory class	Microphone protection radius (MPR)
USA	Stationary fixed	±25 m
USA	Portable (Mode I & II)	±25 m
CAN	Stationary fixed	—
—	—	—

### A.3.5 Spectrum sensing requirements

Table A.11 specifies the sensing requirements authorized for the various regulatory domains.

**Table A.11—Channel sensing requirements**

STA Index	Signal type	Regulatory domains		
		USA	CAN	—
0	Undetermined	Optional	Not required	—
1	IEEE 802.22 WRAN	Not required	Not required	—
2	ATSC	Optional	Not required	—
3	DVB-T	N/A	N/A	—
4	ISDB-T	N/A	N/A	—
5	NTSC	Optional	Not required	—
6	PAL	N/A	N/A	—
7	SECAM	N/A	N/A	—
8	Wireless Microphone	Optional	Not required	—
9	IEEE 802.22.1 Sync Burst	Not required	Not required	—
10	IEEE 802.22.1 PPDU MFS1	Not required	Not required	—
11	IEEE 802.22.1 PPDU MSF2	Not required	Not required	—
12	IEEE 802.22.1 PPDU MSF3	Not required	Not required	—
13–32	Reserved	—	—	—

### A.3.5.1 Spectrum sensing specifications for the USA

Table A.12 lists the rules applicable to spectrum sensing in the United States of America as established by the Federal Communication Commission (FCC R&O 08-260, MO&O 10-174).

**Table A.12—Channel sensing**

Regulatory domain	Type of signal	Sensing detection threshold (in dBm)	Data fusion rule for distributed sensing <sup>a</sup>	Monitoring requirements
USA	ATSC	−114 (averaged over 6 MHz)	“OR” rule	Detection threshold referenced to an omnidirectional receive antenna with a gain of 0 dBi
USA	NTSC	−114 (averaged over 100 kHz)	“OR” rule	Detection threshold referenced to an omnidirectional receive antenna with a gain of 0 dBi
USA	Wireless microphone	−107 (averaged over 200 kHz)	“OR” rule	Detection threshold referenced to an omnidirectional receive antenna with a gain of 0 dBi

<sup>a</sup>The value “1” indicates detection.

### A.3.5.2 Channel monitoring requirements for the USA

Table A.13 specifies the channel monitoring requirements authorized for the U. S. regulatory domain.

**Table A.13—Channel monitoring requirements**

<b>Regulatory domain</b>	<b>Type of signal</b>	<b>Monitoring requirements</b>	<b>Monitoring period (seconds)</b>
USA	ATSC NTSC Wireless microphone	Acquiring a channel	30
USA	ATSC NTSC Wireless microphone	In-service	60

### A.3.6 Applicable Spectrum Manager policies

Table A.14 specifies the policies in Table 234 that the SM has to implement in the various regulatory domains.

**Table A.14—Applicable Spectrum Manager policies**

<b>Regulatory domain</b>	<b>Spectrum Manager policies</b>
USA	1a, 1b, 1c, 1d, 1e, 1f, 2, 3a, 3b, 4, 5, 6, 7, 8
CAN	N/A
—	—

## A.4 Device identification requirements

Table A.15 specifies the device identification requirements for the various regulatory domains.

**Table A.15—Device identification requirements**

<b>Regulatory domain</b>	<b>Minimum period</b>	<b>Maximum period</b>	<b>Signaling process</b>	<b>Timer</b>	<b>Note</b>
USA	8 seconds	15 minutes	CBP burst	$T_{CBP}$	The minimum time between transmission of a CBP packet carrying a Device ID and Serial Number for identification by spectrum monitoring systems to document potential interference situations.
CAN	N/A	N/A			
—	—	—			

Table A.16 specifies the frequency of accessing a database service for the different regulatory classes of devices for the various regulatory domains.

**Table A.16—Database service access requirements**

Regulatory domain	Maximum time without database service refresh (hours)	Maximum time without database service refresh
USA	Stationary fixed and nomadic	24 hours
USA	Portable (Mode II)	24 hours
CAN	N/A	N/A
—	—	—

## A.5 Channelization based on the regulatory domain

The system frequencies are the frequencies at which the transmitter and the receiver equipment operate. These frequencies and their utilization shall conform to the Radio Regulations of the International Telecommunication Union (ITU) as well as the various Regional ITU Agreements as appropriate. The following Tables list the frequencies corresponding to the TV channels used for WRAN operation in various regulatory domains.

### A.5.1 Frequency of TV channels in the USA

Table A.17 lists the center frequency of the TV channels in the USA regulatory domain.

**Table A.17—Frequency of TV channels in the USA regulatory domain**

Country	Regulatory class (3Bytes)	Channel number (1 Byte)	Center frequency	Max. bandwidth (MHz)
USA	USA	2	57	6
USA	USA	3	63	6
USA	USA	4	69	6
USA	USA	5	79	6
USA	USA	6	85	6
USA	USA	7	177	6
USA	USA	8	183	6
USA	USA	9	189	6
USA	USA	10	195	6
USA	USA	11	201	6
USA	USA	12	207	6
USA	USA	13	213	6
USA	USA	14	473	6
USA	USA	15	479	6
USA	USA	16	485	6
USA	USA	17	491	6
USA	USA	18	497	6
USA	USA	19	503	6
USA	USA	20	509	6
USA	USA	21	515	6
USA	USA	22	521	6

<b>Country</b>	<b>Regulatory class (3Bytes)</b>	<b>Channel number (1 Byte)</b>	<b>Center frequency</b>	<b>Max. bandwidth (MHz)</b>
USA	USA	23	527	6
USA	USA	24	533	6
USA	USA	25	539	6
USA	USA	26	545	6
USA	USA	27	551	6
USA	USA	28	557	6
USA	USA	29	563	6
USA	USA	30	569	6
USA	USA	31	575	6
USA	USA	32	581	6
USA	USA	33	587	6
USA	USA	34	593	6
USA	USA	35	599	6
USA	USA	36	605	6
USA	USA	37	611	6
USA	USA	38	617	6
USA	USA	39	623	6
USA	USA	40	629	6
USA	USA	41	635	6
USA	USA	42	641	6
USA	USA	43	647	6
USA	USA	44	653	6
USA	USA	45	659	6
USA	USA	46	665	6
USA	USA	47	671	6
USA	USA	48	677	6
USA	USA	49	683	6
USA	USA	50	689	6
USA	USA	51	695	6

### A.5.2 Frequency of TV channels in Canada

The center frequency of the TV channels listed in Table A.17 also applies to Canada.

### A.5.3 Frequency of TV channels in Western Europe (System B)

Table A.18 lists the center frequency of the TV channels in Western Europe and many other countries in Africa, Asia, and the Pacific (BW = 7 MHz).

**Table A.18—Frequency of TV channels in Western Europe and many other countries in Africa, Asia, and the Pacific (BW= 7 MHz) (System B)**

Channel	Center frequency	Channel	Center frequency	Channel	Center frequency
2	50.5	6	184.5	10	212.5
3	57.5	7	191.5	11	219.5
4	64.5	8	198.5	12	226.5
5	177.5	9	205.5		

### A.5.4 Frequency of TV channels in Western Europe (System H)

Table A.19 lists the center frequency of the TV channels in Western Europe and many other countries in Africa, Asia, and the Pacific (BW = 8 MHz).

**Table A.19—Frequency of TV channels in Western Europe and many other countries in Africa, Asia, and the Pacific (BW= 8 MHz) (System H)**

Channel	Center frequency	Channel	Center frequency	Channel	Center frequency
21	474	38	610	55	746
22	482	39	618	56	754
23	490	40	626	57	762
24	498	41	634	58	770
25	506	42	642	59	778
26	514	43	650	60	786
27	522	44	658	61	794
28	530	45	666	62	802
29	538	46	674	63	810
30	546	47	682	64	818
31	554	48	690	65	826
32	562	49	698	66	834
33	570	50	706	67	842
34	578	51	714	68	850
35	586	52	722	69	858
36	594	53	730		
37	602	54	738		

#### A.5.5 TV channels prohibited from broadcasting operation in various regulatory domains

Table A.20 lists the TV channels in which broadcast incumbent operation is prohibited in various regulatory domains. This information can be used to speed up the spectrum sensing process by avoiding spectrum sensing in these channels since no broadcast incumbents will ever be present (see IPC-UPD, 7.7.17.4).

**Table A.20—Frequency of TV channels in Western Europe and many other countries in Africa, Asia, and the Pacific (BW= 8 MHz) (System H)**

Regulatory domain	TV channels prohibited from broadcast operation
U. S.	37
CA	37
—	—

## Annex B

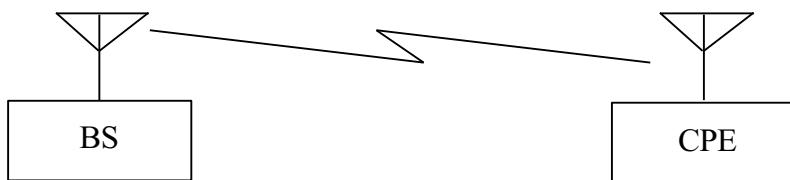
(informative)

### Multicarrier fine ranging method

#### B.1 General description

Fine terrestrial ranging enables IEEE 802.22 base stations to locate their CPEs. It does this by providing a fine receiver timing alignment, in the order of a nanosecond, amidst multipath propagation, even if the sampling interval of the receiver is around 146 ns (i.e., corresponding to  $8/7 \times 6$  MHz). It also provides for detection and acquisition of the channel impulse response representative of the received signal distortion caused by the transmission channel. Such information lies in understanding and processing the arrangement of carriers at reception.

One of the methods to obtain or confirm the geographic location of a device is to estimate the distance between a given device and many other devices with known geographic positions. Figure B.1 illustrates the downstream process. The converse is valid in upstream by swapping the BS and CPE roles as transmitters and receivers of the ranging signal. First, a known set of coherent carriers is transmitted in an OFDM symbol. The transmitted symbol then propagates from the transmitter to the receiver through the channel. This convolves the channel characteristics with the set of coherent carriers.



**Figure B.1—Transmitter-receiver setup**

Bandwidth restrictions cause time spreading and blurring of multipath rays but do not affect the precision of the time of arrival of these rays. An extraction of the exact time of arrival of the multipath rays relative to the OFDM symbol sampling time at the receiver (channel impulse response relative to the receiver timing alignment) is done by capturing an OFDM symbol. Once captured, the balance of the process may be done locally at the receiver or remotely, even offline. The captured sample set is processed by performing a Digital Fourier Transform (DFT), which makes it pass from the time domain to the frequency domain. In the frequency domain, all carriers not used for the ranging process are decimated by multiplying them by zero. On the carriers used for ranging, the transmitter's PN sequence is removed (which modulated the initial transmitted ranging carriers). An IDFT is then applied. To deconvolve the channel characteristics, a correlation function (representing the theoretical perfect channel model including the effect of the filters at the transmit and receive ends) is used to recover the channel impulse response as received.

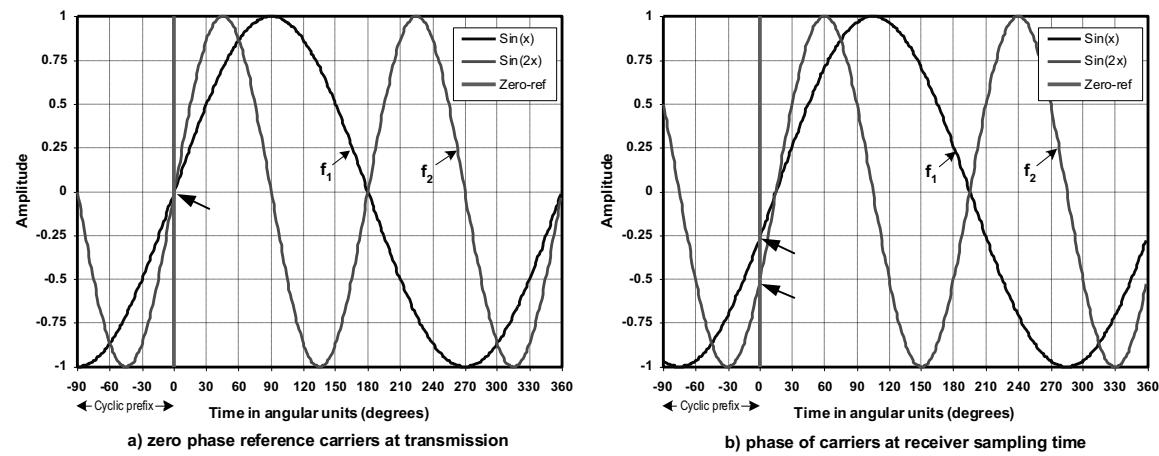
Assume a set of coherent OFDM carriers simultaneously or sequentially sent over the air by the transmitter, located at the transmission origin space-time point. If the receiver, located at the reception destination space-time point, locks to the longest wavelength carrier in the OFDM symbol, the phase difference between the signal at the origin point and the signal at the destination point can be equated to a flight time equal to the propagation time of the signal from the origin to the destination along the medium. (For the moment let's assume a single transmission ray with no multipath.) Even in such a simplistic case, an

OFDM receiver will receive with a phase that can be considered arbitrary since there is no reference to which it can be compared at the receiving point. Furthermore, the receiver per se, has no way of knowing the absolute delay between the transmitter and the receiver as the receiver has no knowledge of when the signal it received was transmitted.

Transmitting a second carrier with a known phase relationship to the first carrier at a different frequency allows the comparison of phase between the two carriers at the receiver. Assuming that the phase relationship of the signal emitted at transmission time is known, the reception phase warp caused by receive timing misalignment allows one to compute the receiver's time of arrival relative to its sampling time because a given time of arrival relative to the receiver sampling time will cause a predictable and measurable phase difference between these two carriers.

Figure B.2a) depicts an example of sine wave components of an OFDM symbol as emitted by the transmitter with a 1/4 cyclic prefix added in front of the symbol to allow absorption of channel multipath to alleviate inter-symbol interference. As a reference in this example, the phase of the subcarriers of the OFDM multiplex at time zero (0) is at zero degrees ( $0^\circ$ ) as illustrated by  $f_1$  and  $f_2$ , the two first subcarriers of the multiplex. Figure B.2b depicts the same symbol components as received by an OFDM receiver, with a timing misalignment. As can be seen on the green reference time line, this introduces a warp by offsetting  $f_1$  and  $f_2$  by different phase angles. Although the reception alignment error is apparently unknown at the receiver, it can be computed from this offset.

Receiver circuits also suffer from unwanted quantization misalignment. For example, with a 2048 sample IFFT in a 6 MHz band, samples are taken on a 146 nanosecond clock period. The misalignment of the receiver sampling time will therefore have a quantization step of 146 ns due to the sampling interval. Such misalignment can be fully quantified with precision from the phase relationship between the subcarriers of the OFDM multiplex at reception relative to this relationship at emission. Although the real misalignment may be of a fraction of the sampling clock, this method can precisely compute the sub-quantization misalignment as well as the channel multipath characteristics.



**Figure B.2—OFDM subcarriers phase relationship at transmission and reception**

This phase difference, for a given time of arrival relative to the receiver sampling time increases linearly with the difference in frequency between the two carriers. If multiple carriers are used in the transmitted signal, the phase difference is linearly related to their difference in frequency. This is a component of what will be called multicarrier “phase warping” from now on. In a multi-mode propagation scenario where multiple echoes will be generated in the transmission channel (i.e., multipath, channel time spreading), many carriers will be required to resolve these multiple transmission paths and the sum of all the received signals may cause complex and significant amplitude and phase variations from one carrier to the next, which will hereon be referred to as “complex warping” (i.e., a multicarrier phase/amplitude twist or curve

in the frequency domain that has developed in the transmission channel and from the receiver sampling time misalignment and the convolution with the channel multipath characteristics from something that would otherwise be ideally be flat).

Such complex warping has been viewed as a nuisance in conventional communication systems, i.e., an impairment that must be compensated for and eliminated as much as possible. Conventionally, this is done in multicarrier systems by interpolating the variations extracted from known reference pilot carriers in the time and frequency domains and subtracting it from the data carriers. This complex warping "nuisance" is in fact rich with information related to the multipath characteristics of the transmission channel and precise information on the time of arrival of the transmitted signal relative to the receiver sampling time. The fine ranging process capitalizes on the fact that any complex phase/amplitude sensitive receiver apparatus, such as coherent quadrature amplitude demodulators found in OFDM receivers already acquire multi-carrier amplitude and phase with a given resolution. Utilization of such complex warping information, which is normally used to help the receiver to recover the transmitted data, can be used to re-establish the precise timing of the received signal relative to the receiver sampling time with minimal hardware addition.

The following example will be used to further illustrate some of the aspects of the operating principles. All the ranging carrier tones are sine waves transmitted with known phase relationship defined by a known, well-chosen PN sequence to minimize the peak-to-average ratio of the transmitted signal while allowing other data to be simultaneously sent over the carriers that are not used for ranging purposes.

Note that the impulse and the chirp waveforms used in conventional radar applications can be modeled as special PN sequences cases of multicarrier waveforms. The impulse corresponds to all carriers being transmitted at the same amplitude and with the same phase (i.e., the PN-sequence in this case is equal to [1 1 1 ...]). A linear chirp corresponds to the amplitude and phase of the carriers being modulated by other known complex sequences, well documented in public references.

Let  $f_1$  be the first carrier and  $f_2$  be the second, as per Table B.1. The output signal may be decomposed as the sum of approximately 2000 orthogonal waves (Table B.1 depicts a few selected carriers). Wave  $f_1$  has a longer wavelength than  $f_2$  as the wavelength is equal to  $c/f$  where  $c$  is the speed of light in the example medium (free space);  $c = 299792458$  m/s. This mechanism is invariant, even when the tones are up-converted to a set of RF carrier waves or down-converted to an IF or baseband level, whatever the RF frequency of the carrier wave (or channel).

**Table B.1—Example list of some OFDM carriers**

Carrier/ Tone	Frequency (Hz)	Wavelength (m)	15° flight time uncertainty (m)
$f_1$	3,000	99930.819333	4163.78
$f_2$	6,000	49965.409666	2081.89
$f_4$	12,000	24982.704833	1040.95
$f_8$	24,000	12491.352417	520.47
$f_{16}$	48,000	6245.676208	260.24
$f_{32}$	96,000	3122.838104	130.12
$f_{64}$	192,000	1561.419052	65.06
$f_{128}$	384,000	780.709526	32.53
$f_{256}$	768,000	390.354763	16.26
$f_{512}$	1,536,000	195.177382	8.13
$f_{1024}$	2,997,000	100.030850	4.17
$f_{1999}$	5,997,000	49.990404	2.08

The tones are issued in a coherent fashion as part of an OFDM symbol where the IDFT of the transmitter was instructed to output all tones with a zero phase offset at the beginning of the burst (ignoring the PN sequence modulation at this time for simplicity).

NOTE—Any tone pair may be used, the tones are selected here for illustrative purposes only, and their phases may be arbitrary, provided their relative emitted phase is known by the transmitter and receiver, i.e., the coherence between carriers referred to above.

When the receiver locks onto carrier tone  $f_1$ , it will be able to lock with a phase resolution proportional to its phase discrimination ability. Let's assume that the receiver apparatus is able to receive 64-QAM symbols, then as per Table B.2, it should at least be able to phase lock to the  $f_1$  QAM-64 within approximately 15°. This sample 15° uncertainty translates into a large time of arrival uncertainty as depicted in the rightmost column of 0. Note that other reception and demodulation modes have different resolution but this in no way denies the warp measurement principles.

**Table B.2—64-QAM Constellation angle limits**

(first value is the relative amplitude, second value is the phase angle, and the pair of values represents the 64-QAM modulation levels)

<b>135°</b>		<b>127°</b>		<b>117°</b>		<b>104°</b>		<b>90°</b>		<b>76°</b>		<b>63°</b>		<b>53°</b>		<b>45°</b>
9.9 135° -7,+7		8.6 125° -5,+7		7.62 113° -3,+7		7.07 98° -1,+7		7.07 82° +1,+7		7.62 67° +3,+7		8.6 57° +5,+7		9.9 45° +7,+7		
143°		<b>135°</b>		<b>124°</b>		<b>108°</b>		<b>90°</b>		<b>72°</b>		<b>56°</b>		<b>45°</b>		<b>37°</b>
		7.07 135° -5,+5		5.83 121° -3,+5		5.1 101° -1,+5		5.1 79° +1,+5		5.83 59° +3,+5		7.07 45° +5,+7		8.6 36° +7,+5		
153°		<b>146°</b>		<b>135°</b>		<b>117°</b>		<b>90°</b>		<b>63°</b>		<b>45°</b>		<b>34°</b>		<b>27°</b>
		5.83 149° -5,+3		4.24 135° -3,+3		3.16 108° -1,+3		3.16 72° +1,+3		4.24 45° +3,+3		5.83 31° +5,+3		7.62 23° +7,+3		
166°		<b>162°</b>		<b>153°</b>		<b>135°</b>		<b>90°</b>		<b>45°</b>		<b>27°</b>		<b>18°</b>		<b>14°</b>
		5.1 169° -5,+1		3.16 162° -3,+1		1.41 135° -1,+1		1.41 45° +1,+1		3.16 18° +3,+1		5.1 11° +5,+1		7.07 8° +7,+1		
180°		<b>180°</b>		<b>180°</b>		<b>180°</b>		n/a		<b>0°</b>		<b>0°</b>		<b>0°</b>		<b>0°</b>
		5.1 191° -5,-1		3.16 198° -3,-1		1.41 225° -1,-1		1.41 315° +1,-1		3.16 342° +3,-1		5.1 349° +5,-1		7.07 352° +7,-1		
194°		<b>198°</b>		<b>206°</b>		<b>225°</b>		<b>270°</b>		<b>315°</b>		<b>334°</b>		<b>342°</b>		<b>346°</b>
		5.83 211° -5,-3		4.24 225° -3,-3		3.16 252° -1,-3		3.16 288° +1,-3		4.24 315° +3,-3		5.83 329° +5,-3		7.62 337° +7,-3		
206°		<b>214°</b>		<b>225°</b>		<b>243°</b>		<b>270°</b>		<b>297°</b>		<b>315°</b>		<b>326°</b>		<b>333°</b>
		7.07 225° -5,-5		5.83 239° -3,-5		5.1 259° -1,-5		5.1 281° +1,-5		5.83 301° +3,-5		7.07 315° +5,-3		8.6 325° +7,-3		
217°		<b>225°</b>		<b>236°</b>		<b>252°</b>		<b>270°</b>		<b>288°</b>		<b>304°</b>		<b>315°</b>		<b>323°</b>
		8.6 237° -5,-7		7.62 247° -3,-7		7.07 262° -1,-7		7.07 278° +1,-7		7.62 293° +3,-7		8.6 306° +5,-7		9.9 315° +7,-7		
<b>225°</b>		<b>233°</b>		<b>243°</b>		<b>256°</b>		<b>270°</b>		<b>284°</b>		<b>297°</b>		<b>307°</b>		<b>315°</b>

When the receiver receives carrier tone  $f_2$ , it detects its phase relative to the phase of the carrier  $f_1$  (i.e., part of the complex warping) and hence determines by demodulation of these two carriers the precise received timing of these tones relative to the receiver sampling time.

Receiving and demodulating tones with further spectral separation will result in even larger phase differences from the complex warping effect as, for a given misalignment between the timing of the sampling process used to build the analog signal from its digital representation at the transceiver and the timing of the sampling process to convert the received signal from its analog form to its digital representation at the receiver, the phase difference is proportional to the frequency spacing between the carriers (see Figure B.2). This permits further refinement to the measurement of the relative timing of the received signal, improving the precision of the timing measurement. The CPE may now transmit back the complex warp information to the BS when requested. The CPE is also asked to transmit a set of reference carriers on the upstream. The BS, upon reception and measurement of the signal, can then establish its own received complex warp and determine the time of arrival of this signal relative to its own sampling time.

The total back and forth flight time can then be determined with high accuracy based on the number of sampling periods lapsed since the transmission of the signal less the number of sampling periods that took the CPE to respond (assuming that the size of the sampling period at both ends is exactly the same, i.e., the terminals are in frequency lock), and corrected by the delays of arrival at both transceivers relative to their respective sampling times from both sets of complex warp information, i.e., that recovered by the receiver in the CPE and that recovered by the receiver in the BS. The reason why flight time may now be computed precisely is because, although the CPE has no knowledge of when the BS transmitted its original signal, the BS does have this information. Since the flight time is the sum of the time from the BS to the CPE and then the response from the CPE to the BS, the resulting uncertainty in this implementation example is half that depicted in Table B.2 or approximately 1 meter for a 6 MHz channel bandwidth and 64-QAM demodulation phase resolution. Note that the time at which the CPE sends its reference upstream burst is known by the BS since it is the BS that determines this time in the upstream map.

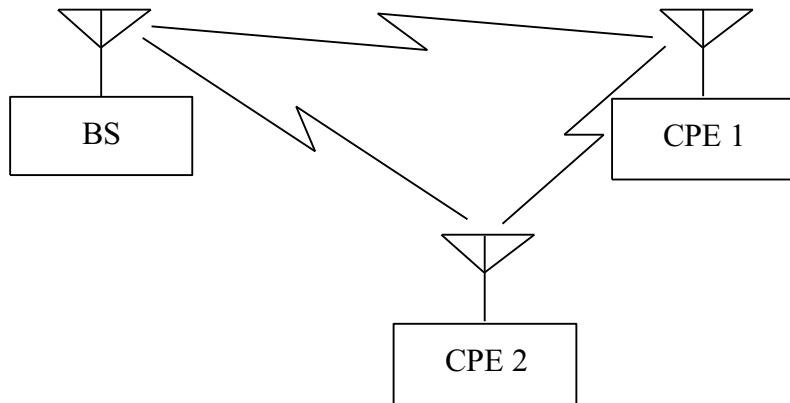
When  $N$  multiple carriers are used, an equation of  $N$  unknowns may be solved. One of these unknowns is the receiver sampling time misalignment that is represented by a linear slope in the frequency domain while channel multipath echoes will cause nutations around this slope. Therefore, in theory,  $N$  ideally positioned carriers should allow for the resolution of  $N-1$  echo paths in such a multipath environment.

Other demodulation processes may be used to achieve the same intention. For example, one may elect to use an apparatus where the receiver decodes the incoming signal “as is” and passes “whatever” information it acquired from the received carriers on the complex warping back to the signal originator in a timely manner for post processing, thereby allowing the originator to estimate with required or desired precision, the flight time of the carrier tones from the BS to the CPE. In fact, once the information has been acquired, it may be transmitted to one or a network of computing devices that collectively, embody the processing apparatus to extract and arrive at the time of arrival of the signal relative to the sampling time at the receiver and thus to the total flight time of the signal and thus the distance between the transceivers.

The above described ranging function between the BS and one of its CPEs can also be performed with the assistance of third party devices (see Figure B.3). As such, the BS may send a command to the first CPE to transmit a ranging burst at a specific time. It may also send a command to another CPE to listen to the first CPE while still being locked to the BS and then send the complex warp information acquired from the first CPE to the BS. Once the BS has established the ranges with the first CPE and the second CPE using the same method as described above, this new information will allow the system to determine the range between the two CPEs.

The BS then has all the information needed to carry out geometric triangulation calculations for locating itself and these two CPEs relative to each other. By doing this with many CPEs, the BS may build a map of the relative position of these CPEs, whether they are in line-of-sight or not, outdoor or indoor, etc. The BS may also collect additional information that will allow the system to build, among others, a multi-

dimensional map of the network, the distances between transceivers, the obstacles and terrain effects between these transceivers, multi-path propagation properties of the transmission medium, etc. Given adequate signal processing apparatus, a collectivity of such devices may reveal a valuable signal propagation map and a “radar image” including reflectors, refractors, scatterers, of the medium or of a geographical area in cases where the medium covers a given terrain and this may be enhanced if the devices may transmit or receive with directional discrimination.

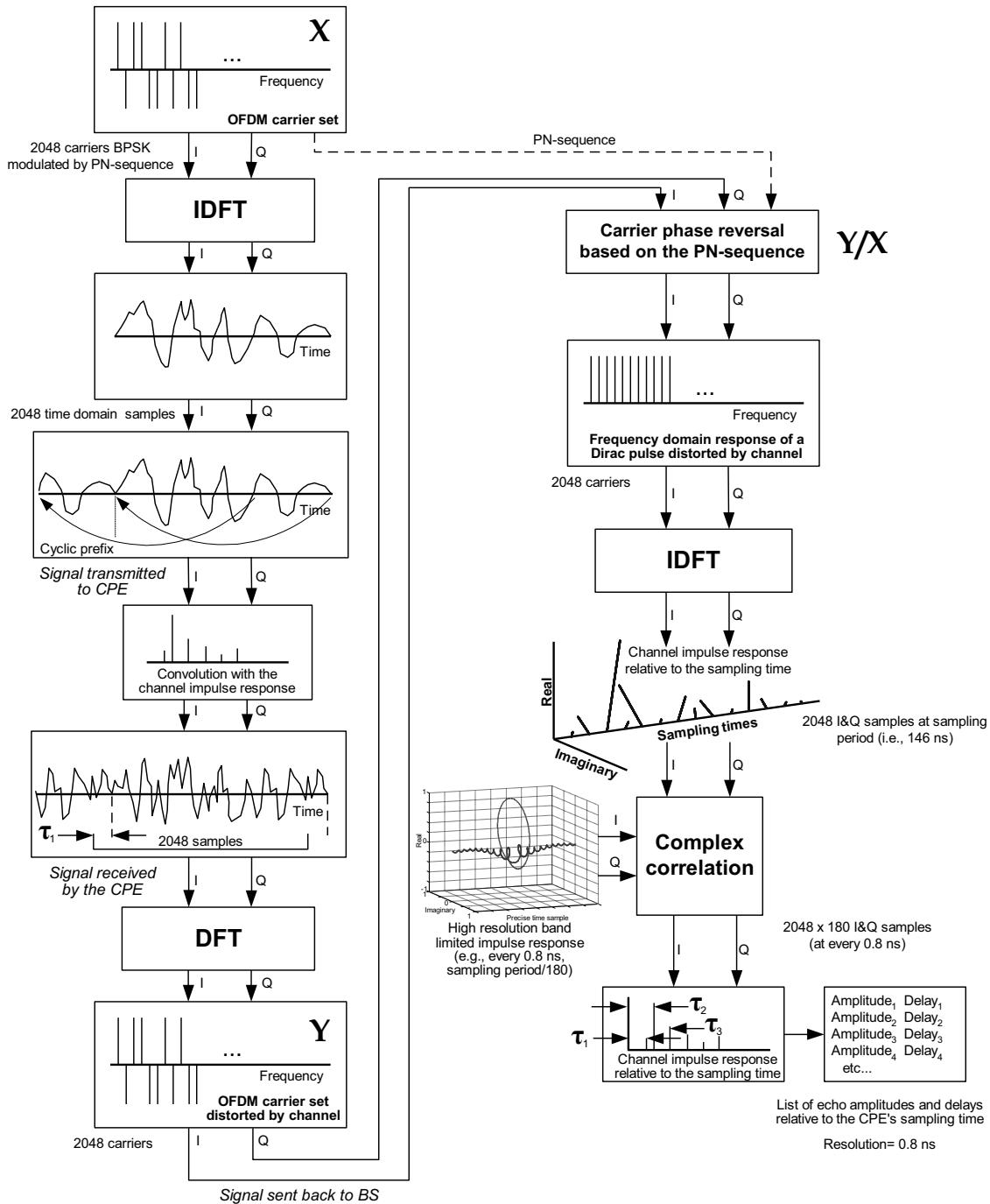


**Figure B.3—Multiple transmitter-receiver setup**

The above process can also be extended to a number of transceivers for which the geolocation is known (waypoints) so that the relative positioning obtained above can be converted into absolute location information. Again, the signal processing element does not need to be located at the transceivers as long as the information on the complex warping captured at each receiver is relayed to one or a network of computation devices where the calculation can be carried out and the precise ranging estimation can be translated into actual location estimation using this information and usual triangulation algorithms.

## B.2 Practical embodiment of the proposed multicarrier fine ranging method

A generic description of the concept of using a 64-QAM demodulator to recover the phase information from each of the OFDM carriers has been described above with the analysis of the complex spectrum warp to extract the time of arrival of the signal relative to the sampling time at the receiver. A more practical embodiment consists in using DFT and IDFT to recover the complex channel impulse response and a high resolution complex prototype function (corresponding to the precise time domain representation of the carrier set used for ranging in the case of the recovery of the OFDM signal from a perfect transmission channel) to carry-out a correlation with the coarser complex channel impulse response to extract the precise time of arrival of the signal relative to the sampling time of the receiver, see Figure B.4.



**Figure B.4—Practical embodiment of the multicarrier fine ranging method**

The above ranging can operate in very low SNR situation. It can operate in very high multipath conditions since all the information can be made available to a network ‘server’ where extensive off-line analysis of the channel impulse response collected at the receiver can be carried out to identify the echo that is closest to a line-of-sight condition. The time accuracy of the echo localization is only limited by the channel bandwidth, which will tend to smear echoes that are close to each other (i.e., within  $n/BW$  where  $n$  is to be determined empirically for different relative echo amplitudes). For more largely separated specular echoes, the accuracy is only limited by the quantization noise of the demodulator used at the receiver (QPSK, 16-

QAM, 64-QAM, etc.) and the channel SNR. However, repeated ranging and appropriate averaging of the results can allow for significant processing gain by reducing quantization noise. Some residual noise in the channel actually creates a probabilistic situation (dithering) that can be used to take advantage of further processing gain on the quantization resolution on the amplitude and phase measurements made by the demodulation process and thereby, remove some of the limitations imposed by the quantizing process. Two orders of magnitude more precision can typically be achieved beyond the size of the sampling period with the generation of an ‘over-defined’ prototype function used for the correlation with the complex channel impulse response.

A detailed description of the principles and methods used to implement this multi-carrier fine ranging method for terrestrial geolocation in the IEEE 802.22 WRAN systems is given in the two presentation listed in reference below.

### B.3 References

[1] [https://mentor.ieee.org/802.22/dcn/10/22-10-0054-01-0000\\_OFDM-based Terrestrial Geolocation.ppt](https://mentor.ieee.org/802.22/dcn/10/22-10-0054-01-0000_OFDM-based Terrestrial Geolocation.ppt)

[2] <https://mentor.ieee.org/802.22/dcn/10/22-10-0055-0000-Multicarrier-ranging.pdf>

## Annex C

(informative)

### Sensing

This annex contains descriptions of a number of sensing techniques. A sensing technique is an implementation of the spectrum sensing function.

There are several classifications of sensing techniques. First a sensing technique can be classified as either signal specific or blind. A signal specific sensing technique is based on features of specific signal type. A blind sensing technique does not rely on features of a specific signal type.

The WRAN can begin sensing a channel using a coarse sensing technique. If a signal is detected then the channel is occupied. If a signal is not detected then fine sensing can be used to sense for weaker signals.

A sensing technique can be classified as either a fine sensing technique or a coarse sensing technique. A fine sensing technique is able to detect the presence of a signal at the required signal power level. A coarse sensing technique may not be able to detect the presence of a signal at the required signal power; however, it may still be useful for detecting higher-power signals often in a shorter period of time.

Each subclause in this annex describes a specific sensing technique. The first three sensing techniques are blind sensing techniques and the next eleven are signal specific sensing techniques.

Performance for each of the sensing techniques is also included in each subclause. The primary performance metric is the required SNR at which the probability of detection is greater or equal to 0.9 for all multipath conditions. For the ATSC signals the multipath was modeled by using twelve representative signals from IEEE 802.22 Contribution 22-07-0359-00-0000 [6]. For each sensing technique the sensing time is also included. In many cases if the sensing time is increased the required SNR will decrease.

Some sensing techniques are sensitive to uncertainty in the noise power. In other words the estimate of the noise power  $\hat{P}_N$  is within  $\pm\Delta$  of the true noise power,

$$\hat{P}_N = P_N + P_E$$

where

$$-\Delta \leq P_E \leq \Delta$$

In some sensing techniques the detector threshold is a function of the noise power estimate, so an error in that estimate can affect the detector performance.

If the sensing technique is sensitive to noise uncertainty then the required SNR is given for various values of the noise uncertainty parameter  $\Delta$ .

#### C.1 Blind sensing techniques

A blind sensing technique does not depend on specific signal features. There are three blind sensing techniques described in this annex: the energy detector, the eigenvalue sensing technique and the multi-resolution sensing technique.

