

2006-08-01

IEEE P802.16h™/D0, August 2006

~~Draft IEEE Standard for~~
Local and metropolitan area networks

Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems

Amendment for Improved Coexistence Mechanisms for License-Exempt Operation

Sponsor

~~LAN MAN Standards Committee~~

of the

~~IEEE Computer Society~~

and the

~~IEEE Microwave Theory and Techniques Socie~~

Copyright © <2005> by the IEEE.

3 Park Avenue

New York, NY 10016-5997, USA

All rights reserved.

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

IEEE Standards Activities Department

Manager, Standards Intellectual Property

445 Hoes Lane, P.O. Box 1331
Piscataway, NJ 08855-1331, USA

Abstract: Should be based on the scope and purpose of the standard as indicated on the PAR.

Keywords: Should highlight key terms and phrases from the abstract or text of the draft standard.

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

Copyright © 2005 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published xx Month 2005. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by the Institute of Electrical and Electronics Engineers, Incorporated.

Print: ISBN 0-7381-xxxx-x SHxxxxx
PDF: ISBN 0-7381-xxxx-x SSxxxxx

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 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. When a document is more than five years old and has not been reaffirmed, 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 the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

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.

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. Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

Note: 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. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

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 P802.16h, Draft Amendment to IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems - Amendment for Improved Coexistence Mechanisms for License-Exempt Operation.

Participants

This document was developed by the IEEE 802.16 Working Group on Broadband Wireless Access, which develops the WirelessMAN™ Standard for Wireless Metropolitan Area Networks.

IEEE 802.16 Working Group Officers

Roger B. Marks, *Chair*

Ken Stanwood, *Vice Chair*

Dean Chang, *Secretary*

Primary development was carried out by the Working Group's License-Exempt Task Group:

TG Officers

Mariana Goldhamer, *Chair*

Paul Piggin, *Vice-chair*

Xuyong Wu, *Editor*

Paul Piggin, *Secretary* (acting)

Barry Lewis, *Pre Vice-chair* (till July 2006)

Nader Zein, *Pre Secretary* (till Sept 2005)

~~The following members of the IEEE 802.16 Working Group on Broadband Wireless Access participated in the Working Group Letter Ballot in which the draft of this standard was prepared and finalized for IEEE Ballot:~~

~~*/to be determined/*~~

~~The following participated as non-members in the Working Group Letter Ballot:~~

~~*/to be determined/*~~

~~The following members of the IEEE Balloting Committee voted on this standard, whether voting for approval or disapproval, or abstaining.~~

[to be determined]

The following persons, who were not members of the IEEE Balloting Committee, participated (without voting) in the IEEE Sponsor Ballot in which the draft of this standard was approved:

[to be determined]

When the IEEE-SA Standards Board approved this standard on [date], it had the following membership:

[to be determined]

Contents

1. Overview	1
1.3 Frequency bands.....	1
1.3.3License-exempt and uncoordinated frequencies below 11 GHz (primarily 5-6 GHz)	2
2. References	2
3. Definitions.....	2
4. Abbreviations and acronyms.....	4
5. Service-specific CS	5
6. MAC common part sublayer	5
6.3 Data/Control plane	5
6.3.2MAC PDU Format	5
6.3.2.3MAC management messages.....	5
6.3.2.3.33Channel measurement Report Request/Response (REP-REQ/RSP)	5
6.3.2.3.62Base Station Descriptor (BSD) message.....	6
6.3.2.3.63Subscriber Station Uplink Radio Frequency (SSURF) message	7
6.3.2.3.64Master Advertisement Discovery Descriptor (MADD) message	8
6.3.2.3.65Slave Advertisement Discovery Descriptor (SADD) message.....	9
6.3.2.3.66Advertisement Discovery Policy Descriptor (ADPD) message.....	10
6.3.2.3.67BS_CCID_IND message.....	11
6.3.2.3.68BS_CCID_RSP message.....	13
6.3.2.3.69Coexistence Protocol Request MAC message (CP-REQ-MAC).....	13
6.3.2.3.70Coexistence Protocol Response MAC message (CP-RSP-MAC)	14
6.3.15DFS for license-exempt operation	15
6.3.15.1Introduction.....	15
6.4 MAC enhancement for coexistence	16
6.4.1General concepts	16
6.4.1.1Capability Negotiation	16
6.4.1.2Extended channel numbering structure.....	16
6.4.1.3MAC CX-Frame numbering.....	17
6.4.2OFDMA PHY support for WirelessMAN-CX	17
6.4.2.1Co-existence zone (CXZ) for downlink and uplink.....	17
6.4.2.2Measurement and Reporting	18
6.4.3Dynamic Channel Selection (DCS)	18
6.4.3.1Introduction.....	18
7. Privacy sublayer	19
8. PHY	19
8.4 WirelessMAN-OFDMA PHY	19
8.4.4Frame structure.....	19
8.4.4.2PMP frame structure	19
8.4.5.3.28Co-existence zone (CXZ) downlink IE format	20
8.4.5.4.29Co-existence zone (CXZ) uplink IE format	21

9. Configuration	21
10. Parameters and constants	21
10.5 Coexistence specific values	21
10.5.1 Radio signaling	21
10.5.2 Control Channel	22
11. TLV encodings	23
11.7 REG-REQ/RSP management message encodings	23
11.7.8 SS capability encodings	23
11.7.8.14 WirelessMAX-CX capability	23
11.11 REP-REQ management message encodings	23
11.12 REP-RSP management message encodings	24
11.20 BSD and SSURF Message and Encodings	26
12. System profiles	26
13. 802.16 MIB structure for SNMP	26
14. Management Interfaces and Procedures	26
15. Mechanism for improved coexistence	26
15.1 General	26
15.1.1 Components and Relationships	26
15.1.2 Mechanisms in WirelessMAN-CX	29
15.1.3 Procedure flow in WirelessMAN-CX	31
15.1.3.1 Procedure flow for BS	31
15.1.3.2 Procedure flow for SS	36
15.1.4 Frame Structure for WirelessMAN-CX	36
15.1.4.1 Frame Structure for interference identification	36
15.1.4.1.1 Coexistence signaling interval	37
15.1.4.1.2 Coexistence messaging interval	39
15.1.4.2 Frame Structure for interference prevention & resolution	40
15.1.5 Architecture for WirelessMAN-CX	42
15.2 Provision for the WirelessMAN-CX procedure	48
15.2.1 Synchronization of the WirelessMAN-CX systems	48
15.2.1.1 Synchronization using the Control Channel	49
15.2.2 Scanning before interference identification	50
15.2.2.1 Acceptable $S/(N+I)$	50
15.2.2.2 Acceptable time occupancy	50
15.2.3 Power Control	50
15.2.4 Dynamic Frequency Selection – DFS	50
15.2.4.1 Frequency selection for regulatory compliance	50
15.2.5 Same PHY Profile	50
15.3 Interference identification and basic connectivity creation	51
15.3.1 Coexistence signaling mechanisms	52
15.3.1.1 Coexistence Signalling Interval	52
15.3.1.1.1 CSI scheduling	52
15.3.1.1.2 CSI Frame Structure	54
15.3.1.1.3 Energy keying in time domain	56
15.3.1.2 Energy keying in frequency domain	57

15.3.1.2.1 Signaling procedures using frequency-keyed energy pulses	57
15.3.1.2.2 Using the coexistence slot for transmitting the BS IP identifier	57
15.3.1.3 Community entry of new BS using signaling	57
15.3.2 Coexistence messaging mechanism	60
15.3.2.1 Coexistence Messaging Interval (CMI) Use for Same Profile Systems	60
15.3.2.2 Candidate Channel Determination (Using GPS/UTC Synchronized CMI and Common Profile)	60
15.3.2.3 Entry of a new BS into a Interference Neighborhood and the Creation of a Coexistence Community Using GPS/UTC Time Synchronization and Common System Profile	62
15.3.3 Information table	65
15.3.3.1 Information table in distributed database	65
15.3.3.2 Information table in centralized database	70
15.4 Interference prevention	70
15.4.1 Adaptive Channel Selection – ACS	72
15.4.1.1 How to select a "free" channel (for ACS and DFS)	72
15.4.1.2 Optimization of Channel Distribution	73
15.4.2 Adaptive Sub frame Allocation - ASFA	75
15.4.2.1 Sub frame sharing & scheduling	75
15.4.2.1.1 Cooperation with other systems	75
15.4.2.1.2 Scheduling of interference free intervals in the context of IEEE 802.16 MAC	76
15.4.2.2 Sub frame distribution optimization	80
15.4.2.3 Creation of a new sub-frame	82
15.4.2.4 Interference Control in sub-frames	83
15.4.2.4.1 Controlling interference during master sub-frame	84
15.4.2.4.1.1 Interferer identification	84
15.4.2.4.1.2 Interference to BS	84
15.4.2.4.1.3 Interference to SS	84
15.4.2.4.2 Controlling interference during not-interfering traffic sub-frames	85
15.4.2.5 Credit token based coexistence protocol	85
15.4.2.5.1 General principle	86
15.4.2.5.2 Credit tokens assignment and usage principles	86
15.4.2.5.3 Negotiation between master systems	87
15.4.2.5.3.1 Definition and notation	87
15.4.2.5.3.2 Dynamic credit tokens based scheduling cycle	87
15.4.2.5.3.3 Negotiation mechanisms between master systems	88
15.4.2.5.4 Inter BSs communication	91
15.4.2.5.5 Radio Resources Sharing Opportunities Advertisement Discovery	91
15.4.2.5.5.1 Mechanisms enabling the discovery and the exploitation of the master cells originated advertisement discovery messages by the slave cells	93
15.4.2.5.5.2 Mechanisms enabling the discovery and the exploitation of the slave cells originated requests discovery messages by the master cells	95
15.4.3 Interference prevention from Ad-Hoc systems	96
15.4.3.1 Operating principles	96
15.4.3.2 Registration	96
15.4.3.3 Selection of suitable reception sub-frames	98
15.4.3.4 Signaling procedures using frequency-keyed energy pulses	98
15.5 Messages for WirelessMAN-CX	99
15.5.1 Sequencing and Retransmission	99
15.5.2 Coexistence Protocol (CP) messages (CP-REQ/ CP-RSP)	99
15.5.2.1 Identify Coexistence Request message	105
15.5.2.2 Identify Coexistence Reply message	105
15.5.2.3 Coexistence Neighbor Topology Request message	106
15.5.2.4 Coexistence neighbor Topology Reply message	106
15.5.2.5 Registration Request message	106

15.5.2.6Registration Reply message.....	107
15.5.2.7Registration Update Request message.....	107
15.5.2.8Registration Update Reply message.....	107
15.5.2.9De-registration Request message.....	107
15.5.2.10De-registration Reply message.....	108
15.5.2.11Add Coexistence Neighbor Request message.....	108
15.5.2.12Add Coexistence Neighbor Reply message.....	108
15.5.2.13Update Coexistence Neighbor Request message.....	108
15.5.2.14Update Coexistence Neighbor Reply message.....	109
15.5.2.15Delete Coexistence Neighbor Request message.....	109
15.5.2.16Delete Coexistence Neighbor Reply message.....	109
15.5.2.17Get_Param_For_Radio_Signature_Request message.....	109
15.5.2.18Get_Param_For_Radio_Signature_Reply message.....	109
15.5.2.19Evaluate_Interference_Request message.....	110
15.5.2.20Evaluate_Interference_Reply message.....	111
15.5.2.21Work_In_Parallel_Request message.....	112
15.5.2.22Work_In_Parallel_Reply message.....	112
15.5.2.23Reduce_Power_or_Quit_Sub_Frame_Request message.....	113
15.5.2.24Reduce_Power_or_Quit_Sub_Frame_Reply message.....	113
15.5.2.25Create_New_Sub_Frame_Request message.....	114
15.5.2.26Create_New_Sub_Frame_Reply message.....	114
15.5.2.27SS_CCID_IND message.....	115
15.5.2.28SS_CCID_RSP message.....	116
15.5.2.29PSD_REQ message.....	116
15.5.2.30PSD_RSP message.....	117
15.5.2.31Channel Switch Negotiation Request message.....	118
15.5.2.32Channel Switch Negotiation Reply message.....	118
15.5.2.33Channel Switch Request message.....	118
15.5.2.34Channel Switch reply message.....	118
15.5.2.35Advertisement Request.....	119
15.5.2.36Advertisement Reply.....	119
15.5.2.37Negotiation Process Request.....	120
15.5.2.38Negotiation Process Reply.....	120
15.5.2.39Credit Token Proposal Request.....	120
15.5.2.40Credit Token Proposal Reply.....	121
15.5.2.41Negotiation Results Request.....	121
15.5.2.42Negotiation Results Reply.....	121
15.5.2.43Granting Request.....	122
15.5.2.44Granting Reply.....	122
15.5.3Message Validity Check.....	122
15.5.4Fragmentation.....	123
15.5.5Transport Protocol.....	123
15.5.6Using dedicated messages.....	123
15.5.6.1Common PHY.....	123
15.5.6.2Between BS and SS.....	123
15.5.6.2.1BS Neighborhood Update Request BroadCasting (BS_NURBC).....	123
15.6Recommended practice for WirelessMAN-CX.....	124
15.6.1Grouping of interfering/not-interfering units.....	124
15.7Coexistence with non-WirelessMAN-CX systems.....	124
15.7.1Interference from Non-IEEE 802.16 systems.....	124
15.7.1.1Non-IEEE 802.16 Systems capable of GPS/UTC Timing Recovery.....	125
15.7.1.2Non-IEEE 802.16 Systems not capable of GPS/UTC Timing Recovery.....	125
15.7.2Coexistence with non-WirelessMAN wireless access systems.....	125

Annex A	126
Mechanism of security in coexistence –reference	126
A.1 General Principal	126
A.2 Coexistence Protocol	130
A.3 Base Station Identification Server	132
A.4 RADIUS Protocol Usage	133
A.5 Privacy Key Management protocol usage	135
A.6 Security consideration.....	139
A.7 RADIUS Protocol Messages	139
A.8 Privacy Key Management protocol messages	142
Annex B	145
GPS Timing and Base Station Synchronization	145
Annex C	146
interference scenario case study.....	146
C.1 Base Station initialization scenario case study	146
C.2 Interference Scenario Case Studies for Synchronized WirelessMAN-CX Systems conforming to a Common PHY Profile.....	150

List of figures

Figure h1—Flowchart showing generic operation in bands with specific spectrum users.....	15
Figure h2—Representation of 'Channel Centre Frequency' calculation.....	17
Figure h3—Link level representation of DCS operation.....	19
Figure h4—Neighbor relationship formed by bidirectional interference	27
Figure h5—Neighbor relationship formed by unidirectional interference	28
Figure h6—Concept of neighborhood	29
Figure h7—Summarization diagram of coexistence mechanism	31
Figure h8—Initialization procedures — BS	33
Figure h9—Initialization procedures - BS radio resource allocation	34
Figure h10—CSI and CMI locations in WirelessMAN-CX.....	37
Figure h11—Timing of Coexistence Signaling Interval.....	37
Figure h12—CSI parameters	38
Figure h13—ICSI/OCSI occupation and timing example	39
Figure h14—CMI Timing.....	40
Figure h15—Interference due to overlapping systems	41
Figure h16—examples of WirelessMAN-CX Subframes	41
Figure h17—System Architecture	43
Figure h18—Inter-system Communication Architecture	43
Figure h19—WirelessMAN-CX BS Protocol Layering Model	44
Figure h20—BSIS and CX BS layering diagram with the Coexistence Protocol	45
Figure h21—using centralized server	46
Figure h22—WirelessMAN-CX neighbor BSs discovery and definition of coexistence neighbor and community	47
Figure h23—The first 4 slots of the Control Channel	50
Figure h24—format of ICSI/OCSI allocation MAP	53
Figure h25—Example of CSI allocation MAP in one BS's database	53
Figure h26—CSI frame construction with no less than 4 symbols in one slot.....	54
Figure h27—CSI frame construction with 1 symbol in 1 slot.....	55
Figure h28—CSI frame PLD.....	55
Figure h29—CSI symbol transmission and receiving	57
Figure h30—IBS entering the community by neighborhood update request broadcasting.....	58
Figure h31—IBS entering the community with proxy	59
Figure h32—CCD Process.....	62
Figure h33—IBS community entry process	64
Figure h34—IBS3 Entry Signalling	65
Figure h35—Process of ACS.....	73
Figure h36—Process of channel distribution optimization	75
Figure h37—Sub-frame structure type1	76
Figure h38—Sub-frame structure type 2	77
Figure h39—Allocation of slots for BS and SS radio signature.....	78
Figure h40—Relation between Master sub-frame type 1 and the CXZ	79
Figure h41—Relation between Master sub-frame type 2 and the CXZ	80
Figure h42—The procedure to find a current subframe as its master subframe.....	81
Figure h43—Process of subframe distribution optimization.....	82
Figure h44—Example of TDD based MAC frame sharing structure between M SYSs	86
Figure h45—Dynamic (iterative) credit tokens based scheduling cycle (sequences (1) to (5)).....	87
Figure h46—Dynamic (iterative) credit tokens based scheduling cycle (sequences (5) to (10)).....	88
Figure h47—Simplified MAC frame structure illustrating master system sub-frame renting principle and associated notations.....	88
Figure h48—Policy instructions to the slave SSs by the slave BSs	93
Figure h49—Detection and identification of the MATIs content by the slave SSs	94

Figure h50—Relaying of the MATIs content to the slave cell by the slave SSs	94
Figure h51—Master-Slave BS communication through the backhaul	95
Figure h52—Detection and identification of the SATIs content by the master SSs	95
Figure h53—Relaying of the SATIs content to the master cell by the master SSs	96
Figure h54—Master BS - Slave BS communication through the backhaul	96
Figure h55—Desired spectral densities for different channel BWs	98
Figure h56—Example of PSD Display	118
Figure h-A1—Network Architecture	126
Figure h-A2—BSs/BSISs connection encrypted in IPSec	127
Figure h-A3—Network Architecture under multi-Operators with multi-RADIUS Servers	129
Figure h-A4—Individual Session-Key	130
Figure h-A5—WirelessMAN-CX BS Protocol architecture Model	131
Figure h-A6—LE BS architecture with Coexistence Protocol	131
Figure h-A7—BSIS architecture with co-located regional LE database	132
Figure h-A8—RADIUS protocol example	133
Figure h-A9—PKM Session-Key-Handshaking procedures	136
Figure h-A10—PKM Session-Key Re-Key procedures	137
Figure h-A11—PKM Session-Key Re-Key procedures with the MK update of PKM-Target	138
Figure h-A12—the 640-bits Key generated by PRF640	139
Figure h-A13—Session-Key-Start message format	143
Figure h-A14—Session-Key-Request message format	144
Figure h-A15—Session-Key-Response message format	144
Figure h-A16—Session-Key-Accept message format	144
Figure h-B1—GPS 1pps Pulse	145
Figure h-C1—Environment of initializing basestation	146
Figure h-C2—Legend of arrow indicating interference direction	147
Figure h-C3—Legend of line indicating interference situation and symbols indicating wirelink usability	147
Figure h-C4—case 1x study	148
Figure h-C5—case 2x study	148
Figure h-C6—Enhanced mechanism dealing with case 2x	149
Figure h-C7—case 3x study	149
Figure h-C8—BS_CCID_IND BS_CCID_RSP procedure case 1	154
Figure h-C9—BS_CCID_IND BS_CCID_RSP procedure case1	155

List of Tables

Table 108aa—BSD message format	7
Table 108ab—SSURF message format	8
Table 108ac—MADD message format	9
Table 108ad—SADD message format	10
Table 108ae—ADPD message format	11
Table 108af—BS_CCID_IND message format	12
Table 108ag—BS_CCID_RSP message format	13
Table 108ah—CP-REQ-MAC message format	14
Table 108ai—CP-RSP-MAC message format	14
Table 286aa—CXZ downlink IE	20
Table 302w—CXZ uplink IE	21
Table 345a—parameter of absolute time reference	22
Table 345b—parameter of radio signaling timer	22
Table 345c—parameter of control channel timer	22
Table h1—coexistence mechanism list for WirelessMAN-CX	30
Table h2—Sequence of radio signals sent in the Control Channel	49
Table h3—CSI symbol Format	56
Table h4—Information table for the BS containing this database	65
Table h5—Information table for the systems inside the neighborhood or community	67
Table h6—Information table for the SSs inside the system containing this database	68
Table h7—Radio signal definition	98
Table h8—CP messages	99
Table h9—CP message format	100
Table h10—CP message codes	101
Table h11—TLV types for CP payload	102
Table h12—Identify Coexistence Request message attribute	105
Table h13—Coexistence neighbor Topology Parameter Set	105
Table h14—Coexistence Neighbor Topology Request message attribute	106
Table h15—Coexistence neighbor Topology Parameter Set	106
Table h16—Registration Request message attributes	107
Table h17—De-registration Request message attributes	107
Table h18—Add Coexistence Neighbor Request message attributes	108
Table h19—Update Coexistence Neighbor Request message attributes	108
Table h20—Delete Coexistence Neighbor Request message attributes	109
Table h21—Get_Param_Replay Parameter set	110
Table h22—Evaluate_Interference_Request Parameter set	110
Table h23—Evaluate_Interference_Replay Parameter set	111
Table h24—Work_In_Paralel_Request Parameter set	112
Table h25—Work_In_Parallel_Replay Parameter set	112
Table h26—Reduce_Power_or_Quit_Sub_Frame_Request Parameter set	113
Table h27—Reduce_Power_or_Quit_Sub_Frame_Replay Parameter set	113
Table h28—Create_New_Sub_Frame_Request Parameter set	114
Table h29—Create_New_Sub_Frame_Replay Parameter set	114
Table h30—SS_CCID_IND TLV encoding	115
Table h31—SS_CCID_RSP TLV encoding	116
Table h32—Channel Switch Request message attributes	118
Table h33—Channel Switch Reply message attributes	119
Table h34—Advertisement Request message attributes	119
Table h35—Advertisement Reply message attributes	119
Table h36—Negotiation Process Request message attributes	120
Table h37—Negotiation Process Reply message attributes	120

Table h38—Credit Token Proposal Request message attributes	120
Table h39—Credit Token Proposal Reply message attributes	121
Table h40—Negotiation Results Request message attributes	121
Table h41—Negotiation Results Reply message attributes.....	121
Table h42—Granting Request message attributes	122
Table h43—Granting Reply message attributes	122
Table h44—BS_NURBC message TLV encoding.....	123
Table h-A1—Security Block Format.....	134
Table h-A2—RADIUS-BS/BSIS-Registration-Access-Request.....	140
Table h-A3—RADIUS-BS/BSIS-Registration-Access-Accept	140
Table h-A4—RADIUS-BS/BSIS- Access-Request.....	141
Table h-A5—RADIUS-BS/BSIS- Access-Accept	141
Table h-A6—ESP Transform identifiers	141
Table h-A7—ESP Authentication algorithm identifiers.....	142
Table h-A8—Session Key frame TLV	142

Draft IEEE Standard for
Local and Metropolitan Area Networks

Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems

Amendment for Improved Coexistence Mechanisms for License-Exempt Operation

NOTE—The editing instructions contained in this amendment/corrigendum define how to merge the material contained herein into the existing base standard IEEE Std 802.16-2004.

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

1. Overview

scope: This amendment specifies improved mechanisms, as policies and medium access control enhancements, to enable coexistence among license-exempt systems based on IEEE Standard 802.16 and to facilitate the coexistence of such systems with primary users.

applicability: This amendment improves the coexistence of 802.16 systems in interference environments characteristic of license-exempt operation, including operation in lightly licensed situations where frequencies are not assigned exclusively. Some of the defined procedures could be applied in other cases, which require improved inter-system coexistence.

1.3 Frequency bands

[change the text as indicate in subclause 1.3.3]

1.3.3 License-exempt and uncoordinated frequencies below 11 GHz ~~(primarily 5-6 GHz)~~

The physical environment for the license-exempt bands and uncoordinated frequencies below 11 GHz is similar to that of the licensed bands in the same frequency range, as described in 1.3.2. However, the license-exempt nature introduces additional interference and co-existence issues, whereas regulatory constraints limit the allowed radiated power. In addition to the features described in 1.3.2, the ~~PHY and~~ MAC introduces mechanisms such as dynamic frequency selection (DFS) to detect and avoid interference to specific spectrum users. This is specified in section 6.3.15 concerning shared frequency band usage.

Further enhancements to facilitate co-existence for license-exempt and uncoordinated systems in utilizing improved co-existence mechanisms is embodied in MAC enhancements specified in 6.4. This section provides a definition for the WirelessMAN-CX designation. WirelessMAN-CX operation is intended to cover a number of license-exempt and uncoordinated band operation scenarios. Section 6.4 describes support functions for WirelessMAN-CX operation for non-collaborative operation. These procedures provide robust co-existence operation in the presence of non-cooperative and unknown wireless technologies, together with application to interference avoidance of adjacent licensed and license-exempt bands.

Based on the WirelessMAN-CX designated section 15 provides enhancements to the MAC protocol to provide for better interference measurement, reporting and management; together with negotiation for spectrum sharing to allow different WirelessMAN-CX systems to coexist in the band of operation.

[Insert the following row into table-1:]

Designation	Applicability	PHY	Additional MAC requirements	Options	Duplexing alternative
WirelessMAN-CX	Below 11 GHz license-exempt or when needed for inter-system improved coexistence	Section 8	MAC enhancements for coexistence (6.4)	Those applicable to PHY implemented. Section 15	TDD FDD

2. References

3. Definitions

[Insert following sections after 3.85:]

3.86 WirelessMAN-CX: The designation used to describe the realization that adds co-existence procedures to systems implemented below 11GHz, in license-exempt bands or whenever improved inter-system coexistence is needed. This designation is PHY independent and adds additional MAC functionality, together with a recommended practice as high level protocols for achieving coexistence.

1 **3.87 Interference Neighborhood:** Interference neighborhood is relative to a system (BS and its subscrib-
2 ers). A system (BS and its SSs) will perceive as interference neighbors, all other systems (BSs and their SSs)
3 which create/receive interference to/from it.
4

5
6 **3.88 Community:** is composed of those systems (BSs and their SSs) which coordinate to resolve their inter-
7 ference.
8

9
10 **3.89 Coexistence Community:** is composed of those systems (BSs and their SSs) which have resolved their
11 interference and coexist.
12

13 **3.90 Coexistence Proxy(CXPRX):** Coexistence proxy acts as an agent to forward the Coexistence Protocol
14 (CP) messages between its BSs and other BSs and terminals over the internet.
15

16
17 **3.91 Random Temporary Key (RTK):** The temporary key generated and sent by the BS over the air, and is
18 required to be contained in the request messages of the coexistence protocol sent to this BS. RTK is used to
19 obstruct the coexistence requests from unauthenticated internet terminals.
20

21
22 **3.92 Alternative Channel (ALTCH):** The alternative working channel decided by the base station, on
23 which the base station has not detected any user and also not currently chosen to be the working channel of
24 this base station.
25

26
27 **3.93 Alternative Subframe (ALTSF):** The alternative working subframe by the base station in the system,
28 able to be used as its master subframe in its capable channel, on which the base station haven't detected any
29 user and also not currently chosen to be the working channel of this base station.
30

31
32 **3.94 Coexistence Signaling Interval (CSI):** a predefined time slot for the coexistence protocol signaling
33 purpose, especially for the BS to contact its coexistence neighbor BS through one or more coexistence
34 neighbor SSs in the common coverage area.
35

36
37 **3.95 Initialization Coexistence Signaling Interval (ICSI):** the periodically appointed CSI specially used
38 by IBS to contact its neighbor OBS. When the IBS gets the OCSI allocation and starts the operating stage, it
39 will cease from using the ICSI.
40

41
42 **3.96 Operation Coexistence Signaling Interval (OCSI):** the rest CSI other than ICSI, periodically reallo-
43 cated to OBSs.
44

45
46 **3.97 Coexistence Signaling Interval Number (CSIN):** the periodical number of CSI according to the time
47 order. The range of CSIN is from 0 to the number of CSI in one OCSI cycle.
48

49
50 **3.98 Coexistence Signaling:** the signaling mechanism defined in WirelessMAN-CX to exchange informa-
51 tion between wireless systems with or without the same PHY profiles.
52

53
54 **3.99 Coexistence Messaging:** the messaging mechanism defined in WirelessMAN-CX to exchanged infor-
55 mation between wireless systems with the same PHY profiles.
56

57
58 **3.100 Master sub-frame:** part of the MAC frame, with special coexistence properties for systems ownning
59 this sub-frame as Masters; during this sub-frame a Master system operates with reduced interference and
60 may use its maximum transmission power.
61

62
63 **3.101 Slave sub-frame:** part of the MAC frame, with special restrictions for systems operating as Slaves;
64 Slave systems shall not create interference to systems which operate during their Master sub-frame.
65

66
67 **3.102 Dynamic Channel Selection (DCS):** The ability of a system to switch to a different logical channel
68 based on channel measurements avoiding interference in license-exempt and uncoordinated bands of opera-

tion. Logical channels can be constructed from: frequency band, portion of a frequency band, time, or a combination of these elements.

4. Abbreviations and acronyms

[Insert the following abbreviations at appropriate location:]

ADPD	Advertisement Discovery Policy Descriptor
AH	Authentication Header
ALTCH	Alternative Channel
BSD	Base Station Descriptor
BSIS	Base Station Identification Server
CCD	Candidate Channel Determination
CMI	Coexistence Messaging Interval
CNTI	Cognitive Network Time Interval
CoNBR	Coexistence Neighbor
CR	Cognitive Radio
CR_NOC	Cognitive Radio Network Operations Centre.
CSI	Coexistence Signaling Interval
CSIN	Coexistence Signaling IntervalNumber
CTG	CSI Transmission Gap
CTS	Coexistence Time Slot
CX	Co-eXistence
CXPRX	Coexistence Proxy
DCS	Dynamic Channel Selection
DRRM	Distributed Radio Resource Management
DSM	Distribution System Medium
EOF	End of Frame (of the CSI message)
ESP	IP Encapsulating Security Payload
IANA	Internet Assigned Numbers Authority
IBS	Initializing Base Station
ICSI	Initialization Coexistence Signaling Interval
IETF	Internet Engineering Task Force
IPBC	IP address Broadcast
IPsec	Internet Protocol Security
MATI	Master Advertisement Time Interval
NOC	Network Operation Center
NURBC	Neighborhood Update Request BroadCast
OBS	Operating Base Station
OCSI	Operation Coexistence Signaling Interval
PKM	Private Key Management
PLD	PayLoaD (of the CSI message)
PLE	Path Loss Exponent
PSD	Power Spectrum Density
RADIUS	Remote Authentication Dial-in User Service
RCG	Receive CSI Gap
RTK	Random Temporary Key
SAP	Service Access Point
SATI	Slave Advertisement Time Interval
SOF	Start of Frame (of the CSI message)

SSURF	Subscriber Station Uplink Radio Frequency
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTC	Universal Coordinated Time
WirelessMAN-CX	Wireless Metropolitan Access Network Co-eXistence

Notes: the IP broadcasting in the airlink is to be reconsidered and call for contribution for modification.

5. Service-specific CS

6. MAC common part sublayer

6.3 Data/Control plane

6.3.2 MAC PDU Format

6.3.2.3 MAC management messages

[Insert the following rows into Table-14. MAC Management messages as indicate.]

Type	Message Name	Message Description	Connection
67	BSD	Base Station Descriptor	Broadcast
68	SSURF	SS Uplink RF Descriptor	Basic
69	MADD	Master Advertisement Discovery Descriptor	Broadcast
70	SADD	Slave Advertisement Discovery Descriptor	Broadcast
71	ADPD	Advertisement Discovery Policy Descriptor	Broadcast
72	BS_CCID_IND	<i>[Base Station Co-Channel Interference Detection Indication]</i>	Basic
73	BS_CCID_RSP	<i>[Base Station Co-Channel Interference Detection Response]</i>	Basic
74	CP-REQ-MAC	Coexistence Protocol Request MAC message	Broadcast
75	CP-RSP-MAC	Coexistence Protocol Response MAC message	Broadcast
76-255		reserved	

6.3.2.3.33 Channel measurement Report Request/Response (REP-REQ/RSP)

[Change the text in section 6.3.2.3.33 as indicated:]

If the BS, operating in bands below 11 GHz, requires RSSI and CINR channel measurement reports, or requires neighbor detection reports, it shall send the channel measurements Report Request message. The

Report Request message shall additionally be used to request the results of the measurements the BS has previously scheduled. Table 62 shows the REP-REQ message.

The REP-REQ message shall contain the following TLV encoded parameters:

Report Request

The channel measurement Report Response message shall be used by the SS to respond to the channel measurements listed in the received Report Requests. Where regulation mandates detection of specific signals by the SS, the SS shall also send a REP-RSP in an unsolicited fashion upon detecting such signals on the channel it is operating in, if mandated by regulatory requirements. The SS may also send a REP-RSP containing channel measurement reports, in an unsolicited fashion, or when other interference is detected above a threshold value. In cases where specific signal detection by an SS is not mandated by regulation, the SS may indicate 'Unmeasured. Channel not measured.' (see 11.12) in the REP-RSP message when responding to the REP-REQ message from the BS. For a system compliant with WirelessMAN-CX, has the SS detected the broadcasting signaling from the coexistence neighbor BS, it shall use REP_RSP to report the information to its serving BS in an unsolicited manner. Table 63 shows the REP-RSP message.

[add a new section 6.3.2.3.62 as indicate:]

6.3.2.3.62 Base Station Descriptor (BSD) message

The base station descriptor (BSD) message specifies the base station identification information. This message is sent only in the CMI (see 15.1.4.1.2) claimed by the Base Station and it is intended to be decoded by SSs associated to other systems.

The BSD has two purposes. First, it contains pertinent information related to the base station, allowing foreign (interfered-with) Subscriber Stations to identify it as interference. Secondly, it allows the differentiation of a CMI from a non-CMI. When it is received, the SS associated with the BS will recognize the interval containing the BSD message as a CMI, and will transmit SSURF messages in response to it. Note that SSURF will use the uplink bandwidth granted only in the CMI, and is not transmitted in the data link.

The length of BSD message is an integral number of bytes. The BSD messages are generated and broadcast within the downlink portion of a CMI every minute by a base station.

A BSD message shall include the following parameters:

IP_Proxy address information: The Coexistence Proxy IP address information provides the IP address of the Coexistence Proxy Server. The encoding of this field is given below in TLV format.

BS EIRP: The BS EIRP field is included within this message to help determine the interference potential. It is signed in units of 1 dBm.

BS ID: Base Station Identifier.

RF Antenna Sector ID: The RF antenna sector ID is used to identify the RF antenna in a base station if multiple RF antennas are used for RF reuse purpose.

Table 108aa—BSD message format

Syntax	Size	Notes
BSD_Message_Format () {		
Management Message Type =67	8 bits	
BS EIRP	8 bits	dBm
BSID	48 bits	
BS RF antenna sector ID	8 bits	0-reserved for no RF reuse BS 1-255 for RF reuse BS
IP_Proxy_Address_IE()	Variable	TLV specific
}		

[add a new section 6.3.2.3.63 as indicate:]

6.3.2.3.63 Subscriber Station Uplink Radio Frequency (SSURF) message

The Subscriber Station uplink radio frequency (SSURF) message is the complement to the BSD message except it is sent on the uplink during the CMI interval claimed by the Base Station to which the SS is registered.

This message if received by foreign (interfered-with) Base Stations, will identify the SS as being an interferer.

A SSURF message shall includes the following parameters to identify a subscriber station:

SS ID: Subscriber station identifier, in the context of this message, identifies the transmitting SS. This SS is the source of co-channel interferences reported in this message.

BS ID: Serving Base Station associated with the SS.

BS Antenna Sector ID: The RF antenna sector ID is used to identify the RF antenna in a base station if multiple RF antenna are used for RF reuse purpose.

BS IP_Proxy address information: The BS IP address information uniquely identifies a associated base station. The encoding of this field is given above in TLV format.

Table 108ab—SSURF message format

Syntax	Size	Notes
SSURF_Message_Format() {		
Management Message Type =68	8 bits	
SS ID	8 bits	
BS ID	48 bits	Associated base station identifier
BS Antenna sector ID	8 bits	
BS IP Proxy_Address_IE()	Variable	
}		

[add a new section 6.3.2.3.64 as indicate:]

6.3.2.3.64 Master Advertisement Discovery Descriptor (MADD) message

The Master Advertisement Discovery Descriptor (MADD) message specifies the advertisement discovery information sent by the master BS towards the SSs located in the overlapped area of this master cell with the surrounding slave cells. This information is sent by the master BS in MATI in downlink (section 15.4.2.5.5) on a given channel (frequency domain). This information is sent every TMATI in the advertisement discovery period TS, and the advertisement discovery sequence occurs every TAD. MADD provides the necessary information to the SSs of the surrounding slave cells to inform the slave BSs about possibilities of radio resources sharing with this master cell.

A MADD message shall include the following parameters:

BSID_M: ID of the master BS.

BS_IP_Proxy_address_M: The Coexistence Proxy IP address of the master BS.

T_START_M: The Starting time of the period opened for renting by the master cell on that channel.

T_End_M: The Ending time of the period opened for renting by this master cell on that channel.

MRCTN: Minimum number of credit tokens required by the master BS to share its radio resources.

LC: List of other channels (frequency domain) of the master cell opened for renting.

Table 108ac—MADD message format

Syntax	Size	Notes
MADD_Message_Format() {		
Management Message Type =69	8 bits	
BSID_M	48 bits	
IP_Proxy_address_M	variable	TLV specific
T_START_M	16 bits	Starting time of the period opened for renting by the master cell (in microseconds)
T_End_M	16 bits	Ending time of the period opened for renting by the master cell (in microseconds)
MRCTN	TBD	Minimum number of credit tokens required by the master BS
LC	TBD	List of other channels (frequency domain) of master cell opened for renting
}		

[add a new section 6.3.2.3.65 as indicate:]

6.3.2.3.65 Slave Advertisement Discovery Descriptor (SADD) message

The Slave Advertisement Discovery Descriptor (SADD) message specifies the advertisement discovery information sent by the slave BS towards the SSs located in the overlapped area of this slave cell with the surrounding master cells. This information is sent by the slave BS in SATI in downlink (section 15.4.2.5.5) on a given channel (frequency domain). This information is sent every TSATI in the advertisement discovery period TS, and the advertisement discovery sequence occurs every TAD. SADD provides the necessary information to the SSs of the surrounding master cells to inform the master BSs about possibilities of radio resources sharing with this master cell.

A SADD message shall include the following parameters:

BSID_S: ID of the slave BS.

BS_IP_Proxy_address_S: The Coexistence Proxy IP address of the slave BS.

T_START_S: Starting time from which the slave BS would be interested to rent a period opened for renting (in microseconds).

T_End_S: Ending time of the period the slave BS would be interested to rent (in microseconds).

Table 108ad—SADD message format

Syntax	Size	Notes
SADD_Message_Format() {		
Management Message Type =70	8 bits	
BSID_S	48 bits	
IP_Proxy_address_S	variable	TLV specific
T_START_S	16 bits	
T_End_S	16 bits	
}		

6.3.2.3.66 Advertisement Discovery Policy Descriptor (ADPD) message

The Advertisement Discovery Policy Descriptor (ADPD) message is sent by the slave BS in SATI in down-link (section 15.4.2.5.5) on a given channel (frequency domain). ADPD specifies when some SSs (located in the overlapped area between this slave cell and surrounding master cells and getting MADD message from master BS) associated to this slave BS have to report the MADD conveyed in MATI towards this BS.

ADPD message shall include the following parameters:

T_START_S: Starting time from which the slave BS would be interested to rent a period opened for renting (in microseconds). Before that time, the SSs associated to that slave BS are not allowed to report MADD content to their BS.

T_End_S: Ending time of the period the slave BS would be interested to rent (in microseconds). After this time, the SSs associated to that slave BS are not allowed to report MADD content to their BS.

RCTN_MAX: Maximum admissible number of credit tokens per radio resource unit the slave BS will provide to get the radio resources rented by the master BSs. Above this number of tokens, the SSs associated to that slave BS are not allowed to report MADD content to their BS.

Table 108ae—ADPD message format

Syntax	Size	Notes
ADPD_Message_Format() {		
Management Message Type =71	8 bits	
T_START_S	16 bits	
T_End_S	16 bits	
RCTN_MAX	16 bits	
}		

6.3.2.3.67 BS_CCID_IND message

The subscriber station co-channel interference indication (BS_CCID_IND) message contains co-channel interference information detected at a subscriber station. The source of co-channel interference can be foreign sources such as radars or non-WirelessMAN-CX compliant devices, as well as other WirelessMAN-CX base stations that may or may not be members of the coexistence community.

This is a MAC management message sent by a SS to its home base station when unresolved co-channel interference is detected at a SS. Unresolved co-channel interference typically is interference which is new to the SS and which is not recorded in the SS Interference Table as having been resolved using the Coexistence Protocol by the home base station of the SS. Resolved interference implies that messages destined to the SS will not be corrupted by interference emanating from a foreign WirelessMAN-CX base station. This message is sent either every time (or after a set number of detection instances) the foreign BSD interference is detected and until the interference is resolved.

The message is sent also when non-WirelessMAN-CX systems are detected, such RLAN signals or radars which have higher regulatory priority to the bandwidth.

The length of BSD message is an integral number of bytes.

This BS_CCID_IND MAC management message shall contain the following minimum information to help determine the source and victim of co-channel interference:

BS_ID: The foreign BS identity taken from the BSD message.

IP_BS Proxy_Address_IE: The proxy IP address associated with a foreign base station, derived from the BSD.

BS RF_Sector_ID: The RF antenna sector ID is used to identify the RF antenna in a base station if multiple RF antenna are used for RF reuse purpose; it is taken from the BSD.

BS EIRP: The EIRP of the interfering Base Station, taken from the BSD.

CMI_ID_XX

The Coexistence Messaging Interval during which the interference was received.

SS_ID: The subscriber station identifier: a 48 bit long field identifying the subscriber station that generated this BS_CCID_IND management message. This subscriber station is a victim of co-channel interference reported in this message.

INT_BSD_Frq: The frequency of interference BSD events detected per CMI cycles (calculated as the number of BSD interference events per N full CMI cycles [1 cycle= 1 min TBD]). For this specific BSD, as relayed by this BS_CCID_IND message. This value can be set by the home base station to make the SS less responsive to interference detection (such as highly sporadic and transient events).

DFS_LE_PWR_FRQ: This parameter is used to identify the mean RSSI of the radar signals or non-WirelessMAN-CX systems detected in CMI_ID_54. Radar signals may be detected at below DFS threshold values and the value given for their signature will be radar events (pulses) per minute. If non-WirelessMAN-CX systems their signature will be given as number of detected CMI_ID_54 events per N CMI cycles [1 minute=1 Cycle TBD]

Table 108af—BS_CCID_IND message format

Syntax	Size	Notes
BS_CCID_IND_Message_Format() {		
Management Message Type =72	8 bits	
SS_ID	48 bits	Subscriber station ID
DFS_LE_PWR_FRQ	32 bits	Bits 0-3: Device Type Bits 4-15: Device detection specific Bits 16-23: 8 bit mean RSSI Bits 24-31: TBD
INT_BSD_Frq	16 bits	The frequency of interference BSD (or non-WirelessMAN-CX) interference events at set detection power threshold
BS ID	48 bits	Foreign Base Station ID
BS_RF_Sector_id	8 bits	1-255 for RF reuse BS 0 reserved for no RF reuse BS
BS EIRP	8 bits	Nominal EIRP of interfering BS
CMI_ID_XX	8 bits	Coexistence Messaging Interval ID (CMI_ID_54 for non-WirelessMAN-CX)
IP_BS Proxy_Address	Variable	(Proxy IP)
}		

6.3.2.3.68 BS_CCID_RSP message

This message is sent to the SS initiating the BS_CCID_IND message. It is sent by the BS and it is used to indicate whether the interference events identified in the BS_CCID_IND have been resolved. For DFS and non-WirelessMAN-CX responses, other responses will be issued by the network management systems, which can entail moving to other channels, reducing EIRP, etc, at the SS.

BS_CCID_RSP shall contain the following parameters:

BS_ID: The identity of the foreign BS noted in the BS_CCID_RSP. This can be null if the message was originally due to DFS or non-WirelessMAN-CX sources.

RSP_FIELD: The response field indicates:

- (1) Interference with foreign BS is/is not resolved
- (2) Sub DFS threshold and non-WirelessMAN-CX users noted, no response at present
- (3) TBD threshold/response adjustment variables (TBD)

Table 108ag—BS_CCID_RSP message format

Syntax	Size	Notes
BS_CCID_RSP_Message_Format() {		
Management Message Type =73	8 bits	
BS_ID	48 bits	Interfering BS station ID for which this response is sent to SS; set to zero if non-WirelessMAN -CX
RSP_Field	16 bits	The response field indicates: Bit 0: Response to Radar=1 Response to Non-WirelessMAN CX =0 Bit 1-2: 0 - Resolved 1 - Pending Resolution 2 - Adjust threshold 3 - Inhibit Response Bit 3-9: Interference RSSI Power threshold Adjust (-95 to -55 dBm (TBD) Bit 10-15: TBD Threshold for number of interference events per CMI Cycle)
}		

6.3.2.3.69 Coexistence Protocol Request MAC message (CP-REQ-MAC)

This message encapsulates the Coexistence Protocol Request MAC messages.

CP-REQ-MAC is a broadcast message and shall include the following parameters:

Requesting BSID: the BSID of the BS requesting an action through the Coexistence Protocol

Target BSID: the BSID of the BS that should receive the message or the BSID of the Base Station Identification Server

CP_Message: this is a TLV described in the paragraph 15.5.2

CP-REQ-MAC has the following format:

Table 108ah—CP-REQ-MAC message format

Syntax	Size	Notes
CP-REQ-MAC_Message_Format () {		
Management Message Type = 74	8 bits	
CP_Message	variable	See the description of the Coexistence Protocol messages in 15.5.2
}		

6.3.2.3.70 Coexistence Protocol Response MAC message (CP-RSP-MAC)

This message encapsulates the Coexistence Protocol Response MAC messages.

CP-RSP-MAC is a broadcast message and shall include the following parameters:

CP_Message: this is a TLV described in the paragraph 15.5.2

CP-RSP-MAC has the following format:

Table 108ai—CP-RSP-MAC message format

Syntax	Size	Notes
CP-RSP-MAC_Message_Format () {		
Management Message Type = 75	8 bits	
CP_Message	variable	See the description of the Coexistence Protocol messages in 15.5.2
}		

6.3.15 DFS for license-exempt operation

6.3.15.1 Introduction

[Add the following text at the end of section 6.3.15.1.]

Figure h 1 illustrates the flowchart representation of a generic scheme for operation in bands with specific spectrum users. WirelessMAN-CX provides enhanced reporting for specific spectrum users and addresses the need in situations where more than one type of specific spectrum user is operational in a given band.

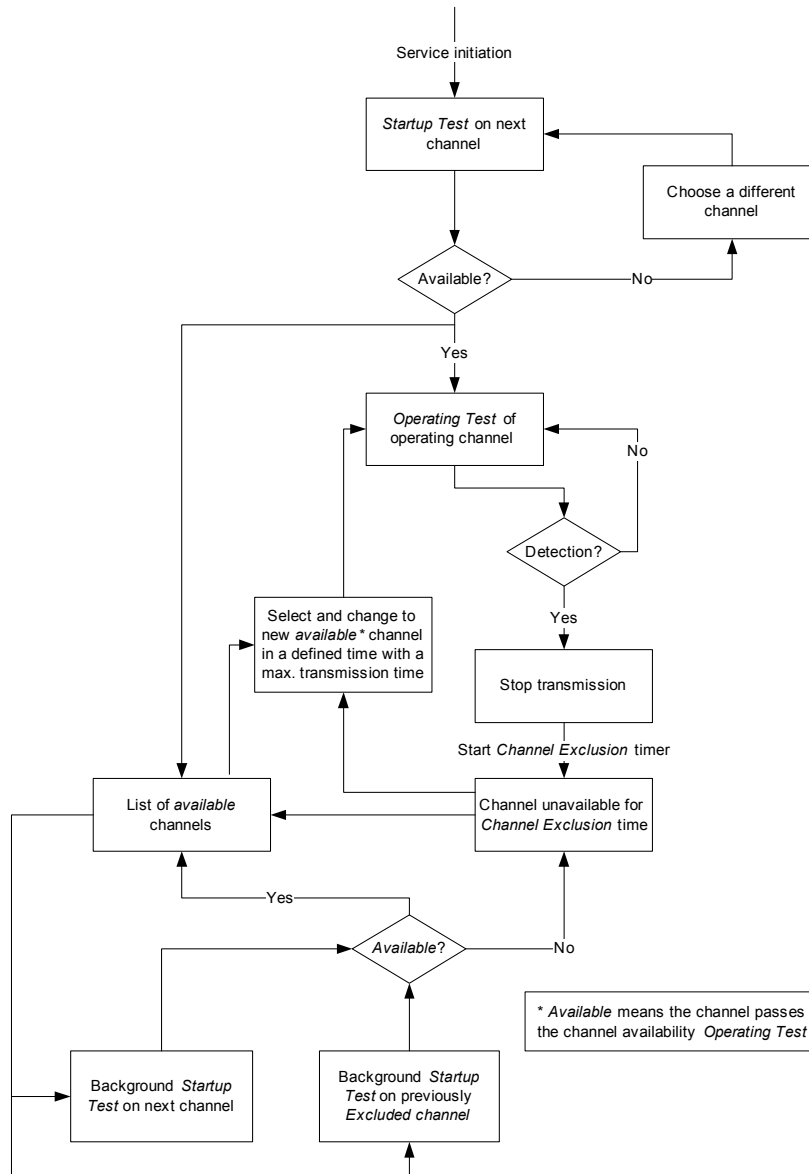


Figure h1—Flowchart showing generic operation in bands with specific spectrum users

[Insert a new section 6.4 :]

6.4 MAC enhancement for coexistence

This section describes MAC enhancements for WirelessMAN-CX in support of license-exempt and uncoordinated bands. Firstly concepts are described which are general to the MAC, after which PHY specific interactions are considered. PHY specific discussion is required since WirelessMAN-CX operation is dependant on the features supported for a given PHY.

6.4.1 General concepts

This section describes WirelessMAN-CX operation specific to the MAC and support of the MAC from the PHY.

6.4.1.1 Capability Negotiation

A Base Station is made aware of the WirelessMAN-CX capabilities and functionality support by the SS using the field described in section 11.7.8.

A mechanism is provided by which WirelessMAN-CX and non-WirelessMAN-CX devices are to interwork. This is an important mechanism for deployment scenarios where regulatory designation of WirelessMAN-CX operation is required. Some examples of how the capability negotiation can be used are given:

- A device with WirelessMAN-CX functionality will need to interwork with infrastructure that knows nothing of WirelessMAN-CX.
- A non-WirelessMAN-CX device will need to interwork with WirelessMAN-CX compliant infrastructure.
- A non-WirelessMAN-CX device shall have the ability to be barred from working in a WirelessMAN-CX system - this is deployment specific.
- A WirelessMAN-CX device shall work in a non-WirelessMAN-system as 'normal' non-WirelessMAN-CX device.

