

1

2

3 ~~Draft IEEE Standard for~~4 ~~— Local and Metropolitan Area Networks~~

5

6 **Part 16: Air Interface for Fixed Broadband**
7 **Wireless Access Systems**8 **Amendment for Improved Coexistence Mechanisms for**
9 **License-Exempt Operation**

10

11

12

13

Sponsor

14

LAN MAN Standards Committee

15

of the

16

IEEE Computer Society

17

and the

18

19

IEEE Microwave Theory and

20

Techniques Society

21

22

23

24

25

26

Copyright © 2005 by the Institute of Electrical and Electronics Engineers, Inc.

27

Three Park Avenue

28

New York, New York 10016-5997, USA

29

All rights reserved.

30

31

This document is NOT 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 Licensing and Contracts, IEEE Standards Activities Department. Other entities seeking permission to reproduce this document, in whole or in part, must obtain permission from the Manager, Standards Licensing and Contracts, IEEE Standards Activities Department.~~

32

33

34

35

36

37

38

39

40

41

IEEE Standards Activities Department

Standards Licensing and Contracts

445 Hoes Lane, P.O. Box 1331

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44

Participants

IEEE 802.16 Working Group Officers

Roger B. Marks, Chair
Ken Stanwood, Vice Chair
Dean Chang, Secretary

Primary development is to be carried out by the Working Group's License-Exempt Task Group:

Mariana Goldhamer, Chair
Barry Lewis, Vice-chair
Xuyong Wu, Technical Editor
Nader Zein, Secretary

~~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}*~~

1 Contents

2	1	Overview	10
3	1.1	General	10
4	1.2	IEEE 802.16h scope	10
5	1.3	IEEE 802.16h applicability	10
6	2	Interference detection and prevention – general architecture	10
7	2.1	Shared Radio Resource Management	10
8	2.1.1	Operational Principles	11
9	2.1.1.1	General Principles	11
10	2.1.1.2	Interference Control	16
11	2.1.1.3	Community Entry of new BS	16
12	2.1.1.4	Network and Community Entry for SS	17
13	2.1.1.5	BS regular operation	17
14	2.1.1.6	Operational dynamic changes	17
15	2.1.1.7	Coexistence with non-802.16 wireless access systems	18
16	2.1.2	Shared distributed system architecture	18
17	2.1.2.1	Architecture	18
18	2.1.2.2	Inter-network communication	20
19	3	Interference victims and sources	25
20	3.1	Identification of the interference situations	25
21	3.1.1	Interferer identification	25
22	3.1.2	Grouping of interfering/not-interfering units	25
23	3.2	Identification of spectrum sharers	25
24	3.2.1	Regulations	25
25	3.2.2	Messages to disseminate the information	25
26	3.2.3	Avoid false-identification situations	25
27	3.2.4	Storage of identification information	25

1	3.2.4.1	Regional LE database	25
2	3.2.4.2	Coexistence Identification Server.....	30
3	3.2.4.3	RADIUS Protocol Usage.....	31
4	3.2.5	Security consideration <i>[Note: to be reviewed by expert on security.]</i>	33
5	4	Interference prevention.....	33
6	4.1	Adaptive Channel Selection – ACS.....	33
7	4.1.1	Between 802.16 systems.....	33
8	4.2	Dynamic Frequency Selection – DFS	33
9	4.2.1	Frequency selection for regulatory compliance.....	33
10	5	Pro-active cognitive approach	33
11	5.1	Signaling to other systems.....	33
12	5.2	Recognition of other systems	33
13	6	Transmission of information	33
14	6.1	Coexistence Protocol (CP) messages (LE_CP-REQ/ LE_CP-RSP).....	33
15	6.1.1	Send-Security-Block message	37
16	6.1.2	ACK-Security-Block message.....	38
17	6.1.3	Neighbor Topology Request message	38
18	6.1.4	Neighbor Topology Reply message.....	39
19	6.1.5	Registration Request message	39
20	6.1.6	Registration Reply message.....	40
21	6.1.7	Registration Update Request message.....	40
22	6.1.8	Registration Update Reply message	40
23	6.1.9	De-registration Request message.....	40
24	6.1.10	De-registration Reply message	40
25	6.1.11	Add Coexistence Neighbor Request message	40
26	6.1.12	Add Coexistence Neighbor Reply message.....	41
27	6.1.13	Update Coexistence Neighbor Request message.....	41

1	6.1.14	Update Coexistence Neighbor Reply message	41
2	6.1.15	Delete Coexistence Neighbor Request message	42
3	6.1.16	Delete Coexistence Neighbor Reply message	42
4	6.1.17	Get_Param_Request message	42
5	6.1.18	Get_Param_Reply message	42
6	6.1.19	Evaluate_Interference_Request message	42
7	6.1.20	Evaluate_Interference_Reply message	43
8	6.1.21	Work_In_Parallel_Request message	43
9	6.1.22	Work_In_Parallel_Reply message	43
10	6.1.23	Quit_Sub_Frame_Request message	43
11	6.1.24	Quit_Sub_Frame_Reply message	43
12	6.1.25	Create_New_Sub_Frame_Request message	43
13	6.1.26	Create_New_Sub_Frame_Request message	44
14	6.1.27	Reduce_Power_Request message	44
15	6.1.28	Reduce_Power_Reply message	44
16	6.1.29	Stop_Operating_Request message	44
17	6.1.30	Stop_Operating_Reply message	44
18	6.2	RADIUS Protocol Messages	44
19	6.2.1	Radius-BS/CIS-Registration-Request (BS/CIS → RADIUS server)	45
20	6.2.2	Radius-BS/CIS-Registration-Accept (RADIUS server → BS/CIS)	46
21	6.2.3	Radius-BS/CIS-Access-Request (BS/CIS → RADIUS server)	47
22	6.2.4	Radius-BS/CIS-Access-Accept (RADIUS server → BS/CIS)	47
23	6.3	Association	48
24	6.4	Sequencing and Retransmission	48
25	6.5	Message Validity Check	49
26	6.6	Fragmentation	49
27	6.7	Transport Protocol	49

1	6.8	Message Format.....	49
2	6.8.1	Header Format.....	50
3	6.8.2	Payload Format.....	50
4	6.9	Using dedicated messages.....	51
5	6.9.1	Common PHY.....	51
6	6.9.2	Between BS and SS.....	51
7	6.9.3	BS to BS.....	51
8	6.9.4	Connection sponsorship.....	51
9	6.9.5	Using a common management system.....	51
10	6.9.6	Higher layers communication.....	51
11	6.9.7	Decentralized control.....	51
12	6.9.8	Information sharing.....	51
13	6.9.9	IP / MAC address dissemination.....	51
14	7	Common policies.....	51
15	7.1	How to select a “free” channel (for ACS and DFS).....	51
16	7.1.1	Acceptable S/(N+I).....	51
17	7.1.2	Acceptable time occupancy.....	51
18	7.1.3	Capability of sharing the spectrum.....	51
19	7.2	Interference reduction policies.....	51
20	7.2.1	BS synchronization.....	51
21	7.2.1.1	GPS.....	51
22	7.2.1.2	Ad-hoc.....	51
23	7.2.2	Shared Radio Resource Management.....	51
24	7.2.2.1	Fairness criteria.....	51
25	7.2.2.2	Distributed scheduling.....	57
26	7.2.2.3	Distributed power control.....	57
27	7.2.2.4	Distributed bandwidth control.....	57

1	7.2.2.5 Beam-forming.....	57
---	---------------------------	----

2
3

4 List of Figures

5

6	Figure 1 Sub-frame structure type1	12
7	Figure 2 Sub-frame structure type 2.....	12
8	Figure 3 Sub-frame structure type 3.....	13
9	Figure 4 Allocation of for BS and SS radio signature.....	15
10	Figure 5 System Architecture.....	19
11	Figure 6 Network Architecture.....	20
12	Figure 7 802.16h BS Protocol architecture Model.....	22
13	Figure 8 LE BS architecture with Coexistence Protocol.....	22
14	Figure 9 CIS architecture with co-located regional LE database	23
15	Figure 10 802.16 LE Neighbor BSs discovery and definition of neighbor and community	27
16	Figure 11 Initialization procedures — BS.....	29
17	Figure 12 General architecture of inter-network communication across 802.16 LE systems	30
18	Figure 13 RADIUS protocol example – between BS and RADIUS server	31
19	Figure 14 Interference due to overlapping networks.....	53
20	Figure 15 Equal splitting of radio resource between networks	53
21	Figure 16 Usage of the spectrum by every system.....	54
22	Figure 17 Sharing same MAC frame.....	55
23	Figure 18 Sharing same MAC frame – alternative mode	55
24	Figure 19 Repetitive scheduling.....	56

25

26

27 List of Tables

28

29	Table 1 LE_CP MAC messages.....	34
30	Table 2 LE_CP request (CP-REQ) message format.....	34

1	Table 3 LE_CP response (CP-RSP) message format	34
2	Table 4 LE_CP message codes.....	36
3	Table 5 TLV types for CP payload.....	37
4	Table 6 Send-Security-Block message attribute.....	38
5	Table 7 ACK-Security-Block message attributes.....	38
6	Table 8 Neighbor Topology Request message attribute.....	39
7	Table 9 Registration Request message attributes	39
8	Table 10 De-registration Request message attributes.....	40
9	Table 11 Add Coexistence Neighbor Request message attributes	41
10	Table 12 Update Coexistence Neighbor Request message attributes.....	41
11	Table 13 Delete Coexistence Neighbor Request message attrubutes	42
12	Table 14 Table RADIUS-BS/CIS-Registration-Access-Request.....	45
13	Table 15 ESP Transform identifiers.....	45
14	Table 16 ESP Authentication algorithm identifiers.....	46
15	Table 17 RADIUS-BS/CIS-Registration-Access-Accept	46
16	Table 18 RADIUS-BS/CIS- Access-Request.....	47
17	Table 19 RADIUS-BS/CIS- Access-Accept	47
18	Table 20 Information elements in the Originating-BS-Security-Block.....	48
19		
20		

1 2.1.1 Operational Principles

2 2.1.1.1 General Principles

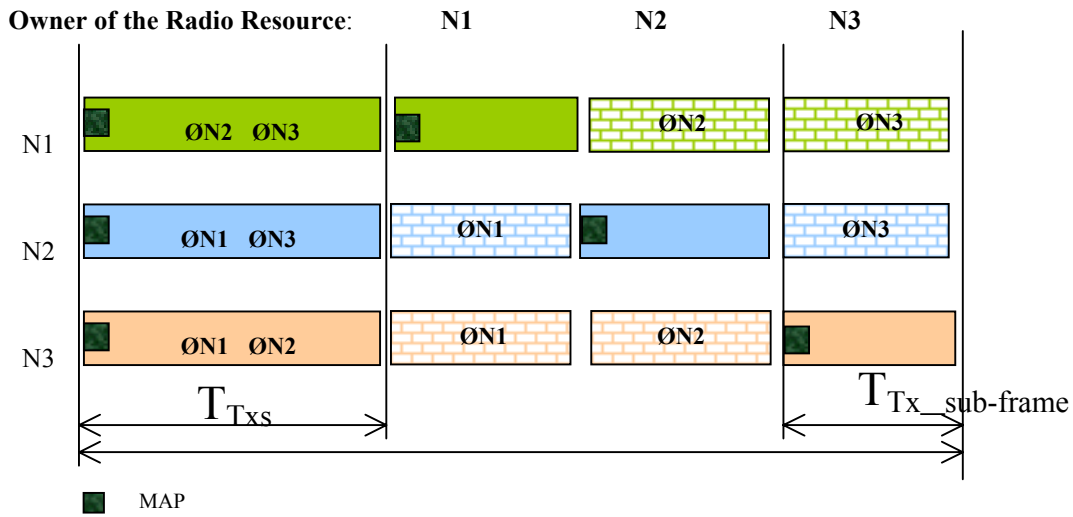
3 A possibility of 802.16h usage is in close relation with a database, including both deployment information
4 and an IP identifier for allowing the operation of a technology-independent coexistence approach. It is
5 assumed that:

- 6 • There is country/region data base, which includes, for every Base Station:
 - 7 ○ *Operator ID*
 - 8 ○ *Base Station ID*
 - 9 ○ *Base Station GPS coordinates*
 - 10 ○ *IP identifier*
- 11 • There is a Server that manage the write/reading of this Data Base, using the 802.16h standardized
12 procedures;
- 13 • Every Base Station includes a data base, open for any other Base Station; the BS data-base
14 contains information necessary for spectrum sharing, and includes the information related to the
15 Base station itself and the associated SSs; a Base Station and the associated SSs form a System.
16 Other Base Stations can send queries related to the information in the database to the DRRM
17 entity;
- 18 • The access to Data Bases is secured by authentication and possibly encryption
- 19 • A community of BSs is formed in an ad-hoc mode; in this community are included Base Stations,
20 if at least two of the Base Stations interfere; every Base Station maintains the list of the Base
21 Stations forming the community. Supplementary, when using the IP-based communication
22 approach:
 - 23 ○ An SS will not communicate directly with a foreign BS;
 - 24 ○ It is no need to register the SS location.
- 25 • All the Base Stations forming a community will have synchronized MAC frames
- 26 • A community will be limited to a reasonable size; the size limitations and interactions between
27 different neighborhoods: t.b.d. in further meetings
- 28 • For every community of Base Stations is created a repetitive pattern, based on one of the
29 following possibilities, mentioned in 802.16h Working Document, chapt. 7.2.2.1.3.2:
 - 30 ○ *Type 1 (par. 7.2.2.1.3.2.1)*: The MAC frame, for each Tx and Rx part, is split in N+1
31 sub-frames:
 - 32 ▪ One for non-interfering traffic
 - 33 ▪ Every other one to be used by a single BS or more non-interfering BSs which
34 are assuming the Master role
 - 35 ○ *Type 2 (par. 7.2.2.1.3.2.2)*: The MAC frame, for each Tx and Rx part, is split in N sub-
36 frames, every one to be used by a single BS or more non-interfering BSs which are
37 assuming the Master role during a sub-frame
 - 38 ○ *Type 3: (par. 7.2.2.1.3.2.3)* The MAC frame is split in two sub-frames: one for non-
39 interfering traffic and one in which a single BS or more non-interfering BSs are
40 assuming the Master role; each Base Station will assume the Master role after M frames

41 The duration of each sub-frame, in a given community, is calculated (here down are some of
42 possible relations and corresponding MAC frames notation):

- 43 • for type 1:
 - 44 ○ $T_{Tx_sub-frame} = T_{TxMAC} / (N+1)$
 - 45 ○ $T_{Tx_sub-frame} = (T_{TxMAC} - T_{Txsh}) / N$
 - 46 ○ $T_{Rx_sub-frame} = T_{RxMAC} / (N+1)$
 - 47 ○ $T_{Rx_sub-frame} = (T_{RxMAC} - T_{Rxsh}) / N$

48



1

2

Figure 1 Sub-frame structure type1

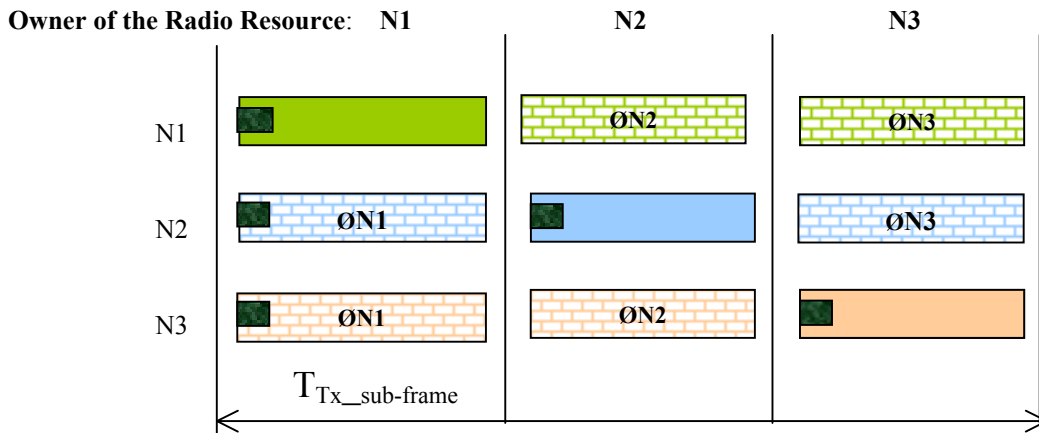
3

4

5

6

- for type 2:
 - $T_{Tx_sub-frame} = T_{TxMAC} / N$
 - $T_{Rx_sub-frame} = T_{RxMAC} / N$



7

8

Figure 2 Sub-frame structure type 2

9

10

11

12

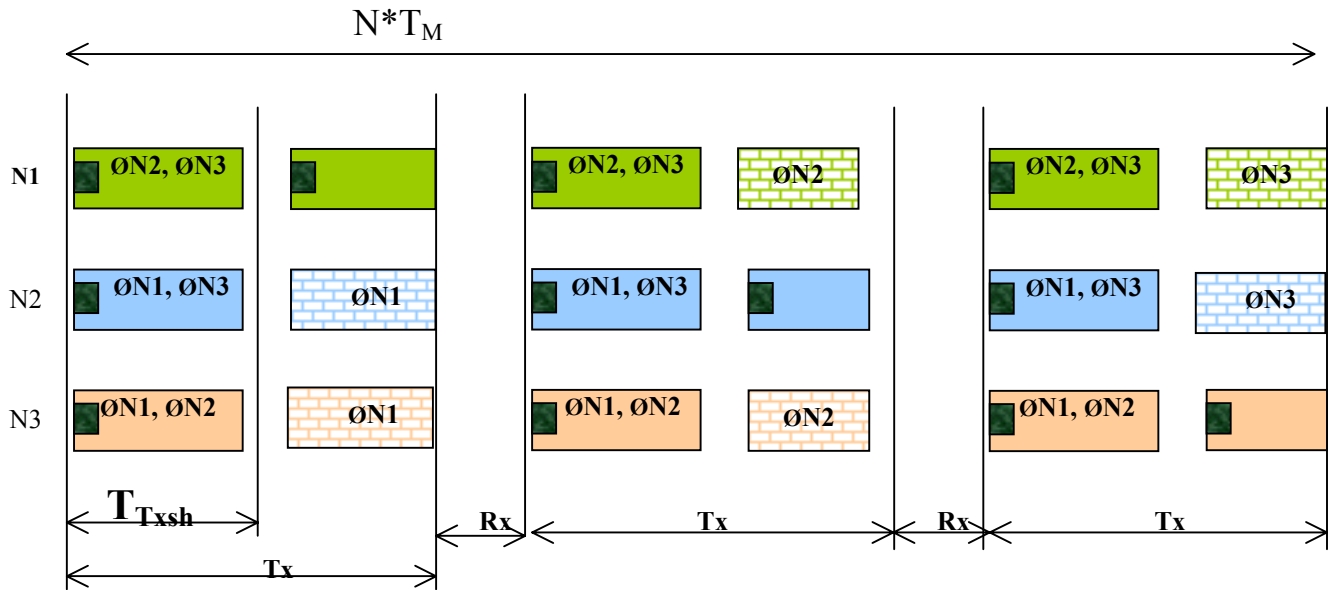
13

14

15

- for type 3:
 - $T_{Tx_sub-frame} = T_{TxMAC} / 2$
 - $T_{Tx_sub-frame} = T_{TxMAC} - T_{Txsh}$
 - $T_{Rx_sub-frame} = T_{RxMAC} / 2$
 - $T_{Rx_sub-frame} = T_{RxMAC} - T_{Rxsh}$
 - repetition interval = $N * T_{MAC}$

1



2
3

4

Figure 3 Sub-frame structure type 3

5 where T_{MAC} , T_{TxMAC} , T_{RxMAC} , T_{Txsh} , T_{Rxsh} are the durations of the respectively the MAC frame, Tx interval
6 and Rx interval of the MAC frame or of the sub-frame used for shared used in the non-interfering sub-
7 frame. In the above relations, the meaning of Tx or Rx is relative to the usage of the MAC Frame by a Base
8 Station.