### C.1.1 Energy (power) detector

The energy, or power, detector is a blind detector that does not rely on features of a specific signal type. This sensing technique may not be able to meet the co-channel sensing requirements; however, this sensing technique is a simple method of quickly determining if a signal is present in the channel, except for the case of weak signals. Hence this is a coarse sensing technique.

To sense channel N with this sensing technique the sensing receiver is tuned to that channel and the RF signal is converted to an intermediate frequency (IF) where a 6 MHz wide filter is used to filter out signals outside the channel N. After IF filtering the signal is down-converted to a base-band signal. The base-band signal is band-limited to  $\pm 3$  MHz. The band-limited signal is complex (in-phase and quadrature) sampled at 6 MHz. The sampled signal is,

$$y(n) = x(n) + w(n)$$

where  $x(n)$  is the signal component and  $w(n)$  is the noise component. The power of  $x(n)$  is  $P_S$  and the power of  $w(n)$  is  $P_N$ .

The test statistic for this sensing technique is,

$$T = \frac{1}{M} \sum_{n=1}^M y(n)y^*(n)$$

This is an estimate of the signal power. M is the number of samples. If the summation was not scaled by dividing by M then T would be an estimate of the signal energy. The choice of whether or not to scale by M does not affect the performance of the sensing technique. Since this is a rather simple test statistic it is possible to write an analytic formula for its probability density function. This is not always possible for a sensing technique.

The mean and variance of the test statistic are,

$$\begin{aligned} E[T] &= P_S + P_N \\ \text{var}[T] &= \frac{(P_S + P_N)^2}{M} \end{aligned}$$

For a large number of samples ( $M \gg 1$ ), by the Central Limit Theorem, we can approximate the test statistic as a Gaussian random variable,

$$f_T(t) = N\left(P_S + P_N, \frac{(P_S + P_N)^2}{M}\right)$$

Given this probability density function for the test statistic one can write a formula for the detector threshold based on the required false alarm probability,

$$\gamma = P_N \left[ 1 + \frac{Q^{-1}(P_{FA})}{\sqrt{M}} \right]$$

where  $Q(x)$  is the tail probability of a normalized zero-mean Gaussian random variable, and is given by,

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} e^{-x^2/2} dx$$

The sensing technique can be represented as a threshold comparison. If  $T > \gamma$  then the channel is classified as occupied and if  $T \leq \gamma$  then the channel is classified as vacant. The probability of detection depends on the signal power. The formula for the probability of detection is given by,

$$P_D = 1 - Q \left[ \frac{\sqrt{M}}{P_S + P_N} (P_S + P_N - \gamma) \right]$$

The performance of this sensing technique in detecting weak signals relies heavily on accurate knowledge of the value of the noise power. This dependency on accurate knowledge of the noise power can be seen by writing our estimate of the noise power  $\hat{P}_N$  as the sum of the true noise power  $P_N$  and an error in the noise power estimate,

$$\hat{P}_N = P_N + P_E$$

The magnitude of the error in the noise power estimate is less than  $\Delta$ , so we have,

$$-\Delta \leq P_E \leq \Delta$$

The threshold is set using the noise power estimate. And the actual probability of false alarm and probability of detection depend on the true noise power. If the noise power estimate  $\hat{P}_N$  is higher than the actual noise power  $P_N$  then the actual probability of false alarm and actual probability of detection will be lower than expected. This dependency on accurate knowledge of the noise power significantly limits the ability of this sensing technique to detect very weak signals ( $SNR << 0 dB$ ).

The primary performance metric for a sensing technique is the required SNR. For the following required SNR values the detector threshold has been set to give a probability of false alarm of 0.1. The required SNR is the SNR at which the sensing technique has a probability of detection of at least 0.9 for all multipath conditions. The energy detector is not significantly impacted by multipath since the bandwidth of 6 MHz is quite wide. The required SNR does depend on the noise uncertainty, so results are given for various values of noise uncertainty. The required SNR, for several sensing times and several values of noise uncertainty are given in Table C.1.

**Table C.1—Required SNR for the energy detector**

Sensing time	$\Delta = 0 \text{ dB}$	$\Delta = 0.5 \text{ dB}$	$\Delta = 1 \text{ dB}$
	Required SNR (dB)		
0.2 ms	-11	-5	-2.5
1 ms	-15	-6	-3
5 ms	-18	-6	-3

### C.1.2 Eigenvalue sensing technique

This sensing technique is blind since it does not rely on the specific signal characteristics. It is a coarse sensing technique for DTV detection but it meets the fine sensing requirements for wireless microphones.

### C.1.2.1 Eigenvalue-based sensing algorithms

Let  $y(t)$  be the continuous time received signal. Assume that we are interested in the frequency band with central frequency  $f_c$  and bandwidth  $W$ . We sample the received signal  $y(t)$  at a sampling rate  $f_s$ . In some applications, such as DTV detection, it is better that the sampling rate is larger than the channel bandwidth  $W$ . Let  $T_s = 1/f_s$  be the sampling period. The received discrete signal is then  $x(n) = y(nT_s)$ . There are two hypotheses:  $H_0$ : signal not exists; and  $H_1$ : signal exists. The received signal samples under the two hypotheses are therefore respectively as follows:

$$H_0 : x(n) = \eta(n)$$

$$H_1 : x(n) = s(n) + \eta(n),$$

where  $s(n)$  is the transmitted signal passed through a wireless channel (including fading and multipath effect), and  $\eta(n)$  is the white noise samples. Note that  $s(n)$  can be a superposition of multiple signals. The received signal is generally passed through a filter. Let  $f(k)$ ,  $k = 0, 1, \dots, K$  be the filter. The value of  $K$  is ... After filtering, the received signal is turned to

$$\tilde{x}(n) = \sum_{k=0}^K f(k)x(n-k), n = 0, 1, \dots$$

Let

$$\tilde{s}(n) = \sum_{k=0}^K f(k)s(n-k), n = 0, 1, \dots$$

$$\tilde{\eta}(n) = \sum_{k=0}^K f(k)\eta(n-k), n = 0, 1, \dots$$

Then

$$H_0 : \tilde{x}(n) = \tilde{\eta}(n)$$

$$H_1 : \tilde{x}(n) = \tilde{s}(n) + \tilde{\eta}(n)$$

Note that here the noise samples  $\tilde{\eta}(n)$  are correlated. If the sampling rate  $f_s$  is larger than the channel bandwidth  $W$ , we can down-sample the signal. Let  $M \geq 1$  be the down-sampling factor. If the signal to be detected has a much narrower bandwidth than  $W$ , it is better to choose  $M > 1$ . For notation simplicity, we still use  $\tilde{x}(n)$  to denote the received signal samples after down-sampling, that is:  $\tilde{x}(n) \approx \tilde{x}(Mn)$ .

Choose a smoothing factor  $L > 1$  and define

$$\mathbf{x}(n) = [\tilde{x}(n) \quad \tilde{x}(n-1) \quad \dots \quad \tilde{x}(n-L+1)]^T, n = 0, 1, \dots, N_s - 1$$

A suggested value of  $L$  is about 10. Define a  $L \times (K+1+(L-1)M)$  matrix as

$$X = \begin{bmatrix} f(0) & \dots & \dots & f(K) & 0 & \dots & 0 \\ 0 & \dots & f(0) & \dots & f(K) & \dots & 0 \\ & & \dots & & \dots & & \\ 0 & \dots & \dots & \dots & f(0) & \dots & f(K) \end{bmatrix}$$

Let  $\mathbf{G} = \mathbf{X}\mathbf{X}^H$ . Decompose the matrix into  $\mathbf{G} = \mathbf{Q}\mathbf{Q}^H$ , where  $\mathbf{Q}$  is a  $L \times L$  Hermitian matrix. The matrix  $\mathbf{G}$  is not related to signal and noise and can be computed offline. If analog filter or both analog

filter and digital filter are used, the matrix  $\mathbf{G}$  should be revised to include the effects of all the filters. In general,  $\mathbf{G}$  can be obtained to be the covariance matrix of the received signal, when the input signal is white noise only (this can be done in laboratory offline). The matrix  $\mathbf{G}$  and  $\mathbf{Q}$  are computed only once and only  $\mathbf{Q}$  is used in detection.

#### **C.1.2.1.1 Maximum-minimum eigenvalue (MME) detection**

**Step 1:** Sample and filter the received signal as described above.

**Step 2:** Choose a smoothing factor  $L$  and compute the threshold  $\gamma$  to meet the requirement for the probability of false alarm.

**Step 3:** Compute the sample covariance matrix

$$\mathbf{R}(N_s) = \frac{1}{N_s} \sum_{n=0}^{N_s-1} \mathbf{x}(n)\mathbf{x}^H(n)$$

where  $N_s$  is the number of samples.

**Step 4: Transform the sample covariance matrix to obtain**

$$\tilde{\mathbf{R}}(N_s) = \mathbf{Q}^{-1}\mathbf{R}(N_s)\mathbf{Q}^{-H}$$

**Step 5:** Compute the maximum eigenvalue and minimum eigenvalue of the matrix  $\tilde{\mathbf{R}}(N_s)$  and denote them as  $\lambda_{\max}$  and  $\lambda_{\min}$ , respectively.

**Step 6:** Determine the presence of the signal based on the eigenvalues and the threshold: if  $\lambda_{\max} / \lambda_{\min} > \gamma$ , signal exists; otherwise, signal not exists.

#### **C.1.2.1.2 Energy with minimum eigenvalue (EME) detection**

**Step 1:** Sample and filter the received signal as described above.

**Step 2:** Choose a smoothing factor  $L$  and compute the threshold  $\gamma$  to meet the requirement for the probability of false alarm.

**Step 3:** Compute the sample covariance matrix

$$\mathbf{R}(N_s) = \frac{1}{N_s} \sum_{n=0}^{N_s-1} \mathbf{x}(n)\mathbf{x}^H(n)$$

**Step 4:** Transform the sample covariance matrix to obtain

$$\tilde{\mathbf{R}}(N_s) = \mathbf{Q}^{-1}\mathbf{R}(N_s)\mathbf{Q}^{-H}$$

**Step 5:** Compute the average energy of the received signal  $\rho$ , and the minimum eigenvalue of the matrix  $\tilde{\mathbf{R}}(N_s)$ ,  $\lambda_{\min}$ .

**Step 6:** Determine the presence of the signal: if  $\rho / \lambda_{\min} > \gamma$ , signal exists; otherwise, signal not exists.

### C.1.2.2 Performance of the algorithms

The threshold  $\gamma$  in MME is determined by the ratio  $\lambda_{\max} / \lambda_{\min}$  and the required probability of false alarm ( $P_{fa}$ ). When there is no signal, the ratio is not related to noise power at all. Hence, it does not have the noise uncertainty problem. The same is valid for EME. Both methods do not need noise power estimation. The performances of the methods are not only related to SNR but also related to signal statistic properties.

In the following the performances of the methods are given based on simulations, where  $L = 10$ . The required SNR is the lowest SNR which meets the requirement of  $P_{fa} \leq 0.1$  and the probability of misdetection  $P_{md} \leq 0.1$ . Note that the SNR is always measured in one TV channel with 6 MHz bandwidth. For DTV, the results are averaged on the 12 specified DTV signals. Note that the performance of the methods can always be improved by increasing the sensing time.

- a) Simulations for DTV (single channel sensing). The simulation is done at IF band.

**Table C.2—Required SNR for DTV signal detection (single channel)**

Method	4 ms	8 ms	16 ms	32 ms
MME	-11.6 dB	-13.2 dB	-15 dB	-16.9 dB
EME	-10.5 dB	-12.1 dB	-14 dB	-15.8 dB

- b) Simulations for wireless microphone. The wireless microphone signal is down-converted into baseband. Table C.3 gives the simulation results for wireless microphone signals [average on 3 types of signals: soft speaker, loud speaker, and silence (Clanton, Kenkel, and Tang [3])]. The settings and procedures for the simulation are as follows. Baseband microphone signal is generated. The signal is sampled at sampling rate 12 MHz. The signal is then filtered with a low-pass filter with 6 MHz bandwidth. The signal is passed through a multipath simulator (Rayleigh fading with 5 taps). White noise samples (sampling rate 12 MHz) are generated and passed through the same filter. The signal and scaled noise are added together and then down-sampled (decimated) by a factor  $M = 2$ .

**Table C.3—Required SNR for wireless microphone signal detection**

Method	4 ms	10 ms
MME	-21.0 dB	-23.1 dB
EME	-16.4 dB	-18.4 dB

- c) Simulations for DTV (multiple channel sensing). The method can be used to detect multiple consecutive channels at the same time. Here an example is given for detecting three consecutive channels at the same time. The input signal is the captured DTV signal (one channel is occupied and the remaining two channels are vacant). The signal is down-converted into baseband. The signal and noise are then filtered by a baseband filter with bandwidth 18 MHz.

**Table C.4—Required SNR for DTV signal detection (three consecutive channels)**

Method	4 ms	16 ms
MME	-17.5 dB	-20.9 dB
EME	-15.6 dB	-19.1 dB

### C.1.3 Multi-resolution sensing technique

This is a coarse sensing technique for DTV.

#### C.1.3.1 MRSS overview

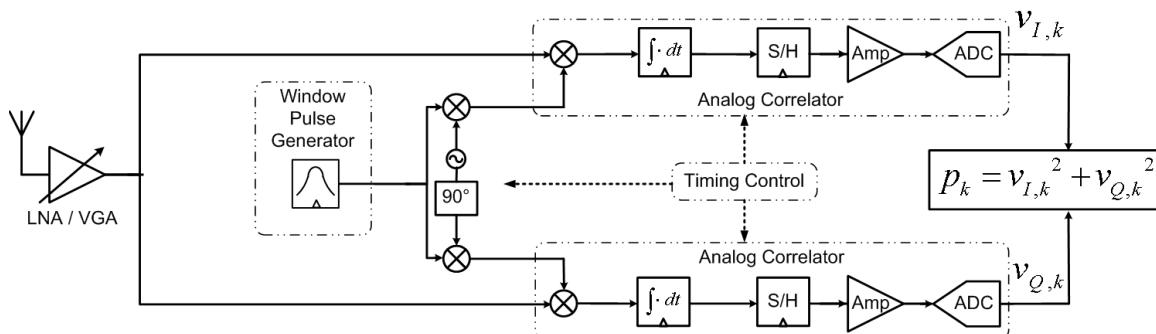
The basic theory of MRSS is presented as follows. Let's say  $w(t)$  is one pulse of a modulated window, as defined in Equation (C1), where  $f_c$  is the modulation frequency.  $y(t)$  is the convolution of  $w(t)$  with the incoming RF signal,  $r(t)$ . Equation (C3) is obtained with  $t = 0$  in Equation (C2). It shows that time-domain multiplication of the RF signal and modulated window is the same as the band-pass filtered RF signal by the band-pass characteristic of the modulated window.

$$w(t) = \begin{cases} \cos^4(\pi f_w t) \exp(j2\pi f_c t), & \text{if } -\frac{1}{2f_w} < t < \frac{1}{2f_w} \\ 0, & \text{elsewhere} \end{cases} \quad (\text{C1})$$

$$y(t) = \int_{-\infty}^{\infty} r(s)w(t-s)ds = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} R(\omega)W(\omega)e^{j\omega t}d\omega \quad (\text{C2})$$

$$y(0) = \int_{-\infty}^{\infty} r(s)w(-s)ds = \int_{-1/(2f_w)}^{1/(2f_w)} r(s)w(s)ds = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} R(\omega)W(\omega)d\omega \quad (\text{C3})$$

Figure C.1 shows a possible functional block diagram of MRSS. The receiving path is split into in- and quadrature-phase path to eliminate the need for the synchronization process. A window pulse generator generates one pulse of a window with various window frequencies,  $f_w$ , which are modulated with the sine or cosine wave from the local oscillator. The broadband RF signal from the omni-directional antenna is amplified with a low-noise amplifier (LNA). The gain of LNA should be maximized to have a minimum noise figure of the system, but too large of a gain will saturate the following multiplier, generating many unwanted harmonics. Therefore, an adequate gain control block is required before a multiplier. The analog correlator multiplies and integrates the amplified signal and modulated window pulse. With adequate timing control, the integrated output is sampled and digitized to generate the band-pass filtered amplitude information in in-phase and quadrature-phase components. A linear amplifier or a logarithmic amplifier can be placed in front of an analog-to-digital converter (ADC) in order to maximize the dynamic range utilization of the ADC. The digitized result is further processed in the digital domain. The detected signal power can be processed in a logarithmic domain to have a processing gain over the Gaussian noise.



**Figure C.1—Functional block diagram of the MRSS system**

### C.1.3.2 MRSS examples

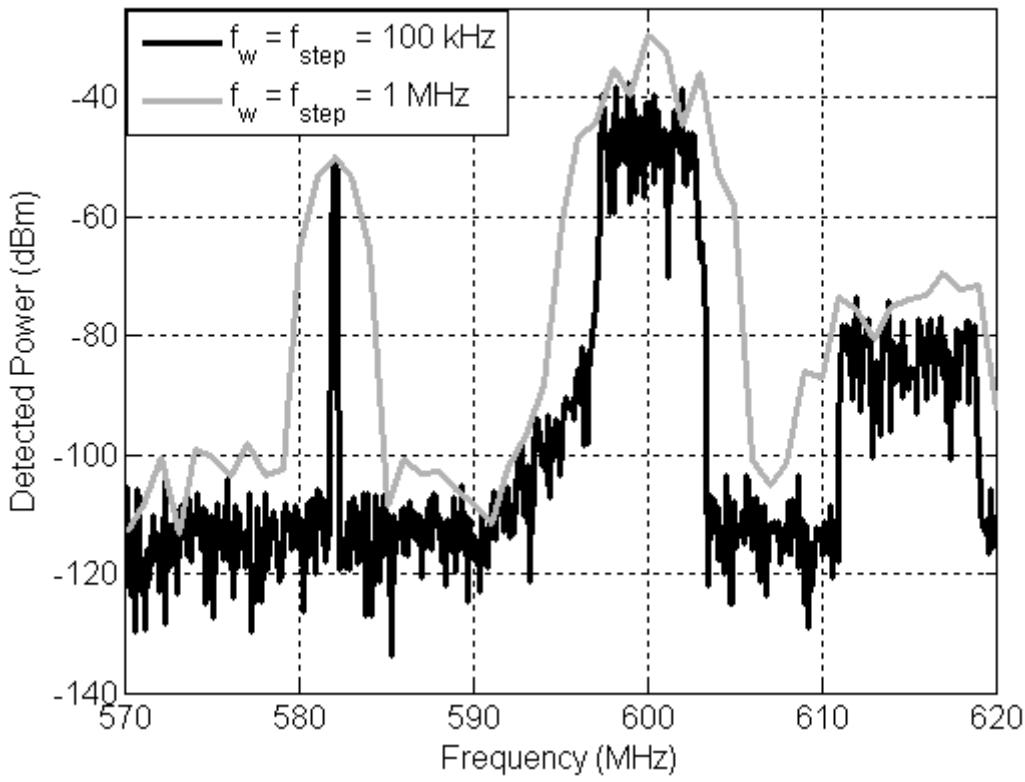
Figure C.2 shows the multi-resolution property of MRSS with two window frequencies, one with  $f_w = 100$  kHz and the other with  $f_w = 1$  MHz. The inputs to this simulation are a continuous wave (CW) signal of  $-50$  dBm at 582 MHz, Advanced Television Systems Committee (ATSC) signal of  $-30$  dBm at 600 MHz, and Digital Video Broadcasting-Terrestrial (DVB-T) signal of  $-70$  dBm at 615 MHz. ATSC uses 8-level vestigial sideband (8-VSB) modulation, and DVB-T uses the Orthogonal Frequency-Division Multiplexing (OFDM) modulation scheme. The total required time in performing MRSS can be calculated as

$$t_{Total} = \left( \frac{f_{end} - f_{start}}{f_{step}} + 1 \right) \times \left( \frac{N_{AVG}}{f_w} + t_{SW} \right) (\text{sec}) \quad (\text{C4})$$

where

- $f_{start}$  and  $f_{end}$  is the frequency sweep range of the local oscillator
- $f_{step}$  is the amount of frequency change in the oscillator
- $N_{AVG}$  is the number of averaging in one window modulation frequency
- $t_{SW}$  is the maximum switching settling time of the local oscillator

In Figure C.2, the window-modulation frequency of MRSS is swept from 570 MHz to 620 MHz with  $f_{step}$  equals  $f_w$ . No averaging is done in this case. Therefore, when  $f_w = 100$  kHz, it will have 500 results, each representing the detected signal power at the given window modulation frequency. In the same way, 1 MHz of  $f_w$  will have 50 results. If  $t_{SW}$  is assumed to be 10  $\mu\text{s}$ , the total processing time is 10.02 ms and 561  $\mu\text{s}$  for  $f_w = 100$  kHz and 1 MHz, respectively.



**Figure C.2—Fine ( $f_w = 100$  kHz) and coarse ( $f_w = 1$  MHz) resolution property of MRSS using the  $\cos^4(\pi f_w t)$  window. Inputs are CW ( $-50$  dBm @ 582 MHz), ATSC ( $-30$  dBm @ 600 MHz) and DVB-T ( $-70$  dBm @ 615 MHz)**

#### C.1.3.3 MRSS performances

MRSS has simulation has been performed for the case of ATSC signal. Captured TV signals provided by MSTV have been used as incumbent signal sources, and MRSS simulation has been preformed to get sensing threshold, required SNR and sensing time. The result of the simulation is summarized in Table C.5. In the simulation, FAR is set to 0.01 and 12 signals (W4748, W31148, W31135, W31136, W8648, W634, W327, W5135, W4939, W3248, W6836, W4934) has been used. For the window,  $f_w = 10$  kHz (time duration is 0.1 ms) is selected to get maximum accuracy. For the fast sensing, MRSS can be reconfigured easily to get faster but less accurate sensing by simply choosing wider window.

**Table C.5—Performance of MRSS**

NAVG		1	10	20	40	80	160
Sensing Time (ms)		0.1	1	2	4	8	16
Required SNR (dB)	PMD = 0.1	-3.19	-11.64	-14.00	-16.55	-19.67	-24.47
	PMD = 0.01	-0.01	-8.98	-11.43	-13.83	-16.36	-19.88

## C.2 Signal specific sensing techniques

A signal specific sensing technique relies upon specific signal features. There are seven signal specific sensing techniques described in this annex. Six of the techniques are for ATSC signals and one of the techniques is for wireless microphones. These are coarse sensing techniques.

### C.2.1 ATSC signature sequence correlation sensing technique

The ATSC signal contains several pseudo random noise (PN) sequences (ATSC [1]). The ATSC signal consists of 313 segments. One of these segments is called the Data Field Sync, which contains the PN sequences. This sensing technique involves converting the received signal to baseband and correlating the signal with a signature sequence based on these PN sequences. The output of the correlator is then processed to obtain a test statistic that is then compared to a threshold. C.2.1.1 explains the construction of the ATSC signature sequence. C.2.8.3 described the processing of the received signal, which consists of converting the IF signal to baseband and then correlating with the ATSC signature sequence. C.2.1.3 describes the construction of the test statistic when the sensing time is sufficient to guarantee observation of at least one ATSC Data Field Sync. C.2.1.4 describes the construction of the test statistic when the sensing time is sufficient to guarantee observation of at least two ATSC Data Field Syncs.

#### C.2.1.1 ATSC signature sequence

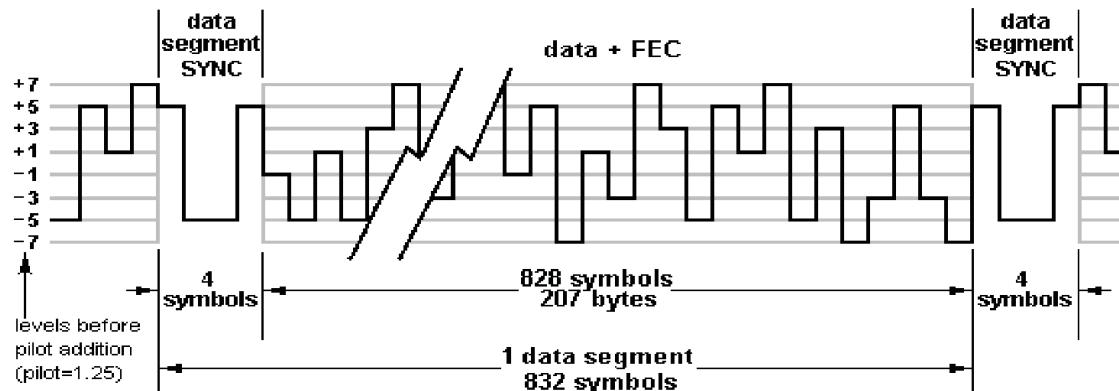


Figure C.3—ATSC DTV signal data segment

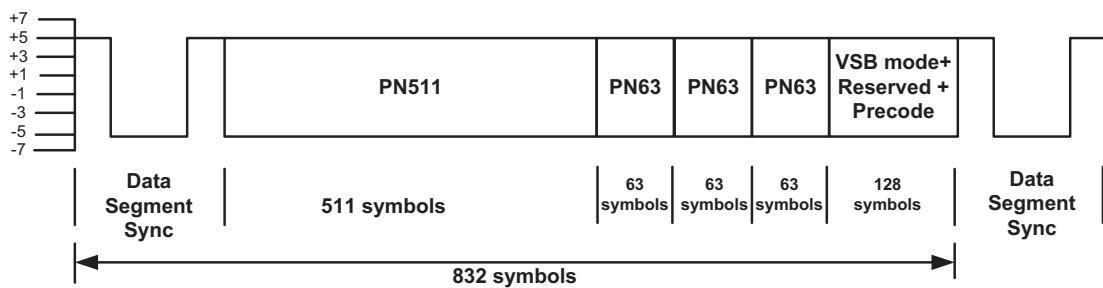


Figure C.4—ATSC DTV signal field sync segment

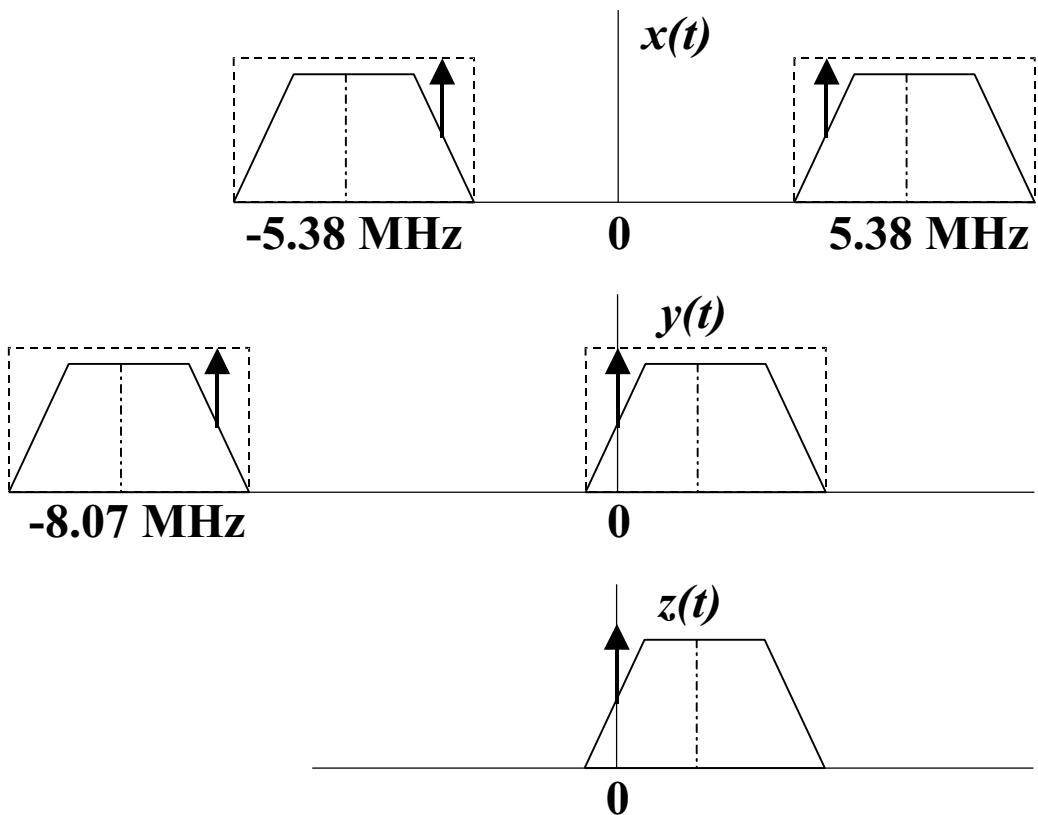
According to ATSC Digital Television Standard [1], DTV data are modulated using 8-Vestigial Sideband (8-VSB). Besides the eight-level digital data stream, a two-level (binary) four-symbol data Segment Sync is inserted at the beginning of each data segment. As shown in Figure C.3, a complete segment consists of

832 symbols: four symbols of 1001 pattern for data segment sync (Segment Sync), and 828 data symbols. Multiple data segments (313 segments) comprise a data field. The first data segment in a data field is called the data field sync segment (Field Sync). The structure of the data field sync segment is shown in Figure C.4. Therefore, a Field Sync occurs regularly every 24.2 ms. Hence, it is intuitive to implement a correlation detector to perform spectrum sensing using the Field Sync.

### C.2.1.2 Pilot recovery and down-conversion to base band

Since the received ATSC signal can have frequency offsets, rudimentary carrier recovery needs to be implemented before correlation can proceed. Also, since the symbol timing is unknown, correlation should be done with the complex signal, and the pilot value (+1.25) should be added to the reference signal. The algorithm steps are described below and the frequency domain representation is shown in Figure C.5.

- a) ATSC-DTV Signal:  $x(t)$ , at low intermediate frequency (IF) (as shown in Figure C.5).
- b) Perform carrier recovery, estimate carrier frequency,  $f_c$  as follows:
  - Perform a 2K FFT on a section of the received low-IF sequence  $x(t)$ .
  - Average the absolute value of the FFT output over a number of adjacent data sections, e.g., four sections.
  - Look for a peak in the vicinity of the ideal pilot position (e.g., within  $\pm 20$  kHz of the nominal pilot position).
  - Compare the peak to a threshold, and if greater than the threshold, the peak position is used to determine  $f_c$ .
- c) Demodulate:  $y(t) = x(t)e^{-j2\pi fct}$ . Note that  $y(t)$  is a complex signal with the pilot nominally at DC.
- d) Matched filter: filter  $y(t)$  with a SQRC filter with 11.5 % excess bandwidth and centered at 2.69 MHz, to get  $z(t)$ , which is still complex.



**Figure C.5—Frequency domain operations**

The complex base band signal is then processed by correlating the received signal to the reference signal, as described in C.2.1.3.

### C.2.1.3 Test Statistic using a Single ATSC Data Field

There are two possible synchronization patterns that can be used to detect the ATSC signal: field sync and data sync. The field sync pattern is described in C.2.1.3.1 while the segment sync pattern is described in C.2.1.3.2.

#### C.2.1.3.1 Field-sync based sensing technique

This subclause described correlation with the field sync pattern.

##### C.2.1.3.1.1 Binary sequence approach

Let  $q[n]$  denote the 832 symbols of the Field Sync segment shown in Figure C.4. Because the second PN63 sequence was flipped every other Field Sync segment and the last 128 symbols are unknown, we will simply zero these two parts in  $q[n]$ . Furthermore,  $q[n]$  will be zero padded to form  $p[n]$  because  $y[n]$  has a sampling rate of 21.524476 MHz, which is double of the symbol rate in the transmitter. For the convenience of statistic analysis, we will normalize  $p[n]$  so that

$$\sum_{n=0}^{L-1} p^2[n] = 1 \quad (C5)$$

where

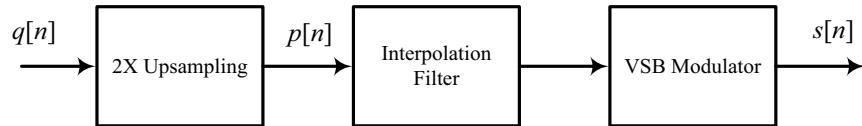
$L = 1664$  is the length of  $p[n]$ . Finally, the test statistic  $T_{FS}$  is defined as

$$T_{FS} = \max_{0 \leq i \leq W_{FS}-1} \left| \sum_{n=0}^{L-1} p[n] y[i+n] \right| \quad (C6)$$

where

$W_{FS} = 520892$  is the number of samples of  $y[n]$  in 24.2 ms

#### C.2.1.3.1.2 Complex sequence approach



**Figure C.6—Generation of the complex sequence**

In the previous subclause, we use a binary pilot sequence  $p[n]$  and correlate it with the received signal. However, the received pilot sequence is not binary. Thus, we should use a sequence that, of our knowledge best matches the received pilot sequence. The transmitted signal is a Vestigial Sideband (VSB) modulated signal. Therefore, instead of simply 2X up-sampling  $q[n]$  to form the pilot sequence  $p[n]$ , we shall add a low-pass interpolation filter and a VSB modulator so that the sequence  $s[n]$  shown in Figure C.6 best matches the transmitted Field Sync sequence. It is shown through simulations, that with this modification, the detection performance can be improved by 1.5 dB to 2.5 dB in terms of SNR.

#### C.2.1.3.1.3 Threshold calculation

For hypothesis  $H_0: y[n] = w[n]$ . After some calculations, we have

$$F_{T_{FS}}(t : H_0) = \left( \int_0^t \frac{2r}{\sigma^2} e^{-\frac{r^2}{\sigma^2}} dr \right)^{W_{FS}} \quad (C7)$$

where:  $F_{T_{FS}}(t : H_0)$  is the cumulative density function of TFS when the hypothesis is  $H_0$ . Then, for a desired false alarm rate PFA, the corresponding threshold  $\gamma_{FS}$  is given by

$$\gamma_{FS} = \sigma \left( \ln \frac{1}{1 - (1 - P_{FA})^{1/W_{FS}}} \right)^{1/2} \quad (C8)$$

#### C.2.1.3.1.4 Simulation results

The performances of the Field-Sync based algorithm with both binary and complex pilot sequences were demonstrated using computer simulations according to the spectrum sensing simulation model (Mathur, Tandra, Shellhammer, and Ghosh [9]). We set the false alarm rate equaling to 0.1 and use Equation (C8) to calculate corresponding threshold. The 12 reference Capture Data files are simulated. The required SNR for 0.1 of misdetection rate are given in Table C.6, Table C.7, and Table C.8 for the best, worst, and average case of the 12 reference captured data files. The parameter  $\Delta$  in the tables is the amount of the noise uncertainty.

**Table C.6—Required SNR for the Field-Sync based detector (Best case)**

Sensing Time/Sequence	$\Delta=0$ dB	$\Delta=0.5$ dB	$\Delta=1$ dB
	Required SNR (dB)		
24.2 ms/Binary	-12	-11.5	-11
24.2 ms/Complex	-14.5	-14	-13.5

**Table C.7—Required SNR for the Field-Sync based detector (Worse case)**

Sensing Time/Sequence	$\Delta=0$ dB	$\Delta=0.5$ dB	$\Delta=1$ dB
	Required SNR (dB)		
24.2 ms/Binary	-6	-5.5	-5
24.2 ms/Complex	-6.5	-6	-5.5

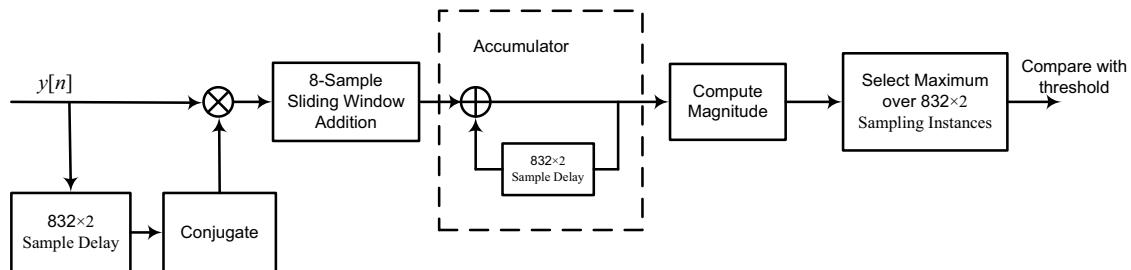
**Table C.8—Required SNR for the Field-Sync based detector (Average)**

Sensing Time/Sequence	$\Delta=0$ dB	$\Delta=0.5$ dB	$\Delta=1$ dB
	Required SNR (dB)		
24.2 ms/Binary	-8.5	-8	-7.5
24.2 ms/Complex	-10	-9.5	-9

### C.2.1.3.2 Segment-Sync based sensing technique

This subclause described correlation with the segment sync pattern.