6.4.1.2 Extended channel numbering structure

License-exempt or uncoordinated bands may require or provide scope for the use of a defined channel raster or channel bandwidth. This section provides a means to achieve this, and therefore offer simplification to issues of interference managements. Extended channel numbering provides an enhancement to channelization and definition of channel number for WirelessHUMAN operation in section 8.5.1. This extension provides channelization references beyond the limits of 5-6GHz as defined. The channelization is defined accordingly.

- Extended Channel Number (ExChNr) – 2 byte specific channel number reference.
- Base Channel Reference (BaseChRef) – 1 byte base reference to frequency range or deployment band. This reference maps to an absolute frequency value
- Channel spacing (ChSp) - 2 byte channel spacing value (10kHz increments)

In summary the definition of the *Channel Centre Frequency* is:

$$\text{Channel Centre Frequency [MHz]} = \text{BaseFrequency}(\text{BaseChRef})[\text{MHz}] + ((\text{ExChNr} + 1/2) * \text{ChSp} * 0.01)[\text{MHz}]$$

This is shown in a graphical representation in Figure h 2.

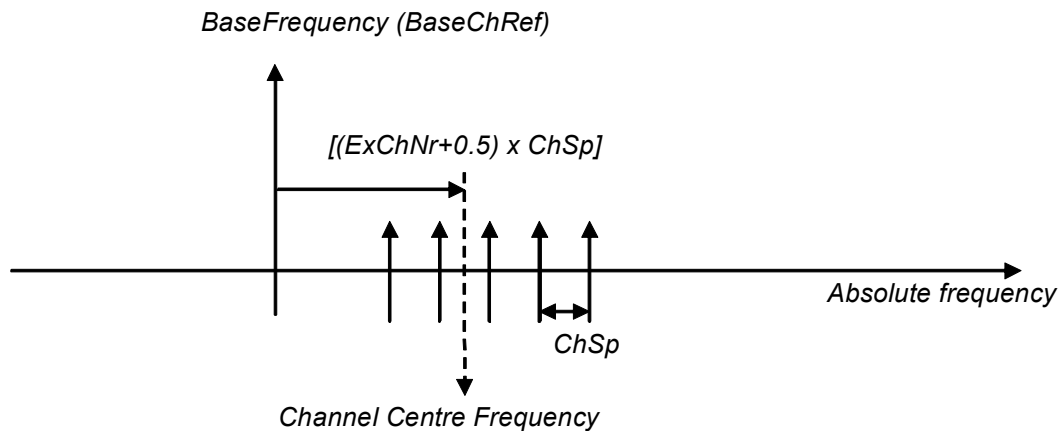


Figure h2—Representation of 'Channel Centre Frequency' calculation.

ExChNr is used in *REP-REQ/REP-RSP* messages while *BaseChRef*, and *ChSp* are communicated at a session setup or reconfiguration.

6.4.1.3 MAC CX-Frame numbering

The MAC Frame number used by the Coexistence Protocol (CX_MAC_NO) is a running number. The MAC Frame no.1 starts at the absolute time of the day 00:00:30sec and includes the first slot of the Control Channel.

CX_MAC_NO has a length of 16bit and wraps-around according to the repetition time of the Control Channel.

6.4.2 OFDMA PHY support for WirelessMAN-CX

This section provides a description of WirelessMAN-CX support for the WirelessMAN-OFDMA PHY.

6.4.2.1 Co-existence zone (CXZ) for downlink and uplink

The addition of a CXZ provides the means to include all co-existence enhancements in a defined region within the WirelessMAN-OFDMA PHY. It is expected that all co-existence operation will occur within this zone.

6.4.2.2 Measurement and Reporting

In order to meet strict requirement on measurement and reporting in license-exempt and uncoordinated bands enhanced reporting for WirelessMAN-CX is supported through the REP-REQ/REP-RSP MAC messages (see sections 11.11 and 11.12 respectively). Also the use of the WirelessMAN-OFDMA fast feedback channel is used to enhance reporting capabilities. Section 6.3.18.2 discusses periodic CINR report with fast-feedback (CQICH) channel. It is recommended that interference measurements are undertaken on the effective (feedback type=0b01) or physical (feedback type=0b00) CINR measurement for a CXZ permutation zone (Zone permutation=0b110 and report type=1) from pilot subcarriers (measurement type=0). Section 8.4.5.4.12 gives specific details of the CQICH allocation IE.

6.4.3 Dynamic Channel Selection (DCS)

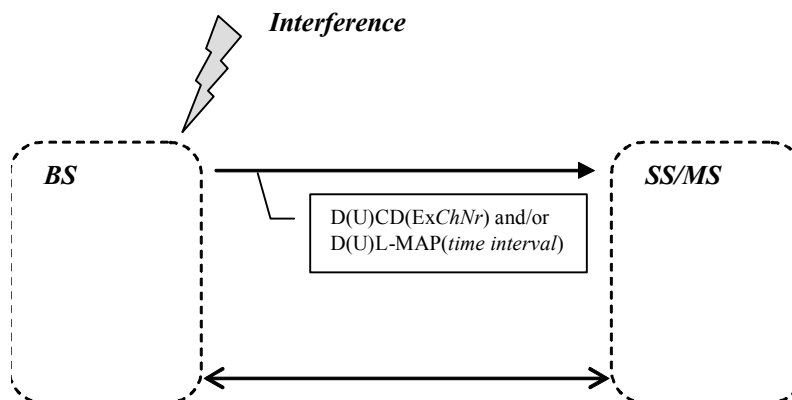
6.4.3.1 Introduction

Dynamic Channel Selection (DCS) provides the ability of a system to switch to different logical channel based on channel measurements thus avoiding interference in license-exempt and uncoordinated bands of operation. Logical channels can be constructed from: frequency band, portion of a frequency band, time, or a combination of these.

The main distinction for DCS from avoidance of specific spectrum users (6.3.15) is that there are no regulatory demands placed on the DCS solution. However both mechanisms are supported with the REP-REQ/REP-RSP (6.3.2.3.33) MAC messages. DCS provides a solution for bands in which there is no inter-system collaboration possible. DCS supports the solutions described in section 15.

A general example of a DCS solution is provided in figure xyz in which interference detection provides agility in frequency and time to reduce the affects of the incident interference. Figure h 1 (section 6.3.15.1), although for specific spectrum users, provides a further example of how DCS can be used to provide resource management.

(a) Interference and remedial action at the BS



(b) Interference and remedial action at the MS/SS

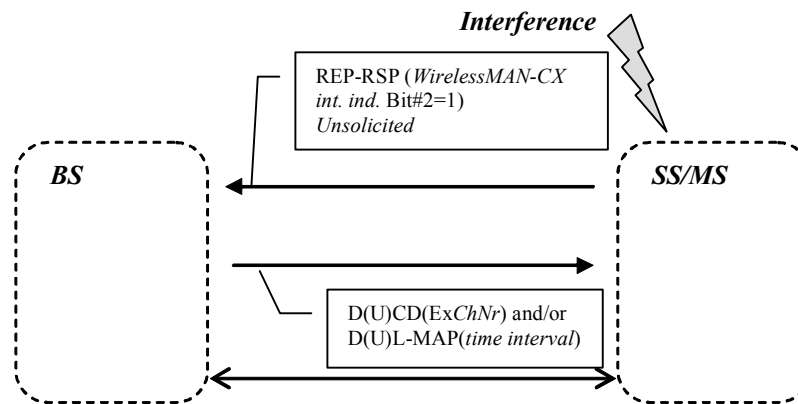


Figure h3—Link level representation of DCS operation

7. Privacy sublayer

8. PHY

8.4 WirelessMAN-OFDMA PHY

8.4.4 Frame structure

8.4.4.2 PMP frame structure

[change the last paragraph of section 8.4.4.2 into the following text in 802.16 primary standard:]

The OFDMA frame may include multiple zones (such as PUSC, FUSC, PUSC with all subchannels, optional FUSC, ~~and~~ AMC, CXZ, TUSC1, and TUSC2), the transition between zones is indicated in the DL-Map by the STC_DL_Zone IE (see 8.4.5.3.4), CXZ_DL_IE (see 8.4.5.3.11), or AAS_DL_IE (see 8.4.5.3.3). No DL-MAP or UL-MAP allocations can span over multiple zones. Figure 219 depicts the OFDMA frame with multiple zones.

[change figure 219 as following:]

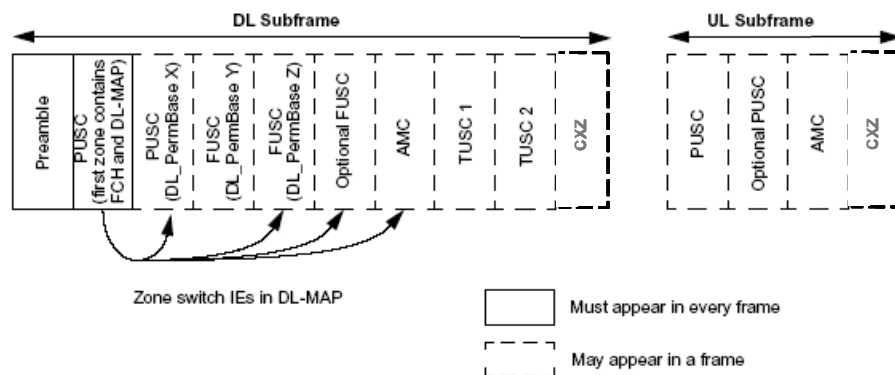


Figure 219—Illustration of OFDMA frame with multiple zones

[insert the following rows to table 277a, section 8.4.5.3.2.1.]

Extended DIUC (hexadecimal)	Usage
09	<u>CXZ_DL_IE</u>
09-0A	reserved

[Insert a new section 8.4.5.3.28:]

8.4.5.3.28 Co-existence zone (CXZ) downlink IE format

Within a frame, the switch to co-existence operation is marked by using the extended DIUC = 15 with the CXZ_DL_IE(). The CXZ_DL_IE defines a DL CX zone and spans continuous OFDMA symbols. Multiple CXZ zones can exist within the same frame. When used, the CID in the DL_MAP_IE() shall be set to the broadcast CID.

Table 286aa— CXZ downlink IE

Syntax	Size	Notes
CXZ_DL_IE() {		
Extended DIUC	4 bits	CXZ = 0x09
Length	4 bits	Length = 0x01
OFDMA symbol offset	8 bits	Denotes the start of the zone (counting from the frame preamble and starting from 0).
CXZ duration	10 bits	Denotes the duration of the zone
Next CXZ start	12 bits	The time interval, in symbols, until the start of the next downlink CXZ.
}		

[insert following row into table-289a as indicate(section 8.4.5.4.4.1):]

Extended UIUC (hexadecimal)	Usage
<u>0B</u>	<u>CXZ_UL_IE</u>
0B 0C ... 0F	<i>reserved</i>

[change the row in table 300 as indicate (section 8.4.5.4.12)]

Syntax	Size	Notes
Zone permutation	3 bits	The type of zone for which to report 0b000 - PUSC with 'use all SC = 0' 0b001 - PUSC with 'use all SC = 1' 0b010 - FUSC 0b011 - Optional FUSC 0b100 - Safety Channel region 0b101 - AMC zone (only applicable to AAS mode) <u>0b110 - CXZ</u> 0b110 -111 - Reserved

[Insert a new section 8.4.5.4.29]

8.4.5.4.29 Co-existence zone (CXZ) uplink IE format

Within a frame, the switch to co-existence operation is marked by using the extended UIUC = 15 with the CXZ_UL_IE(). The CXZ_UL_IE defines a DL CX zone spans continuous OFDMA symbols. Multiple CXZ zones can exist within the same frame. When used, the CID in the DL_MAP_IE() shall be set to the broadcast CID.

Table 302w—CXZ uplink IE

Syntax	Size	Notes
CXZ_UL_IE() {		
Extended DIUC	4 bits	CXZ = 0x09
Length	4 bits	Length = 0x01
CXZ zone length offset	8 bits	The length of the uplink CXZ zone.
CXZ duration	10 bits	Denotes the duration of the zone
Next CXZ start	12 bits	The time interval, in symbols, until the start of the next uplink CXZ.
}		

9. Configuration

10. Parameters and constants

[insert a new section 10.5 as indicate:]

10.5 Coexistence specific values

10.5.1 Radio signaling

The absolute time runs on a periodic base of 1800 sec. (30 minutes). For cases when one or more seconds are added/subtracted at the mid-night, the absolute time is supposed to follow those changes. All the values below are repeating based on the relation:

$$\text{Time} = (\text{Absolute time}) \bmod 1800.$$

The time is expressed as sec: ms, according to the decimal format xxxx:yyy.

Table 345a—parameter of absolute time reference

Absolute time reference	Chapter	Reference	Value
AT1	Radio signaling (15.4.3.2)	Start of the first MAC Frame (no. N) including cognitive radio signaling	0003:000, 15:000, 27:000, 39:000, 51:000

AT2	Radio signaling (15.4.3.2)	Start of the 2nd MAC Frame including cognitive radio signaling	AT1+0001:000
AT3	Radio signaling (15.4.3.2)	Start of the 3rd MAC Frame including cognitive radio signaling	AT1+0002:000
AT4	Radio signaling (15.4.3.2)	Start of the 4th MAC Frame including cognitive radio signaling	AT1+0004:000

Table 345b—parameter of radio signaling timer

Timer	Chapter	Reference	Value
T_cogn	Radio signaling (15.4.3.2)	Repetition period of the cognitive signaling	12s
Tad_reg	Radio signaling (15.4.3.2)	Maximum time-interval in which an ad-hoc unit has to repeat the registration	1800s
T_iptx	Radio signaling (15.4.3.2)	Time interval between the start of consecutive CSI slots for the transmission of the IP address using frequency-keyed energy pulses	20ms

10.5.2 Control Channel

Table 345c—parameter of control channel timer

Timer	Chapter	Reference	Value
Tcc	6.4.1.3	Average period of the Control Channel time-slots or 1/2 period between DL slots or 1/2 period of the UL slots	200ms
Tcc_s	6.4.1.3	Duration of the Control Channel slots	1.9ms
Tcc_ss	6.4.1.3	Offset of the DL Control Channel slots from the start of the first MAC Frame	1ms
Tcc_se	6.4.1.3	Duration from the end of the UL Control Channel slots to the end of the MAC Frame, for MAC Frames of 5,10 and 20ms	0.2ms

11. TLV encodings

11.7 REG-REQ/RSP management message encodings

[Insert the following row into table 369a:]

Type	Parameter
45	WirelessMAX-CX capability
46	Base Channel Reference (BaseChRef)
47	Channel Spacing (ChSp)

11.7.8 SS capability encodings

[insert new subclause 11.7.8.14:]

11.7.8.14 WirelessMAX-CX capability

Name	Type (1 byte)	Length (1 byte)	Value	Scope
WirelessMAX-CX capability	45	1	Bit #0: No WirelessMAX-CX capability Bit #1: WirelessMAX-CX capability Bits #2 - #7: Reserved	REG-REQ
Base Channel Reference (BaseChRef)	46	1	Base Channel Reference in MHz providing base reference to frequency range or deployment band	REG-RSP
Channel Spacing (ChSp)	47	2	Channel Spacing in 10kHz increments.	REG-RSP

11.11 REP-REQ management message encodings

[In the fourth row, fourth column of the second table in 11.11 change the first 8 rows as indicated]:

Name	Type (1 byte)	Length (1 byte)	Value
------	------------------	--------------------	-------

Zone-specific physical CINR request	1.4	3	<p>Bits #0-2: Type of zone on which CINR is to be reported</p> <p>0b000: PUSC zone with 'use all SC=0'</p> <p>0b001: PUSC zone with 'use all SC=1' / PUSC AAS zone</p> <p>0b010: FUSC zone</p> <p>0b011: Optional FUSC zone</p> <p>0b100: Safety Channel region</p> <p>0b101: AMC zone (only applicable to AAS mode)</p> <p>0b110: CX zone</p> <p>0b110-0b111: Reserved</p> <p>Bit #3: 1 if zone for which CINR should be estimated is STC zone, 0 otherwise.</p> <p>Bit #4: 1 if zone for which CINR should be estimated is AAS zone, 0 otherwise.</p> <p>Bits #5-6: PRBS_ID of the zone for which CINR should be estimated. Ignored for Safety Channel.</p> <p>Bit #7: Data/pilot-based CINR measurement:</p> <p>0 - Report the CINR estimate from pilot subcarriers,</p> <p>1 - Report the CINR estimate from data subcarriers</p> <p>Bits #8-13: Reported CINR shall only be estimated for the subchannels of PUSC major groups for which the corresponding bit is set. Bit #(k+7) refers to major group k. Only applicable for CINR measurement on a PUSC zone</p> <p>Bits #14-17: in multiples of 1/16 (range is [1/16,16/16])</p> <p>Bit #18: 0 - report only mean of CINR</p> <p>1 - report both mean and standard deviation of CINR</p> <p>Bits #19-23: Reserved, shall be set to zero</p>
-------------------------------------	-----	---	---

[insert the following entry in the second table of 11.11:]

Coexistence neighbor Interference Report	1.9	1	<p>Bit #0: 1-include information received in BS_NURBC</p> <p>Bit #1: 1-include RSSI of CSI symbols(only valid when bit#0 is set to one)</p> <p>Bit #2: 1-include frame number that start to receive BS_NURBC</p> <p>Bit #3~7: reserved, shall be set to zero</p>
ExChNr	1.10	2	Physical extended channel number (WirelessMAX-CX only)
Extended report type (WirelessMAN-CX only)	1.11	1	<p>Bit #0 = 1: Include summary extended report</p> <p>Bit #1 = 1: Include full extended report</p> <p>Bit #2 = 1: Specific spectrum user extended report</p> <p>Bits #3 - #7: Reserved</p>

11.12 REP-RSP management message encodings

[insert the following entry in the first table of 11.12:]

Coexistence neighbor Report	7	variable	Compound
Extended report type	8	variable	Compound

[insert the following table into 11.12 as indicates:]

Coexistence neighbor Inter- ference Report type	Name	Type	Length	Value
all	CoNBR system count /new neigh- bour system discov- ery indication	7.1	1	Bit #0:1-New CoNBR Discovered by BS_NURBC received Bit #1-7:The number of CoNBR that interference to this SS
bit #0=1	Neighborhood update request report IPv4	7.2	12	Bits 15:0 - RTK Bits 63:16 - BSID Bits 95:64 - BS IP address(IPv4) 4bytes IPv4 address of CoNBR interference to this SS, 255. 255. 255. 255 indicate the fail of CRC check.
bit #0=1	Neighborhood update request report IPv6	7.3	24	Bits 15:0RTK Bits 63:16BSID Bits 191:64BS IP address(IPv4) 16bytes IPv6 address of CoNBR interference to this SS, all ones indicate the fail of CRC check.
bit #1=1	BS_NURBC RSSI	7.4	2	1byte RSSI mean (see also 8.2.2, 8.3.9, 8.4.11) for details) 1byte standard deviation
Bit #2=1	Starting Frame Serial Number of BS_NURBC	7.5	3	Bit# 0-24: frame number of BS_NURBC starting frame

REP-REQ Extended report type	Name	Type	Length	Value
Bit #0 = 1 OR Bit #1 = 1 OR Bit #2 = 1	ExChNr	8.1	2	Extended physical channel number to be reported on.
Bit #0 = 1 OR Bit #1 = 1 OR Bit #2 = 1	Start frame	8.2	2	16 LSBs of Frame number in which measurement for this channel started
Bit #0 = 1 OR Bit #1 = 1 OR Bit #2 = 1	Duration	8.3	3	Cumulative measurement duration on the channel in multiples of Ts. For any value exceeding 0xFFFFFFFF, report 0xFFFFFFFF
Bit #0 = 1	WirelessMAX- CX interference indicator	8.4	1	Bit #0: Low interference indication Bit #1: Medium interference indication Bit #2: High interference indication Bit #3: Specific spectrum user detected on the channel Bit #4: Channel not measured.
Bit #1 = 1	Zone specific CINR report	8.5	2	1 byte: mean 1 byte: standard deviation
Bit #1 = 1	Zone specific RSSI report	8.6	2	1 byte: mean 1 byte: standard deviation

Bit #2 = 1	Specific spectrum user detection report	8.7	1	Bit #0: Specific spectrum user type #0 Bit #1: Specific spectrum type #1 Bit #2: Specific spectrum type #2 Bit #3: Specific spectrum type #3 Bit #4: Specific spectrum type #4 Bit #5: Specific spectrum type #5 Bit #6: Specific spectrum not known Bit #7: Channel not measured
------------	---	-----	---	--

[insert a new section 11.20 in clause 11 as indicate:]

11.20 BSD and SSURF Message and Encodings

IP_Proxy_Address_IE Encoding:

Name	Type (1 byte)	Length (1 byte)	Value	PHY Scope
ProxyIPv4 Address	1	4	Proxy IP address if IPv4 is supported.	all
ProxyIPv6 Address	2	16	Proxy IP address if IPv6 is supported.	all

There can be one and only one information element in an IP_Address_IE.

12. System profiles

13. 802.16 MIB structure for SNMP

14. Management Interfaces and Procedures

[insert new clause 15:]

15. Mechanism for improved coexistence

[Editor's notes: the figure number and table number is temporarily marked as Figure hxxx. And Table hxxx, these number should be corrected according to WG rules before the draft release]

15.1 General

This clause describes high-level protocols and policies to be used for coordinating the system operation in order to reduce the inter-system interference.

15.1.1 Components and Relationships

System: the BS and its associated SSs form a system. An WirelessMAN-CX system that is a member of a community of systems granted access to shared spectrum resources only if it forms an actual system comprised of at least one base station and one subscriber station and supports a bi-directional link.

Neighbor Relationship: it is a relationship between two systems, when the BS in at least one of these two systems creates interference higher than a certain threshold to at least one SS in another system, or at least one of the SSs in at least one of these two systems creates interference higher than a certain threshold to the BS in another system.

It is assumed that SS to SS interference and BS to BS interference are resolved apriori by frequency separation (in case of FDD systems) or transmission frame synchronization (in case of TDD). It should also be noted that some deployments and installations may cause interference that are beyond the capability of any automatic policy or procedure to resolve.

Figure h 4 shows some examples of neighbor relationship formed by bidirectional interference. In the Figure h 4, system A have neighbor relationship with system B, system C and system D, vice versa, system B have neighbor relationship with system A, so do system C and system D.

Figure h 5 is an example of neighbor relationship formed by unidirectional interference. System E and system F have neighbor relationship with each other, although all the interference between the two systems is caused by system E.

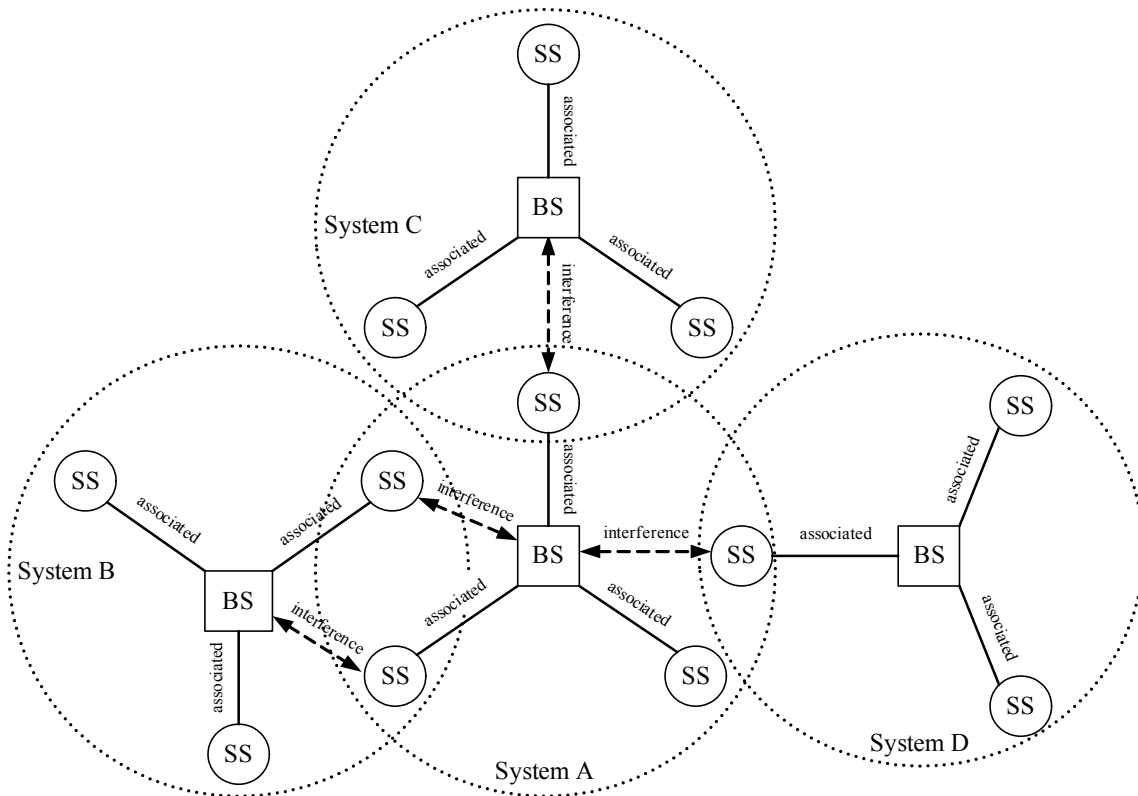


Figure h4—Neighbor relationship formed by bidirectional interference

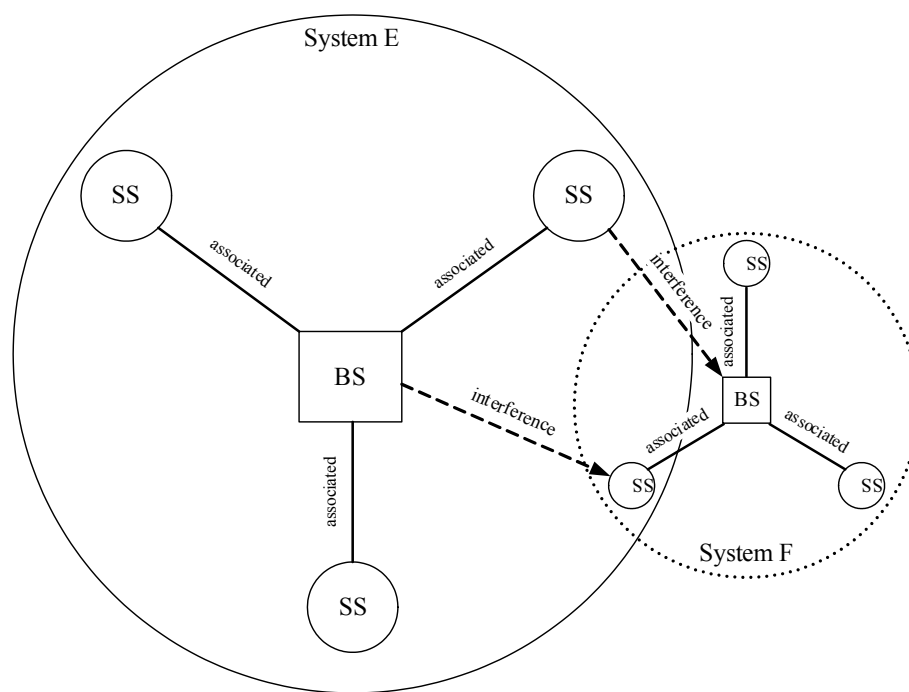


Figure h5—Neighbor relationship formed by unidirectional interference

Neighbor: A system is called a neighbor of system A, when it has a neighbor relationship with system A.

Interference Victim : A system is an Interference Victim , when there are at least one BS or one SS in this system which are interfered by a system's neighbor . The Interference Victim could be an Interference Source to its neighbors at the same time (eg. system A/B/C/D in Figure h 4), or only a victim of its neighbors.(eg. system F in Figure h 5).

Interference Source : A system is an Interference Source , when there are at least one BS or one SS in this system which interfere with its neighbors. The Interference Source could be an Interference Victim of its neighbors at the same time (eg. system A/B/C/D in Figure h 4), or only an Interference Source to its neighbors (eg. system E in Figure h 5).

Interference Victim BS/SS: the BS/SS in an interference victim system is an interference victim BS/SS, when the BS/SS is interfered by the SS/BS in this system's neighbor system, and the interference is higher than a certain threshold. The interference victim system could be an interference source BS/SS to the SS/BS in its neighbor system at the same time(eg. BS in system A/B/C and the interference victim SSs in system A/B/C/D in Figure h 4), or only an interference victim BS/SS of the interference source SS/BS in its neighbor system(eg. interference victim BS/SS in System F in Figure h 5).

Interference Source BS/SS: the BS/SS in an interference source system is an interference source BS/SS, when the BS/SS make interference to the SS/BS in the system's neighbor system, and the interference is higher than a certain threshold. The interference source BS/SS could be an interference BS/SS to the SS/BS in its neighbor system at the same time(eg. BS in system A/B/C and the interference source SSs in system A/B/C/D in Figure h 4), or only an interference source system of its neighbor system(eg. Interference source BS/SS in system E in Figure h 5).

Interference Neighborhood: An Interference neighborhood relates to a specific system. A system will perceive as interference neighbors, all other systems which create/receive interference to/from it. The Figure h 6 shows some examples of neighborhood.

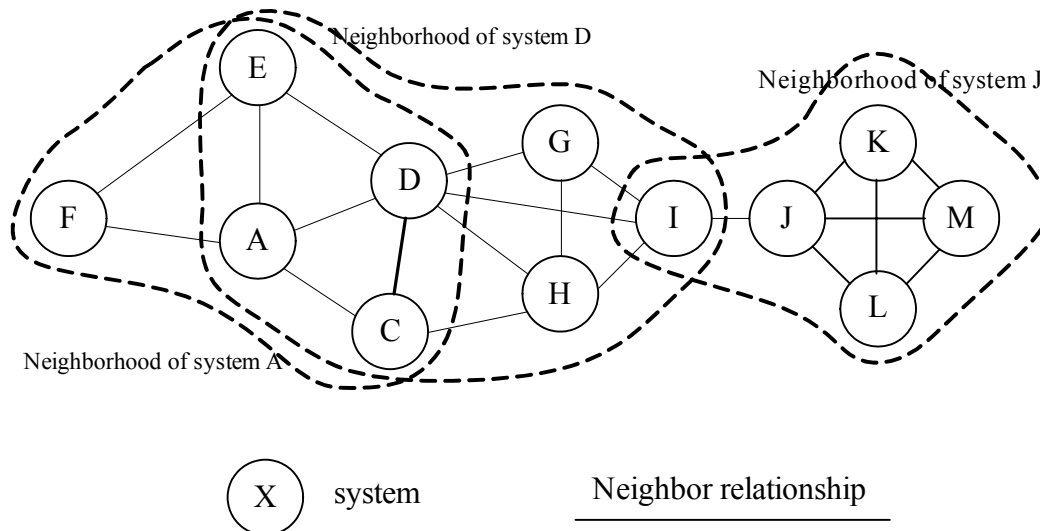


Figure h6—Concept of neighborhood

Community: A Community is composed of those systems, which coordinate to resolve their interference.

15.1.2 Mechanisms in WirelessMAN-CX

The basic mechanisms for achieving better coexistence are different for managed systems and for ad-hoc systems. It is recognized that the managed systems, generally deployed by operators, should receive a higher priority than the ad-hoc systems.

Three basic mechanisms for achieving coexistence are:

- MAC Frame Synchronization, including Tx and Rx intervals, for separating BS and SS transmissions and enable operation in synchronized zones;
- Adaptive channel selection, for finding a less interfered or less used frequency;
- Separation of the remaining interference in the time domain, by using coordinated scheduling and a fairness approach.

For inter-system communication, IP-level messages, MAC level messages and Cognitive Radio Signaling are defined at infrastructure and radio level.

Communication using IP-level messages is the most general case and is PHY independent. It allows distributed BS-BS communication as well as communication with a central database. The messages defined for such communication constitute the Coexistence Protocol.

The MAC-level messages are intended for systems using the same PHY profile. These messages may convey special information between the BS and its subscribers, or may send messages between systems. In the later case, the communication takes place during the Coexistence Messaging Interval.

The Cognitive Radio signaling uses elements of the existing PHY modes and allows simple communication between different systems. The radio signaling may be used to communicate with ad-hoc systems, or to indirectly transmit contact information for the IP network during the Coexistence Signaling Interval.

[These simple signals are selected in such a way, to allow in the future the extension of these procedures for communication with other systems, not belonging to IEEE 802.16 family.]

Different system parameters, including GPS coordinates and timing, may be shared between systems, through distributed communication between Base Stations grouped in a Coexistence Community.

The level of interference and the interference source may be assessed using the Radio Signatures and the interferer identification procedures.

Interference-free sub-frames are initially created based on the selection of one of two possible rules and control of system power. The Coexistence Protocol includes procedures, which allow the interference-free radio resource re-allocation. Some of these procedures use credit tokens and negotiations, such that the interference-free resources may be dynamically apportioned to support the changing character of the traffic.

The protocols and policies described in this chapter enable operation with reduced interference. The Coexistence Zone provides support at the MAC level for scheduling the interference-free sub-frames.

The following table shows a list of the coexistence mechanisms for WirelessMAN-CX. The mechanisms are classified with collaborated and non-collaborated. Collaborated means information exchanges between the systems in the mechanism, while non-collaborated means the systems do not exchange information in the mechanism:

Table h1—coexistence mechanism list for WirelessMAN-CX

Applicable Condition	1: with wired IP communication available	Yes				No			
	2: same PHY profile	Yes		No		Yes		No	
	3: in signaling/messaging range*	Y	N	Y	N	Y	N	Y	N
non-collaborative mechanism	dynamic frequency selection(DFS)6.3.15	✓	✓	✓	✓	✓	✓	✓	✓
	GPS timing recovery(GPS/UTC)15.2.1	✓	✓	✓	✓	✓	✓	✓	✓
collaborative mechanism	IP network message(CP message)15.5.2	✓	✓	✓	✓				
	coexistence proxy(CXPRX)15.1.5	✓	✓	✓	✓				
	coexistence signaling (CSI/ radio signature)15.3.1	✓		✓		✓		✓	
	coexistence messaging(CMI/CCD) 15.3.2	✓				✓			
	sub frame sharing(master sub frame)15.4.2	✓	✓	✓	✓	✓		✓	
	channel reallocation(ACS)15.4.1	✓	✓	✓	✓	✓		✓	
	Subframe Reallocation(ASFA)15.4.2.2	✓	✓	✓	✓	✓		✓	
	credit token15.4.2.5	✓	✓	✓	✓				

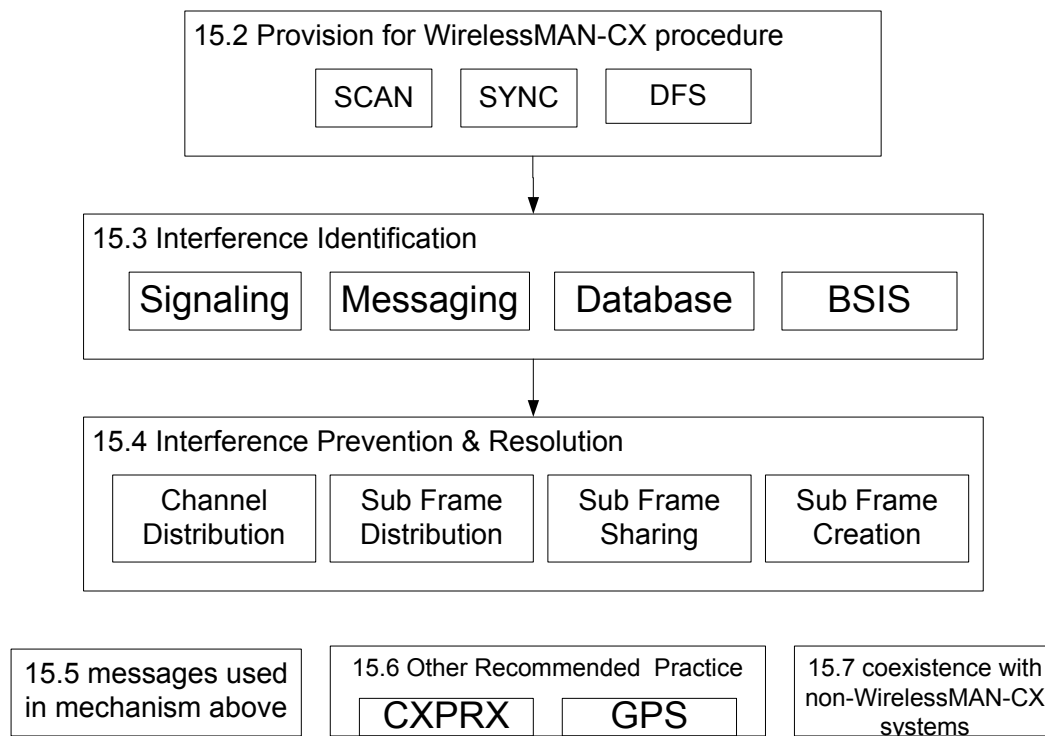


Figure h7—Summarization diagram of coexistence mechanism

15.1.3 Procedure flow in WirelessMAN-CX

15.1.3.1 Procedure flow for BS

In general, the coexistence detection, avoidance and resolution are performed in two stages, initialization stage and operating stage.

(1) *Initialization stage*

In the initialization stage the BSs may avoid the co-channel or adjacent channel interference by scanning the available frequencies (even those frequencies allocated for BS transmission only in FDD cases). But this method cannot avoid the hidden neighbor system problem, i.e. the BS that cannot be heard directly by the initializing BS but may have overlapping service coverage and interfere with the initializing system SSs. Thus, with the knowledge of coexistence neighbor topology the IBS can take the potentially hidden neighbor systems into account and can, therefore, avoid the possible interferences from those neighbors.

Alternatively, if the country/region database is not available in this stage, the initializing BS will use the initialization coexistence signaling interval (ICSI) to broadcast its contact information to its coverage area using its maximum power. In this way, SSs susceptible to the interference of the new BS will receive the signaling and forward the contact information to their serving BSs. After the neighbor BSs get the address via the SSs' reports, they will contact their new coming neighbor via the IP network and update the database on both sides. Thus, in an ad-hoc fashion, the procedure will solve the hidden neighbor problem by the SSs in

1 the neighbor systems. Therefore, using the information that the IBS has from its neighbors, the IBS can get
2 the information of the collaborative systems in a potential community.
3

4 If the IBS finds that there is no "free" channel, the information in the distributed database can be used to fig-
5 ure out which system it should negotiate with. The IBS may decide whether a free channel can be made
6 available by channel reallocation within the community, If the IBS can figure out an optimized channel dis-
7 tribution in the community, which enables every member in the community to occupy exclusive channels,
8 the IBS can contact the BSs in the community, which need to reallocate the channels (the candidate BS's)
9 and negotiate with them the reallocation. After receiving the confirmation by all candidate BSs, the IBS
10 should send a CP message to the candidate BSs to indicate the success, all the candidate BS should then con-
11 tinue operation on the new set of channels. Otherwise, if the IBS can't get a "free" frequency after the effort
12 of reallocation, the IBS should try to share a frequency with some of its neighbors.
13
14
15

16 Similarly to the channel allocation, the IBS will then first try to find a vacant sub-frame in the potential
17 channels using the information of the distributed database; if it fails the IBS will then try to vacate an exclu-
18 sive existing sub-channel by sub-frame distribution optimization, if supported. If an exclusive existing sub-
19 channel is not available, the IBS will then try to negotiate with the systems inside the community to create a
20 new sub frame. If all these attempts fail, the IBS will not be able to get any interference free resource for
21 operation. These procedures are described in Figure h 8.
22
23
24

25 (2) *Operating stage*

26 In the operating stage, the BS has SSs associated with it; however, until the operating system parameters are
27 determined, the co-channel or adjacent channel interference from LE BSs of different systems may still
28 occur due to the detection of interference from primary users (which may cause the neighbor BS to switch to
29 an interfering channel). Channel switching of coexistence neighbor systems or the entry of new coexistence
30 neighbor BS might make the community so crowded that there are not enough channels. If the LE BS finds
31 that there is no "free" channel at that moment, synchronous channel switching maybe executed, or the coex-
32 istence neighbor topology provides the guidelines of with whom it should negotiate to share the channel.
33
34
35
36 *[detailed procedures are to be defined]*
37

38 Figure h 8 shows the initialization procedures for the 802.16 LE BSs. Note, that the procedures that the BS
39 used to create a Master slot or channel switching are also applicable for the operating stage. The detailed
40 negotiation and update procedures are described in section 15.5.2 and 15.4.1.2.
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

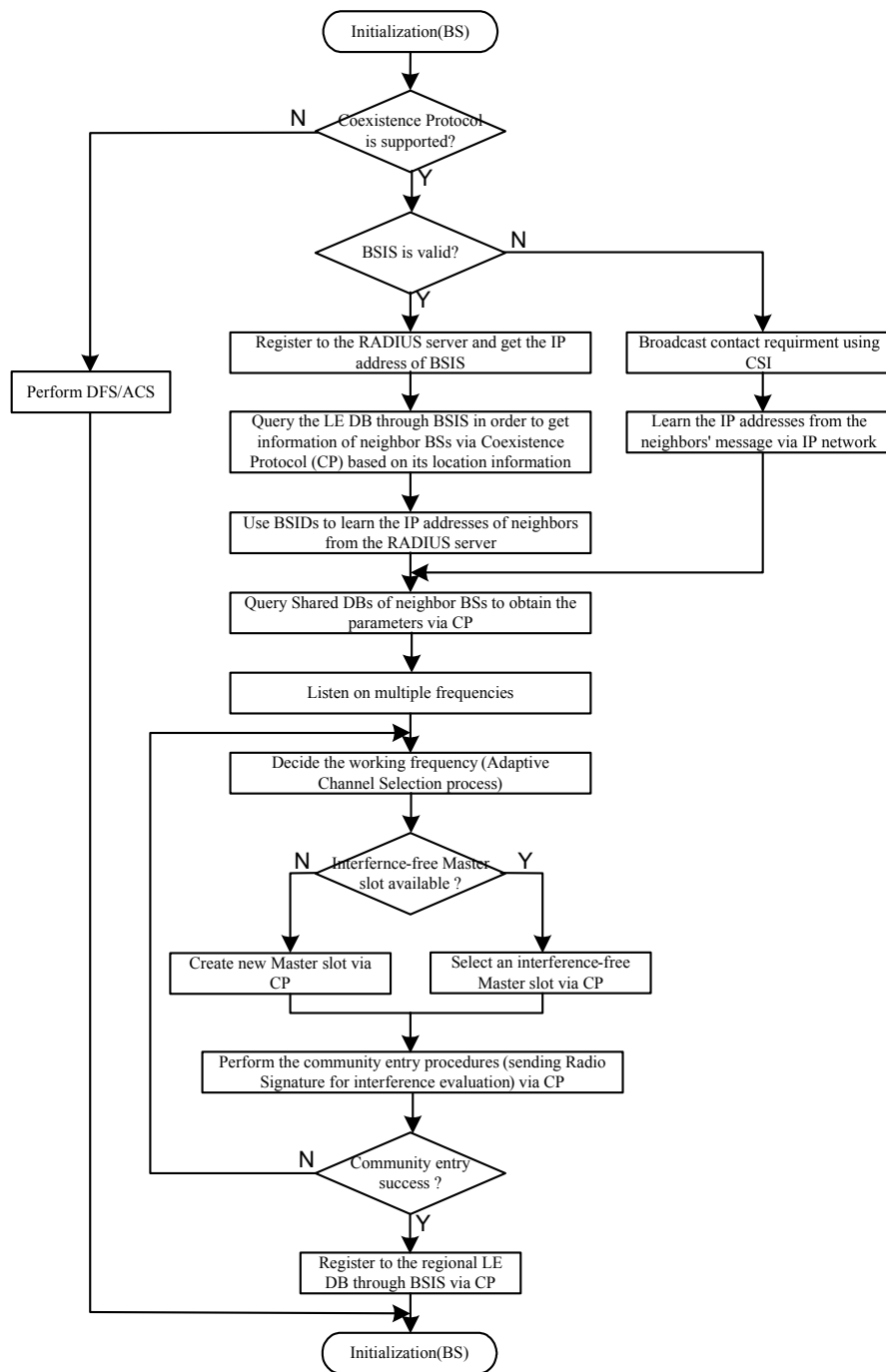


Figure h8—Initialization procedures — BS

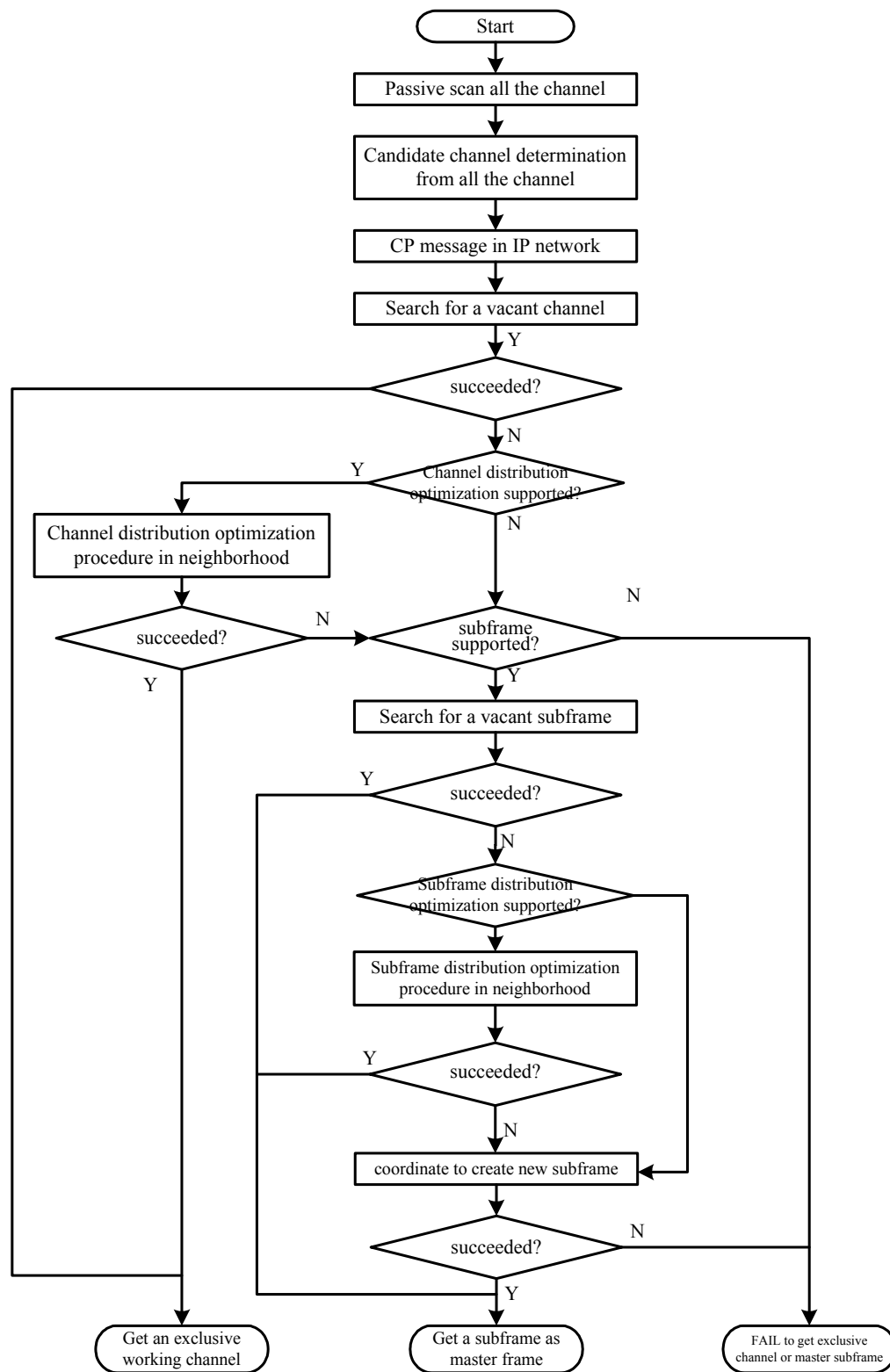


Figure h9—Initialization procedures - BS radio resource allocation

[Note: the following text needs further consideration]

- 1 — The first phase of the Community Entry is to determine the availability of the country/region data-
- 2 base. If the country/region Root RADIUS server is available and the database is valid(t.b.c: what
- 3 means valid?), the process queries the Root RADIUS server:
- 4
- 5 o Get the BSISs from the country/region Root RADIUS server;
- 6
- 7 o Read the data base maintained by BSIS via the Coexistence Protocol;
- 8
- 9 o Identify which Base Stations might create interference, based on the location information;
- 10
- 11 o The IBS learns the IP identifiers of those Base Stations;
- 12
- 13 Otherwise (the contry/region database is not available):
- 14
- 15 o A new BS uses the interference free slot to broadcast the message containing the contact
- 16 request and/or the cognitive radio signal transmitting the IP address
- 17
- 18 o An SS in the common coverage area, identifying the new BS signals, will forward the
- 19 information to its operating base station. using REP_RSP message
- 20
- 21 o The operating BS updates its database and sends feedback informationto the IBS, using
- 22 the IP network
- 23
- 24 o The new BS learns the IP identifier of the coexistence neighbor BS from the message
- 25 sent by the coexistence neighbor BS via the IP network
- 26
- 27 — Build the local image of the relevant information in the community BS's, by copying the info in
- 28 those BSs
- 29
- 30 — Listen on multiple frequencies
- 31
- 32 o Identify the level of interference on each frequency channel;
- 33
- 34 — Decide the working frequency (ACS – Adaptive Channel Selection process);
- 35
- 36 o If no interference detected on some channels, select one randomly as working channel;
- 37
- 38 o If interference detected by the IBS or the OBS system on all the channels, then the IBS
- 39 should decide whether an optimized channel distribution can allocate an exclusive channel
- 40 for each BS, including the IBS, in the community.
- 41
- 42 o If every BS in the community can be allocated an exclusive channel without interfering
- 43 with the others, that means default interference-free Master slot is available for this ini-
- 44 tializing BS.
- 45
- 46 — If available, select an interference-free Master sub-frame; if not, use the procedure for creating new
- 47 Master sub-frames;
- 48
- 49 — Search the Base Station data base for finding the BSs using the selected Master sub-frame;
- 50
- 51 — Request those Base Stations, by sending IP unicast messages, to listen during the BS_entry slot in
- 52 order to evaluate the interference from the new Base Station;
- 53
- 54 — Use the allocated slots for transmitting the “radio signature” at maximum power, maximum power
- 55 density and in all the used directions;
- 56
- 57 — Ask for permission of the Base Stations, using the sub-frame as Masters, to operate in parallel and
- 58 use the same sub-frames;
- 59
- 60 — If all of them acknowledge, the Base Station acquires a “temporary community entry” status; the
- 61 final status will be achieved after admission of the SSs;
- 62
- 63 — If no free Master slot sub-frame is found, use the procedure for creating new Master slots sub-
- 64 frames.
- 65

[Notes: the general procedure flow of **Operating stage** are to be described here]

15.1.3.2 Procedure flow for SS

The procedure of system and community entry for SS in WirelessMAX-CX is shown below:

- Start listening;
- Determine interference intervals;
- Assume that the interference is reciprocal;
- Build database for possible working slots and sub-frames;
- Wait for the Base Station community entry and start of operation;
- At BS request, send a list of the above identified time intervals;
- If an old Base Station will perceive interference from the new SSs, it will ask the new Base Station to find another sub-frame for that SS operation;

If the SS will sense interference, will request their Base Station to find another sub-frame for operation as Master.