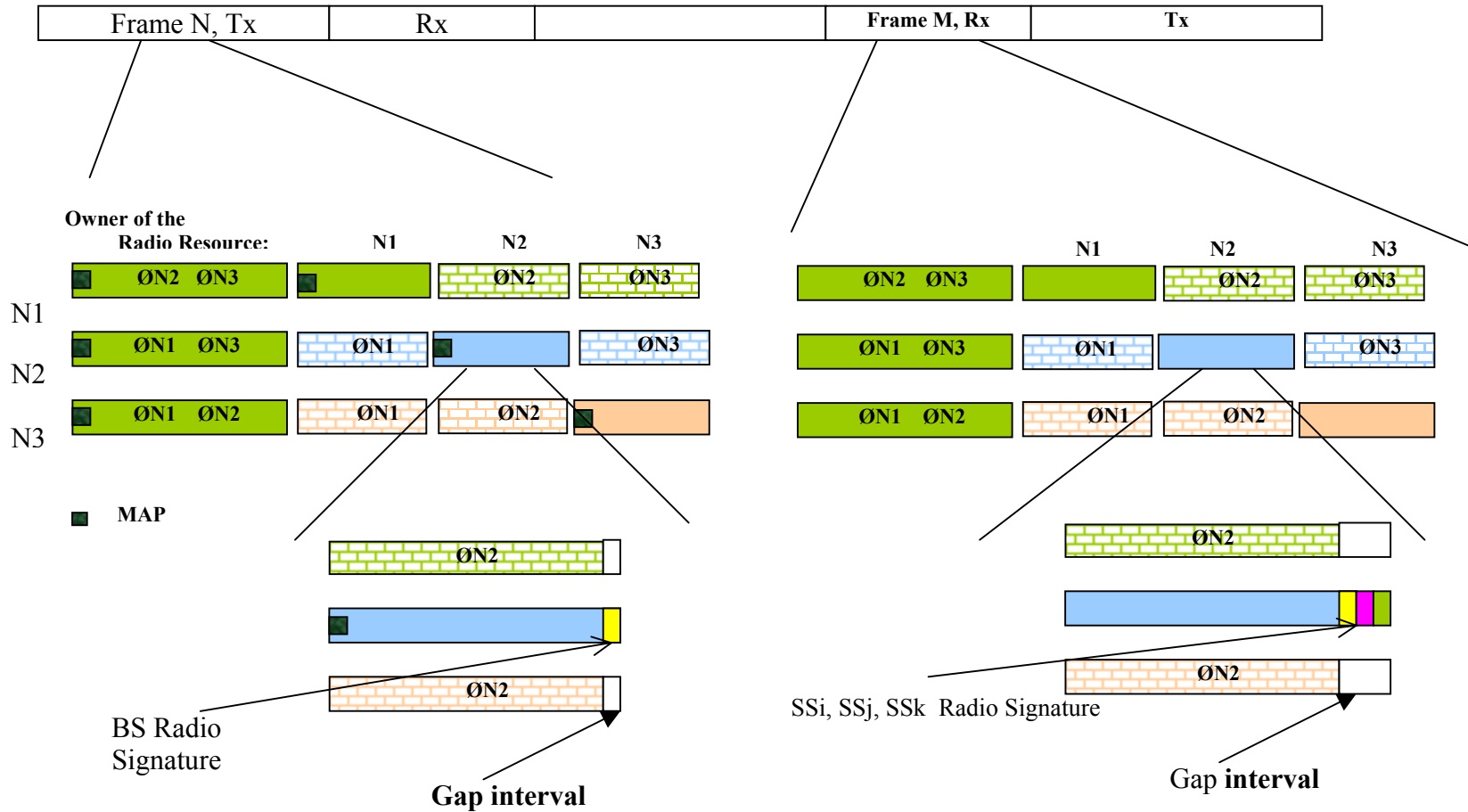
- 9
- During the Master sub-frame the Base Stations assuming Master role may use their maximum
10 power
 - During every Master sub-frame, the Base Stations will create a slot, possibly not overlapping with
11 another slot of a neighbor Base Station, during each every transmitter (BS or associated SS) will
12 send a predefined signal; this signal, called “radio signature”, will be used to measure the
13 interference created by that transmitter.
14
 - The “radio signature slot” for a Base Station will be created during its Tx Master sub-
15 frame, every B MAC-frames;
 - The “radio signature slot” for a Subscriber Station will be created during the Rx Master
16 sub-frame;
 - *UL MAP and suitable UIUC for scheduling the “radio signature” shall be defined.*
17
18
19

20 The figure below shows the possible allocation of the “radio signature” transmission opportunity for a
21 given system, using for example the Type 1 repetitive pattern, with a focus on Network 2.

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

28 The transmission of “radio-signatures” used by the active SSs will take place during the Master sub-frame,
29 from time to time (a timer shall be defined). The repetition period and the duration of the signature

- 1 transmission shall be a parameter in the BS Data Base. The active SSs will provide a signature for every
- 2 used power/OFDMA/sub-channelization/ direction partition.
- 3 The Base Station shall take care to provide enough transmit opportunities for the active SSs.
- 4 During “radio signature” intervals, all the other BSs and SSs shall use a GAP interval.



1

2

Figure 4 Allocation of for BS and SS radio signature

- 1 • The BS data base will include:
 - 2 ○ *Operator ID*
 - 3 ○ *Base Station ID*
 - 4 ○ *MAC Frame duration (same for a community)*
 - 5 ○ *Shared Tx and Rx sub-frame durations (same for a community)*
 - 6 ○ *Type of sub-frame allocation (same for a community)*
 - 7 ○ *MAC Frame number and sub-frame number chosen for the Master sub-frame (same for a*
 - 8 *community)*
 - 9 ○ *Repetition period for Base Station radio-signature, measured in MAC-frames*
 - 10 ○ *Repetition interval between two Master sub-frames, measured in MAC-frames*
 - 11 ○ *List of other used sub-frames, in the interval between two Master sub-frames*
 - 12 ○ *Time_shift from the Master sub-frame start, duration and the repetition information for*
 - 13 *the Base Station radio-signature transmission*
 - 14 ○ *Time_shift from the Master sub-frame start, duration and the repetition information for*
 - 15 *the Subscriber Station radio-signature transmission*
 - 16 ○ *Time_shift from the Master sub-frame start and duration for network entry of a new*
 - 17 *Base Station, which is evaluating the possibility of using the same Master slot.*

18 2.1.1.2 Interference Control

- 19 • Interferer identifier
 - 20 ○ A receiver will listen to the media and will find out which are the strongest interferers; by
 - 21 scanning the BS data bases will be possible to identify, due to the knowledge of the
 - 22 frame number, sub-frame number and offset, to which BS is the interferer associated;
 - 23 based on time-shift information, the Base Station will be able to identify the Subscriber
 - 24 Station ID. During the allocated radio-signature transmit opportunity no other radio
 - 25 transmitters will operate.
- 26 • Interference reduction
 - 27 ○ A BS has the right to *request an interferer to reduce its power by P dB*, for transmissions
 - 28 during the time in which a Base Station is a Master; if the requested transmitter cannot
 - 29 execute the request, it has to cease the operation during the Master sub-frame of the
 - 30 requesting Base Station; this applies also for systems using the sub-frame as a Master
- 31 • Sharing the Master time
 - 32 ○ A Base Station will indicate in the data base *what portion of the sub-frame time,*
 - 33 *separately for Tx and Rx, is actually used*
 - 34 ○ Other systems, which do not interfere one with each other, may use that time interval
- 35 • Target acceptable interference levels during Master sub-frames:
 - 36 ○ For the Base Station and its SS, using the Master sub-frame: min. 14dB above the noise +
 - 37 interference level (16QAM 1/2 (*note: we should define the interference criteria; the*
 - 38 *existing one may be too stringent and not necessary for short links*))

39 2.1.1.3 Community Entry of new BS

- 40 • The first phase of the Community Entry process uses the country/region (FCC) data base:
 - 41 ○ *Read the Regional/country (FCC) data base;*
 - 42 ○ Identify which Base Stations might create interference, based on the location
 - 43 information;
 - 44 ○ Learn the IP identifier for those Base Stations;
- 45 • Build the local image of the relevant information in the community BS's, *by copying the info in*
- 46 *those BSs*
- 47 • Listen on multiple frequencies
 - 48 ○ Identify the level of interference on each frequency channel;
- 49 • Decide the working frequency (ACS – Adaptive Channel Selection process);
- 50 • If available, select an interference-free Master sub-frame; if not, use the procedure for creating
- 51 new Master sub-frames;
- 52 • Search the Base Station data base for finding the BSs using the selected Master sub-frame;

- 1 • *Request those Base Stations, by sending IP unicast messages, to listen during the BS_entry slot in*
 2 *order to evaluate the interference from the new Base Station;*
 3 • *Use the allocated slots for transmitting the “radio signature” at maximum power, maximum power*
 4 *density and in all the used directions;*
 5 • *Ask for permission of the Base Stations, using the sub-frame as Masters, to operate in parallel and*
 6 *use the same sub-frames;*
 7 • *If all of them acknowledge, the Base Station acquires a “temporary community entry” status; the*
 8 *final status will be achieved after admission of the SSs;*
 9 • *If no free Master slot sub-frame is found, use the procedure for creating new Master slot sub-*
 10 *frames.*

11 **2.1.1.4 Network and Community Entry for SS**

- 12 ○ *Start listening;*
 13 ○ *Determine interference intervals;*
 14 ○ *Assume that the interference is reciprocal;*
 15 ○ *Build database for possible working slots and sub-frames;*
 16 ○ *Wait for the Base Station community entry and start of operation;*
 17 ○ *At BS request, send a list of the above identified time intervals;*
 18 ○ *If an old Base Station will perceive interference from the new SSs, it will ask the new*
 19 *Base Station to find another sub-frame for operation;*
 20 ○ *If the SS will sense interference, will request their Base Station to find another sub-frame*
 21 *for operation as Master.*

22 **2.1.1.5 BS regular operation**

- 23 ○ *Schedule SS traffic;*
 24 ○ *Set Tx power levels, such to use minimum power levels for both BS and SSs;*
 25 ○ *Maintain it own database when other BSs join the network.*

26 **2.1.1.6 Operational dynamic changes**

27 **2.1.1.6.1 Creation of a new sub-frame**

28 If none sub-frame can be used, a *new Base Station may request the addition of another sub-frame*. The
 29 effect of such a request will be the reduction of operating time for those Base Stations that interfere with
 30 the new Base Station. However, all the others, that do not interfere one with each other and with the new
 31 one, may work in parallel and use the same operating time.

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

- 33 • *Sending IP messages to all BS members of the community, and indicating:*
 34 ○ *The interfering operator ID and BS ID*
 35 ○ *The MAC frame-number in which the addition of a new sub-frame will take place.*
 36 • *All the requested BSs will acknowledge the request, by*
 37 ○ *Sending back a message having as parameters:*
 38 ▪ *Frame-number for the change (must be the same as the requested one*
 39 ▪ *Master sub-frame number for the new BS (SF = Sfold+1).*
 40 ○ *If are missing acknowledges, those BS will be asked again, for another M attempts, after*
 41 *that will be considered that they are not working;*
 42 ○ *At the above specified MAC frame number, a new sub-frame partition will take place, by*
 43 *inserting in the sub-frame calculation relation:*
 44 ▪ $N=N+1$
 45 ○ *The BSs will up-date the own SSs about the change*
 46 • *Start to use the created Master sub-frame.*

47

1 2.1.1.6.2 Controlling interference during master sub-frame

2

3 2.1.1.6.2.1 Interferer identification

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

- 6 • Peak power
- 7 • Relative spectral density
- 8 • Direction of arrival.

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

11

12 2.1.1.6.2.2 Interference to BS

- 13 ○ Identify the interferers;
- 14 ○ Send messages to interfering BSs, *asking to drop the power of the specified transmitter*
15 *by P dB;*
- 16 ○ Alternatively, send messages to related BSs, *asking to stop operating during the BS*
17 *master slot*
 - 18 ○ The requested Base Station has the alternative of looking for another Master
19 slot.
 - 20 ○

21 2.1.1.6.2.3 Interference to SS

- 22 ○ *Report to BS about experienced interference*
 - 23 ○ *List of frame_number, sub-frame, offset*
- 24 ○ BS start process for interference reduction with *feedback from the SS.*

25 2.1.1.7 Coexistence with non-802.16 wireless access systems

26 The above principles are also applicable to non-802.16 systems, like 802.11. During every 802.16 MAC
27 frame, a 802.11 system may find that a sub-frame may be used, due to the low created interference levels.
28 In the case that no operation in parallel is possible, the new system will ask for the creation of a new
29 Master sub-frame. The Coexistence Protocol, working at IP level, will allow the communication between
30 systems using different PHY/MAC standards.

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

32

33 2.1.2 Shared distributed system architecture

34 2.1.2.1 Architecture

35 The architecture for Radio Resource Management in the context of IEEE 802.16h it is a distributed one and
36 allows communication and exchange of parameters between different networks. A network consists from a
37 Base Station and its associated Subscriber Stations.

38 Every Base Station includes a Distributed Radio Resource Management entity, to apply the 802.16h
39 spectrum sharing policies, and a Data Base to store the shared information regarding the actual usage and
40 the intended usage of the Radio Resource.