#### C.2.1.3.2.1 Segment-Sync Autocorrelation Detector (SSAD)

**Figure C.7—Segment-Sync autocorrelation detector**

When we utilize the Field Sync segment as shown in Figure C.4 to perform spectrum sensing, a problem arises that the Field Sync segment is very sparse in the transmission of the ATSC DTV signal. There is only one Field Sync segment every 24.2 ms; hence, we have to observe a long window of 520892 samples and complete this number of correlations and amplitude comparisons. Therefore, the complexity is high for the correlation detector. Furthermore, the effects of multi-path fading channel and frequency offset will severely destroy the detection ability of the correlation detection method. As a result, instead of utilizing Field Sync segment, we make use of the data Segment Sync as shown in Figure C.3 to perform spectrum sensing. As shown in Figure C.3, there is a data Segment Sync consisting of four symbols as a head of every ATSC DTV signal data segment. Because the time difference between two consecutive data Segment Sync is only 0.077 ms (828 symbols) which is very short, we can assume that they encounter the same channel effects including frequency offset, timing offset, and multi-path fading effect. Thus, we use autocorrelation of the two consecutive data Segment Sync as our basic approach to eliminate channel

effects. Furthermore, using data Segment Sync to perform spectrum sensing has the advantage that we only need to observe a window length that is  $WSS = 1664$  samples for which is a much shorter observation time compared to that of using Field Sync. Figure C.7 shows the block diagram of the Segment-Sync autocorrelation detector (SSAD). Define the test statistic TSSAD as

$$T_{SSAD} = \max_{0 \leq i \leq W_{SS}-1} \left| \frac{1}{N_D} \sum_{n=0}^{N_D-1} \frac{1}{8} \sum_{k=0}^{K-1} y[i+k+n \cdot L] y^*[i+k+(n+1) \cdot L] \right| \quad (\text{C9})$$

Where  $L = 1664$  samples, which is the length of one ATSC DTV data segment under 2x sampling rate and  $N_D$  is the number of collected Segment Sync.

#### C.2.1.3.2.2 Threshold calculation

After the construction of the Segment Sync autocorrelation detection, we have to know the threshold for a specific PFA. For hypothesis  $H_0$ , we have  $y[n] = w[n]$ , define

$$T_i = \frac{1}{N_D} \sum_{n=0}^{N_D-1} \frac{1}{8} \sum_{k=0}^{K-1} w[i+k+n \cdot L] w^*[i+k+n \cdot (L+1)] \quad (\text{C10})$$

When  $N_D$  is large, according to the Central Limit Theorem,  $T_i$  will approach complex Gaussian distribution.

$$\lim_{N_D \rightarrow \infty} T_i \sim \text{complex } N(0, \frac{\sigma^4}{8N_D}) \quad (\text{C11})$$

Therefore,

$$F_{|T_i|}(t : H_0) = 1 - e^{-\frac{8N_D t^2}{\sigma^4}}, \quad t \geq 0 \quad (\text{C12})$$

According to Equation (C9), the statistics TSSAD is the maximum of  $T_i$  over an observation window length  $WSS$ . Because  $T_i$ s are identical but not independent distributed, it is hard to find the exact distribution of the statistics TSSAD. However, we can assume  $T_i$ s are independent to get a distribution and then use this distribution to compute a reference threshold. By doing this, we obtain

$$\gamma_{SSAD} = \mu \cdot \left( \frac{\sigma^4}{8N_D} \ln \left( \frac{1}{1 - (1 - P_{FA})^{1/N_D}} \right) \right)^{1/2} \quad (\text{C13})$$

where the right part except  $\mu$  in Equation (C13) is the threshold obtained by assuming  $T_i$ s are independent and the value of  $\mu$  is a heuristic adjusting factor added artificially to account for the approximation mentioned above.

#### C.2.1.3.2.3 Maximum combining Segment Sync autocorrelation detector (MCSSAD)

When we accumulate a large number of data Segment Sync elements, i.e., when the sensing time is long, timing drift effects will restrict the improvement of the performance that comes from a longer sensing time. In order to alleviate the timing drift effect, we can slice the total sensing time into several time slots and then apply a SSAD detector to each time slot. Then, finally, we use the average of the maximum absolute value of autocorrelation of each time slot as our detection statistic. We call this detector the Maximum Combining Segment Sync Autocorrelation Detector (MCSSAD). The threshold is still determined by Equation (C13) by adjusting the value of  $\mu$ .

#### C.2.1.3.2.4 Simulation results

Again, the performances of the Segment-Sync based algorithms are demonstrated by computer simulations according to the spectrum sensing simulation model (ATSC Digital Television Standard [1]). The false alarm rate is set to 0.1 and for misdetection rate equaling 0.1, the required SNR are given in Table C.9.

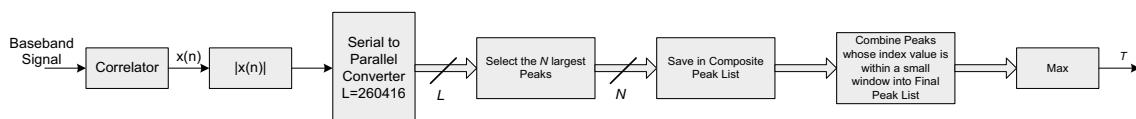
Note that the Segment-Sync based algorithms have an advantage that the detection performances for different capture data files are approximately the same and Table C.9 shows the average performance.

**Table C.9—Required SNR for the Segment-Sync based detector**

Sensing Time/Method	$\Delta=0$ dB	$\Delta=0.5$ dB	$\Delta=1$ dB
	Required SNR (dB)		
4.06 ms/SSAD	-7	-6.5	-6
9.25 ms/MCSSAD	-8	-7.5	-7
92.5 ms/MCSSAD	-13	-12.5	-12

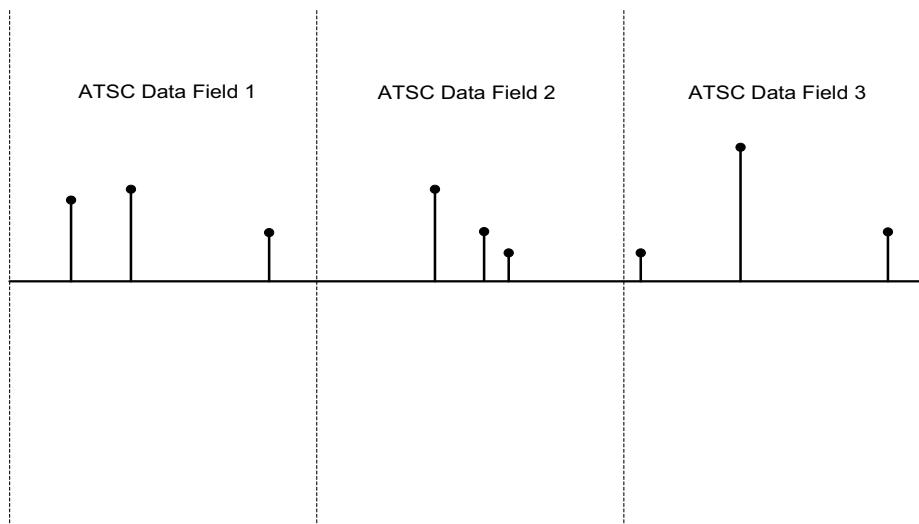
#### C.2.1.4 Test statistic using multiple ATSC data fields

If it is possible to use a sensing duration of 48.4 ms (the duration of two ATSC data frames) or longer, then it is possible to obtain better performance than with a sensing time of 24.2 ms (the duration of a single ATSC data frame). The method of constructing the test statistic for this longer observation time is described in this subclause. Let the correlator output be denoted  $x(n)$ . One ATSC data frame consists of  $L = 260416$  samples. Figure C.8 illustrates the steps used to construct the test statistic T.



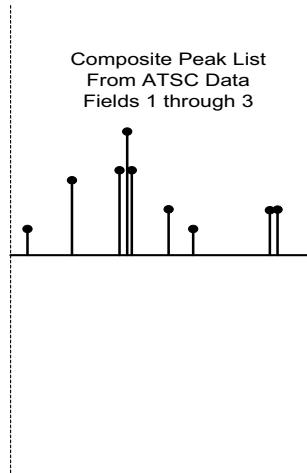
**Figure C.8—Block diagram**

The first step in constructing the test statistic is to take the absolute value of the correlator output. The next step is a serial to parallel converter that selects L samples. The value of L is selected to span an entire ATSC data frame. The next step is to select the N largest peaks. A peak is represented as the index of the sample and the magnitude of the sample. This process is repeated for multiple ATSC data fields. Figure C.9 illustrates the N (three in this illustration) largest peaks from each ATSC data field.



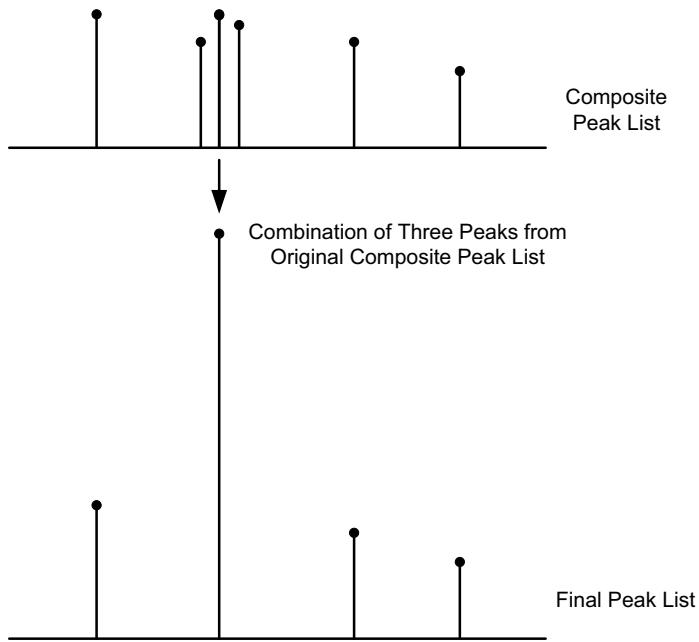
**Figure C.9—N largest peaks from each ATSC data field**

After multiple ATSC data fields have been processed the N largest peaks from each ATSC data field are combining into a composite peak list. The composite peak list is illustrated in Figure C.10.



**Figure C.10—Composite peak list**

The next step is to combine peaks in the composite peak list that are within a few samples. The number of samples should be selected to be large enough to combine peaks due to correlations with the actual ATSC Signature Sequence, but not much larger. The window allows for jitter in the position of the true peak due to timing offsets and small Doppler effects. The combining of peaks in the composite peak list to form the final peak list is illustrated in Figure C.11.



**Figure C.11—Peak combining**

Once the final peak list has been generated the test statistic T is just the magnitude of the largest peak. The test statistic T is compared to a threshold  $g$ . The value of the threshold is selected to meet the false alarm

rate requirement. The performance of this methods compared to the method described in C.2.1.3 is that the required SNR is lower.

**Table C.10—Required SNR versus sensing time**

Number of ATSC Data Fields	Sensing Time (ms)	Required SNR(dB)
1	24.2	-10
4	96.8	-12
16	387.2	-14

## C.2.2 ATSC FFT-based pilot sensing technique

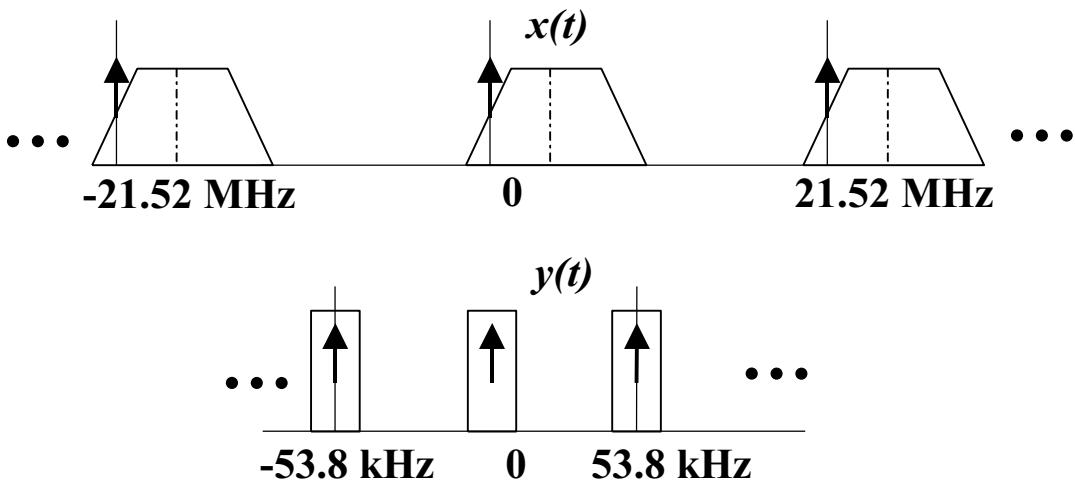
### C.2.2.1 FFT-based pilot sensing algorithms

The FFT-based pilot sensing techniques described in this subclause are **non-blind** (ATSC-specific) sensing techniques that meet the sensing sensitivity requirements of IEEE 802.22 and hence are classified as a **fine** sensing technique.

The ATSC VSB signal has a pilot at the lower band-edge in a known location relative to the signal. For this description, we will assume that the signal to be sensed is a band-pass signal at a low-IF of 5.38 MHz with the nominal pilot location at 2.69 MHz and is sampled at 21.52 MHz. However, the basic steps of the sensing algorithm can be implemented with suitable modifications for any IF and sampling rate. The essential features of the proposed method are as follows:

- 1) Demodulate the signal to baseband by the nominal frequency offset of  $f_c = 2.69$  MHz. Hence, if  $x(t)$  is the real, band-pass signal at low-IF,  $y(t) = x(t)e^{-j2\pi f_c t}$  is the complex demodulated signal at baseband.
- 2) Filter  $y(t)$  with a low-pass filter of bandwidth, e.g., 40 kHz ( $\pm 20$  kHz). The filter bandwidth should be large enough to accommodate any unknown frequency offsets.
- 3) Down-sample the filtered signal from 21.52 MHz to 53.8 kHz, to form the signal  $z(t)$ .
- 4) Take FFT of the down-sampled signal  $z(t)$ . Depending on the sensing period, the length of the FFT will vary. For example, a 1 ms sensing window will allow a 32-point FFT while a 5 ms window will allow a 256-point FFT.
- 5) Determine the maximum value, and location, of the FFT output squared.

Steps 1) and 2) above are shown in Figure C.12.



**Figure C.12—Frequency domain description**

Signal detection can then be done either by setting a threshold on the maximum value, or by observing the location of the peak over successive intervals. Instead of the FFT, other well-known spectrum estimation methods, such as the Welch periodogram can also be used in the previous step 4).

The basic method described above can be adapted to a variety of scenarios as described below:

- Multiple fine sensing windows, e.g., 5 ms sensing dwells every 10 ms. The 256-point FFT outputs squared from each sensing window can be averaged to form a composite statistic as well as the location information from each measurement can be used to derive a detection metric.
- If a single long sensing window, e.g., 10 ms is available, a 512-point FFT or periodogram can be used to obtain better detection performance.

The parameters of the sensor can be chosen depending on the desired sensing time, complexity, probability of missed detection and probability of false alarm. Detection based on location is robust against noise uncertainty since the position of the pilot can be pinpointed with accuracy even if the amplitude is low due to fading. Various combining schemes can be developed for both pilot-energy and pilot-location sensing.

- Pilot-energy sensing: For a single sensing window, the FFT output is simply squared and the maximum value is compared to a threshold. For multiple sensing dwells, there are two possibilities: (i) the decision from each dwell is saved and a “hard-decision” rule is applied to declare “signal detect” if the number of positives is greater than a certain number, or (ii) the square of the FFT output of all dwells is averaged and the maximum level is compared to a threshold. The choice of threshold in all cases is determined by the desired PFA.
- Pilot-location sensing: This is usually used for multiple dwells.
  - a) Let number of dwells = N
  - b) Let  $f_{\max}^{(1)}$  be the location of the maximum of the FFT-output averaged over the first N/2 dwells
  - c) Let  $f_{\max}^{(2)}$  be the location of the maximum of the FFT-output averaged over the second N/2 dwells
  - d) Detection statistic:  

$$D = |f_{\max}^{(1)} - f_{\max}^{(2)}|$$
  - e) If  $D < NT$ , signal present.
- Other variations:
  - a) Any PSD algorithm can be used instead of FFT.

- b) Other averaging intervals could be used.
- c) PFA using this method is extremely low and robust. Threshold value NT will depend on the FFT-size.

### C.2.2.2 Performance of the algorithms

Both pilot-energy and pilot-location based sensing algorithms were tested with the 12 DTV signals specified. The sensing time was multiples of 5 ms, which allowed the use of a 256-point FFT. Table C.11 shows the required SNR for a PFA = 0.05 and PMD = 0.10 and no noise uncertainty.

**Table C.11—Required SNR for DTV signal detection (average over 12 signals)**

Method	5 ms (N = 1)	10 ms (N = 2)	30 ms (N = 6)	50 ms (N = 10)
Pilot-Energy	-18 dB	-20.5 dB	-23.5 dB	-24.5 dB
Pilot-Location (NT = 2)	—	-18.5 dB	-22.0 dB	-24.0 dB

### C.2.3 ATSC Pilot Sensing technique using high order statistics

We present an algorithm to detect the DTV Signals in Gaussian noise using higher order statistics (HOS). The algorithm performs non-Gaussianity check in the frequency domain in the vicinity of the pilot of the DTV. The average results for all the 12 provided DTV Signals are summarized as: At Pfalse alarm = 0.04,

- For a capture of 5 ms (continuous or staggered), Pdetection = 0.9 at SNR = -16.6 dB.
- For a capture of 10 ms (continuous or staggered), Pdetection = 0.9 at SNR = -18.6 dB
- For a capture of 20 ms (continuous or staggered), Pdetection = 0.9 at SNR = -21.6 dB
- For a capture of 40 ms (continuous or staggered), Pdetection = 0.9 at SNR = -23.7 dB

We use a 2048 point FFT to implement the algorithm which may be used for spectrum sensing as well as OFDMA demodulation. Because of the Constant False Alarm Rate (CFAR) (Kay [7], [8]) nature of the detector, the threshold is built into the technique and NO presetting is required. Fine adjustment is possible if needed.

Our technique relies on the non-Gaussianity of a signal to separate it from the Gaussian noise. In the time domain, DTV signals show a Gaussian characteristic. However, in the frequency domain they are non-Gaussian. We will exploit this characteristic to detect the signals in AWGN. The proposed technique on spectrum sensing using HOS may be used to detect wireless microphone, DVB-T and other signals operating in the TV broadcasting bands as well.

#### C.2.3.1 Signal or noise identification using higher order statistics—basic concept

Use of Higher Order Statistics (HOS) is an efficient metric for detecting non-Gaussian signals at low SNRs (Shanmugan and Breipohl [12]). In particular, if we assume the noise to be a Gaussian random process, then all the cumulants of order greater than 2 are supposed to be zero. Given a set of N samples  $x = \{x_0, x_1, \dots, x_{N-1}\}$ , of a random variable x, the  $r^{\text{th}}$  order moment of the collection of samples contained in the array (x) may be approximated as

$$\hat{m}_r = \frac{1}{N} \sum_{n=0}^{N-1} (x_n - \bar{x})^r \quad (\text{C14})$$

where

$$\bar{x} \approx \frac{1}{N} \sum_{n=0}^{N-1} x_n \quad (\text{C15})$$

Let  $c_r = r^{\text{th}}$  order cumulant of  $x$ . Then the relationship between cumulants and the moments may be used to compute the higher order cumulants in a simple fashion as

$$c_n = m_n - \sum_{k=1}^{n-1} \binom{n-1}{k-1} c_k m_{n-k} \quad (\text{C16})$$

$$\text{where: } \binom{n-1}{k-1} = \frac{(n-1)!}{(k-1)! \cdot (n-k)!},$$

$$\text{and } y! = \text{Factorial}(y) = y \cdot (y-1) \cdot (y-2) \cdot (y-3) \dots 2 \cdot 1$$

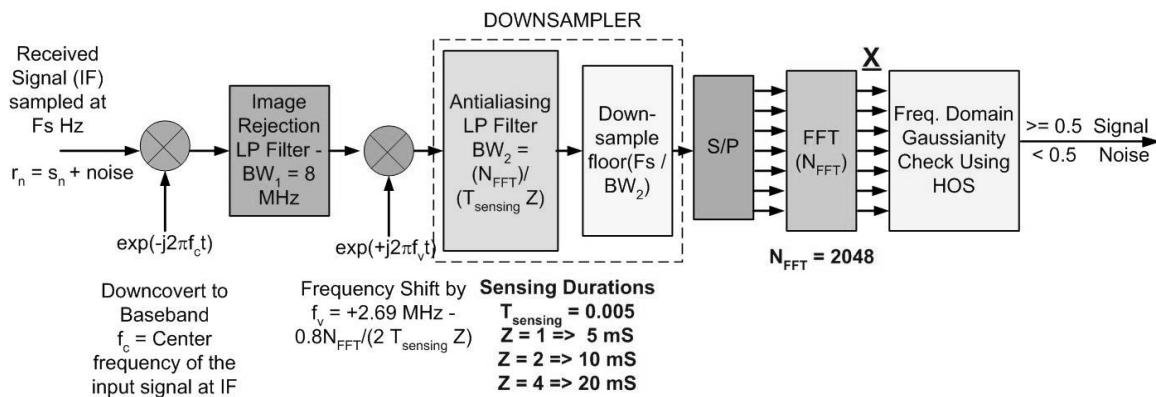
This relationship may also be written for each of the cumulants by expanding Equation (C16) as shown in Equation (17).

$$\begin{aligned} c_1 &= m_1 \\ c_2 &= m_2 - m_1^2 \\ c_3 &= m_3 - 3m_1m_2 + 2m_1^3 \\ c_4 &= m_4 - 4m_1m_3 - 3m_2^2 + 12m_1^2m_2 - 6m_1^4 \\ &\vdots \end{aligned} \quad (\text{C17})$$

Since our data record for the determination of the HOS may not be sufficiently long, the cumulants of order greater than 2 may not be exactly zero. Hence, a threshold needs to be set in order to make a decision as to whether the samples belong to signal or noise. In this method, we compare the higher order cumulants with the power of second order moment. This is also known as bi-coherency, tri-coherency etc. tests to determine if the received waveform belongs to DTV signal or the noise.

### C.2.3.2 Signal detection for DTV signals in the vicinity of the pilot using higher order statistics

Following is the description of the DTV spectrum sensing algorithm in the vicinity of pilot using the high order statistics (HOS) as shown in Figure C.13.



**Figure C.13—Signal processing chain for DTV spectrum sensing in the vicinity of pilot using higher order statistics (HOS)**

- Step 1: Downshift (Downconvert) the received samples collected in the TV channel from the Radio Frequency (RF) or the Intermediate Frequency (IF) to the base band,
- Step 2: Pass the down-converted signal through an image rejection Low Pass (LP) of total bandwidth ( $BW_1 = 8$  MHz) to suppress the image.
- Step 3: Upshift (Upconvert) the signal by approximately  $(2.69 \text{ MHz} - 0.8 N_{FFT} / (2T_{\text{sensing}} Z))$  so that if an ATSC DTV signal was present, its pilot would be shifted towards the d.c. or 0 Hertz frequency.  $T_{\text{sensing}}$  = Sensing Duration,  $Z = 1, 2, 3, \dots$  determines the multiples of the sensing duration. For example,  $T_{\text{sensing}} = 0.005$  and  $Z = 1$  implies the total sensing duration of 5 ms. Similarly,  $T_{\text{sensing}} = 0.005$  and  $Z = 2$  implies the total sensing duration of 10 ms.  $F_s$  = sampling frequency of the original received signal at RF or IF, and  $N_{FFT}$  = Size of the FFT used. Factor  $0.8 N_{FFT} / (2T_{\text{sensing}} Z)$  is used to make sure that the pilot is shifted just enough (before the next stage of down-sampling) and there are no residual contributions from the neighboring channel in the samples that are being analyzed.
- Step 4: Pass the resultant signals through a Low Pass (LP) filter of total bandwidth ( $BW_2 = N_{FFT} / ((T_{\text{sensing}} Z))$ ) followed by down-sampling of the signals by a factor of floor ( $F_s/BW_2$ ).
- Step 5: Convert the input samples from serial to parallel and transform them to the frequency domain using a Fast Fourier Transform (FFT) of length  $N_{FFT}$ . As an example, keeping the FFT length,  $N_{FFT} = 2048$  is advantageous since the same FFT implementation may be used for spectrum sensing as well as OFDMA demodulation of WRAN.
- Step 6: Collect the samples at the output of the FFT and store them in a buffer. Determine the higher order moments and cumulants of the real and imaginary portions of the stored samples using Equation (C14), Equation (C15), and Equation (C16). Perform the frequency domain Gaussianity check and hence DTV detection by applying the following steps.
- Step 7: Let  $\mathbf{R}$  be the number of moments  $(m_r^{\text{real}}, m_r^{\text{imaginary}})$  and cumulants  $(c_r^{\text{real}}, c_r^{\text{imaginary}})$  of the order **greater than two available** for computation of the real and the imaginary parts of each of the segments ( $X$ ) of data at the output of the FFT respectively,
  - Choose a Probability Step Parameter  $0 < \delta < 1$ ; as an example let  $\delta = 0.5 / \mathbf{R}$ .
  - Let  $P_{\text{Signal}}^{\text{real}} = P_{\text{Signal}}^{\text{imaginary}} = 0.5$ ;
  - Choose some  $\gamma > 0$ ;  $\gamma_{\text{typical}} = 1$
  - for  $r = 3$  to  $(\mathbf{R} + 2)$ ;
    - if  $|c_r^{\text{real}}| < \gamma |m_2^{\text{real}}|^{\frac{r}{2}}$   $\Rightarrow P_{\text{Signal}}^{\text{real}} = P_{\text{Signal}}^{\text{real}} - \delta$
    - elseif  $|c_r^{\text{real}}| \geq \gamma |m_2^{\text{real}}|^{\frac{r}{2}}$   $\Rightarrow P_{\text{Signal}}^{\text{real}} = P_{\text{Signal}}^{\text{real}} + \delta$
    - end,
    - if  $|c_r^{\text{imaginary}}| < \gamma |m_2^{\text{imaginary}}|^{\frac{r}{2}}$   $\Rightarrow P_{\text{Signal}}^{\text{imaginary}} = P_{\text{Signal}}^{\text{imaginary}} - \delta$ ,
    - elseif  $|c_r^{\text{imaginary}}| \geq \gamma |m_2^{\text{imaginary}}|^{\frac{r}{2}}$   $\Rightarrow P_{\text{Signal}}^{\text{imaginary}} = P_{\text{Signal}}^{\text{imaginary}} + \delta$
    - end,
    - end
  - $P_{\text{Signal}} = a \cdot P_{\text{Signal}}^{\text{real}} + b \cdot P_{\text{Signal}}^{\text{imaginary}}$  where  $a$  and  $b$  are weight parameters. As an example  $a=b=0.5$
  - Due to the constant false alarm rate (CFAR) nature of the detector, the threshold is built into the system, and NO presetting is required. However, in order to carry out fine adjustment, we have provided the fine sensing threshold parameter  $\gamma$ , which is used to make fine adjustments

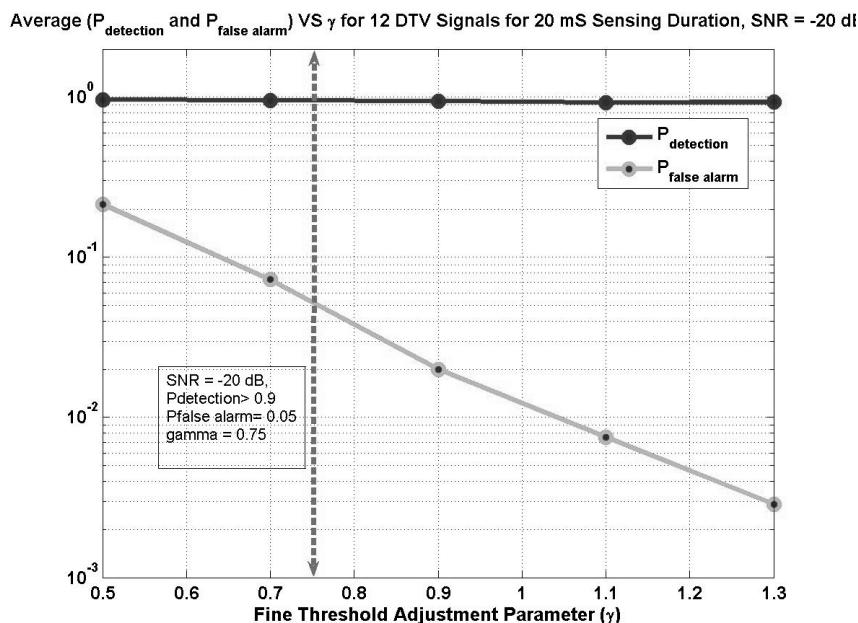
of  $P_{\text{false alarm}}$  if needed. As  $\gamma$  increases  $P_{\text{false alarm}}$  decreases and vice-versa. In most cases  $\gamma$  is kept close to unity.

Step 8: if  $P_{\text{Signal}} \geq 0.5$  then the segment X belongs the DTV signal we conclude that the TV channel is occupied by the incumbent.

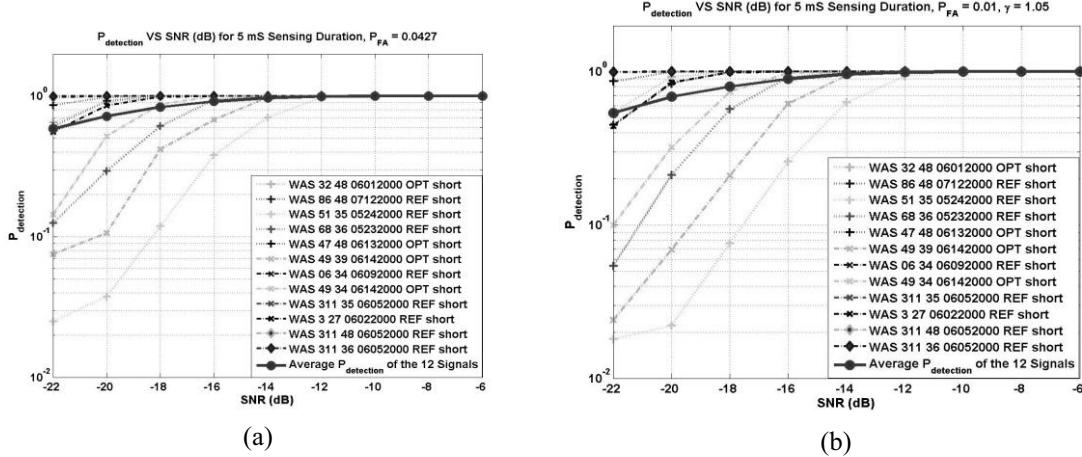
if  $P_{\text{Signal}} < 0.5$  then the segment X belongs to noise and we conclude that the TV channel is NOT occupied by an incumbent.

### C.2.3.3 Performance results

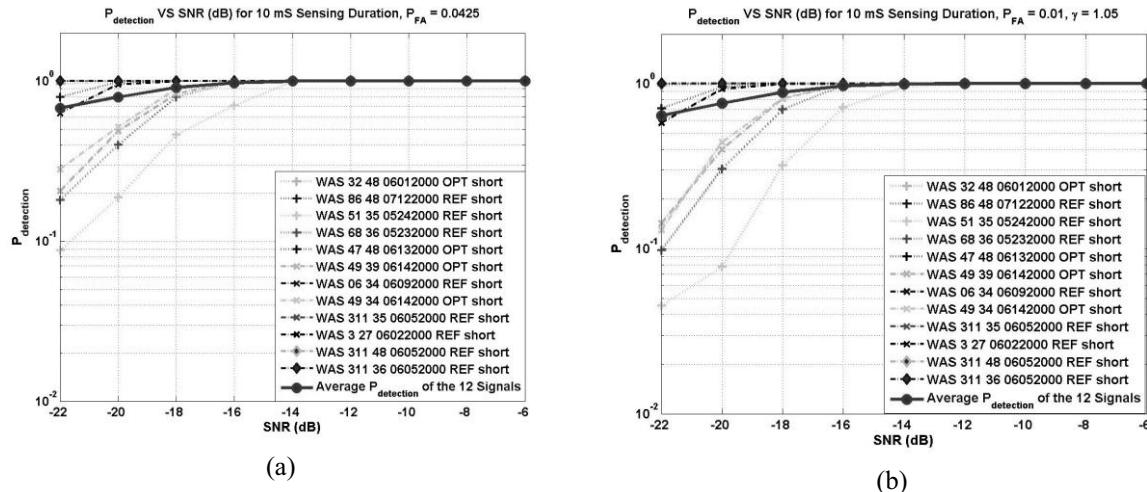
The spectrum sensing algorithm using HOS was tested on the 12 DTV signals that were provided (IEEE 802.22 Contribution 22-07-0359-00-0000 [6]). The simulations were carried out for sensing times in multiples of 5 ms however any length sensing time may be used for the actual implementation. The length of the FFT was kept at  $N_{\text{FFT}} = 2048$  keeping in mind that the same hardware may be used for spectrum sensing as well as OFDMA demodulation of WRANs. Due to the CFAR nature of the detector, the threshold is built into the system, and NO presetting is required. However, in order to carry out fine adjustment, we have provided the fine sensing threshold parameter  $\gamma$ , which enables fine adjustment of the  $P_{\text{false alarm}}$  at little degradation in  $P_{\text{detection}}$ . Figure C.14 shows the average ( $P_{\text{detection}}$  and  $P_{\text{false alarm}}$ ) of the 12 provided DTV signals vs. the fine sensing threshold parameter  $\gamma$ , at SNR = -20 dB and sensing duration of 20 ms. Based on this simulation, the value of the fine sensing threshold parameter  $\gamma$  was chosen in order to obtain a specific  $P_{\text{false alarm}}$ . Similar simulations were carried out for other sensing durations as well. Based on the results from Figure C.14, the parameter  $\gamma$  was kept at 0.8 and 1.05 in order to obtain  $P_{\text{false alarm}} \leq 0.05$  and  $P_{\text{false alarm}} \leq 0.01$  respectively. Figure C.15, Figure C.16, Figure C.17, and Figure C.18 show the  $P_{\text{detection}}$  vs. SNR performance of the 12 provided DTV signals for 5, 10, 20, and 40 ms sensing times respectively.