15.1.4 Frame Structure for WirelessMAN-CX

There is two basic kinds of frame structure enhancement for the WirelessMAN-CX compare to other WirelessMAN systems. One enhancement (see 15.1.4.1.1) is for the interference identification between neighbor systems using time intervals within the frames. Another (see 15.1.4.1.2) is for interference prevention and resolution between neighbor systems operating in the same band using resource sharing in the time domain, defining multiple subframes in each DL period and UL period of the frame structure.

15.1.4.1 Frame Structure for interference identification

There are two types of time interval defined in WirelessMAN-CX, called coexistence signaling interval (CSI) (see 15.1.4.1.1) and coexistence messaging interval (CMI) (see 15.1.4.1.2). While CSI is time slots reserved periodically in some of the frame structure in cycles counted by frames, and CMI is longer intervals reserved periodically in absolute time in cycles counted by seconds. CSI is defined to carry signaling between neighbor systems which may use different PHY or profile, whereas CMI is defined to carry messages between neighbor systems which are using the same profile.

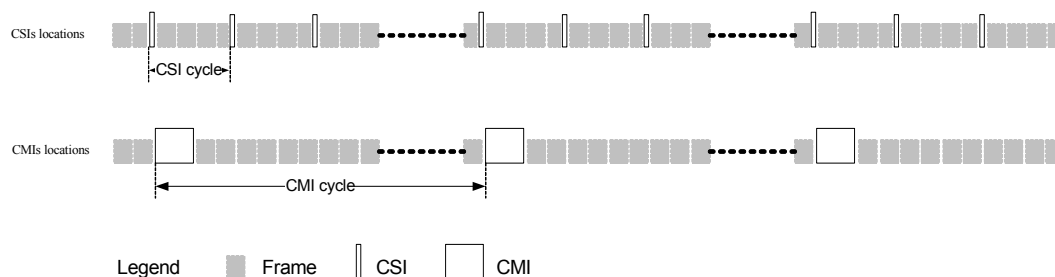


Figure h10—CSI and CMI locations in WirelessMAN-CX

[Notes: should describe what to do with these two different approach.]

15.1.4.1.1 Coexistence signaling interval

The CSI (Coexistence Signaling Interval) is a predefined time slot, in which the BS may contact its coexistence neighbor BSs through one or more coexistence neighbor SSs in the common coverage area. Every CSI has its number, called CSIN (Coexistence Signaling Interval Number). The sequence of CSINs is periodic with a period of $NCSI_{intv}$ (see below). For the Initializing BS (IBS), the correspondent CSI is called the ICSI (Initialization Coexistence Signaling Interval) and is used by the IBS to contact its neighbor Operating BSs (OBSs). By coordination with the other BSs, the IBS will get its OCSI (Operation Coexistence Signaling Interval), which is allocated only for this BS, and start the operating stage, hence releasing the ICSI for another IBS.

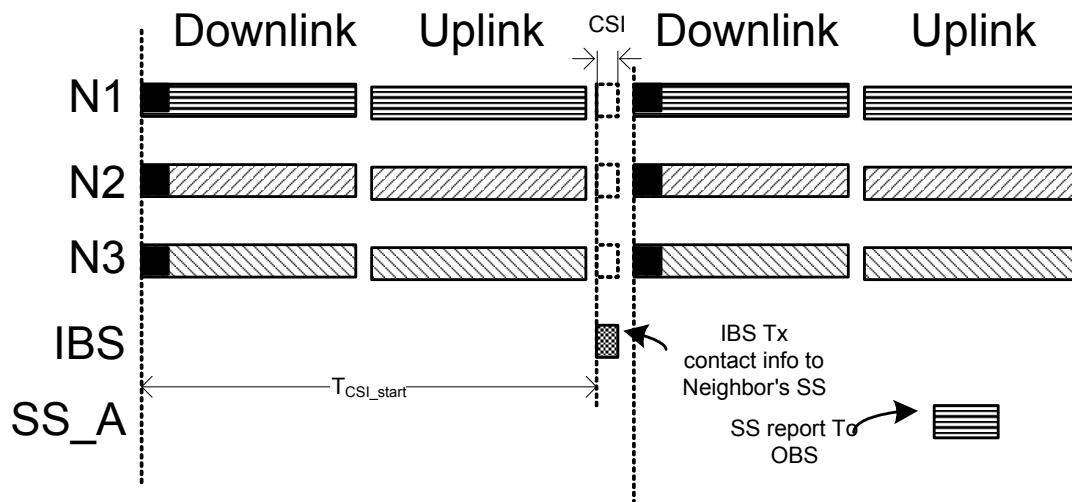


Figure h11—Timing of Coexistence Signaling Interval

In order not to change the structure of the downlink PDUs and to avoid the overhead of more preamble and gaps, CSI slots shall be located before the RTG/TTG in the TTD frame structure or before the preamble of the downlink frame in FDD frame structure. To unify the location in these two kinds of duplexing methods, in an FDD frame CSI slots shall be transmitted right before the preamble, and shall be located right before the RTG in a TDD frame.

The CSI/ICSI parameters need to be unified in a particular region, and to be well known by the BSs. So that each BS could know the exact time to transmit the broadcasting message in its initialization. The parameters include:

- $T_{CSIstart}$: CSI starting time from the beginning of the frame (ms)
- $T_{CSIdurat}$: CSI duration time (ms)

- $N_{CSIstart}$: CSI starting frame number frames
- N_{CSIntv} : number of frames in CSI interval

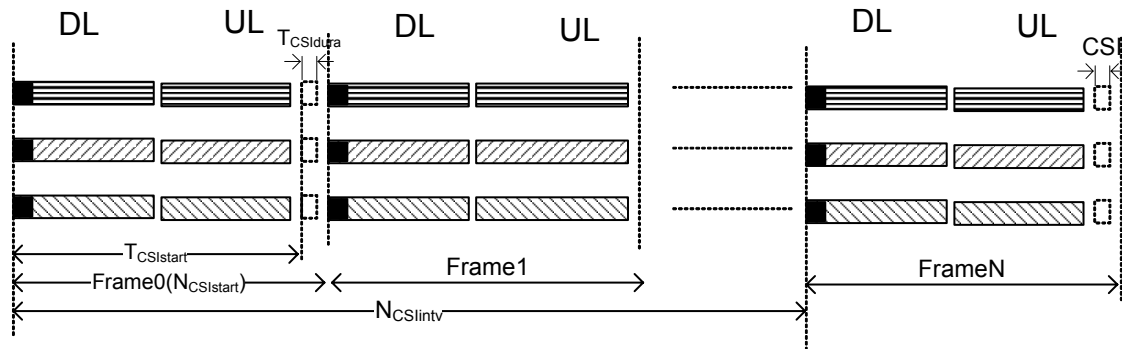


Figure h12—CSI parameters

- N_{ICSI_Cycle} : ICSI cycle counted in CSI cycles
- N_{OCSI_Cycle} : OCSI cycle counted in ICSI cycles

Assuming $N_{CSIntv} = 4$, $N_{ICSI_Cycle} = 4$, $N_{OCSI_Cycle} = 2$, an example of the timing indication is illustrated in Figure h 13. The first IBS come into an environment without occupation of any OCSI, using ICSI to broadcasting coexistence signaling, become OBS1 and choose OCSI1 as the OCSI occupied for its system. Afterwards IBS2 starts up and uses ICSI to broadcasting coexistence signaling, finding its neighbor system of OBS1, and find OCSI1 occupied by it, IBS2 choose OCSI2 as its OCSI for its system and become OBS2 after the initializing phase. (also see 15.3.1.1.1) For IBS2, the occupation of OCSI1 by OBS1 can be aware by detected signaling from the system of OBS1, or to be informed by the CP message as the feedback of the IBS2's broadcasting signaling from OBS1's system.

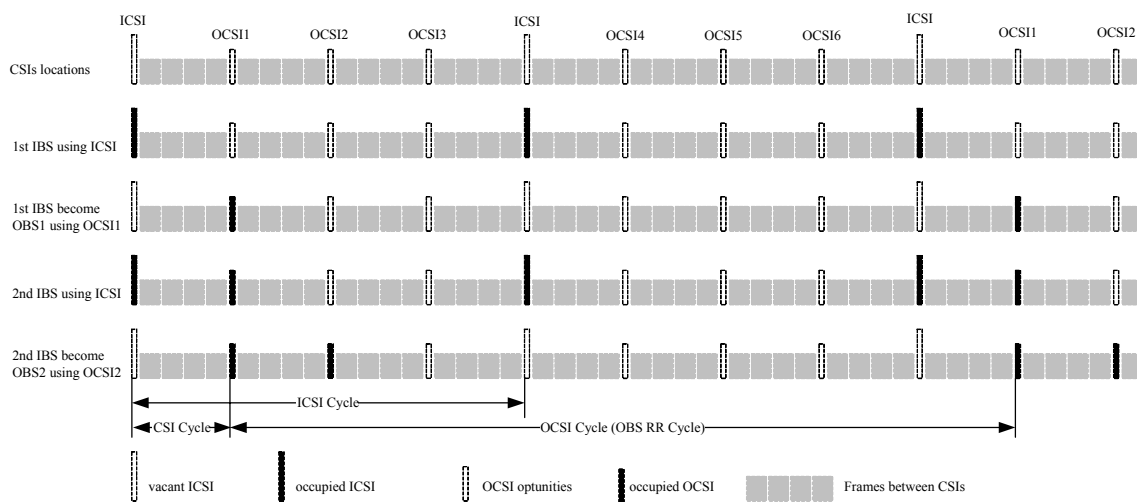


Figure h13—ICSI/OCSI occupation and timing example

15.1.4.1.2 Coexistence messaging interval

A Coexistence Messaging Interval (CMI) is a reserved physical frame used for the coexistence protocol signaling purposes. The CMI is used with systems having the same profile (15.2.5) and synchronized MAC frames. The position of the CMI and the subsequent IEEE 802.16 MAC frames are synchronized to a GPS timing signal (15.2.1). Furthermore, the CMI are identified by UTC time stamps (). For example, the beginning of the first CMI is at HH:MM:00 UTC, the second CMI is at HH:MM:06 UTC, etc. The beginning of every CMI is specified by a UTC message (time stamp) (Figure h 14).

The CMI is used by WirelessMAN-CX systems (BSs and their SSs) to mediate their co-channel coexistence. The CMI will be an opportunity for systems (BSs and their SSs) to indicate to other systems (BSs and their SSs) the extent of the interference they can cause; newly arriving interfering base stations (IBS) will use the CMI to make themselves known to established communities of operating base stations (OBS). Newly entering SS will make their presence known when they are detected by base stations to which they are not associated (see Section **TBD**). Sporadic interference from BS or SS will also be detected by the same process.

A Coexistence Community can consist of a maximum of 9 systems (**TBD**). Each system claims a unique CMI by a process outlined in Section 15.3.2.3. There are a total of 10 CMI which repeat every minute (**TBD**), but since CMI_ID 54 is reserved for noise measurement and foreign system identification purposes, there are only 9 CMI available to the Coexistence Community. A system must broadcast its BSD and SSURF messages once a minute on its CMI; when it does this all other members of the Coexistence Community remain silent and monitor to detect the extent of the interference that is caused by this.

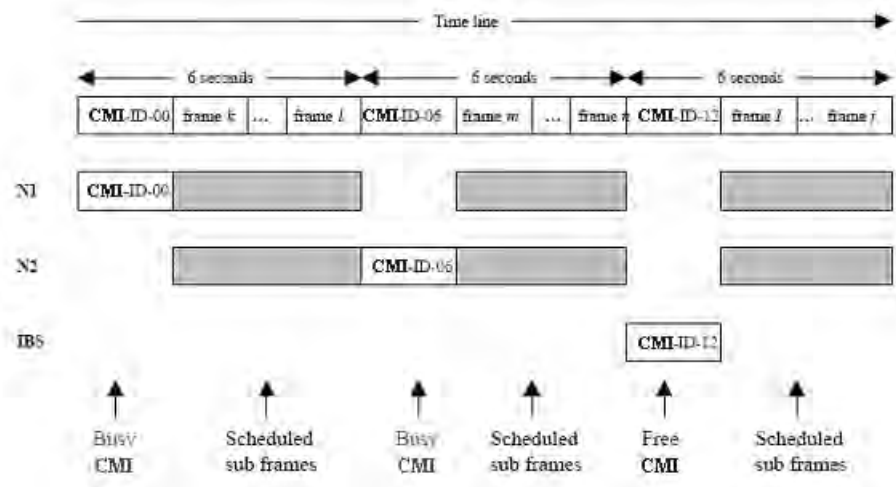


Figure h14—CMI Timing

15.1.4.2 Frame Structure for interference prevention & resolution

In order to isolate the interference in the time-domain are provided repetitive MAC frame structures, which include Master and Slave sub-frames. During a Master sub-frame the data reception will not be affected by harmful interference and the data transmission will be allowed to use the maximum available powers. The activity during the Slave sub-frames is restricted, such that will not cause interference to systems using their Master sub-frame.

The assignment of different MAC sub-frames as Master/Slave sub-frames is based on the observation that in real deployment (see Figure h 15) not all the data transmission connections create or are affected by interference. The overlapping radio systems create different interference zones based on the spatial distance between transmitters and receivers. As an example, system 1's SSs in Zone A are interfered by the BS of system 2 and vice versa.

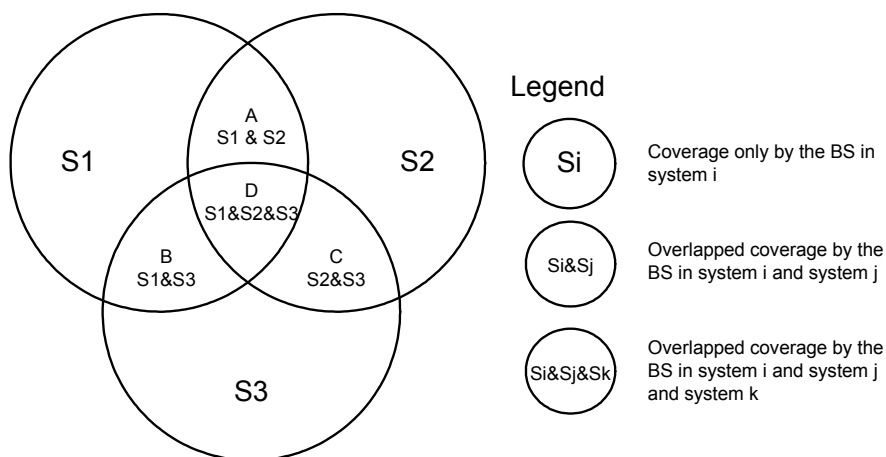


Figure h15—Interference due to overlapping systems

Operationally, a component of any of the three systems in Figure h 15 may be in one of the the following situations:

- o Zones S1, S2, S3 in which the systems 1, 2 and 3 do not interfere and the traffic can take place in parallel, using the same common sub-frame;
- o Zone A: systems 1 and 2 interfere;
- o Zone B: systems 1 and 3 interfere;
- o Zone C: systems 3 and 2 interfere;
- o Zone D: systems 1 and 2 and 3 interfere.

In order to avoid the interference, the traffic in the interfering areas A, B, C and D shall be scheduled in such a way that the interfering connections will not operate in the same time. A sub-frame called Master subframe is allocated to each system (see Figure h 16), such that the interfering systems have Master sub-frames which do not overlap.

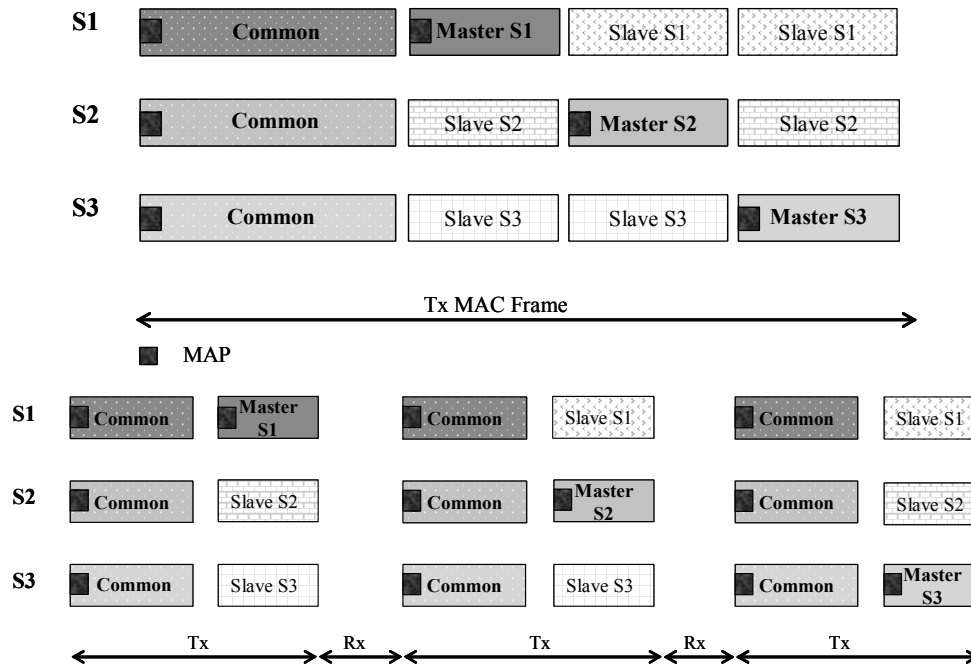


Figure h16—examples of WirelessMAN-CX Subframes

The system specific Master sub-frames can be scheduled during same MAC Frame (Figure h 16-upper part) or in consecutives MAC Frame (Figure h 16 - lower part). They should start with a private MAP, scheduling the traffic for the users that are affected by harmful interference, like those in the overlapping areas S_i & S_j in Figure h 15. The isolation of interference is achieved by the allocation of different transmission/reception times for the traffic in the overlapping areas, such that each system will have its own interference-free "Master" subframe.

However, the diagram of Figure h 15 is conceptual and does not necessarily refer to specific geographical layout. Being adaptive, the WirelessMAN BS can control the working conditions of each SS using power control, sub-channel allocation, sectorization and beamforming. Power and interference can also be traded off for working rate, thus a SS of system 1, for example, can be considered to be interfered by system 2 for a given rate, while the same level of interference could be considered acceptable for a lower operation rate. This particular SS can operate in a setting where it does not interfere with other systems, while for another frame it can be operated with such parameters that it does interfere with other systems and then it will be allocated time in the zone where system 1 is the master. In the latter case it will probably be able to operate at a higher data rate than the first.

The examples in Figure h 16 show three systems having the Master sub-frames scheduled in one long MAC Frame or in three consecutive short MAC Frames.

The initial frame allocation is defined by a set of possible rules (see 15.4.2.1.2). The change of the rules is supported by the Coexistence Protocol(see 15.5) and the token protocol(see 15.4.2.5). See more details in 15.4.2.1.2.

15.1.5 Architecture for WirelessMAN-CX

The architecture for Radio Resource Management in the context of this clause it is a distributed one and allows communication and exchange of parameters between different systems. A system consists from a base station and its associated subscriber stations and its coexistence proxy.

Every base station includes a distributed radio resource management (DRRM) entity, to apply the spectrum sharing policies, and a data base (DB) to store the shared information regarding the actual usage and the intended usage of the radio resource.

A subscriber station may include an instance of DRRM, adapted to SS functionality. Figure h 17 illustrate the System Architecture .

[Editor's note: the following figure shows the CX proxy usage is optional, text modification may needed accordingly.]

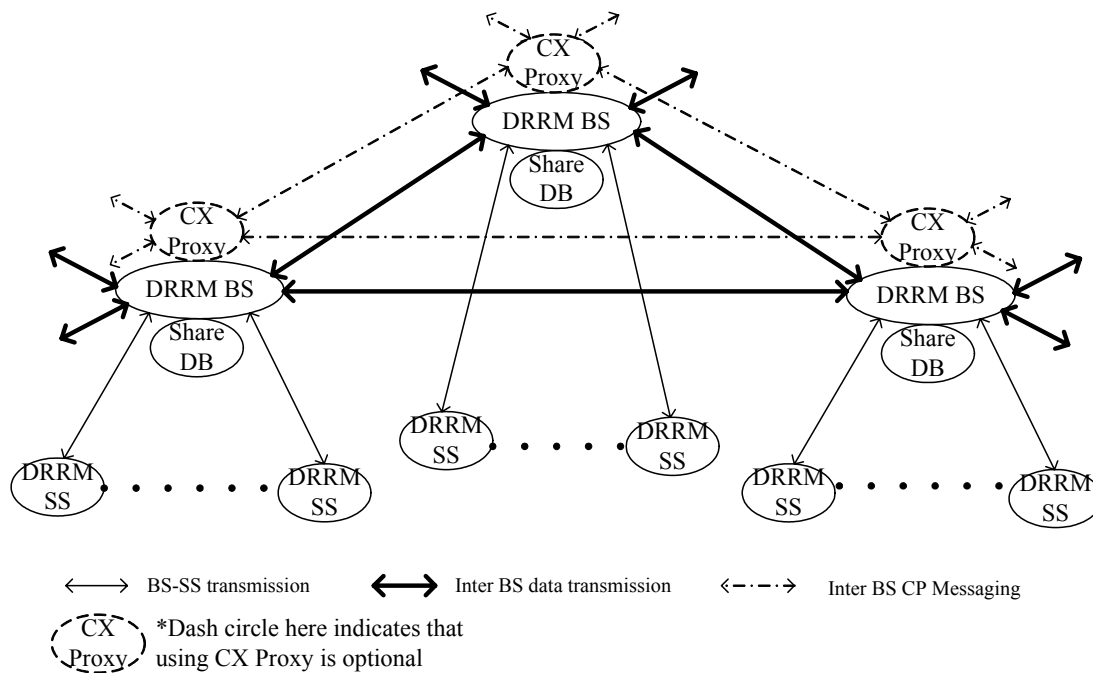


Figure h17—System Architecture

Figure h 18 shows the IEEE 802.16 LE inter-system communication architecture:

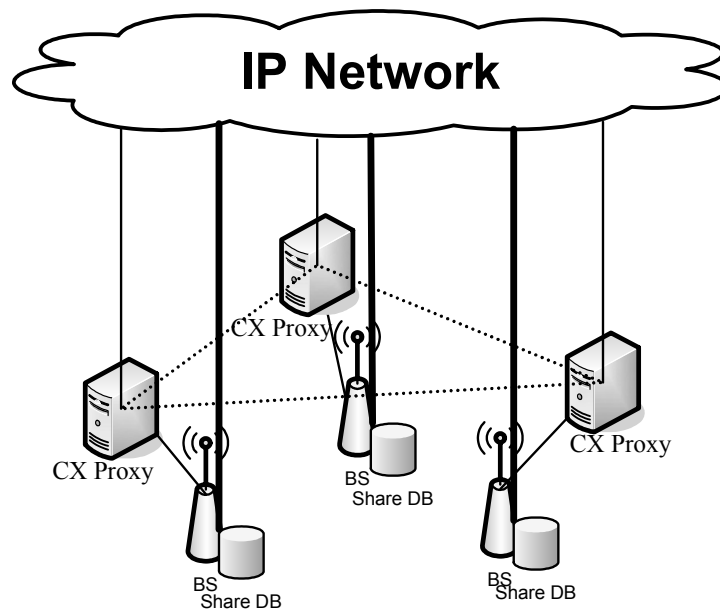


Figure h18—Inter-system Communication Architecture

General architecture includes the components operating over IP-based network:

The coexistence proxy of every base station maintains the mapping of the IP address and the BSID of their serving BSs. All the CP messages between the different systems which should be sent and received via their coexistence proxies instead of directly between the base stations. So the IP address will not be known outside the system. The coexistence proxy will forward the CP messages for the base station.

Inter-system communication

The inter-system communication consists of:

- Inter-system *messages*
 - o Base Station to/from Base Station
 - o Base Station to/from Subscriber Station to/from a foreign Base Station; the subscriber Station is used as a relay of the signaling, if the two Base Stations are hidden from each other
- Open access to the DRRM Data Base (*optionally via a coexistence proxy*):
 - o To read the parameters of the hosting Base Station
 - o To request changes of the hosting Base Station operating parameters.

Coexistence Protocol

In order to obtain a coexistence neighbor topology, the Base Station accesses the database(see 15.3.3.2), registers to peer, negotiates for Shared RRM etc. using the Coexistence Protocol (CP). Figure h 19 describes the coexistence protocol protocol layering for WirelessMAN-CX systems. The diagram indicates that the

DRRM, the Coexistence Protocol and the Shared DB belong to the CX Management Part located in management plane and the CP messages (see 15.5.2) will be exchanged over an IP network. Thus, the DRRM in the CX Management Part uses the Coexistence Protocol to communicate with other BSs and with the Regional LE DB over the CP SAP in order to interact with the MAC or PHY. Figure h 20 illustrates the CX BS architecture with the Coexistence Protocol. The gray area indicates that there is no connection between blocks. The Distribution System Medium (DSM) is another interface to the backbone network which carries the ip communication. Note that this layering diagram is only for reference. Similarly, Figure h 20 also illustrates the BSIS layering protocol, which is co-located with the regional CX database. The service primitives are described in [Appendix? t.b.d.] A BS uses the Coexistence Protocol to perform the coexistence resolution and negotiation procedures.

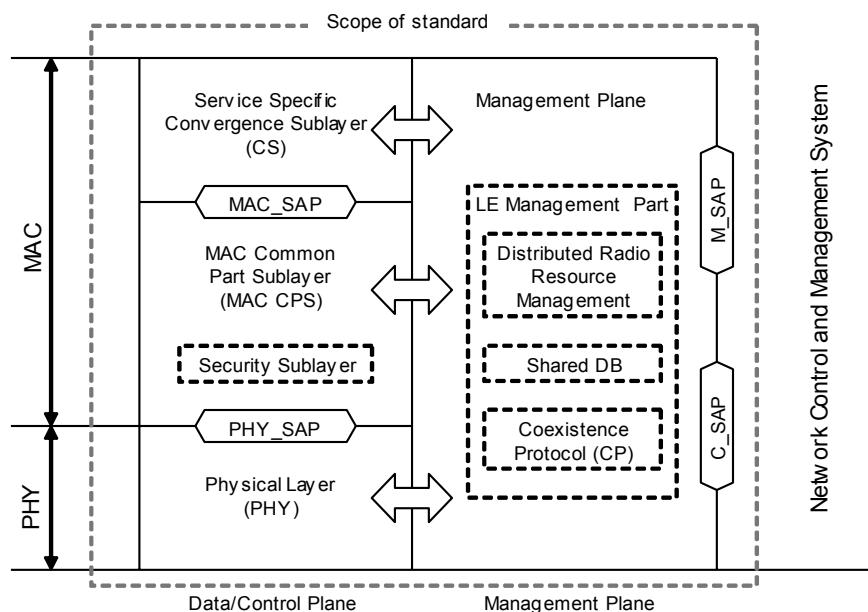


Figure h19—WirelessMAN-CX BS Protocol Layering Model

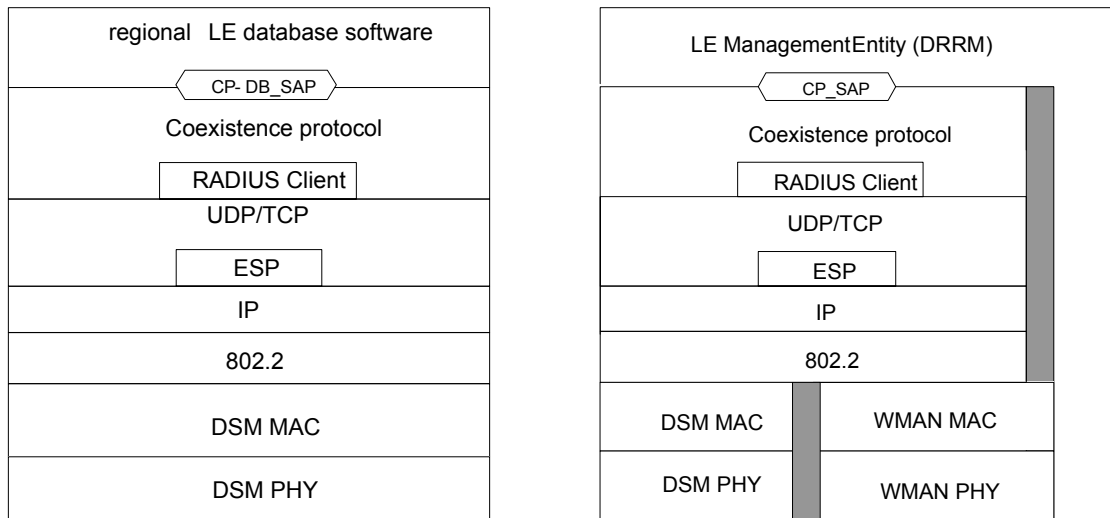


Figure h20—BSIS and CX BS layering diagram with the Coexistence Protocol

Coexistence Proxy

Every BS shall use its coexistence proxy to exchange CP messages while it sends/receives signaling containing the IP contact information over the air, so that malevolent interceptors will not know the real IP address of the BSs from the signaling over the air. The coexistence proxy should have a stand alone physical port and an IP address to connect to the internet using either direct link or an internal interface. The coexistence proxy could be a module of the BS or a stand alone server.

A coexistence proxy can also be optionally used to forward the CP messages between BSs when the IP address of the BS is not transmitted over the air, so that the proxy will act as an agent between the BSs and other BSs and terminals in the internet. By using the coexistence proxy, all the BSs know other BSs' coexistence proxy's IP address instead of their actual IP address, and contact them only via coexistence proxy and the BSID information. In order to prevent various attacks from the internet, the proxy could utilize various approaches to protect the BSs without affecting the data services of the BSs. *[The proxy could limit the forwarding bandwidth from one IP address or to one BSID. The proxy could qualify or block the messages using various approaches.]*

[Note: detail description of the Coexistence Proxy deployment could be written in 15.6 Recommended practice for WirelessMAN-CX.]

Using centralized server

The *Base Station Identification Server* (BSIS) acts as an interface between 802.16 LE BSs and the regional LE DB which stores the geographic and important operational information, e.g. latitude, longitude, BSID etc., of the LE BSs belonging to the same region. It converts the actions carried in PDUs received from the 802.16 LE BSs to the proper formats, e.g. SQL (Structured Query Language) string, and forwards the strings to the regional LE DB, which can be any available database software. BSIS converts the query results from the regional LE DB to the proper format, e.g. TLV encodings, and replies to the requested BSs. Figure h 21 shows the general architecture of inter-system communication across 802.16 LE systems. BSIS acts as a peer of 802.16 LE BSs in this architecture. The BSID of regional BSIS is well known among the 802.16 LE

systems within certain domain. The messages exchanged between the LE BSs and the BSIS will be revealed in the next section.

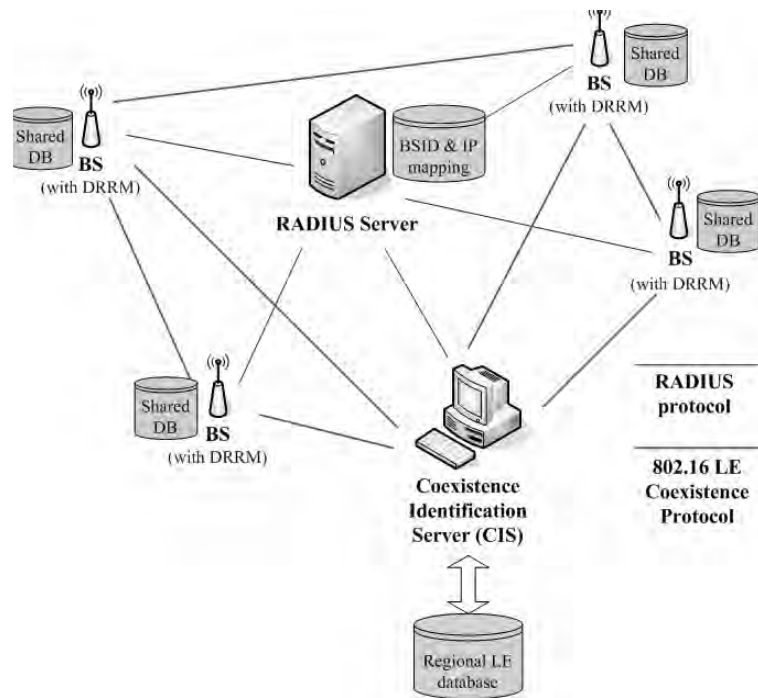


Figure h21—using centralized server

Figure h 22 explains how one IBS discovers its coexistence neighbor BSs. The new entry BS-5 uses its GPS coordinates (x_5 , y_5) and its maximum coverage radius in LOS, R_m , at allowed maximum transmission power. A BS is a *potential* coexistence neighbor BS of another BS if:

- In co-channel operation the LOS maximum coverage areas of the two BSs, calculated for the allowed maximum transmission power overlap. As depicted in Figure h 22, the regional LE DB will return BS-1, BS-2 and BS-3 as the *potential* coexistence neighbor BSs of the new entry BS.
- In first or alternate adjacent channels operation, the BS should consider the net filter discrimination of the received power, corresponding to the actual operation channels of different Base Stations.

Once a LE BS has learnt its *potential* coexistence neighbor topology from the regional LE DB, it evaluates the coexisting LE BSs and identifies which BSs might create interference. The Adaptive Channel Selection will select the actual operating frequency, such that the probability of interference will be minimized. Each LE BS tries to form its own community, by including the coexistence neighbor BSs that create interference to the associated SSs. The members of a community will change when the working frequency of any BS changes or a new interfering coexistence neighbor BS comes in.

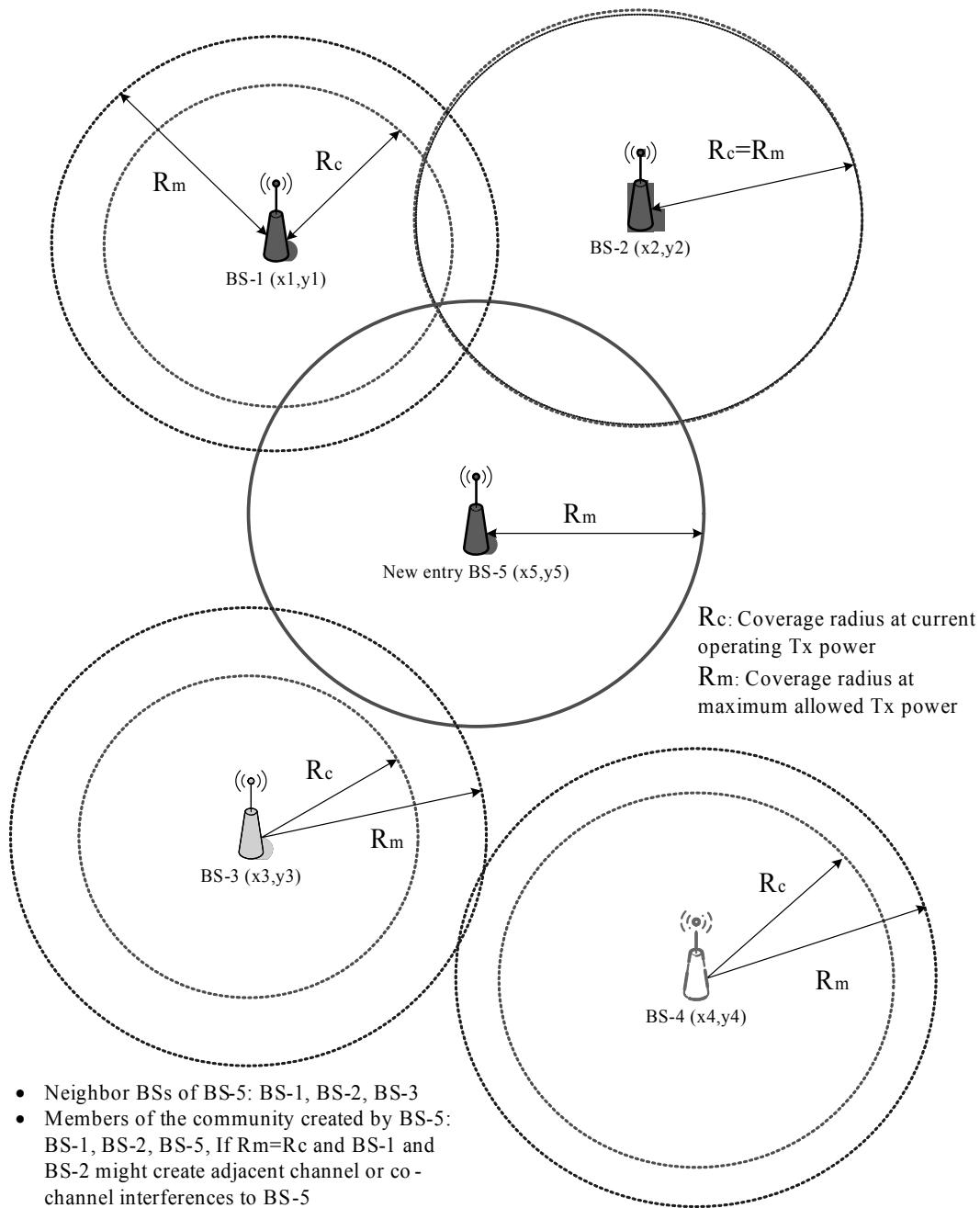


Figure h22—WirelessMAN-CX neighbor BSs discovery and definition of coexistence neighbor and community

Within a regional LE DB, a LE BS can construct its coexistence neighbor topology and acquire the IP addresses of its coexistence neighbors securely.

[Note that the interface between BSIS and regional LE DB is out of scope.]

Mixed-PHY Profile communication

1 In the case of different PHY Profiles the coexistence communication will be done at IP Level. Every Base
2 Station needs to know the IP address of the DRRM of the Base Stations in its area, by provisioning or/and by
3 using a regional data base approach or/and by using cognitive radio signaling.
4

11 **15.2 Provision for the WirelessMAN-CX procedure**

14 Before starting the WirelessMAN-CX procedure for interference identification and interference prevention
15 and resolution, we need some provision within WirelessMAN-CX systems.
16

18 **15.2.1 Synchronization of the WirelessMAN-CX systems**

20 All the base stations forming a community of users sharing a common radio spectrum will use a common
21 clock to synchronize their MAC frames. The common clock will be available to all outdoor WirelessMAN-
22 CX systems.
23

25 Such a clock can be provided by global navigational systems such as GPS (ANNEX B) or can be distributed
26 by the Control Channel. Every BS, will as a first step upon activation, ensure the derivation of the common
27 system clock.
28

30 Systems, which do not see a global navigation system satellite, will synchronize their BS with the operating
31 WirelessMAN-CX systems. Such systems shall check their synchronization status every 60sec.
32

34 **Network Time Interval and MAC Frame start**

36 All synchronized WirelessMAN-CX base stations will either synthesize or derive a 1 pps clock broadcast by
37 a global navigational system or other means. The 1 sec duration is called the Network Time Interval (NTI).
38 The rising edge of the 1 pps synchronization pulse will be considered as the start of the NTI and of the
39 WirelessMAN-CX MAC Frame. The 1pps pulse will have a stability of +/- 1 microseconds, as measured
40 from rising edge to rising edge.
41

44 **Granularity of the NTI**

46 The NTI will be comprised of 1000 1 Millisecond slotsNTI_S unit that will be used by both TDD and FDD
47 systems to negotiate times and durations of co-channel occupancy. Negotiation for access time to common
48 spectrum will be specified in terms of the NTI_S unit 1 millisecond units. Occupancy times will be specified
49 in terms of time from the beginning of the NTI and in terms of negotiated number of NTI_S unit1 millisecon-
50 d intervals.
51

54 **UTC Standard Time**

56 The common clock specified in section15.2.1 will provide a Universal Coordinated Time (UTC) signal to
57 all WirelessMAN-CX systems, making all systems synchronized to this referenced time stamp. Wireless-
58 MAN-CX base stations will use the UTC time standard for coordinating and identifying specific NTI inter-
59 vals. See further explanations in 15.7.
60

61 *[Note: detail description of the GPS deployment could be written in 15.6 Recommended practice for WirelessMAN-*
62 *CX.]*
63

65 **Ad-Hoc systems and systems not able to recover the GPS clock**

There is a category of systems which either do not include the needed hardware for GPS synchronization, either are installed in such a way that the satellite visibility is limited or obstructed.

In order to synchronize the operation of such systems, systems which are synchronized by a GPS receiver shall send, during the reserved Control slots, radio signalling as defined in 15.3.1.2 to indicate the start of a Control slot and to mark the Control slot starting the sequence. The Header signal will be used to mark the start of a Control Slot. In the first Control Slot of a sequence, this signal will be followed, after a guard interval with the length of 1/8 from the FFT duration, by the Rx end and Tx end signals, separated by the same guard time. Systems which are synchronized by a system using a GPS synchronization will mark the second Control slot of a sequence in a similar way, by sending the sequence of Header, followed by Rx start and Tx start signals.

15.2.1.1 Synchronization using the Control Channel

The first two time-slots of the Control Channel, scheduled during the DL MAC sub-frames and during the UL sub-frames are used for the synchronization. A synchronization signal will be placed at the start of the Control time-slot, in the following way:

- BS synchronized by GPS will use the first DL slot
- BS synchronized by another BS will use the 2nd DL slot
- SS associated with a BS which is synchronized by GPS will send the synchronization signal in the first UL slot, if instructed by the BS to do so;
- SS associated with a BS, which is synchronized by another BS, will send the synchronization signal in the 2nd UL slot, if instructed by the BS to do so.

The synchronization signal is a sub-set of the radio signals defined in 15.4.3.4, Table h 7. The Table h 2 indicates the sequence of the Radio signals to be used for marking the slots of the Control Channel.

Table h2—Sequence of radio signals sent in the Control Channel

	1st signal	2nd signal	3rd signal
1st DL slot	Header	Rx_end	Tx_end
2nd DL slot	Header	Rx_start	Tx_start
1st UL slot	CSI_Start	NACK	CSI_Continuation
2nd UL slot	CSI_Start	Tx_end	Rx_start

The interval between the radio signals is 1/8 of the symbol length.

The first 4 slots of the Control Channel are shown in the Figure h 23.

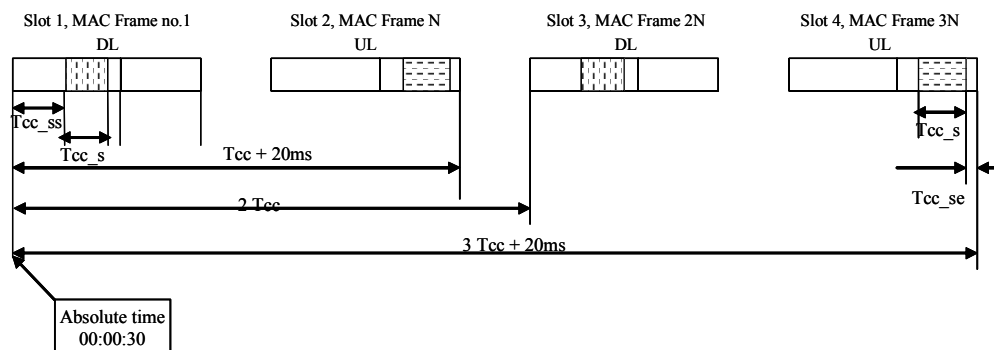


Figure h23—The first 4 slots of the Control Channel

The positioning of the DL/UL Control Channel slots is done in a way that will keep their DL/UL characters for a MAC Frame duration of 5, 10 and 20ms. The interval between two consecutive DL slots is $2T_{cc}$ and is defined in Chapt. 10.5.2.

15.2.2 Scanning before interference identification

The IBS should monitor candidate frequencies during the selection of a working frequency. If the interference level is greater than the detection threshold, which is the required strength level of a received signal within the channel bandwidth, the channel is considered as an interfered channel.

15.2.2.1 Acceptable $S/(N+I)$

15.2.2.2 Acceptable time occupancy

15.2.3 Power Control

Every system will strive to reduce its transmit powers during the common sub-frames to the minimum, such that the $C/I+N$ will be sufficient to allow the operation at the minimum common rate, considered as QPSK1/2 for all the 802.16 systems. An exception from this rule is possible only when a system is operating during its interference-free period. The power control mandatory algorithm will be defined in chap. *[t.b.c.]*

15.2.4 Dynamic Frequency Selection – DFS

15.2.4.1 Frequency selection for regulatory compliance

15.2.5 Same PHY Profile

For systems using the same PHY Profile in this standard, the profile elements are:

- Mandatory channel spacing for LE system in[tbd.] MHz will be[tbd.] MHz;
- PHY mode option:
 - o WirelessMAN-OFDM (256 FFT points)
Mandatory profiles for operation in the LE 5725-5850 MHz band will be:
 - profM3_pmp,profP3_10,profC3_23,TDD,profR13
 - o WirelessMAN OFDMA 2k (in future 128, 512, 1k) FFT points
 - o *WirelessMAN SCA*,

the inter-system communication will be undertaken using messages over the air, as specified in this standard.

15.3 Interference identification and basic connectivity creation

In order to coordinate with the neighbor systems, a system should be aware of its interference situation and identify the victims and sources around it. Based on this, the systems can proceed with further Interference Prevention (section 15.4) procedures.

When able to exchange information between them, the WirelessMAN-CX system and the neighbor systems, may use collaborative mechanisms to become aware of the identity of the interferer, otherwise it will only be possible to use non-collaborative mechanisms (15.1.2) and procedures to coexist, such as interference power detection, DFS and so on. This section defines the identification procedures based on information exchange using signaling and messages.

The BS in the system takes responsibility for gathering and maintaining all the interference information of the system and determines the resources allocated for its own system use. The interference identification is determined by the power detection, CSI signaling decoding, CMI messaging receiving and CP messages received.

All the corresponding interference information should be stored in the distributed database [*as SS and BS interference tables*] for each system (see 15.3.3.1) and maintained regularly. The distributed database has the information related to all the systems in the neighborhood or in other communities.

The Interference information gathering approaches include:

- 1) Using interference power detection to measure the basic interference situation in the candidate channels
- 2) Signaling decoding in candidate channels (15.3.1.1.1)
- 3) Receiving messages in candidate channels
- 4) Exchanging system information using CP message in the IP network

IP address information may be acquired by the following methods:

1) The initializing BS uses a configured IP contact list, the list is either read from a regional centralized server or from an off-line address list;

2) By decoding the contact information from the signaling/messaging sent by the neighbor systems.

The details of the CP message exchanged in the initializing procedure is shown in section 15.5.2.

The interferers will be identified by their radio signature, for example a short preamble for OFDM/OFDMA cases. The radio signature consist of:

- Peak power
- Relative spectral density
- Direction of transmission.

Every transmitter will send the radio signature during an interference-free slot. The *time position of this slot (frame_number, sub-frame, time-shift)* will be used for identification.

The transmitted power of non-interfering radio transmitters using a Master sub-frame will be known from the BS data base, indicating their power attenuation relative to the radio signature, for every used sub-frame.

15.3.1 Coexistence signaling mechanisms

The radio signaling mechanisms are defined in order to provide the basic connectivity information between neighbor systems using different PHY profiles.

15.3.1.1 Coexistence Signalling Interval

[Note: the following 3 sections are subject to further discussion and comment by IEEE 802.16 PHY experts. Energy Keying in CSI applications needs clarifications on its PHY Performance issues and its deemed compliant with the current standard.]

15.3.1.1.1 CSI scheduling

Downlink CSI is used by the BSs to broadcast signaling to the neighbor systems. These signals are used for interference identification and resolution. In order not to collide with the other neighboring interferers, the coordinated community should prevent neighboring BSs from using the same CSI.

There is one ICSI for IBS in an ICSI cycle, in the example figure below, each ICSI cycle has 4 CSIs and CSIN 0/4/8/12 indicate the CSI numbers of the ICSI. The other CSI is left to the OBS as OCSI, as shown in Figure h 24. Every OBS needs to obtain an OCSI allocation in one OCSI cycle, which is formed by multiple ICSI cycle so that an IBS can get more opportunities than OBS. There are 4 ICSI cycles inside one OCSI cycle and 4 CSIs in each ICSI cycle in the example, so that there are 4 ICSI intervals for the IBS and 12 intervals for up to 12 OBSs.

Notice that the CSI allocation MAP should indicate all the CSI allocation in the uncoordinated channel as unusable. The uncoordinated channel information can be gathered in the DFS procedure or by the failure of coordination procedure in the interfered channel.

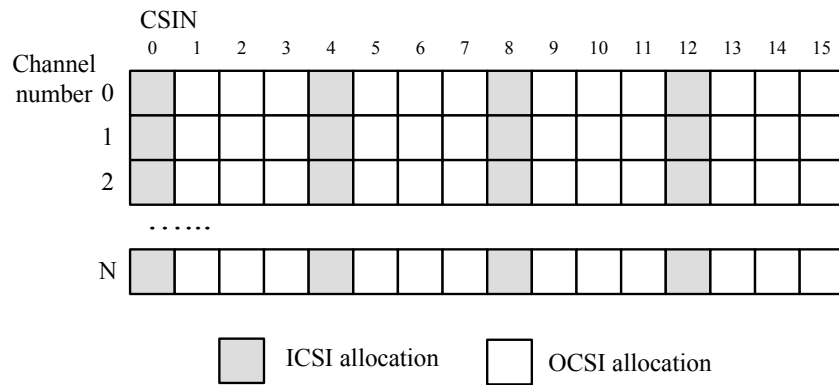


Figure h24—format of ICSI/OCSI allocation MAP

In the initialization phase of a BS, before the BS has an OCSI allocation, the BS should use ICSI to advertise itself at every candidate channels sequentially one by one. The neighbor OBS will then send their current OCSI allocation and current sub frame allocation to the IBS using CP message. After the IBS chooses the working channel for its radio link, the IBS shall choose a vacant CSIN for OCSI in this channel and inform other neighbors about this choice. Then, this BS will start using this OCSI allocation as its exclusive CSI allocation.

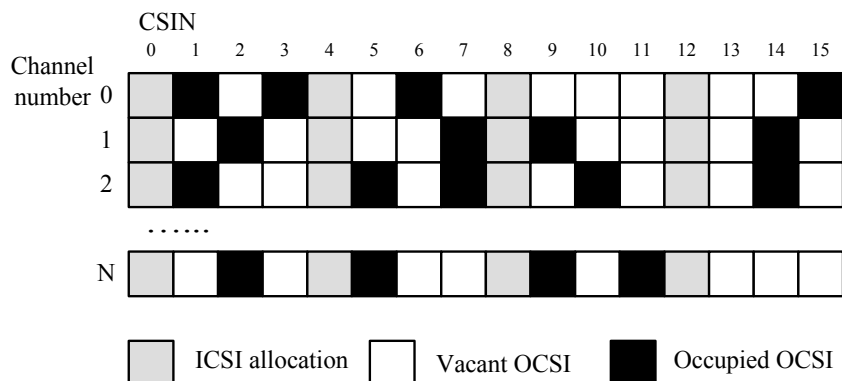


Figure h25—Example of CSI allocation MAP in one BS's database

Figure h 25 illustrates an example of the CSI allocation MAP of one BS during his initialization phase by collecting the CP message information from its neighbors. Assume this BS chooses channel 0 as its working channel, it can then choose any one of the CSIN 2,5,7,9,10,11,13,14 as its OCSI allocation number. Every BS will have its own CSI allocation map indicating the current situation of CSI occupancy by the neighbors in the working channel and potential neighbors in the potential working channel. The CSI allocation MAP table of potential working channel will be used when the BS moves to another channel, however, the switching BS shall acquire the new CSIN for the new channel. The CSI allocation MAP of the BS should be updated in time when any changes are informed by its neighbors in the working channel and potential neighbors in the potential working channel.