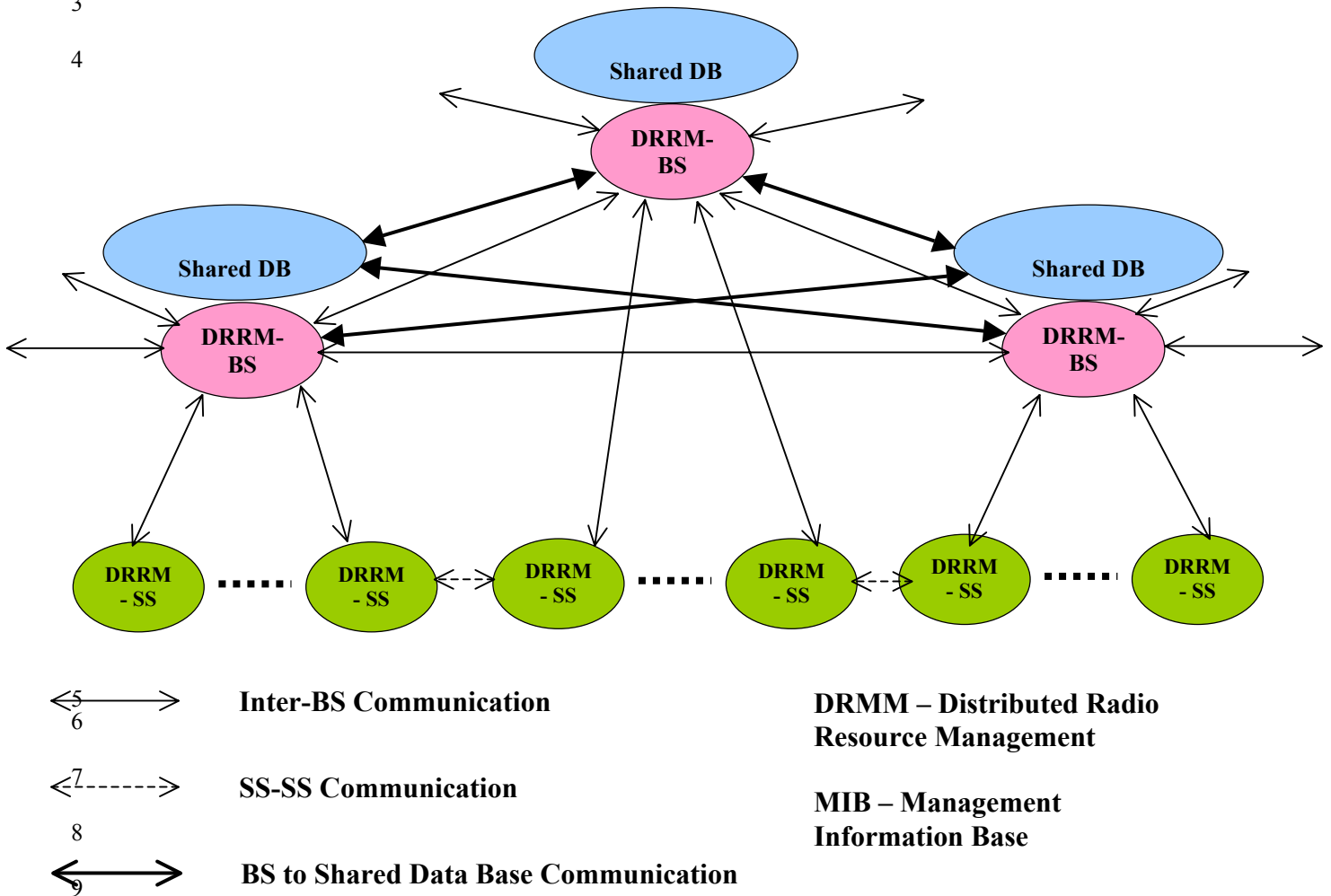
41 A subscriber Station may include an instance of DRRM, adapted to SS functionality in 802.16h context.

1

2 The following figure shows the functional diagram of the IEEE 802.16h network architecture:

3

4



10

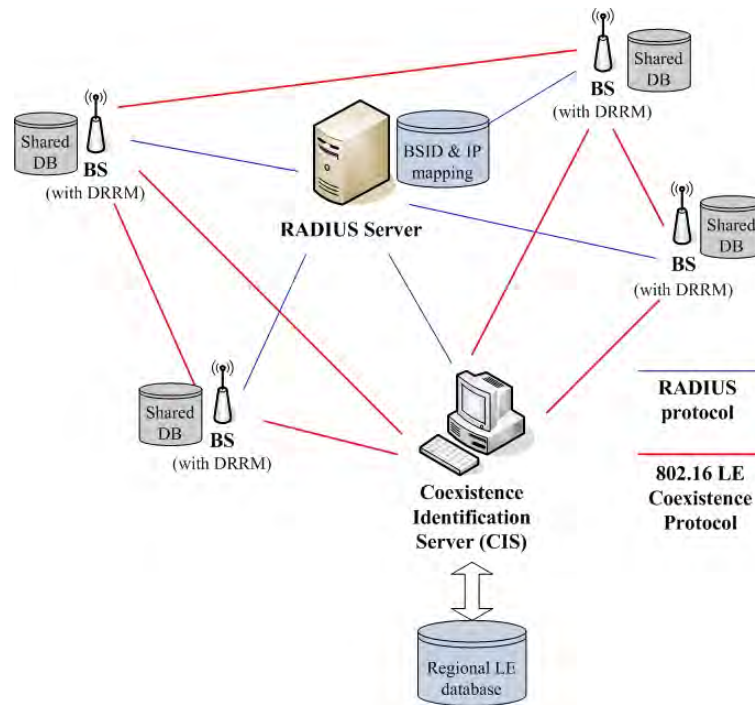
11

Figure 5 System Architecture

12

13 *Note: the security part is a temporary text adopted from contribution C802.16h-05/11r1 and 802.16h is*
 14 *calling for comments*

15 Figure 6 shows the IEEE 802.16 LE inter-network communication architecture:



1

2

Figure 6 Network Architecture

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

4 - The RADIUS Server

5 - The Coexistence Identification Server (CIS) (detail description in section x.x.x)

6 - The BSs cooperating with the Distributed Radio Resource Management (DRRM) procedure

7 RADIUS server performs two primary functions. The first one is to authenticate 802.16 LE BSs and CIS.
 8 Keyed-Hashing for Message Authentication (HMAC) with Message Digest 5 (MD5) (RFC2869:2000) is
 9 adopted for authentication. The second one is to maintain the address mapping of wireless medium
 10 addresses of BSs (their BSID) and medium addresses of CIS to their IP addresses. This mapping is to
 11 distribute the keys for ESP used by BSs belonging to different networks.

12 CIS maintains the geographic and operational information such as latitude, longitude and the BSID of LE
 13 BSs. BSs operating under LE system shall first query the CIS and find the neighbor BSs while starting up,
 14 following the Coexistence Resolution and Negotiation (CRN) protocol (detailed description in section
 15 x.x.x). After the successful query procedure, the BS can obtain the BSIDs of the neighbor BSs.
 16 Intercommunication between BSs belonging to different networks is permitted after the BS acquires
 17 coexisting neighbor's authentication key and encryption key for ESP as well as IP address by querying
 18 RADIUS server.

19 **2.1.2.2 Inter-network communication**

20 The inter-network communication consists in:

21 - Inter-network messages

22 ○ Base Station to/from Base Station

- 1 o Base Station to/from Subscriber Station to/from foreign Base Station; the subscriber
2 Station is used as relay, if the two Base Stations are hidden one from the other
- 3 - Open access to DRRM Data Base:
- 4 o To read the parameters of the hosting Base Station
- 5 o To request change of the hosting Base Station operating parameters.
- 6

7 **2.1.2.2.1 Coexistence Protocol**

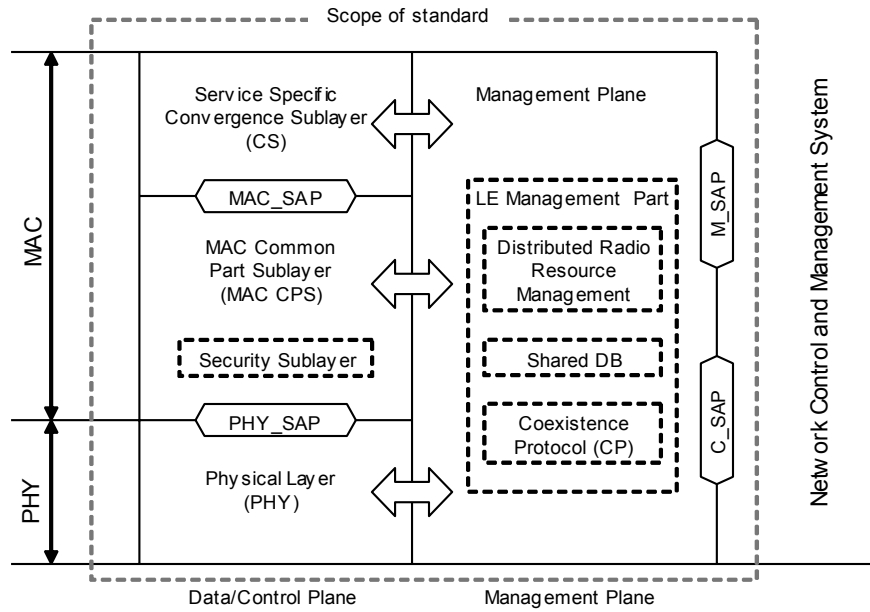
8 *Note: the security part is a temporary text adopted from contribution C802.16h-05/11r1 and is subject to*
9 *further discussion.*

10 In order to get the neighbor topology, perform registration to the database and registration to peer,
11 negotiation for Shared RRM etc. we propose a Coexistence Protocol (CP). Figure 7 reveals the 802.16h
12 protocol architecture. The protocol architecture indicates that DRRM, Coexistence Protocol and Shared DB
13 belong to LE Management Part located in management plane and the messages will be exchanged over IP
14 network. Thus, DRRM in LE Management Part uses the Coexistence protocol to communicate with other
15 BSs and with Regional LE DB and interact with MAC or PHY. Figure 8 is LE BS architecture with
16 Coexistence Protocol. The gray area indicates area where there is an absence of connection between
17 blocks. DSM is Distribution System Medium which is another interface to the backbone network. Note that
18 this architecture is only for reference. Similarly, Figure 9 is the CIS architecture with co-located regional LE
19 database. Other architectures are not being illustrated. The Coexistence Protocol services are accessed by
20 the LE Management Entity through CP SAP. But the service primitives will not be provided in this
21 contribution due to the Coexistence Protocol is incomplete at this stage. This proposal only provides the
22 definition of PDUs exchanged between peer Coexistence Protocol entities. A BS uses the Coexistence
23 Protocol, which is similar to PKM protocol, to perform the coexistence resolution and negotiation
24 procedures. There are two types of messages to support Coexistence Protocol:

25 (1) LE_CP-REQ: BS→BS or BS→CIS

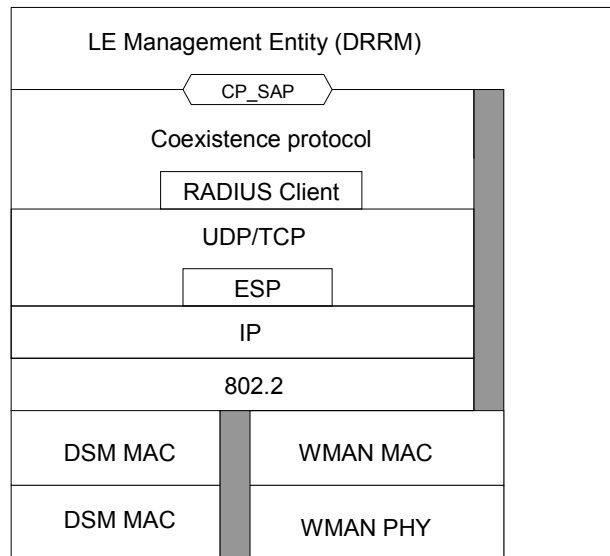
26 (2) LE_CP-RSP: BS→BS or CIS→BS

27



1
2

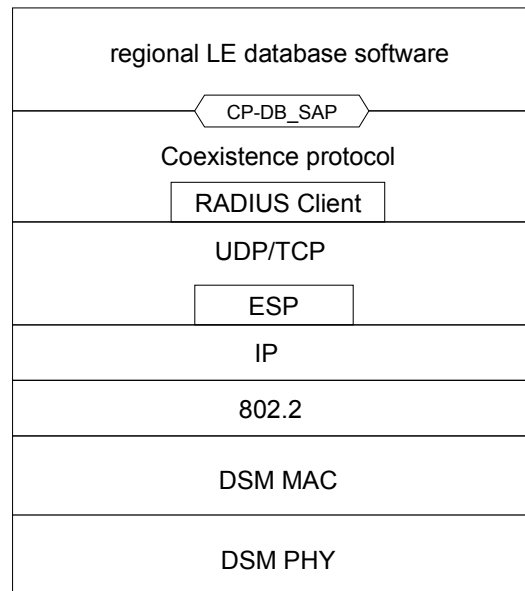
Figure 7 802.16h BS Protocol architecture Model



3
4

Figure 8 LE BS architecture with Coexistence Protocol

1



2

3 **Figure 9 CIS architecture with co-located regional LE database**

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

6 Before any data can be exchanged between BS and BS/CIS, security association must be setup first. IEEE
 7 802.16 LE security associations between peers are established through RADIUS server. Any BS wants to
 8 communicate with another BS or CIS shall first send a *RADIUS Access-Request* to request the
 9 establishment of the security association between originated BS and terminated BS/CIS. RADIUS server
 10 replies a *RADIUS Access-Accept*, which includes security information for ESP operation, to the BS. At this
 11 point, only *virtual* security association is established between the peers. The BS sends the Security Block
 12 for the peer, which it received from the RADIUS Server, as a LE_CP-REQ packet with message type *Send-*
 13 *Security-Block*. This is the first message in the Coexistence Protocol TCP exchange between the BS and
 14 BS or BS and CIS. The peer returns LE_CP-RSP packet with message type *Send-Security-Block*. At this
 15 point both sides have the information to encrypt all further packets for this exchange between the BS and
 16 BS or BS and CIS.

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

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

21

1 **2.1.2.2.2 Same PHY Profile**

2 For networks using the same 802.16 PHY Profile, including elements as:

- 3 - Channel spacing;
- 4 - PHY mode:
- 5 ○ WirelessMAN-OFDM (256 FFT points)
 - 6 ○ WirelessMAN OFDMA 2k (in future 128, 512, 1k) FFT points
 - 7 ○ WirelessMAN SCa,

8 the inter-network communication may be done using 802.16 messages over the air, including messages
9 defined by 802.16h amendment.

10 **2.1.2.2.3 Mixed-PHY Profile communication**

11 In the case of different PHY Profiles the communication will be done at IP Level. Every Base Station
12 should know the IP address of the DRRM of the Base Stations around, by provisioning or/and by a
13 transmitting the IP address over-the-air. The communication shall use a real-time communication protocol
14 – t.b.d.

15 Every system will:

- 16 - Broadcast the IP address of its Data Base entity, such that more elaborated inter-system
17 communication may take place using unicast IP messages;
- 18 - Multicast to neighbor Base Stations the basic information related to the parameters of the spectrum
19 usage, in such a way that any other system, which co-exists in the same area, will be aware of the
20 parameters of shared spectrum usage;
- 21 - The Base Station will forward to the associated SSs the information related to DRRM.

1 **3 Interference victims and sources**

2 **3.1 Identification of the interference situations**

3 **3.1.1 Interferer identification**

4 **3.1.2 Grouping of interfering/not-interfering units**

5 **3.2 Identification of spectrum sharers**

6 **3.2.1 Regulations**

7 **3.2.2 Messages to disseminate the information**

8 **3.2.3 Avoid false-identification situations**

9 **3.2.4 Storage of identification information**

10 **3.2.4.1 Regional LE database**

11 *Regional LE database (LE DB)* is primary for facilitating the coexistence detection, avoidance and
12 resolution. There is country/region database, which includes, for every Base Station:

- 13 1. Operator ID
- 14 2. Base Station ID
- 15 3. Base Station GPS coordinates
- 16 4. IP address (TBD)

17 Every Base Station also includes a database, called *Shared DB*, open for any other Base Station. The BS
18 data-base contains information necessary for spectrum sharing, and includes the information related to the
19 Base station itself and the associated SSs. A Base Station and the associated SSs form a System. Other
20 Base Stations can send queries related to the information in the Shared DB to the DRRM entity.

21 The BS Shared DB includes:

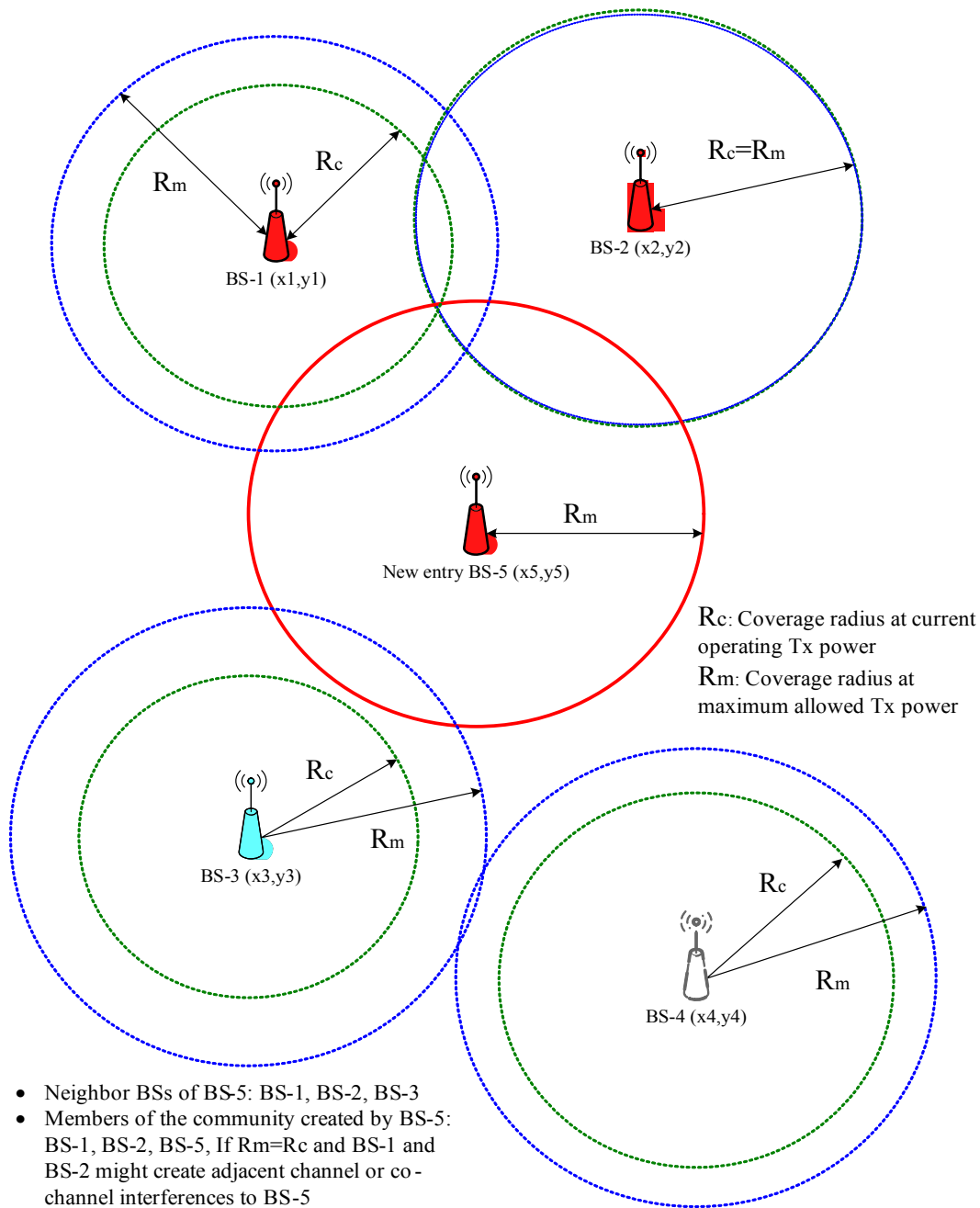
- 22 1. Operator ID
- 23 2. Base Station ID
- 24 3. MAC Frame duration
- 25 4. Frame and sub-frame number chosen for the Master sub-frame
- 26 5. Repetition interval between two Master sub-frames, measured in MAC-frames
- 27 6. List of other used sub-frames, in the interval between two Master sub-frames
- 28 7. Time_shift from the Master sub-frame start, when a transmitter will transmit its
29 radio signature
- 30 8. Slot position for network entry of a new Base Station, which is evaluating the
31 possibility of using the same Master slot

32 The LE BSs can, therefore, have knowledge about the possible interferers such as coexisting BSs and SSs
33 from neighbor BSs by querying the regional LE DB with its geographic position as well as by querying the
34 Shared DBs of its neighbors. Another functionality of the regional LE DB is to deliver the BSIDs of
35 neighbor BSs to the BS who looks up its neighbors in secure manner. As opposed to broadcast IP address
36 over the air, one LE BS uses BSIDs acquired from LE DB to request the corresponding IP addresses by
37 utilizing Remote Authentication Dial-in User Service (RADIUS) protocol.

1 Figure 10 explains how one new entry BS discovers its neighbor BSs. The new entry BS-5 uses its GPS
2 coordinates (x_5, y_5) and its maximum coverage radius, R_m , at allowed maximum transmission power to
3 query the LE DB. A BS is neighbor BS of another BS means their maximum coverages at allowed
4 maximum transmission power overlaps. As Figure 10 depicted, the regional LE DB will return BS-1, BS-2
5 and BS-3 as the neighbor BSs of the new entry BS.