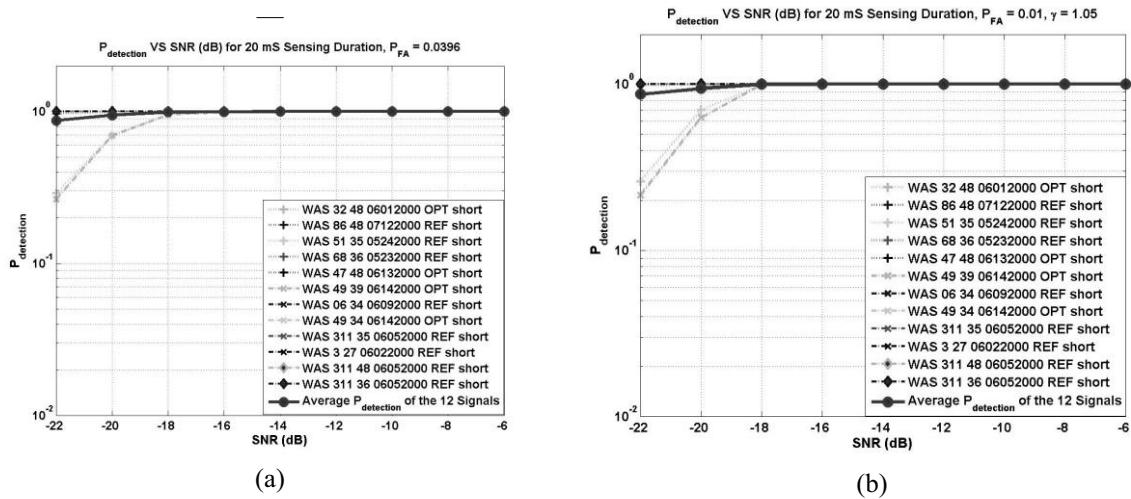
**Figure C.14— Average  $P_{\text{detection}}$  and  $P_{\text{false alarm}}$  of the 12 provided DTV signals vs. the fine sensing threshold parameter  $\gamma$ , at SNR = -20 dB and total sensing duration  $T_{\text{sensing}}Z = 20$  ms.  $N_{\text{FFT}} = 2048$ ,  $a = b = 1$**



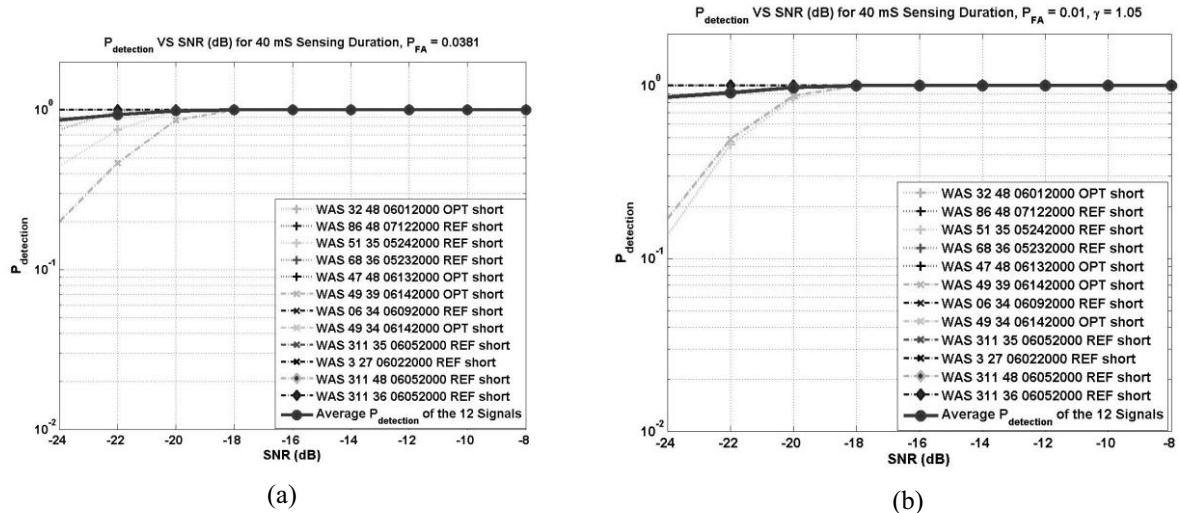
**Figure C.15— $P_{\text{detection}}$  vs. SNR performance for the 12 provided DTV signals for the total sensing duration  $T_{\text{sensing}} Z = 5 \text{ ms}$  using the algorithm utilizing HOS in the vicinity of the pilot.  $N_{\text{FFT}} = 2048, a = b = 1$ , (a)  $\gamma = 0.8, P_{\text{FA}} = 0.0427$  (b)  $\gamma = 1.05, P_{\text{FA}} = 0.01$**



**Figure C.16— $P_{\text{detection}}$  vs. SNR performance for the 12 provided DTV signals for the total sensing duration  $T_{\text{sensing}} Z = 10 \text{ ms}$  using the algorithm utilizing HOS in the vicinity of the pilot.  $N_{\text{FFT}} = 2048, a = b = 1$ , (a)  $\gamma = 0.8, P_{\text{FA}} = 0.0425$  (b)  $\gamma = 1.05, P_{\text{FA}} = 0.01$**



**Figure C.17— $P_{\text{detection}}$  vs. SNR performance for the 12 provided DTV signals for the total sensing duration  $T_{\text{sensing}}Z = 20$  ms using the algorithm utilizing HOS in the vicinity of the pilot.  $N_{\text{FFT}} = 2048$ ,  $a = b = 1$ . (a)  $\gamma = 0.8$ ,  $P_{\text{FA}} = 0.0396$  (b)  $\gamma = 1.05$ ,  $P_{\text{FA}} = 0.01$**



**Figure C.18— $P_{\text{detection}}$  vs. SNR performance for the 12 provided DTV signals for the total sensing duration  $T_{\text{sensing}}Z = 40$  ms using the algorithm utilizing HOS in the vicinity of the pilot.  $N_{\text{FFT}} = 2048$ ,  $a = b = 1$ . (a)  $\gamma = 0.8$ ,  $P_{\text{FA}} = 0.0381$  (b)  $\gamma = 1.05$ ,  $P_{\text{FA}} = 0.01$**

The spectrum sensing algorithm using HOS in the vicinity of the pilot was tested for the 12 provided DTV signals as shown above. Table C.12 summarizes the results for the average SNR required for the collection of the 12 provided DTV signals at a  $P_{\text{false alarm}} = 0.05$  and  $P_{\text{false alarm}} = 0.01$  while keeping  $P_{\text{detection}} \geq 0.90$  for various sensing durations. This algorithm meets the DTV fine sensing requirements as an average over the 12 provided DTV signals for sensing times  $\geq 20$  ms.

**Table C.12—Required SNR for DTV signal detection (averaged over 12 signals)**

Sensing duration	5 ms	10 ms	20 ms	40 ms
Required SNR for $P_{\text{detection}} \geq 0.9$ and $P_{\text{false\_alarm}} \leq 0.05$ )	-16.6 dB	-18.6 dB	-21.6 dB	-23.7 dB
Required SNR for $P_{\text{detection}} \geq 0.9$ and $P_{\text{false\_alarm}} \leq 0.01$ )	-16 dB	-18 dB	-21.4 dB	-23.4 dB

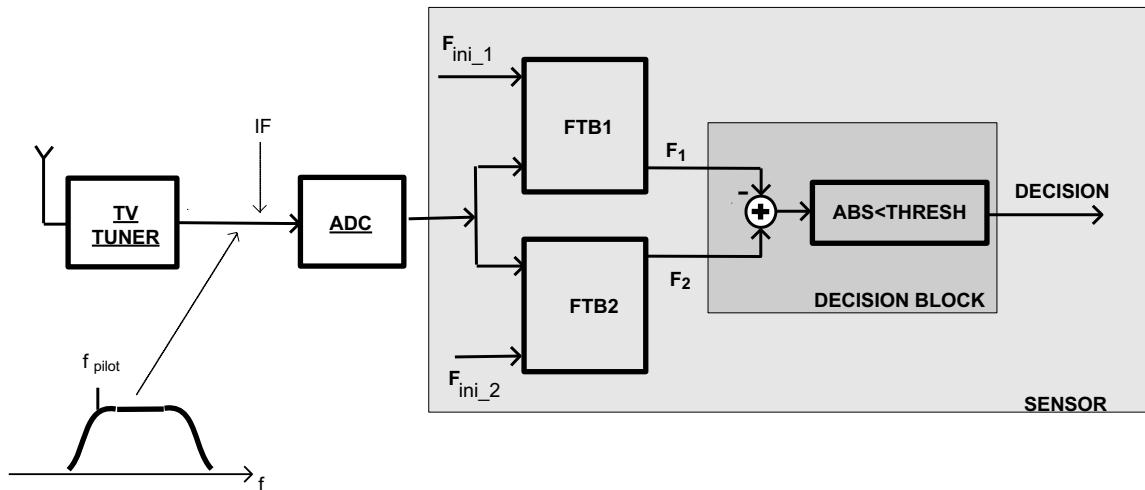
## C.2.4 ATSC PLL-based pilot sensing technique

### C.2.4.1 Dual FPLL pilot sensing algorithm

The Dual FPLL sensing techniques described in this subclause are **non-blind** (ATSC-specific) sensing techniques that do not meet the sensing sensitivity requirements of IEEE 802.22 and hence are classified as a **coarse** sensing technique.

The sensor system, presented in Figure C.19, employs two Frequency Tracking Blocks (FTBs). These blocks are designed to track an a priori known frequency of the ATSC pilot,  $f_{\text{pilot}}$ , within a signal source, an Intermediate Frequency (IF) at the TV tuner output. The outputs,  $F_1$  and  $F_2$ , are frequencies that FTBs are locked into at the given moment. In the absence of the pilot, or when the pilot energy is insufficient, the outputs,  $F_1$  and  $F_2$ , maintain their initial input preset values,  $F_{\text{ini\_1}}$  and  $F_{\text{ini\_2}}$ , respectively. These preset values are selected to be:

$$\begin{aligned} F_{\text{ini\_1}} &= f_{\text{pilot}} + 30 \text{ kHz} \\ F_{\text{ini\_2}} &= f_{\text{pilot}} - 30 \text{ kHz} \end{aligned}$$



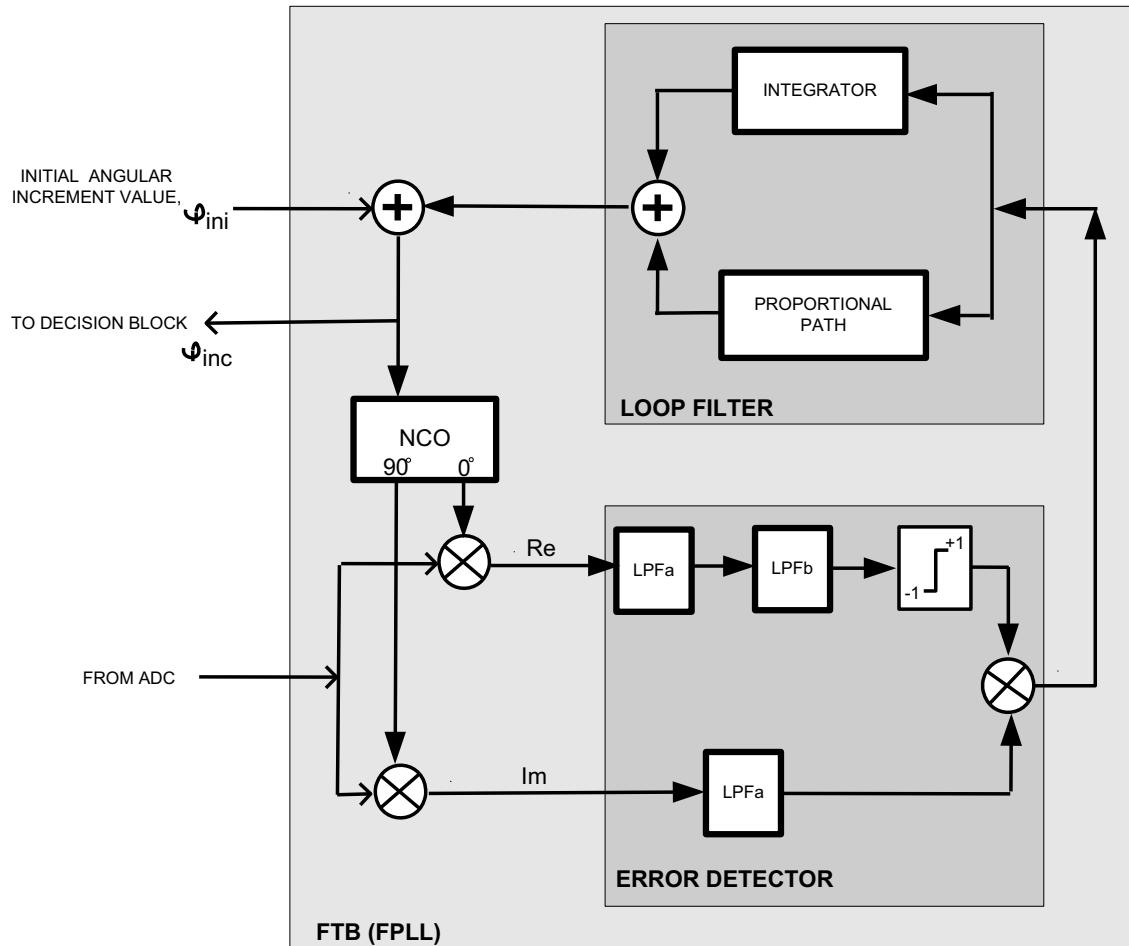
**Figure C.19—Dual FPLL sensor system**

The FTBs are initially and thereafter periodically (period =  $t_{\text{set}}$ ) preset to their respective  $F_{\text{ini}}$  values. The time period,  $t_{\text{set}}$ , is set to anywhere between 30 ms and 100 ms. The detection criterion is based upon a degree of convergence of these FTBs on the same spectral position of the ATSC pilot within preset time period. The detection is true, when at the end of period,  $t_{\text{set}}$ ,

$$|F_1 - F_2| < F_{\text{thresh}}, \quad \text{where } F_{\text{thresh}} \text{ is typically set to } 20\text{--}30 \text{ kHz.}$$

The above equation shows that, though the described sensor system is architecturally synchronous, the actual detection criterion does not require a complete fpilot acquisition.

Figure C.20 outlines a possible architecture for each of the required two FTB blocks in Figure C.19. A Frequency-Phase Locked Loop (FPLL) in Figure C.20 is implemented as a version of the Costas Loop. In this implementation the input/output angular values,  $\phi_{ini}$  /  $\phi_{inc}$ , are used as a convenient functional equivalents of the frequencies,  $F_{ini}$  /  $F_x$ , in Figure C.19. The output,  $\phi_{inc}$ , needs to be fed into the Decision Block (Figure C.19) as one of two required inputs.



**Figure C.20—Possible architecture for FTB blocks**

A signal from the ADC contains a pilot (tone) nominally located at fpilot. This signal is converted into a complex form after being multiplied by two sine waves, shifted by 90 degrees, from a Numerically Controlled Oscillator (NCO). An NCO is, in essence, a sine/cosine lookup table that is fed by a modulo  $2\pi$  accumulator. The NCO input receives a phase increment,  $\phi_{inc}$ , that is added to the accumulator on each system clock. In the described implementation the system clock is at a constant frequency, Fclk. When FPLL is completely locked on the incoming tone, fpilot, the NCO advances by an angle equal to  $2\pi/(F_{clk}/fpilot)$  in each system clock, Fclk, period.

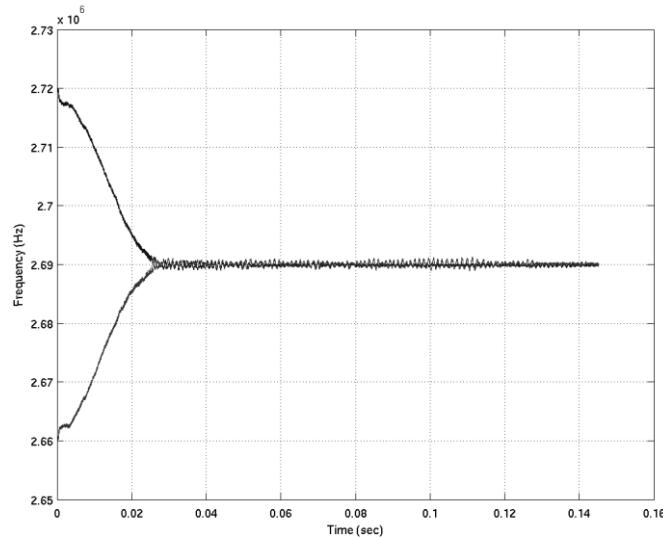
The Real (Re) and Imaginary (Im) parts of the complex signal are fed into the phase detector. The phase detector contains two identical Low Pass Filters LPFa, and an LPFb, that is needed to achieve a phase shift. The LPFa filters define the lock-in range of the FPLL, which is set to  $\pm 100$  kHz to accommodate possible

deviations of the ATSC pilot position. The output of the detector contains the phase error value, both a sign and a magnitude.

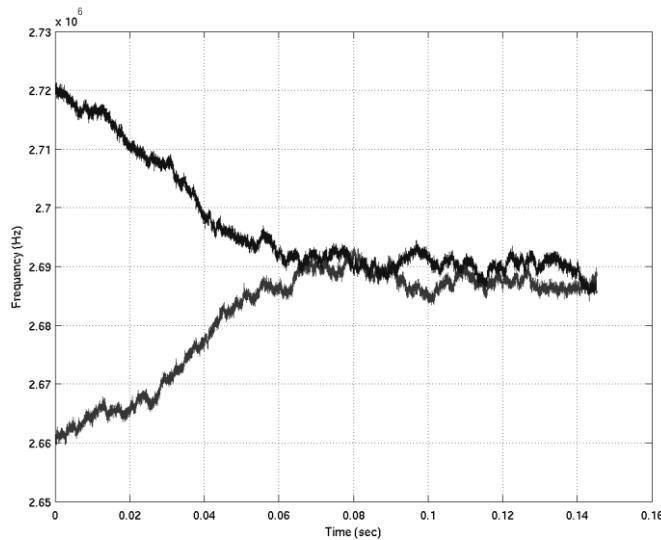
The Loop Filter integrates the phase error value to derive the frequency error in the Integrator branch. The frequency error is a difference between the initial preset frequency, set by  $\varphi_{\text{ini}}$  and the actual pilot frequency in the incoming signal. The Proportional branch adjusts the magnitude of the phase error. The combined phase/frequency error data are added to an initial phase increment,  $\varphi_{\text{ini}}$ , to arrive at  $\varphi_{\text{inc}}$ , a final phase increment value, that defines the NCO output frequency.

#### C.2.4.2 Performance of the algorithms

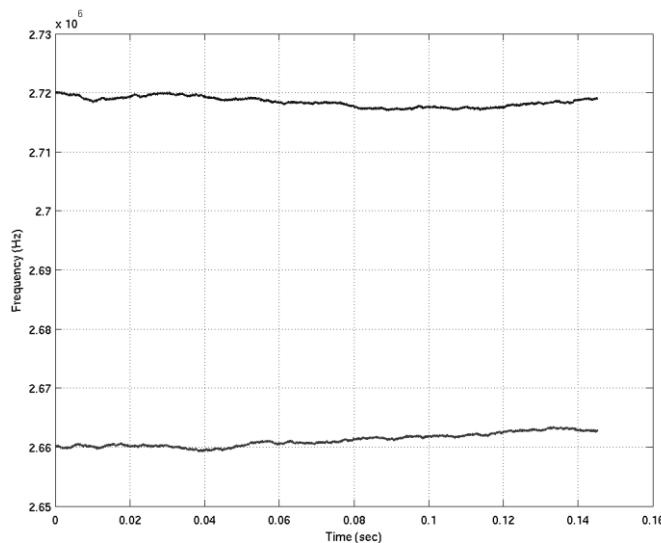
Figure C.21 and Figure C.22 show the convergence behavior of the two FTBs, each set to a different initial frequency, in the presence of an ATSC DTV signal with a low SNR and very low SNR respectively, while Figure C.23 shows the FTB outputs in the absence of an ATSC DTV signal. It can be observed from the plots that the FTB outputs start converging within few milliseconds in the presence of DTV signal and depending on the threshold value a decision can be made as early as 10 ms from the beginning of sensing process.



**Figure C.21—Convergence behavior of the two frequency tracking blocks (FTBs) each set to a different initial frequency in the presence of a low SNR ATSC DTV signal**

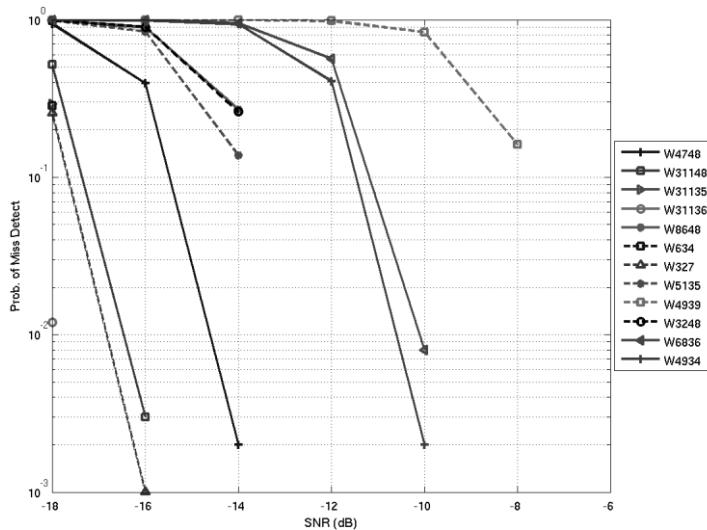


**Figure C.22— Convergence behavior of the two frequency tracking blocks (FTBs) each set to a different initial frequency in the presence of a very low SNR ATSC DTV signal**



**Figure C.23— Convergence behavior of the two frequency tracking blocks (FTBs) each set to a different initial frequency in the absence of an ATSC DTV signal**

The proposed FPLL based sensing algorithm was tested with the 12 DTV signals specified. Figure C.24 shows the probability of misdetection curves for the 12 ATSC DTV capture signals with a sensing time of 75 ms. The threshold value was set such that the probability of false alarm is less than 1%. Table C.13 shows the average of required SNR for these 12 captured signals with PFA << 0.01 and PMD = 0.10.



**Figure C.24—Probability of misdetection curves for the different ATSC DTV signal captures with a sensing time of 75 ms**

**Table C.13—Required SNR for DTV signal detection**

(Averaged over 12 signals)

Sensing Time	50 ms	75 ms
Required SNR	-12.42 dB	-14.88 dB

## C.2.5 Wireless microphone covariance sensing technique

### C.2.5.1 Covariance based sensing algorithms

Let  $y(t)$  be the continuous time received signal. Assume that we are interested in the frequency band with central frequency  $f_c$  and bandwidth  $W$ . We sample the received signal  $y(t)$  at a sampling rate  $f_s$ . Let  $T_s = 1/f_s$  be the sampling period. The received discrete signal is then  $x(n) = y(nT_s)$ . There are two hypotheses:  $H_0$ : signal not exists; and  $H_1$ : signal exists. The received signal samples under the two hypotheses are therefore respectively as follows:

$$H_0 : x(n) = \eta(n)$$

$$H_1 : x(n) = s(n) + \eta(n)$$

where  $s(n)$  is the transmitted signal passed through a wireless channel (including fading and multipath effect), and  $\eta(n)$  is the white noise samples. Note that  $s(n)$  can be the superposition of multiple signals.

The received signal is generally passed through a filter. Let  $f(k)$ ,  $k = 0, 1, \dots, K$  be the filter with  $\sum_{k=0}^K |f(k)|^2 = 1$ . After filtering, the received signal is turned to

$$\tilde{x}(n) = \sum_{k=0}^K f(k)x(n-k), \quad n = 0, 1, \dots$$

Let

$$\begin{aligned}\tilde{s}(n) &= \sum_{k=0}^K f(k)s(n-k), \quad n = 0, 1, \dots \\ \tilde{\eta}(n) &= \sum_{k=0}^K f(k)\eta(n-k), \quad n = 0, 1, \dots\end{aligned}$$

Then

$$\begin{aligned}H_0 : \tilde{x}(n) &= \tilde{\eta}(n) \\ H_1 : \tilde{x}(n) &= \tilde{s}(n) + \tilde{\eta}(n)\end{aligned}$$

Note that here the noise samples  $\tilde{\eta}(n)$  are correlated. If the sampling rate  $f_s$  is larger than the signal bandwidth  $W$ , we can down-sample the signal. Let  $M \geq 1$  be the down-sampling factor. If the signal to be detected has a narrower bandwidth than  $W$ , it is better to choose  $M > 1$ . For notation simplicity, we still use  $\tilde{x}(n)$  to denote the received signal samples after down-sampling, that is,  $\tilde{x}(n) \triangleq \tilde{x}(Mn)$ .

Choose a smoothing factor  $L$  and define

$$\mathbf{x}(n) = [\tilde{x}(n) \quad \tilde{x}(n-1) \quad \dots \quad \tilde{x}(n-L+1)]^T, \quad n = 0, 1, \dots, N_s - 1$$

A suggested value for  $L$  is around 10. Define a  $L \times (K+1+(L-1)M)$  matrix as

$$\mathbf{H} = \begin{bmatrix} f(0) & \dots & \dots & f(K) & 0 & \dots & 0 \\ 0 & \dots & f(0) & \dots & f(K) & \dots & 0 \\ & & \dots & & \dots & & \\ 0 & \dots & \dots & \dots & f(0) & \dots & f(K) \end{bmatrix}$$

Let  $\mathbf{G} = \mathbf{HH}^H$ . Decompose the matrix into  $\mathbf{G} = \mathbf{Q}^2$ , where  $\mathbf{Q}$  is a  $L \times L$  Hermitian matrix. The matrix  $\mathbf{G}$  is not related to signal and noise and can be computed offline. If analog filter or both analog filter and digital filter are used, the matrix  $\mathbf{G}$  should be revised to include the effects of all the filters. In general,  $\mathbf{G}$  can be obtained to be the covariance matrix of the received signal, when the input signal is white noise only (this can be done in laboratory offline). The matrix  $\mathbf{G}$  and  $\mathbf{Q}$  are computed only once and only  $\mathbf{Q}$  is used in detection.

Denote the statistical covariance matrix of the received signal as

$$\mathbf{R}_x = \mathbb{E}(\mathbf{x}(n)\mathbf{x}(n)^H)$$

Then

$$\mathbf{R}_x = \mathbf{R}_s + \sigma_\eta^2 \mathbf{G}$$

where  $\mathbf{R}_s$  is the statistical covariance matrix of the signal (including fading, multipath and filtering) and  $\sigma_\eta^2$  is the noise variance.

Define

$$\begin{aligned}\widetilde{\mathbf{R}}_x &= \mathbf{Q}^{-1} \mathbf{R}_x \mathbf{Q}^{-1} \\ \widetilde{\mathbf{R}}_s &= \mathbf{Q}^{-1} \mathbf{R}_s \mathbf{Q}^{-1}\end{aligned}$$

Then

$$\widetilde{\mathbf{R}}_x = \widetilde{\mathbf{R}}_s + \sigma_\eta^2 \mathbf{I}$$

If there is no signal, then  $\widetilde{\mathbf{R}}_s = 0$ . Hence the off-diagonal elements of  $\widetilde{\mathbf{R}}_x$  are all zeros. If signal presents,  $\widetilde{\mathbf{R}}_s$  is almost surely not a diagonal matrix. Hence, some of the off-diagonal elements of  $\widetilde{\mathbf{R}}_x$  should not be zeros. Denote the elements of the matrix by  $r_{nm}$ .

Let

$$\begin{aligned}T_1 &= \frac{1}{L} \sum_{n=1}^L \sum_{m=1}^L |r_{nm}|, \quad T_2 = \frac{1}{L} \sum_{n=1}^L |r_{nn}| \\ T_3 &= \frac{1}{L} \sum_{n=1}^L \sum_{m=1}^L |r_{nm}|^2, \quad T_4 = \frac{1}{L} \sum_{n=1}^L |r_{nn}|^2\end{aligned}$$

Then if there is no signal,  $T_1 = T_2$ , and  $T_3 = T_4$ . If there is signal,  $T_1 > T_2$ , and  $T_3 > T_4$ . We obtain two detection methods as follows.

#### C.2.5.1.1 Method 1: The covariance absolute value (CAV) detection

**Step 1:** Sample and filter the received signal as described above.

**Step 2:** Choose a smoothing factor  $L$  and compute the threshold  $\gamma$ .  $\gamma$  is chosen to meet the requirement for the probability of false alarm.

**Step 3:** Compute the auto-correlations of the received signal

$$\lambda(l) = \frac{1}{N_s} \sum_{m=0}^{N_s-1} \tilde{x}(m) \tilde{x}^*(m-l), \quad l = 0, 1, \dots, L-1$$

and form the sample covariance matrix as

$$\mathbf{R}(N_s) = \begin{bmatrix} \lambda(0) & \lambda(1) & \dots & \lambda(L-1) \\ \lambda(1)^* & \lambda(0) & \dots & \lambda(L-2) \\ \vdots & \vdots & \vdots & \vdots \\ \lambda(L-1)^* & \lambda(L-2)^* & \dots & \lambda(0) \end{bmatrix}$$

Note that the sample covariance matrix is Hermitian and Toeplitz.

**Step 4:** Transform the sample covariance matrix to obtain

$$\widetilde{\mathbf{R}}(N_s) = \mathbf{Q}^{-1} \mathbf{R}(N_s) \mathbf{Q}^{-1}$$

**Step 5:** Compute

$$\begin{aligned}T_1(N_s) &= \frac{1}{L} \sum_{n=1}^L \sum_{m=1}^L |r_{nm}(N_s)| \\ T_2(N_s) &= \frac{1}{L} \sum_{n=1}^L |r_{nn}(N_s)|\end{aligned}$$

where  $r_{nm}(N_s)$  are the elements of the sample covariance matrix.

**Step 6:** Determine the presence of the signal based on  $T_1(N_s), T_2(N_s)$  and the threshold: if  $T_1(N_s)/T_2(N_s) > \gamma$ , signal exists; otherwise, signal not exists

#### C.2.5.1.2 Method 2: The covariance Frobenius norm (CFN) detection

**Step 1:** Sample and filter the received signal as described above.

**Step 2:** Choose a smoothing factor  $L$  and compute the threshold  $\gamma$ .  $\gamma$  is chosen to meet the requirement for the probability of false alarm.

**Step 3:** Compute the auto-correlations of the received signal

$$\lambda(l) = \frac{1}{N_s} \sum_{m=0}^{N_s-1} \tilde{x}(m)\tilde{x}^*(m-l), \quad l = 0, 1, \dots, L-1$$

and form the sample covariance matrix as

$$\mathbf{R}(N_s) = \begin{bmatrix} \lambda(0) & \lambda(1) & \dots & \lambda(L-1) \\ \lambda(1)^* & \lambda(0) & \dots & \lambda(L-2) \\ \vdots & \vdots & \vdots & \vdots \\ \lambda(L-1)^* & \lambda(L-2)^* & \dots & \lambda(0) \end{bmatrix}$$

Note that the sample covariance matrix is Hermitian and Toeplitz.

**Step 4:** Transform the sample covariance matrix to obtain

$$\widetilde{\mathbf{R}}(N_s) = \mathbf{Q}^{-1} \mathbf{R}(N_s) \mathbf{Q}^{-1}$$

**Step 5:** Compute

$$T_3(N_s) = \frac{1}{L} \sum_{n=1}^L \sum_{m=1}^L |r_{nm}(N_s)|^2$$

$$T_4(N_s) = \frac{1}{L} \sum_{n=1}^L |r_{nn}(N_s)|^2$$

where  $r_{nm}(N_s)$  are the elements of the sample covariance matrix.

**Step 6:** Determine the presence of the signal based on  $T_3(N_s), T_4(N_s)$  and the threshold: if  $T_3(N_s)/T_4(N_s) > \gamma$ , signal exists; otherwise, signal does not exist.

#### C.2.5.2 Performance of the algorithms for wireless microphone signal

The threshold  $\gamma$  in CAV or CFN is determined by the ratio  $T_1(N_s)/T_2(N_s)$  or  $T_3(N_s)/T_4(N_s)$  and the required probability of false alarm ( $P_{fa}$ ). When there is no signal, the ratio is not related to noise power at all. Hence, it does not have the noise uncertainty problem. Both methods do not need noise power estimation. The performances of the methods are not only related to SNR but also related to signal statistic properties.

In the following the performances of the methods are given based on simulations, where  $L = 10$ . The required SNR is the lowest SNR which meets the requirement of  $P_{fa} \leq 0.1$  and the probability of misdetection  $P_{md} \leq 0.1$ . Note that the SNR is measured in one TV channel with 6 MHz bandwidth. The performance of the methods can always be improved by increasing the sensing time.

For wireless microphone detection, choosing a down-sampling factor  $M > 1$  gives better performance. Table C.14 gives the simulation results for wireless microphone signals [average on three types of signals: soft speaker, loud speaker and silence (Clanton, Kenkel, and Tang [3])]. The settings and procedures for the simulation are as follows. Baseband microphone signal is generated. The signal is sampled at sampling rate 12 MHz. The signal is then filtered with a low-pass filter with 6 MHz bandwidth. The signal is passed through a multipath simulator (Rayleigh fading with 5 taps). White noise samples (sampling rate 12 MHz) are generated and passed through the same filter. The signal and scaled noise are added together and then down-sampled (decimated) by a factor  $M = 2$ .

**Table C.14—Required SNR for wireless microphone signal detection**

Method	4 ms	10 ms
CAV	-20.8 dB	-22.8 dB
CFN	-20.8 dB	-22.8 dB

## C.2.6 ATSC pilot covariance sensing technique

### C.2.6.1 Covariance based sensing algorithms

The principles and basic procedures of the algorithms are the same as those in C.2.5. The only difference is the choice of the filter. If a filter with 6 MHz bandwidth is chosen, the methods are exactly the same as those for wireless microphone detection. Since ATSC DTV has a pilot tone with much higher power, it is better to use a narrowband filter to just catch the pilot tone. The location of the pilot tone spans about 59 KHz. We need a filter with more than 60 KHz bandwidth in order to catch the pilot tone at all cases.

### C.2.6.2 Performance of the algorithms for ATSC DTV

In the following the performances of the methods are given based on simulations, where  $L = 10$  and  $M = 1$  (no down-sampling) are chosen. The captured DTV signals and white noises are passed through a narrowband bandpass filter with center frequency 2.381119+0.30944 MHz and bandwidth 60 kHz. The required SNR is the lowest SNR that meets the requirement of probability of false alarm  $P_{fa} \leq 0.1$  and probability of misdetection  $P_{md} \leq 0.1$ . Note that the SNR is measured in the entire TV channel with 6 MHz bandwidth. The results are averaged on the 12 specified DTV signals.

**Table C.15—Required SNR for ATSC DTV signal detection**

Method	4 ms	16 ms	48 ms	100 ms	150 ms
CAV	-13.4 dB	-16.8 dB	-20 dB	-21.8 dB	-23 dB
CFN	-13.5 dB	-16.9 dB	-20 dB	-21.8 dB	-23 dB

## C.2.7 Spectral correlation sensing technique

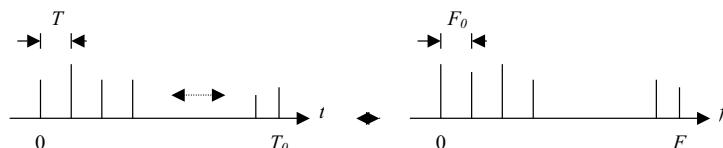
### C.2.7.1 Principle of operation

In this sensing scheme, only spectral components from the received signals are used to extract information on incumbent user signals. No time domain signal components are needed and no time domain analysis is executed for this type of sensing. This makes the receiver less sensitive on other parameters used to design TV band tuners—for example, phase noise, etc.

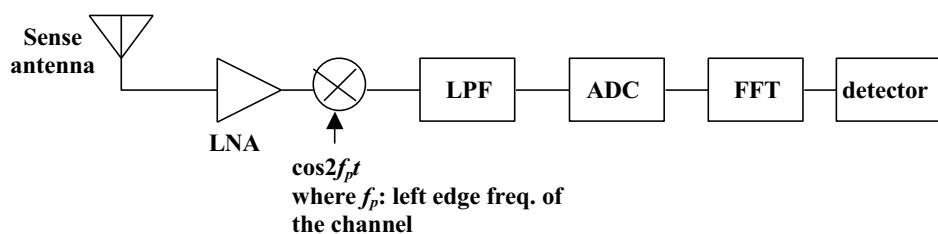
In WRAN systems, inherently frequency spectral components are available as a form of FFT outputs at the receivers. All or part of these components can be utilized for this sensing and this fact makes implementation of this scheme simpler with less cost. Time domain signals can be transformed into the frequency domain spectra as shown in Figure C.25 using the Fourier transform.

In this type of sensing, with one measurement for one symbol duration, all frequency components can be obtained. It means that the whole frequency band can be covered for a period of one symbol duration. For better sensing performance, the measured components will be averaged for more than one symbol duration. For that case, sensing can take place for the duration of a few OFDM symbols.

Correlation detection described in this subclause is not energy detection that simply measures the amount of energy (or power) of the received signal. Correlation detection measures the correlation between spectral signatures of the received signals and pre-stored signature information on various types of incumbent user signals. Thus more accurate information on target signals can be extracted at the receiver with relatively simple implementation. This spectral information for various incumbent signal types is stored in the detector depicted in Figure C.26.



**Figure C.25—Discrete Fourier transform**



**Figure C.26—Sensing receiver structure**

### C.2.7.2 Description of operation

#### C.2.7.2.1 Sensing for one TV channel band

To use only spectral components—not time domain signal components—as described in the above, the received TV band signals are Fourier transformed at the receiver for only one TV band by using FFTs.

After wide band tuning and down converting or down converting and low pass filtering at the receiver, this FFT transform is executed.

Parameters for one typical example for this application are as follows:

- BW =  $F = 6$  MHz for one band case in the United States
- Sampling interval  $T=1/B=1/6$  us, sampling rate = BW = 6 MHz
- Frequency resolution (or frequency separation)  $F_0=3$  KHz
- Time period  $T_0=1/F_0=1/3$  ms
- Number of samples needed  $N_0=T_0/T=2$  KHz
- Needs 2K point FFTs

#### **C.2.7.2.1.1 Sensing procedure for TV signals**

Several to a large number of frequency components are taken in a TV channel band depending on the required sensing accuracy. Refer to C.2.7.4 on how these frequency components can be selected.