In the OCSI mapping table, every neighbor in the working channel or potential neighbor in potential channels is mapped to one OCSI allocation, every OCSI allocation will indicate its status as occupied or vacant.

By inquiring the mapping table of the OCSI allocations to the BSs, one BS can recognize the source of the interference or signaling in each OCSI allocation.

The initializing BS uses the OCSI allocation table to find out its neighbors in the working channel. By the contact information it acquired from the CP messages, the IBS will then use CP messages to negotiate for interference resolution with its neighbors.

15.3.1.1.2 CSI Frame Structure

The CSI frame is broadcast from the base station to the coexistence neighbor's subscriber station, within a series of CSI slots fragmentally. The CSI frame consists of power keying energy symbols as the basic element and carry the information from BS to the coexistence neighbor's SS. The CSI frame has the <SOF> symbols and <EOF> symbols as the boundary of slots when there are more than 4 symbols in each CSI slot. Two consecutive <SOF> and <EOF> indicate the signaling frame boundaries. Each CSI frame shall have 8 bits cyclic redundancy check (CRC) (Polynomial " X^8+X^2+X+1 ") appended to check the validity of the information carried within the CSI frame. In case the last slot of the signaling frame has not been fully used up with the CRC and <EOF>, a pad filled with "one" symbols will be added between the CRC and the double <EOF>. CSI frame should be continuously carried in the serialized CSI slots during the whole CSI frame structure. The basic structure is shown below:

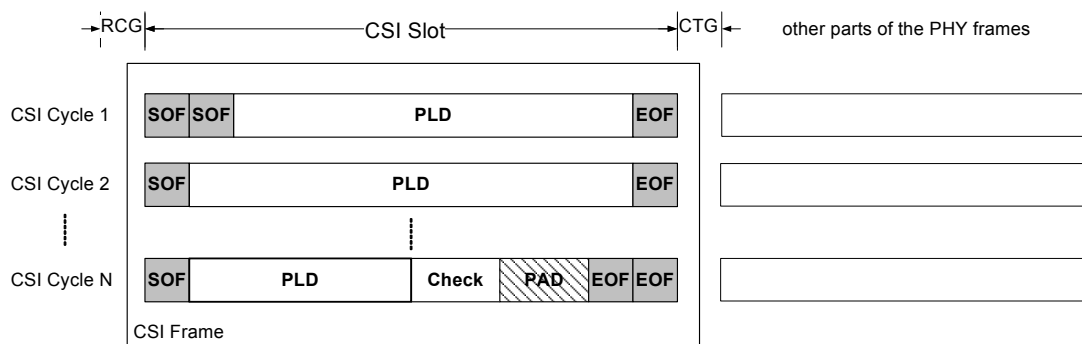


Figure h26—CSI frame construction with no less than 4 symbols in one slot

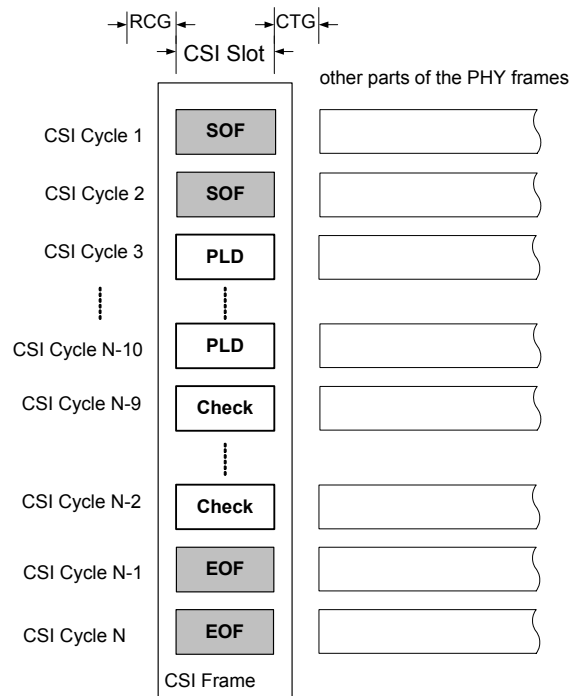


Figure h27—CSI frame construction with 1 symbol in 1 slot

The subscriber station of coexistence neighbor cannot get correct timing offset because there is no ranging process between the SS and IBS, so RCG (Receive-CSI gap) and CTG (CSI-Transmission gap) should be included in the CSI slot for reliable sampling in the SS.

The PLD (payload) part of the CSI frame should be structures as a TLV, as described in Figure h 28 . TYPE indicates the type of the payload, LENGTH corresponds to the number of symbols/bits contained in the VALUE portion. (TYPE and LENGTH are 1 octet each.)

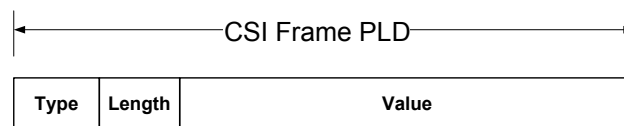


Figure h28—CSI frame PLD

The SS should keep monitoring the RSSI to detect <SOF> in the CSI interval. <SOF> flag can be detected according to the power value against time, When the power in first half of the symbol window is significantly lower than the second part, one <SOF> is expected to have been received, and the SS will pick a value in the middle of the two value as a threshold for the following symbols. If a following symbol shows lower power in the first part than the threshold and in the second part a higher power than the threshold, it will consider as a successful in detection of another <SOF>. A CSI frame considered to start here. When two consecutive <EOF> are detected at the end using a similar method as the <SOF> detection, and all the symbols in the frame are received and verified correctly by the CRC, the whole signaling frame is received correctly and the information inside will be extracted and reported.

Symbols between the two consecutive <SOF> and the two consecutive <EOF> are reassembled into CSI frame while the pad is dropped, when the check is passed. If the check fails, the signaling frame will be reported with an error indication and no value will be reported for the payload. The whole CSI symbol sequence will be ignored if no consecutive two <SOF> were detected.

When there are more than 4 symbols in each CSI slots, there will be a <SOF> and an <EOF> at the beginning and the end of the slots respectively. All the <SOF> and <EOF> will be dropped when reassembling the payload of the CSI frame.

15.3.1.1.3 Energy keying in time domain

The symbols in the CSI slots are broadcast by the BS and received by the SSs in a coexistence neighbor system. The modulation technology of the interference source and victim system could be one of the following: SCa, OFDM or OFDMA, and could be different between the interference source system and interference victim system. The operation bandwidth of the source and victim systems shall have overlapping part, but the bandwidth could be different.

The symbol in the CSI slot is defined only by its power profile in time, and could use any one of the modulation technology and any band that are available in the equipment. The duration of the energy symbol shall be $1/N$ of the CSI length, where N is a natural number specified by the region/country regulator.

There are four kinds of symbols: <SOF>, 0/null, 1, <EOF>, to be used to form any frame in CSI and to carry the information.

- <SOF>: Start Of Frame, indicating the data portion will start at the following symbol.
- 0/null: Binary code 0 used to compose the data portion, same as a null symbol.
- 1: Binary code 1 used to compose the data portion.
- <EOF> End Of Frame, indicating the data portion ended at the last symbol

Each symbol is divided into two equal length parts. For each part, there are two kinds of power keying level defined, H (high) and L (low). The BS uses the maximum power to transmit in the H(high) portion so that the SS can detect higher RSSI, and the BS is silent in the Low(L) portion and the SS can detect lower RSSI at that time.

The format of each of the four kinds of symbols is shown in the table below:

Table h3—CSI symbol Format

format		signification
Part1	Part2	
L	H	<SOF>
H	L	<EOF>
L	L	0
H	H	1

The receiving SS shall follow up the CSI timing and decode each symbol continuously in every symbol space, so that it can acquire the information transmitted by the source system. The SSs shall verify the symbol by this aspect of RSSI and time.

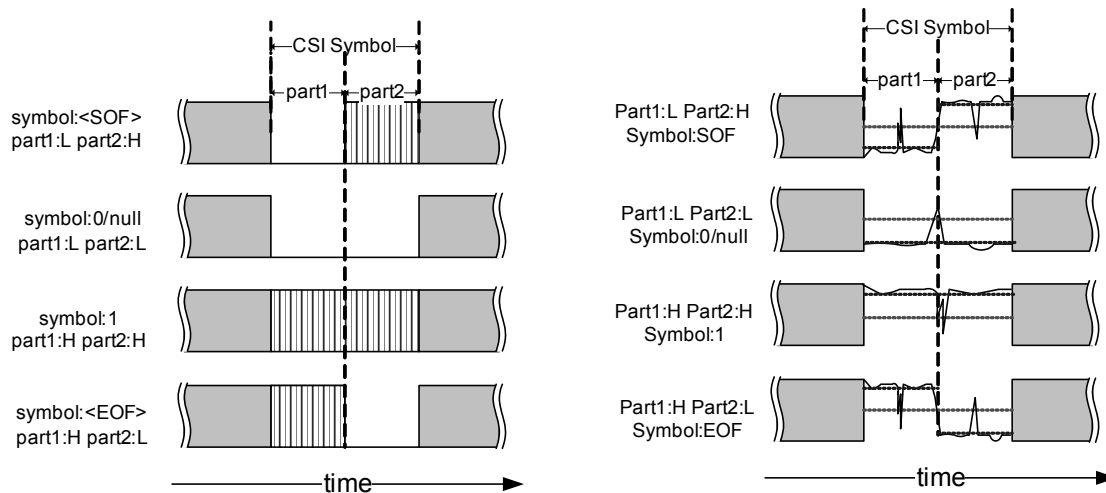


Figure h29—CSI symbol transmission and receiving

15.3.1.2 Energy keying in frequency domain

15.3.1.2.1 Signaling procedures using frequency-keyed energy pulses

The signaling procedures using frequency-keyed energy pulses are described in chapt. 15.4.3 (Radio Signaling to Ad-Hoc Systems).

15.3.1.2.2 Using the coexistence slot for transmitting the BS IP identifier

The radio signaling described in section 15.3.1.2.1 may be also used for the transmission of the BS_NURBC message (see 15.5.6.2.1), when there is no active Base Station Identification Server.

The transmission is done in consecutive coexistence time slots, spaced apart by T_{iptx} seconds. The first CSI in the series starts with CSI start signal, while the CSI in the series contains the Tx_end signal, the continuation in sequential CSI slots starts with the CSI_Continuation, as defined Table h 7. The IP identifier of the BS and a 8bit CRC, are transmitted between these signals, the L.S.B (least significant bit) for each field being transmitted first. The transmission of the above information uses only the preambles for the sub-channels 6,8,10,12,14,18,20,22,24,26 (10bits / symbol), the L.S.B. corresponding to the lowest sub-channel index.

The transmission of an IPV4 address will require $1 + (32+8)/10 + 1 = 6$ symbols and the transmission of an IPV6 address will require $1 + \text{ceil}((128+8)/10) + 1 = 16$ symbols.

15.3.1.3 Community entry of new BS using signaling

To enter the existing community at its neighborhood, a new BS - the Initializing BS (IBS) - without any associated SS contacts its neighbors using the IP network. The new BS should synchronize to the timing of

the CSI and ICSI in the air before using ICSI to broadcast the BS_NURBC (see 15.5.6.2.1) signaling to make its neighbors know of its operation and its contact information.

ICSI is used by the IBS to establish communication with its neighbor BSs. The IBS shall use the ICSI slot to broadcast its coexistence proxy's IP address and the BSID of its IBS, by sending a message and/or cognitive radio signaling. A coexistence neighbor operating BS (OBS) finds the initializing coexistence neighbor in the IP network via its coexistence proxy after receiving the SS report for this signaling. In order to obstruct the coexistence request from an unauthenticated internet terminal (such as a terminal far away or some terminal without any capability of WirelessMAN-CX air signaling which have known the static BSID and IP address information, the BS should use a RTK (Random Temporary Key) in the broadcast signaling. To authenticate the request of a CP message, the RTK sender requires that the request CP message, sent back later via the IP network, contains this random temporary key.

Then the IBS and OBS begin further negotiations via their coexistence proxy using the coexistence protocol. After coordination with the neighbors in the community, the IBS will get a periodic interference-free OCSIs, and become OBS, after that, it will cease using the ICSI.

The BS_NURBC (see 15.5.6.2.1) broadcasting procedure is unidirectional, only from the BS to the SSs in the common coverage area of the BS and its neighbors, and the SSs shall report all the useful information to the OBSs they are associated with. The SSs that succeed in decoding the message should report the content of the message, together with the frame number of the starting frame of BS_NURBC to the BS. The SSs that fail to decode the BS_NURBC, but still identify it as interference in the CSI should report the error status and the starting frame number of receiving the interference in the CSI. The IBS uses ICSI to broadcast the BS_NURBC message, the content of the message will enable its neighboring systems to communicate with the IBS over the IP network and coordinate their operation by the coexistence protocol. Using the IP address of the IBS's coexistence proxy and the BSID reported by the SSs which have successfully decoded the BS_NURBC message, together with the RTK, the OBSs communicates with the IBS over the IP network via their coexistence proxy. By checking the frame number in the report, the OBS determines if the SSs that report the error status in BS_NURBC reception were interfered by the same interference source identified in the BS_NURBC message, then the OBS will update the database and reply to the SSs which have sent the error report. (see Figure h 30.)

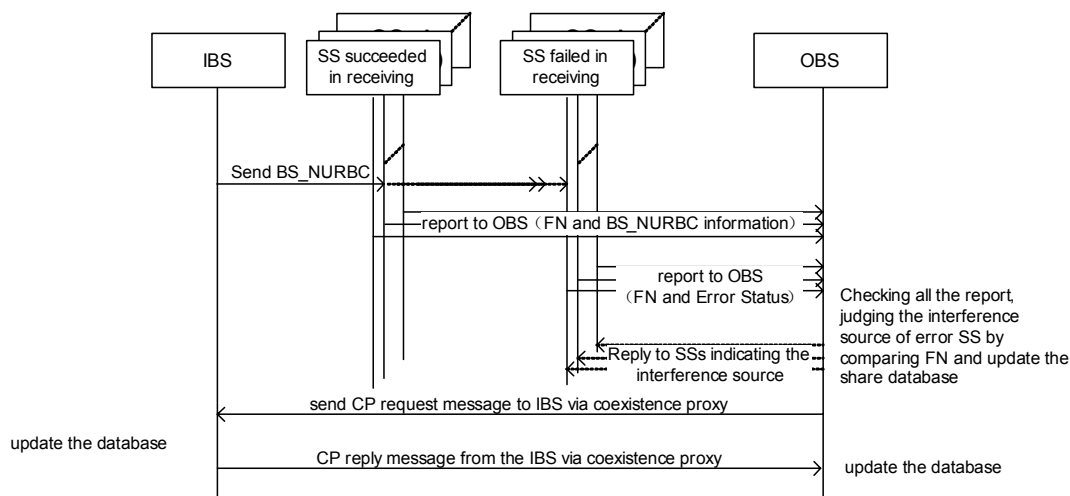


Figure h30—IBS entering the community by neighborhood update request broadcasting

A new entering BS knows the IP address of its coexistence proxy. By receiving the broadcast IP address of the IBS's coexistence proxy and the BSID of the IBS, all the neighbor OBSs which have the contact information of the IBS should start to communicate with this IBS using CP messages through the internet via the coexistence proxy. After receiving the CP request message from the OBS, the OBS's coexistence proxy will transform the source IP address into the IP address of the OBS's proxy, and forward the CP request message to the destination of the coexistence proxy which serves the IBS. The IBS's coexistence proxy should get the destination BSID by parsing the CP request message, and map it into IBS's IP address. If the BSID is in the coexistence proxy service list and the proxy can find the corresponding IP address, the coexistence proxy should forward the authenticated CP request message to the IBS. By receiving the CP messages from its neighbor systems, the IBS can discover its neighbor systems and continue on further negotiation and communication using the IP network through the coexistence proxies. Vice versa, the IBS should send the CP reply message to the OBS via the coexistence proxy after receiving and processing the CP request message.

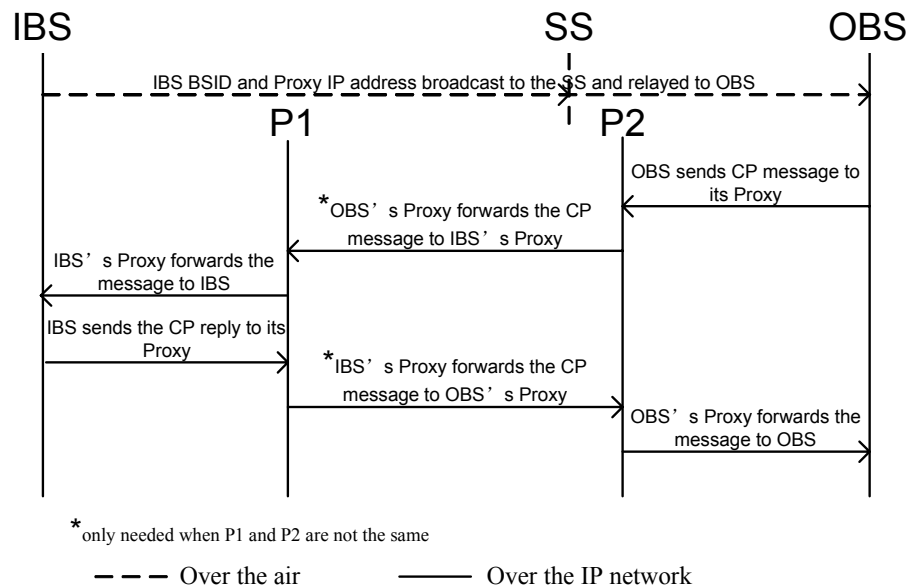


Figure h31—IBS entering the community with proxy

In any case that the new coming BS could not find the regional LE DB, it should start an ad-hoc method to find the neighborhood topology. The entering BS uses the coexistence time slot to broadcast its IP address to the reachable SSs in the neighbor systems. Once the SSs received this signaling, they will report to their serving BS one by one unsolicitedly, the information of the new BS and the interference status that they record during the reception will be reported to their serving BS.

The serving BS will get all the information from the related SSs and will save the useful content in its database. After that, the serving BS will contact new BSs using the IP address reported by the SS and transfer the parameter of its own database to the new coming one with authorization and negotiation, thereafter the serving BS will also get the parameters and other corresponding information from the new coming BS.

15.3.2 Coexistence messaging mechanism

15.3.2.1 Coexistence Messaging Interval (CMI) Use for Same Profile Systems

The CMI is the duration of the MAC frame (20 msec) and consists of an uplink and downlink intervals of equal size (10 msec) (TBD). Downlink messages carry information (BSD messages) unique to the identity of the base station controlling the system to which the particular CMI is associated. Uplink messages carry information (SSURF messages) unique to the subscriber stations within the system and base station associated with the same CMI. During a CMI all other systems, not associated with the particular CMI, remain silent and receive only.

Every BSD (section 6.3.2.3.62) sent downlink has a BS_ID associated with it. This BS_ID tag can be used as an interference identification tag as well. The message contains the UL-MAP, which addresses specific SS to send their SSURF messages. The duration of the BSD message is typically 1 msec (TBD).

There is only one downlink BSD PDU in the CMI and it is transmitted at random starting point within the downlink time interval of the CMI. The rationale for the random placement of the BSD within the downlink subframe is to handle the possibility that two or more potentially interfering base stations inadvertently choose the same CMI. Such base stations and the respective systems they control may coexist peacefully without causing interference to each other because of hidden SS or having no SS in the common coverage area. Essentially, such systems do not form an interference community because they do not interfere with each other. However, when the hidden SS or new SS enters into the common coverage area, co-channel interference will be detected at the new SS resulting in a situation that impacts the neighboring base stations having a common CMI.

A BSD collision occurs in this situation and this is resolved by randomizing the start times of downlink sub frame PDU and uplink SSURF messages in the CMI. This reduces the possibility that two systems, sharing the same CMI will overlap in their downlink and uplink BSD or SSURF transmissions. Realize that the downlink slot will be 10 msec wide and that the downlink sub frame BSD PDU itself is only < 1 msec. For the worst BSD collision case, there are n base stations in the common coverage area, the successful (non-overlapping) BSD transmission probability is

$$p = 1 - \frac{1}{m} \cdot \frac{1}{m} \cdot C_n^2 = 1 - \frac{1}{m} \cdot \frac{1}{m} \cdot \frac{n!}{(n-2)! \cdot 2!} \quad (h1)$$

Where $m = \frac{t}{t_d}$. Assume the CMI downlink duration time length is t which is the uplink portion of a physical frame (physical frame duration is varying from 2, 2.5, 4, 5, 8, 10, 12.5, to 20ms), the BSD downlink PDU time duration is d , which is typically < 1 msec.

15.3.2.2 Candidate Channel Determination (Using GPS/UTC Synchronized CMI and Common Profile)

Candidate Channel Determination (CCD) is the process used by WirelessMAN-CX systems (using a synchronized CMI and common profile) where a base station monitors a band to which it has access and selects, within that band, a channel having minimal use and occupancy by neighboring wireless systems. This process is used, for example, by an IBS prior to undertaking entry into a Coexistence Community. Since a base station can only receive uplink traffic, this process relies on the monitoring uplink transmission intervals and the measurement of interference signal power [I] and noise power [N]. Each candidate channel will be ranked in terms of its (I/N) ratio. Those channels with the lowest ratio or ideally a ratio of 1 will be selected for use by the base station and be candidates for entry by an IBS, since such channels will have the lowest amount of discernable activity on them, hence likely have lower interference.

[I] and [N] will be determined using the RSSI measurement capability of the base station receiver as detailed in Section 8.4.11.2. After synchronization to the GPS and initialization of the base station operating parameters, the base station will select a channel and undertake noise floor measurements on CMI_ID54, which is unoccupied by WirelessMAN-CX systems but may be used by non-WirelessMAN-CX systems (15.7.1.1).

CMI_ID54, in situations when it is unoccupied, will be free from all WirelessMAN-CX transmissions and will provide an interval allowing the measurement of the receiver thermal noise floor [N]. The thermal noise floor is the noise power spectral density of the received channel (N_0) multiplied by the channel bandwidth. Measurements will be undertaken long enough to determine whether [N] has Gaussian characteristics. Characteristics not deemed as Gaussian and/or RSSI measurements that are 3 db (TBD) higher than a predetermined [N] value (which can be provided a priori as a Receiver Noise Figure estimate within RSSI measurement algorithm in the base station receiver) will be indicators that channel may be occupied by non-WirelessMAN-CX users. In this instance the value of the mean RSSI will be taken as the [I] created by the occupying non-WirelessMAN-CX system and the given channel will be discarded from further consideration. Otherwise, the measurement will provide a value for [N].

[I] measurements will be undertaken by calculating the mean signal strength and variance due to uplink SSURF messages summed over intervals CMI_ID00 to CMI_ID48. The number of CMI cycles to be measured will be a variable (**TBD**) set for the base station by the operator. Measurement of the RSSI will be done in accordance with Section 8.4.11.2, with care being taken to ensure that valid signals are being measured, even at close-to noise floor levels. The mean RSSI and variance calculated for the summed CMI intervals of the channel will be construed as interference values [I] and [Var I] for the channel.

The channels are then ranked, with the channel having the lowest I/N and smallest [Var I] measurements likely selected for IBS entry into a Coexistence Community. Figure h 32 shows the CCD process.

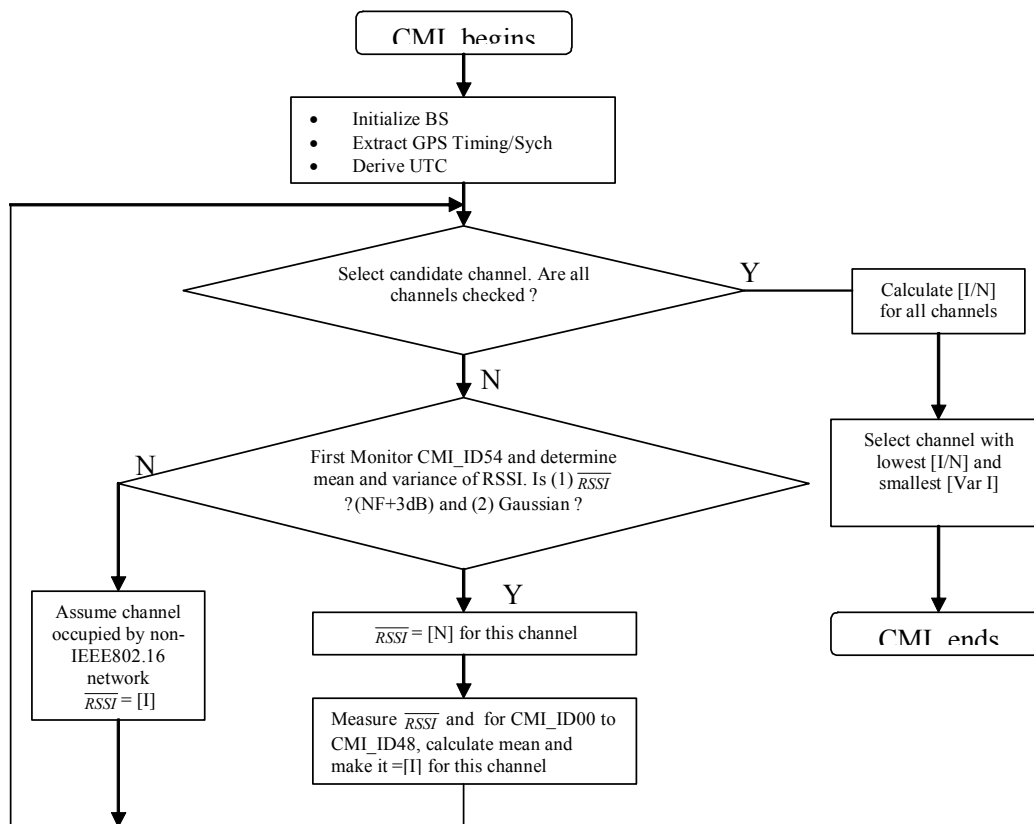


Figure h32—CCD Process

15.3.2.3 Entry of a new BS into a Interference Neighborhood and the Creation of a Coexistence Community Using GPS/UTC Time Synchronization and Common System Profile

In applications where the Coexistence Messaging Intervals (CMI see 15.1.4.1.2) are synchronized to a GPS (or similar precision timing reference) and are given UTC time stamps (Figure h 14), entry of a new Base Station (IBS) will be undertaken in 4 steps, with the IBS:

- (a) Monitoring the CMI Intervals,
- (b) Selecting an Empty CMI interval,
- (c) Claiming an empty CMI interval,
- (d) Membership in a Coexistence Community.

Prior to entry into a Community of Operating Base Stations (OBS) it is assumed that the IBS will have undertaken Candidate Channel Determination (Section 15.3.2.2) and has selected a candidate channel, is synchronized to a downlink GPS signal and can derive a UTC time stamp, and has no operational SS yet deployed. It is assumed that the IBS is deployed within an Interference Neighborhood: ie: active interference from existing Operating Base Stations is present. It is also assumed that the community which entered is WirelessMAN-CX compliant and uses a common (same) profile. The IBS entry process is shown in Figure h 33, Figure h 34 shows aspects of the entry procedure with signalling.

(a) Monitoring the CMI

Having tuned to the candidate channel, the IBS monitors and determines the level of activity on each CMI by demodulating the uplink SSURF (Sec 6.3.2.3.62) messages and storing their parameters in its Base Station Information Table(See Table h 4). All demodulated SSURF messages will be from SSs that will interfere with the BS on the uplink and eventually, coexistence will have to be arranged with each of the OBS controlling these SSs via the Coexistence Protocol (CP). Each CMI from CMI-ID-00 to CMI-ID-54 is monitored. Each CMI is monitored for 5 CMI cycles or minutes (**TBD**). If CMI-ID-54 has detectable power in it, the channel will be construed as occupied by a non-IEEE 802.16 system (See 15.7.1.1) which may also be synchronized to the GPS/UTC. The channel will be abandoned if CMI-ID-54 is occupied (See 15.7.1). The signalling seen by an IBS is shown in Figure h 34.

(b) Selection of an Empty CMI

The monitored CMI in which no (demodulated) SSURF messages are received becomes a candidate CMI, and is considered empty. Empty CMI indicate that it is still possible for the IBS to create a new Coexistence Community including the OBS (only a maximum of 9 (**TBD**) co-channel systems can be accommodated by a single channel. Full loading is indicated when all 9 (**TBD**) CMI are occupied by the systems forming a Coexistence Community).

During each candidate CMI a RSSI (see 8.4.11.2) will be undertaken by the IBS during the uplink duration. RSSI is undertaken to determine the presence or absence of low level (un-demodulated) uplink SSURF messages. Each candidate CMI is monitored in this manner over a duration of 10 CMI cycles or minutes (**TBD**). An interval will be considered as useable and chosen if the mean RSSI power measurement in it is no greater than $[N] + 3 \text{ dB}$ (**TBD**); where $[N]$ is the thermal noise floor of the IBS receiver as determined by the Candidate Channel Determination process (See 15.3.2.2).

The absence of uplink SSURFs means that the CMI is free of uplink (and possibly downlink occupancy). The particular CMI is now considered as being ready for claiming.

(c) Claiming Procedure.

The purpose of the claiming process is to make all adjacent OBS aware of the presence of the IBS. This process results in the delimitation of the Interference Neighborhood, that is, identification of all the adjacent systems that will see interference from the IBS. Claiming is undertaken by having the IBS broadcast its BSD during an empty CMI. Since all the OBS (both base stations and their SS) are silent and are monitoring the downlink on each CMI other than their own, the broadcast BSD message will likely be detected during what was previously an empty CMI (see discussion on undetected broadcasts below).

To begin the claiming procedure the IBS broadcasts at maximum EIRP a BSD (see 6.3.2.3.62) message. This message, when received by SS belonging to adjacent OBS systems that form the Interference Neighborhood, will result in those SS informing their associated base stations (OBS) of the presence of a new base station (the IBS). The SS inform their BS of this by using a MAC message called the BS_CCID_IND. This MAC message contains the Proxy IP address of the IBS, which was extracted by the SS from the interfering BSD message. Now having the proxy IP address, the OBS respond back to the IBS via a backhaul IP link, informing the IBS that it has been detected and is a de facto interferer on the co-channel RF downlink. Having received this communication from the OBS, the IBS will now have discovered the systems in the Interference Neighborhood, and as part of this discovery process now has the identities of the adjacent OBS. The OBS identities are included in the IBS Information Table (see Table h 4). The IBS continues its BSD broadcast routine until no new OBS make themselves evident to the IBS. The IBS continues its BSD broadcasts every CMI cycle (every minute), and does so as long as it confirms to itself that it has formed a Coexistence Community with adjacent systems.

(d) Membership in the Coexistence Community

All of the adjacent systems with which the IBS creates or sustains interference to/from become listed in the BS Information Table (See Table h 4) of the IBS. This table contains the BS_IDs and related IP addresses derived either from uplink SSURF messages that the IBS demodulated during its monitoring phase (above (a)) or from the BS_CCID_IND and IP messages that it received via the IP backhaul from the OBS as part of the claiming procedure ((c) above).

Communication and negotiation with each OBS listed in the BS Information Table is undertaken via the **[TBD]** Coexistence Protocol (CP). Coexistence entails allocation of uplink and downlink transmission intervals in a manner that eliminates co-channel interference amongst users that would otherwise experience it and sustain degraded communications. This is done by parsing uplink and downlink intervals and establishing master subframes (see Sec 15.4.2.1.2). Each OBS that the IBS has listed in its BS Information Table as an interfering system must partake in such a resolution procedure. By undertaking this process the IBS thus creates a Coexistence Community for itself, and consequently becomes accommodated by the neighbouring systems of its interference neighbourhood. If the IBS for some reason cannot resolve all the interference it creates or sustains, then the entry process is repeated on a new channel taken from the rankings provided by the CCD procedures (see 15.3.2.2). In doing so the IBS would then abandon the CMI that it claimed in (c). If the CP process is successful, then the IBS (now OBS) continues its claim to the CMI, thereby now informing all other systems of its active presence in the Coexistence Community.

Undetected BSD Broadcasts/Undetected Uplink SSURF messages:

The BSD and SSURF messages are sent at the lowest, most robust modulation rate specified for IEEE 802.16 transmissions. However, because of the statistical variation in the propagation channel whose variance can exceed 10 dB, there is a finite probability that eventually such signals shall eventually exceed demodulation threshold levels and be detected. The time to achieve this is **TBD**. Furthermore, below threshold signals can be detected by power detectors or detection techniques that will provide indication of signals below demodulation thresholds. These techniques can be instituted either as part of the RF system or in parallel with the demodulation process.

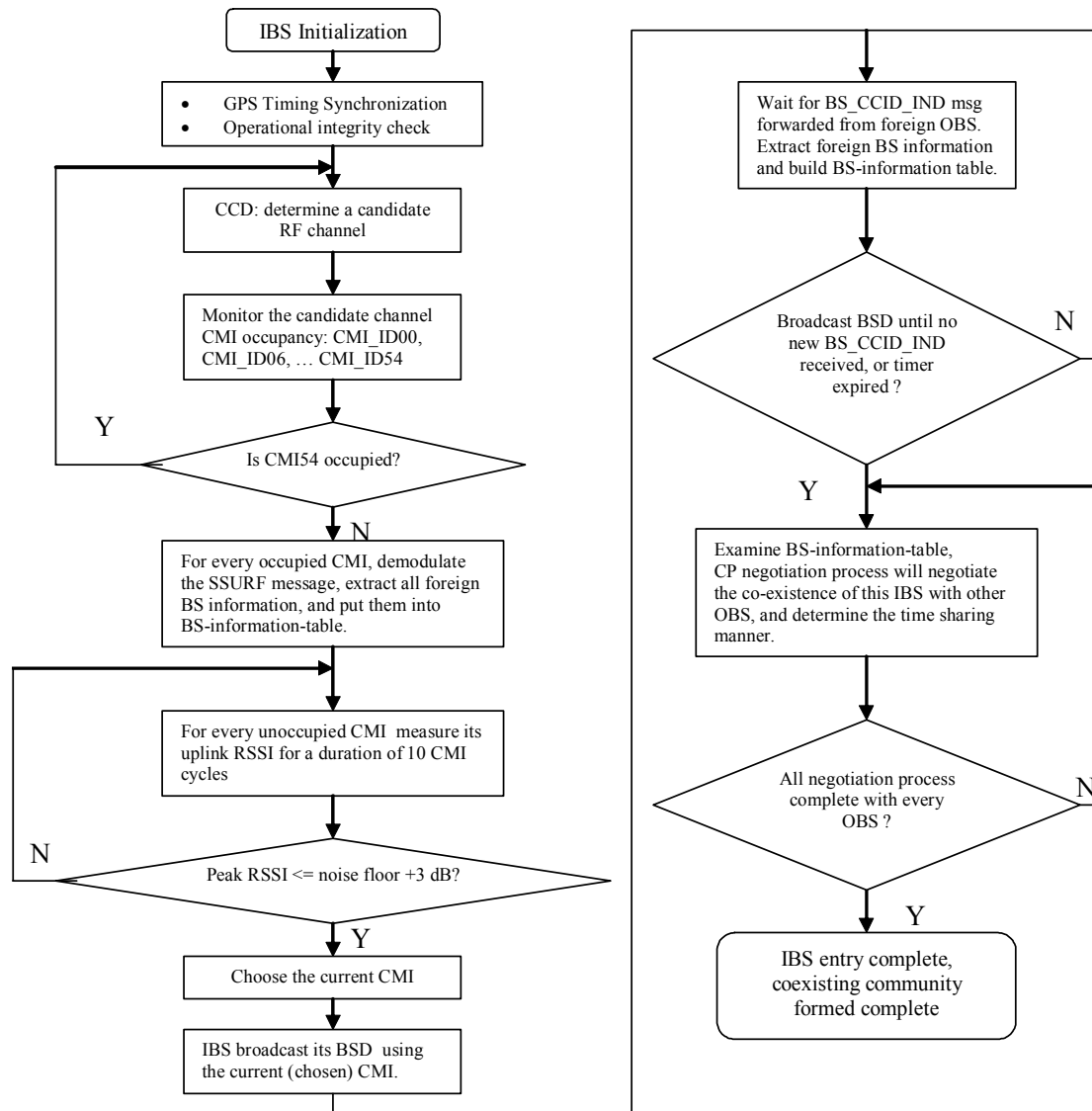
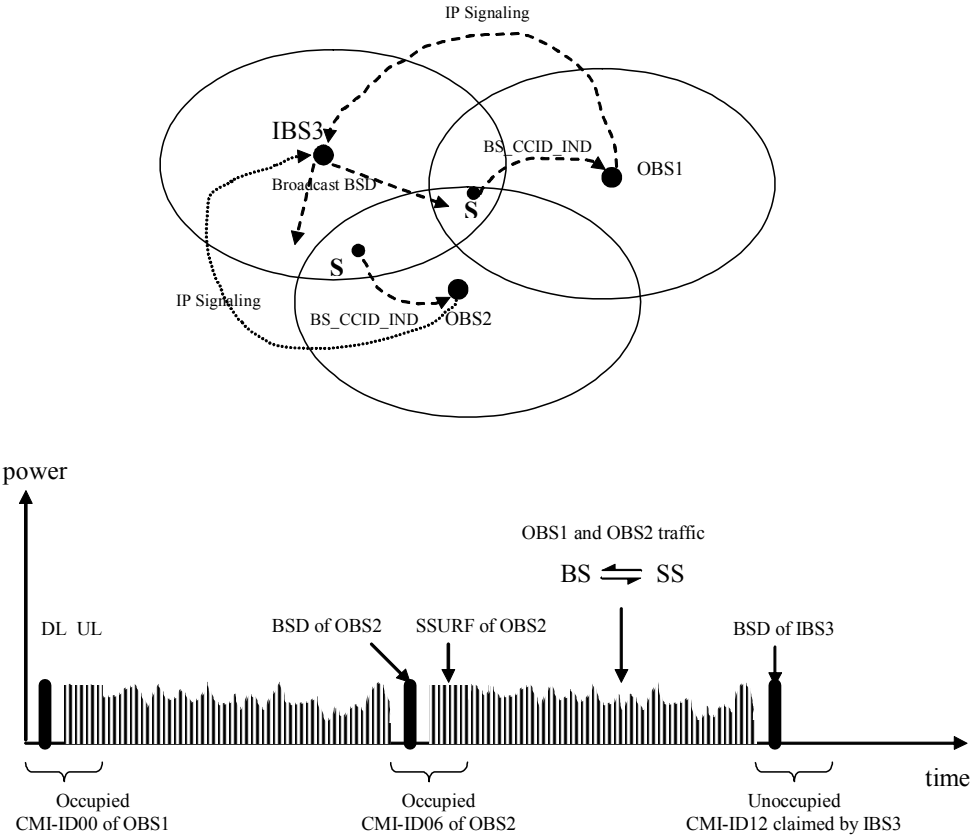


Figure h33—IBS community entry process



15.3.3 Information table

15.3.3.1 Information table in distributed database

The following tables specify the fields (TLVs) to be included in the BS data base, containing information related to its own operation (see Table h 4) and to the operation of the base stations in the community (see Table h 5). Table h 6 specifies the information (TLV) to be included in the SS database.

Table h4—Information table for the BS containing this database

Syntax	Size	Notes
This BS information table(){		
BSID	48bits	
Operator ID	?bits	
IP version	1bits	0-IPv4 1-IPv6
(IP version = 0){		

1	IPv4 address	32bits	IPv4 address of this BS
2	CXPRX IPv4 address	32bits	CXPRX IPv4 address
3	}		
4	Else{		
5	IPv6 address	128bits	IPv6 address of this BS
6	CXPRX IPv6 address	128bits	CXPRX IPv6 address
7	}		
8	RTK	16bits	Random Temporary Key
9	Extended Channel Number (ExChNr)	16bits	2 byte base reference to frequency range or deployment band. This reference maps to an absolute frequency value.
10	Base Channel Reference (BaseChRef)	8bits	1 byte specific channel number reference
11	Channel spacing (ChSp)	16bits	2 bytes channel spacing value (10kHz increments)
12	Master resource ID	8bits	Sub-frame number
13	OCSI ID	8bits	CSIN of OCSI allocation
14	Negotiation status	8bits	Bit0: get communication in the IP network Bit1: be registered in Bit2: registered to Bit3: done for resource sharing(if neighboring) Bit4-7: tbc.
15	CSI parameter(){		Regulated by region/country
16	Tcsi_start	16bits	In microseconds
17	Tcsi_duration	8bits	In microseconds
18	Period of frames	8bits	frames
19	Starting frames offset	16bits	frame serial number of the first frame that CSI presented
20	Length of Symbols	8bits	In microseconds, need to be 1/n of Tcsi_duration
21	ICSI cycle	8bits	ICSI cycle counted in CSI cycles
22	OCSI cycle	8bits	OCSI cycle counted in ICSI cycles
23	}		
24	Number of CoNBRs	8bits	m: The number of coexistence neighbors of this BS
25	for (i= 1; i <= m; i++) {		
26	BSID	48bits	
27	(Tbc.)	(Tbc.)	(Tbc.)
28	}		
29	Profile(){		
30	Band		
31	PHY mode(){		
32	Modulation		
33	Working Channel ID	8bits	Identifier of the working channel of this BS.
34	Number of alternative Channels	8bits	p: The number of alternative channels to which this BS can switch without interference.
35	For(i = 1; i <= p; i++){		
36	Alternative Channel ID	16bits	Identifier of the alternative channel.
37	}		
38	(Tbc.)		
39	}		
40	Maximum power	8 bits	dbm
41	Number of registered SS	12bits	n
42	for (i = 1; i <= n; i++) {		
43	SSID	48bits	
44	(tbc.)	(tbc.)	(tbc.)
45	}		

(tbc.)	(tbc.)	(tbc.)
}		
}		

Table h5—Information table for the systems inside the neighborhood or community

Syntax	Size	Notes
BS information table() {		
Index	16bits	
BSID	48bits	
Operator ID	?bits	
RTK	16bits	Random Temporary Key
IP version	1bits	0-IPv4 1-IPv6
(IP version = 0) {		
CXPRX IPv4 address	32bits	CXPRX IPv4 address
}		
Else {		
CXPRX IPv6 address	128bits	CXPRX IPv6 address
}		
Sector ID	8bits	
Extended Channel Number (ExChNr)	16bits	2 byte base reference to frequency range or deployment band. This reference maps to an absolute frequency value.
Base Channel Reference (BaseChRef)	8bits	1 byte specific channel number reference
Channel spacing (ChSp)	16bits	2 bytes channel spacing value (10kHz increments)
Master resource ID	8bits	Sub-frame number
OCSI ID	8bits	CSIN of OCSI allocation
Negotiation status	8bits	Bit0: get communication in the IP network Bit1: be registered in Bit2: registered to Bit3: done for resource sharing(if coexistence neighboring) Bit4-7: tbc.
Coexistence neighboring	1bit	Coexistence neighbor with this BS? 1=yes 0=no
BS GPS coordinates	TBD	GPS coordinates of this Base Station
BS RF antenna sector ID	8bits	Identifier of antenna creating this sector
BS nominal EIRP	TBD	Nominal EIRP of this Base Station
BS PSD Vector	TBD	PSD as determined by this BS of all available channels using RSSI scanning process
BS antenna azimuth	TBD	Azimuth orientation of this Base Station's antenna
BS antenna beamwidth	TBD	Azimuth Beam width of this Base Station's antenna
If (Coexistence neighbor) {		
Number of victim SSs	16bits	n: The number of victim SSs of this coexistence neighbor, in this system
for (i = 1; i <= n; i++) {		
SSID	48bits	
RSSI	16bits	1byte RSSI mean (see also 8.2.2, 8.3.9, 8.4.11) for details) 1byte standard deviation
}		
(Tbc.)	(Tbc.)	(Tbc.)
}		

1	Number of Coexistence neighbors	8bits	m:The number of coexistence neighbors of this BS
2	for (i= 1; i <= m; i++) {		
3	BSID	48bits	
4	Working Channel ID	16bits	Identifier of the working channel of this neighbor.
5	Escape Channel Flag	1bit	Flag indicates this neighbor has one or more escape channels.
6	(Tbc.)	(Tbc.)	(Tbc.)
7	}		
8	Profile(){		
9	Band		
10	PHY mode(){		
11	Modulation		
12	Working Channel ID	16bit	Identifier of the working channel of this neighbor.
13	alternative Channel Flag	1bit	Flag indicates this neighbor has one or more alternative channels.
14	alternative Subframe Flag	1bit	Flag indicates this neighbor has one or more ALTSF.
15	(Tbc.)		
16	}		
17	Maximum power	8 bits	dbm
18	Number of registered SS	12bits	
19	(tbc.)	(tbc.)	(tbc.)
20	}		
21	If (CMI Interval used) {		
22	Number of coexistence neighbors		
23	For (i=0; i<=n; i++) {	TBD	All Co-existing neighbor BS information. This is the list of foreign BS, which may be causing interference to this BS and its SS
24	Foreign BSID	TBD	BS_ID of this foreign BS
25	Foreign BS IP address	TBD	IP address of this foreign BS
26	Foreign BS CMI-ID	TBD	CMI_ID of this foreign BS
27	Number of foreign SSs causing Co-channel interfering	TBD	Number of SS associated with this foreign BS causing interference to this BS
28	For (j=0; j<=m; j++) {	TBD	All SSs associated with this foreign BS, which cause co-channel interference
29	Interfering SSID	TBD	SS_ID of this SS causing interference to this BS
30	CMI Interfering occurrence	TBD	Number of instances where interference recorded.
31	RSSI of interfering SS	TBD	RSSI of this interfering SS
32	SS interference resolved	1 bit	Has the interference caused by this SS been resolved by use of the CP between this BS and the foreign system?
33	}		
34	}		
35	}		
36	(Tbc.)	(tbc.)	(tbc.)
37	}		

Table h6—Information table for the SSs inside the system containing this database

Syntax	Size	Notes
SS information table(){		
Index	16bits	
SSID	48bits	
SS location	TBD	Optional
SS GPS location	TBD	Optional

SS antenna beam width	TBD	Beam width of this SS antenna
SS nominal uplink EIRP	TBD	Nominal EIRP of this SS
SS PSD vector	TBD	Power Spectral Density determined by the SS by RSSI process scanning all available channels
Interference status	1bit	Interfered by coexistence neighbor? 1=yes 0=no
If (Interfered){		
Number of source BSs	8bits	n: The number of interference source of coexistence neighbor
for (i = 1; i <= n; i++) {		
BSID	48bits	
BS_NURBC detected	1bits	1=yes 0=no
If (BS_NURBC detected){		
IP version	1bits	0-IPv4 1-IPv6
(IP version = 0){		
CXPRX IPv4 address	32bits	the v4 IP address of the CXPRX reported by the SS
}		
Else{		
CXPRX IPv6 address	128bits	the v6 IP address of the CXPRX reported by the SS
}		
IBS BSID	48bits	The BSID reported by SS
RTK	16bits	RTK in the BS_NURBC reported by SS
Sector ID	?bits	Reported by SS
Frame number	24bits	Reported by SS
Error Status	?bits	0 -no error 1 - not capable to decode the energy pulse symbol; 2 - not able to find the eligible <SOF>; 3 - not able to find the eligible <EOF>; 4 - not able to pass the CRC check for message;
(tbc.)	(tbc.)	(tbc.)
}		
RSSI	16bits	1byte RSSI mean (see also 8.2.2, 8.3.9, 8.4.11 for details) 1byte standard deviation
(tbc.)	(tbc.)	(tbc.)
}		
(tbc.)	(tbc.)	(tbc.)
}		
If (CMI frame used) {		
Associated BS ID	TBD	BS_ID to which this SS is associated
Associated BS RSSI	TBD	Mean RSSI of BS downlink to which this SS is associated
Associated BS RSSI Var	TBD	Variance of RSSI of downlink
Associated BS BER	TBD	BER of downlink
Number of foreign BSs	TBD	Number of foreign BS this SS has detected via BSD
For (I=0; I <=n; I++) {		
Foreign BS ID	TBD	BS_ID of this foreign BS as determined from its BSD
Foreign BS EIRP	TBD	EIRP of this foreign BS as determined from its BSD
Foreign BS antenna sector ID	TBD	Antenna sector ID of this foreign BS as per BSD
Foreign BS Proxy IP address	TBD	Proxy IP address of this foreign BS as per BSD

Foreign BSD occurrence ratio	TBD	Defined as the ratio of demodulated foreign BSD messages to CMI cycles. A metric indicating severity of interference caused by this foreign co-channel BS.
Interference resolution	1 bit	An indication that interference from this foreign BS has been resolved by the CP.
CMI-ID	TBD	CMI_ID of this foreign BS
}		
}		
(tbc.)	(tbc.)	(tbc.)
}		

15.3.3.2 Information table in centralized database

[notes: Centralized server should contain the information necessary for system's neighbor discovery procedure, and should describe the content here.]

15.4 Interference prevention

This subclause describes the methods of preventing the interference, based on the information of the interference that the system had identified (section 15.3).

The approaches for interference resolution are based on MAC Frame synchronization and separation of the interference in the frequency and time domains.

The separation of interference in the frequency domain is undertaken first, followed by the separation of remaining interference in the time domain, using procedures of the Coexistence Protocol. The Coexistence Protocol is defined at the IP level and is mainly intended for BS-BS communication.

In order to obtain the IP addresses of the Base Stations within the Coexistence Neighborhood, a number of procedures are defined, based on operator coordination, or on indirectly transmitting the contact information for the IP network.

The operators can exchange information tables containing the deployment information, such as GPS coordinates, IP address of the CX entity in the Base Station, etc.

Operators may also maintain a common database, including both deployment information and an IP identifier for allowing the operation of a technology-independent coexistence approach. In this case, it is assumed that:

- 1) Every Base Station includes a data base, based on which the Base Station negotiates with other systems in the community; the BS data-base contains information necessary for spectrum sharing, and includes the information related to the Base Station itself and the associated SSs. Other Base Stations can send queries related to the information in the database to the DRRM entity, located in a Base Station (see [Figure h 17](#)). The base station shall represent its system in the cooperation with other systems when communicating over the backbone. It is possible to use the subscriber station to relay the control messages in some situations. The base station locations may be obtained by GPS or other positioning systems, however there is no need to register the subscriber locations;
- 2) In some cases there is country/region data base, which includes, for every Base Station, the following parameters:

- o Operator ID
- o Base Station ID
- o Base Station GPS coordinates
- o IP identifier

The local Radio Administration may maintain, for light licensing purpose, its own database, generally not including the Base Station ID and IP identifier information.

There is a server that manages the country/region Database, using the WirelessMAN-CX standardized procedures; the server and the country/region database can be hosted by one of the operators or a trusted entity, such as the local Radio Administration.

Otherwise, if the region/country database is not available, the base stations should try to find their neighbors and the community topology in a coordinatively distributed fashion.