6 Once a LE BS has learnt its neighbor topology from the regional LE DB, it evaluates the coexisting LE
7 BSs and identifies which BSs might create interferences. While it decides its working frequency after
8 scanning, the *community* to which the LE BS belongs is determined. Each LE BS tries to form its own
9 community. The members of community come from the neighbor BSs of one BS, i.e. the members of
10 community are the subset of neighbor BSs. Those neighbor BSs that might create interferences to the BS or
11 to the associated SSs under current working frequency are the members of its own community. For
12 example, BS-1 and BS-2 are the members of the community create by BS-5 if $R_m = R_c$ and BS-1 and BS-2
13 might create adjacent channel or co-channel interferences to BS-5. One BS creates and maintains one
14 community of it at the same time. The members of community will change when its working frequency
15 changes or new interfering neighbor BS comes in. Every BS maintains the list of the member BSs forming
16 the community. An SS will not communicate directly with a foreign BS and there is no need to register the
17 SS location. All the Base Stations forming a community will have synchronized MAC frames.

18



1

2 Figure 10 802.16 LE Neighbor BSs discovery and definition of neighbor
3 and community

4

5 In summary, with the regional LE DB a LE BS can construct its neighbor topology and
6 acquire the IP addresses of its neighbor securely. With the neighbor topology and
7 corresponding IP addresses, the coexistence detection, avoidance and resolution is easier.
8 In general, the coexistence detection, avoidance and resolution are performed in two
9 stages, initialization stage and operating stage.

1 (1) *Initialization stage*

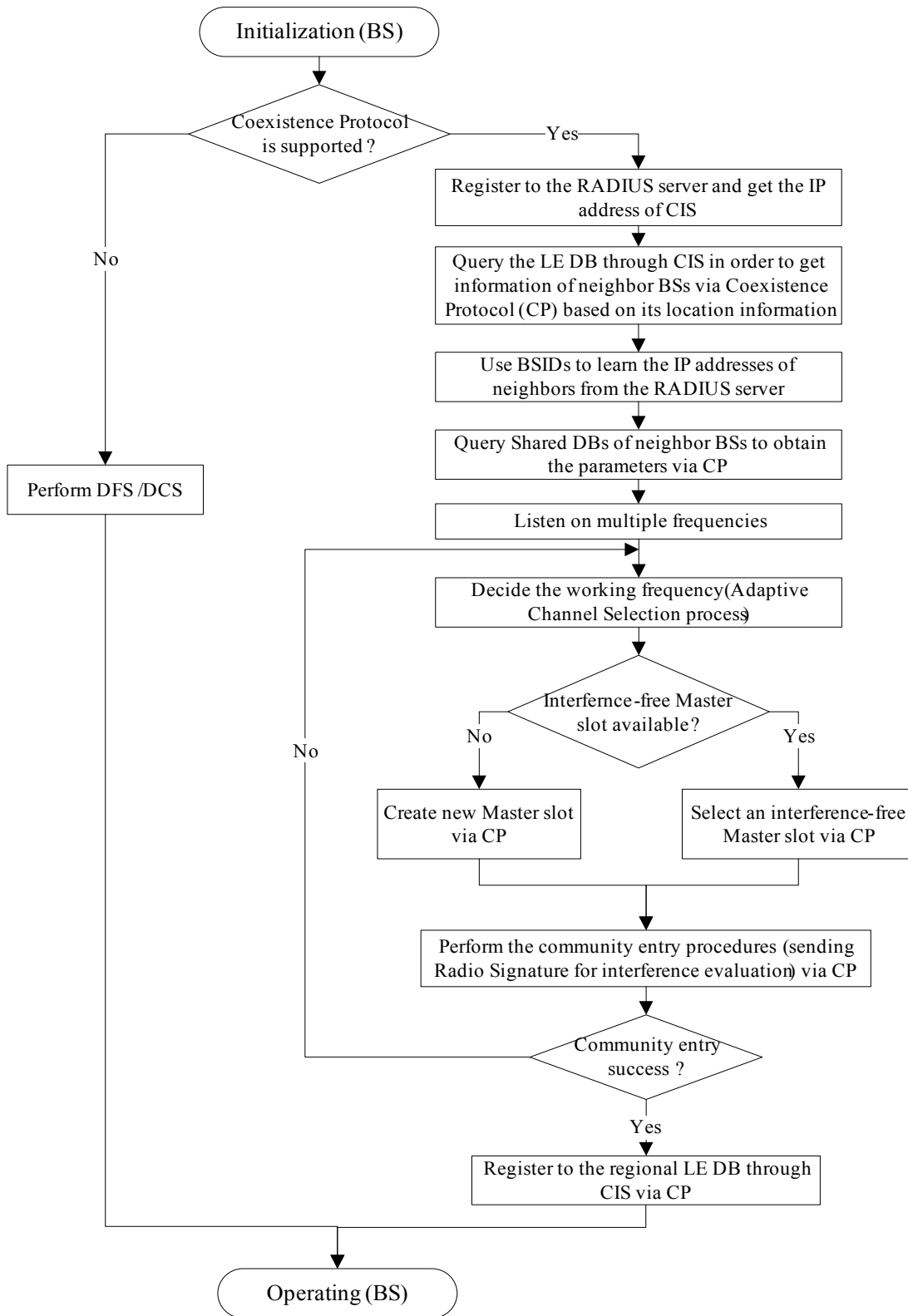
2 In initialization stage the LE BSs may avoid the co-channel or adjacent channel interference by scanning
3 the available frequencies. But this method cannot avoid the *hidden* LE BS problem, i.e. the BS that cannot
4 be heard directly but may have overlapping service coverage. Thus, with the knowledge of neighbor
5 topology the LE BSs can detect the *hidden* LE BSs and can, therefore, avoid the possible interferences
6 from coexisting neighbors. The procedures are described in Figure 11. If the LE BS finds that there is no
7 “free” channel, the neighbor topology provides the guidelines of with whom it should negotiate.

8

9 (2) *Operating stage*

10 In operating stage the LE BS has SS associated with it, however, even the operating system parameters has
11 decided, the co-channel or adjacent channel interference from LE BSs of different network may still have a
12 chance to happen due to the detection of interference from primary user, channel switching of neighbor BS
13 or the entry of new neighbor BS makes the community so crowded that there is no enough channels. If the
14 LE BS finds that there is no “free” channel at that moment, the neighbor topology provides the guidelines
15 of with whom it should negotiate. [detailed procedures are to be defined]

16 Figure 11 shows the proposed initialization procedures for the 802.16 LE BSs. Note that the procedures
17 that BS tries to create a Master slot are also applicable for operating stage. The detailed negotiation and
18 update procedures are described in section 2.1.2.2.1.



1

2

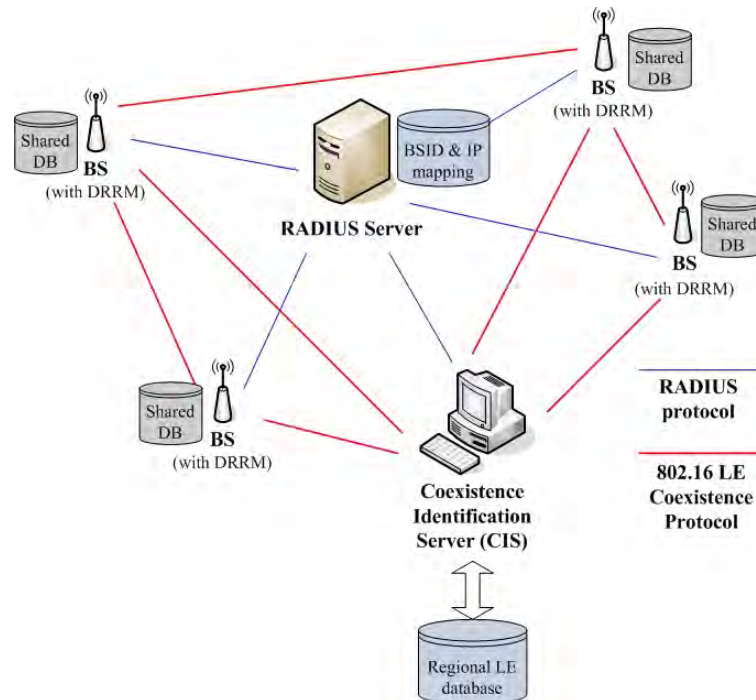
Figure 11 Initialization procedures — BS

1 3.2.4.2 Coexistence Identification Server

2 *[Note: The following part from 3.2.4.2 is a temporary text adopted from contribution C802.16h-*
 3 *05/11r1 and is subject to further discussion. A call for comment from security experts is open to*
 4 *comment on this text.]*

5 The coexistence resolution will rely on a regional LE DB but there should be an entity between the LE BSs
 6 and the regional LE DB in order to let the coexistence resolution processes to be independent of the
 7 database technologies. Therefore, we propose an entity named *Coexistence Identification Server* (CIS) acts
 8 as an interface between 802.16 LE BSs and the regional LE DB which stores the geographic and important
 9 operational information, e.g. latitude, longitude, BSID etc., of the LE BSs belonging to the same region. It
 10 converts the actions carried in PDUs received from the 802.16 LE BSs to the proper formats, e.g. SQL
 11 (Structured Query Language) string, and forwards the strings to the regional LE DB, which can be any
 12 available database software. CIS converts the query results from the regional LE DB to the proper format,
 13 e.g. TLV encodings, and replies to the requested BSs. Figure N6 shows the general architecture of inter-
 14 network communication across 802.16 LE systems. In this architecture, the 802.16 LE systems (BSs and
 15 CIS) from different networks set up security association (including BS and BS, BS and CIS) with each
 16 other by utilizing the services provided by the RADIUS server. CIS acts as a peer of 802.16 LE BSs in this
 17 architecture, therefore, it also needs to register to the RADIUS server as the LE BSs do. The MAC address
 18 of CIS is well known among the LE operators. The LE BSs can use the MAC address of CIS, which may
 19 be provisioned, to acquire the IP address and keys for Encapsulating Security Payload (ESP)
 20 (RFC2406:1998) operation of the CIS by utilizing RADIUS protocol. As shown in figure N6, the RADIUS
 21 server maintains the BSID and IP mapping. In summary, ESP with RADIUS can discover a Rogue BS or
 22 CIS. The messages exchanged between the LE BSs and the CIS will be revealed in the next section. Note
 23 that the interface between CIS and regional LE DB is out of scope.