To compare values of these components with pre-stored information, the following two methods are applied:

- Correlation calculation: to compare the shape of spectrum of the received signal with the well-known shapes of possible incumbent signals
- Calculate correlations with pre-stored values of spectral information for NTSC and DTV signals or other TV signals
- If one of these correlation values is larger than predetermined values, the judgment is that NTSC or DTV or one of other TV signal exists.
- Pilot detection: to check whether a pilot signal exists or not
- Calculate the ratio of a pilot component to another component around the pilot after another component is picked such that this ratio is maximized.
- For the example in the above, if  $F417/F1200 > th_n$ , this signal is NTSC where  $th_n$  is the predetermined threshold for NTSC signals where  $F_n$  is the  $n^{\text{th}}$  spectral component. If  $F103/F1200 > th_d$ , this signal is DTV where  $th_d$  is the predetermined threshold for DTV signals.

Frequency component values or correlation values or ratios for several symbol periods can be averaged to have better sensing results.

#### **C.2.7.2.1.2 Sensing procedure for wireless microphone signals**

Wireless microphone systems should not be operated on the same frequency channel band as a local TV station uses. It means only open (unoccupied) frequencies should be used for microphones. Most microphone signals are FM modulated with a bandwidth of much less than 200 kHz and at most 200 kHz. (Refer to IEEE 802.22-07/0124r0 Wireless Microphone Signal Simulation Method, March 2007.)

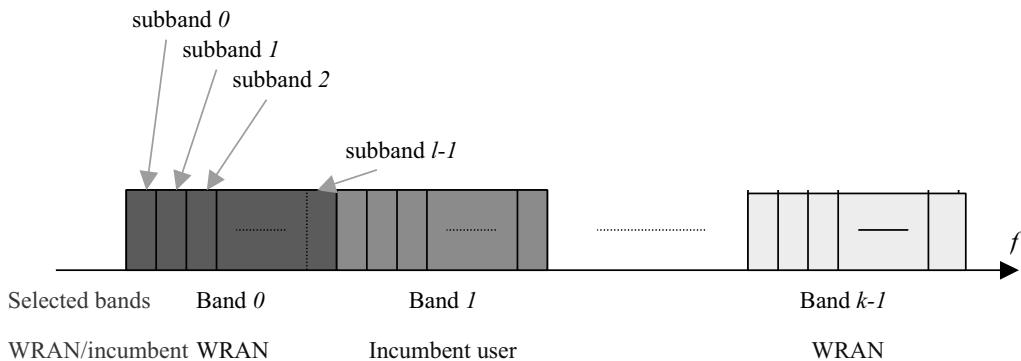
With these above assumptions, microphone signals can be detected using the following procedure by sensing the spectral components using FFT devices:

- For the above example, for every 3 kHz in a 6 MHz band a spectral component is measured and compared with other components.

- If considerable components in a 200 kHz band exist, the judgment is that a wireless microphone is operated in that band as follows:
  - For the previous case, for example, if consecutive six components spaced equally in 200 kHz have considerable amount of energy, it is judged that a microphone signal is detected.
  - Or if more correlation with stored information on various microphone signal spectral signatures (mainly FM signatures) than predetermined value exists, a wireless microphone is operated in that band using correlation calculation.

### C.2.7.2.2 Sensing for multiple TV channel band

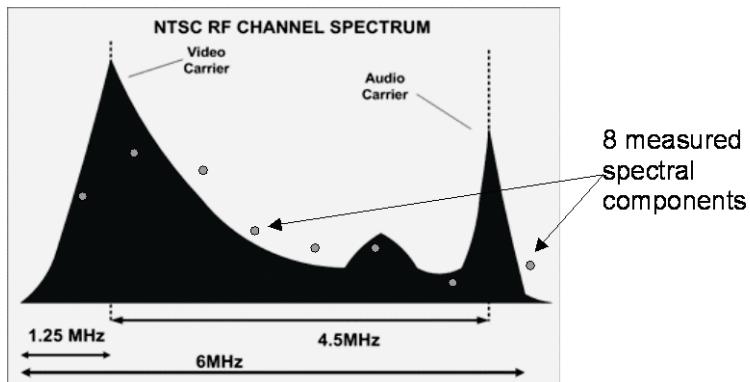
The above method for one TV channel band can also be applied extensively for multiple TV channel band. Multiple channel band which has  $k$  TV channels as shown in Figure C.27 is divided into  $k \times l$  sub-bands where each TV channel is divided into  $l$  sub-bands. Each sub-band has one frequency spectral component. Only difference between one TV channel band case and multiple TV channel case is that for multiple TV channel band case some of every  $l$  components are used to compare with the pre-stored information. To compare the spectral components with the pre-stored information, the above comparison methods are applied.



**Figure C.27—Multiple TV channel band by selecting  $k$  consecutive channel band out of  $n$  channels**

### C.2.7.3 Example of spectral correlation for NTSC signals

One spectral correlation example is as shown in Figure C.28. In this example for NTSC signals, eight uniformly spaced frequency components are chosen to compare the components.



**Figure C.28— Spectral correlation example using eight measured component**

#### C.2.7.4 Selection of frequency components: emphasizing near parts with abrupt changes

How to pick frequency components and how many components to be picked to compare them with pre-stored information are important factors to improve the performance. The simplest way to pick the components is in a uniformly spaced manner.

To have better performance for this sensing scheme, these components do not need to be selected evenly with equal spacing. Some parts of this spectrum have flat characteristics while some other parts have abrupt changes in spectral amplitudes especially near pilot components. For the parts with abrupt changes, more components can be selected while fewer components are picked for the flat parts. Through this emphasizing, higher correlation can be obtained.

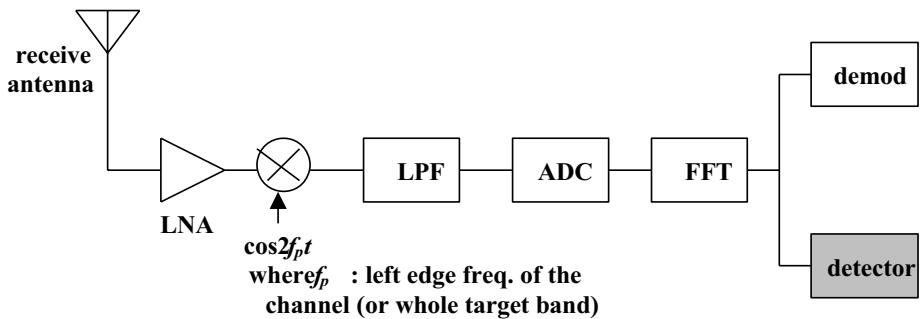
If more components are used for correlation calculation, better performance can be achieved, entailing higher complexity. However, relatively simple calculations can be needed for this comparison. If  $m$  components are used, only  $m$  multiplications need to be executed.

#### C.2.7.5 Typical receiver structure

A typical receiver structure is shown in Figure C.29. The WRAN OFDM receiving structure can be used for this sensing by adding one detector block. This detector calculates correlations or averages of the received signal amplitudes, or compares the signal amplitude of pilot signal components with adjacent components as described in the above. The information on incumbent user signals is stored in this block.

At the receiver, data receiving for WRAN services and incumbent signal sensing are executed simultaneously without having separate receiving and processing branches.

Using the sensing method for multiple TV channels case, relatively coarse sensing can be done for a wider band by covering multiple TV channels simultaneously. If more precise sensing is needed, sensing for single TV channel may be applied with an additional signal processing block. For this case, one more ADC and FFT are added to this structure.



**Figure C.29—Typical sensing receiver structure by mainly using OFDM receiver blocks**

### C.2.7.6 Required SNRs

To provide a brief glimpse for the performance, the required SNR values are given in Table C.16 for a probability of false alarm of 0.1 to achieve probabilities of detection of 0.9 and 0.1 for real DTV signals. These numbers are obtained for three cases of sensing times and numbers of frequency components for correlation calculation as shown in the table. Sensing time is a multiple of one OFDM symbol duration of 1/3 ms while numbers of components are at most 200 points, which means only at most 200 multiplications are needed for the calculations. The required SNRs vary as the noise uncertainty changes. The simulation results show that there is 4 dB degradation on SNRs for the noise uncertainty of 1 dB.

**Table C.16—Required SNRs vs. Sensing Time/Number of components for correlation calculation**

Sensing time, number of components for calculation	Required SNR(dB), Prob. of detection of 0.9	Required SNR(dB), Prob. of detection of 0.99
1/3 ms, 50 components	-7	-3.5
2 ms, 100 components	-12	-8
10 ms, 200 components	-29	-15.5

## C.2.8 ATSC cyclostationary sensing technique

### C.2.8.1 General

It has been recognized that many random time series encountered in the field of signal processing are more appropriately modeled as cyclostationary, rather than stationary, due to the underlying periodicities in these signals (Gardner [5]). Another reason to use cyclostationary signal model is that random signals such as white Gaussian noise are not cyclostationary. Thus, cyclostationarity provides us a way to separate desired signals from noise.

### C.2.8.2 Cyclostationary feature of ATSC DTV signals

According to the ATSC Digital Television Standard [1], DTV data are VSB modulated. Before VSB modulation, a constant of 1.25 is added to the 8-level pulse amplitude modulated signal (8-PAM). Therefore, there is a strong pilot tone on the power spectrum density (PSD) of the ATSC DTV signal. Let

$s(t)$  be this pilot tone signal which is a sinusoidal signal in the time domain and further assume that this strong pilot tone is located at frequency  $f_0$ , i.e.,

$$s(t) = \sqrt{2P} \cos(2\pi f_0 t + \theta) \otimes h(t) \quad (\text{C18})$$

where  $P$  and  $\theta$  are the power and the initial phase of the sinusoidal function respectively. The function  $h(t)$  is the channel impulse response and  $\otimes$  is the convolution operator. The received signal must contain the signal as shown in Equation (C19).

$$x(t) = s(t)e^{-j2\pi vt} + w(t) \quad (\text{C19})$$

where  $w(t)$  is the additive white Gaussian noise (AWGN) and  $v$  is the amount of frequency offset in the unit of Hz. We will assume that  $w(t)$  is zero-mean with autocorrelation function  $Rw(\tau) = E[w(t)w^*(t-\tau)] = \sigma^2 \delta(\tau)$ . The cyclic spectrum of the received signal must contain the cyclic spectrum of  $x(t)$ , which is given by

$$S_x^\alpha(f) = \begin{cases} \frac{P}{2} [\delta(f - f_0 - v) + \delta(f + f_0 + v)] |H(f)|^2 + \sigma^2 & \text{for } \alpha = 0 \\ \frac{P}{2} \delta(f) H(f - f_0 - v) H^*(f + f_0 + v) & \text{for } \alpha = \pm 2(f_0 + v) \\ 0 & \text{otherwise} \end{cases} \quad (\text{C20})$$

where  $H(f)$  is the frequency response of the channel. The parameter  $\alpha$  is the cyclic frequency. From Equation (C20), ideally, the noise does not contribute to the cyclic spectrum of  $x(t)$  when cyclic frequencies  $\alpha = \pm(2f_0 + v)$ . Thus, performing spectrum sensing by detecting the peaks on the cyclic spectrum of the signal should be better than that of using PSD.

### C.2.8.3 Initial processing of received signal

The RF ATSC DTV signal for a given DTV channel is first filtered and down-converted to a given intermediate frequency (IF). The IF signals are usually sampled at a rate that is multiple times of the symbol rate. The samples can be expressed as

$$y[n] = x[n] + w[n] \quad (\text{C21})$$

where  $x[n]$  are samples of the transmitted DTV signal. The noise  $w[n]$  is assumed to be zero-mean with variance  $\sigma^2$ . Then,  $y[n]$  is used to perform cyclostationarity based sensing algorithms.

### C.2.8.4 Test statistic using cyclic spectrum

First, we use a proper narrow band-pass filter to filter  $y[n]$  and obtain a small frequency bands which contains the pilot tone. Then,  $y[n]$  is down-converted to have lower central frequency. Note that we will perform down-conversion for multiple times. Let  $z_l[n]$  denote the down-converted signal that has a central frequency  $f_{IF} + lf\Delta$ . Note that  $f\Delta$  is chosen to be small, which depends on the sample rate and FFT size used in computation of the cyclic spectrum. We will decimate  $z_l[n]$  by a proper decimation ratio  $D$  to obtain  $z_lD[n]$ , which has a lower sampling rate. Finally, we compute the cyclic spectrum by

$$S_z^\alpha(k) = \frac{1}{2L+1} \frac{1}{\Delta t} \sum_{l=-L}^L Z_l^D(k + \alpha/2) \cdot Z_l^{D*}(k - \alpha/2) \quad (\text{C22})$$

where

$$Z_l^D(k) = \sum_{n=0}^{N-1} z_l^D[n] e^{-j2\pi kn/N} \quad (\text{C23})$$

Note that in Equation (C22), we use a spectral smoothing method by averaging  $2L+1$  times to obtain cyclic spectrum. In Equation (C23),  $N$  is the number of time samples used to compute short-term Fourier transform. The parameter  $\Delta t$  is the length of data segment which equals to  $(N-1)T_s$  where  $T_s$  is the time-sampling increment of the signal  $zID[n]$ . Finally, we use

$$T = \max_{\alpha} |S_z^{\alpha}(0)| \quad (C24)$$

as our decision statistic.

The range of  $\alpha$  depends on  $f_{IF}$  and frequency offset.

### C.2.8.5 Simulation results

The performances of the cyclostationarity based algorithm were demonstrated using computer simulations according to the spectrum sensing simulation model (Mathur, Tandra, Shellhammer, and Ghosh [9]). The band-pass filter used to filter the pilot tone has a bandwidth of 40 KHz and  $f_{IF}$  is 17 KHz. The decimation factor is 200 and the decimation filter is a  $\pm 50$  KHz low-pass filter. The size of FFT is 2048. The parameter  $L$  in Equation (C22) is 2 and  $f/\Delta$  is set to be half of the carrier spacing divided by  $2L+1$ . We set the false alarm rate equal to 0.1. The 12 reference Capture Data files are simulated. The required SNR for 0.1 of misdetection rate are given in Table C.17, Table C.18, and Table C.19 for the best, worst and average case of the 12 reference Capture Data files. The parameter  $\Delta$  in the tables is the amount of the noise uncertainty.

**Table C.17— Required SNR for the cyclostationary feature detector (Best case)**

Sensing Time/Sequence	$\Delta=0$ dB	$\Delta=0.5$ dB	$\Delta=1$ dB
	Required SNR (dB)		
19.03 ms	-31	-30.5	-30

**Table C.18— Required SNR for the cyclostationary feature detector (Worse case)**

Sensing Time/Sequence	$\Delta=0$ dB	$\Delta=0.5$ dB	$\Delta=1$ dB
	Required SNR (dB)		
19.03 ms	-21	-20.5	-20

**Table C.19— Required SNR for the cyclostationary feature detector (Average)**

Sensing Time/Sequence	$\Delta=0$ dB	$\Delta=0.5$ dB	$\Delta=1$ dB
	Required SNR (dB)		
19.03 ms	-25	-24.5	-24

## C.2.9 Time domain correlation based method (CBM) for sensing analog TV signals

### C.2.9.1 Analog TV signals basics

In analog TV technology, moving pictures are produced by scanning horizontal lines (625 for all varieties of PAL, except PAL-M and SECAM, 525 for NTSC and PAL-M) and showing those in two fields. Each horizontal line has duration of 64 microseconds in all varieties of PAL except PAL-M and SECAM, 63.49 microseconds in PAL-M, and 63.56 microseconds in NTSC. In most of the standards, all except 25 lines per field contain video signal and are composed of several segments as shown in Figure C.30. It includes a horizontal sync pulse that has the highest amplitude normalized to unity or 100%. In the receiver, this helps synchronization and decoding of each line video signal (luminance and chrominance signals) that follows

it. The luminance signal (also called Y signal, the black and white video signal) can vary within 0% to 75%. PAL and SECAM signals are usually channelized in 7 MHz or 8 MHz channel and NTSC signals are usually channelized in a 6 MHz channel.

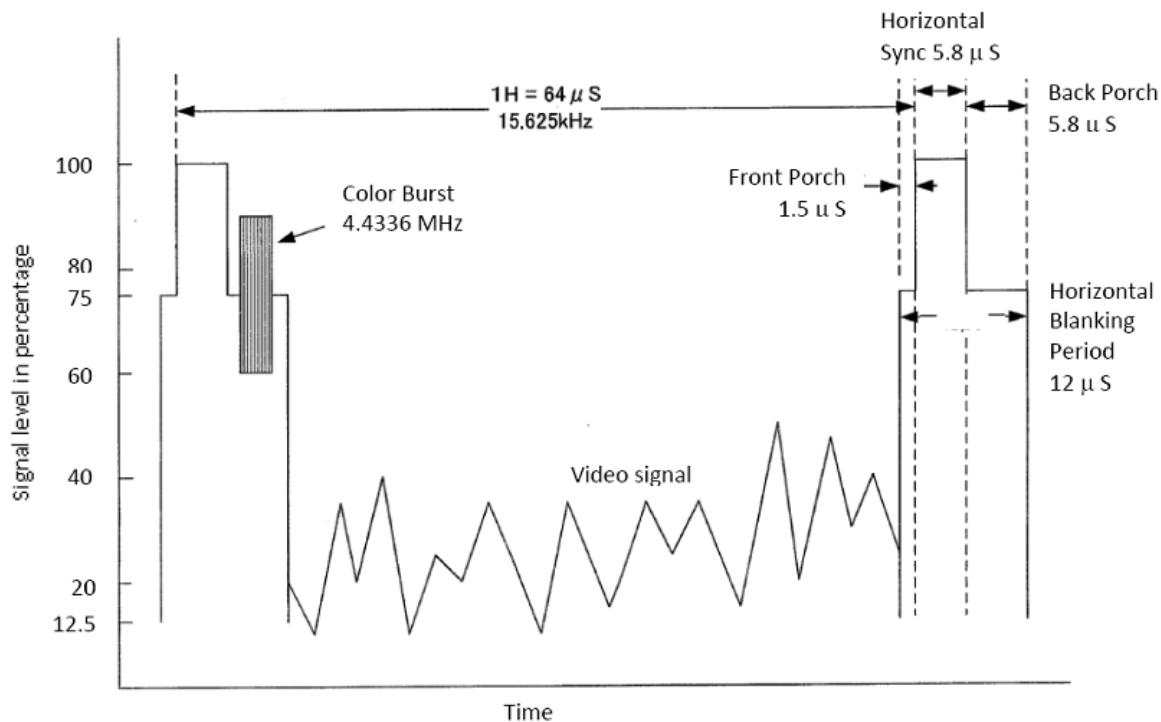
### C.2.9.2 Sensing system and method

Figure C.31 shows a block diagram of the sensing system described in this subclause. The boxes shown in dashed line are optional. The procedure of the sensing technique has the following steps:

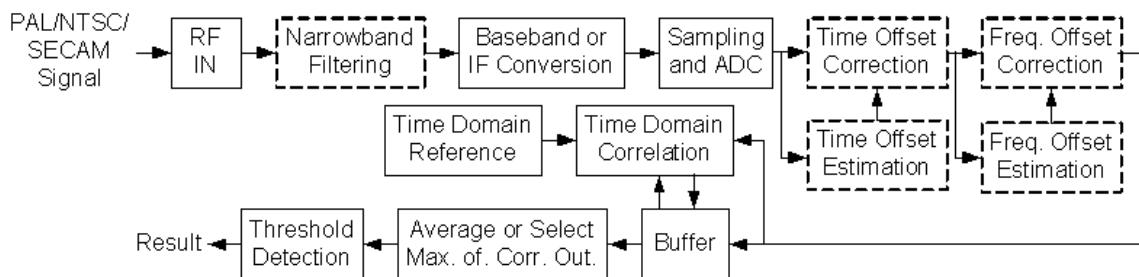
- 1) The analog TV signal enters the radio frequency front end, which is then passed through a narrowband filter, if any, centered at the luminance or Y signal of the channel.
- 2) The signal is converted to baseband if the sensor is equipped with such a block, otherwise intermediate frequency conversion is performed.
- 3) The down converted signal is sampled and analog to digital converted.
- 4) Time offset is estimated and corrected if supported by hardware. This may be followed by frequency offset estimation and correction.
- 5) The sampled data is correlated with a prior-stored reference template signal, for example, as shown in Figure C.32, which matches with the horizontal sync pulse. Since, video signal is unknown, mid value is used as reference for that segment. The data before and after correlation are stored in a buffer.
- 6) Average the correlation outputs or select the maximum of the correlation outputs, if correlation is performed more than once.
- 7) Detect based on a predefined threshold as decided following the above mentioned steps in the absence of any signal input.

### C.2.9.3 Sensing performance

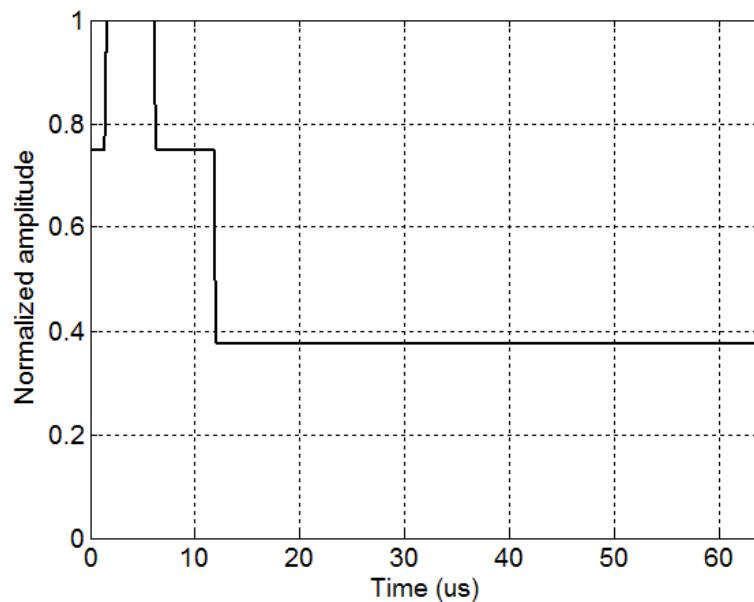
The algorithms were tested by computer simulations and hardware implementations for PAL signal detection. In simulation studies, the PAL signal was simulated according to ITU-R, Conventional television systems [11]. AWGN channel was considered. Figure C.33 shows the simulated receiver operating curves ( $P_D$  vs.  $P_{FA}$ ) for time and phase asynchronous CBM method. The baseband conversion was considered, however, narrowband filter was not used. Sampling was done at 100 MHz. The figure shows that averaging over 2 correlations over two arbitrary horizontal lines suffices to fulfill the requirement ( $P_{FA}=0.1$  and  $P_D=0.9$ ) for  $SNR = -18$  dB. Averaging over 4 lines meets similar requirements for  $SNR = -25$  dB. The minimum sensing time is 128 microseconds for the former and 256 microseconds for the latter case. Figure C.34 shows the performance of the algorithm implemented in hardware while detecting  $-120$  dBm PAL signal input from a signal generator, in a 8 MHz channel ( $SNR = -15$  dB without considering the noise figure). The narrowband filtering, baseband conversion operations were not realized. Time and phase asynchronous CBM method was utilized. Sampling frequency was 64 MHz on a signal down converted to intermediate frequency of 70 MHz, implying effective center frequency of 6 MHz of the sampled data. Two variants of the CBM method were used, where detection was performed based on the average of the correlation outputs or the maximum correlation output among 32 trials (lines). Both the variants show robust sensing capability in such level. However, as the sensing level becomes much lower, due to the sharp nature of the curves obtained from average CBM, it might have an edge over the maximum selection CBM. Note that performing 32 correlations means a minimum sensing duration of about 2 milliseconds. However since all the horizontal lines do not contain video, the sensing reliability may be improved by performing a predefined number of correlations scattered over frame duration. To decrease sensing time considerably, using a narrowband filter that has a center frequency at the luminance signal or Y signal of the channel would help.



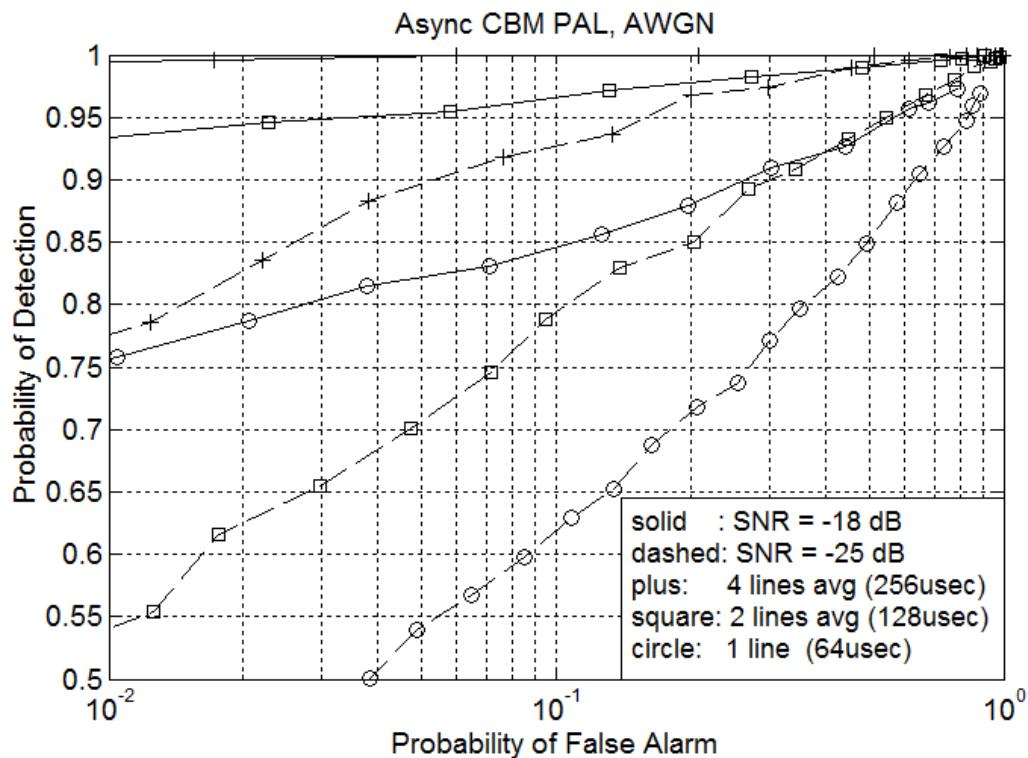
**Figure C.30—Component of a PAL TV signal horizontal line**



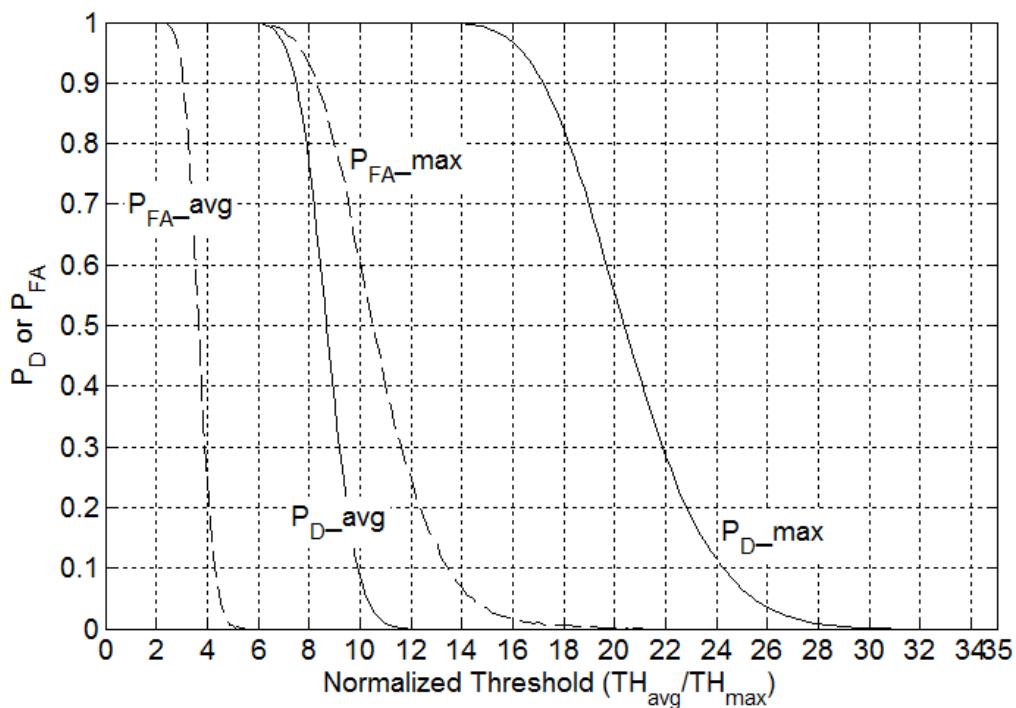
**Figure C.31—Block diagram of analog TV signal sensing system**



**Figure C.32—Baseband equivalent of the reference template for analog TV signal sensing based on CBM**



**Figure C.33—Simulations: Probability of detection vs. probability of false alarm of PAL Sensing in AWGN channel based on CBM**



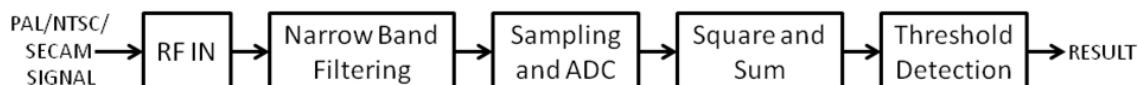
**Figure C.34—Hardware Performance: Probability of detection and probability of false alarm vs. normalized threshold for sensing  $-120 \text{ dBm}/8\text{MHz}$  (or  $\text{SNR} = -15 \text{ dB}$  excluding noise figure) PAL TV sign**

### C.2.10 Sensing system and method

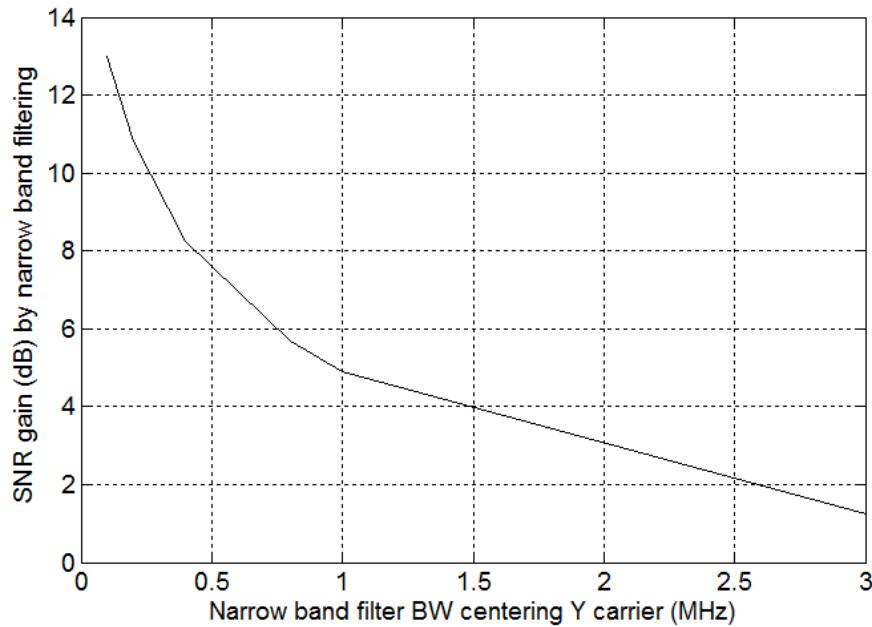
Figure C.35 shows a block diagram of the sensing system described in this subclause. The procedure of the sensing technique is as follows:

- 1) The analog TV signal enters the radio frequency front end, which is then passed through a narrowband filter centered at the luminance or Y signal of the channel.
- 2) The filtered signal is sampled and analog to digital converted, squared and summed, and detection is performed based on a predefined threshold.

As seen in Figure C.36, an SNR gain of around 10 dB can be obtained, if a 300 kHz filter is used centering the Y signal.



**Figure C.35—Improved energy detection method for analog TV detection**



**Figure C.36—Simulation: SNR gain by using a narrow band filter centering Y carrier of PAL signal**

### C.2.11 Time domain correlation based method (CBM) for sensing DVB-T

#### C.2.11.1 DVB-T signal specification

The DVB-T standard was developed by European Telecommunications Standards Union (ETSI) for the terrestrial broadcasting of digital TV. It is currently widely adopted by more than 30 countries. The DVB-T uses orthogonal frequency division multiplexing (OFDM) modulation and is organized in frames. One DVB-T signal super frame consists of four consecutive frames, each frame consisting of 68 OFDM symbols.

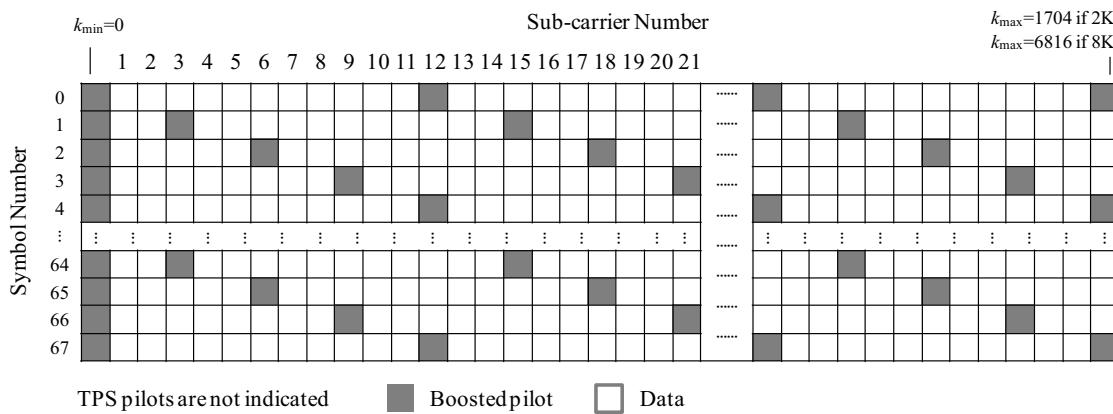
In DVB-T signals, pilots consist of around 10% of the total used subcarriers. Pilots are transmitted at a higher power by about 2.5 dB compared to the data subcarriers. These boosted pilots include continual pilots (CP) and scattered pilots (SP). The CPs are placed at fixed subcarrier locations and their locations do not vary from symbol to symbol, while the SPs are distributed at the positions if  $k - 3 \times (l \bmod 4)$  (the operation ‘mod’ calculates the modulus after division) is divisible by 12, where  $k$  is the subcarrier location and  $l$  is the symbol number. In consequence, as shown in Figure C.37, the pattern of boosted pilots (CPs and SPs) repeats every four OFDM symbols.

The features of boosted pilot subcarriers as shown in Figure C.37 are exploited to achieve reliable detection of DVB-T signals. We generate a reference sequence by conducting inverse Fourier transform (IFFT) of a vector that is only composed of such pilot subcarriers, defined as  $s_p(t)$ .

Let us define the sequence achieved by sampling the  $s_p(t)$  over  $4T$  ( $T$ : one OFDM symbol duration) as

$$s_p[n] = s_p(nT_{sp}), \quad n=0,1,\dots N_{CPPP}-1 \quad (\text{C25})$$

where  $1/T_{sp}$  is the sampling rate, and  $N_{CPPP}$  is the sequence length of one cycle period of pilot pattern.