- 3) All the Base Stations forming a community will have synchronized MAC frames and frame numbers.
- 4) A community will be limited to a reasonable size.
- 5) All the Base Stations and their systems will be equipped with a spectrum detection and monitoring capability that prevents co-channel utilization of the same spectrum.
- 6) All base stations are synchronized to a GPS clock. The start of all MAC frames and other events are referenced to the rising edge of this clock.
- 7) All non-WirelessMAN-CX systems, operating in the LE bands, will be provided with the opportunity to signal their presence to WirelessMAN-CX systems within the dedicated CMI slot.
- 8) The WirelessMAN-CX systems will recognize the operation of radars and other systems having higher priority in the LE spectrum.
- 9) Every system will have a guaranteed minimum access time for the interference free use of the radio resource, being able to receive with minimum interference and to transmit at the needed powers for allowing communication between its Base Station and the remote subscribers.

BS regular operation

The regular operation of BS includes:

- **Radio resource allocation and re-allocation:** including channel allocation and sub frame allocation.
- **SS traffic Scheduling:** The traffic of each served SS should be scheduled into the corresponding sub-frame/resource based on the SSs' interference situation. Traffic of SSs in the interference free zone could be scheduled into any available sub-frame/resource of the serving BS, and traffic of SSs in the interference zone should use only corresponding master subframe/resource of the serving BS.
- **System power controlling:** Set Tx power levels in order to use the minimum power levels for both BS and SSs;
- **Interference situation identification:** The BS needs to keep updated information for all BS in the community including the coexistence neighbor BS, and the information of the served SSs in the own system. The information includes the profile and the interference situation of the stations. The interference situation information includes the interference status, the interference source and corresponding RSSI, the interference victims founded, etc.

- **Distributed database maintenance:** Update and maintain database when other BS's join the community.

15.4.1 Adaptive Channel Selection – ACS

This section describes the method of Adaptive Channel Selection (ACS) to prevent interference. The first step is to attempt to identify a vacant channel using the gathered information from the system and the neighbor systems (see 15.3.3). If a vacant channel is not found, the BS then tries to obtain an exclusive channel by optimization of channel distribution (see 15.4.1.1& 15.4.1.2).

Success of either step will enable the BS start working with an exclusive working channel. If no vacant channel can be found, then the BS will attempt the channel sharing coordination procedure.

15.4.1.1 How to select a "free" channel (for ACS and DFS)

After Scanning before interference identification, the IBS should try to figure out whether it interferes with other systems in each of these candidate channels. By the feedback messages received after the signaling broadcasting, the IBS will collect the information of its interference victims on each channel.

If there is neither interference detected nor interference victims found in some channel by the IBS, the channel is marked as a "free" channel of the IBS. Otherwise, the IBS should figure out whether a "free" channel can be vacated by optimized channel distribution, as described in 15.4.1.2.

The process of ACS is shown in Figure h 35. The ACS process concludes with either one of two possible results: a) a "free" channel is validated with or without channel distribution optimization, or b) no "free" channel.

If a "free" channel is validated, it means default interference-free master slot is to be used; otherwise, the IBS needs to share the channel with coexistence neighbors, as described in 15.4.2.1.

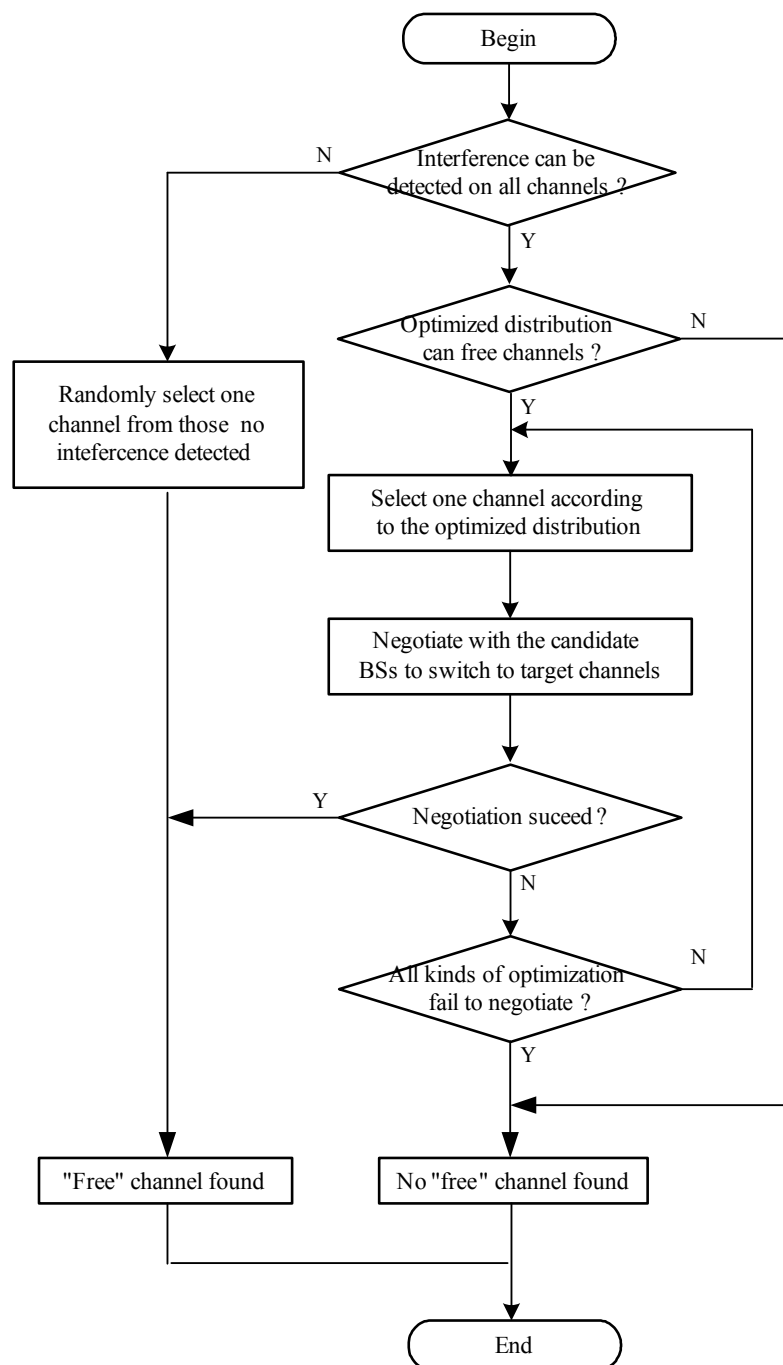


Figure h35—Process of ACS

15.4.1.2 Optimization of Channel Distribution

In the initialization phase of an IBS, its neighbors will send it their current working channel ID, OCSI allocation and subframe allocation using CP messages, as well as a flag of having alternative channels. The IBS maintains the channel information of all neighbors in the BS information table.

1 When the IBS cannot find any free channel at the initialization phase, it should try to change the channel dis-
2 tribution and to vacate a free channel for the IBS by switching some of its neighbors' working channels to
3 others.
4

5
6 First, the IBS picks all the channels that all the neighbors operating on it have alternative channels, and sorts
7 them according to the number of neighbor systems working on each.
8

9
10 Second, the IBS selects one of the channels used by the fewest BS, and considers this channel as its poten-
11 tial working channel. The IBS should now negotiate with all the neighbors working on the selected channel.
12

13 Third, to negotiate with every neighbor BS working on this channel, the IBS should send a channel switch
14 request message to each. A neighbor OBS, which has received this message should select one of its alterna-
15 tive channels as the their target working channel, and try to move its working channel to that channel as long
16 as the request is valid. After the working channel was switched to its alternative, the neighbor OBS should
17 acknowledge the swotch to the IBS by sending back a channel switch reply message with success indication,
18 otherwise it should send back a fail indication. If the IBS received any rejection from the neighbors, to
19 which the IBS had sent the request, the IBS should cancel the request by sending another message with the
20 indication for the neighbors to switch back to the channel they used before the IBS's channel switching
21 request.
22
23

24
25 Finally, when the IBS receives a positive acknowledge messages from all of its neighbor OBSs, it means the
26 channel redistribution optimization procedure has succeeded to vacate a channel for the IBS, and the IBS
27 should use it as a working channel afterwards. Otherwise, the IBS should try to vacate the next potential
28 channel.
29

30
31 If the channel redistribution procedure failed and all the potential channels can not be vacated to become the
32 IBS's working channel, the IBS shall try to share one channel with some of its neighbors.
33

34
35 If the channel redistribution procedure succeeds, a list of alternative channels of related BSs should be
36 updated if their neighbors have changed their working channels. The IBS should broadcast to all its neigh-
37 bors that it will be working on the selected channel, all its neighbors should add it as their new neighbor in
38 the BS information table, and exclude its target working channel from the list of potential alternative chan-
39 nels. The neighbor OBSs that moved away from this channel should also notify the change to all of their
40 neighbors, so their neighbors can update the database according to the change.
41
42

43 The above process of channel selection optimization is shown in Figure h 36.
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

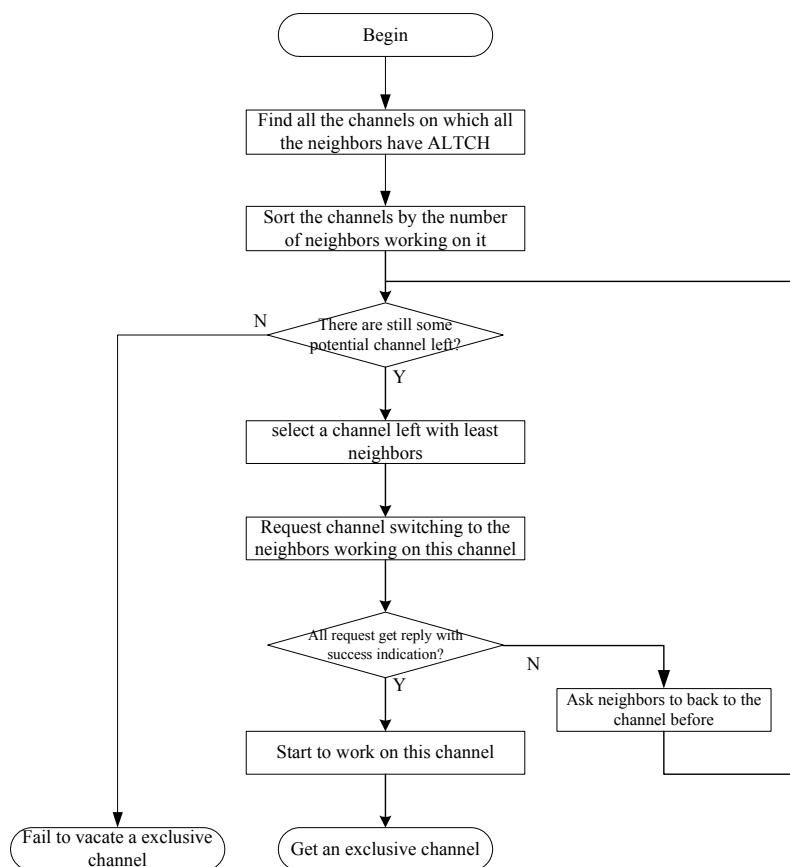


Figure h36—Process of channel distribution optimization

15.4.2 Adaptive Sub frame Allocation - ASFA

15.4.2.1 Sub frame sharing & scheduling

15.4.2.1.1 Cooperation with other systems

A system may need more bandwidth, as time allocated resource, for its BS communication with the SSs, than available for its operation in the assigned interference-free time interval. In this case, the specific system may request from one or more adjacent systems to reduce their interference free transmission intervals. The other systems will consider the request, and when possible will accept the request, by indicating an agreed new interference-free operating interval. The duration of each sub-frame may be negotiated through inter-system communication and using the common DRRM policy.

15.4.2.1.2 Scheduling of interference free intervals in the context of IEEE 802.16 MAC

A number of repetitive scheduling approaches are presented below, for Tx synchronized intervals. The same approach is valid for Rx intervals.

- *Type I*: The MAC frame, for each Tx and Rx part, is split into N+1 sub-frames:

- o One for non-interfering traffic, when systems can use the sub-frame in common, by operating in parallel
 - o All the other subframes are each used by another single system, which assumes the Master role for that sub frame, and traffic of other systems that do not interfere with it.
- *Type 2:* The MAC frame is split into two sub-frames: one for non-interfering traffic and one in which a single system is assuming the master role and traffic of other systems that does not interfere with it. Each Base Station will assume the Master role after M frames

The duration of each sub-frame, in a given community, is calculated as follows:

For type 1:

$$T_{Tx_sub-frame} = T_{TxMAC} / (N+1)$$

or

$$T_{Tx_sub-frame} = (T_{TxMAC} - T_{Txsh}) / N$$

$$T_{Rx_sub-frame} = T_{RxMAC} / (N+1)$$

or

$$T_{Rx_sub-frame} = (T_{RxMAC} - T_{Rxsh}) / N$$

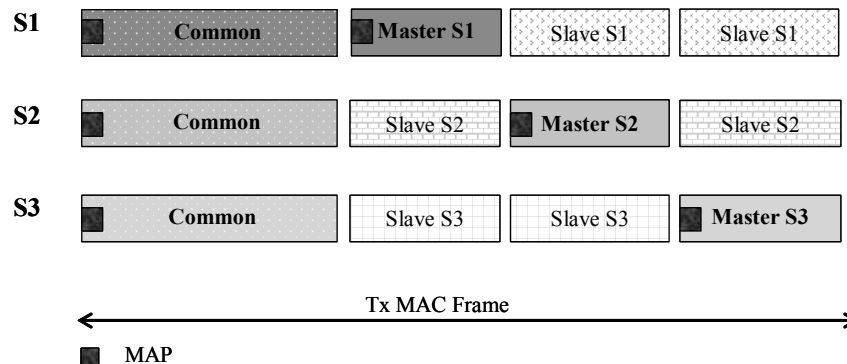


Figure h37—Sub-frame structure type1

For type 2:

$$T_{Tx_sub-frame} = T_{TxMAC} / 2$$

or

$$T_{Tx_sub-frame} = T_{TxMAC} - T_{Txsh}$$

$$T_{Rx_sub-frame} = T_{RxMAC} / 2$$

or

$$T_{Rx_sub-frame} = T_{RxMAC} - T_{Rxsh}$$

and the repetition interval equals to $N \cdot T_{MAC}$,

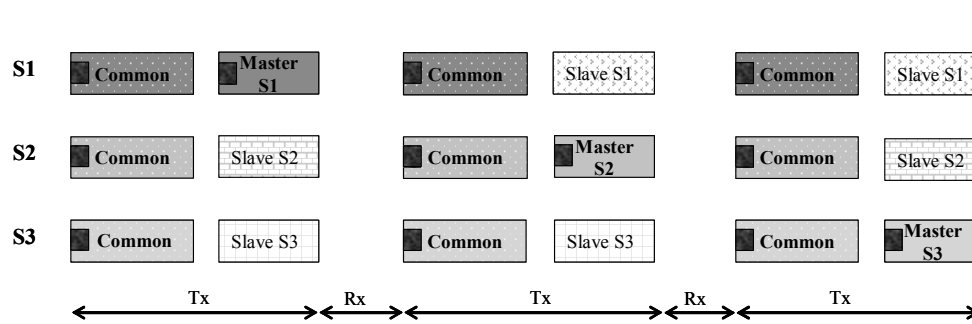


Figure h38—Sub-frame structure type 2

where:

— T_{MAC} , T_{TxMAC} , T_{RxMAC} are the durations of the respectively the MAC frame, Tx interval and Rx interval of the MAC frame;

— T_{Txsh} , T_{Rxsh} are the durations of the shared sub-frames. In the above relations, the meaning of Tx or Rx is relative to the usage of the MAC Frame by a Base Station.

During a sub-frame the Base Station which has the Master role may use its maximum power;

During some of the Master sub-frames, the Base Station will create a slot, possibly not overlapping with another slot of a coexistence neighbor Base Station, during which every transmitter (BS or associated SS) will send a predefined signal; this signal, called “radio signature”, will be used to measure the interference created by that transmitter.

- The “radio signature slot” for a Base Station will be created during its Tx Master sub-frame, every B MAC-frames;
- The “radio signature slot” for a Subscriber Station will be created during the Rx Master sub-frame;
- UL MAP and suitable UIUC for scheduling the “radio signature” are t.b.d.
- During the “radio signature” intervals, all the other BSs and SSs shall use a GAP interval, during which no transmission is to be made;
- The Base Station shall provide enough transmit opportunities for the active SSs.

Figure h 39 shows the possible allocation of the “radio signature” transmission opportunity for a given system, using for example the Type 1 repetitive pattern, with a focus on system 2.

The system 2 will transmit its Base Station radio signatures from time to time (every N MAC intervals); different radio signatures will be sent for every used power/sub-channelization/OFDMA sub-channel/ spatial direction combination. During these intervals the other Base Stations will schedule a GAP interval, in order to identify one Base Station solely. Base Stations using the same MAC sub-frame as the Master sub-frames shall schedule the transmission of their “radio-signatures” in such a way that they will not interfere with each other.

The transmission of “radio-signatures” used by the active SSs will take place during the Master sub-frame, from time to time (a timer shall be defined). The repetition period and the duration of the signature transmission shall be a parameter in the BS Database. The active SSs will provide a signature for every used power/OFDMA/sub-channelization/ direction setting.

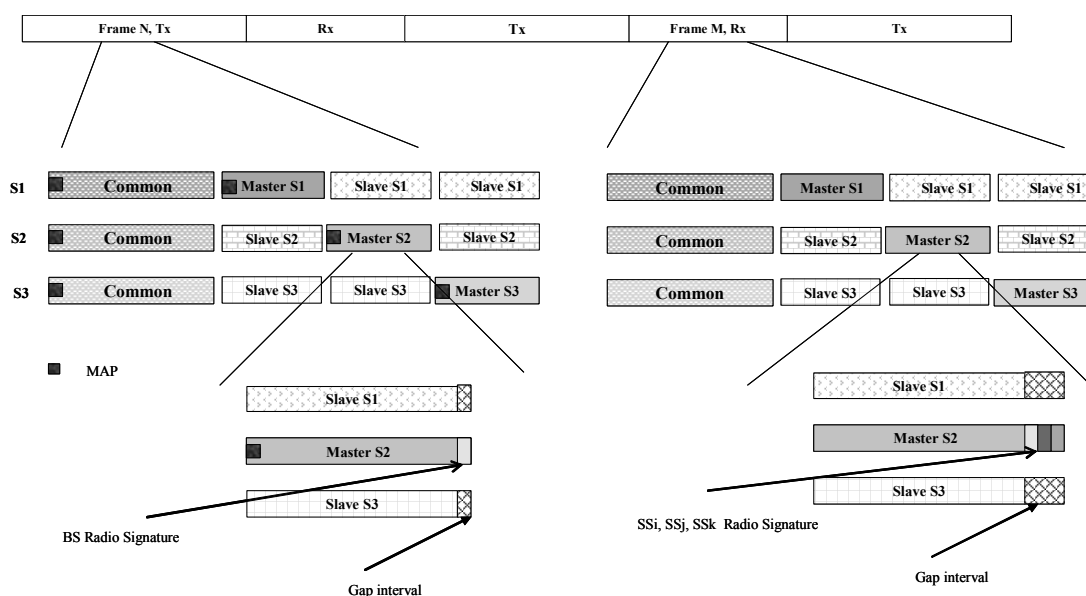


Figure h39—Allocation of slots for BS and SS radio signature

The BS data base will include:

- Operator ID
- Base Station ID
- MAC Frame duration (same for a community)
- Shared Tx and Rx sub-frame durations (same for a community)
- Type of sub-frame allocation (same for a community)
- MAC Frame number and sub-frame number chosen for the Master sub-frame (same for a community)
- Repetition period for Base Station radio-signature, measured in MAC-frames
- *Repetition interval between two Master sub-frames*, measured in MAC-frames
- *List of other used sub-frames*, in the interval between two Master sub-frames
- Time_shift from the Master sub-frame start, duration and the repetition information for the Base Station radio-signature transmission
- Time_shift from the Master sub-frame start, duration and the repetition information for the Subscriber Station radio-signature transmission
- *Time_shift from the Master sub-frame start and duration for network entry of a new Base Station*, which is evaluating the possibility of using the same Master slot.
- BS power relative to radio-signature, in the used sub-frames, in the interval between two Master subframes;
- For every active SS: SSID and its attenuation relative to radio-signature power, in the used sub-frames, in the interval between two Master sub-frames;

- For every coexistence neighbor BS: the BSID, the IP address of the coexistence neighbor and other profile information, and the SSs it interfered to, (and the SSs belong to it that interfered by the database owner BS.tbd.)
- For every BS in the same community: the contact IP address and the interference situation between this BS and other BS, including the interference situation with the DB owner.
- For every SS registered: the interference situation, the number of interference source, the IP address and RSSI of each source detected by the SS.

At the MAC level, the Master sub-frame is scheduled by using the Coexistence Zone.

The following figures show examples of the usage of the CXZ and the relation with the Master sub-frame types 1 and 3:

The Coexistence Zone attributes will indicate to the SS the mode in which a CXZ is used. The CXZ scheduling as Master sub-frame gives an indication of limited interference during this time. An SS is allowed to use its maximum power during a CXZ.

The coexistence Zone may use a private MAP, due to the fact that users of the zone may not be able to decode the MAP at the beginning of the MAC Frame. The duration and scheduling of the CXZ are included in the CXZ IE (see 8.4.5.3.28 and 8.4.5.4.29).

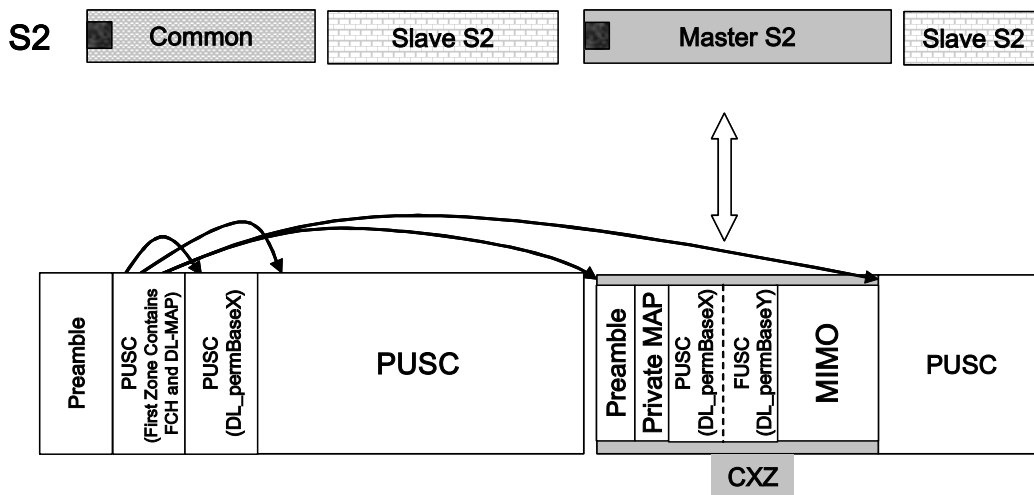


Figure h40—Relation between Master sub-frame type 1 and the CXZ

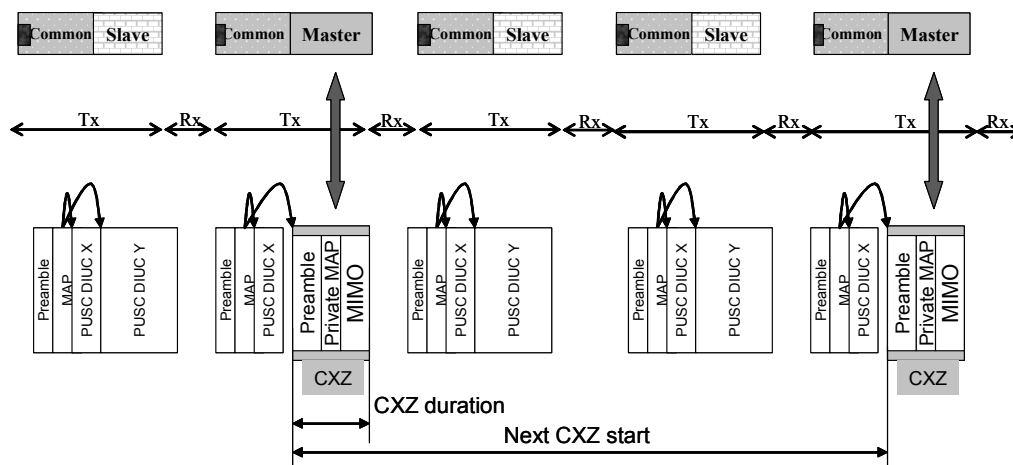


Figure h41—Relation between Master sub-frame type 2 and the CXZ

15.4.2.2 Sub frame distribution optimization

When WirelessMAN-CX system have to share one channel with its neighbor system, it shall allocated a sub-frame as its master subframe. By checking the information table (see 15.3.3), if it can find some subframes free in any channel it can take up in its neighborhood, it can randomly choose one of them as it's master sub-frame and start operation.

When not able to find a free subframe currently, the system shall check in any of it capable channel if there is some subframe on which all the neighbor systems using it as the master subframe have alternative sub-frame (ALTSF). The system can negotiate with the systems occupying one of these subframe to move to there ALTSF and vacate a subframe for itself without change the current structure of WirelessMAN-CX frame.

The system shall check with these kind of subframe one by one and negotiate with its neighbors taking it as its master subframe to move to it's ALTSF before it succeed. If the system succeeded on one of this sub-frame, it can take this subframe as it's master subframe, otherwise, it means that the system fails in vacating a current subframe as its master subframe by subframe distribution optimization. The figure of procedure to find a current subframe as its master subframe for a system is shown below:

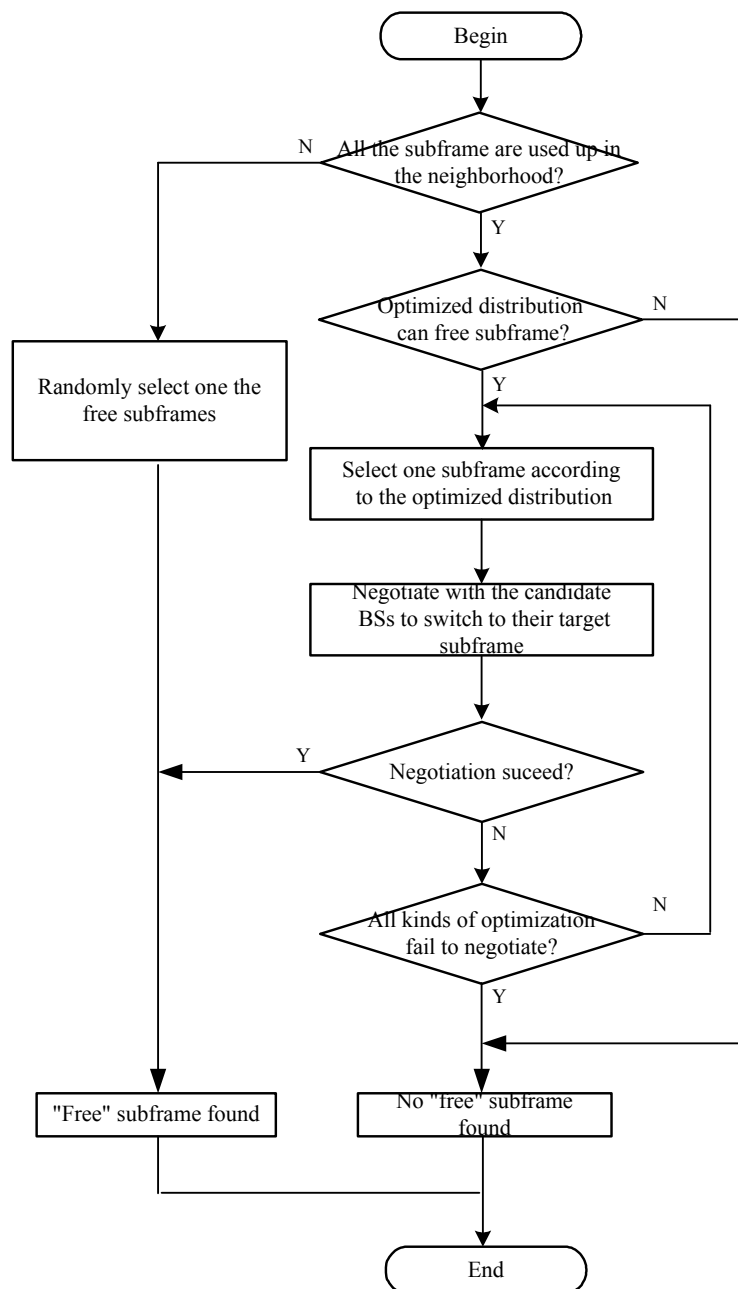


Figure h42—The procedure to find a current subframe as its master subframe

Similar to the channel distribution optimization (see 15.4.1.2), the order of the subframe to be checked maybe counted on the user using it as master subframe.

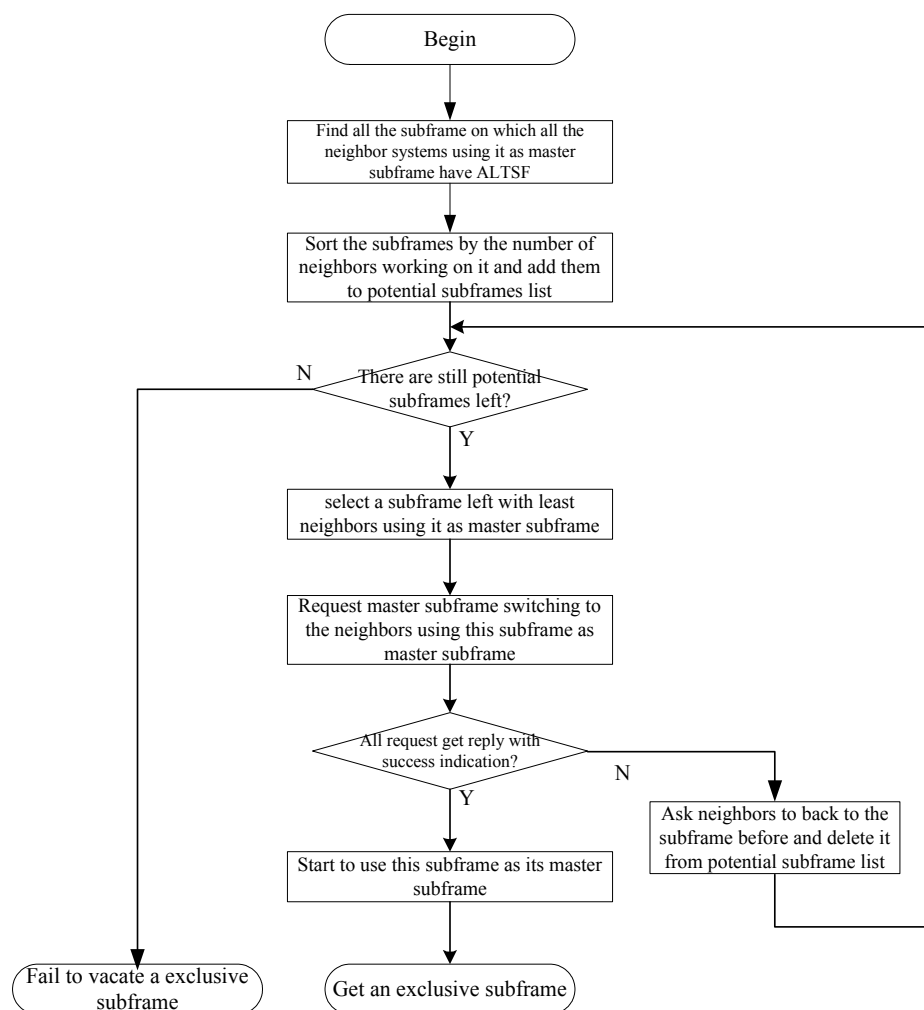


Figure h43—Process of subframe distribution optimization

Finding all the subframe on which all the neighbor systems using it as master subframe have ALTsf, the system can sort the subframes by the number of neighbors working on it and add them to potential subframe list. Everytime the system should choose a subframe with least neighbors using it as master subframe and negotiate to the neighbors, requesting the neighbor systems currently using this subframe as its master subframe to switch to one of its ALTsf. If all the request succeed, the system can switch to this channel and start to use this subframe as its master subframe, otherwise the system need to ask all the neighbors to keep using their original subframe and deleted the subframe from the potential subframe list. If all the potential subframes in the list have been checked and no one can be vacated as master subframe of the system, the process of subframe distribution optimization is failed to get a exclusive current subframe as the master subframe for the system.

15.4.2.3 Creation of a new sub-frame

If none of the existing sub-frames can be used, a *new Base Station may request the addition of another sub-frame*. The effect of such a request will be the reduction of operating time for those Base Stations that inter-

1 fere with the new system. However, all the others, which do not interfere with it, may work in parallel and
 2 use the same operating time as before the introduction of the new BS.
 3

4 A Base Station will request the creation of a new sub-frame by:
 5

- 6 — Sending IP messages to all the member BSs of the community, indicating:
 - 7 o The interfering operator ID and BS ID
 - 8 o The MAC frame-number in which the addition of a new sub-frame will take place.
- 9 — All the requested BSs will *acknowledge the request*, by
 - 10 o Sending back a message having as parameters:
 - 11 o Frame-number for the change (must be the same as the requested one
 - 12 o Master sub-frame number for the new BS ($SF = \text{old SF} + 1$).
 - 13 o If a neighbor BS fails to acknowledge, it will be asked again, for additional M attempts,
 - 14 after that other means (such as cognitive radio signalling) should be applied, or it will be
 - 15 considered as a non WirelessMAN-CX compliant;
 - 16 o At the above specified MAC frame number, a new sub-frame partition will take place, by
 - 17 inserting in the sub-frame calculation relation $N=N+1$
 - 18 o The BSs will up-date their own SSs about the change
- 19 — Start to use the created Master sub-frame.

30 15.4.2.4 Interference Control in sub-frames

31 The interference control procedures can use interferer identification obtained from the radio signature

- 32 — A receiver will listen to the media during the radio signature slot and will find out which are the
 33 strongest interferers; by then scanning the BS databases it will be possible to identify, by the frame
 34 number, sub-frame number and offset, which BS is the associated interferer; based on time-shift
 35 information, the Base Station will be able to identify the Subscriber Station ID. During the allo-
 36 cated radio-signature transmit opportunity no other radio transmitters will operate.

37 Interference reduction

- 38 — A BS has the right to request any interferer to reduce its power by P dB, for transmissions during
 39 the time in which this Base Station is the Master; if the requested transmitter cannot execute the
 40 request, it has to cease the operation during the Master sub-frame of the requesting Base Station;
 41 The system which uses the sub-frame as a Master can use the maximum powers with no limitation.
 42 A newly entering system is allowed to use the same sub-frame at its maximum power if the first
 43 system allows this, otherwise it has to reduce its power to a level acceptable by the first system
 44 using the sub-frame as Master. The first system has the right to not allow the operation of any other
 45 system in parallel, if this causes harmful interference to it. A system cannot use more than one sub-
 46 frame as a Master.

47 Sharing the Master time

- 48 — A Base Station shall indicate in the data base *what portion of the sub-frame time, Tx and Rx sepa-*
 49 *rately, is actually used*
- 50 — Other systems, which do not interfere with each other, may use that time interval

1 Target acceptable interference levels during Master sub-frames:

2
3 An acceptable interference level during a Master sub-frame should be lower than 3dB above the noise or
4 12dB below the signal.
5

6 7 8 9 **15.4.2.4.1 Controlling interference during master sub-frame**

10 11 **15.4.2.4.1.1 Interferer identification**

12
13
14 *[editor's note: the following 2 paragraph is redundant with the text in 15.3.]*
15

16 The interferers will be identified by their radio signature, for example a short preamble for OFDM/OFDMA
17 cases. The radio signature is defined by the following parameters:

- 18 — Peak power
- 19 — Relative spectral density
- 20 — Direction of transmission.

21
22 Every transmitter will send the radio signature during an interference-free slot. The time position of this slot
23 (frame_number, sub-frame, time-shift) will be used for identification.
24

25 In IBS's coexistence neighbor discovery phase, the IBS's contact information and RTK shall be broadcast
26 using the BS_NURBC frame with pulse energy keying. And this shall be detected by coexistence neighbor's
27 SS in the IBS's coverage (see ANNEX C.1 case 3) and reported to its serving BS.
28

29 The BSID is used to identify the coexistence neighbor BS by the receiver SS. And also be the identifier of
30 the BS for its coexistence neighbor BS.
31

32 33 34 **15.4.2.4.1.2 Interference to BS**

35 The BS of the system which experience interference from the SSs in the neighbor systems can control the
36 interference, using the following procedures:

- 37 — Identification of the source of interference, using the procedures defined above;
- 38 — Request for transmit power reduction. If the sources of the interference are identified, the BS
39 should send message to the BSs of the interfering systems, asking them to drop the power of the
40 specified transmitter inside the neighbor systems by P dB.
- 41 — Request for stopping the operation. Alternatively, the BS could send message to the BSs of the inter-
42 ference source systems, asking the interference source system to stop operating during this BS's
43 master slot.

44
45 The interference status information of this BS in the system and the interference status information in the
46 coexistence message from its neighbor systems should be stored and updated regularly into the database of
47 this system.
48

49 50 51 **15.4.2.4.1.3 Interference to SS**

- 52 — Report to BS about experienced interference
- 53 — List of frame_number, sub-frame, offset, IP address of source BS (if detected)
- 54 — BS start process for interference reduction with feedback from the SS.

15.4.2.4.2 Controlling interference during not-interfering traffic sub-frames

The Base Station data base shall keep the following information regarding the usage of “ non-interfering sub-frame” or Master sub-frames belonging to other systems:

- BS power, relative to the radio signature *power*, when using each of the sub-frames;
- List of SSs and their power, relative to the radio signature *power*, when using each of the sub-frames.

The received power during other sub-frames can be obtained by using the radio signature measurement and suitable calculations, according to data-base information on used powers. Messages as Stop_Operating_Request and Reduce_Power_Request can be used for controlling the interference levels.

15.4.2.5 Credit token based coexistence protocol

Spectrum sharing between several systems (SYSs) can be achieved by the sharing a common MAC frame among different systems as exemplified by [Figure h 44](#). In such a MAC frame structure, dedicated portions (denoted as “master system sub-frames”) of the frame are periodically and exclusively allocated to a system (denoted as the “master system”) respectively in the forward and reverse link. The terminology used hereafter defines a slave system as a system that may operate during the other master systems sub-frames. With respect to this definition, the slave system sub-frames are the time intervals operating in parallel of the master systems sub-frames.

Additional flexibility can be provided by such a frame structure if the length of each master sub-frame(interference free sub-frame) can be dynamically adjusted as a function of the spatial and temporal traffic load variations of each system as stated in section 15.1.4.

To achieve this, this section proposes the dynamic coordination of the frame structure sharing between BSs when several master systems compete to share this common shared MAC frame.

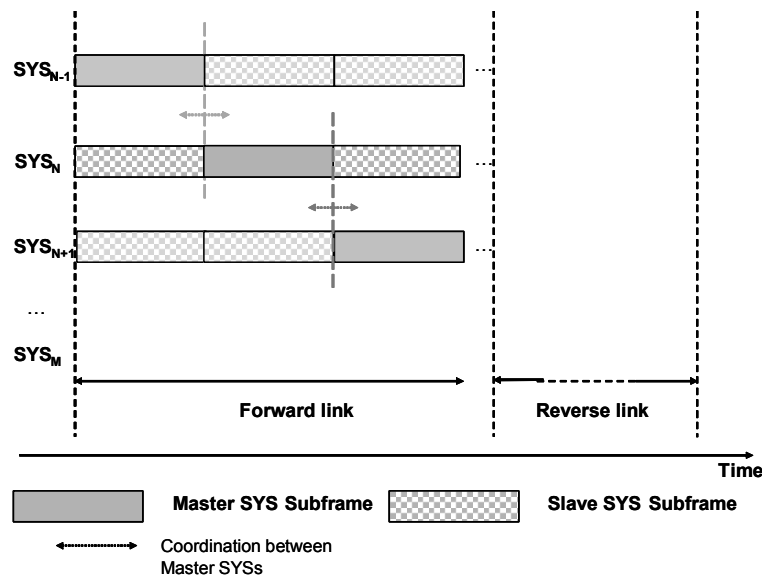


Figure h44—Example of TDD based MAC frame sharing structure between M SYSs

15.4.2.5.1 General principle

In order to resolve contention in accessing the channel and resources scheduling issues between systems, the first step consists of defining credit tokens and designing appropriate negotiation mechanisms. Then, on the basis of the usage of the credit tokens based mechanisms, the second step consists of managing dynamically(temporally) the bandwidth requests and grants mechanisms for the sharing of the master sub frames within the common MAC frame.

Based on the credit tokens transactions (assignment, release and awarding), these two steps provide the mechanisms to enable spectrum efficiency and a fair spectrum usage in a real time fashion, while ensuring both the master and slave systems QoS. These two steps enable to manage spectrum sharing between master systems themselves. The result is the dynamic shaping of the MAC frame structure sharing as a function of the traffic intensity variations, and the dynamic credit tokens portfolio account of the master systems. The transaction mechanisms are detailed in the following sections.

15.4.2.5.2 Credit tokens assignment and usage principles

- Each system is initially allocated with a given credit tokens budget.
- Negotiation for spectrum sharing between systems is based on credit tokens transactions.
- Credit tokens transactions occur dynamically between a credit tokens offeror (master system owner of the radio resources during the active master sub-frame) and one or several credit tokens requesters (the other master systems).
- The negotiation occurs dynamically between master systems to agree the length of each master sub-frame as a function of the spatial and temporal traffic load variations need of each master system.

15.4.2.5.3 Negotiation between master systems

15.4.2.5.3.1 Definition and notation

- BS_N denotes the BS belonging to the master SYS_N .
- BS_k denotes the BS belonging to the slave SYS_k .
- Each BS_k can dynamically propose a number of credit tokens $BS_CT^{(n)}_k$ at the n th iteration. This proposal corresponds to the number of credit tokens per time unit corresponding to the BS_k during the n^{th} iteration of the negotiation phase.
- Resource scheduling is carried out by an auction inspired mechanism. The negotiation type used for the scheduling is dynamic in time. Starting from minimum number of credit tokens required (MRCTN) by the master BS to its share radio resources, the number of credit tokens is iteratively increased (at each iteration n) until the winning requesters remain.

15.4.2.5.3.2 Dynamic credit tokens based scheduling cycle

The dynamic scheduling cycle aims at coordinating between one BS_N of master SYS_N and several BS_k of different slave SYS_k . For the sake of simplicity, the cycle is illustrated (Figure h 45 and Figure h 46) for one BS_N and one BS_k of a given slave SYS_k . The cycle is composed of different phases, and each phase can be composed of several sequences as follows.

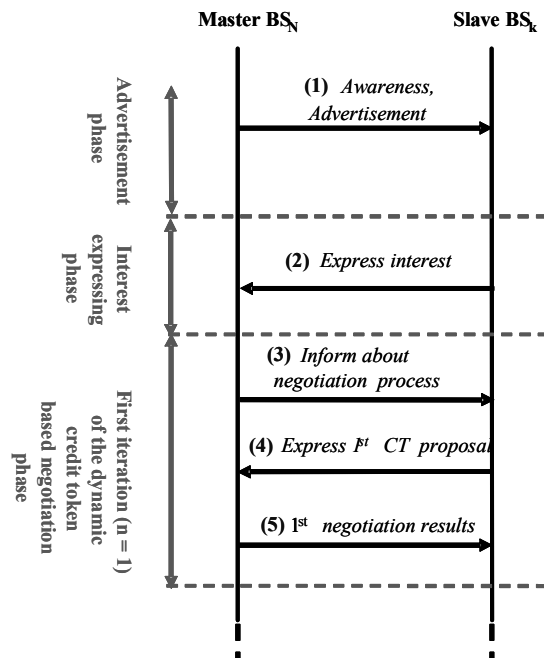


Figure h45—Dynamic (iterative) credit tokens based scheduling cycle (sequences (1) to (5))

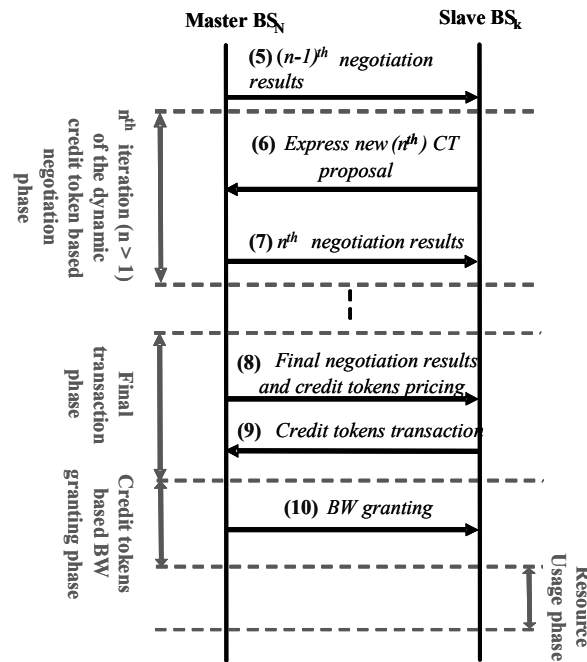


Figure h46—Dynamic (iterative) credit tokens based scheduling cycle (sequences (5) to (10))

15.4.2.5.3.3 Negotiation mechanisms between master systems

For each of the phase of the credit tokens based scheduling cycle presented in section 15.4.2.5.3.2, this section 15.4.2.5.3.3 describes the details of the enhanced mechanisms.

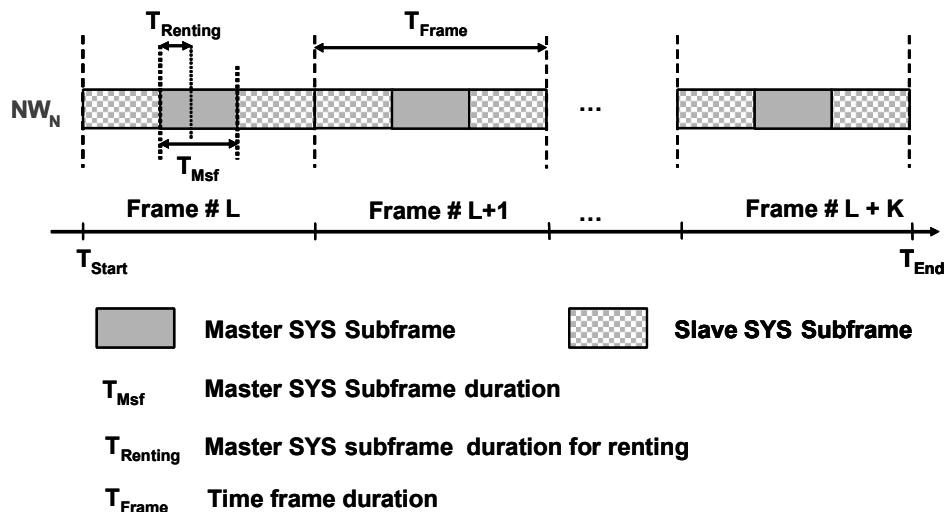


Figure h47—Simplified MAC frame structure illustrating master system sub-frame renting

principle and associated notations

Advertising/Awareness phase

This phase is composed of the single sequence (1) as follows:

- The master SYS_N (offeror) advertises that its periodic assigned master sub-frame is open for renting (Figure h 47) from starting time T_{Start} to ending time T_{End} for a fraction ($T_{Renting}/T_{Msf}$) of its master sub-frame duration T_{Msf} . $T_{Renting} = T_{End} - T_{Start}$.
- The master SYS_N proposes a minimum number of credit tokens required (MRCTN) for this renting. The MRCTN is expressed as a number of credit tokens per time unit.

Interest expressing phase

This phase is composed of the single sequence (2) as follows: each BS_k informs the master BS_N about its willingness (or not) to participate to the negotiation. If the BS_k is interested, it communicates its id_k to the master BS_N .

First iteration ($n = 1$) of the dynamic credit tokens based negotiation phase

This phase is divided into 3 sequences as follows:

- In sequence (3), the master BS_N provides the following information to the slave BS_k s that have expressed the interest to participate to the negotiation:
 - o $T_{Start\ Negotiation}$: time from which the negotiation phase will start,
 - o $T_{End\ Negotiation}$: time at which the negotiation phase will end ($T_{End\ Negotiation} < T_{Start}$),
 - o Note: For this first iteration ($n = 1$), the initial $\{id_k\}$ is noted $\{id^{(1)}_k\}$.
- In sequence (4), each BS_k provides the following information to BS_N : $CTP^{(1)}_k = \{BS_CT^{(1)}_k, x_k, T_{Start\ k}, T_{End\ k}\}$ where:
 - o $CTP^{(1)}_k$ is the credit tokens proposal vector of BS_k at the first ($n = 1$) iteration of the negotiation with the master BS_N . $CTP^{(1)}_k$ is composed of $BS_CT^{(1)}_k, x_k, T_{Start\ k}$ and $T_{End\ k}$
 - o $BS_CT^{(1)}_k$ is the number of credit tokens per time unit proposed by BS_k for the first iteration,
 - o x_k is the fraction of $T_{Renting}$ for which $BS_CT^{(1)}_k$ applies for,
 - o $[T_{Start\ k}, T_{End\ k}]$ is the time interval for which $BS_CT^{(1)}_k$ applies for. $[T_{Start\ k}, T_{End\ k}] \subset [T_{Start}, T_{End}]$.
- In sequence (5), BS_N performs the following action:
 - o Given the set of intervals $\{[T_{Start\ k}, T_{End\ k}]\}$ received from different requesters $\{id^{(1)}_k\}$, BS_N partitions $\{[T_{Start}, T_{End}]\}$ into contiguous time segments $\{TS_m\}$. Each TS_m corresponds to a time window (integer number of T_{Frame}) in which a subset of intervals of $\{[T_{Start\ k}, T_{End\ k}]\}$ overlap.
 - o The different requesters $\{id^{(1)}_k\}$ assigned to a given TS_m are identified by $\{id^{(1)}_{k,m}\}$. $\{id^{(1)}_{k,m}\}$ compete for each TS_m . Each involved requesters $id^{(1)}_{k,m}$ competes with his respective $CTP^{(1)}_k$.