24



25

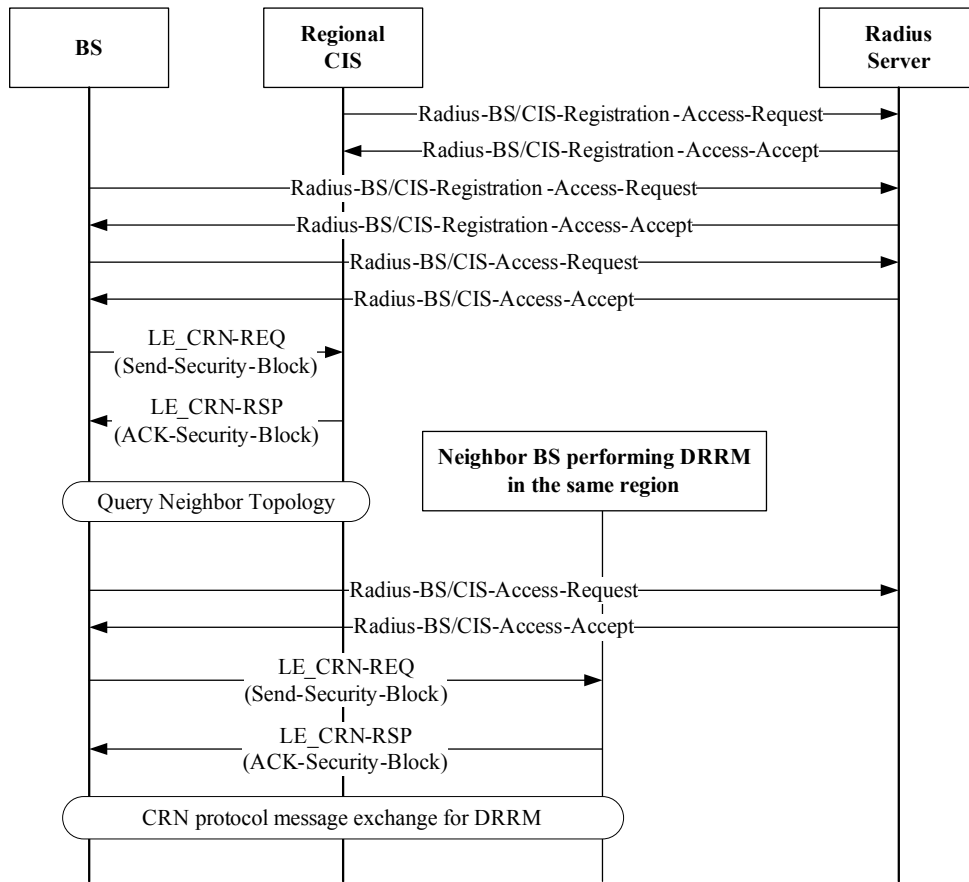
26 Figure 12 General architecture of inter-network communication across 802.16 LE
 27 systems

1 **3.2.4.3 RADIUS Protocol Usage**

2 *[Note: the following part “RADIUS Protocol Usage” is from contribution C802.16-05/012r1 , calling for*
 3 *comments.]*

4 For future interoperability consideration, mechanisms similar to [4] is proposed. Secure exchange of
 5 802.16 LE signaling information can be achieved after successful procedures of the RADIUS protocol. To
 6 include RADIUS support, the RADIUS server and the BS/CIS RADIUS client must be configured with the
 7 shared secret and with each other’s IP address. Each BS/CIS acts as a RADIUS client and has its own
 8 shared-secret with the RADIUS server. The shared secret may be different from that of any other BS/CIS.

9



10

LE_CRN-REQ and LE_CRN-RSP are 802.16 LE CRN protocol messages (refer to [6])

11

Figure 13 RADIUS protocol example – between BS and RADIUS server

12

13 Figure 13 shows the RADIUS protocol message exchange sequence. At starting up, each BS or CIS must
 14 send a Radius-BS/CIS-Registration-Access-Request (shown in table A1) to the RADIUS server for
 15 authentication purpose and leave the address mapping (BSID to IP) information in the server. At this time,
 16 the RADIUS server will retain the following information of registered BS or CIS:

- 17 (a) Wireless medium address of BS (BSID) or medium address of CIS,
- 18 (b) RADIUS BSID Secret at least 160 bits in length,

- 1 (c) IP address or DNS name, and
2 (d) Cipher suites supported by the BS or CIS for the protection of CRN protocol
3 communications

4 RADIUS BSID Secret is used as decryption key for the security parameters, which will be described later.
5 Same as [4], Microsoft Point-to-Point Encryption (MPPE) (RFC 2548:1999) key is introduced. The MS-
6 MPPE-Send-Key, which could be got in the Radius-BS/CIS-Registration-Access-Accept message (shown
7 in table B), is used for encrypting the security parameters (named as Security Block, shown in table D2) in
8 the accept message. A registration access reject message may be issued due to a BS not supporting the ESP
9 Transform or ESP Authentication algorithm selected for use in securing the following intercommunication,
10 or for other RADIUS configuration reasons not discussed here.

11 Once a BS wants to get the knowledge of neighbor topology, it must first send Radius-BS/CIS-Access-
12 Request message (shown in table C) to the RADIUS server in order to acquire the regional CIS's IP
13 address, and also to deliver the ESP Security Blocks necessary for establishing a secure connection with
14 the CIS. The wireless medium addresses of regional CIS, similar to BSID, well known by all BSs
15 supporting LE operation, is sent in the Radius-BS/CIS-Access-Request message to the RADIUS server for
16 looking up IP address of the CIS. Upon receiving the request message, the RADIUS server will respond
17 with a Radius-BS/CIS-Access-Accept message (shown in table D1) if the CIS is a valid member which is
18 allowed to perform inter-communication.

19 After succeeded query process between the BS and the regional CIS the CIS will respond to the BS with
20 possible neighbor BSs candidates and their BSIDs. The BS, then, tries to establish secure connections with
21 the neighbor BSs after evaluating the coexistence relationships with these candidates. The BS sends
22 Radius-BS/CIS-Access-Request message to the RADIUS server to query the IP address and Security Block
23 for each evaluated neighbor BS.

24 All Security Blocks in the Radius-BS/CIS-Access-Accept messages is authenticated using the ESP
25 authentication algorithm (indicated from the previous Radius-BS/CIS-Registration-Access-Accept
26 messages) and encrypted/decrypted using the ESP transform cipher (also indicated from the previous
27 Radius-BS/CIS-Registration-Access-Accept messages) with RADIUS BSID secret as the decryption key.
28 The key used is extracted from the RADIUS BSID secret by using HMAC with Secure Hash Algorithm 1
29 (SHA1), known as HMAC-SHA-1 (RFC2404:1998), and is shown in the following method.

30 $\text{secret1} = \text{HMAC-SHA1}(\text{null}, \text{secret})$
31 $\text{secret2} = \text{HMAC-SHA1}(\text{null}, \text{secret} \parallel \text{secret1})$
32 $\text{secret3} = \text{HMAC-SHA1}(\text{null}, \text{secret} \parallel \text{secret2})$
33 ...
34 ...
35 $\text{secretN} = \text{HMAC-SHA1}(\text{null}, \text{secret} \parallel \text{secretN-1})$
36 $\text{key} = \text{secret1} \parallel \text{secret2} \parallel \text{secret3} \parallel \dots \parallel \text{secretN}$

37 The transform key is the first N bits and the authentication key is the next M bits (the value of N and M are
38 dependent on the cipher suite). The security association (SA) then is created from the information carried
39 in the Security Block. The Security Block contains the ESP transform key and ESP authentication key used
40 for securing CRN protocol message exchange between BS and CIS, or BS and BS.

41

1 The Radius-BS/CIS-Access-Accept message contains two Security Blocks. One is used for the original
2 requesting BS, and the other is used for the neighbor BS or regional CIS performing the inter-
3 communication. Therefore, the first CRN protocol message exchanged between them is of the CRN
4 message type “Send-Security-Block” sent by the original requesting BS. The second one is of the type
5 “ACK-Security-Block”, sent by the neighbor BS or regional CIS, indicating the correct reception of the
6 security parameters used for the following secure inter-communication.

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

10 **3.2.5 Security consideration** *[Note: to be reviewed by expert on security.]*

11
12 In this model, data traffic is protected by using IPsec.
13 The IP Security Protocol [[IPsec](#)] provides cryptographically based security for IPv4. The
14 protection offered by IPsec is achieved by using one or both of the data protection
15 protocols (AH and ESP). Data protection requirements are defined in the Security Policy
16 Database (SPD). IPsec assumes use of version 2 of the Internet Key Exchange protocol
17 [[IKEv2](#)], but a key and security association (SA) management system with comparable
18 features can be used instead.

19 **4 Interference prevention**

20 **4.1 Adaptive Channel Selection – ACS**

21 **4.1.1 Between 802.16 systems**

22 **4.2 Dynamic Frequency Selection – DFS**

23 **4.2.1 Frequency selection for regulatory compliance**

24 **5 Pro-active cognitive approach**

25 **5.1 Signaling to other systems**

26 **5.2 Recognition of other systems**

27 **6 Transmission of information**

28 **6.1 Coexistence Protocol (CP) messages (LE_CP-REQ/ LE_CP-RSP)**

29 Coexistence Protocol employs two MAC message types: LE CP Request (LE_CP-REQ) and LE CP
30 Response (LE_CP-RSP), as described in Table 1.

1

Table 1 LE_CP MAC messages

Type Value	Message name	Message description
nn	LE_CP-REQ	LE Coexistence Resolution and Negotiation Request [BS -> BS/CIS]
nn	LE_CP-RSP	LE Coexistence Resolution and Negotiation Response [BS/CIS -> BS]

2 These MAC management messages are exchanged between peers, e.g. BS and CIS or BS and BS, and
 3 distinguish between CP requests (BS -> BS/CIS) and CP responses (BS/CIS -> BS). Each message
 4 encapsulates one CP message in the Management Message Payload. Coexistence Protocol messages
 5 exchanged between the BS and BS or between BS and CIS shall use the form shown in Table 2 and
 6 Table 3.

7

Table 2 LE_CP request (CP-REQ) message format

Syntax	Size	Notes
CP-REQ_Message_Format() {		
(Version of protocol in use)	? bits	1 for current version
Management Message Type = nn(Flags???)	8??bits	<i>[The content in () in this table is from the contribution C802.16h-05_009 ,need to be harmonized with C802.16h-05_011r1 in terminology and the bit width. And to be reviewed by expert on security]</i>
Code(opCode???)	8 bits	
(Length of Payload)	??bits	
(AssociationID???)	??bits	
CP Identifier(MessageID???)	8 bits	
TLV Encoded Attributes	variable	TLV specific
}		

8

9

Table 3 LE_CP response (CP-RSP) message format

Syntax	Size	Notes
CP-RSP_Message_Format() {		
(Version of protocol in use)	? bits	1 for current version
Management Message Type = nn(Flags???)	8?? bits	<i>[The content in () in this table is from the contribution C802.16h-05_009 ,need to be harmonized with C802.16h-05_011r1 in terminology and the bit width.And to be reviewed by expert on security.]</i>
Code(opCode???)	8 bits	

(Length of Payload)	??bits	
(AssociationID???)	??bits	
CP Identifier (MessageID???)	8 bits	
Confirmation Code	8 bits	
TLV Encoded Attributes	variable	TLV specific
}		

1

2 The parameters shall be as follows:

3

4 ***Version of protocol in use***5 *This specification of the protocol is version 1.*6 **Code(*opCode*???)**7 The Code is one byte and identifies the type of CP packet. When a packet is received with an invalid
8 Code, it shall be silently discarded. The code values are defined in Table D.9 **Length of payload**10 **CP Identifier(*Message ID*???)**11 The Identifier field is one byte. A BS/CIS uses the identifier to match a BS/CIS response to the BS's
12 requests. The BS shall increment (modulo 256) the Identifier field whenever it issues a new CP message.
13 The retransmission mechanism relies on TCP. The Identifier field in a BS/CIS's CP-RSP message shall
14 match the Identifier field of the CP-REQ message the BS/CIS is responding to.15 ***Association identifier(Association ID)***16 *For uniquely identifying an CP connection between a initiator and responder*17 **Confirmation Code** (see *x.xx*)

18 The appropriate CC for the entire corresponding LE_CP-RSP.

19 **Attributes**

20 CP attributes carry the specific authentication, coexistence resolution, and coexistence negotiation data

21 exchanged between peers. Each CP packet type has its own set of required and optional attributes. Unless
22 explicitly stated, there are no requirements on the ordering of attributes within a CP message. The end of
23 the list of attributes is indicated by the LEN field of the MAC PDU header.