**Figure C.37— Locations of scattered boosted subcarriers in DVB-T OFDM symbols**  
 [The horizontal axis represents the subcarrier number (frequency)  
 and the vertical axis represents the symbol number (time)]

### C.2.11.2 Improved cross correlation method

#### C.2.11.2.1 Description of the method

The system block diagram is as shown in Figure C.38. Sensing is achieved through following the steps:

- 1) The received DVB-T signal that also contains noise is passed through RF front end and LNA
- 2) The above signal is sampled and converted to digital sequence by ADC
- 3) The above sequence is stored in a buffer
- 4) Averaging of the samples is done over a time span equal to multiple of  $N_{CPPP}$

As described in Figure C.37 and Equation (C25), the pilot pattern of DVB-T sequence repeats with a periodicity of  $N_{CPPP}$ ; we then average the received DVB-T sequence based on  $N_{CPPP}$ , as

$$x_L(n) = \frac{1}{L} \sum_{l=0}^{L-1} x(n - l * N_{CPPP}), \quad n = 0, \dots, N_{CPPP} \quad (\text{C26})$$

- 5) Frequency offset estimation and correction is performed. This is an optional step and the block is shown using dotted lines
- 6) Time offset estimation and correction are done

The purpose of conducting time offset correction is to find the same starting point of the DVB-T sequence and the pilot sequence that is used as a reference in a latter step. Assuming the estimation result shows that the synchronization point locates between the  $M_1$ -th sample and the  $M_2$ -th sample ( $M_2 \geq M_1$ ) of the  $N_{CPPP}$  samples, i.e., locates inside the window of  $[M_1, M_2]$ , then the window size represents the time synchronization level and it is expressed using a metric,  $\Gamma$ , as:

$$\Gamma = 1 - \frac{M_2 - M_1}{N_{CPPP}} \leq 1 \quad (\text{C27})$$

- 7) According to the synchronization level, either correlation or sliding correlation over a specific window is applied:

when the time synchronization level  $\Gamma=1$ , i.e.,  $M_1=M_2$ , correlation is applied, as:

$$R_{xp} = \sum_{n=0}^{N_{CPP}-1} s_p(n)x^*(n) \quad (C28)$$

otherwise ( $\Gamma < 1$ ), sliding correlation is applied over the window of  $[M_1, M_2]$ , as:

$$R_{xp}(m) = \sum_{n=0}^{N_{CPP}-1} s_p(n)x^*(n+m) , m = M_1, \dots, M_2 \quad (C29)$$

where  $x$  is the DVB-T sequence and  $s_p(n)$  is the pilot sequence obtained in Equation (C25).

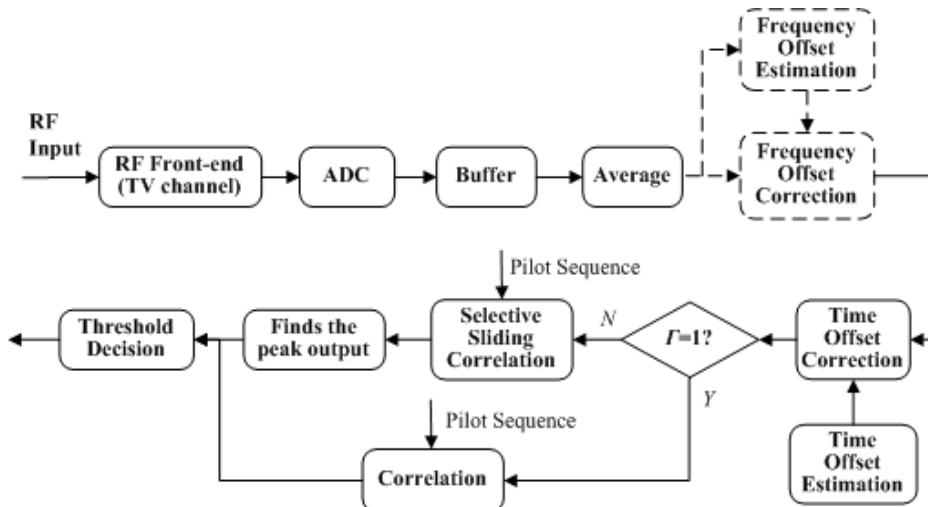
The computation in step 6) is called the selective sliding correlation here since the sliding window of  $[M_1, M_2]$  is selectively decided according to synchronization level achieved in Equation (C26).

- 8) Compare the correlation output (if  $\Gamma = 1$ ) or the maximum of the  $M_2 - M_1 + 1$  correlation outputs (if  $\Gamma < 1$ ) with pre-decided threshold and judge presence/absence of TV signal: if the output is above the threshold, the presence of DVB-T signal is judged

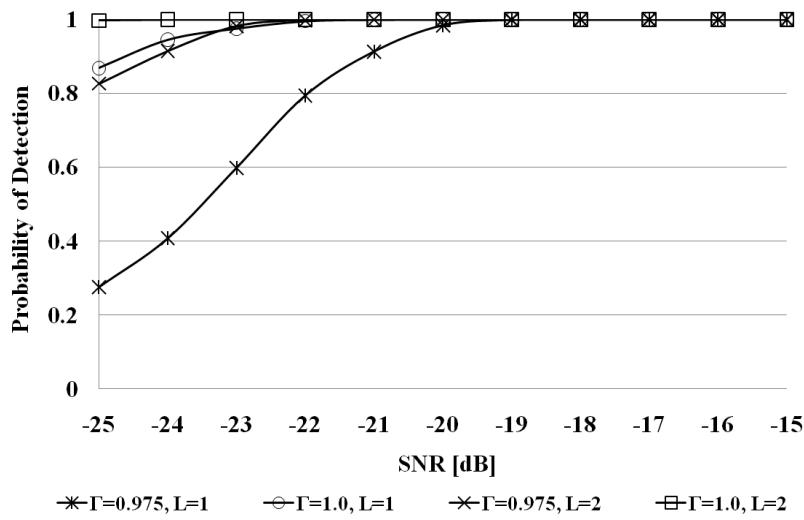
### C.2.11.2.2 Simulation results

Clean DVB-T signals (SNR > 30 dB) generated by DVB-T signal generator (SG) are used as source data in the computer simulation. The DVB-T is the 2K mode with  $T_{CP} = T/32$  ( $T_{CP}$  is the cyclic prefix duration).

Figure C.39 shows the Probability of Detection ( $P_D$ ) vs. SNR by fixing False Alarm Probability ( $P_{FA}$ ) to 0.01 and Figure C.40 shows the receiver operating characteristic (ROC) curves. Sensing performance of the improved cross correlation detection is directly proportional to the time synchronization level,  $\Gamma$ ; it can also be improved by averaging the received DVB-T sequence over the duration of  $N_{CPP}$ . To achieve the sensing performance of  $P_D \geq 0.9$  and  $P_{FA}=0.01$  at SNR = -20 dB in AWGN, the improved cross correlation at both  $\Gamma = 0.975$  and  $\Gamma = 1.0$  requires the same sensing time of 4 OFDM symbol duration, which is around 1.2 ms.

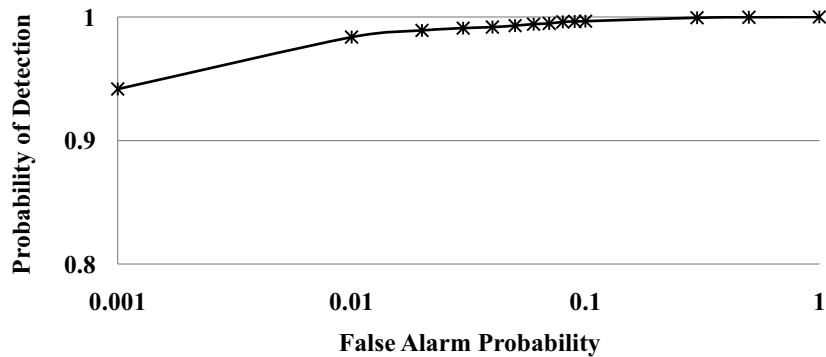


**Figure C.38— Simplified block diagram of the improved cross correlation method**  
**The pilot sequence is the clean SP(n) generated in C.2.11.1**



**Figure C.39—Probability of Detection ( $P_D$ ) vs. SNR in AWGN:  $P_{FA}=0.01$**

The  $\Gamma$  is the time synchronization level defined in C.2.11.2.1,  
 $L$  is the conducted number of average operation defined in C.2.8.4



**Figure C.40—ROC curve in AWGN: the improved cross correlation:  $\Gamma=0.975$ ,  $SNR=-20dB$**

### C.2.11.3 Combined feature and energy detection

#### C.2.11.3.1 Description of the method

As shown in Figure C.34, the combined feature and energy detection method consists of following steps:

- 1) The received DVB-T signal that also contains noise is passed through RF front end and LNA.
- 2) The above signal is sampled and converted to digital sequence by an ADC.
- 3) Frequency offset correction is performed. This is an optional step and the block is shown using dotted lines.
- 4) The sequences with length of  $N_{CPPP}$  are firstly multiplied with the pilot sequence generated in Equation (C25) and then their absolute products are integrated, as:

$$R_{xp} = \sum_{n=0}^{N_{CPP}-1} |s_p(n)x(n)| \quad (C30)$$

- 5) Conduct computation of Equation (C30) for  $\kappa$  ( $\kappa \geq 1$ ) times while shifting the sequence timing by a random interval,  $\tau$ , and calculates the average value, as:

$$\bar{R}_{xp} = \frac{1}{\kappa} \sum_{J=1}^{\kappa} \left[ \sum_{n=0}^{N_{CPP}-1} \left| s_p(n)x\left(n + \sum_{i=1}^J \tau_i\right) \right| \right] \quad (C31)$$

subjects to

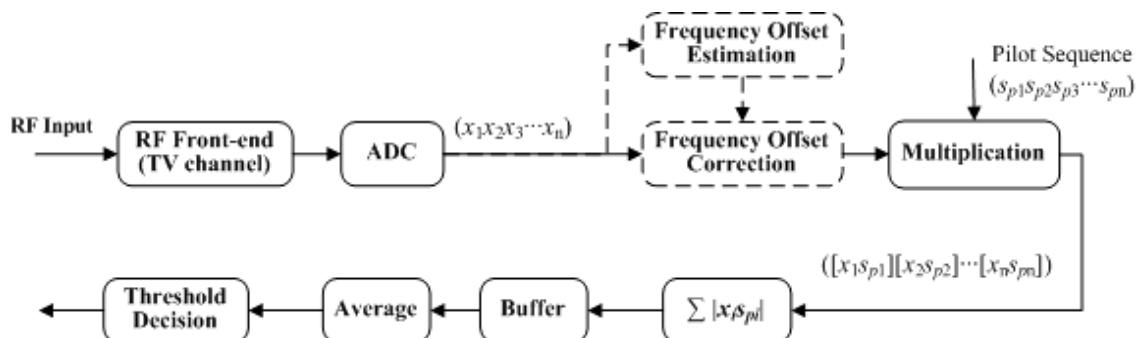
$$\sum_{i=1}^{\kappa} (\tau_i) = 4T \quad (C32)$$

- 6) Compare the output in Equation (C31) with pre-decided threshold and judge presence/absence of DVB-T signal: if the output is above the threshold, the presence of DVB-T signal is judged.

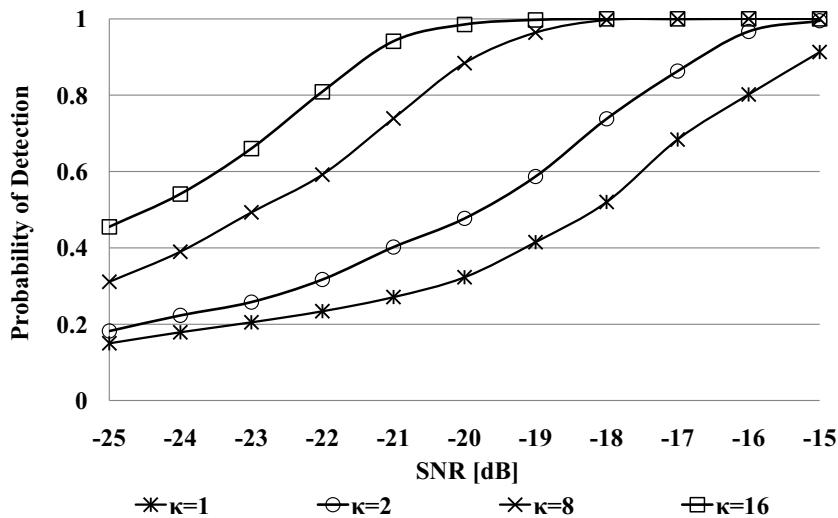
#### C.2.11.3.2 Simulation results

Clean DVB-T signals ( $\text{SNR} > 30$  dB) generated by DVB-T SG are used as source data in the computer simulation. The DVB-T is the 8K mode with  $T_{CP} = T/8$ .

Figure C.42 shows  $P_D$  vs. SNR by fixing  $P_{FA}$  to 0.1. The sensing performance is significantly improved by increasing operation times,  $\kappa$ , defined in Equation (C31). This feature is attractive since as shown in Equation (C32), the increase of  $\kappa$  may not increase the sensing time considerably. Therefore, to achieve the sensing performance of  $P_D \geq 0.9$  and  $P_{FA} = 0.1$  at  $\text{SNR} = -20$  dB in AWGN, the sensing technique requires sensing time of 8 OFDM symbol duration ( $\kappa \geq 8$ ), which is equivalent of around 8 ms.



**Figure C.41—Simplified block diagram of the combined feature and energy detection**

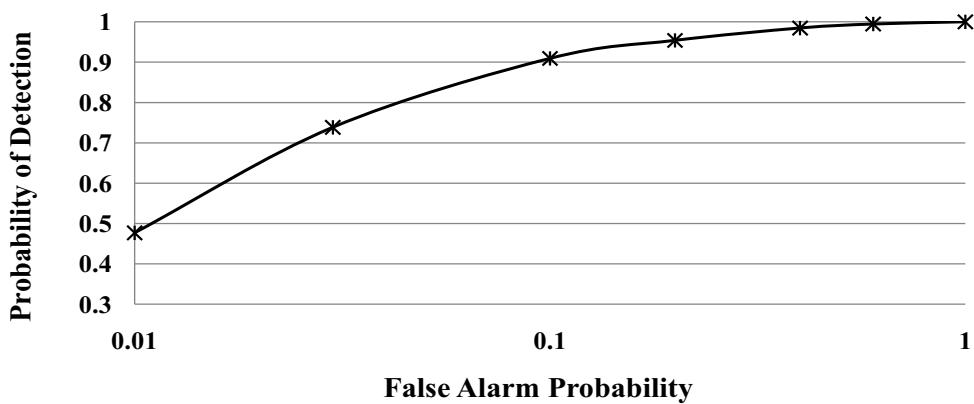


**Figure C.42—PD vs. SNR in AWGN: PFA=0.1. The  $\kappa$  is the operation times defined in Equation (C31)**

#### C.2.11.3.3 Test results of hardware sensing prototype

Sensing performance of the combined feature and energy detection is also verified by hardware tests. In the hardware tests, the 8K mode DVB-T signals ( $T_{CP}=T/8$ ) generated by SG are tuned to  $-120$  dBm/8 MHz using attenuators and then input into the hardware sensing prototype through a cable.

We conducted 5000 runs of tests for each  $P_{FA}$  shown in Figure C.42. Although the results are degraded in comparison with simulation results shown in Figure C.43, they have verified that using the combined feature and energy detection we can achieve  $P_D \geq 0.9$  and  $P_{FA}=0.1$  in the very low SNR regime. Please note that the  $\kappa=32$  operations are conducted for DVB-T sequence of 8 OFDM symbol duration as shown in Equation (C31) and Equation (C32).



**Figure C.43—Hardware test results: ROC curve: DVB-T input level =  $-120$  dBm/8 MHz,  $\kappa=32$**

#### C.2.11.4 Smart threshold setting

##### C.2.11.4.1 Dynamic threshold selection

Dynamic threshold selection (DTS) can be applied to extend sensing capability to lower SNR regime by partially overcoming the limitation due to environment and system noise variance. The DTS is realized through the following two steps:

- 1) Develop a threshold table. Measure the system noise variance and threshold statistics for an extended period of time. Divide the captured whole noise variance range into a number of narrower and non-overlapping ranges and for each range, divide the threshold statistics in similar groups and for each range/group, define a threshold corresponding to a target detection level. Especially, using relaxed target detection level would be useful for sensing in the presence of interference.
- 2) Measure system noise variance immediately prior to sensing and select an appropriate threshold by mapping the noise variance to the threshold table. For example, it can be done by using a programmable switched isolator behind the antenna with impedance that matches the inside RF part. Switching off the isolators isolates the RF part and the noise variance can be measured.

##### C.2.11.4.2 Real-time threshold setting

If the system is equipped with a switched isolator as mentioned in the previous subclause, the necessity of a threshold table can be relaxed. In such a case, the isolator can be switched off and the threshold can be set on a real-time basis immediately prior to sensing.

### C.3 References

- [1] Advanced Television Standards Committee, ATSC Digital Television Standard, ATSC A/53E, April 2006.
- [2] Advanced Television Standards Committee, ATSC Recommended Practice: Receiver Performance Guidelines, ATSC A74, June 2004.
- [3] Clanton, Chris, Kenkel, Mark, and Tang, Yang, "Wireless Microphone Signal Simulation Method," IEEE 802.22-07/0124r0, March 2007.
- [4] ETSI EN 300 744 V1.6 .1 (2009-01), "Digital video broadcasting (DVB); framing structure, channel coding and modulation for digital terrestrial television," ETSI, Tech. Rep., 2009.
- [5] Gardner, W. A., "Exploitation of Spectral Redundancy in Cyclostationary Signals," *IEEE Signal Processing Magazine*, Vol. 8, No. 2, pp. 14–36, April 1991.
- [6] IEEE 802.22 Contribution 22-07-0359-00-0000 at [http://grouper.ieee.org/groups/802/22/Meeting\\_documents/2007\\_July/22-07-0359-00-0000\\_mody\\_spectrum\\_sensing\\_hos\\_1.ppt](http://grouper.ieee.org/groups/802/22/Meeting_documents/2007_July/22-07-0359-00-0000_mody_spectrum_sensing_hos_1.ppt).
- [7] Kay, S. M., Fundamentals of Statistical Signal Processing, Detection Theory, Prentice Hall Signal Processing Series, 1993.
- [8] Kay, S. M., Fundamentals of Statistical Signal Processing, Estimation Theory, Prentice Hall Signal Processing Series, 1993.

- [9] Mathur, S., Tandra, R., Shellhammer, S., and Ghosh, M., "Initial Signal Processing of Captured DTV Signals for Evaluation of Detection Algorithms," *IEEE 802.22-06/0158r4*, Sept. 2006.
- [10] Rahman, M. A., Song, C., and Harada, H., "Spectrum Sensing and Detection of PAL TV Signals," *IEICE Technical Report*, SR2010-64, pp. 169–176, Oct. 29, 2010.
- [11] Recommendation ITU-R, BT.470.5, Conventional television systems.
- [12] Shanmugan, K., A. M. Breipohl, *Random Signals, Detection Estimation and Data Analysis*, John Wiley and Sons, 1988.
- [13] Song, C., Rahman, M. A., Funada, R., and Harada, H., "Robust Spectrum Sensing of DVB-T Signals," *IEICE Technical Report*, SR2010-63, pp. 161–168, Oct. 29, 2010.
- [14] Zeng, Yonghong and Liang, Ying-Chang, "Covariance based signal detections for cognitive radio," *IEEE DySpan*, 2007.
- [15] Zeng, Yonghong and Liang, Ying-Chang, "Maximum-minimum eigenvalue detection for cognitive radio," *IEEE PIMRC*, 2007.
- [16] Zeng, Yonghong and Liang, Ying-Chang, "Simulations for wireless microphone detection by eigenvalue and covariance based methods," *IEEE 802.22-07/0325r0*, July 2007.

## Annex D

(informative)

### Summary of the characteristics of the IEEE 802.22.1 beacon signal and protocols

#### D.1 General

IEEE Std 802.22.1-2010 defines the protocol and data format for communication devices forming a beaconing network offering enhanced protection for licensed low-power auxiliary devices operating in television broadcast bands. In such beaconing network, the following three types of protecting devices (PD) are identified:

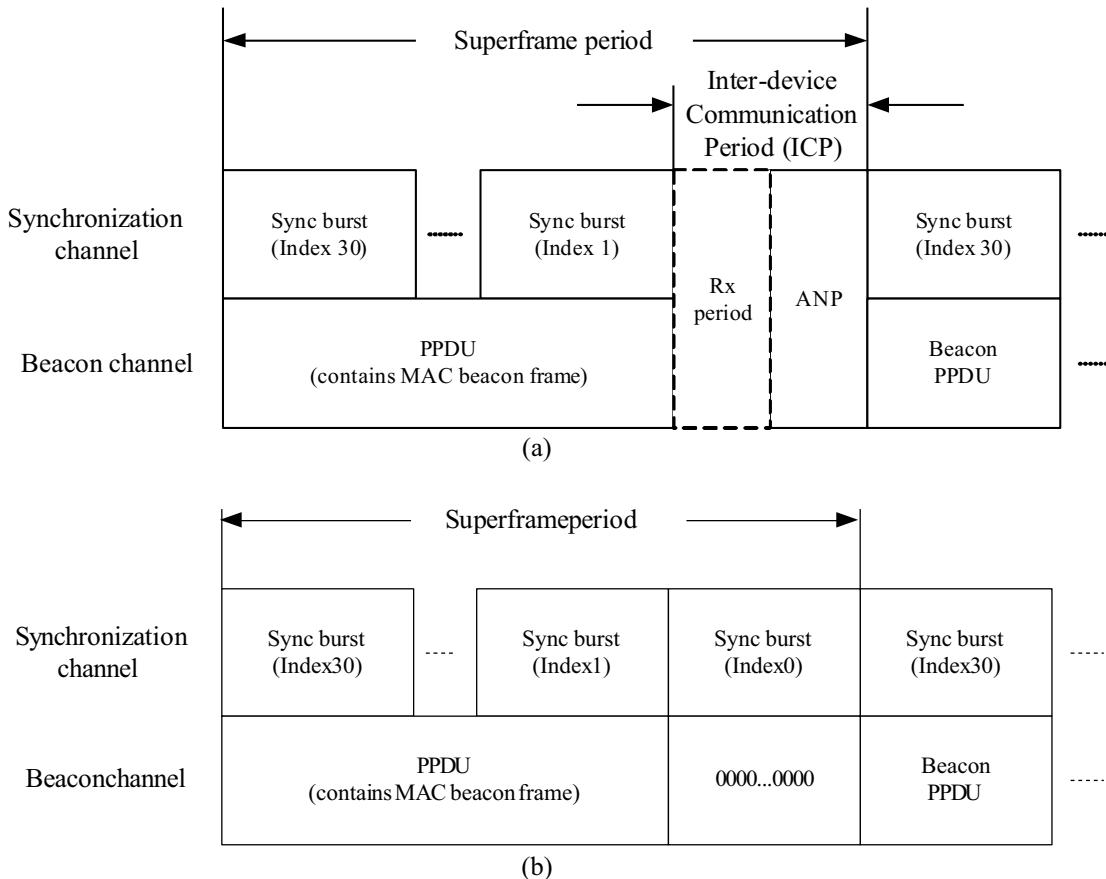
- Primary Protecting Device (PPD): the PPD is the main device responsible for providing incumbent protection. IEEE Std 802.22.1-2010 requires that it transmit beacon data at least every other superframe. The information within the PPD beacon transmissions may or may not include information aggregated as a result of inter-device communication with other PDs.
- Secondary Protecting Device (SPD): an SPD is a PD that has chosen to have another PD to provide protection on its behalf. The protection information is shared with the PPD via inter-device communication, and subsequently broadcasted as part of the PPD's regular beacon transmissions.
- Next-In-Line Protecting Device (NPD): an NPD is an SPD that has been selected by a PPD to become the new PPD in the event that the current PPD ceases beacon transmission.

A beaconing device shall operate using the following parameters:

- Offset from lower TV channel edge: 309.4 kHz
- Chip rate: 76.873 kchips/s
- Symbol rate: 9.6091 kBaud
- Occupied bandwidth: 77 kHz at -3 dB and 110 kHz at -20 dB

#### D.2 Superframe structure

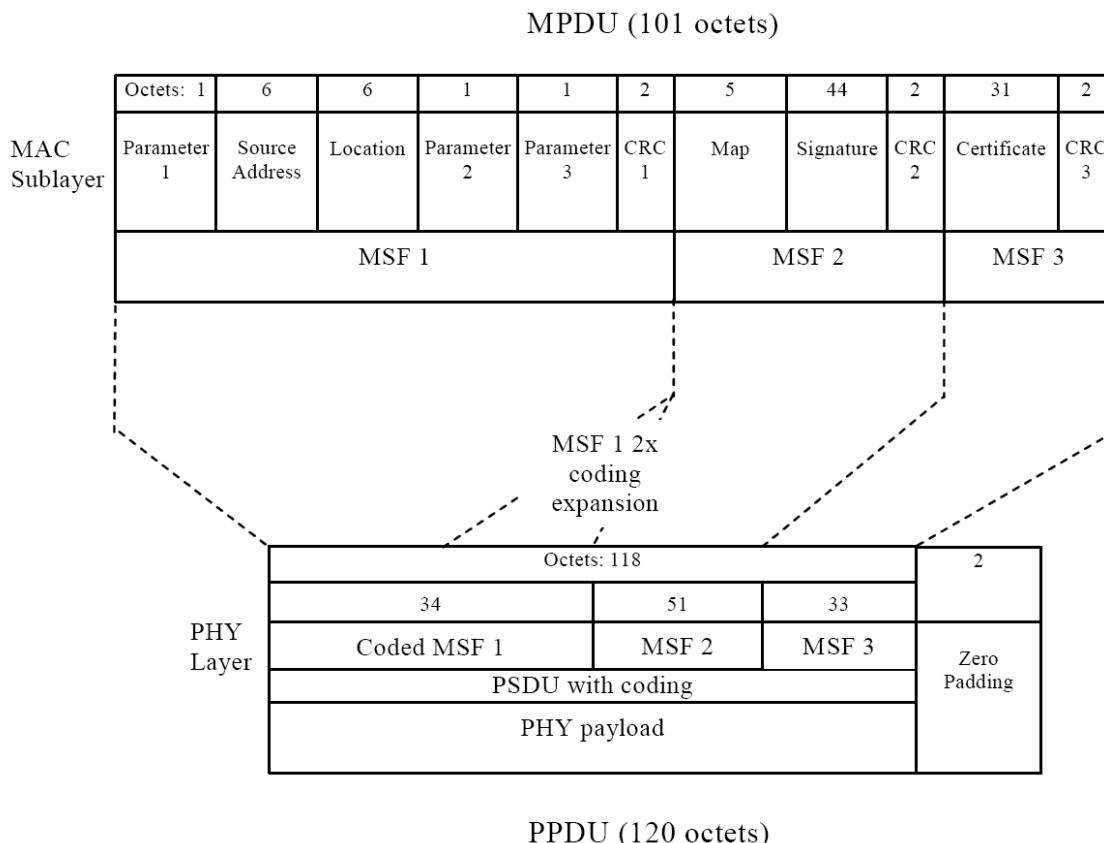
The standard employs the superframe structure shown in Figure D.1. The superframe structure consists of 31 slots. Each slot is comprised of 32 DQPSK symbols, where the symbol duration is 1/9609.1 seconds (i.e., 104.1 microseconds) in length. The superframe is comprised of a synchronization channel and a beacon channel transmitted continuously in parallel. The synchronization channel consists of a succession of synchronization bursts. The beacon channel consists of the PHY Packet Data Unit (PPDU), which contains the MAC beacon frame. Following 30 synchronization bursts and the PPDU, if the PPD is in its initial transmission period, the last slot transmits the synchronization burst of index zero, in which case the PPDU data are all set to zero. Otherwise, the last slot is an inter-device communication period (ICP), which is composed of a receive period (Rx) and an acknowledgement/no-acknowledgement period (ANP) as well as three transit gaps separating those periods.



**Figure D.1—Superframe logical format**

### D.3 Beacon frame structure

The PPDU consists largely of the MAC beacon frame. The MAC beacon frame contains information relevant to the device or devices protected by the protecting device, including the physical location of the beaconing device and the estimated duration of TV channel occupancy. Figure D.2 shows the structure of the beacon frame, which originates from within the MAC sublayer of either a PPD or an SPD. The beacon frame contains three MAC subframes (MSF). MSF1 contains the source address field, location field and three MAC parameter fields. MSF2 contains the channel/subchannel map and signature fields. MSF3 contains the certificate field. The signature and certificate fields are part of the public-key cryptography security solution. Figure D.2 gives a schematic view of the beacon frame and the PHY packet (PPDU).



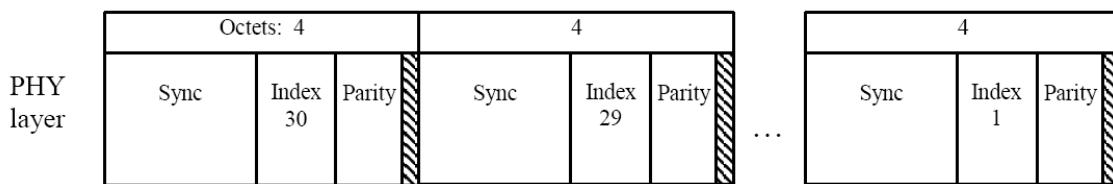
**Figure D.2— Schematic view of the beacon frame and the PHY packet (PPDU)**

#### D.4 Synchronization burst

Each slot contains a synchronization burst, as well as a fixed number of PPDU bits. The synchronization bursts, consist of a 15-bit synchronization field followed by 7-bit index field that decrements with each burst transmission, an 8-bit parity field for detecting and correcting errors on the index value, and a 2-bit reserved field, as is shown in Figure D.3. Each synchronization burst occupies one 32-bit long synchronization channel slot of duration  $32 \text{ bits}/9609.1 \text{ Hz} = 3.3301 \text{ ms}$ .

In the synchronization burst, the sync field is used by the receiver to detect the presence of the synchronization burst and to synchronize to the slot timing. The index field is used to obtain frame synchronization with an incoming beacon. It contains a numerical value equal to the number of slots remaining before the start of the next superframe. The index field is decremented by one each time the data contained within a slot is transmitted until the index reaches either zero or one, depending on whether the PPDU will be followed by an ICP period.

If the PPDU is not followed by an ICP period, the final index is zero, and the next superframe starts immediately. If the PPDU is to be followed by an ICP period, the final index is one, and the next superframe starts after the ICP period.



**Figure D.3—Schematic view of the synchronization burst sequence**

## D.5 Inter-device communication period (ICP)

The inter-device communication period is only included in the superframe if the PPD is not executing the device initialization procedure. The order of symbols within the period is as follows: 5 symbols of turnaround time, 8 symbols for the receive period, 6 symbols of turnaround time, 8 symbols for the ANP and another 5 symbols of turnaround time.

The RTS period is used by an SPD to reserve a superframe to transmit its beacon frame to the PPD. Each RTS burst consist of an RTS codeword field, wherein a RTS codeword shall randomly be selected from the list of available RTS codewords. An NPD codeword can also be sent by the NPD during the RTS period to inform that the NPD is still active. Both RTS codeword and NPD codeword are cyclically shifted sequences of the 15-bit sync field except for the first zero bit in the sequences.

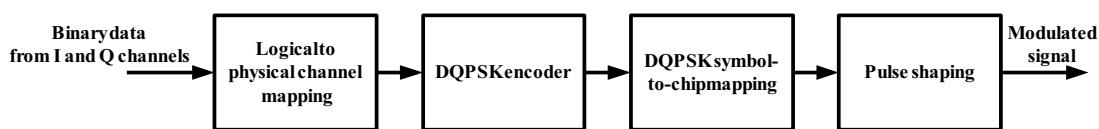
The ANP period is used by the PPD to respond to information received during previous receive periods and, more generally, to communicate with other PDs. The list of possible ACKs in this period is identical to the possible RTS codewords. NACK is also a cyclically shifted sequence of the 15-bit sync field except for the first zero bit in the sequences.

## D.6 PHY specifications

The IEEE 802.22.1 PHY employs direct sequence spread spectrum (DSSS) with differential quadrature phase-shift keying (DQPSK). Figure D.4 provides a functional block diagram describing the PHY modulation and spreading function.

Data bits either belong to the synchronization logical channel, the beacon logical channel, the RTS burst, or the ANP burst, and are parsed between the physical I channel and the physical Q channel, which are used as input for the DQPSK encoding. DQPSK encoding is a phase change applied to the previous DQPSK symbol according to the two raw data bits from the I and Q channels being encoded. After DQPSK encoding, each DQPSK symbol is mapped into an 8-chip, complex, pseudo-random noise (PN) sequence. The chip sequence is modulated onto the carrier with square-root-cosine pulse shaping applied separately to the in-phase and quadrature components of the complex modulation chips.

FEC is applied to portions of both the synchronization burst and the beacon frame. A (15,7) block code is applied to the Index field of the synchronization burst. A half-rate, binary convolutional code is applied to the first MAC subframe (MSF1) of the beacon frame. Details can be found in IEEE Std 802.22.1-2010.

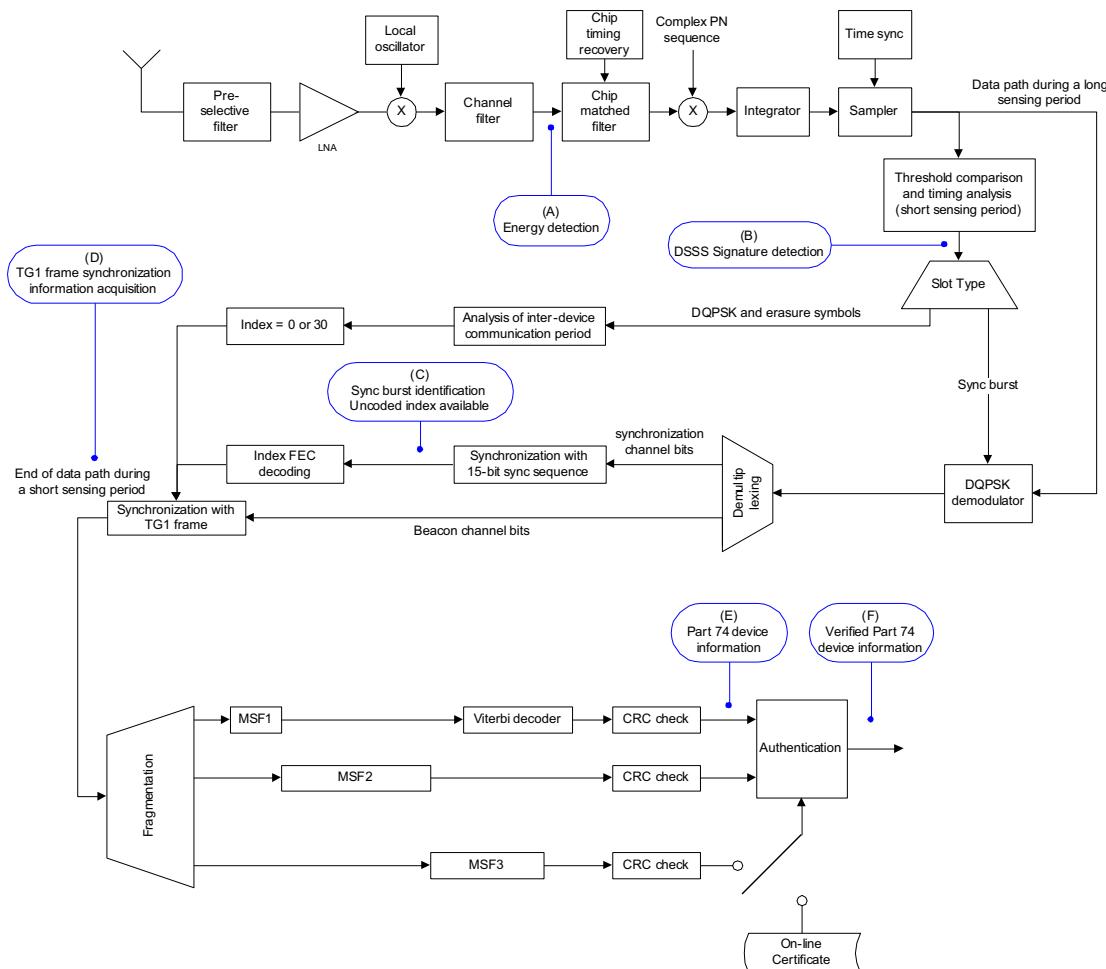


**Figure D.4—Modulation and spreading function**

## D.7 Reference architecture for the WRAN receiver

The reference receiver block diagram is shown in Figure D.5. Decision points along the receiver path are highlighted with numbered boxes. The information that can be extracted at each decision point according to specific implementations is described in Table D.1.

Two data paths are shown in Figure D.5. One data path is used for sensing during short regular quiet periods, and the other data path is used for sensing during a long scheduled quiet period. Note that a different implementation could be used for the data path used for sensing during a short quiet period, where the detection of the presence of the inter-device communication period, and the analysis of the location of the different data fields in the inter-device communication period, could be done after DQPSK demodulation. The demodulator may need to recognize silent symbols, and replace them by erasures rather than make hard bit decisions.