- o Then, for each TS_m , the master BS_N calculates the payoff $P_k^{(1)} = BS_CT_k^{(1)} * x_k * T_{Renting} * N_{Frame\ m}$ for each requester k , and searches the subset ($\{id_{k,m}^{(1)}\}_{selected}$) of $\{id_{k,m}^{(1)}\}$ such as $\sum(x_k) = 1$ and $\sum(P_k^{(1)})$ is maximal. $N_{Frame\ m}$ is the number of frames within TS_m ($N_{Frame\ m} = TS_m / T_{Frame}$).
- o For each TS_m , BS_N informs all $\{id_{k,m}^{(1)}\}$ about $P_m^{min, (1)}$ and $P_m^{max, (1)}$ where $P_m^{min, (1)}$ is the minimal payoff from $\{id_{k,m}^{(1)}\}_{selected}$ and $P_m^{max, (1)}$ is the maximal payoff from $\{id_{k,m}^{(1)}\}_{selected}$ during the first iteration. With this approach, each BS_k is directly informed whether it has been selected or not, and has some information on how far it is from $P_m^{min, (1)}$ while still having some information on $P_m^{max, (1)}$. This approach enables to keep the privacy of competing $\{id_{k,m}^{(1)}\}$ on TS_m .

n^{th} iteration of the credit dynamic tokens based negotiation phase

This phase is composed of 2 sequences as follows:

— In sequence (6):

- o If $P_k^{(1)} < P_m^{min, (1)}$, this means that BS_k has not been selected for being granted the resources he has requested for during the first iteration $n = 1$. More generally speaking, for $n > 1$, if $P_k^{(n-1)} < P_m^{min, (n-1)}$, this means that BS_k has not been selected for being granted the resources he has requested for during the $(n-1)^{th}$ iteration.
- o If $P_k^{(n-1)} < P_m^{min, (n-1)}$ and if BS_k is still interest to be allocated with the additional resources he initially requested for, it can propose a new $BS_CT_k^{(n)}$ for the n^{th} iteration. Then, BS_k computes the new $P_k^{(n)} = BS_CT_k^{(n)} * x_k * T_{Renting} * N_{Frame\ m}$ where $x_k, T_{Renting}$ and $N_{Frame\ m}$ are fixed for all n on TS_m .
- o If $P_k^{(n)} > P_k^{(n-1)}$ and $P_k^{(n)} > P_m^{min, (n-1)}$, BS_k expresses its interest to keep on participating in the negotiation with the new proposal $P_k^{(n)}$. In that case, it informs BS_N with its new (update) value of $BS_CT_k^{(n)}$. In case $P_k^{(n)} = P_k^{(n-1)}$ or $P_k^{(n)} < P_m^{min, (n-1)}$, BS_k leaves the negotiation phase and will not be granted with the additional resources he asked for.

— In sequence (7), BS_N updates $\{id_{k,m}^{(n-1)}\}$ into $\{id_{k,m}^{(n)}\}$. Based on the new received proposals $\{BS_CT_k^{(n)}\}$ for each TS_m , the master BS_N calculates the new payoff $P_k^{(n)} = BS_CT_k^{(n)} * x_k * T_{Renting} * N_{Frame\ m}$ for each requester k who still participates to the negotiation. Then, for each TS_m , BS_N searches the subset ($\{id_{k,m}^{(n)}\}_{selected}$) of $\{id_{k,m}^{(n)}\}$ such as $\sum(x_k) = 1$ and $\sum(P_k^{(n)})$ is maximal. Next, BS_N performs the same actions as in sequence (5): for each TS_m , BS_N informs all $\{id_{k,m}^{(n)}\}$ about $P_m^{min, (n)}$ and $P_m^{max, (n)}$ where $P_m^{min, (n)}$ is the minimal payoff from $\{id_{k,m}^{(n)}\}_{selected}$ and $P_m^{max, (n)}$ is the maximal payoff from $\{id_{k,m}^{(n)}\}_{selected}$ during the n^{th} iteration.

Final negotiation results and credit tokens pricing

This phase is composed of two sequences as follows:

— In sequence (8):

- o As long as $T_{Start\ Negotiation}$ has not been reached (i.e. the negotiation phase duration has not yet elapsed), n is increased and the credit tokens based negotiation phase mechanisms of the previous paragraph “ **n^{th} iteration of the dynamic credit tokens based negotiation phase**” are applied.

- o When $T_{\text{Start negotiation}}$ has been reached, negotiation phase is over. None BS_k can propose a new credit token proposal. $\{id_{k,m}^{(n \text{ final})}\}_{\text{selected}}$ is derived. At this point, BS_N derives the final credit tokens price BS_CPA_k (expressed as a number of credit tokens per time unit) for each TS_m and each k from $\{id_{k,m}^{(n \text{ final})}\}$. For each k and m , BS_CPA_k can correspond to the $BS_CT^{(final)}_k$, or for example can follow another price derivation method.
- In sequence (9), each BS_k is requested to provide $Pr_k = BS_CPA_k * x_k * T_{\text{Renting}} * N_{\text{Frame } m}$ credit tokens to BS_N to be allowed to use the resources it has been assigned after the negotiation on its corresponding TS_m . Provided that Pr_k does not exceed the credit tokens budget of BS_k , the credit tokens transaction between BS_N and each BS_k is performed.

Credit tokens based bandwidth granting phase

This phase is composed of the single sequence (10). During this phase, BS_N grants the resource to each BS_k who has successfully performed the credit transaction operation in sequence (9).

Resource usage phase

After BS_k has been granted with the resources, BS_k can use them during $x_k * T_{\text{Renting}}$ time unit of SYS_N and for $N_{\text{Frame } m}$ frames from the beginning on its corresponding TS_m .

15.4.2.5.4 Inter BSs communication

The credit tokens mechanisms (section 15.4.2.5.3) require inter BSs communication between different systems. This inter BS communications is necessary to exchange the parameters related to the credit tokens based negotiation cycle.

The primitive parameters include: T_{Start} , T_{end} , $T_{\text{End_Renting}}$, $T_{\text{Start_Renting}}$, T_{Msf} , $MRCTN$, id_k , $BS_CT^{(n)}_k$, x_k , T_{Start_k} , T_{End_k} .

The derived parameters include: TS_m , $\{id_{k,m}^{(n)}\}_{\text{selected}}$, $p_{m}^{\text{min}, (n)}$, $p_{m}^{\text{max}, (n)}$.

These parameters are stored into the regional LE DB and into the local database of each LE BS of the shared distributed system architecture (section 15.1.5).

The information exchange about these parameters between these databases and the RADIUS/BSIS servers is performed by IP based wired using the co-existence protocol (CP). This inter BS communication is supported by the inter system messages defined in the shared distributed system architecture (section 15.1.5).

The inter BS communications to support the signaling messages related to the awareness/advertisement sequence of the credit tokens based co-existence protocol can also be implemented by secured over the air mechanisms described in section 15.4.2.5.5.

15.4.2.5.5 Radio Resources Sharing Opportunities Advertisement Discovery

Over the air signaling for the first phase (advertisement) of the negotiation cycle would be also of great support to facilitate urgent (critical time) radio resources sharing opportunities discovery between IEEE Wire-

lessMAN-CX systems themselves, but also between IEEE WirelessMAN-CX systems and non IEEE WirelessMAN-CX systems. This section describes signaling discovery procedures so that:

- Master BSs can advertise periodically to the neighbouring slave BSs about their offers of radio resources for renting. This enables the slave BSs to be aware of master BSs' offers.
- Slave BSs can inform periodically the surrounding cells about their search of radio resources sharing opportunities for renting. This enables slave BSs to inform the master BSs that they are looking for temporally some additional radio resources.

Specific master BS and slave BS downlink time intervals (TBD) are used to support the over the air advertisement discovery messages in support of the credit tokens based negotiation. These messages, not yet defined, are temporary called respectively MATI (Master Advertisement Time Interval) and SATI (Slave Advertisement Time Interval).

Usage of the advertisement discovery MAC frame structure

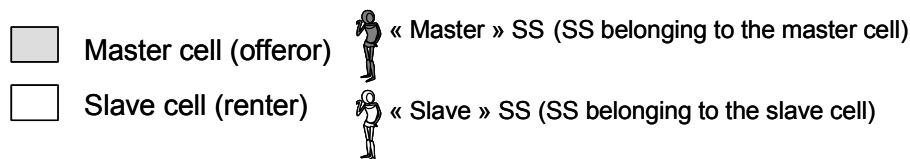
The usage of MATI and SATI is described in this paragraph.

- The MATIs are dedicated to master BS transmissions in downlink.
- Each MATI is used by a master BS in downlink for broadcasting. At a given time, each MATI can only be used by a single BS among the co-existence neighbourhood. However, a same MATI can be used by different BSs at different times.
- Each master BS can use any MATI provided it is not already used by any other MATI BS of the co-existence neighbourhood.
- MADD (Master Advertisement Discovery Descriptor) message is sent in MATI (Section 6.3.2.3.64).
- The MATIs are ranked in each *Advertisement discovery sequence* in such a way that the first MATI is assigned to the master BS whose renting period will occur first (i.e. min of the T_Start_M), the second MATI is assigned to the master BS whose renting period will occur in second, and so on. Re-ranking is updated dynamically each time a new master BS is arriving. This mechanism avoids the SSs of the slave cells (see paragraph "*Advertisement discovery from master cell by slave cell*" below) to scan all MATIs when the slave cells have to find very shortly some available resources to rent. In this manner, they have directly knowledge of the next available resources they can propose credit tokens for.
- Each master cell releases the MATI it is using when its negotiation starting time has elapsed. This enables new arriving master cells to use this MATI (eventually after the re-ranking) to advertise incoming channels reuse opportunities.
- The SATIs are dedicated to slave BS transmissions in downlink.
- Each SATI is used by a slave BS in downlink for broadcasting. Each SATI can only be used by a single BS among the co-existence neighbourhood. However, a same SATI can be used by different slave BSs at different times.
- Each slave BS can use any SATI provided it is not already used by any other slave BS of the co-existence neighbourhood.
- SADD (Slave Advertisement Discovery Descriptor) message is sent in SATI (Section 6.3.2.3.65).

- A "master" SS is a SS belonging to a master cell. A "slave" SS is a SS belonging to a slave cell.
- The MATI and SATI time positions are known by the "master" and "slave" SSs.
- There are no direct RF communications between the master and slave BSs. The master-slave BS communications are performed via master and slave SSs which act as RF bridges to convey the information as follows:
 - o A "slave" SS performs the RF bridge between its slave BS and the master BS (provided the coverage of the master cell overlaps with the slave cell area, and this slave SS is located in the overlapping area).
 - o A "master" SS performs the RF bridge between its master BS and the slave BS (provided the coverage of the slave cell overlaps with the master cell area, and this master SS is located in the overlapping area).
- Slave SSs in the overlapped (master/slave) cell area listen to the MATIs. Master SSs in the overlapped (master/slave) cell area listen to the SATIs.

15.4.2.5.5.1 Mechanisms enabling the discovery and the exploitation of the master cells originated advertisement discovery messages by the slave cells

This paragraph describes the mechanisms enabling the discovery and the exploitation of the master cells originated advertisement discovery messages by the slave cells. The terminology used in the following is:



These mechanisms are described by the different steps as illustrated in the following:

- 1- Policy instructions to the slave SSs by the slave BS

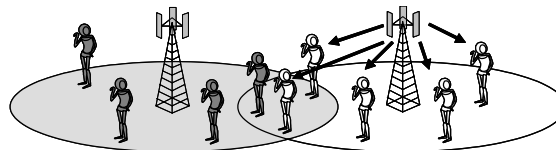


Figure h48—Policy instructions to the slave SSs by the slave BSs

- During this step, the slave BS initially instructs (by broadcasting) its SSs (in red) about the behaviours they have to adopt when some of these SSs get the messages from the different MATIs.
- The behaviour is instructed by the ADPD (Advertisement Discovery Policy Descriptor) message (section 6.3.2.3.66) specifies when some SSs (located in the overlapped area between this slave cell and surrounding master cells and getting MADD message from master BS) associated to this slave BS have to report the MADD information conveyed in MATI towards this slave BS.

- The slave SSs that can hear the MATIs and meeting the requirements sent in ADPD are the only SSs that are allowed to make the RF bridge between the master and slave cells. This means, the policy rules the transmissions from any slave SS towards the slave BS when these SSs are mandated to get feedback about the MATIs proposals. This mechanism avoids having incessant transmissions from the slave SSs towards the slave BS when the MATIs are not aligned with the slave BSs strategy. This saves bandwidth. Any policy can be established. Moreover, the policy can be adapted dynamically in time by the slave BS.

2- Detection and identification of the MATIs content by the slave SSs

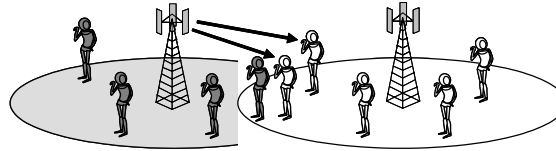


Figure h49—Detection and identification of the MATIs content by the slave SSs

- During this step, the slave SSs in the overlapping area between the master cell and their slave cell listen to the different MATIs sequentially. For each master cell, these slave SSs can get the information sent in the MADD message (Section 6.3.2.3.64).
- Provided the MADD message information received and the ADAP message received about the policy (section 6.3.2.3.66) established by the slave BS, the slave SS is able to decide whether it has to transmit this information to the slave BS or not.

3- Relaying of the MATIs content to the slave cell by the slave SSs

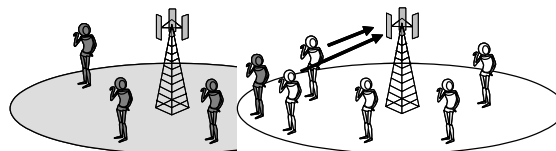


Figure h50—Relaying of the MATIs content to the slave cell by the slave SSs

- In case the policy requirements are met, the information collected by the slave SS is conveyed to the slave BS. The information the slave SS sends to its BS is the content of the MADD message.
- In order to ensure this information is appropriately received by the slave BS, the information is sent by several slave SSs (e.g. 2 slave SSs circulate this information to the slave BS in Figure h 50). This ensures both reliability and security check.

Note: In case the policies requirements sent in ADAP are not met, the slave SSs do not transmit the information. However, it would be possible for the slave SS to convey the information about the list LC (message included in MADD) to its slave BS since it will provide it some further information about other radio resources renting opportunities on other channel (frequency domain). This decision to send the LC information can be ruled by the policy.

4- Master BS - Slave BS communication through the backhaul

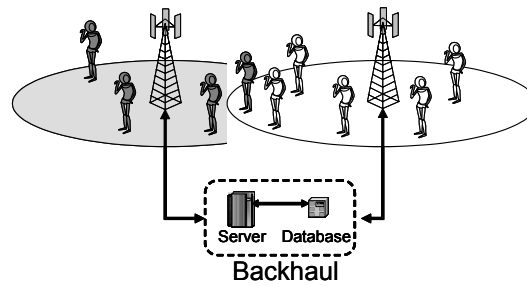


Figure h51—Master-Slave BS communication through the backhaul

After step 3, the slave BS knows the IP_Proxy_address_M (Section 6.3.2.3.64) associated to the master cell. Accordingly, the communications between master and slave cells (BSs) is performed through the backhaul to make the negotiation (Figure h 51) with the co-existence protocol (CP). The remaining phases of the credit tokens based negotiation cycle is performed via this backhaul with IP based communications using server(s) and database(s).

15.4.2.5.5.2 Mechanisms enabling the discovery and the exploitation of the slave cells originated requests discovery messages by the master cells

This paragraph describes the mechanisms enabling the discovery and the exploitation of the slave cells originated request discovery messages by the master cells. The terminology used in the following is the same as in the previous paragraph.

These mechanisms are described by the different steps illustrated as follows:

- 1- Detection and identification of the SATIs content by the master SSs

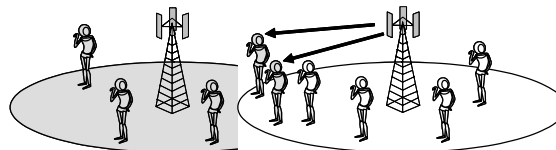


Figure h52—Detection and identification of the SATIs content by the master SSs

During this step (Figure h 52), the master SSs in the overlapping area between the master cell and their slave cell listen to the different SATIs sequentially. For each slave cell, these master SSs can get the information contained in the SADD message.

- 2- Relaying of the SATIs content to the master cell by the master SSs

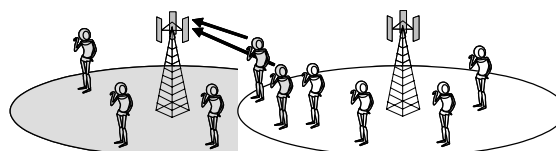


Figure h53—Relaying of the SATIs content to the master cell by the master SSs

- The SADD message information is reported by the master SS to its master cell (Figure h 53).
- In order to ensure this information is appropriately received by the master BS, the information is sent by several masters (e.g. 2 master SSs convey this information to the master BS in Figure h 53). This ensures both reliability and security check.

3- Master BS - Slave BS communication through the backhaul

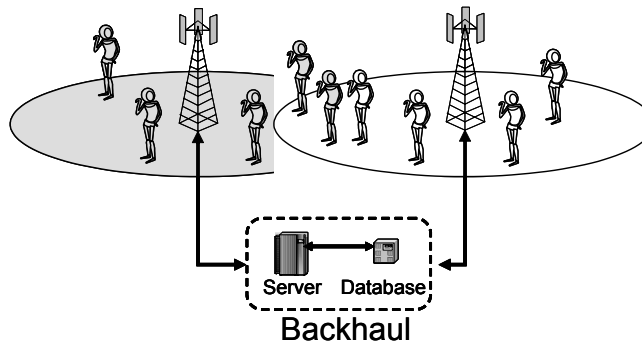


Figure h54—Master BS - Slave BS communication through the backhaul

After step 2, the master BS knows the IP_Proxy_address_S (Section 6.3.2.3.65) of the slave cell. Accordingly, the communications between master and slave cells (BSs) is performed through the backhaul to make the negotiation (Figure h 54) with the co-existence protocol (CP). The remaining phases of the credit tokens based negotiation cycle is performed via this backhaul with IP based communications using a server and database.

15.4.3 Interference prevention from Ad-Hoc systems

15.4.3.1 Operating principles

There could be deployments in which there is a combination of systems forming a community via an IP network and thus using the Coexistence Protocol, and other systems, deployed in the same area and frequency band, but are not connected via the IP network. These systems will be called here 802.16 ad-hoc systems. It should be clarified that those ad-hoc systems are still considered to comply with WirelessMAN-CX. The 802.16 ad-hoc systems will apply the Adaptive Channel Selection procedures and use radio signaling procedures to interact with systems using a Coexistence Protocol. The ad-hoc systems obtain a temporary Community registration status, that has to be renewed from time to time.

15.4.3.2 Registration

The WirelessMAN-CX pro-active radio approach defines signals and procedures for the reservation of the activity intervals and registration of ad-hoc systems. The operational procedures are described below:

- 1 — WirelessMAN-CX Community registered systems, using a Coexistence Protocol, will reserve the
2 MAC frame Tx/Rx intervals by using, during the MAC Frame N, starting at the absolute time AT1,
3 radio signals to indicate the MAC Tx_start, MAC Tx_end, MAC Rx_start, MAC Rx_end. These
4 signals are transmitted by Base Stations and Repeaters. These procedures will repeat after T_cogn
5 seconds; the values of these parameters are specified in section 10.5; No regular data transmission
6 should take place 20 ms from the start of AT1 (the maximum IEEE802.16 MAC frame duration).
7
8
- 9 — During the MAC frame starting at the absolute time AT2, cognitive signals will indicate the begin-
10 ning and the end of Master sub-frames, by transmitting signals indicating by their transmission start
11 the Tx_start, Tx_end, Rx_start, Rx_end for the specific sub-frame; these signals are transmitted by
12 Base Stations, Repeaters and those SSs which experience interference, at intervals equal with Ncog
13 MAC Frames; no regular data transmission should take place 20 ms from the start of AT2 (the
14 maximum IEEE802.16 MAC frame duration).
15
16
- 17 — The MAC frame starting at the absolute time AT3 is the beginning of a registration interval using
18 the cognitive signaling; the registration interval has the duration of Tcr_reg seconds; The ad-hoc
19 transmitters shall use during the MAC frame starting at the absolute time AT3, the marked master
20 sub-frames for sending their radio signature. The radio signature will be used for the evaluation of
21 the potential interference during the Master slot, to systems which use the sub-frame as Master sys-
22 tems.
23
 - 24
 - 25 o The radio signature will consist of a preamble and a MAC header, sent on the working
26 channel and using the same power and sub-carrier allocation, as used in the regular data
27 transmission mode;
28
 - 29 o The sub-frame starting at Tx_start is slotted, each slot having the duration of 100us. The
30 transmission of a radio signature will start at a slot boundary, as perceived by ad-hoc sys-
31 tems. No ranging assumptions were taken in the assessment of the slot duration.
32
 - 33 o An ad-hoc radio unit (BS, Repeater or SS) will send this signal using a random access
34 mode for Tcr_reg seconds, using the sub-frame intended for their regular transmission
35 (BSs and SSs use different sub-frames for transmission).
36
 - 37 o The ad-hoc transmitters will have to use the registration procedures every Tad_reg sec-
38 onds.
39
 - 40 o No regular data transmission should take place 20 ms from the start of AT3 (the maximum
41 IEEE802.16 MAC frame duration).
42
43
- 44 — Registration replay
45
 - 46 o The radio units using the Master sub-frame will send a NACK(see Table h 7) signal, dur-
47 ing the MAC Frame starting at the absolute time AT4, and using the same sub-frame as
48 used by the un-acceptable transmitter, if they appreciate that the ad-hoc transmitter will
49 cause interference. Typically, to a registration signal sent during a DL sub-frame, the
50 NACK will be sent by one or more SSs, while to a registration signal sent during UL sub-
51 frame, the NACK signal will be sent by a Base Station.
52
53
 - 54 o The NACK signal indicates that the requesting ad-hoc device cannot use the specific sub-
55 frame, while using the requesting radio signature
56
 - 57 o Same device may try again, if using a different radio signature (for example, lower
58 power).
59
 - 60 o Lack of response indicates that the registration is accepted for transmission during the spe-
61 cific sub-frame.
62
 - 63 o No regular data transmission should take place 20 ms from the start of AT4 (the maximum
64 IEEE802.16 MAC frame duration).
65

15.4.3.3 Selection of suitable reception sub-frames

An ad-hoc unit will identify suitable reception sub-frames, by using the ACS and Registration processes repetitively, searching for a suitable operation frequency. The practical interference situations, with synchronized MAC frames are BS-SS and SS-BS interference. Assuming similar transmit powers, the above mentioned processed will find, as result, Master sub-frames in which the path attenuations between interfering units are maximized.

15.4.3.4 Signaling procedures using frequency-keyed energy pulses

The signaling and message exchange between an ad-hoc system and systems which are members of a Community use frequency-keyed pulses. The frequency-keyed energy pulses use for every single sub-channel the preambles defined for subchannelization in the chapter 8.3.3.5.3. Every energy bin is mapped to a OFDM sub-channel (see Table 213-OFDM symbols parameters), as shown in the Table h 7. The channels using sub-carriers at band edge or in the center are avoided.

The following figures show the desired spectral density for radio signaling. Independent of the actual channel width, the preambles are sent using the narrowest channel possible in the band. In the following example, in which channels of 5, 10 and 20MHz may be used, the narrowest channel is 5MHz and any other system will be able to detect the preambles, which are not attenuated by any radio filter. The narrowest channel will be centered in the frequency domain around the actually used channel center.

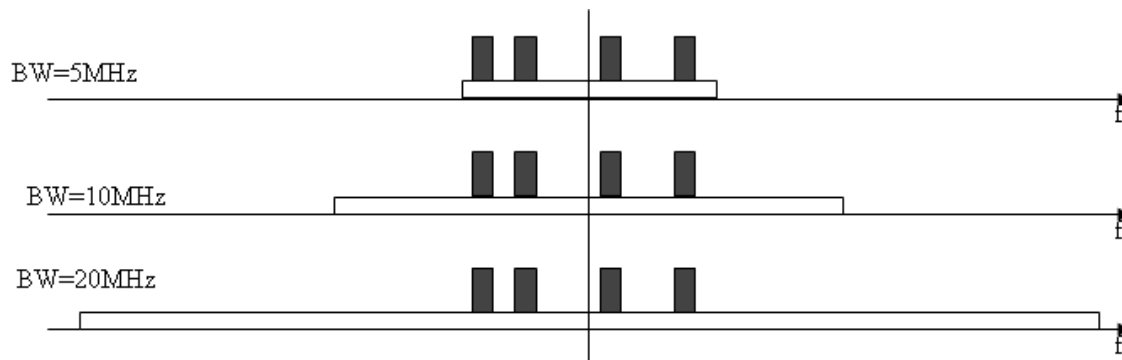


Figure h55—Desired spectral densities for different channel BWs

In Table h 7 the radio signal is defined to minimize the inter-correlation properties.

Table h7—Radio signal definition

Bin number /Signal number	6	8	10	12	14	18	20	22	24	26
sub-channel index (1..31)	7	9	11	13	15	17	25	27	29	31
1 (Header)	H	L	L	H	H	L	L	L	H	L
2 (Tx_start)	L	H	L	L	H	H	L	L	L	H
3 (Rx_start or Rx_slot)	H	L	H	L	L	H	H	L	L	L
4 (Tx_end)	L	H	L	H	L	L	H	H	L	L
5 (Rx_end)	L	L	H	L	H	L	L	H	H	L
6 (NACK)	L	L	L	H	L	H	L	L	H	H

7 (CSI_Start)	H	L	L	L	H	L	H	L	L	H
8 (CSI_Continuation)	L	H	H	L	L	H	L	H	L	L
9	L	L	H	H	L	L	H	L	H	L

15.5 Messages for WirelessMAN-CX

15.5.1 Sequencing and Retransmission

The CP is a request-response protocol. In any particular message exchange, one party acts as the initiator (sends a request) and the other party acts as the responder (sends a response message).

The initiator sets the Message ID in the header to any value in the first message of the CP association, and increases the Message ID by one for each new request using serial number arithmetic. Retransmissions do not increment the Message ID. The responder sets the message ID in the response to the value of the message ID in the request.

The initiator is always responsible for retransmissions. The responder only retransmits a response on seeing a retransmitted request; it does not otherwise process the retransmitted request.

The retransmitted requests/responses are exact duplicates of previous requests/responses. The initiator must not send a new request until it receives a response to the previous one. Packets with out-of-sequence Message IDs are considered invalid packets and are discarded.

The initiator must retransmit after a configurable interval until either it gets a valid response, or decides after a configurable number of attempts that the CP association has failed. (Since the retransmission algorithm is implementation-dependent, it is not defined here.)

15.5.2 Coexistence Protocol (CP) messages (CP-REQ/ CP-RSP)

The Coexistence Protocol employs two message types: CP Request (CP-REQ) and CP Response (CP-RSP), as described in Table h 8.

Table h8—CP messages

CP-Type Value	Message name	Message description
0	CP-REQ	Coexistence Resolution and Negotiation Request
1	CP-RSP	Coexistence Resolution and Negotiation Response

These CP messages can be encapsulated as MAC Messages, over the 802.16 air interface, or as Internet Protocol messages (TCP/IP or UDP). The CP management messages are exchanged between peers, e.g. BS and

BSIS or BS and BS or BS and SS., and distinguish between CP requests (BS -> BS/BSIS/SS or SS-> BS) and CP responses (BS/BSIS/SS -> BS or SS->BS). Each MAC/IP message encapsulates one CP message in the Management Message Payload. Coexistence Protocol messages exchanged between the BS and BS or between BS and BSIS or between BS and SS shall use the form shown in Table h 9.

Table h9—CP message format

Syntax	Size	Notes
CP_Message_Format() {		
Version of protocol in use	4 bits	1 for current version
Code	8 bits	See <u>Table h 10</u>
Management Message Type	8 bits	0-CP-REQ 1-CP-RSP 2-255 - Reserved
Length of Payload	16bits	In bytes
Confirmation Code (only for CP-RSP)	4 bits	0-OK/success 1-Reject-other 2-Reject-unrecognized-configuration-setting 3-Reject-unknown-action 4-Reject-authentication-failure 5-255 Reserved
Source BSID	48 bits	
Destination BSID	48 bits	
AssociationID	16 bits	
CP Message Seq_ID	8 bits	
TLV Encoded Attributes	variable	TLV specific
}		

A detailed description of the parameters is the following:

Version of protocol in use

This standard specification of the protocol is version 1.

Code

The Code is one byte and identifies the type of CP packet. When a packet is received with an invalid Code, it shall be silently discarded. The code values are defined in Table h 10.

Length of payload

The length of payload in bytes .

CP Message Sequence Identifier (CP Message Seq_ID)

The CP Message Sequence Identifier field is one byte. A BS/BSIS uses the identifier to match a BS/BSIS response to the BS's requests. The BS shall increment (modulo 256) the Identifier field whenever it issues a new CP message. The retransmission mechanism relies on TCP, if the message is sent over the IP backbone.

The Identifier field in a BS/BSIS's CP-RSP message shall match the Identifier field of the CP-REQ message the BS/BSIS is responding to.

Source BSID

A 48bit field indicating the ID of the entity sending the CP message. This entity may be a Base Station or a BSIS.

Destination BSID

A 48bit field indicating the ID of the entity that is the destination of the CP message. This entity may be a Base Station or a BSIS.

Association identifier(Association ID)

The Association ID is used to uniquely identify a CP connection between an initiator and responder.

It is a parameter used to uniquely assign or relate a response to a request. The association identifier used on the responder and initiator MUST be a random number greater than zero to protect against blind attacks and delayed packets.

When the initiator sends subsequent messages, it uses the responder's association identifier in the Association ID field; when the responder sends a message it uses the initiator's association identifier in the Association ID field.

Confirmation Code

The Confirmation Code is the appropriate CC for the entire corresponding CP-RSP.

Attributes

CP attributes carry the specific authentication, coexistence resolution, and coexistence negotiation data exchanged between peers. Each CP 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 CP message. The end of the list of attributes is indicated by the LEN field in the MAC PDU header.

Table h10—CP message codes

Code	CP Message Name	CP Message Type	Protocol type	Direction
0	Reserved	—	—	—
1	Identify Coexistence Request	CP-REQ	TCP	BSIS->BSIS
2	Identify Coexistence Response	CP-RSP	TCP	BSIS->BSIS
3	CoNBR Topology Request	CP-REQ	TCP	BS-> BSIS
4	CoNBR Topology Reply	CP-RSP	TCP	BSIS->BS
5	Registration Request	CP-REQ	TCP	BS-> BSIS
6	Registration Reply	CP-RSP	TCP	BSIS->BS
7	Registration Update Request	CP-REQ	TCP	BS-> BSIS
8	Registration Update Reply	CP-RSP	TCP	BSIS->BS
9	De-registration Request	CP-REQ	TCP	BS-> BSIS
10	De-registration Reply	CP-RSP	TCP	BSIS->BS
11	Add Coexistence Neighbor Request	CP-REQ	TCP	BS->BS

12	Add Coexistence Neighbor Reply	CP-RSP	TCP	BS->BS
13	Update Coexistence Neighbor Request	CP-REQ	TCP	BS->BS
14	Update Coexistence Neighbor Reply	CP-RSP	TCP	BS->BS
15	Delete Coexistence Neighbor Request	CP-REQ	TCP	BS->BS
16	Delete Coexistence Neighbor Reply	CP-RSP	TCP	BS->BS
17	Get_Param_For_Radio_Signature_Request	CP-REQ	UDP	BS->BS
18	Get_Param_For_Radio_Signature_Reply	CP-RSP	UDP	BS->BS
19	Evaluate_Interference_Request	CP-REQ	UDP	BS->BS
20	Evaluate_Interference_Reply	CP-RSP	UDP	BS->BS
21	Work_In_Parallel_Request	CP-REQ	UDP	BS->BS
22	Work_In_Parallel_Reply	CP-RSP	UDP	BS->BS
23	Reduce_Power_or_Quit_Sub_Frame_Request	CP-REQ	UDP	BS->BS
24	Reduce_Power_or_Quit_Sub_Frame_Reply	CP-RSP	UDP	BS->BS
25	Create_New_Sub_Frame_Request	CP-REQ	UDP	BS->BS(MC?)
26	Create_New_Sub_Frame_Reply	CP-RSP	UDP	BS->BS
27	SS_CCID_IND	CP-REQ	UDP	BS->BS
28	SS_CCID_RSP	CP-RSP	UDP	BS->BS
29	PSD_REQ	CP-REQ	UDP	BS->BS
30	PSD_RSP	CP-RSP	UDP	BS->BS
31	Channel Switch Negotiation Request	CP-REQ	TCP	BS->BS
32	Channel Switch Negotiation Reply	CP-RSP	TCP	BS->BS
33	Channel Switch Request	CP-REQ	TCP	BS->BS
34	Channel Switch Reply	CP-RSP	TCP	BS->BS
35	Advertisement Request	CP-REQ	TCP	BS->BS
36	Advertisement Reply	CP-RSP	TCP	BS->BS
37	Negotiation Process Request	CP-REQ	TCP	BS->BS
38	Negotiation Process Reply	CP-RSP	TCP	BS->BS
39	Credit Token Proposal Request	CP-REQ	TCP	BS->BS
40	Credit Token Proposal Reply	CP-RSP	TCP	BS->BS
41	Negotiation Results Request	CP-REQ	TCP	BS->BS
42	Negotiation Results Reply	CP-RSP	TCP	BS->BS
43	Granting Request	CP-REQ	TCP	BS->BS
44	Granting Reply	CP-RSP	TCP	BS->BS
45-255	reserved			

Formats for each of the CP messages are described in the following subclauses. The descriptions list the CP attributes contained within each CP message type. The attributes themselves are described in each message. Unknown attributes shall be ignored on receipt and skipped over while scanning for recognized attributes. The BS/BSIS shall silently discard all requests that do not contain ALL required attributes. The BS shall silently discard all responses that do not contain ALL required attributes.

[Note: The following security part is a temporary text adopted from contribution C802.16h-05/11r1 and is subject to further discussion. A call for comment from security experts is open to comment on this text.]

The following Type-Length-Value (TLV) types may be present in the CP payload depending on the Message_Type:

Table h11—TLV types for CP payload

Type	Parameter Description	Length (bits)	Comment
------	-----------------------	---------------	---------

01	Operator ID	16	ASCII stream, max. 40 bytes long
02	BS-ID	8	
03	GPS coordinates	16	
04	BS IP Address	8	
05	MAC Frame duration	8	
06	Type of sub-frame allocation	8	
07	MAC Frame number	8	
08	Sub-frame number	8	
09	Repetition interval between two Master sub-frames, measured in MAC-frames	8	
10	Time shift from the MAC Frame start	16	(in microsec)
11	Duration of the time slot	16	(in microsec)
12	Repetition of the Base Station radio-signature transmission	16	In MAC Frames number
13	Repetition of the Subscriber Station radio-signature transmission	16	In MAC Frames number
14	List of other used sub-frames, in the interval between two Master sub-frames		
15	Country Code	8	(in ASCII - bytes)(tbd.)
16	Operator contact - phone	8	(in ASCII - bytes)(tbd.)
17	Operator contact – E-mail	8	(in ASCII - bytes)(tbd.)
18	PHY mode	16	Coding ?(tbd.)
19	Maximum coverage at Max. power		
20	Tx power	8	in dBm
21	Base Channel Reference (BaseChRef)	8	in MHz
22	Extended Channel Number (ExChNr)	16	In 0.01MHz
23	Extended Channel Number 2 (ExChNr 2)	16	In 0.01MHz
24	Extended Channel Number 3 (ExChNr 3)	16	In 0.01MHz
25	Transmit antenna type (1 - omni, 2 - directional)	8	
26	Transmit antenna gain (dBi)	8	Signed value
27	Acceptance indication:	8	(tbd.) 1 - accepted 2 - rejected 3,... - message dependent
28	Channel width	16	In 0.01MHz
29	Type	8	message specific
30	Reduction of transmit power	8	in dB
31	GAP DIUC/UIUC insertion	8	1 - for this system 2 - for systems which do not comply with the criteria at type
32	Number (message specific)	8	Number of distinct BS configurations < 20 Number of SSs < 200
33	Two field structure	16	Each element in the structure is coded with 8 bits)

34	Radio signature type	8	Radio Signature type: 1 - RSS1 of this system, signature from SS1 (logical numbering) 2 - RSS2 of this system . . 199 - RSS199 of this system 200 - RBS1 of this system (BS in configuration 1, logical numbering) 201 - RBS2 of this system, configuration 2 . . 220 - RBS20 of this system, configuration 20 221 - maximum interference from the CX_SS (compatible with WirelessMAN-CX), which operate inside the frequency block 222- maximum interference from all the CX_BS, which operate inside the frequency block 223 - maximum interference from all the CX_SS, which operate in a channel, which overlaps the operating channel of the requesting BS 224 - maximum interference from all the CX_BS, which operate in a channel, which overlaps the operating channel of the requesting BS 225 - maximum interference from all the NON-CX_SS, which operate in a channel, which overlaps the operating channel of the requesting BS 226 - maximum interference from all the NON-CX_BS, which operate in a channel, which overlaps the operating channel of the requesting BS 227 - maximum interference from all the CX_SS, which operate in the upper adjacent channel relative to the operating channel of the requesting BS 228 - maximum interference from all the CX_BS, which operate in the upper adjacent channel relative to the operating channel of the requesting BS 229 - maximum interference from all the CX_SS, which operate in the lower adjacent channel relative to the operating channel of the requesting BS 230 - maximum interference from all the CX_BS, which operate in the lower adjacent channel relative to the operating channel of the requesting BS
35	T _{Start} [Notes: For Credit Token till 49]	16	In microsecond
36	T _{End}	16	In microsecond
37	T _{Start Renting}	16	In microsecond
38	T _{End Renting}	16	In microsecond
39	MRCTN	16	In number of credit token
40	T _{Start Negotiation}	16	In microsecond
41	T _{End Negotiation}	16	In microsecond
42	BS_CT	16	In number of credit token
43	x	16	
44	T _{Start proposal}	16	In microsecond
45	T _{End proposal}	16	In microsecond
46	p _{min}	16	In number of credit token
45	p _{max}	16	In number of credit token
46	Pr	16	In number of credit token
47	Credit token transaction confirmation	1	

48	Resource usage confirmation	1	
49	Resource usage confirmation notification	1	

15.5.2.1 Identify Coexistence Request message

The BSIS requests to the foreign BSIS with geographical information of the requesting LE BS.

Code: 1

Attributes are show in Table h 12

Table h12—Identify Coexistence Request message attribute

Attribute	Contents
Operator identifier	The operator ID of the BSIS.
Country code	The country code of the BSIS
Latitude	The latitude information of the BS.
Longitude	The longitude information of the BS.
Altitude	The altitude information of the BS.
Maximum coverage at Max. power	The maximum radius at maximum allowed/designed power that the BS intends to detect its coexistence neighbors.

15.5.2.2 Identify Coexistence Reply message

The BSIS responds to the foreign BSIS to Identify Coexistence Request with a Identify Coexistence Reply message.

Code: 2

The query results is in the format of Coexistence Neighbor Topology Parameter Set, each result will contain the attributes shown in Table h 13. Each BSID TLV indicates start of new result.

Table h13—Coexistence neighbor Topology Parameter Set

Attribute	Contents
BSID	The BSID of the requested BS.
Operator identifier	The operator ID.
Operator contact - phone	The phone number in ASCII string of the operator.
Operator contact – E-mail	The E-mail address in ASCII string of the operator.
Country code	The country code of the BS
PHY mode	The PHY modes of the requested BS.
Latitude	The latitude information of the BS.
Longitude	The longitude information of the BS.
Altitude	The altitude information of the BS.
Maximum coverage at Max. power	The maximum radius at maximum allowed/designed power that the BS intends to detect its coexistence neighbors.

15.5.2.3 Coexistence Neighbor Topology Request message

This message is sent by the BS to the BSIS to request its coexistence neighbor topology with its geometric information.

Code: 3

Attributes are shown in Table h 14.

Table h14—Coexistence Neighbor Topology Request message attribute

Attribute	Contents
Latitude	The latitude information of the BS.
Longitude	The longitude information of the BS.
Altitude	The altitude information of the BS.
Maximum Coverage at Max. power	The maximum radius at maximum power that the BS intends to detect its coexistence neighbors.

15.5.2.4 Coexistence neighbor Topology Reply message

The BSIS responds to the BS's Coexistence neighbor Topology Request with a Coexistence neighbor Topology Reply message.

Code: 4

Specification of the query results of coexistence neighbor topology from BSIS specific parameters.

The query results is in the format of Coexistence Neighbor Topology Parameter Set, each result will contain the attributes shown in Table h 15. Each BSID TLV indicates start of new result.

Table h15—Coexistence neighbor Topology Parameter Set

Attribute	Contents
BSID	The BSID of the requested BS.
Operator identifier	The operator ID.
Operator contact - phone	The phone number in ASCII string of the operator.
Operator contact – E-mail	The E-mail address in ASCII string of the operator.
Country code	The country code of the BS
PHY mode	The PHY modes of the requested BS.
Latitude	The latitude information of the BS.
Longitude	The longitude information of the BS.
Altitude	The altitude information of the BS.
Maximum coverage at Max. power	The maximum radius at maximum allowed/designed power that the BS intends to detect its coexistence neighbors.

15.5.2.5 Registration Request message

This message is sent by the BS to the regional LE DB to perform the registration.

Code: 5

Attributes are shown in [Table h 16](#).

Table h16—Registration Request message attributes

Attribute	Contents
BSID	The BSID of the requested BS.
Contact IP address	The IP address of BS or Coexistence Proxy
Operator identifier	The operator ID.
PHY mode	The PHY modes of the requested BS. Containing Modulation mode, working channel ID, alternative Channel Flag etc.
<optional>:Operator contact - phone	The phone number in ASCII string of the operator.
<optional>:Operator contact – E-mail	The E-mail address in ASCII string of the operator.
<optional>:Country code	The country code of the BS
<optional>:Latitude	The latitude information of the BS.
<optional>:Longitude	The longitude information of the BS.
<optional>:Altitude	The altitude information of the BS.
<optional>:Operational Range at Max. Power	The maximum operational radius of the BS at Max. power.

15.5.2.6 Registration Reply message

The BSIS responds to the BS's Registration Request with a Registration Reply message.

Code: 6

No Attributes.

15.5.2.7 Registration Update Request message

This message is sent by the BS to the regional LE DB to update the registration.

Code: 7

Attributes are shown in [Table h 16](#).

15.5.2.8 Registration Update Reply message

The BSIS responds to the BS's Registration update Request with a Registration update Reply message.

Code: 8

No Attributes.

15.5.2.9 De-registration Request message

This message is sent by the BS to the BSIS to perform de-registration.

Code: 9

Attributes are shown in [Table h 17](#).

Table h17—De-registration Request message attributes

Attribute	Contents
BSID	The BSID of the request BS.

15.5.2.10 De-registration Reply message

The BSIS responds to the BS's De-registration Request with a De-registration Reply message.

Code: 10

No Attributes.

15.5.2.11 Add Coexistence Neighbor Request message

This message is sent by the BS to the coexistence neighbor BS to request to add it to coexistence neighbor list.

Code: 11

Attributes are shown in [Table h 18](#).

Table h18—Add Coexistence Neighbor Request message attributes

Attribute	Contents
BSID	The BSID of the requested BS.
Contact IP address	The IP address of the requested BS or Coexistence Proxy of the requested BS.
Operator identifier	The operator ID.
PHY mode	The PHY modes of the requested BS. Containing Modulation mode, working channel ID, alternative Channel Flag etc.
<optional>:Country code	The country code of the requested BS.
<optional>:Latitude	The latitude information of the BS.
<optional>:Longitude	The longitude information of the BS.
<optional>:Altitude	The altitude information of the BS.
<optional>:Current Tx power	Current Tx power of the BS.
<optional>:Operational Range	The operational radius of the BS.
<optional>:PHY specific parameters	The PHY specific encodings.

15.5.2.12 Add Coexistence Neighbor Reply message

The BSIS responds to the BS's Add Coexistence Neighbor Request with an Add Coexistence Neighbor Reply message.

Code: 12

No Attributes.

15.5.2.13 Update Coexistence Neighbor Request message

This message is sent by the BS to the coexistence neighbor BS to request to update its neighbor list.

Code: 13

Attributes are shown in [Table h 19](#).

Table h19—Update Coexistence Neighbor Request message attributes

Attribute	Contents
-----------	----------

BSID	The BSID of the requested BS.
PHY mode	The PHY modes of the requested BS.
Latitude	The latitude information of the BS.
Longitude	The longitude information of the BS.
Altitude	The altitude information of the BS.
Operational Range	The operational radius of the BS.
PHY specific parameters	The PHY specific parameters.

15.5.2.14 Update Coexistence Neighbor Reply message

The BSIS responds to the BS's Update Coexistence Neighbor Request with an Update Coexistence Coexistence neighbor Reply message.

Code: 14

No Attributes.

15.5.2.15 Delete Coexistence Neighbor Request message

This message is sent by the BS to the coexistence neighbor BS to request to delete from its coexistence neighbor list.

Code: 15

Attributes are shown in [Table h 20](#).

Table h20—Delete Coexistence Neighbor Request message attributes

Attribute	Contents
BSID	The BSID of the requested BS.

15.5.2.16 Delete Coexistence Neighbor Reply message

The BSIS responds to the BS's Delete Coexistence Neighbor Request with a Delete Coexistence Neighbor Reply message.

Code: 16

No Attributes.

15.5.2.17 Get_Param_For_Radio_Signature_Request message

Messages between BSs, used to request the up-dated list of parameters

Code: 17

Parameter: none

15.5.2.18 Get_Param_For_Radio_Signature_Reply message

Messages between BSs, reply to the Get_Param_Request

Code:18

Table h21—Get_Param_Replay Parameter set

Attribute	Contents
GPS coordinates	The GPS coordinates of the IBS
Base Channel Reference (BaseChRef)	Base Channel Reference of the BS
Extended Channel Number (ExChNr)	Extended Channel Number (ExChNr) of the BS
Maximum Power to be used	Electrical transmitted power in dBm
Transmit antenna type (1 – omni, 2 – directional)	
Transmit antenna gain (dBi)	
MAC Frame number	Requested MAC Frame number to place the Radio signature (see the MAC Frame numbering starting from the absolute time)
Number of distinct BS configurations	Number of distinct BS configurations, for different combinations of powers and beam directions, to be used for radio signatures (<20)
Number of SSs	Total number of SSs to be used for radio signatures (<200)
Type of sub-frame allocation	The type of sub-frame scheduling (15.4.2.1.2)
Sub-frame number	The number of Master sub-frames per MAC Frame
Repetition interval between two Master sub-frames	The repetition interval between two Master sub-frames, measured in MAC-frames
MAC Frame number	The first MAC Frame number which contains the Master sub-frame

15.5.2.19 Evaluate_Interference_Request message

A message sent by a new BS wishing to evaluate the maximum co-channel and total interference, for separate or aggregated systems in the Community. The message is sent to every Base Station in the Community, indicating either the request to send the Radio Signature or the request to be inserted a GAP DIUC/UIUC interval for the duration of the Radio Signature. Alternatively, a BSIS can broadcast the message to an IP-multicast group including all the BSs in the community. The Radio signature may be transmitted by the BS or by the associated SSs. In case of the Radio Signature transmission by the BS, noted as RBS, is given the possibility for 20 radio signatures, which may differ due to Beam Forming or power concentration on specific sub-channels. The various RBS signatures are identified by the configuration number. The various SS signatures are identified by the RSS number, which runs from 1 to 199. The message is indicating the MAC Frame number, the offset from its start and the duration of the requested Radio Signature time-slot. A number of radio signatures may be concatenated, such that will be respected the total time-slot duration, including the propagation delays. It is recommended that this duration will be lower than 1ms. The time-slot shall use the DL sub-frame for BS signatures and UL sub-frame for SS signatures. The Radio Signature shall use the max. power used during the operation.

Code:19

The attributes are indicated in the Table h 22.

Table h22—Evaluate_Interference_Request Parameter set

Attribute	Contents
-----------	----------

GPS coordinates	The GPS coordinates of the IBS
Base Channel Reference (BaseChRef)	Base Channel Reference of the requesting BS, for sending the Radio signature (see 6.4.1.2)
Extended Channel Number (ExChNr)	Extended Channel Number (ExChNr) of the requesting BS for sending the Radio Signature
Channel width	Channel width of the Requesting BS, in units of 10kHz
Extended Channel Number 2 (ExChNr 2)	Extended channel Number of the block start frequency
Extended Channel Number 3 (ExChNr 3)	Extended channel Number of the block end frequency
Number of concatenated signatures	The number of concatenated radio signatures in a time-slot = N
Radio signature type	List with N values
	GAP DUIC/UIUC insertion for this system or systems which do not comply with
MAC Frame number	MAC Frame number for sending the radio signature
Time shift from the MAC Frame start	Start of the signature slot or GAP interval, as offset from the MAC Frame start, in microseconds
Duration of the time-slot	Duration of the signature slot or GAP interval, in microseconds; the duration of the GAP interval may be higher than the duration of the Radio signature slot, in order to cover the propagation delays. The duration of the time-slot shall be less than 1ms.

15.5.2.20 Evaluate_Interference_Replay message

A message sent by the existing Master BSs, reply to the Evaluate_Interference_Request. It provides the timing and the identification of the scheduled radio signatures.

Code:20

The attributes are indicated in the Table h 23.

Table h23—Evaluate_Interference_Replay Parameter set

Attribute	Contents
Acceptance indication	Acceptance code: 1, if the request is fully accepted 2, if the request is rejected 3, if the requested will be executed at a different time; in this case the message will supplementary include the following three fields indicating when will be transmitted the radio signatures.
MAC Frame number	MAC Frame number for sending the radio signature
Time shift from the MAC Frame start	Start of the signature slot or GAP interval, as offset from the MAC Frame start, in microseconds
Duration of the time-slot	Duration of the signature slot or GAP interval, in microseconds; the duration of the GAP interval may be higher than the duration of the Radio signature slot, in order to cover the propagation delays.
Number of concatenated signatures	The number of structures in the list
Two field structure	{ - Offset from the start of the signature slot, in microseconds (8 bits) - Radio Signature type (8 bits) }

15.5.2.21 Work_In_Parallel_Request message

A message sent by a new BS to request the use an existing Master sub-frame, to a BS already acting as Master in the specific sub-frame, and requesting the existing BS to evaluate its interference.

If more than one Base Station is using the sub-frame as Master, the IBS will send this message to every BS separately.

The Radio Signature will be transmitted during the claimed Master sub-frame and will consist of a DL sub-frame, starting with the first zone using the mandatory permutation (if applicable) and continuing with other used zones and their permutations. Each zone will be transmitted using the maximum power.

Code: 21

The attributes are indicated in the Table h 24.

Table h24—Work_In_Parallel_Request Parameter set

Attribute	Contents
GPS coordinates	The GPS coordinates of the IBS
Base Channel Reference (BaseChRef)	Base Channel Reference of the requesting BS, for sending the Radio signature (see 6.4.1.2)
Extended Channel Number (ExChNr)	Extended Channel Number (ExChNr) of the requesting BS for sending the Radio Signature
Power to be used in dBm	
Transmit antenna type (1 – omni, 2 – directional)	
Transmit antenna gain (dBi)	
MAC Frame number	Requested MAC Frame number to place the BS Radio Signatures (see the MAC Frame numbering starting from the absolute time)
Time shift from the MAC Frame start	Start of the claimed Master sub-frame, relative to start of the mentioned MAC frame, in μ s
Duration of the time-slot	Duration of the Radio signature (shall be shorter than the claimed sub-frame duration), in μ s

15.5.2.22 Work_In_Parallel_Reply message

A message sent by a existing Master BS in response to the Work_In_Paraller_Request message.

Code: 22

The attributes are indicated in the Table h 25.

Table h25—Work_In_Parallel_Reply Parameter set

Attribute	Contents
Base Channel Reference (BaseChRef)	Channel identifier of the responding OBS
Extended Channel Number (ExChNr)	Channel identifier of the responding OBS

Receive antenna type (1 – omni, 2 – directional)	For the OBS
Receive Antenna Gain	For the OBS
Acceptance indication	1:=Acceptance 2 = Rejection 3 – Accepted if the IBS transmit power is reduced
Request for reduction of the transmit power, in dB	indicates the request for transmit power reduction, in dB

15.5.2.23 Reduce_Power_or_Quit_Sub_Frame_Request message

A message sent by an operating Base Station, using the sub-frame as Master, in order to request the newer Base Station to cease the operation as Master or Slave in the current sub-frame. Supplementary, the message may indicate the power reduction for accepting the Base Station to use the sub-frame as Slave.

Code:23

The attributes are indicated in the Table h 26.

Table h26—Reduce_Power_or_Quit_Sub_Frame_Request Parameter set

Attribute	Contents
Base Channel Reference (BaseChRef)	Base Channel Reference of the requesting BS,
Extended Channel Number (ExChNr)	Extended Channel Number (ExChNr) of the requesting BS
MAC Frame number	MAC Frame number containing the Master sub-frame
Time shift from the MAC Frame start	Start of the claimed Master sub-frame, relative to start of the mentioned MAC frame, in μ s
Duration of the time-slot	Duration of the sub-frame
Number of concatenated structures	
Two field structure	{ - Radio Signature identifier (8bits) - Reduction of transmit power for operating in parallel; 255 dB has the significance of a request to STOP using the sub-frame (8 bits) }

15.5.2.24 Reduce_Power_or_Quit_Sub_Frame_Reply message

A message sent by a new Base Station, in response to the old Base Station's Quit_Sub_Frame_Request message. The message indicates the actual power reduction for the requested signatures.

Code:24

The attributes are indicated in the Table h 27.

Table h27—Reduce_Power_or_Quit_Sub_Frame_Replay Parameter set

Attribute	Contents
Base Channel Reference (BaseChRef)	Base Channel Reference of the replaying BS

Extended Channel Number (ExChNr)	Extended Channel Number (ExChNr) of the replaying BS
Number of concatenated structures	
Two field structure	{ - Signature identifier (8bits) - Reduction of transmit power for operating in parallel; 255 dB has the significance of a request to STOP using the sub-frame (8 bits) }

15.5.2.25 Create_New_Sub_Frame_Request message

A message sent by a BSs to all the community BSs, to request the creation of a new Master sub-frame; the message will include the intended operating channel and the frame-number in which the change will take place

Code:25

The attributes are indicated in the Table h 28.

Table h28—Create_New_Sub_Frame_Request Parameter set

Attribute	Contents
Base Channel Reference (BaseChRef)	Intended Base Channel Reference of the requesting BS
Extended Channel Number (ExChNr)	Intended Extended Channel Number (ExChNr) of the requesting BS
Type of sub-frame allocation	The type of requested sub-frame scheduling (15.4.2.1.2)
Sub-frame number	The number of Master sub-frames per MAC Frame
Repetition interval between two Master sub-frames, measured in MAC-frames	The repetition interval between two Master sub-frames
MAC Frame number	The first MAC Frame number which contains the change

15.5.2.26 Create_New_Sub_Frame_Replay message

A message sent in response to the Create_New_Sub_Frame_Request message. In case of reject

Code:26

The attributes are indicated in the Table h 29.

Table h29—Create_New_Sub_Frame_Replay Parameter set

Attribute	Contents
Acceptance indication	Acceptance code: 1, if the request is fully accepted 3, rejected due to unacceptable type of Frame allocation 4, rejected due to un-acceptable repetition interval 5, rejected due to other causes

15.5.2.27 SS_CCID_IND message

A message sent by SSs to indicate co-channel interference detected.

Code: 27

This is a message sent by an interfered-with BS to the master BS or its peer BS when co-channel interference due to an interfering SS is detected. This message shall contain the following information to determine the source of the co-channel interference and its RF emission characteristics. This information is extracted from the SSURF messages sent by the interfering SS.

- **SS_ID**: The interfering subscriber station identity, as derived from the SSURF.
- **BS_ID_Source**: The identity of the base station associated with the interfering SS, as derived from the interfering SSURF
- **EIRP**: EIRP of the interfering base station, as derived from the interfering SSURF.
- **M_RSSI**: Mean RSSI of the interfering SSURF.
- **Base Station RF Antenna Sector ID**: Antenna sector ID of interfering BS system associated with the interfering SS.
- **BS_ID_Victim**: Identity of interfered-with Base Station.
- **CMI_ID**: The Coexistence Messaging Interval during which the interference was received.
- **INT_SSURF_Frq**: The frequency of interference SSURF events detected per CMI cycles (calculated as the number of detected SSURF interference events per N full CMI cycles [1 cycle= 1 min TBD]). This value relates to the severity of the interference from the foreign SS

SS_CCID_IND TLV encoding are provided in the following table

Table h30—SS_CCID_IND TLV encoding

Name	Type (1 byte)	Length (1 byte)	Value (Variable length)	PHY scope
SS_ID	1	6	Foreign Interfering SS ID derived from SSURF	
BS_ID	2	6	Foreign Base Station ID detected at SS Derived from foreign SSURF	
EIRP	3	1	Nominal EIRP of interfering signal () or the per burst EIRP	
CMI_ID	4		Common messaging interval ID	
M_RSSI	5	2	Mean RSSI of detected and identity interference (SSURF)	
INT_SSURF_FRQ	6	2	frequency of interference SSURF events.	
Base station RF antenna sector ID	7	1	The RF antenna sector identifier for a base station. 1-255 for FDD only 0- reserved for TDD only	
BS_ID	8	6	ID of BS generating this message; the interfered-with BS ID	

None of above TLV in this message is repeatable.

15.5.2.28 SS_CCID_RSP message

A “set” message to SS.

Code: 28

This CP message is usually sent in response to a SS_CCID_IND to inform the interfered-with base station on the status of the interference resolution being undertaken at the foreign base station. Since there may be longer timed negotiations being undertaken as a consequence of the SS_CCID_IND message; this message may be used to indicate to the interfered-with BS a wait time. In most instances the message will indicate a resolution to the uplink interference, achieved by scheduling uplink transmissions from the foreign subscriber station.

- **RES:** Information to the inquiring base station (originating SS_CCID_IND) on the status of the resolution of identified interference. This could be a number of options: interference resolved (rescheduling of SS uplink traffic to non-interference zone); lowering EIRP or modulation of SS; unresolved (due to inability to find uplink rescheduling zones) etc.
- **CNTI_BS_TBD:** Pending scheduling changes, as part of CP {TBD}

The message shall have the following information:

SS_CCID_RSP TLV encoding are provided in the following table

Table h31—SS_CCID_RSP TLV encoding

Name	Type (1 byte)	Length (1 byte)	Value (Variable length)	PHY scope
BS_ID	1	6	Foreign Base Station ID detected at SS Derived from foreign SSURF	All
SS_ID	2	6	Foreign SS generating interference.	
EIRP	3		EIRP of Foreign BS	
RES	4	2	Resolution status pertaining to original SS_CCID_IND; Either resolved, pending, unresolved. {TBD}	
CNTI_BS_TBD	5	4	Pending CP scheduling changes directed to BS (TBD)	

None of above TLV in this message is repeatable.

15.5.2.29 PSD_REQ message

A “set” message to start PSD (power spectrum density) sampling

Code: 29

All co-channel interference that is created cannot necessarily be demodulated or decoded correctly, allowing the extraction of Tagged information from interference frames. Additionally, some users of license-exempt spectrum may not comply with any of the IEEE standards and be impossible to identify. In this event it is useful for a to be able to monitor the LE spectrum to determine available spectrum “white space” and determine sub-detection interference. “Snapshots” of spectrum space are useful to CR systems, especially when new base stations or terminals are installed and are searching for unoccupied spectrum.

This is a “set” message, it requests a BS or SS to sample PSD (power spectrum density) data for next “get” message. Since sampling PSD data will take some time, depending on environment, nature of bursty users, the following “get” message shall wait long enough for BS/SS to complete the PSD data sampling.

There shall be only one scalar MIB object defined for this operation.

15.5.2.30 PSD_RSP message

A “get” message to get PSD (power spectrum density) data table.

Code: 30

This is a “get” response message, MIB objects shall be defined accordingly; it shall contain the following values for a complete PSD:

- Antenna Parameter List containing attributes of antenna undertaking PSD
- X-min, the lower bound of channel frequency (in kilohertz)
- X-max, the upper bound of channel frequency (in kilohertz)
- Resolution bandwidth
- Power spectrum density measurement

Resolution bandwidth is scalar, it is used together with X-max and X-min to determine how many PSD values are collected and contained in the STRUF_REP message (i.e.).

$$(X_{max} - X_{min}) / (resolutionBandwidth) + 1 \quad (h2)$$

Upon reception of this message, CR_NMS will stamp the message based on the arrival time and translate the information into internal format and store it into database.

Here is an example of PSD display:

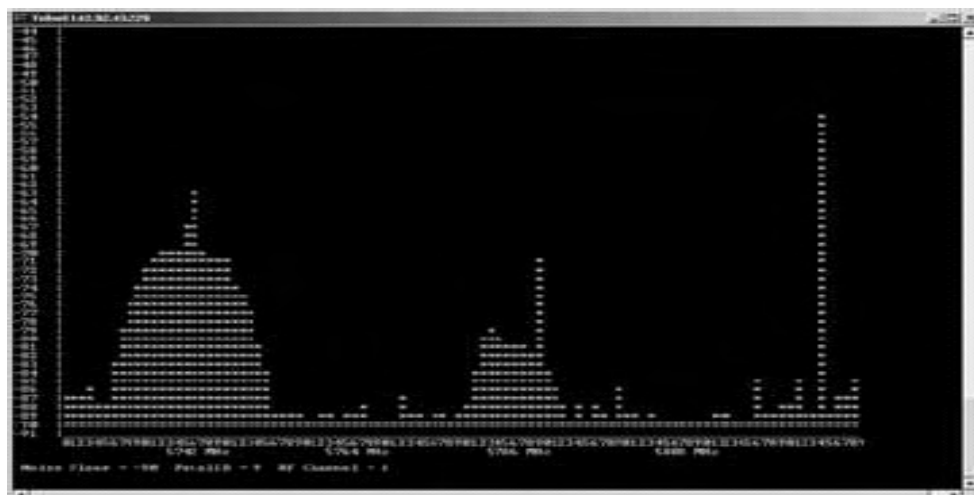


Figure h56—Example of PSD Display

15.5.2.31 Channel Switch Negotiation Request message

This message is sent by a BS to another coexistence BS in the community to negotiate to switch to a different target channel.

Code: 31

Parameters: tbc.

15.5.2.32 Channel Switch Negotiation Reply message

A message sent by a BS in reply to a Channel Switch Negotiation Request message whether it agrees or refuses to switch.

Code: 32

Parameters: tbc.

15.5.2.33 Channel Switch Request message

This message is sent by a BS to another coexistence BS in the community to request to switch to an alternative channel.

Code: 33

Parameters:

Table h32—Channel Switch Request message attributes

Attribute	Contents
Operator ID	The Operator identifier of requesting BS.
BSID	The requesting BS identifier
Requested BSID	BS identifier of the requested BS
Working Channel ID	The current working channel ID of the requested BS
Rolling back indication	0: to switch to one of the alternative channels 1: to switch back to the channel before the last channel switching request
FSN	Frame sequence number to switch channel

15.5.2.34 Channel Switch reply message

A message sent by BS, reply to Channel Switch Request message indicating the result of the channel switching.

Code: 34

Parameters:

Table h33—Channel Switch Reply message attributes

Attribute	Contents
Operator ID	The Operator identifier of requesting BS.
BSID	The requesting BS identifier
Requested BSID	BS identifier of the requested BS
Acknowledge	0: rejection for fail in switching 1: succeeded in switching
Target working channel ID (new working channel)	The channel ID of the requested BS will switch to
FSN	Frame sequence number of the channel switching

15.5.2.35 Advertisement Request

The master BS advertises to the surrounding slave BSs that it offers temporally some resources for renting.

Code: 35

Attributes are shown in Table h 34.

Table h34—Advertisement Request message attributes

Attribute	Contents
BSID	BSID of the master BS
Operator ID	Operator ID of the master BS
T _{Start}	Starting time of the renting period
T _{End}	Ending time of the renting period
T _{Start Renting}	Starting time of the subframe under renting
T _{End Renting}	Ending time of the subframe under renting
MRCTN	Minimum number of credit tokens required for renting

15.5.2.36 Advertisement Reply

The interested slave BSs respond to the master BS with an Advertisement Reply message mentioning their interest or not to rent totally or partially the resources offered by the master BS.

Code: 36

Attributes are shown in Table h 35.

Table h35—Advertisement Reply message attributes

Attribute	Contents
BSID	BSID of the slave BS
Operator identifier	Operator ID of the slave BS

15.5.2.37 Negotiation Process Request

The master BS provides the following information to the interested slave BSs to initiate the negotiation process.

Code: 37

Attributes are shown in Table h 36.

Table h36—Negotiation Process Request message attributes

Attribute	Contents
$T_{\text{Start Negotiation}}$	Time from which the negotiation will start
$T_{\text{End Negotiation}}$	Time at which the negotiation will end

15.5.2.38 Negotiation Process Reply

In response, each slave BS informs the master BS about its first number proposition of credit token per time unit.

Code: 38

Attributes are shown in Table h 37.

Table h37—Negotiation Process Reply message attributes

Attribute	Contents
BS_CT	Number of credit tokens per time unit
x	Fraction of [$T_{\text{Start Renting}}$, $T_{\text{End Renting}}$] for which BS_CT applies for.
$T_{\text{Start proposal}}$	Starting time from which BS_CT applies for.
$T_{\text{END proposal}}$	Ending time from which BS_CT applies for.

15.5.2.39 Credit Token Proposal Request

The master BS informs the slave BSs about the minimal and maximal payoffs resulting from the scheduling process applied by the master BS.

Code: 39

Attributes are shown in Table h 38.

Table h38—Credit Token Proposal Request message attributes

Attribute	Contents
p^{min}	Minimal payoff

p^{\max}	Maximal payoff
------------	----------------

15.5.2.40 Credit Token Proposal Reply

In response to the Credit Token Proposal Request message, the slave BS proposes a new BS_CT for the previous x, TStart proposal and TEnd proposal values.

Code: 40

Attributes are shown in Table h 39.

Table h39—Credit Token Proposal Reply message attributes

Attribute	Contents
BS_CT	Updated number of credit tokens per time unit

The messages "Credit Token Proposal Request" and "Credit Token Proposal Reply" are repeated as long as TEnd Negotiation is not reached.

15.5.2.41 Negotiation Results Request

When TEnd Negotiation is reached, the master BS informs individually each winning slave BS about the number of credit token it has to provide to the master BS.

Code: 41

Attributes are shown in Table h 40.

Table h40—Negotiation Results Request message attributes

Attribute	Contents
Pr	Number of requested credit token that the slave BS has to provide to the master BS after the negotiation

15.5.2.42 Negotiation Results Reply

In response to the "Negotiation Results Request" message, each slave BS confirms to the master BS that it allows performing the credit token transaction from the slave BS towards the master BS.

Code: 42

Attributes are shown in Table h 41.

Table h41—Negotiation Results Reply message attributes

Attribute	Contents
-----------	----------

Credit token transaction confirmation	The slave BS confirms the CT transaction towards the master BS.
---------------------------------------	---

15.5.2.43 Granting Request

Based on the "Negotiation Results Reply" message, the master BS grants the usage of its resources opened for renting to each winning slave BS which has performed the transaction.

Code: 43

Attributes are shown in Table h 42.

Table h42—Granting Request message attributes

Attribute	Contents
Resource usage confirmation	The master BS approves the usage of the resources he has agreed to rent.

15.5.2.44 Granting Reply

In response to the "Granting Request" message, each slave BS notifies it will use the resources in the agreed won renting period.

Code: 44

Attributes are shown in Table h 43.

Table h43—Granting Reply message attributes

Attribute	Contents
Resource usage confirmation notification	The slave BS notifies its willingness to use the resources he has been granted with.

15.5.3 Message Validity Check

A message is only accepted if all the following holds true:

- Message version *field* = 1.
- Association ID must match a current association
- Message Code is valid
- Message length equals size of payload
- Message ID must match the expected sequence number
- The payload contains only those TLVs expected given the value of the Code

— All TLVs within the payload are well-formed, TLVs marked as mandatory are recognized.

15.5.4 Fragmentation

CP does not provide support for fragmentation.

15.5.5 Transport Protocol

CP uses UDP as the transport protocol with port number[tbd.]. All messages are unicast.

15.5.6 Using dedicated messages

15.5.6.1 Common PHY

15.5.6.2 Between BS and SS

15.5.6.2.1 BS Neighborhood Update Request BroadCasting (BS_NURBC)

The BS_NCRBC message is broadcast by the initializing BS or the operating BS in order to update the neighbor list in the database. This message is sent from the BS to the SS in the coexistence neighbor systems. It uses the CSI frame to carry the IP address information of its coexistence proxy and the BSID from the BS to the SS, and the IP & BSID information shall be reported by the SS to its serving coexistence neighbor BS. The serving coexistence neighbor BS should communicate to the initializing BS in the IP network via the coexistence proxy, and proceed with further coexistence negotiation.

An RTK (*Random Temporary Key*) shall be randomly generated in the BS and broadcast using BS_BURBC. The neighbor BS which sends the CP request message needs to carry the RTK in the message. This will prevent the BS from being easily attacked by someone far away without any WirelessMAN-CX airlink capability which have know the static contact information. Table h 44 lists the TLV encoding for the BS_NURBC message.

Table h44—BS_NURBC message TLV encoding

Name	Type(Byte)	Length	Value (Variable length)
NURBC_V4	0	12	Bits 15:0 - RTK Bits 63:16 - BSID Bits 95:64 - BS IP address(IPv4)
NURBC_V6	1	24	Bits 15:0 - RTK Bits 63:16 - BSID Bits 191:64 - BS IP address(IPv6)

15.6 Recommended practice for WirelessMAN-CX

15.6.1 Grouping of interfering/not-interfering units

The system needs to group of interfering/not interfering units of all the systems in the community and all the SSs in the native system for various purposes.

For all the neighbor systems (which can be either an interference victim or a source in any one of the candidate channels), the initializing BS will group them all as its potential interfering systems before choosing the operation channel. When the initializing BS have allocated the operation channel, only the neighbor systems, which are interfering in the current channel are grouped as interfering neighbor systems. An interfering neighbor system should share the same band of spectrum by coordinating into different master sub frame or controlling the power spectrum density etc. The other neighbor systems are to be maintained in the database, for the case of such as channel reallocation coordination.

For all the SSs associated with the serving systems, the BS needs to group them into interfering or not-interfering ones, according to their operational parameters (e.g. transmission power, sub-channels, modulation and coding state etc.), so that the BS can schedule their data traffic into different sub-frame to prevent interference. The SS that operates such that it does not interfere with other systems can use either the Common sub-frame or the Master sub frame for their data traffic, while the data traffic of SSs operating with interfering conditions can only be scheduled within the Master sub-frame.

15.7 Coexistence with non-WirelessMAN-CX systems

Subsequently we provide a review of the main mechanisms that can be used for providing better spectrum sharing with non-IEEE802.16 systems, other than those considered as "preferred spectrum users".

The Candidate Channel Selection, which is, as previously presented, useful for the detection of co-channel interference, can be used in a much larger scale for interference determination. A slot is reserved for non-IEEE802.16 systems, which may, in the future, to signal their presence in a controlled mode to IEEE802.16 systems.

The Signaling to Ad-hoc Systems, by using a simple, well-known PHY transmission, with increased power on the used sub-carriers, provides a better level of penetration. These transmissions may be detected in the future by non-IEEE802.16 systems, and used by them for choosing an optimal operation channel and to further isolate the interference in time domain.

For non-IEEE802.16 systems, these mechanisms are complementary: the first will allow non-IEEE802.16 systems to signal their presence to IEEE802.16 systems, while the second will permit to non-IEEE802.16 systems to:

- Detect the potential interference caused by IEEE802.16 systems in both frequency and time domains
- Select the operating channels and time intervals, such that interference to IEEE802.16 systems is avoided.

15.7.1 Interference from Non-IEEE 802.16 systems.

Non-IEEE802.16 systems can make use of the coexistence procedures by using the collaborative mechanisms or the non-collaborative mechanisms. When sharing information and coordinating with Wireless-

MAN-CX systems using CP messaging or signaling, non-IEEE802.16 systems, such as IEEE802.11 systems, can share the same spectrum band or do radio resource distribution optimization using the collaborative mechanisms (summarized in 15.1.2) with WirelessMAN-CX systems. Otherwise, only non-collaborative mechanisms can be used for coexistence between IEEE802.16 and non-IEEE802.16 systems.

15.7.1.1 Non-IEEE 802.16 Systems capable of GPS/UTC Timing Recovery

Other wireless systems, not specified in this standard, using uncoordinated bands that are capable of GPS/UTC timing recovery can monitor the CMI intervals to determine the existence of co-channel IEEE 802.16 users. Monitoring the intervals and undertaking CCI measurements over CMI cycles will allow those other systems to determine the occupancy of a channel and avoid settling on it. *[NOTE THAT BS AND SS MAY NOT BE DEFINED IN OTHER SYSTEMS.]*

Additionally, [CMI_ID54] [tbd.] will be left unoccupied by IEEE 802.16 systems. Non -IEEE 802.16 systems occupying the same uncoordinated spectrum can insert downlink and uplink power bursts [tbd.] into this interval. Such energy should be detected by the IEEE 802.16 WirelessMAN-CX systems, which will consequently avoid the use of the given channel.

15.7.1.2 Non-IEEE 802.16 Systems not capable of GPS/UTC Timing Recovery

The majority of co-channel interferers will be systems and devices that cannot perform rudimentary of signaling specified for IEEE 802.16 coexistence and channel detection. To deal with such interferers the WirelessMAN_CX systems in this standard will have to opt for avoidance of such users. To facilitate this avoidance, both the BS and SS will have the ability to undertake [Power Spectral Density mappings] of selected bandwidth and disseminate such information as part of their [tbd.] inter-system messaging.

Sections 15.5.2.28. and 15.5.2.30 describe the instructions and formatting that will be used by the LE systems to undertake [PSD] measurements of contented spectrum. These measurements should be undertaken by a BS prior to occupancy of spectrum space and they can be undertaken throughout the operational period of a system to determine encroachments and to identify other spectrum that may have to be used in the event of uncontrolled interference arising in the occupied spectrum. The [PSD] measurements will be undertaken by the SS as well and this sensor information will be sent to the BS. [PSD] measurement information forms part of the data base that is exchanged between systems as part of their mutual spectrum management tasks. SSURF messages [tbd.] could be used to transport spectrum information.

15.7.2 Coexistence with non-WirelessMAN wireless access systems

The principles in section 15.4.2.4.2 are also applicable to non-WirelessMAN systems, like IEEE 802.11, as the Coexistence Protocol, working at IP level, allows the communication between systems independent of their PHY/MAC standards. During every WirelessMAN MAC frame, the other system, e.g. a 802.11 access point may find that a sub-frame may be used, due to the low created interference levels. In the case that no operation in parallel is possible, the new system will ask for the creation of a new Master sub-frame.

The scheduled use of the MAC frame is possible by using the IEEE 802.11 PCF mode.

Annexes

Annex A

(informative)

Mechanism of security in coexistence –reference

A.1 General Principal

The access to Data Bases is secured by authentication and possibly encryption

[Note: the security part is a temporary text adopted from contribution C802.16h-05/11r1 and WirelessMAN-CX is calling for comments]

Figure h A1 shows the IEEE 802.16 LE inter-system communication architecture:

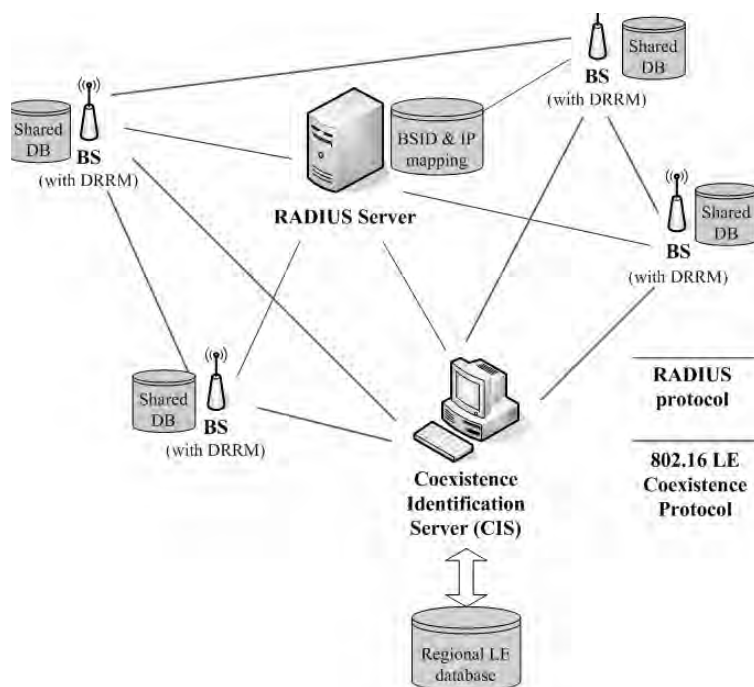


Figure h-A1—Network Architecture

General architecture includes the components operating over IP-based network:

- The RADIUS Server- The Base Station Identification Server (BSIS), ~~described in detail in section xxx~~
The BSs cooperating with the Distributed Radio Resource Management (DRRM) procedure RADIUS server performs two primary functions. The first one is to authenticate 802.16 LE BSs and BSIS. Keyed-Hashing for Message Authentication (HMAC) with Message Digest 5 (MD5) (RFC2869:2000) is adopted for authentication. The second one is to maintain the address mapping of wireless medium addresses of BSs (their

BSID) and medium addresses of BSIS to their IP addresses. This mapping is to distribute the keys for ESP used by BSs belonging to different systems.

BSIS maintains the geographic and operational information such as latitude, longitude and the BSID of LE BSs within certain management domain. BSs operating under LE system shall first query the foreign BSISs which are geographically close to the local BSIS and find the coexistence neighbor BSs while starting up, following the Coexistence protocol (detailed description in section 15.2.2.3). After the successful query procedure, the BS can obtain the BSIDs of the coexistence neighbor BSs. Intercommunication between BSs belonging to different systems is permitted after the BS acquires coexisting neighbor's Pairwise Master-key, and PMK-index for ESP.

Considering the IP network firewalls and different filtering rules, we should find a common security solution to make BSs/BSISs data connection transparent under almost common network management cases. IPSec is used to IPv4 and also included in IPv6 for the IP-Layer security solution. And all BSs/BSISs don't just reside in the same network environment. The data connections should go through some routers/firewalls and need to follow a common security rules.

Figure h A2 shows the BSs/BSISs connections encrypted in IPSec. Based on IPSec, all data connections between BSs/BSISs could pass through firewalls and routers unless some firewalls block IPSec connections.

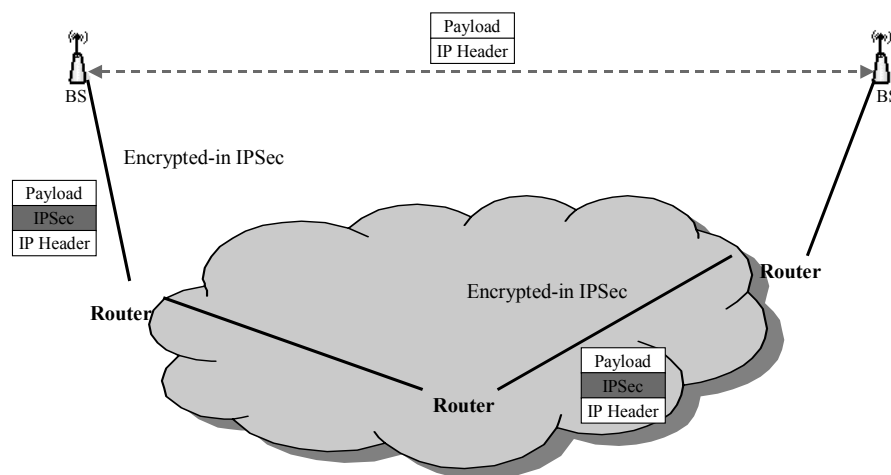


Figure h-A2—BSs/BSISs connection encrypted in IPSec

Figure h A2 demonstrates the IEEE 802.16 LE inter-network communication architecture under multi-Operators with multi-RADIUS Servers.

If BS-1 wants to communicate with BS-2, it must get BS-2's Country's Code, Operator ID and BSID from local BSIS first. And then work as the following steps

(1) BS-1 send RADIUS-Access-Request frame with BS-2's Country's Code, Operator ID and BSID to local RADIUS-Server

(2) Local RADIUS-Server will act as RADIUS-Proxy and transfer this RADIUS-Access-Request to the target RADIUS-Server

(3) Target RADIUS-Server will response RADIUS-Access-Accept with Pairwise-Master-Key and PMK-index for BS-1 and Security-Block for BS-2

(4) Local RADIUS-Server will generate Security-Block including Pairwise-Master-Key and PMK-index from target RADIUS-Server

(5) BS-1 will receive RADIUS-Access-Accept from its local RADIUS-Server and get the Pairwise-Master-Key PMK-index and ESP Authentication/Transform IDs in Security-Block for BS-1

(6) BS-1 will act as a PKM-initiator to send Session-Key-Start to BS-2 with Security-Block for BS-2

(7) BS-2 will calculate the ESP-Key-Stuffs with Pairwise-Master-Key, choose the ESP Authentication/Transform IDs supported by BS-2 and response Session-Key-Request to BS-1

(8) BS-1 will also calculate the ESP-Key-Stuffs with Pairwise-Master-Key to verify Key-Signature, compare ESP Authentication/Transform IDs support by BS-2 with current settings supported by BS-1 and response Session-Key-Response to BS-2

(9) BS-2 will verify Key-Signature and response Session-Key-Accept to BS-1

(10) After the above procedures, BS-1 and BS-2 could communicate in IPSec with the ESP-Key-Stuffs generated dynamically

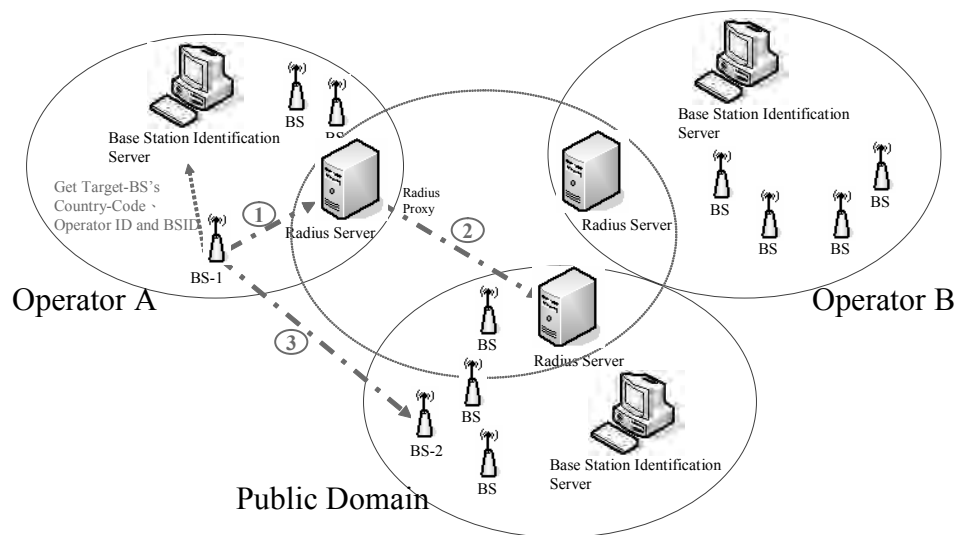


Figure h-A3—Network Architecture under multi-Operators with multi-RADIUS Servers

The following figure shows the each connection of BSs/BSISs will be encrypted in individual Session-Key in IPsec

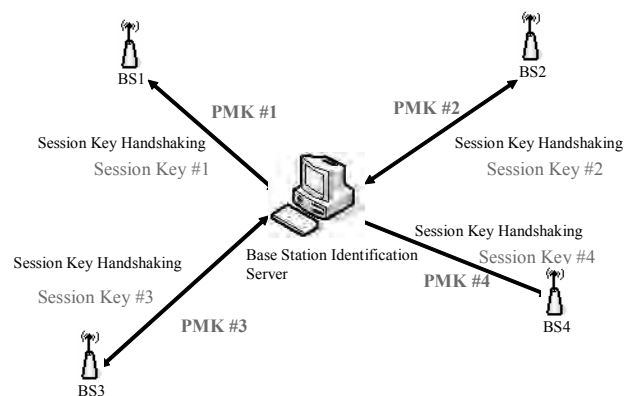


Figure h-A4—Individual Session-Key

For the BSs/BSISs, each connection with different BSs/BSISs will use individual Session-Key in IPsec. Those Session Keys would be generated from PKM-Handshaking with Pairwise-Master-Keys between each pair BSs/BSISs. The re-key procedures also don't need RADIUS-Servers and just use Pairwise-Master-Keys.

A.2 Coexistence Protocol

[Note: the security part is a temporary text adopted from contribution C802.16h-05/11r1 and is subject to further discussion.]

In order to get the coexistence neighbor topology, perform registration to the database and registration to peer, negotiation for Shared RRM etc. will be used a Coexistence Protocol (CP). [Figure h A5](#) describes the WirelessMAN-CX protocol architecture. The protocol architecture indicates that DRRM, Coexistence Protocol and Shared DB belong to LE Management Part located in management plane and the messages will be exchanged over IP network. Thus, DRRM in LE Management Part uses the Coexistence protocol to communicate with other BSs and with Regional LE DB and interact with MAC or PHY. [Figure h A5](#) is LE BS architecture with Coexistence Protocol. The gray area indicates area where there is an absence of connection between blocks. DSM is Distribution System Medium which is another interface to the backbone network. Note that is architecture is only for reference. Similarly, [Figure h A5](#) is the BSIS architecture with co-located regional LE database. Other architectures are not being illustrated. The Coexistence Protocol services are accessed by the LE Management Entity through CP SAP. The service primitives are described in t.b.d A BS uses the Coexistence Protocol, which is similar to PKM protocol, to perform the coexistence resolution and negotiation procedures. There are two types of messages to support Coexistence Protocol:

(1) CP-REQ: BS->BS or BS->BSIS

(2) CP-RSP: BS->BS or BSIS->BS

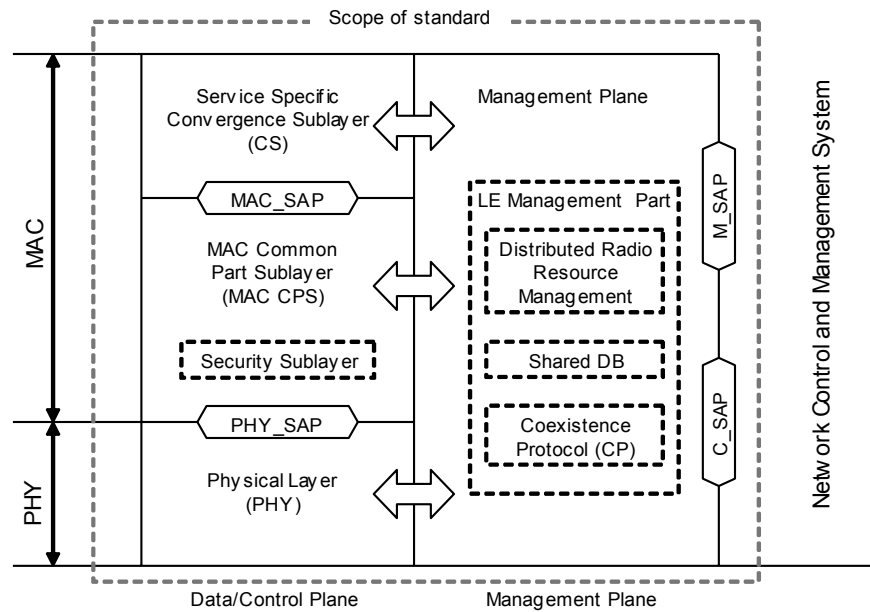


Figure h-A5—WirelessMAN-CX BS Protocol architecture Model

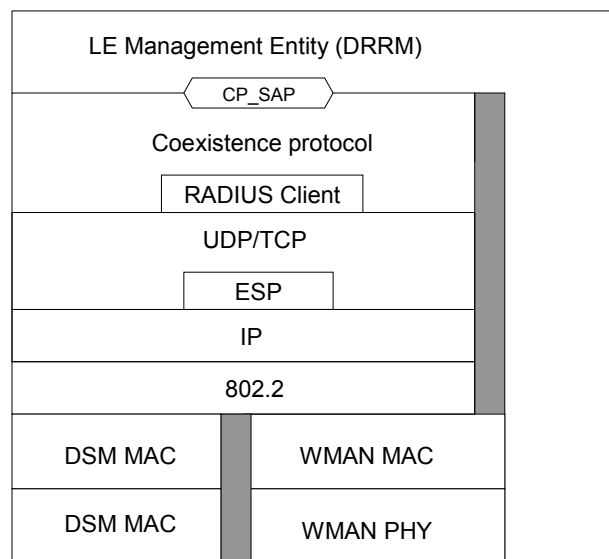


Figure h-A6—LE BS architecture with Coexistence Protocol

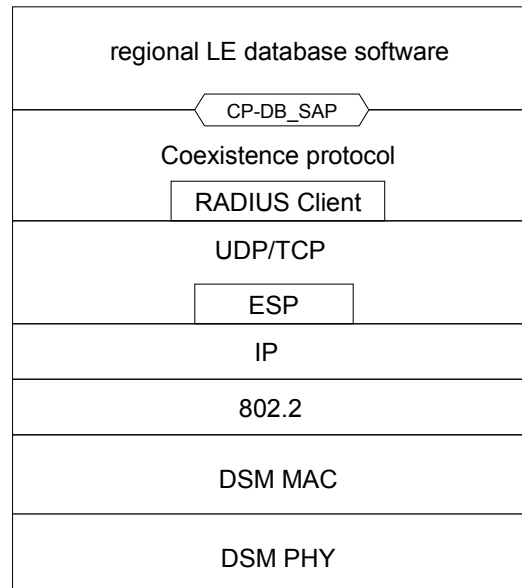


Figure h-A7—BSIS architecture with co-located regional LE database

To use the Coexistence Protocol, which is similar to PKM protocol, to perform the coexistence resolution and negotiation procedures a BS sends a CP-REQ to another BS or BSIS and waits for the CP-RSP.

Before any data can be exchanged between BS and BS/BSIS, security association must be setup first. IEEE 802.16 LE security associations between peers are established through RADIUS server. Any BS wants to communicate with another BS or BSIS shall first send a *RADIUS Access-Request* to request the establishment of the security association between originated BS and terminated BS/BSIS. RADIUS server replies a *RADIUS Access-Accept*, which includes security information for ESP operation, to the BS. At this point, only *virtual* security association is established between the peers. The BS sends the Security Block for the peer, which it received from the RADIUS Server, as a CP-REQ packet with message type *Send-Security-Block*. This is the first message in the Coexistence Protocol TCP exchange between the BS and BS or BS and BSIS. The peer returns CP-RSP packet with message type *Send-Security-Block*. At this point both sides have the information to encrypt all further packets for this exchange between the BS and BS or BS and BSIS.

The UDP port number assigned by IANA to be opened for the CP for transmission and reception of CP packets is TBD.

The TCP port number assigned by IANA to be opened for the CP for transmission and reception of CP packets is TBD.

A.3 Base Station Identification Server

[Note: The following part from 3.2.4.1 is a temporary text adopted from contribution C802.16h-05/11r1 and is subject to further discussion. A call for comment from security experts is open to comment on this text.]

The *Base Station Identification Server* (BSIS) acts as an interface between 802.16 LE BSs and the regional LE DB which stores the geographic and important operational information, e.g. latitude, longitude, BSID etc., of the LE BSs belonging to the same region. It converts the actions carried in PDUs received from the 802.16 LE BSs to the proper formats, e.g. SQL (Structured Query Language) string, and forwards the strings to the regional LE DB, which can be any available database software. BSIS converts the query results from the regional LE DB to the proper format, e.g. TLV encodings, and replies to the requested BSs. Figure h A7 shows the general architecture of inter-network communication across 802.16 LE systems. In this architecture, the 802.16 LE systems (BSs and BSIS) from different networks set up security association (including BS and BS, BSIS and BSIS) with each other by utilizing the services provided by the RADIUS server. BSIS acts as a peer of 802.16 LE BSs in this architecture. The BSID of regional BSIS is well known among the 802.16 LE systems within certain domain. In summary, ESP with RADIUS can discover a Rogue BS or BSIS. The messages exchanged between the LE BSs and the BSIS will be revealed in the next section. Note that the interface between BSIS and regional LE DB is out of scope.

A.4 RADIUS Protocol Usage

For future interoperability consideration, similar mechanisms are maintained. Secure exchange of 802.16 LE signaling information can be achieved after successful procedures of the RADIUS protocol. To include RADIUS support, the RADIUS server and the BS/BSIS RADIUS client must be configured with the shared secret key and with each other's IP address. Each BS/BSIS acts as a RADIUS client and has its own shared secret key with the RADIUS server. The shared secret key may be different from that of any other BS/BSIS.

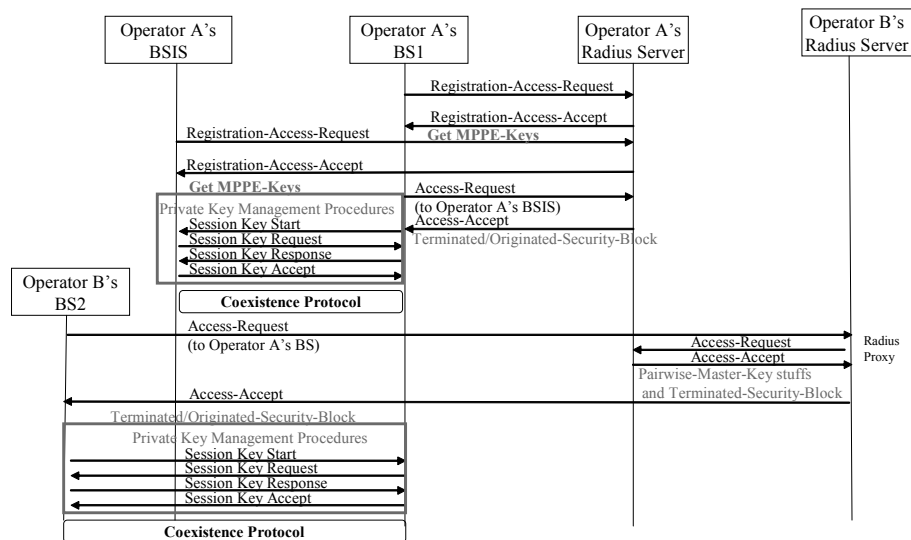


Figure h-A8—RADIUS protocol example

Figure h A8 shows the RADIUS protocol message exchange sequence. At starting up, each BS or BSIS must send a RADIUS-BS/BSIS-Registration-Access-Request (shown in Table h A1) to the RADIUS server

for authentication purpose and leave the address mapping (BSID to IP) information in the server. At this time, the RADIUS server will retain the following information of registered BS or BSIS:

- a) Wireless medium address of BS (BSID) or medium address of BSIS,
- b) MPPE-Keys in RADIUS-BS/BSIS-Registration-Access-Request/Accept Procedures
- c) IP address or DNS name,
- d) Cipher suites supported by the BS or BSIS for the protection of Coexistence Protocol communications,
- e) and Pairwise-Master-Key for BS or BSIS to establish Session-Key-Handshaking procedures

Same as [2], Microsoft Point-to-Point Encryption (MPPE) (RFC 2548:1999) key is introduced. The MS-MPPE-Send-Key, which could be got in the RADIUS-BS/BSIS-Registration-Access-Accept message (shown in Table h A1) and RADIUS-BS/BSIS-Access-Accept message (shown in Table h A1), is used for encrypting the security blocks in the RADIUS-BS/BSIS-Access-accept message for PKM-target and PKM-initiator. A registration access reject message may be issued due to a BS not supporting the ESP Transform or ESP Authentication algorithm selected for use in securing the following intercommunication, or for other RADIUS configuration reasons not discussed here.

Once a BS wants to get the knowledge of coexistence neighbor topology, it must first send RADIUS-BS/BSIS-Access-Request message (shown in Table h A1) to the RADIUS server in order to acquire the regional BSIS's IP address. The wireless medium addresses of regional BSIS, similar to BSID, well known by all BSs supporting LE operation, is sent in the RADIUS-BS/BSIS-Access-Request message to the RADIUS server for looking up IP address of the BSIS. Upon receiving the request message, the RADIUS server will respond with a RADIUS-BS/BSIS-Access-Accept message (shown in Table h A1) if the BS is a valid member which is allowed to perform inter-communication. The RADIUS-BS/BSIS-Access-Accept message would contain Originated-BS-Security-Block(for BS encrypted in MPPE-Send-Key from current RADIUS-BS/BSIS-Access-Request/Accept message) and Terminated-BS/BSIS-Security-Block(for BSIS encrypted in MPPE-Send-Key from BSIS's RADIUS-BS/BSIS-Registration-Access-Request/Accept message). Security-Block (shown in Table h A1) contains Pairwise Master Key IndexPairwise-Master-KEYKey Lifetime-the list of ESP Authentication/Transform IDs for initiator-send/receive for establishing a secure connection with the BSIS .

After querying process between the BS and the regional BSIS in Coexistence Protocol, the BSIS will respond to the BS with possible coexistence neighbor BSs candidates and their BSIDs. The BS, then, tries to establish secure connections with the coexistence neighbor BSs after evaluating the coexistence relationships with these candidates. The BS sends RADIUS-BS/BSIS-Access-Request message to local RADIUS server for Originated/Terminated-BS/BSIS-Security-Blocks. After getting Security-Blocks from RADIUS-BS/BSIS-Access-Accept messages, the BS establishes secure connections with each evaluated coexistence neighbor BS.

An access reject message may be issued due to a BS or the regional BSIS not supporting the ESP Transform or ESP Authentication algorithm selected for the following intercommunication, or for other RADIUS configuration reasons not discussed here.

Table h-A1—Security Block Format

Element ID	Length	Information
1	1	Pairwise Master Key Index for BS/BSIS (0-255)
2	32	Pairwise-Master-KEY
3	4 * number	The list of ESP Authentication IDs corresponding to the ESP Authentication algorithms for initiator-send
4	4 * number	The list of ESP Transform IDs corresponding to the ESP transforms for initiator-send

5	4 * number	The list of ESP Authentication IDs corresponding to the ESP Authentication algorithms for initiator-receive
6	4 * number	The list of ESP Transform IDs corresponding to the ESP transforms for initiator-receive
7	4	Pairwise-Master-KEY Lifetime

The Security-Block would be encrypted in 32-bytes MPPE-Send-Key with the following manner ('+' indicates concatenation):

$$b(1) = \text{MD5}(\text{MPPE-Send-Key} + \text{BSID}) \quad c(1) = p(1) \text{ xor } b(1) \quad C = c(1)$$

$$b(2) = \text{MD5}(\text{MPPE-Send-Key} + \text{BSID} + c(1)) \quad c(2) = p(2) \text{ xor } b(2) \quad C = C + c(2)$$

. .

. .

. .

$$b(i) = \text{MD5}(\text{MPPE-Send-Key} + \text{BSID} + c(i-1)) \quad c(i) = p(i) \text{ xor } b(i) \quad C = C + c(i)$$

Break plain text into 16 octet chunks $p(1), p(2) \dots p(i)$, where $i = \text{len}(P)/16$. Call the ciphertext blocks $c(1), c(2) \dots c(i)$ and the final ciphertext C . Intermediate values $b(1), b(2) \dots c(i)$ are required. The resulting encrypted String field will contain $c(1)+c(2)+\dots+c(i)$.

For Originated Security Block, the encrypted MPPE-Send-Key is from "RADIUS-Access-Request/Accept". For Terminated Security Block, the encrypted MPPE-Send-Key is from "RADIUS-Registration-Access-Request/Accept".

A.5 Privacy Key Management protocol usage

The PKM protocol would provide a flexible and easy-to-maintain key exchange mechanism. The PKM is based on the Pairwise-Master-Key to provide a symmetric key for the PKM-Initiator and PKM-Target side.

The following figure shows the PKM Session-Key-Handshaking procedures

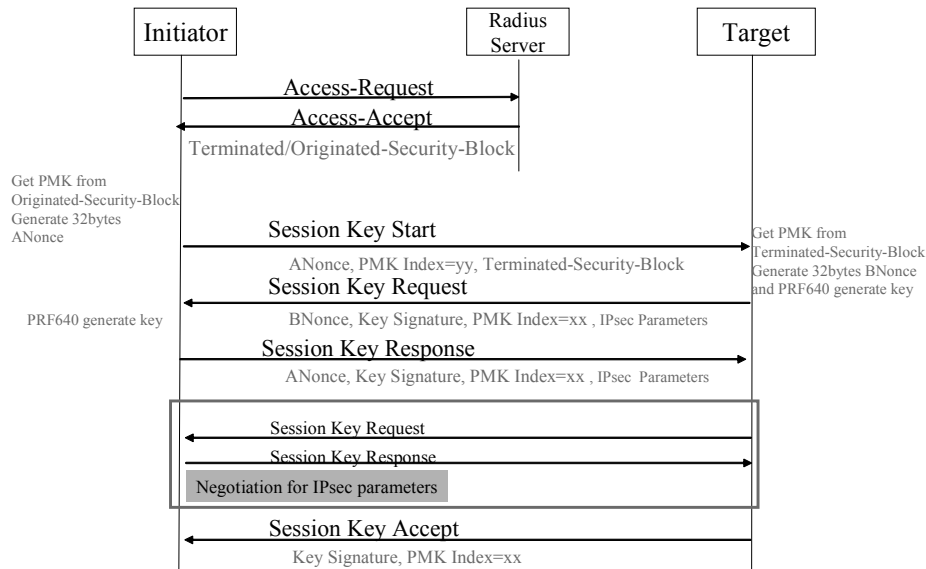


Figure h-A9—PKM Session-Key-Handshaking procedures

The PKM-Initiator will need to get the Pairwise-Master Key in Originated-BS-Security-Block from RADIUS-Server. And then perform the following steps

- 1) PKM-Initiator would get Pairwise-Master-Key-IndexPairwise -Master-KeyESP Authentication/Transform IDs and Key-Lifetime in originated Security-Block in RADIUS-BS/BSIS-Access-Accept message and then generate a random 32-bytes ANonce.
- 2) PKM-Initiator would will send Session-Key-Start message to PKM-Target with “ANonce””Pairwise-Master-Key-Index” and “Terminated Security-Block”.
- 3) After receiving Session-Key-Start message, PKM-Target would generate a random 32-bytes BNonce. And perform the PRF640 algorithm to generate the 640-bits Key. Keep the first 512-bits ESP-Transform/Authentication Keys and use the last 128-bits M-Key as the HMAC-MD5 key to generate 16-bytes Key-Signature.
- 4) PKM-Target would will send Session-Key-Request message to PKM-Initiator with “BNonce””Pairwise-Master-Key-Index” and ” ESP Authentication/Transform IDs”(PKM-Target chosen).
- 5) After receiving Session-Key-Request message, PKM-Initiator would perform the PRF640 algorithm to generate the 640-bits Key. Keep the first 512-bits ESP-Transform/Authentication Keys and use the last 128-bits M-Key as the HMAC-MD5 key to generate 16-bytes Key-Signature to verify the Key-Signature field on the Session-Key-Request message. If it is wrong, PKM-Initiator would perform silent-drop and doesn’t response any message. If it is correct, PKM-Initiator would prepare the Session-Key-Response message and use HMAC-MD5 generate Key-Signature filed.
- 6) PKM-Initiator would will send Session-Key-Response message to PKM-Target with “ANonce””Pairwise-Master-Key-Index” and ” ESP Authentication/Transform IDs”(PKM-Initiator chosen) .
- 7) After receiving Session-Key- Response message, PKM-Target would check the ANonce value if equal to the previous ANonce value in Session-Key-Start message and use HMAC-MD5

- 1 generate Key-Signature field to verify the Key-Signature field. Compare the values of "ESP
- 2 Authentication/Transform IDs" to make sure the security parameters.
- 3
- 4 8) After the above, PKM-Target will send Session-Key-Accept with Key-Signature field to PKM-
- 5 Initiator to verify.
- 6
- 7 9) The following IPsec connection will use the first 512-bits ESP-Transform/Authentication Keys
- 8 from PRF640 as keys and perform the ESP-Transform/Authentication algorithms from chosen
- 9 ESP Authentication/Transform IDs.