**Figure D.5—Reference receiver block diagram**

**Table D.1—Decision points in the data paths of the receiver**

<b>Decis ion point</b>	<b>Description</b>	<b>Result</b>
(A)	Energy detection of the IEEE 802.22.1 beacon signal within the 76.8731 kHz bandwidth provides improved coverage over the direct detection of the protected wireless microphone signal due to the larger power of the beacon. However, the type of signal detected cannot be deduced from simple energy detection. Measurement of the signal level is an indication of the distance of the IEEE 802.22.1 transmitter from the WRAN receiver.	A certain device is occupying the channel.
(B)	The detection of the 8-chip DSSS PN sequence offers a 9.0309 dB processing gain over energy detection. This is a feature detection technique, which uniquely identifies an IEEE 802.22.1 signal. Reliable detection of the PN sequence is a strong indication of the presence of an IEEE 802.22.1 beaconing device. Measurement of the signal level can give an indication of the distance of the IEEE 802.22.1 transmitter from the WRAN receiver.	An IEEE 802.22.1 beacon is in the channel. Estimated distance of the IEEE 802.22.1 transmitter from the receiver. No synchronization information.
(C)	Identification of the 15-bit sync sequence offers no improvement in terms of signal level (no processing gain), nor any additional information relative to the authenticity of the IEEE 802.22.1 beaconing device, beyond what could be achieved in (B). The sole purpose of the 15-bit sync sequence is to synchronize the bit sequence with the start of the index bit field.	Same as (B)
(D)	At this point, the WRAN receiver may also read the index, but without the error detection and correction capability. Depending on the received signal strength, the receiver may decide that the index was likely received without error and try and schedule a long quiet period to capture the beacon frame. No reduction in short sensing time can be expected with this feature that still needs to capture the 15-bit m-sequence and one index field.	Unconfirmed frame synchronization information from the index
(E)	Successful decoding of the index allows determining the start time of the IEEE 802.22.1 frame in the Q channel. The WRAN can use that information to schedule a quiet period synchronized with the start of a future IEEE 802.22.1- frame.	Confirmed frame synchronization information from the index
(F)	Successful decoding of the bits of the MSF1 field provides all the information that the WRAN needs to protect the Part 74 device. However, the MSF1 bits alone do not allow the WRAN to authenticate the IEEE 802.22.1 beaconing device. The WRAN could be faced with a rogue beacon.	Beacon data available Beacon device not authenticated
	After successful authentication of the IEEE 802.22.1 beaconing device, the WRAN has no further doubt on the presence of a legitimate Part 74 incumbent device in its vicinity, and it must leave the channel.	Beacon data available Beacon device authenticated

## D.8 Sensing and detection at the WRAN receiver

### D.8.1 Sensing thresholds

The threshold input signal measured at the antenna terminals for 1% packet error rate (PER) in a Gaussian channel for the synchronization word, the index value and MSF 1 is expected to be no worse than -116 dBm. This can be achieved with a sensing RF front-end with a Noise Figure of 8 dB, an implementation margin of 2.5 dB and a receiving bandwidth of 77 kHz. This allows for a 5.7 dB margin in additional selective fading for the IEEE 802.22.1 beacon compared to the WRAN 5.625 MHz signal on the

otherwise reciprocal RF path between a 4 W WRAN device and the 250 mW IEEE 802.22.1 beacon (i.e., the radius of sensitivity of the IEEE 802.22.1 beacon is equal to the radius of interference of the 4 W WRAN device with a 5.7 dB margin for extra frequency selective fading expected on the IEEE 802.22.1 beacon signal because of its narrower transmission bandwidth. (Gerald Chouinard spreadsheet on TG1 beacon analysis, February 2009 [4].)

The 1% PER Gaussian channel sensitivity for both MSF 2 and MSF 3 is expected to be no worse than  $-109$  dBm. This difference in sensitivities is due to the omission of error protection redundancies in MSF 2 and MSF 3 to minimize the overall sensing dwell time.

For energy detection correlated on the beacon spreading sequence, the sensing threshold is expected to be no worse than  $-122$  dBm for 5 ms sensing time. Energy detection without lock to the spreading sequence over 5 ms will result in a threshold no worse than  $-113$  dBm. If shorter sensing time is used for energy detection correlated on the beacon spreading sequence, the  $-122$  dBm threshold will raise as a function of  $5 \times \log_{10}(\text{time(ms)}/5)$ . If the energy detection does not rely on the spreading sequence, shorter sensing time will raise the  $-113$  dBm threshold by  $10 \times \log_{10}(\text{time(ms)}/5)$ .

The transmitted center frequency tolerance for the IEEE 802.22.1 beacon is expected to be  $\pm 2$  ppm maximum. This has to be combined with the  $\pm 2$  ppm of the 802.22 system. Automatic Frequency Control will therefore be needed in the IEEE 802.22.1 decoder to counter the constellation rotation resulting from the total  $\pm 4$  ppm frequency tolerance.

The transmit rms error vector magnitudes of the IEEE 802.22.1 burst is expected to be less than 14% averaged over one superframe ( $N = 124$  octets  $\times 8 = 992$  symbols). This EVM measurement is made on baseband I and Q data after recovery through an ideal reference receiver system. The ideal reference receiver is to perform carrier lock, chip timing recovery, and amplitude adjustment while making the measurements. The ideal reference receiver is assumed to have a data filter impulse response that approximates that of an ideal root raised cosine filter with 50% excess bandwidth.

Sensing of the IEEE 802.22.1 beacon will need to be done during quiet periods of the WRAN systems on the channel to be sensed as well as its adjacent channels to avoid desensitization of the sensing receiver by WRAN transmissions.

## D.8.2 Sensing times

The basic timing parameters of the IEEE 802.22.1 signal, and the minimum detection times (worst cases) to meet the sensitivity performance given in D.8.1, are summarized in Table D.2. Note that due to the DQPSK modulation, a single DQPSK symbol duration has been added to the duration of the signal in order to determine the minimum sensing time when demodulation is required. The total minimum sensing time for the superframe is 102.2374 ms.

**Table D.2— Minimum sensing times**

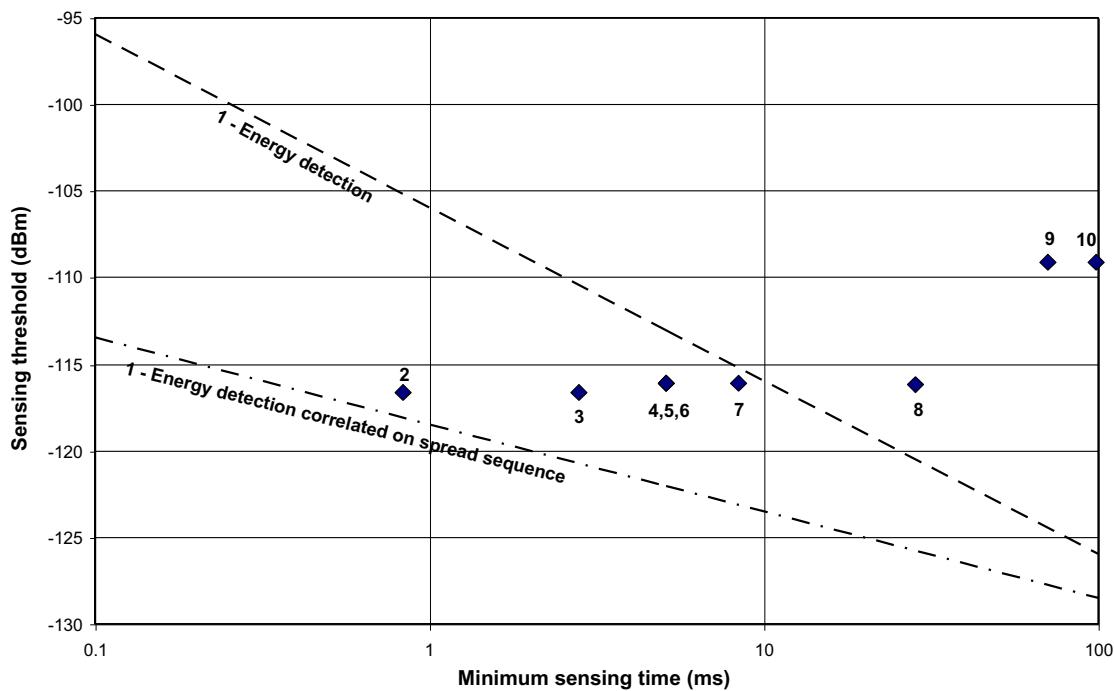
Sensing type	Signal feature	Signal duration	Minimum sensing time	Detection strategy	Related subclause
(1)	Energy	Continuous except in ICP slot	5.1 ms. See 3.1 for more details.	Energy detection in 77 kHz bandwidth	D.8.2.1
(2)	8-chip PN spreading sequence	0.1041 ms (0.1041 ms period)	0.8328 ms within initialization period	Capture 8 consecutive PN sequences <sup>a</sup>	D.8.2.2
(3)	8-chip PN spreading sequence	0.1041 ms (periodicity broken every 30 slots)	2.8107 ms outside initialization period	Capture 8 consecutive PN sequences <sup>a</sup>	D.8.2.3

Sensing type	Signal feature	Signal duration	Minimum sensing time	Detection strategy	Related subclause
(4)	Synchronization information: sync sequence and index	3.3302 ms (3.3302 ms period)	5.1009 ms within initialization period	Capture one sync sequence, and index + parity bits either before or after the sync sequence	D.8.2.4
(5)	Synchronization information: sync sequence and index, and slot type (sync burst or inter-device communication period)	3.3302 ms	5.1009 ms outside initialization period	Capture one sync sequence and index + parity bits, otherwise recognize that the signal contains an inter-device communication period	D.8.2.5
(6)	Synchronization information: sync sequence and index	3.3302 ms (3.3302 ms period)	5.1009 ms twice within 2 seconds asynchronously outside initialization period	Capture one sync sequence, and index + parity bits either before or after the sync sequence	D.8.2.6
(7)	Synchronization information: sync sequence and index (no analysis of the type of slot)	3.3302 ms (periodicity broken every 30 slots)	8.4311 ms outside initialization period	Capture one sync sequence and index + parity bits either before or after the sync sequence	D.8.2.7
(8)	MSF1 (FEC encoded)	28.3070 ms	28.4111 ms	Capture MSF1 synchronously (already synchronized by index)	D.8.2.8
(9)	MSF1+MSF2	70.7676 ms	70.8717 ms	Capture MSF1+MSF2 synchronously (already synchronized by index)	D.8.2.9
(10)	MSF1+MSF2+MSF3	98.2421 ms	98.3462 ms	Capture MSF1+MSF2+MSF3 synchronously (already synchronized by index)	D.8.2.10

<sup>a</sup> Capturing 8 consecutive 8-chip PN sequences is for reference herein.

Note that the detection strategy that would consist in detecting non-adjacent parts of the beacon frame, to later reconstruct the whole beacon, was not considered. This strategy could work in some cases, but there is no guarantee on the integrity of the data. One typical case would be when part of the frame is captured from the transmission of a PPD, while another part of the frame is captured from the transmission of an SPD. It could also be possible that the information in the frame be updated from one superframe to the next, due to aggregation of SPD data into the PPD data.

Figure D.6 describes various sensing time regions together with the corresponding sensing thresholds for the 10 sensing types listed above, according to the receiver sensitivity defined in D.8.1.



**Figure D.6—Summary of sensing thresholds and sensing durations**

#### D.8.2.1 Sensing Type 1

Energy detection can be performed within the 77 kHz bandwidth of the beacon signal, without possibility of identifying the type of signal detected in case of positive detection.

#### D.8.2.2 Sensing Type 2

0.8328 ms is used for capturing 8 consecutive 8-chip PN sequences within initialization period. Since  $0.1041\text{ms} (1/9.6091=0.1041\text{ms})$  is used for correlating 8-chip PN sequences,  $8 \times 0.1041=0.8328\text{ms}$  is needed for sensing 8 continuous 8-chip PN sequences. For this sensing scenario, only chip sequences from the initialization period are considered.

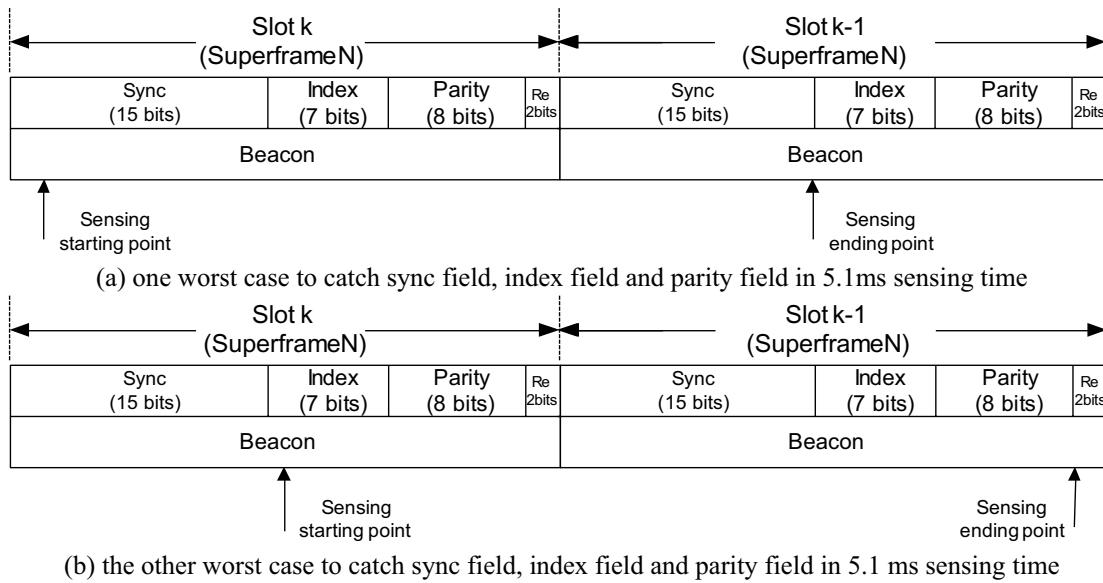
#### D.8.2.3 Sensing Type 3

The 2.8107 ms sensing time is obtained by adding the duration of 8 PN spreading sequences to the maximum time without transmission that could occur within an inter-device communication period, which corresponds to the absence of transmission of RTS sequence surrounded by two turnaround times for a total duration of 19 symbols ( $(8+19) \times 0.1041=2.8107\text{ ms}$ ).

#### D.8.2.4 Sensing Type 4

The 5.1 ms sensing time for the sync burst within the beacon device initialization period can be achieved by capturing 5.1 ms of signal, demodulating the DQPSK symbols to obtain hard bit decisions, and then looking for the 15-bit synchronization sequence. Once the position of that sequence has been determined, the receiver looks before or after that sequence, in order to identify the uncoded and parity bits of the index. The index bits and parity bits must be consecutive, whereas the synchronization can be obtained when the synchronization sequence is located before or after the index and parity bits.

Figure D.7 shows both worst cases for the receiver to detect sync burst and index within 5.1ms sensing time.



**Figure D.7—Worst cases for synchronization within the initialization period**

In both Figure D.7 (a) and Figure D.7 (b), 46 DQPSK symbols need to be detected after de-spreading for getting the sync burst, the index and parity bits. Additionally, one more symbol shall be received for demodulating differential QPSK symbols. Therefore, at least 47 DQPSK symbols shall be received within the sensing window. The filters with roll-off factor shall be taken into further consideration for getting the whole 47 DQPSK symbols. In total, a sensing window with 49 symbols should be properly designed for receiving 47 DQPSK symbols for safety, which is equal to 5.099 ms ( $49/9.6091 = 5.099$  ms).

In both worst cases shown in Figure D.7 (a) and Figure D.7 (b), after DQPSK demodulation, hard decision bits shall be synchronized with the 15-bit synchronization sequence to detect one sync burst successfully. For the first worst scenario in Figure D.7 (a), the sync field is first detected in slot k-1, then the index field and parity field in slot k will be detected after synchronization. Therefore, index k should be decoded without errors while k-1 will be presented as current index number. For the second worst scenario in Figure D.7 (b), the sync field is detected firstly in slot k-1, then the index field and parity field will be detected in the same slot after synchronization. Therefore, index k-1 should be decoded without errors and thus k-1 will be regarded as the current index number.

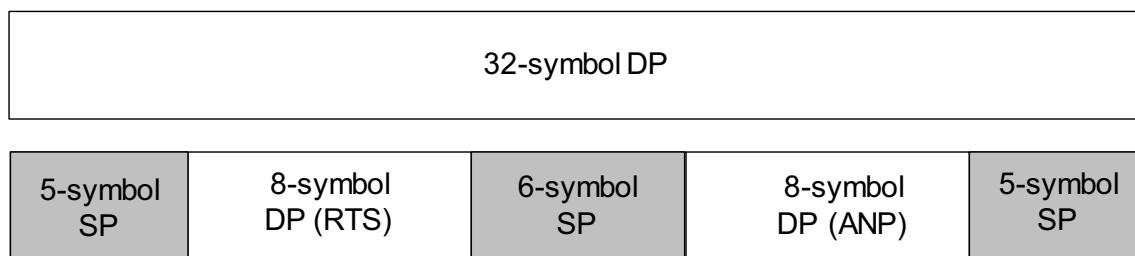
For cases other than the two worst cases described above, after synchronization with the 15-bit synchronization sequence, the position of the 15-bit sync field in 5.1 ms sensing window will be decided before decoding the index field and parity field, so that the current index number will be the one generated.

### D.8.2.5 Sensing Type 5

Synchronization information is obtained by decoding the index, or by obtaining non-ambiguous information about the type of slots contained in the signal captured during the sensing period. A cognitive radio could easily conclude that an inter-device communication period has been sensed rather than a sync burst slot, due to the structure of the inter-device communication period, which contains periods of signal and periods of silence of precise durations. In this case, there can be no doubt that the last slot of a superframe is contained within the sensed signal, and therefore the WRAN can acquire synchronization information as if it had decoded the index in a regular sync burst slot. The assumption in the notations of

Figure D.5 is that the index retained by the receiver corresponds to the most recent slot present in the sensed signal. With this additional cognition, the WRAN only needs 5.1 ms of quiet sensing time to obtain the synchronization information, whether the captured signal contains a sync burst or whether an inter-device communication period falls within the captured signal. A simple comparator with threshold detection is sufficient for this additional cognition.

According to Figure D.5, the slot type will be decided after one 49-symbol DQPSK sequence is acquired by PN spreading sequence detection. Because of the special character with inter-device communication period (slot 0), the 49-symbol sequence will show obvious difference from other normal slots (slot 1 to slot 30). From the inter-device communication period structure, it can be seen that the whole slot 0 is separated into five parts: 5 symbols of turnaround time 1, 8 symbols of RTS, 6 symbols of turnaround time 2, 8 symbols of ANP and 5 symbols of turnaround time 3 as shown in Figure D.8. If there is a whole or partial inter-device communication period involved in the 49-symbol DQPSK sequence, at least one silence symbol shall be detected within the sequence.



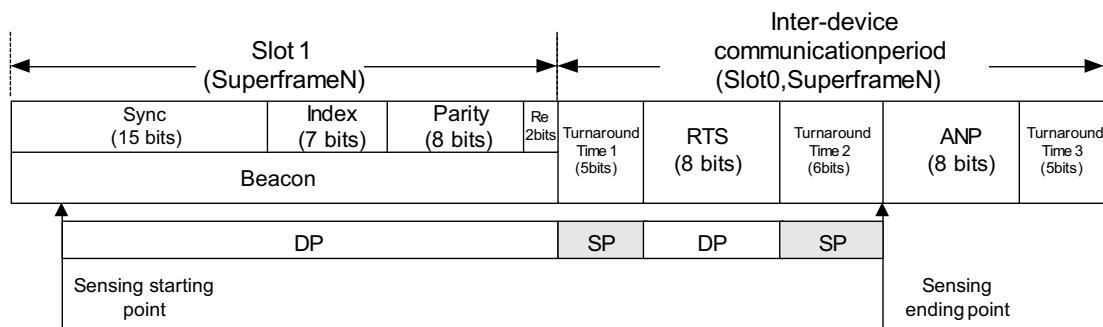
**Figure D.8— Data and silence periods in IEEE 802.22.1 slots**  
(DP: data period; SP: silence period)

Figure D.7 displays an example of a map of a detected DQPSK sequence for both a normal slot 1 to 20 and a special inter-device communication period (slot 0). In the DQPSK sequence obtained after detection with the PN spreading sequence, if a continuous data period with length larger than 32 symbols is observed, the slot type for the corresponding sensing window will be a normal slot; otherwise the slot type for the sensing window will be the special inter-device communication period. In this case, the 49-symbol DQPSK sequence might include continuous data period (DP) with length shorter than 32 symbols and at least one silence period (SP).

In the following paragraphs, we list all the possibilities that exist with inter-device communication period (slot 0) involved in the 5.1009 ms sensing window.

#### *1) Partial or whole inter-device communication period (slot 0) of superframe N at the end of sensing window*

In this case, the length of a continuous series of DP symbols is smaller than 32, thus a partial or whole inter-device communication period (slot 0) will be present at the end of the 49-symbol sequence. Figure D.9 shows an example of this scenario.



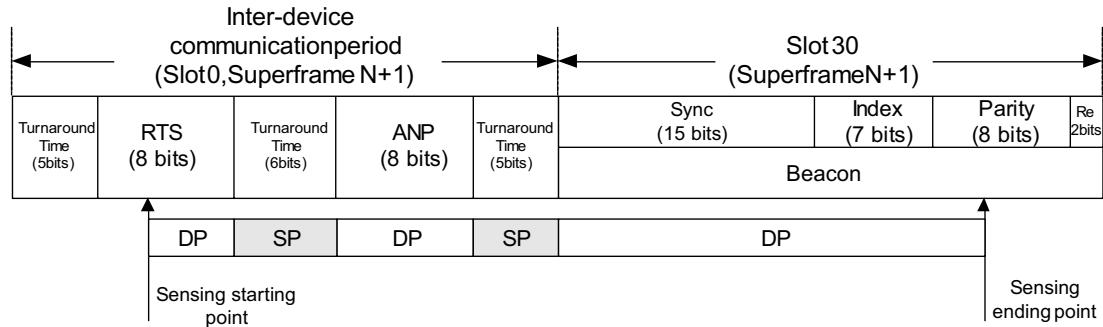
**Figure D.9—Example of data period and silence period distribution with slot 0 at the end of the sensing window**

The 49-symbol DQPSK sequence starts from the third symbol of Slot 1 in beacon superframe N and ends by Turnaround Time 2 in Superframe N. After detection by the PN spreading sequence, if the WRAN receiver gets a 49-symbol sequence with 30-symbol continuous DP followed by a 5-symbol SP, 8-symbol DP and another 6-symbol SP, timing analysis will decide that the present sensing window ends at the 19th symbol of Slot 0 in Superframe N. Therefore, the timing analysis will know that the next superframe will begin after receiving another 13 symbols (8-symbol DP and 5-symbol Turnaround time 3).

**2) Partial or whole inter-device communication period (slot 0) of superframe N at the beginning of the sensing window**

In this case, the length of the continuous DP symbols is also smaller than 32, thus a partial or whole inter-device communication period (slot 0) will be present at the beginning of the 49-symbol sequence.

Figure D.10 shows an example of this scenario.

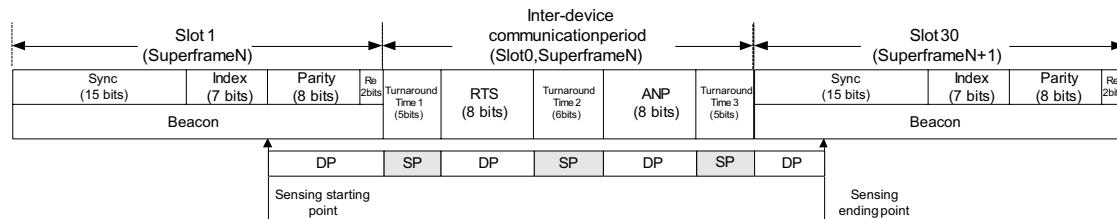


**Figure D.10—Example of data period and silence period distribution with slot 0 at the beginning of sensing window**

The 49-symbol DQPSK sequence starts from the third symbol of the RTS period in beacon superframe N and ends by the 3rd symbol of Parity field in slot 30 of Superframe N+1. After detection by the PN spreading sequence, if the WRAN receiver gets a 49-symbol sequence with a 5-symbol continuous DP followed by a 6-symbol SP, 8-symbol DP, another 5-symbol SP and 25-symbol continuous DP, timing analysis will decide that the present sensing window ends at the 25th symbol of Slot 30 in Superframe N+1. Therefore, the timing analysis will know that slot 29 of superframe N+1 will begin after receiving another 7 symbols (5 symbols in parity field and 2 symbols in reserved field will be included).

### 3) Whole inter-device communication period (slot 0) in the middle of the sensing window

In this case, a whole inter-device communication period (slot 0) will be present in the middle of the 49-symbol DQPSK sequence with several symbols of DP from slot 1 of Superframe N and slot 30 of Superframe N+1 at both the end and the beginning. Figure D.11 shows an example of this scenario.



**Figure D.11—Example of data period and silence period distribution with slot 0 in the middle of the sensing window**

The 49-symbol DQPSK sequence starts from the 1st symbol of the parity field in slot 1 of the beacon superframe N and ends by the 7th symbol of the Sync field in slot 30 of superframe N+1. After detection by the PN spreading sequence, if the WRAN receiver gets a 49-symbol sequence with a 10-symbol continuous DP followed by a 5-symbol SP, 8-symbol DP, 6-symbol SP, 8-symbol DP, 5-symbol SP and another 7-symbol continuous DP, timing analysis will decide that the present sensing window ends at the 7th symbol of Slot 30 in Superframe N+1. Therefore, the timing analysis will know that slot 29 of superframe N+1 will begin after receiving another 25 symbols (10 symbols in sync field, 7 symbols in index field, 8 symbols in parity field and 2 symbols in reserved field will be included).

### 4) No data is transmitted by SPD in RTS period

One special scenario should be reminded here with no data transmitted by the SPD in the RTS period. In this case, a simplified map of the detected DQPSK sequence for the inter-device communication period is redrawn in Figure D.12.



**Figure D.12—Detected DQPSK sequence in inter-device communication period with no data transmission in the RTS period**

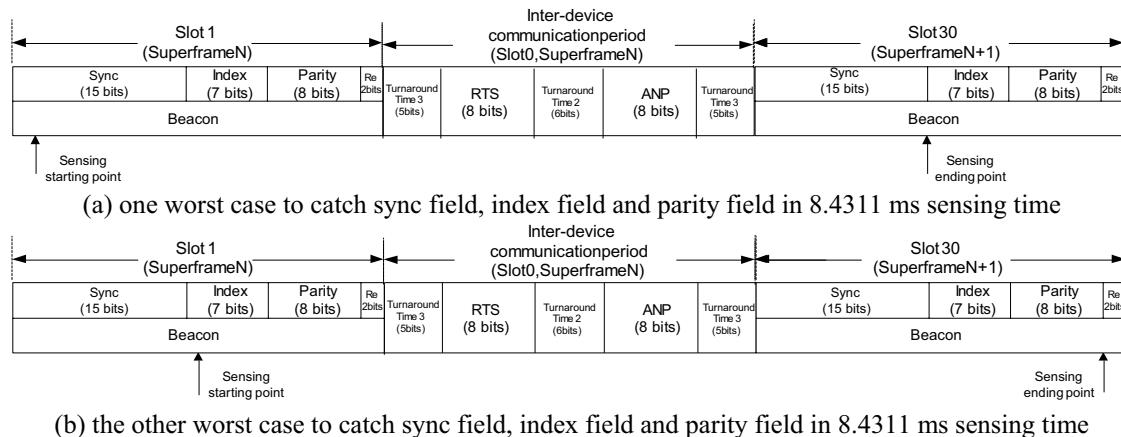
#### D.8.2.6 Sensing Type 6

If the signal in the 5.1 ms sensing window which contains an inter-device communication period can not be recognized by a WRAN receiver that is not equipped with the detection method described in D.8.2.5, then the 5.1 ms sensing window might need to be used twice for capturing the sync burst and index information outside the initialization period.

#### D.8.2.7 Sensing Type 7

If the inter-device communication period can not be recognized by the WRAN receiver with the method in D.8.2.5, a longer sensing window of 8.4311 ms will be needed rather than two 5.1 ms sensing windows described in D.8.2.6. In Figure D.13, two worst cases are listed to show that 8.4311 ms will be the minimum sensing time for these cases. As is shown in D.8.2.4 and both Figure D.7(a) and Figure D.7(b), if all continuous slots in sensing windows are captured from normal slots, it will take at least 5.1009 ms for sensing a sync burst and the index number. Since there is a special ICP period between two normal slots,

one more slot of duration 3.3302 ms will be needed in the calculation of the minimum sensing time, resulting in  $5.1009\text{ ms} + 3.3302\text{ ms} = 8.4311\text{ ms}$ .



**Figure D.13—Worst cases for synchronization outside the initialization period**

#### D.8.2.8 Sensing Type 8

MSF1 has a duration of 28.3070 ms, so the minimum sensing time for MSF1 is 28.4111 ms, including an additional DQPSK symbol involved for differential demodulation.

#### D.8.2.9 Sensing Type 9

MSF1+MSF2 has a duration of 70.7676 ms, so the minimum sensing time for MSF2 is 29.2437 ms, including an additional DQPSK symbol involved for differential demodulation.

#### D.8.2.10 Sensing Type 10

MSF1+MSF2+MSF3 has a duration of 98.2421 ms, so the minimum sensing time for MSF1+MSF2+MSF3 is 98.3462 ms, including an additional DQPSK symbol involved for differential demodulation.

### D.8.3 Sensing times

The WRAN and IEEE 802.22.1 frames are not synchronized, even after the WRAN has acquired timing information for the IEEE 802.22.1 superframe. The WRAN receiver needs to synchronize to the IEEE 802.22.1 frame, but this will not change the timing of the WRAN transmissions. Once the WRAN receiver has determined the start of the next IEEE 802.22.1 frame, it needs to wait for a certain amount of time, referred to as latency.

The IEEE 802.22.1 beacon was designed so that the required quiet period duration is smaller than one WRAN superframe, so the WRAN does not need to interrupt the superframe preamble in order to schedule a quiet period, but it needs to wait until the desired part of the beacon frame does not interrupt the superframe preamble.

According to the sensing timing parameters defined in D.8.2, the WRAN would need to capture

- 3.3302ms sync burst within 5.1ms short quiet period
- 29.1396ms MSF1+FEC of MSF1
- 70.7676ms MSF1+FEC of MSF1 + MSF2

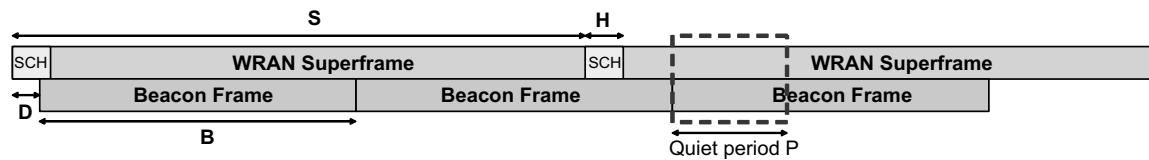
- 98.2421ms MSF1+FEC of MSF1 + MSF2+MSF3

After a 5.1 ms short quiet period, the WRAN receiver can successfully schedule a quiet period to capture each beacon frame with the minimum sensing duration. Therefore, once the WRAN receiver has determined the start of the next IEEE 802.22.1 frame, it needs to wait for a latency T.

0 shows the scheduling of a quiet period synchronized with the IEEE 802.22.1 beacon frame after the WRAN receiver has captured a sync burst and index number. The WRAN superframe length is 160 ms, and the WRAN frame length is 10 ms. At the beginning of each superframe, the first symbol shall be the superframe preamble, followed by a frame preamble symbol. The third symbol shall be the SCH. Therefore, the SCH is taken into account in the analysis so that the beacon can be captured in its entirety without interrupting the SCH.

As shown in Figure D.14,

- P is the quiet period (see Table D.3)
- S is the WRAN superframe period;
- H is defined as the length of the beginning of each superframe that can not be interrupted by a quiet period, which at least includes the first three OFDM symbols (2 ms is suggested here to be safe);
- B is the length of the beacon frame;
- D is the beacon frame offset, which is defined as the time offset between the beginning of the first beacon frame and the beginning of the current WRAN superframe after sync burst and index capture.



**Figure D.14—Scheduling of a quiet period synchronized with the IEEE 802.22.1 beacon frame**

If  $D+P < S$ , the quiet period could be scheduled in the current superframe (it is assumed that  $B < S$ , which is the case with the parameters of the WRAN and beacon signals). Otherwise the minimum number of superframes to wait for before scheduling a quiet period of length P is:

$$\arg \min_m \left\{ (m+1)S - \left( B \left\lceil \frac{mS + H - D}{B} \right\rceil + D + P \right) \geq 0 \right\}$$

Table D.3 gives a list of the typical values for latency with different quiet period durations P. Here, quiet periods of duration 29.1396 ms, 70.7676 ms and 98.2421 ms are considered for detecting MSF1, MSF1+MSF2 and MSF1+MSF2+MSF3 respectively. In the table, H is set as 2 ms. In addition, the maximum number of quiet frames at the end of a superframe is 16 frames ( $160 - 2 = 158$  ms), which means that the quiet period can be scheduled to start at any time and end at any time within a superframe, except during the H period, which includes a superframe preamble, a frame preamble, and the SCH.