10 The following figure shows the PKM Session-Key Re-Key procedures

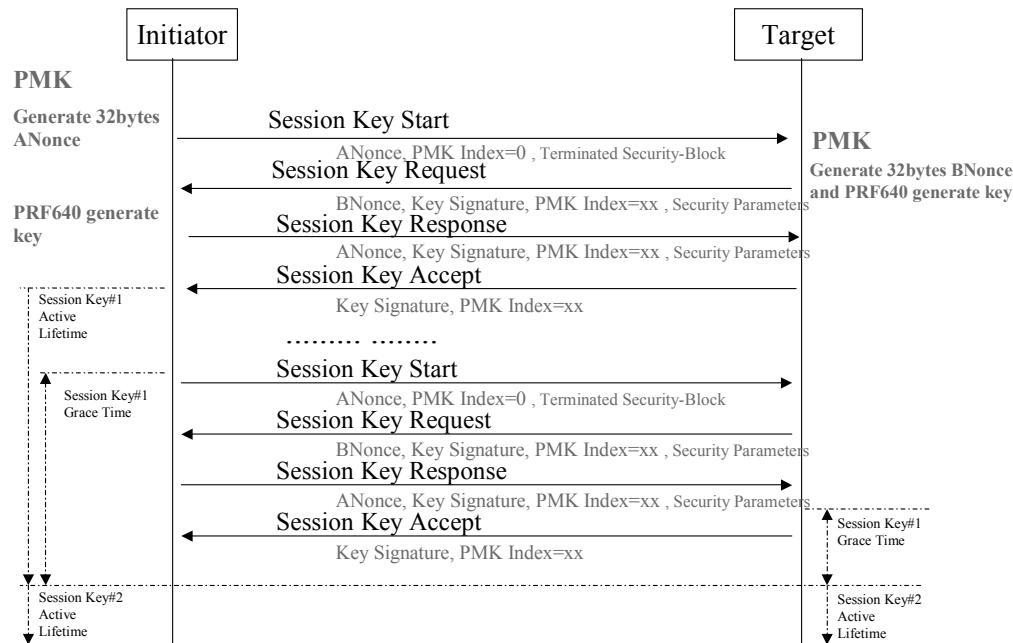


Figure h-A10—PKM Session-Key Re-Key procedures

Each Session-Key would set a Key-Lifetime, and PKM-Initiator could set a Session-Key grace time to perform Session-Key-Handshaking for the next new Session-Key#2 to be generated until the end of the key lifetime. The Session-Key#1 could use up its lifetime and then activate the Session-Key#2. If each side use the Session-Key#2 first in IPsec connection, it could also activate the Session-Key#2. If the lifetime of Session-Key#1 use up, the PKM-Initiator doesn't perform the Session-Key Re-Key procedures. PKM-Target would disconnect the IP connection until the Session-Key#2 generated.

The following figure shows the PKM Session-Key Re-Key procedures with the PMK update

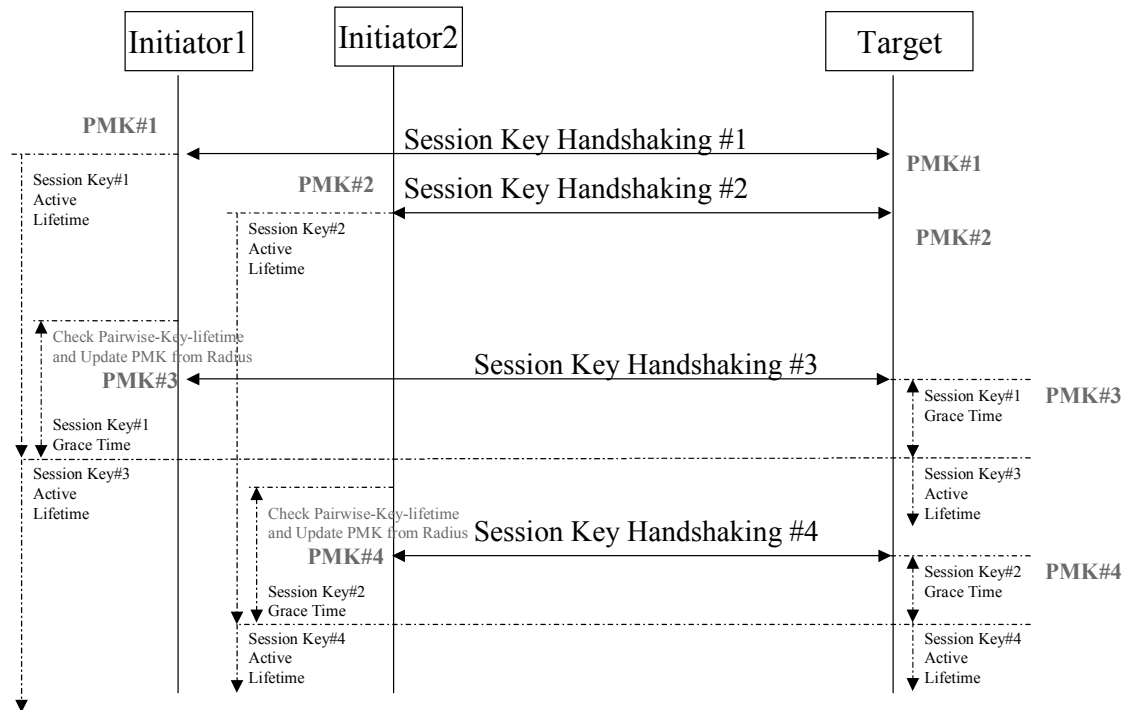


Figure h-A11—PKM Session-Key Re-Key procedures with the MK update of PKM-Target

The PKM-Initiator will check the current Pairwise-Key-Lifetime if still valid. If the PKM-Initiator detects the Pairwise-Key-Lifetime used up, it would perform RADIUS-BS/BSIS- Access-Request/Accept procedures to get the latest Pairwise-Master-Key in Security-Blocks from RADIUS-Server.

Each Pairwise-Master-Key would set a Pairwise-Master-Key-Lifetime, and BSs/BSISs could set a Pairwise-Master-Key grace time to perform Access-Request/Accept procedures for the new Pairwise-Master-Key until the end of the Pairwise-Master-Key lifetime. If the lifetime of Pairwise-Master-Key use up, the originated BSs/BSISs don't perform the Access-Request/Accept procedures, the terminated BSs/BSISs should discard the connections.

The following figure shows the 640-bits Key generated by PRF640

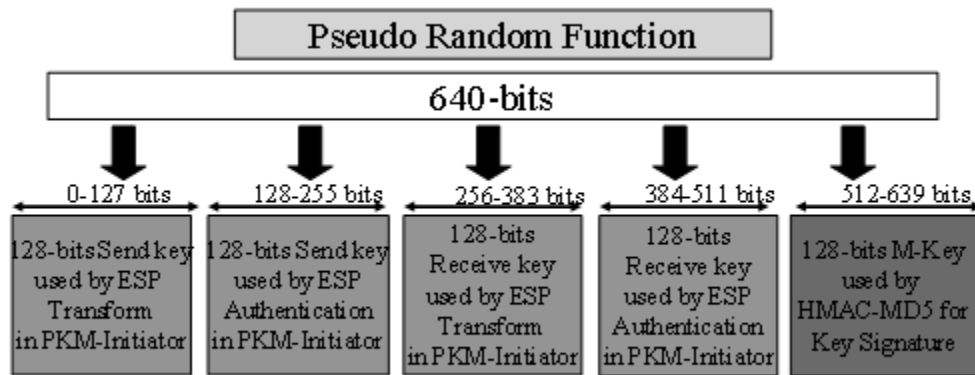


Figure h-A12—the 640-bits Key generated by PRF640

The BSs/BSISs get Pairwise-Master-Key from RADIUS-Servers and generate 32-bytes Nonce value to derive 640-bits key as follows

*PRF-640(PMK, "BS-BSIS key expansion", Min(BS1ID,BS2ID) || Max (BS1ID,BS2ID)||
Min(ANonce,BNonce) || Max(ANonce,BNonce))*

Where

PRF-640 (K,A,B) =
for $i=0$ to 4 do
 $R=R|HMAC-SHA-1(K, A||0||B||i)$

return LeastSignificant-640-bits(R)
and " $|$ " denotes bitstring concatenation

A.6 Security consideration

In this model, data traffic is protected by using IPsec.

The IP Security Protocol provides cryptographically based security for IPv4. The protection offered by IPsec is achieved by using one or both of the data protection protocols (AH and ESP). Data protection requirements are defined in the Security Policy Database (SPD). IPsec assumes use of version 2 of the Internet Key Exchange protocol, but a key and security association (SA) management system with comparable features can be used instead.

A.7 RADIUS Protocol Messages

The following messages are listed to support RADIUS protocol:

Note that[tbd.] means To Be Defined.

- *RADIUS-BS/BSIS-Registration-Request (BS/BSIS RADIUS server): A startup BS/BSIS sends this message for authentication purpose.*

Table h-A2—RADIUS-BS/BSIS-Registration-Access-Request

Attribute number	Attribute name	Value
1	User-Name	BSID. The BSID should be represented in ASCII format, with octet values separated by a “-”. Example: “00-10-A4-23-19-C0”.
4	NAS-IP-Address	BS’s IP Address
6	Service-Type	Coexistence-Protocol-Register (value =[tbd.], ex. IAPP-Register, value = 15)
26	Vendor-Specific-Attribute (VSA)	The list of ESP Authentication IDs corresponding to the ESP Authentication algorithms supported by this BS (See Table h A7)
26-TBD	Supported-ESP-Authentication-Algorithms	
26-TBD	Supported-ESP-Transforms	
32	NAS-Identifier	BS’s NAS Identifier
80	Message-Authenticator	The RADIUS message’s authenticator

According to RFC 2865:2000, other RADIUS attributes may be included in the RADIUS-BS/BSIS-Registration-Access-Request packet in addition to the ones listed in Table h A3.

- *RADIUS-BS/BSIS-Registration-Accept (RADIUS server BS/BSIS): After RADIUS server verifies the valid membership, it will respond with this accept message.*

Table h-A3—RADIUS-BS/BSIS-Registration-Access-Accept

Attribute number	Attribute name	Value
1	User-Name	BSID.
6	Service-Type	Coexistence-Protocol -Register (value =[tbd.], ex. IAPP-Register, value = 15)
26	Vendor-Specific-Attribute (VSA)	The list of ESP Authentication IDs corresponding to the ESP Authentication algorithms approved by Radius Server
26-TBD	Supported-ESP-Authentication-Algorithms	
26-TBD	Supported-ESP-Transforms	
27	Session-Timeout	Number of seconds until the BS should re-issue the registration Access-Request to the RADIUS server to obtain new key information.
80	Message-Authenticator	The RADIUS message’s authenticator

According to RFC 2865:2000, other RADIUS attributes may be included in the RADIUS-BS/BSIS-Registration-Access-Accept packet in addition to the ones listed in Table h A4.

- RADIUS-BS/BSIS-Access-Request (BS/BSIS RADIUS server): The BS sends this message to request for inter-communication with another coexistence neighbor BS or a regional BSIS.

Table h-A4—RADIUS-BS/BSIS- Access-Request

Attribute number	Attribute name	Value
1	User-Name	User-Name must include Country-CodeOperator ID and Regional BSIS's WM address or coexistence neighbor BS's BSID
4	NAS-IP-Address	Original BS's IP Address (the BS sending this request message)
6	Service-Type	CS/BSIS-Check (value =[tbd.], ex. IAPP-AP-Check, value = 16)
61	NAS-Port-Type	Wireless – Other (value = 18)
80	Message-Authenticator	The RADIUS message's authenticator

According to RFC 2865:2000, other RADIUS attributes may be included in the RADIUS-BS/BSIS-Access-Request packet in addition to the ones listed in Table h A5.

RADIUS-BS/BSIS-Access-Accept (RADIUS server BS/BSIS): After verifying that the coexistence neighbor BS is valid member, RADIUS server will respond with the security blocks necessary for establishing a secure connection between the coexistence neighbor BS and requesting BS or between BSIS and requesting BS.

Table h-A5—RADIUS-BS/BSIS- Access-Accept

Attribute number	Attribute name	Value
1	User-Name	User-Name must include Country-CodeOperator ID and Regional BSIS's WM address or coexistence neighbor BS's BSID
8	Framed-IP-Address	IP Address of Regional BSIS or coexistence neighbor BS.
26	Vendor-Specific-Attribute (VSA)	Security Block encrypted using originated BS's MPPE-SEND-KEY, to be decrypted and used by the original BS Security Block encrypted using coexistence neighbor BS's MPPE-SEND-KEY (or BSIS's), to be decrypted and used by the coexistence neighbor BS (or BSIS)
26-TBD	Originated-BS-Security-Block	
26-TBD	Terminated-BS/BSIS-Security-Block	
80	Message-Authenticator	The RADIUS message's authenticator

According to RFC 2865:2000, other RADIUS attributes may be included in the RADIUS-BS/BSIS-Access-Accept packet in addition to the ones listed in Table h A6.

Table h-A6—ESP Transform identifiers

Transform identifier	Value	Reference
RESERVED	0	[RFC2407]
ESP_DES_IV64	1	[RFC2407]
ESP_DES	2	[RFC2407]
ESP_3DES	3	[RFC2407]
ESP_RC5	4	[RFC2407]
ESP_IDEA	5	[RFC2407]
ESP_CAST	6	[RFC2407]
ESP_BLOWFISH	7	[RFC2407]
ESP_3IDEA	8	[RFC2407]
ESP_DES_IV32	9	[RFC2407]

ESP_RC4	10	[RFC2407]
ESP_NULL	11	[RFC2407]
ESP_AES-CBC	12	[RFC3602]
Reserved for privacy use	249-255	[RFC2407]

Table h-A7—ESP Authentication algorithm identifiers

Transform identifier	Value	Reference
RESERVED	0	[RFC2407]
HMAC-MD5	1	[RFC2407]
HMAC-SHA	2	[RFC2407]
DES-MAC	3	[RFC2407]
KDPK	4	[RFC2407]
HMAC-SHA2-256	5	[Leech]
HMAC-SHA2-384	6	[Leech]
HMAC-SHA2-512	7	[Leech]
HMAC-RIPEMD	8	[RFC2857]
RESERVED	9-61439	
Reserved for privacy use	61440-65535	

A.8 Privacy Key Management protocol messages

The PKM protocol procedures contain 4 message actions, and each-side could check the code value of the begin of PKM message to recognize which action need to perform this moment. The meaning of codes for PKM message as follows

- 0 = Session Key Start
- 1 = Session Key Request
- 2 = Session Key Response
- 3 = Session Key Accept

The PKM message uses TLV format to add the following attributes

Table h-A8—Session Key frame TLV

Type	Length	Value Information
1	32	Nonce
2	8	Replay Counter
3	8	Key lifetime in seconds
4	16	Key Signature
5	4	Security Parameter Index
6	4 * number	The list of ESP Authentication IDs corresponding to the ESP Authentication algorithms for initiator-send supported by this BS
7	4 * number	The list of ESP Transform IDs corresponding to the ESP transforms for initiator-send supported by this BS
8	4 * number	The list of ESP Authentication IDs corresponding to the ESP Authentication algorithms for initiator-receive supported by this BS
9	4 * number	The list of ESP Transform IDs corresponding to the ESP transforms for initiator-receive supported by this BS

10	33 + 4*n	Security Block
----	----------	----------------

The Length field contains a 16-bits value to record the whole frames size starting from Code field, with the ESP-Transforms-and-Authentication-Algorithms-Codes field filled in if present.

The PMK-Index field contains a 8-bits value to record the current Pairwise-Master-Key-Index each PKM-side used. If the PKM-Target detects the PMK-Index different of PKM-Initiator, it must update the latest Pairwise-Master-Key.

The Replay-Counter field contains a 64-bits random number (such as 64-bit NTP timestamp) and does not repeat within the life of the Master-Key material.

The Key-Lifetime field contains a 64-bits value to record the Session-Key lifetime in seconds.

The Key-Signature field contains an HMAC-MD5 message integrity check computed over the Session-Key-Frame starting from Code field, with the ESP-Transforms-and-Authentication-Algorithms-Codes field filled in if present, but with the Key Signature field set to zero. The M-Key is used as the HMAC-MD5 key.

The Security-Parameters-Index field contains a 32-bits value to assign to the IPsec Security Association (including the encryption and authentication keys, the authentication algorithm for AH and ESP, the encryption algorithm for ESP, the lifetime of encryption keys...etc in this session). PKM-Initiator/Target could check the SPI value in ESP-Header to detect to use which SA for this IPsec connection.

The following figure shows the Session-Key-Start message format

Code(1) =0	Length(2)	PMK Index(1)	Source_BSSID(6)	Destination_BSSID(6)
TLV Attributes..... NONCE(32) Security Parameters Index (4) Terminated Security Block (33 + 4*n)				

Figure h-A13—Session-Key-Start message format

The following figure shows the Session-Key-Request message format

Code(1) =1	Length(2)	PMK Index(1)	Source_BSSID(6)	Destination_BSSID(6)
TLV Attributes..... NONCE (32) Replay Counter (8) Key Lifetime (8) Key Signature (16) Security Parameters Index (4) ESP Authentication IDs for initiator-send supported by this BS (Codes Number(1) + Codes Number *4) ESP Transform IDs for initiator-send supported by this BS (Codes Number(1) + Codes Number *4) ESP Authentication IDs for initiator-receive supported by this BS (Codes Number(1) + Codes Number *4) ESP Transform IDs for initiator-receive supported by this BS (Codes Number(1) + Codes Number *4)				

Figure h-A14—Session-Key-Request message format

The following figure shows the Session-Key-Response message format

Code(1) =2	Length(2)	PMK Index(1)	Source_BSSID(6)	Destination_BSSID(6)
TLV Attributes..... NONCE (32) Replay Counter (8) Key Lifetime (8) Key Signature (16) Security Parameters Index (4) ESP Authentication IDs for initiator-send supported by this BS (Codes Number(1) + Codes Number *4) ESP Transform IDs for initiator-send supported by this BS (Codes Number(1) + Codes Number *4) ESP Authentication IDs for initiator-receive supported by this BS (Codes Number(1) + Codes Number *4) ESP Transform IDs for initiator-receive supported by this BS (Codes Number(1) + Codes Number *4)				

Figure h-A15—Session-Key-Response message format

The following figure shows the Session-Key-Accept message format

Code(1) =3	Length(2)	PMK Index(1)	Source_BSSID(6)	Destination_BSSID(6)
TLV Attributes..... Replay Counter (8) Key Signature (16)				

Figure h-A16—Session-Key-Accept message format

Annex B

(informative)

GPS Timing and Base Station Synchronization

Every WirelessMAN-CX systems should be synchronized to a globally distributed reference timing system that is capable of allowing the network Base Stations to synthesize a 1 pps NTI and a UTC time stamp. The Global Positioning System (GPS) is capable of providing these temporal references to the Base Stations that are equipped with GPS receivers.

The Base stations equipped with a GPS receiver are capable of receiving a UTC synchronized 1 pps timing signal. The clock pulses derived from a GPS receiver are accurate to ± 100 usec and the derived pulses typically have rise times within ± 2.5 nsec. Figure h B1 shows a typical GPS 1 sec pulse and its duration (Trimble Inc. Palisade output).

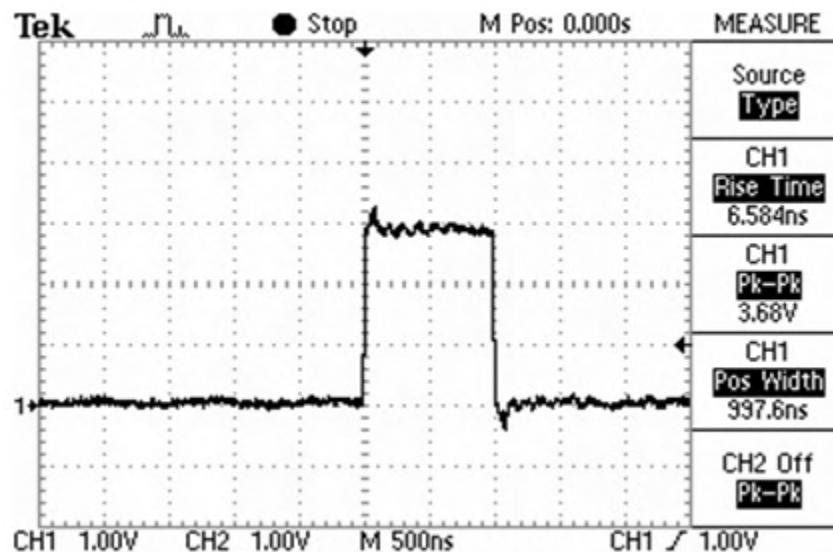


Figure h-B1—GPS 1pps Pulse

The availability of a globally distributed clock will result in a common temporal unit that can be used in negotiating access times to spectrum shared by a community of ad-hoc users. Non- WirelessMAN-CX networks having different architectures and messaging signals could also use a common 1 second interval for synchronization of their networks. This would conceivably allow communication between all IEEE 802.16 networks in a synchronized manner, to facilitating the exchange of information related to coexistence and spectrum sharing.

The one second reference time is appropriate because it is distributed directly by the GPS. WirelessMAN-CX networks typically have frames on the order of several to tens of milliseconds, which is a granularity that could allow several to several tens of networks to negotiate coexistence subintervals within the 1 second span. Additionally, for IP networks, the 1 second interval is of a length sufficient to accommodate inter-router TCP/IP latency, especially over networks that are likely to be close to each other, such as ad-hoc licence exempt systems.

Annex C

(informative)

interference scenario case study

C.1 Base Station initialization scenario case study

See to the figure below:

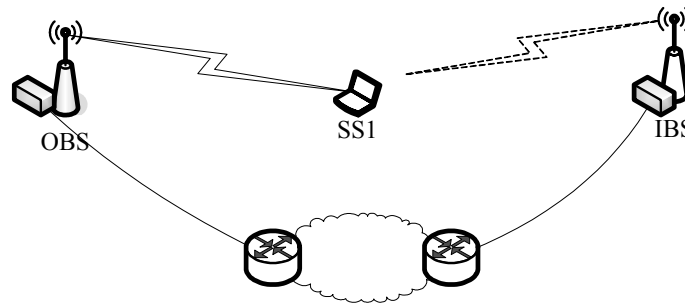


Figure h-C1—Environment of initializing basestation

Suppose OBS and SS1 are part of an operating network, SS1 has a stable air link with OBS and OBS has a wired link. Now assume that IBS comes into this area and already has a wired link IBS could contact OBS if he knows the IP address of OBS., Unfortunately IBS does not know OBS's IP address and there may be no regulatory server to ask for help. Notice also that the IBS will not have any SS attached before IBS itself has finished initialization.

There are three kinds of situations that may exist in both SS2BS and BS2SS interference/signaling:

- No interference/signaling detectable
- Interference/signaling detectable but signaling is not decodable
- interference detected and the signaling is decodable

The following designations will be used to illustrate these three cases in Figure h C2

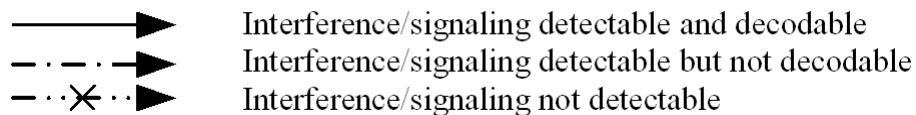


Figure h-C2—Legend of arrow indicating interference direction

[note: based on the synchronization assumption, the BS/BS and SS/SS interference could be ignored.]

The possible cases are:

- Case1x: IBS interference/signaling can not detected by SS1
- Case1a: the IBS can not detect the signal from the operating network
- Case1b: the IBS can detect the signal from the operating network, but not decodable
- Case1c: the IBS can detect and decode the signaling from the operating network
- Case2x: IBS interference/signaling can detected by SS1 but not decodable
- Case2a: the IBS can not detect the signal from the operating network
- Case2b: the IBS can detect the signal from the operating network, but not decodable
- Case2c: the IBS can detect and decode the signaling from the operating network
- Case3x: IBS interference/signaling can detected and decoded by SS1
- Case3a: the IBS can not detect the signal from the operating network
- Case3b: the IBS can detect the signal from the operating network, but not decodable
- Case3c: the IBS can detect and decode the signaling from the operating network

These cases are shown in Figure h C4

1)The red tick signifies that one of the BS may know the IP address of another BS by receiving the signaling from the air; The red cross signifies that the BS can not know the IP address of another BS by the signaling from the air.

2)The red dot line in one side means that from this side, the station can decode the signaling from the transmitter; The red dash line means from this side, the station can detect but can not decode; and the read solid line means the station can not sense transmitter.

✓	Known IP addr wire link is usable	⋮	Interference/signaling detected and decoded
			Interference/signaling detected but not able to decode
✗	Without IP addr wire link is not usable		Interference/signaling not detected

Figure h-C3—Legend of line indicating interference situation and symbols indicating wire-link usability

Case 1x:

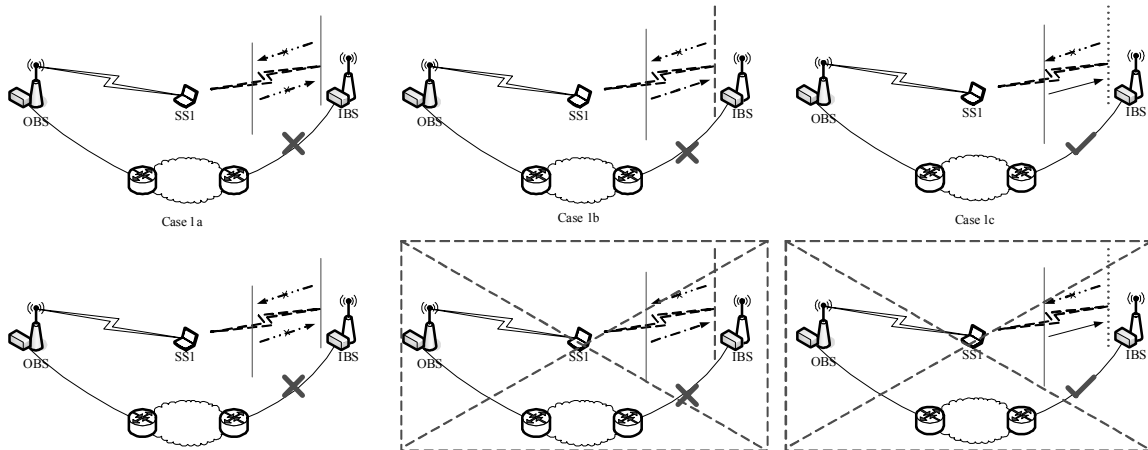


Figure h-C4—case 1x study

[Note: although logically case 1b and 1c could happen, these cases are not normally exist, because the channel propagation are symmetric in both direction, but the BSs' transmission power are normally higher than the SSs'. So when the IBS couldn't been detected by SS1, the IBS will not detect SS1's signal also.]

In these cases IBS doesn't interference with SS1, which means that the OBS's network does not need to contact the IBS. This Case 1x is not a target initialization scenario for WirelessMAN-CX base station .

Case 2x:

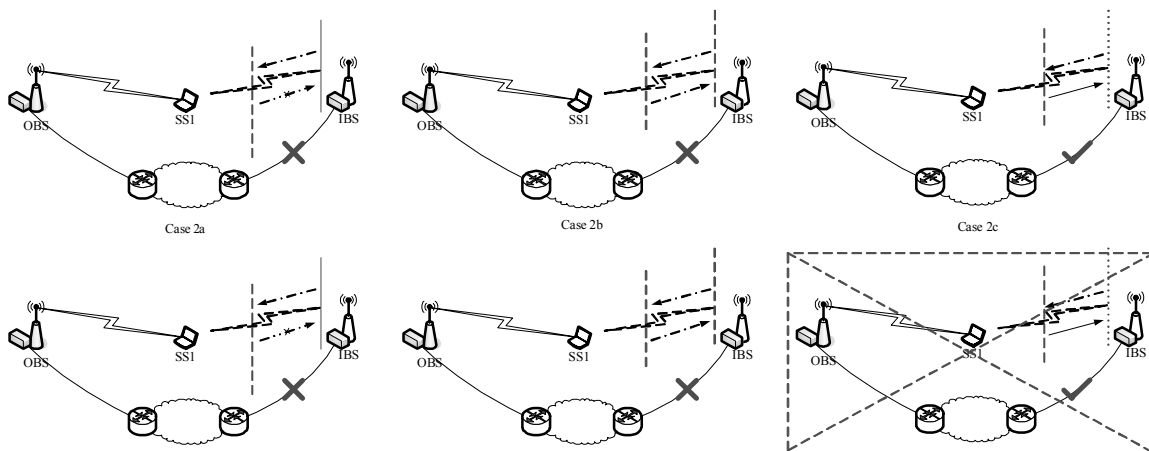


Figure h-C5—case 2x study

[Note: case 2c normally doesn't happen for the same reason with case 1b & 1c.]

In case 2x, , IBS's signaling may be detected by SS1, but SS1 cannot decode the signaling. IBS may interfere to SS1, but SS1 can not identify the interferer, so SS1 can not inform the OBS who is the interferer, so the OBS could not contact IBS for cooperation. Case 2x is the worst case for WirelessMAN-CX.

This worst case problem is due to the difference of SNR conditions between decodable signaling and troubling interference. The condition could be specified by a SNR requirement, the lower SNR required for the signaling, the lower probability to have this problem; another approach may help was introduced to the working document 15.3.2.3 in the meetings before is shown in IEEE C802.16h-05/041, and we could easily understand it in the following figure.

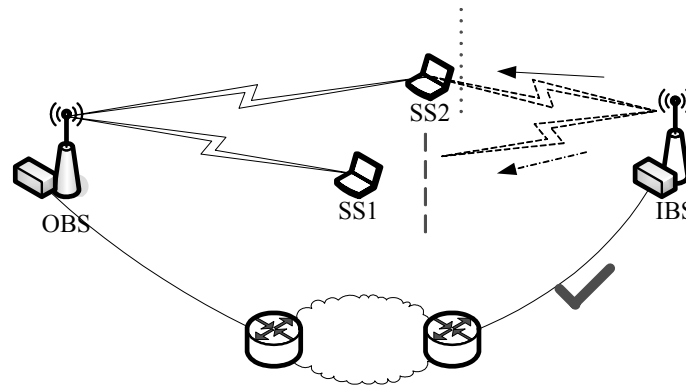


Figure h-C6—Enhanced mechanism dealing with case 2x

Some SSs (eg. SS1 in the Figure h C6) interfered by IBS can not decode the information contained in the broadcast signaling while some SSs decode it at the same time (eg. SS2 in the Figure h C6). All these interfered SS will report to OBS for the signaling. Dealing with all the report, OBS will try to figure out the interferer of the SSs which can not decode the signaling by report message of other SS at the same time, and make use of the interference time/frame_number inside each report message.

We could not absolutely get rid of the difference of the signal requirement between to be decoded and to interfere the transceiver, so we can not totally get rid of the possibility of the SSs to be not able to decode the signaling while being interfered, all we could do is to make the bad effect as little as possible. I don't understand this solution. Once in operating network all the interfered SSs could not decode the signaling, we have no chance to tell who is coming to interfere the network, and this operating network may need to switch/escape to another channel.

Case 3x:

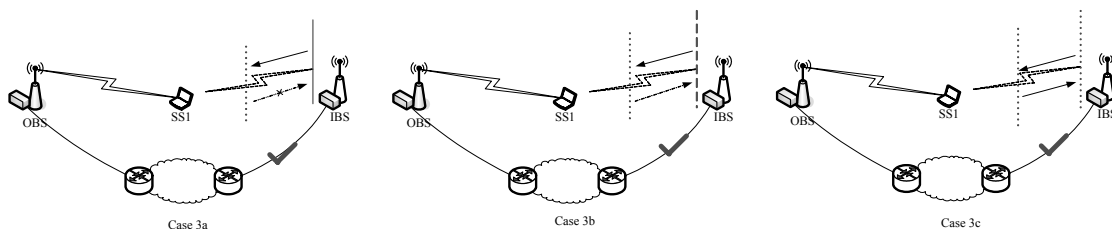


Figure h-C7—case 3x study

Case 3x is the most applicable use of WirelessMAN-CX solution. The common condition of Case3x is that SS can decode the IBS signaling. It's understood that if we don't depend on the IBS signaling transmission, in case 3a and 3b, operation network will not be able to find IBS in the core network. And the only way we

may enable the operating network to do this is using the SS to relay the signaling which is managed to contain the IP address information.

One security issue of CP message between BSs through IP network is roused, how to qualify that the message is from a neighbor station. The BS should make sure that the sender system of the message received its signaling broadcast. It means that the send system of the CP message should have air interface which can receive and decode the air signaling, nevertheless the system is close enough in distance so that it can receive and decode the signaling send in the air by the BS. If BS send only static information in the signaling, it will not be able to find out if the CP message sender is really its neighbor or just someone who have got the static information unexpected before. This security issue may be mitigated by checking the instant random key and frame numbering in the contact requirement message sent by the OBS. That may prevent the IBS being cheated by someone faraway or by someone which is not able to control or access the WirelessMAN-CX air link. We may need to think about this approach if we have no other choice to meet the cooperation contact requirement in case 3a and 3b.

For the sake of Case 2a and 3a, it's not logical to randomly choose the periodically silent CSI to occupy by the IBS, otherwise in the CSI which the IBS choose will cause collusion and make the initializing procedure not effective. Instead, it's needed to have a predefined periodical ICSI among all the CSI, and every IBS know the timing of ICSI as well. And the rest CSI will be used as OCSI and reallocated periodically to carry the signaling such as radio signature by the OBSs.

C.2 Interference Scenario Case Studies for Synchronized WirelessMAN-CX Systems conforming to a Common PHY Profile.

A case study for WirelessMAN-CX systems is provided. These systems are assumed to conform to the same PHY profile (Section 15.2.5), they are synchronized to a universal time standard such as GPS and can support CMI timing and signaling as outlined in Sections 15.4.2.3 and 15.3.2.1.

In the Common PHY profile concept the following system features are given:

(1) Each System (consisting of a base station (BS) and its subscriber stations (SS)) claims a special interval in time called a CMI in which the BS sends a unique identifier called a BSD and the SS send unique identifiers called SSURF messages. Only one system in a Coexistence Neighborhood can transit during its CMI, all other systems remain quiet and monitor.

(2) All systems are universally synchronized to a common timing standard such as GPS; the beginning of a CMI is universally known. Additionally, the sub-frame sizes in the Time Division Duplexing (TDD) access scheme are all exactly the same across all networks (another common PHY characteristic).

(3) The BSD and SSURF messages can be demodulated and their RSSI values can be determined by systems with which they interfere, hence the rationale for the common PHY and the ability to quantify interference as it occurs on a per burst basis.

(4) Every Subscriber Station and Base Station contains an Interference Table in which is registered the RF emission characteristics, locations, and identities (as IP addresses, SS_ID, BS_ID, etc.) of all the interferers that the SS or BS have ever detected. The table also contains an indication as to whether the interference has been resolved by the Coexistence Protocol (CP) or not. These tables also contain the statistics pertaining to the interference detected, such as its frequency of occurrence, mean RSSI, etc.

(5) Every Subscriber Station and Base Station uses a special series of MAC and CP messages to resolve and indicate interference. The MAC messages are specifically for interference detected at the Subscriber Station and are called BS_CCID_IND and BS_CCID_RSP. These messages detail foreign BS interference detected by the SS. The Coexistence Protocol messages are specifically for interference detected at the Base Station and are called SS_CCID_IND and SS_CCID_RSP. These messages detail foreign SS interference detected by the BS.

There are 4 interference scenarios seen by WirelessMAN-CX systems when they are in an Interference Neighbourhood. It is assumed co-channel interference is at a nominal level where it is capable of being demodulated; it is detected. Interference below such levels, which is sporadic and changes with the variations in the propagation environment, is only occasionally detectable. It is assumed that the SSURF and BSD messages are received at S/N levels to make them at least occasionally detectable as interference. These scenarios assume the interference, when it occurs, is at least occasionally detectable and trigger the responses that are described (ie just one instance of sporadic interference will trigger a response). In more sophisticated control scenarios it will be possible to adjust the levels at which responses are triggered. For example, very occasional sporadic interference may not be worth considering and responses will be inhibited, as long as such unresolved interference is minimal.

Scenarios:

1. New interference is detected by a subscriber stations of one system with the interference generated by base stations of another system (the foreign system). Both systems are independent but form a Coexistence Community, (see Section 15.1.1 Definitions). The interference now generated, for example, can be of one in which a hidden SS which becomes exposed to the foreign BS because of some physical change in the coverage area; for example, the removal of a tree that once hid the affected SS or the erection of a metal clad building. This scenario can also happen when a new SS is installed. See Figure h C8.

2. New interference is detected by a base station which is a member of a Coexistence Community. This interference is generated by a foreign subscriber station which is also a member of the same community. This scenario is equivalent to the one discussed in (1) above, but from the BS perspective. The physical changes discussed in (1) could give rise to the scenario described here.

3. New interference is detected at the SS and originates from foreign base stations which are not members of the Coexistence Community of the SS. The SS and foreign BS are initially not Coexistence Neighbors in this scenario. Figure h C9 shows this scenario.

4. New interference is detected at the base station which originates from a foreign SS which is not a member of the Coexistence Community of the base station.. The foreign SS and its BS are initially not Coexistence Neighbors in this scenario. This is equivalent to scenario (3) but from the BS perspective.

Interference Resolution Process

Scenario 1 [Figure h C8]:

- Subscriber Stations have a SS Interference Table (Section 15.3.3.1 Table h 6). Additionally, each system in the Coexistence Community has a unique CMI associated with it. During the CMI of the foreign system, the interfering (foreign) BS transmits a downlink BSD message (Section 6.3.2.3.62) which is received as interference at the SS. Since it is new interference (caused by the removal of a tree, for example), the SS will demodulate the interfering BSD and extract its contents.

- Since the interference is new and the BSD from the foreign BS is not registered in the SS Interference Table, the SS will then create a new entry in the table for the foreign BS, labeling it as new unresolved interference. The SS then sends a BS_CCID_IND message to its home BS, indicating the identity of the interfering BS.

Since the interfering BS is part of the Coexistence Community, the home BS will have negotiated non-interfering intervals between itself and the interfering BS (this being done previously via the Coexistence Protocol — See 15.1.5). If this were not the case, the two base stations would negotiate scheduling via the CP protocol. This undertaken successfully, the home BS will then schedule downlink transmissions directed to the reporting (interfered-with) SS to a time interval that is free of downlink interference from the interfering BS. This being done, the BS then sends a BS_CCID_RSP message to the SS, indicating that interference is resolved (this actually meaning that the BS transmissions to the SS will not be interfered because of scheduling).

— The SS, on receiving the BS_CCID_RSP from its BS, now assumes that downlink interference has been resolved. The SS then updates its SS Interference Table and will not send BS_CCID_IND messages whenever it detects the BSD of foreign BS. The SS will only listen for its downlink messages only during specifically scheduled intervals within the downlink subframe which are interference free and to which it has been assigned by its home BS.

Scenario 2.

— All Base Stations have a BS Interference Table (Section 15.3.3.1 Table h 4). Additionally, each WirelessMAN-CX system in the Coexistence Community has a unique CMI associated with it. During the CMI of the foreign system the interfering (foreign) SS transmits an uplink SSURF message (See 6.3.2.3.63) which is received as interference at the BS. The SSURF contains information about the identity of the interfering SS and the BS which controls it.

— The interfered-with BS compares this information with the information it has in its BS Interference Table. The BS will determine that (a) the interference is from a new interfering SS and (b) that the interfering SS is registered to a system which is a known Coexistence Neighbor. Since both WirelessMAN-CX Systems are Coexistence Neighbors, they have interference free intervals scheduled amongst themselves. A SS_CCID_IND message is then sent by the interfered-with BS to the BS controlling the interfering SS, indicating a need to resolve the uplink interference. This message is sent via the backbone IP network; usually to the proxy IP address of the interfering BS (this address being registered in the Interference Tables).

— The BS of the interfering system, having received a SS_CCID_IND message realizes that one of its SS is causing unresolved interference. Since this interference is being caused to a Coexistence Neighbor system with which interfering-free scheduling exists; the interfering BS schedules that particular SS to only transmit during non-interfering intervals.

— A SS_CCID_RSP message is sent back via the IP backbone to the interfered-with BS, indicating a resolution of the uplink interference and that the SS causing the interference is scheduled only to transmit on the uplink during previously negotiated non-interfering intervals.

— The BS Interference Table at the previously interfered-with BS is updated to show the resolved status and the interference is deemed resolved. The interfered-with BS will now not send SS_CCID_RSP messages when it receives SSURF from the interfering SS.

Scenario 3 [Figure h C9]:

— Interference from the foreign BS will be detected at the SS during the CMI of the foreign BS. Since the foreign BS (and its system) is not registered as a known interferer to the SS (by not being in the SS Interference Table), the SS will then create a new entry in the table for the foreign BS. By using the proxy IP address of the foreign BS extracted from the BSD of the foreign BS, the interfered-with SS sends a BS_CCID_IND message to its home BS thus indicating the identity of the interfering BS. At this point the interference is registered as detected and unresolved by the SS.

1 — The foreign BS is considered as an Interference Neighbour by the home BS. The home BS on receiving
2 the BS_CCID_IND then contacts the interfering BS via the IP and initiates the Coexistence Protocol (CP)
3 between the two BS. The negotiation necessitates the creation of a downlink slot which the interfering BS
4 can use without interfering the SS. The home BS also needs to reschedule its downlinks also to accommo-
5 date this change. The process can result in changes to EIRP and scheduling and the creation of spatial isola-
6 tion (if smart antennas are used), for example.
7
8

9
10
11 — On completing a successful CP negotiation the home BS will schedule its downlink messages to the SS
12 during the interference free intervals. The interfering BS will accommodate this by appropriated modifying
13 (or ceasing) its downlink transmissions during such intervals. A BS_CCID_RSP message is sent to the SS
14 by the home BS, indicating a resolution of the interference.
15

16
17
18 — The SS, on receiving the BS_CCID_RSP from its BS, now assumes that downlink interference has been
19 resolved. The SS then updates its SS Interference Table and will inhibit any further interference responses
20 due to detection of the foreign BS's BSD messages. The SS now has specific downlink intervals in which it
21 will look for traffic destined to itself. All other intervals are ignored.
22

23
24
25 — As a consequence of this process, the formerly interfering BS is now a member of a Coexistence Commu-
26 nity that includes both BSs. Both BSs update their BS Interference Tables so that new interference can be
27 more easily resolved now that the CP has established interference free intervals for the BSs.
28

29 30 Scenario 4:

31
32
33 — Interference from the foreign SSURF will be detected during the interfering system's CMI. Interference
34 is detected at the BS.
35

36
37
38 — The SSURF message will be decoded by the BS which will determine that the interference originates
39 from a system not registered in its BS Interference Table. The proxy IP address of the foreign BS control-
40 ling the interfering SS is derived from the SSURF. The interfered-with BS sends a SS_CCID_IND message
41 to the foreign BS indicating that interference was received from its SS, thus there is a need to negotiate
42 uplink coexistence.
43

44
45
46 — Both BS undertake the Coexistence Protocol and mutually determine interference free uplink slots which
47 the foreign SS can use. The interfered-with BS will also modify (or altogether cease) its use of these slots
48 for its uplink traffic
49

50
51
52 — On completion of the CP, both BSs update their Interference Tables to contain the characteristics of each
53 other, such as location, IP address, emission characteristics, etc.
54

55
56 — The two base stations and their associated SS are now members of a Coexistence Community.
57

58
59 — The interfering BS sends a SS_CCID_RSP message via the IP backbone; indicating that it has completed
60 its rescheduling, and that the interfering SS is now only transmitting uplink data during non-interfering
61 slots.
62

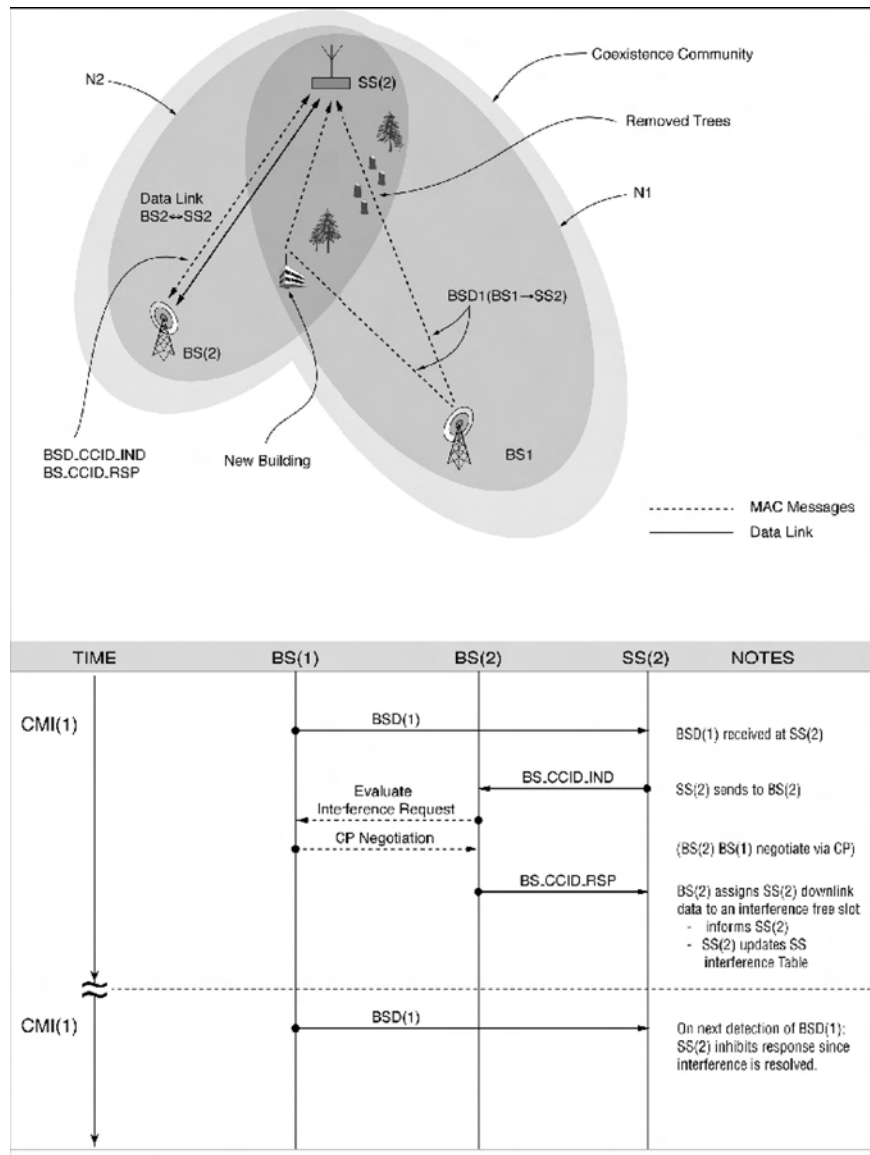


Figure h-C8—BS_CCID_IND BS_CCID_RSP procedure case 1

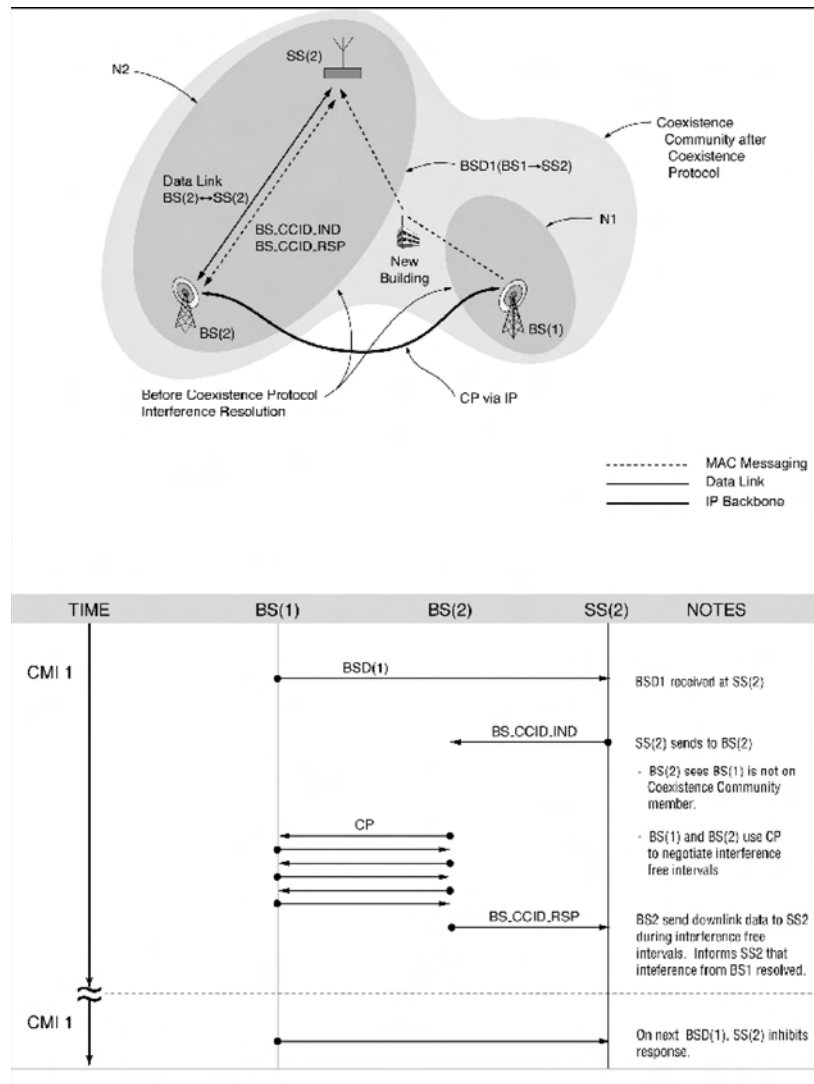


Figure h-C9—BS_CCID_IND BS_CCID_RSP procedure case1