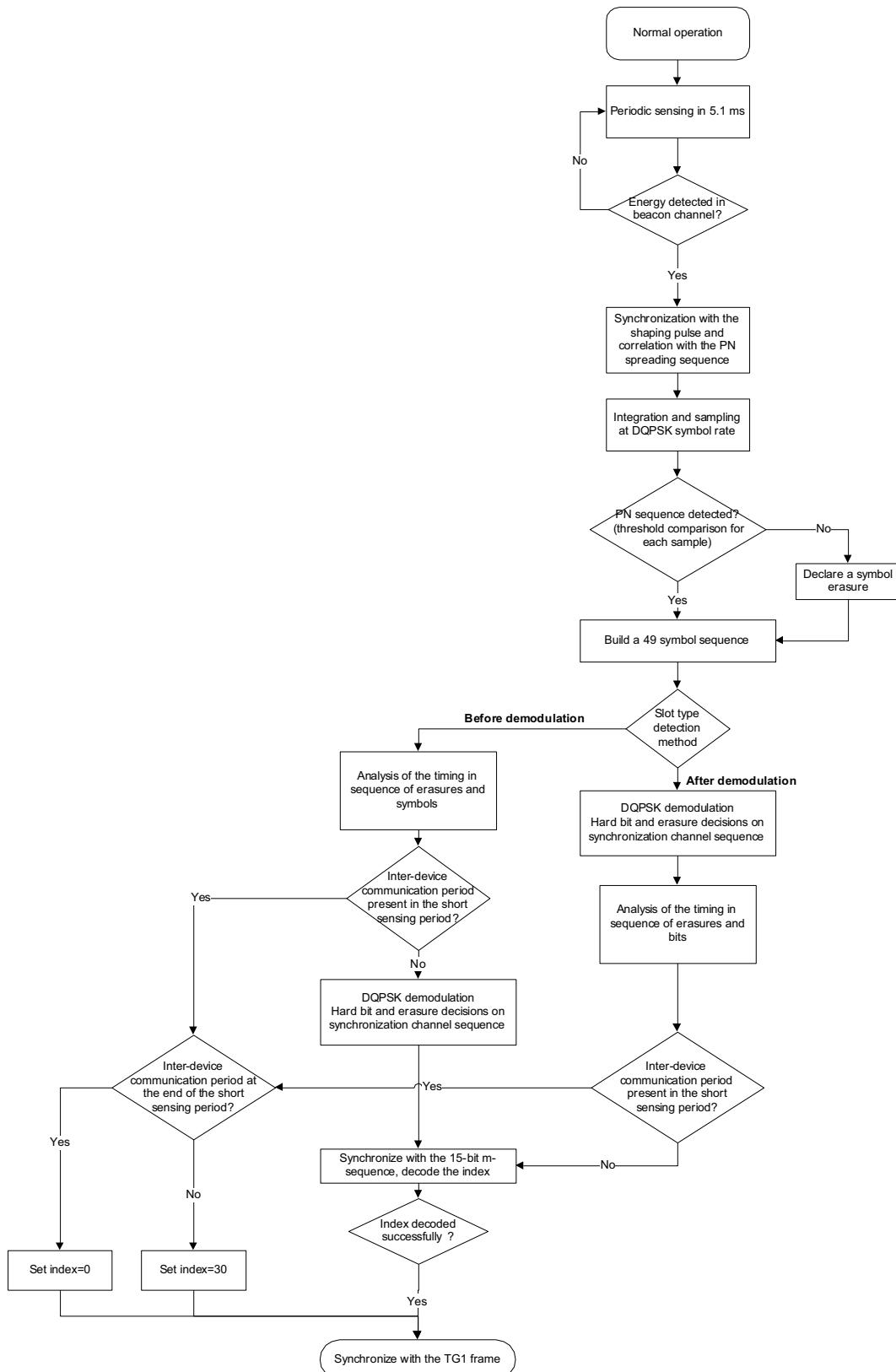
**Table D.3—Latency with different quiet period values (P)**

<b>Length of required quiet period</b>	29.1396 ms (MSF1)	71.600160 ms (MSF1+MSF2)	98.2421 ms (MSF1+MSF2+MSF3)
<b>Mean latency before scheduling a long period</b>	32 ms (<1 superframe)	88 ms (<1 superframe)	145 ms (<1 superframe)
<b>Max latency before scheduling a long period</b>	160 ms (1 superframe)	320 ms (2 superframes)	320 ms (2 superframes)

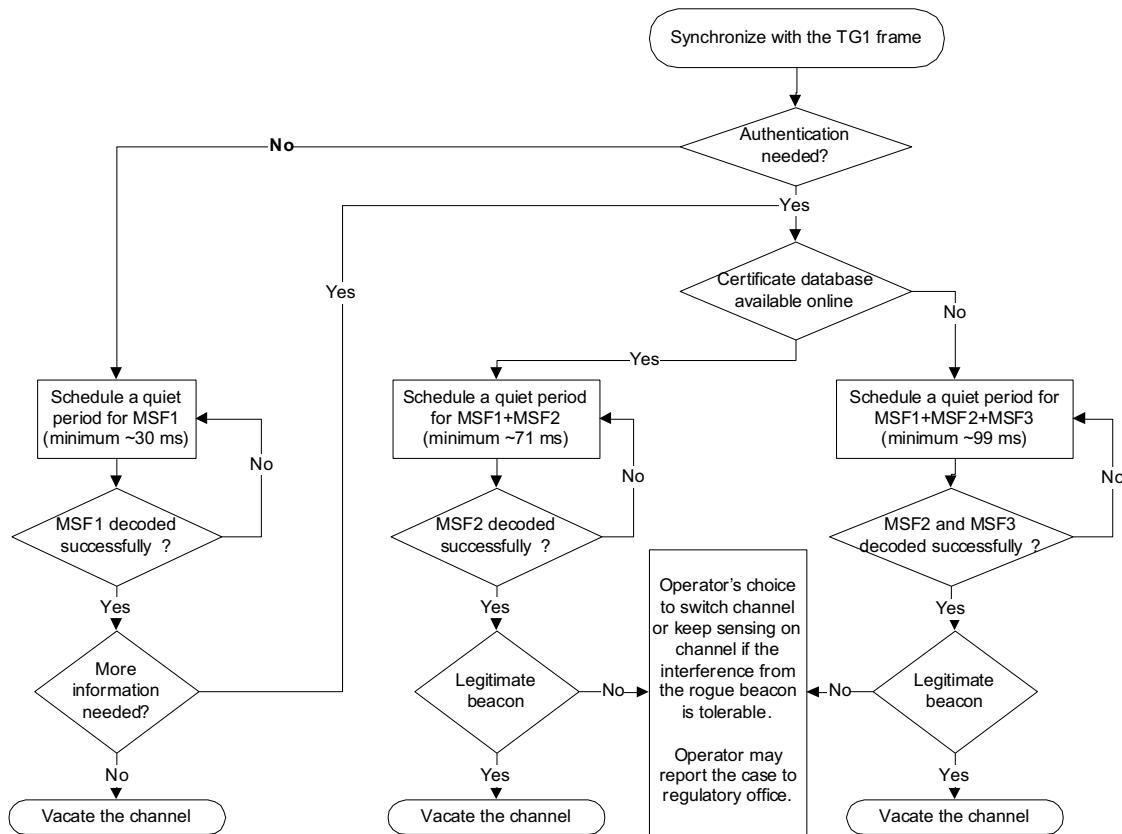
## D.9 Options for detecting the IEEE 802.22.1 beacon signal

### D.9.1 Decision Options

The following flow chart describes the complete path and options for detecting the various states of the IEEE 802.22.1 beacon signal. Figure D.15 shows the decision flowchart during a short sensing period. Figure D.16 shows the decision flowchart after synchronization with the IEEE 802.22.1 beacon frame.



**Figure D.15—Decision flowchart during a short sensing period**



**Figure D.16—Decision flowchart after synchronization with the IEEE 802.22.1 beacon frame**

## D.9.2 Tradeoffs

The various sensitivity thresholds indicated in D.8.1 and depicted in Figure D.6 can be improved upon if more sensing time can be afforded. For example, doubling the number of sensing periods in case longer integration time can be used may improve the sensing threshold by 3 dB. This is especially true for the basic energy detection that is illustrated by one of the dotted lines depicted in Figure D.6. This dotted line has a slope of 10 dB per decade. In the case of the other dotted line that represents the variation of the sensing threshold for energy detection when correlation is achieved with the spread PN-sequence. The slope is 5 dB per decade which provides a slower increase in sensing threshold for smaller sensing periods than would be afforded by simple energy detection.

## D.10 Operation scenarios for the coexistence of IEEE 802.22.1 and IEEE 802.22

### D.10.1 Decision Options

This subclause summarizes the various coexistence scenarios investigated.

- The WRAN is operating on TV channel N and a beacon comes up on TV channel N.
- The WRAN is operating on TV channel N and a beacon comes up on TV channel N+1 or N-1.

- The WRAN is operating on TV channel N and a beacon comes up one of its backup TV channels K.
- The WRAN is operating on TV channel N and a beacon comes up on a channel adjacent to the backup TV channel K+1 or K-1.
- The WRAN comes up and starts monitoring a TV channel that may have been used by a beacon. The WRAN will need to verify if it is still being used. The channel availability time will need to be met before the WRAN can move to this channel.
- The WRAN starts sensing a channel that it has not sensed for a long time (e.g., that channel was just added to the list of potential available channels). Sensing will need to take place during the channel availability time before allowing the WRAN to declare this channel available. Any detection of at least one IEEE 802.22.1 beacon will result in the channel not being available at that time.
- A beacon comes up when the WRAN has finished its channel monitoring time. A refresh period of 2 seconds applies.
- During a CPE power up initialization sequence, the CPE will need to use a number of quiet periods to clear the channel that it is to use (N), its adjacent channels (N+1 and N-1) and each of its backup channels (K, K+1, and K-1), in each case clearing the channel during the entire channel availability time.

The list of relevant scenarios will likely be augmented with more thorough analysis. Clause 10 of the main standard on the SM is to cover all these possible scenarios.

#### **D.10.2 Sensing and detection strategies**

The description of the different sensing scenarios for the IEEE 802.22.1 beacon and the resulting strategies for WRAN systems to avoid interference into wireless microphone operation is contained in Clause 10 of the main standard.

### **D.11 References**

- [1] IEEE Std 802.22.1-2010, Part 22.1: Enhanced Protection for Low-Power, Licensed Devices Operating in Television Broadcast Bands, November 2010.
- [2] Yuchun Wu computer simulations on TG1 beacon performance, March 2008:  
22-08-0042-01-0001\_Simulation Results for TG1 according to Draft 2.01.ppt
- [3] Steve Kuffner computer simulations on TG1 beacon performance, March 2008:  
22-08-0104-00-0001-tg1-per-in-awgn-and-wran-b.ppt
- [4] Gerald Chouinard spreadsheet on TG1 beacon analysis, February 2009:  
22-08-0040-01-0000-WRAN and TG1 Beacon link analysis.xls

## Annex E

(informative)

### Distributed spectrum sensing and authentication to provide protection against thermal noise

Let

$H_0$ : Hypothesis such that the incumbent *is not* occupying the channel being sensed  
 $H_1$ : Hypothesis such that the incumbent *is* occupying the channel being sensed

Let  $x(n)$  be the received signal at the input of the SSF, where n is the running index of the samples

$$x(n) = \begin{cases} w(n) & \rightarrow H_0 \\ s(n) + w(n) & \rightarrow H_1 \end{cases} \quad (\text{E1})$$

where  $s(n)$  is the *authentic incumbent signal*, and  $w(n)$  is the noise. Hence the goal of the SSF is to decide between hypotheses  $H_0$  and  $H_1$ .

Let  $y(n)$  be the decision statistic, and  $\lambda$  be some threshold used to choose between the Hypotheses  $H_0$  and  $H_1$  respectively. Then the detection probability ( $P_d$ ) and the false alarm probability ( $P_f$ ) can be denoted by

$$\begin{aligned} P_d &= P(y > \lambda | H_1) \\ P_f &= P(y > \lambda | H_0) \end{aligned} \quad (\text{E2})$$

Consider a group of  $N$  localized sensors, monitoring a specific area, collaboratively trying to distinguish between Hypotheses  $H_0$  and  $H_1$ . If the group collectively decides that the incumbent signal is detected when the detection statistic at, *at least one* of the sensors exceeds the threshold, then the sensors are said to follow the *OR* rule of the collaborative sensing. Under these circumstances, the network detection and false alarm probabilities are denoted by  $Q_d$  and  $Q_f$  respectively, and given by

$$\begin{aligned} Q_d^{OR} &= 1 - (1 - P_d)^N \\ Q_f^{OR} &= 1 - (1 - P_f)^N \end{aligned} \quad (\text{E3})$$

Under the *OR* rule of collaborative sensing, the net detection as well as false alarm probabilities increase.

However, consider another signal  $c(n)$ , which statistically looks similar to the authentic signal  $s(n)$ , such that, when transmitted, it may result in false detection of the signal  $s(n)$ . Assume that  $c(n)$  is *being transmitted at a lower power than  $s(n)$  and hence, will be detected by  $L$  sensors where ( $L < N$ )*. Let  $P_C$  be the probability that  $c(n)$  is transmitted (ON) at a particular instant of time. If the *OR* rule of the collaborative sensing is followed, then the probability of detection of an *authentic incumbent signal* is give by

$$Q_d^{C,OR} = P_C + (1 - P_C) \left( 1 - (1 - P_d)^N \right) = 1 - (1 - P_C)(1 - P_d)^N \quad (\text{E4})$$

and the false alarm probability = probability that Hypothesis  $H_1$  is selected when  $H_0$  is true is given similarly by

$$Q_f^{C,OR} = 1 - (1 - P_C)(1 - P_f)^N . \quad (\text{E5})$$

This means that if the other signal is present along with the true signal, it helps detection. For instance, if  $c(n)$  is ON all the time (that is  $P_C = 1$ ), then,  $Q_d^{C,OR} = Q_f^{C,OR} = 1$ , which means that a particular channel always appears to be occupied, whether or not an authentic incumbent signal is present. If  $c(n)$  is OFF all the times then  $Q_d^{C,OR} = (1 - (1 - P_d)^N)$  and probability of authentic incumbent detection is the same as in E.3. Note that the false alarm probability increases with an increasing value of  $P_C$ .

Now consider a case where instead of the *OR* rule of collaborative sensing, the *AND* rule is followed. Under these circumstances, the incumbent signal is said to be detected *if and ONLY if* all the  $N$  localized sensors detect the signal. In *absence of*  $c(n)$ , the detection and false alarm probabilities are given by

$$\begin{aligned} Q_d^{AND} &= (P_d)^N \\ Q_f^{AND} &= (P_f)^N \end{aligned} \quad (\text{E6})$$

which means that both, the detection as well as the false alarm probabilities, decrease with increasing  $N$ .

Let  $P_C$  be the probability that  $c(n)$  is transmitted at a particular instant of time and some  $L < N$  sensors are able to detect it. If the *AND* rule of the collaborative sensing is followed, then the probability that an *authentic* incumbent signal is detected is given by

$$Q_d^{C,AND} = (P_d)^{N-L} \quad (\text{E7})$$

which means that even in presence of a false signal  $c(n)$ , the probability that an authentic incumbent signal is detected increases, but is not automatic. Similarly, the false alarm probability = probability that Hypothesis  $H_1$  is selected when  $H_0$  is true, and is given by

$$Q_f^{C,AND} = (P_f)^{N-L} \quad (\text{E8})$$

As an example, let  $P_d = 0.9$ , let  $P_f = 0.1$ , let  $N = 2$ ,  $L = 1$ , and  $P_C = 0.5$ , then

$P_d = 0.9$	$Q_d^{OR} = 0.99$	$Q_d^{C,OR} = 0.995$	$Q_d^{AND} = 0.81$	$Q_d^{C,AND} = 0.9$
$P_f = 0.1$	$Q_f^{OR} = 0.19$	$Q_f^{C,OR} = 0.595$	$Q_f^{AND} = 0.01$	$Q_f^{C,AND} = 0.1$

Rather than using simple *OR* or *AND* based decision making, it makes sense to use some form of a *VOTING based rule* for decision making which provides a finer granularity, flexibility, and protection against low powered signals  $c(n)$  that may have statistical properties that are similar to  $s(n)$  – the signal of interest.

Given  $N$  collaborative detectors, let  $k$  be the number of these radios that detect a transmitter present in a band. To decide when we declare a transmitter present, we define the collaborative sensing voting rule. The rule has one parameter, the voting threshold  $T$ , a number between 0 and 1. It can be expressed as a percentage, e.g.,  $T = 0.5$  is a threshold of 50%.

The rule is that we declare the signal  $s(n)$  to be present if  $d \geq TN$  nodes detect its presence.

To evaluate the rule, suppose that all detectors can detect the signal of interest  $s(n)$  with probability  $P_d$ , independent of each other. Then the probability of  $k$  successes from  $N$  transmitters is given by the binomial distribution,

$$B(k, N; P_d) = \frac{N!}{k!(N-k)!} (P_d)^k (1-P_d)^{N-k} \quad (\text{E9})$$

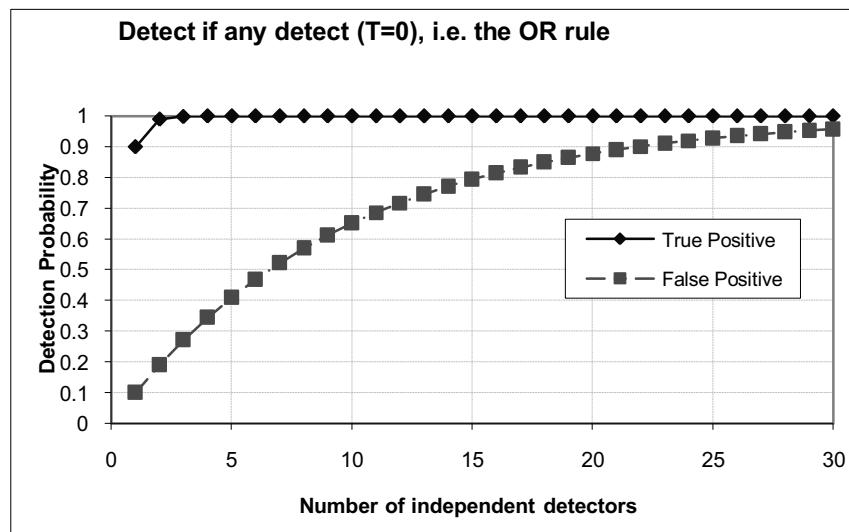
The probability the voting rule declares that the signal of interest  $s(n)$  is present if

$$Q_D^{\text{collaborative}} = \sum_{k \geq TN}^N B(k, N; P_d) \quad (\text{E.10})$$

The probability of the rule declaring no transmitter present is  $1 - Q_D^{\text{collaborative}}$ .

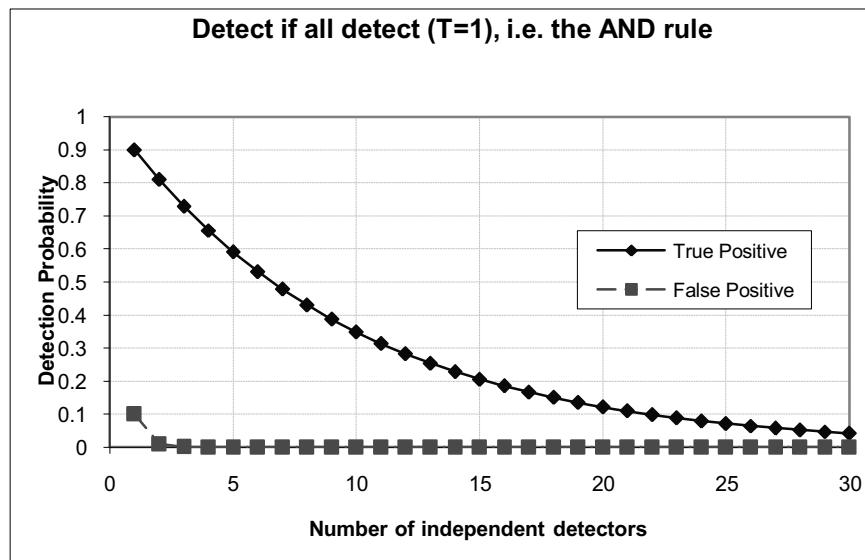
Under this formulation, the *AND* rule that everyone must detect to declare a transmitter present is  $T = 1$ . The *OR* rule that if anyone detects we declare a transmitter present is  $0 < T \leq 1/N$ .

If a transmitter is actually present, then  $Q_D$  represents the true detection rate and  $1 - Q_D$  represents the missed detection rate. If a transmitter is not present then  $Q_D$  represents the false positive rate and  $1 - Q_D$  represents the true negative rate.



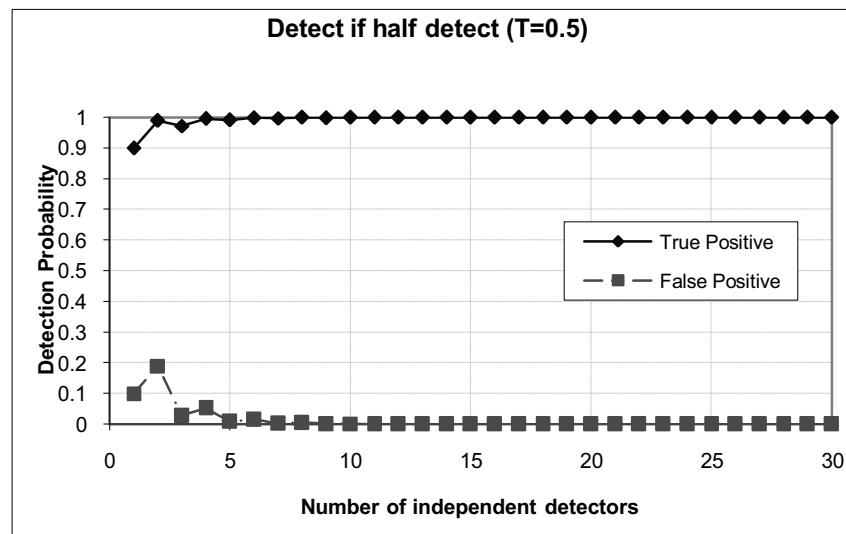
**Figure E.1—OR Rule of Collaborative Sensing and Signal Detection**

Figure E.1 shows the true positive and false positive detection probability curves as a function of the number of independent signal detectors for the *OR* rule of collaborative sensing with  $P_d = 0.9$  and  $P_f = 0.1$ . Simulations assume the sensors are independent. It can be seen that with the *OR* rule, false positives increase with the number of detectors. Hence, the *OR* rule of collaborative sensing fails to provide robust detection of the signal of interest.



**Figure E.2—AND rule of collaborative sensing and signal detection**

Figure E.2 shows the true positive and false positive detection probability curves as a function of the number of independent signal detectors for the *AND* rule of collaborative sensing. It can be seen that the *AND* rule performs much better than the *OR* rule for false positives, however, the true positive performance suffers as the number of independent observations from the detectors increases. Hence once again the *AND* rule of collaborative sensing fails to provide robust detection of the signal of interest  $s(n)$ .



**Figure E.3—Voting based Rule of Collaborative Sensing and Signal Detection where the signal is said to be detected if half the number of sensors detect the signal**

Finally, Figure E.3 shows the true positive and false positive detection probability curves as a function of the number of independent signal detectors for the *VOTING based* rule of collaborative sensing with voting threshold set to 0.5: that is half the number of independent detectors ( $N/2$ ) must confirm the presence of the signal. It can be seen that the *VOTING based* rule performs much better than the *OR* as well as the *AND* rules for true positives as well as the false positives. Probability of detection for true and false positives reaches an optimal value with observations from around 6 sensors.

The voting rule can also perform well in the presence of a false signal,  $c(n)$ , that affects a limited number,  $L$ , of detectors. As the number of independent detectors increases, these  $L$  detectors will be overruled by the detection from other sensors.

Hence collaborative sensing with information fusion and decision making based on a VOTING rule can help in enhancing the network detection performance of the true signal  $s(n)$  in presence of a false signal  $c(n)$ . Based on the simulations results, information fusion and decision making from approximately 6 to 10 independent sensors is likely to be sufficient to obtain satisfactory performance results.

#### Correlation of the voting results with the geographical location of the sensing CPEs

Collaborative sensing takes all its strength when the information fusion described above takes into account the knowledge on the geographic location of the specific sensing devices providing sensing reports. The correlation of the reports of the sensing devices that will have sent an urgent coexistence situation (UCS) message to the base station and their respective geographic location that is, by definition, known at the base station from the time of their registration on the network will provide powerful means to identify the characteristics of the sensed signal and help improve the decision making as to the presence of an incumbent and its type versus presence of other devices based on their expected extent of coverage.

In the case of DTV detection, the area where correlation will exist between sensing devices will be large and will be in the direction of the DTV transmitter. In the case of a wireless microphone, the correlation will exist over a more limited area. This limited area correlation will also be used in the case of the detection of an IEEE 802.22.1 beacon and will help increasing the level of confidence of the decision that it is indeed an IEEE 802.22.1 beacon based on its expected area of coverage, and possibly reducing the need to rely on the full PPDU decoding.

Since all the information will be available at the base station, it will be up to the manufacturers to implement various levels of complexity in fusing the sensing reports and the geographic location of the sensing devices to come up with a reliable assessment of the presence of incumbents, that is true positives, while minimizing the probability of false positives. Artificial intelligence algorithms could be taken advantage of to improve this data fusion and decision process. Since incumbents will need to be protected in all cases and in case of doubt, action will need to be taken to avoid interference to incumbents, more advanced data fusion and decision processes will have the advantage of avoiding false positives and false alarms and therefore reducing cases where WRAN systems would have to change frequency while it is not necessary.

## Annex F

(informative)

### Network security aspects

This annex describes some of the basic network security functions applicable to the IEEE 802.22 WRAN systems and the remediation measures required to protect these functions for these systems.

#### F.1 Availability

This is the primary function of any network. If there is a perception, real or not, that a particular type of network is unreliable due to service or security issues then that network type will not be utilized by WRAN operators or end-users. In the case of cognitive networks availability refers to ability of the BSs to properly sense the available spectrum and make it available to the CPEs. This means that the BSs must have built-in security mechanisms that shall

- Provide for the availability of the spectrum for the primary (incumbents) and the secondary (WRAN) users.
- Mitigate any *DoS-type* attacks against BS, CPE, and other supporting devices such as the ones used to generate IEEE 802.22.1 beacons.

The details of various types of sensing and classification mechanisms have been provided in Clause 10, and the details for IEEE 802.22.1 beacon authentication has been described in 8.6.3.

#### F.2 Authentication

This functionality provides assurance that the communicating parties, sender and receiver, are who they purport to be. In cognitive networks there is the added problem of distinguishing between the valid incumbents of the spectrum and the secondary users. WRAN operators must be able to

- Validate incumbent TV signals and the wireless microphone beacons.
- Detect and counter *man-in-the-middle* and similar type attacks that attempt to steal available spectrum space.
- Detect and counter any *spoofing* and similar type attacks.
- Authenticate geolocation information.
- Authenticate co-existence information of neighboring WRAN systems.
- Detection and reporting of spurious transmissions from other CPEs.

The details on spectrum sensing and signal classification have been provided in Clause 10, 8.6.2 describes mechanisms to authenticate the Co-existence Beacons Protocol (CBP) used to exchange the co-existence information and 8.6.3 describes mechanisms to authenticate the IEEE 802.22.1 wireless microphone beacons. Authentication of the geolocation information will be described in the Management Plane Procedures Addendum at a future date.

### F.3 Authorization

Different network entities will have different privilege levels. For example, a BS may be authorized to forcibly remove an interfering CPE from the network. In cognitive networks the ability of the BS SM to sense the available spectrum, make decisions regarding its use and enforce those decisions at the CPE level is an important authorization example. For a cognitive network to properly function

- Only the authorized parties shall be allowed to configure the SM at the BS and the spectrum automaton at the CPE
- Configuration information shall be identified and protected
- The BS shall be authorized to remove a CPE from the network if it was found to cause interference to the incumbents

The authorization process is briefly described in 8.2. The BS has the ability at any time to de-authorize a CPE from its network. The mechanism on how this decision is made is described in Clause 9, related to the Cognitive Radio Capabilities through various policy sets. The mechanisms for protecting configuration information will be described in the Management Plane Procedures Addendum at a future date.

### F.4 Identification

Identification works hand-in-hand with authentication in assuring both incumbent and secondary spectrum users that the communicating entities are known. To that end it is necessary that cognitive networks provide mechanisms that shall

- Positively identify transmitting/receiving BS and CPE equipment.
- Avoid that the identification methods employed cannot be compromised through *spoofing* or similar type attacks.
- Protect against *replay*-type attacks that employ previously transmitted valid identifiers.

The MAC information elements to identify the transmitting receiving BS and CPE equipment are defined in Clause 7. The security mechanisms providing for identification and integrity have been described in 8.4 and 8.5.

### F.5 Integrity

Integrity is the assurance that the information transmitted over the medium arrives at its destination unaltered. Integrity provides write protection for the content. This is especially difficult in wireless networks because of the uncontrolled nature of the medium. Also the fact that certain portions of the data must be altered to provide proper transmission and delivery (timestamps, source, destination etc.) compounds the problem. Cognitive networks must

- Protect against Co-Existence Beaconing (“CBP”) falsification
- Protect against *replay*-type attacks using previously transmitted valid data

The security mechanisms to authenticate and perform integrity check on the CBP packets are described in 8.6.2. The security mechanisms to provide some degree of protection against *replay*-type attacks have been provided in 8.4.

## F.6 Confidentiality/Privacy

Confidentiality works closely with integrity to provide read as well as write protection for data. This is usually carried out using encryption and ciphers that can operate at the link and higher layers. One must account for the fact that the wireless medium is more sensitive to transmission errors due to propagation effects such as shadowing, fading as well as un-intentional interference. This sensitivity can wreak havoc with complex ciphers and cause numerous re-transmissions resulting in wasted bandwidth. With cognitive networks this sensitivity is especially troublesome because of the opportunistic nature of spectrum use by the secondary users and the fact that use of the spectrum is not guaranteed. Cognitive networks, therefore, must provide the following:

- Support for robust ciphers and encryption methods
- Mechanisms to safeguard WRAN operator's spectrum availability information from eavesdropping by competitors or would-be hackers

The security mechanisms to provide confidentiality and privacy are provided in Clause 7 and 8.4.

## Annex G

(informative)

### Bibliography

At the time of publication, the editions indicated were valid. All standards and specifications are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the references listed below.

- [B1] DIAMETER/RFC 3588, “Diameter Base Protocol,” September 2003.
- [B2] Draft in progress, Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM), December 2004 (draft-haverinen-pppext-eap-sim-16.txt).
- [B3] Draft in progress, Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA), draft-arkko-pppext-eap-aka-15.txt.
- [B4] Fette, B. A., Cognitive Radio Technology, Elsevier, 2009.
- [B5] Haykin, S., “Cognitive Radio: Brain-Empowered Wireless Communications,” IEEE J. Select. Areas Commun., vol. 23, no. 2, pp. 201–220, Feb. 2005.
- [B6] Hoven, N., and Sahai, A., “Power Scaling for Cognitive Radio,” In proceedings of IEEE WirelessCom, Technologies and Standards, Hawaii, USA, June 13–16, 2005.
- [B7] IEEE 802.22 Working Group on Wireless Regional Area Networks, “IEEE 802.22 Functional Requirements Document,” September 2005, doc.: 22-05-0007-47-0000\_RAN\_Requirements.doc.<sup>34</sup>
- [B8] IEEE 802.22 Working Group on Wireless Regional Area Networks, “WRAN Reference Model,” doc.: IEEE 802.22-04/0002.
- [B9] IEEE Std 802.1Q<sup>TM</sup>, IEEE Standard for Local and metropolitan area networks—Virtual Bridged Local Area Networks.
- [B10] IEEE Std 802.1X<sup>TM</sup>-2010, IEEE Standard for Local and Metropolitan area networks—Port-Based Network Access Control.
- [B11] IEEE Std 1363<sup>TM</sup>-2000, IEEE Standard Specifications for Public-Key Cryptography.
- [B12] IEEE Std 1363a<sup>TM</sup>-2004, IEEE Standard Specifications For Public Key Cryptography—Amendment 1: Additional Techniques.
- [B13] IEEE Std 1588<sup>TM</sup>-2008, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.

---

<sup>34</sup> IEEE publications are available from the Institute of Electrical and Electronics Engineers, Inc., 445 Hoes Lane, Piscataway, NJ 08854, USA (<http://standards.ieee.org/>).

- [B14] IEEE Std 1900.1™, IEEE Standard on Definitions and Concepts for Spectrum Management and Advanced Radio System Technologies.
- [B15] IEEE Std 1900.2™, IEEE Recommended Practice for Interference and Coexistence Analysis.
- [B16] IEEE Std 1900.6™-2011, IEEE Standard on Spectrum Sensing Interfaces and Data Structures for Dynamic Spectrum Access and other Advanced Radio Communication Systems.
- [B17] IETF RFC 791, “Internet Protocol,” September 1981.<sup>35</sup>
- [B18] IETF RFC 868, “Time Protocol,” May 1983.
- [B19] IETF RFC 1123, “Requirements for Internet Hosts - Application and Support,” October 1989.
- [B20] IETF RFC 2131, “Dynamic Host Configuration Protocol,” March 1997.
- [B21] IETF RFC 2349, “TFTP Timeout Interval and Transfer Size Options,” May 1998.
- [B22] IETF RFC 2459, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile,” January 1999.
- [B23] IETF RFC 2460, “Internet Protocol, Version 6 (IPv6) Specification,” December 1998.
- [B24] IETF RFC 2474, “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers,” December 1998.
- [B25] IETF RFC 2716, “PPP EAP TLS Authentication Protocol,” October 1999.
- [B26] IETF RFC 2865, “Remote Authentication Dial In User Service (RADIUS),” June 2000.
- [B27] IETF RFC 3095, “RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed,” July 2001.
- [B28] IETF RFC 3243, “RObust Header Compression (ROHC): Requirements and Assumptions for 0-byte IP/UDP/RTP Compression,” April 2002.
- [B29] IETF RFC 3588, “Diameter Base Protocol,” September 2003.
- [B30] IETF RFC 3748, “Extensible Authentication Protocol (EAP),” June 2004.
- [B31] IETF RFC 3749, “Transport Layer Security Protocol Compression Methods,” May 2004.
- [B32] IETF RFC 3843, “RObust Header Compression (ROHC): A Compression Profile for IP,” June 2004.
- [B33] IETF RFC 4017, “Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs,” March 2005.
- [B34] IETF RFC 4055, “Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” June 2005.

---

<sup>35</sup> Internet Requests for Comments (RFCs) are available on the World Wide Web at the following ftp site: [venera.isi.edu](http://venera.isi.edu); logon: anonymous; password: user's e-mail address; directory: in-notes.

- [B35] IETF RFC 4072, "Diameter Extensible Authentication Protocol (EAP) Application," August 2005.
- [B36] IETF RFC 4995, "The ROBust Header Compression (ROHC) Framework," July 2007.
- [B37] IETF RFC 4996, "ROBust Header Compression (ROHC): A Profile for TCP/IP (ROHC-TCP)," July 2007.
- [B38] IETF RFC 5480, "Elliptic Curve Cryptography Subject Public Key Information," March 2009.
- [B39] IETF RFC 5746, "The Transport Layer Security (TLS) Renegotiation Indication Extension," February 2010.
- [B40] IETF RFC 5756, "Updates for RSAES-OAEP and RSASSA-PSS Algorithm Parameters," January 2010.
- [B41] IETF RFC 5758, "Internet X.509 Public Key Infrastructure: Additional Algorithms for DSA and ECDSA," January 2010.
- [B42] IETF RFC 5878, "Transport Layer Security (TLS) Authorization Extension," May 2010.
- [B43] Industry Canada Radio Standards Specification RSS-210 "Low Power License-Exempt Radiocommunication Devices (All Frequency Bands)," Issue 7, June 2007.
- [B44] ISO 3166, English country names and code elements.<sup>36</sup>
- [B45] MIL-PRF-39012E, Connectors, Coaxial, Radio Frequency, General Specification For, Revision E 27 April 2005.<sup>37</sup>
- [B46] MIL-STD-348, Military Standard, Radio Frequency Connector Interfaces.
- [B47] Mitola, J., *Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio*, Ph.D. Thesis, Royal Institute of Technology, Sweden, Spring 2000.
- [B48] Recommendation ITU-R BT.417, Minimum field strengths for which protection may be sought in planning an analogue terrestrial television service.
- [B49] Recommendation ITU-R BT.419. Directivity and polarization discrimination of antennas in the reception of television broadcasting.
- [B50] Recommendation ITU-R BT.470, Conventional analogue television systems.
- [B51] Recommendation ITU-R BT.565, Protection ratios for 625-line television against radionavigation transmitters operating in the shared bands between 582 and 606 MHz.
- [B52] Recommendation ITU-R BT.798, Digital television terrestrial broadcasting in the VHF/UHF bands.
- [B53] Recommendation ITU-R BT.804, Characteristics of TV receivers essential for frequency planning with PAL/SECAM/NTSC television systems.

<sup>36</sup> ISO publications are available from the ISO Central Secretariat, 1, ch. de la Voie-Creuse, Case postale 56, CH-1211 Geneva 20, Switzerland (<http://www.iso.ch/>). ISO publications are also available in the United States from the Sales Department, American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (<http://www.ansi.org/>).

<sup>37</sup> MIL publications are available from Customer Service, Defense Printing Service, 700 Robbins Ave., Bldg. 4D, Philadelphia, PA 19111-5094.

- [B54] Recommendation ITU-R BT.1123, Planning methods for 625-line terrestrial television in VHF/UHF bands.
- [B55] Recommendation ITU-R BT.1125, Basic objectives for the planning and implementation of digital terrestrial television broadcasting systems.
- [B56] Recommendation ITU-R BT.1206, Spectrum shaping limits for digital terrestrial television broadcasting.
- [B57] Recommendation ITU-R BT.1368, Planning criteria for digital terrestrial television services in the VHF/UHF bands.
- [B58] Recommendation ITU-R P.1546, Method for point-to-area predictions for terrestrial services in the frequency range 30 MHz to 3000 MHz.
- [B59] Recommendation ITU-R BT.1735, Methods for objective quality coverage assessment of digital terrestrial television broadcasting signals of System B specified in Recommendation ITU-R BT.1306.
- [B60] Recommendation ITU-R BT.1786, Criterion to assess the impact of interference to the terrestrial broadcasting service.
- [B61] Recommendation ITU-R BT.1833, Broadcasting of multimedia and data applications for mobile reception by handheld receivers.
- [B62] Recommendation ITU-R P.372, Radio noise.
- [B63] Recommendation ITU-T X.690, OSI networking and system aspects—Abstract Syntax Notation One (ASN.1).
- [B64] SEC2, Standards for Efficient Cryptography Group (SECG) – SEC2: Recommended Elliptic Curve Domain Parameters Version 2, January 2010, <http://www.secg.org/download/aid-784/sec2-v2.pdf>.
- [B65] Siaud, I., and Ulmer-Moll, A.M., “A Novel Adaptive Sup-carrier Interleaving Application to millimetre-wave WPAN OFDM System (IST MAGNET Project),” Conference IEEE Portable 2007, Orlando (USA), March 2007.
- [B66] Siaud, I., and Ulmer-Moll A.M., “Turbo-like Processing for Scalable Interleaving Pattern Generation: application to 60 GHz UWB-OFDM systems,” ICUWB’07, Singapore, September 2007.
- [B67] Standards for Efficient Cryptography Group (SECG)—SEC 1: Elliptic Curve Cryptography Version 2.0, 21 May 2009, <http://www.secg.org/download/aid-780/sec1-v2.pdf>.
- [B68] Steven M. Kay, Fundamentals of Statistical Signal Processing, Volume I: Estimation Theory, Prentice Hall, 1993.
- [B69] Steven M. Kay, Fundamentals of Statistical Signal Processing, Volume 2: Detection Theory, Prentice Hall, 1998.