24

1

Table 4 LE_CP message codes

	CP Message type	MAC Message Type	Protocol type	Direction
0	<i>Reserved</i>	—	—	—
1	Send-Security-Block	LE_CP-REQ	TCP	BS->BS/CIS
2	ACK-Security-Block	LE_CP-RSP	TCP	BS/CIS->BS
3	Neighbor Topology Request	LE_CP-REQ	TCP	BS-> CIS
4	Neighbor Topology Reply	LE_CP-RSP	TCP	CIS->BS
5	Registration Request	LE_CP-REQ	TCP	BS-> CIS
6	Registration Reply	LE_CP-RSP	TCP	CIS->BS
7	Registration Update Request	LE_CP-REQ	TCP	BS-> CIS
8	Registration Update Reply	LE_CP-RSP	TCP	CIS->BS
9	De-registration Request	LE_CP-REQ	TCP	BS-> CIS
10	De-registration Reply	LE_CP-RSP	TCP	CIS->BS
11	Add Coexistence Neighbor Request	LE_CP-REQ	TCP	BS->BS
12	Add Coexistence Neighbor Reply	LE_CP-RSP	TCP	BS->BS
13	Update Coexistence Neighbor Request	LE_CP-REQ	TCP	BS->BS
14	Update Coexistence Neighbor Reply	LE_CP-RSP	TCP	BS->BS
15	Delete Coexistence Neighbor Request	LE_CP-REQ	TCP	BS->BS
16	Delete Coexistence Neighbor Reply	LE_CP-RSP	TCP	BS->BS
17	Get Param Request	LE_CP-REQ	UDP	BS->BS
18	Get Param Reply	LE_CP-RSP	UDP	BS->BS
19	Evaluate Interference Request	LE_CP-REQ	UDP	BS->BS
20	Evaluate Interference Reply	LE_CP-RSP	UDP	BS->BS
21	Work In Parallel Request	LE_CP-REQ	UDP	BS->BS
22	Work In Parallel Reply	LE_CP-RSP	UDP	BS->BS
23	Quit Sub Frame Request	LE_CP-REQ	UDP	BS->BS
24	Quit Sub Frame Reply	LE_CP-RSP	UDP	BS->BS
25	Create New Sub Frame Request	LE_CP-REQ	UDP	BS->BS(MC?)
26	Create_New_Sub_Frame_Reply	LE_CP-RSP	UDP	BS->BS
27	Reduce Power Request	LE_CP-REQ	UDP	BS->BS
28	Reduce Power Reply	LE_CP-RSP	UDP	BS->BS
29	Stop Operating Request	LE_CP-REQ	UDP	BS->BS

30	Stop Operating Reply	LE CP-RSP	UDP	BS->BS
31-255	<i>reserved</i>	LE CP-REQ	UDP	—

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

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

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

11 Table 5 TLV types for CP payload

Type	Parameter Description
tbc	Operator ID
tbc	BS-ID
tbc	BS GPS coordinates
tbc	BS IP Address
tbc	MAC Frame duration
tbc	Type of sub-frame allocation
tbc	MAC Frame number chosen for the Master sub-frame
tbc	Sub-frame number chosen for the Master sub-frame
tbc	Repetition interval between two Master sub-frames, measured in MAC-frames
tbc	Time shift from the Master sub-frame start of the Base Station radio-signature transmission
tbc	Duration information for the Base Station radio-signature transmission
tbc	Repetition information for the Base Station radio-signature transmission
tbc	Time shift from the Master sub-frame start of the Subscriber Station radio-signature transmission
tbc	Duration information for the Subscriber Station radio-signature transmission
tbc	Repetition information for the Subscriber Station radio-signature transmission
tbc	List of other used sub-frames, in the interval between two Master sub-frames
tbc	Slot position

13 6.1.1 Send-Security-Block message

14 The Send-Security-Block packet is sent using the Coexistence Protocol, over TCP and IP. This message is
 15 sent from the originated BS who initiates the protocol to the terminated BS/CIS. TCP is used instead of

1 UDP because of its defined retransmission behavior and the need for the exchange to be reliable. The TLV
 2 encoded attributes of the Send-Security-Block message carries the security information needed by the
 3 terminated BS/CIS to decrypt and encrypt ESP packets.

4 The Security Block attribute is a series of TLV encodings. This block is encrypted with the terminated
 5 BS/CIS's RADIUS BSID Secret, using the BS's configured cipher. The terminated BS/CIS has to
 6 authenticate and decrypt it first before processing it.

7 Code: 1

8 Attributes are shown in Table 6.

9 **Table 6 Send-Security-Block message attribute**

Attribute	Contents
Initialization Vector	The Initialization Vector is the first 8 bytes of the ACK nonce. The ACK nonce information element is a 32-byte random value created by the RADIUS server, used by the BS to establish liveness of the terminated BS/CIS. This information element is 4 octets in length.
Security Block	TLV encodings.

10 **6.1.2 ACK-Security-Block message**

11 ACK-Security-Block packet is sent using the Coexistence Protocol, over TCP and IP. This packet is
 12 message from the terminated BS/CIS directly to the originated BS. TCP is used instead of UDP because of
 13 its defined retransmission behavior and the need for the exchange to be reliable.

14 The Initialization Vector is an 8-byte value copied from the Date/Time stamp. The Terminated-BS/CIS-
 15 ACK-Authenticator field carries the content of the Terminated-BS/CIS-ACK-Authenticator information
 16 element that the Terminated BS/CIS received in the Security Block. The content of the Terminated-
 17 BS/CIS-ACK-Authenticator should be interpreted by the new AP. The Terminated-BS/CIS-ACK-
 18 Authenticator is encrypted with the new BS's RADIUS BSID Secret, using the BS's configured cipher.
 19 The Terminated BS/CIS has to authenticate and decrypt it first before processing it. This Terminated-
 20 BS/CIS-ACK-Authenticator protects the new BS from spoofed ACK-Security-Block packets.

21 Code: 2

22 Attributes are shown in Table 7.

23 **Table 7 ACK-Security-Block message attributes**

Attribute	Contents
Initialization Vector	The Initialization Vector is an 8-byte value copied from the Date/Time stamp.
Terminated-BS/CIS-ACK-Authenticator	48 Octets.

24 **6.1.3 Neighbor Topology Request message**

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

- 1 Code: 3
 2 Attributes are shown in Table 8.

3 **Table 8 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 neighbors.

4 **6.1.4 Neighbor Topology Reply message**

5 The CIS responds to the BS' to Neighbor Topology Request with a Neighbor Topology Reply message.

6 Code: 4

7 **Query results of Neighbor Topology Encodings** (see [xx.xx](#))

8 Specification of the query results of neighbor topology from CIS specific parameters.

9 **6.1.5 Registration Request message**

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

11 Code: 5

12 Attributes are shown in Table 9.

13 **Table 9 Registration Request message attributes**

Attribute	Contents
BSID	The BSID of the requested BS.
BS IP [TBD]	The IP address of 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.
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 at Max. Power	The maximum operational radius of the BS at Max. power.

1 **6.1.6 Registration Reply message**

2 The CIS responds to the BS' to Registration Request with a Registration Reply message.

3 Code: 6

4 No Attributes.

5 **6.1.7 Registration Update Request message**

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

7 Code:7

8 Attributes are shown in Table H.

9 **6.1.8 Registration Update Reply message**

10 The CIS responds to the BS' to Registration update Request with a Registration update Reply message.

11 Code: 8

12 No Attributes.

13 **6.1.9 De-registration Request message**

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

15 Code: 9

16 Attributes are shown in Table 10.

17 **Table 10 De-registration Request message attributes**

Attribute	Contents
BSID	The BSID of the request BS.

18

19 **6.1.10 De-registration Reply message**

20 The CIS responds to the BS' to De-registration Request with a De-registration Reply message.

21 Code: 10

22 No Attributes.

23 **6.1.11 Add Coexistence Neighbor Request message**

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

25 Code: 11

1 Attributes are shown in Table 11.

2 **Table 11 Add 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 encodings.

3 **6.1.12 Add Coexistence Neighbor Reply message**

4 The CIS responds to the BS' to Add Coexistence Neighbor Request with an Add Coexistence Neighbor
5 Reply message.

6 Code: 12

7 No Attributes.

8 **6.1.13 Update Coexistence Neighbor Request message**

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

10 Code: 13

11 Attributes are shown in Table 12.

12 **Table 12 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.

13

14 **6.1.14 Update Coexistence Neighbor Reply message**

15 The CIS responds to the BS' to Update Coexistence Neighbor Request with an Update Coexistence

1 Neighbor Reply message.

2 Code: 14

3 No Attributes.

4 **6.1.15 Delete Coexistence Neighbor Request message**

5 This message is sent by the BS to the neighbor BS to request to delete form its neighbor list.

6 Code: 15

7 Attributes are shown in Table 13.

8 **Table 13 Delete Coexistence Neighbor Request message attrubutes**

Attribute	Contents
BSID	The BSID of the requested BS.

9 **6.1.16 Delete Coexistence Neighbor Reply message**

10 The CIS responds to the BS' to Delete Coexistence Neighbor Request with a Delete Coexistence Neighbor
11 Reply message.

12 Code: 16

13 No Attributes.

14 **6.1.17 Get_Param_Request message**

15 Messages between BSs, used to request the list of parameters

16 Code:17

17 Parameters: list of the BS parameters

18

19 **6.1.18 Get_Param_Reply message**

20 Messages between BSs, reply to the Get_Param_Request

21 Code:18

22 Parameters: list of the BS parameters

23 **6.1.19 Evaluate_Interference_Request message**

24 A message sent by a new BS wishing to use an existing Master sub-frame, to the BSs already acting as
25 Masters, requesting them to evaluate its interference

26 Code:19

1 Parameters: tbc.

2 **6.1.20 Evaluate_Interference_Reply message**

3 A message sent by the existing Master BSs, reply to the Evaluate_Interference_Request.

4 Code:20

5 Parameters: tbc.

6 **6.1.21 Work_In_Parallel_Request message**

7 A message sent by a new BS to request the use an existing Master sub-frame

8 Code: 21

9 Parameters: tbc.

10 **6.1.22 Work_In_Parallel_Reply message**

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

12 Code: 22

13 Parameters: tbc.

14 **6.1.23 Quit_Sub_Frame_Request message**

15 A message sent by an old Base Station, in order to request the new Base Station to cease the operation as
16 Master in the current sub-frame

17 Code:23

18 Parameters: tbc.

19 **6.1.24 Quit_Sub_Frame_Reply message**

20 A message sent by an new Base Station, in response to the old Base Station's Quit_Sub_Frame_Request
21 message.

22 Code:24

23 Parameters: tbc.

24 **6.1.25 Create_New_Sub_Frame_Request message**

25 A message sent by a BSs to all the community BSs, to request the creation of a new Master sub-frame; the
26 message will include: interfering BSIDs and the frame-number in which the change will take place

27 Code:25

28 Parameters: tbc.

1 **6.1.26 Create_New_Sub_Frame_Request message**

2 A message sent in response to the Create_New_Sub_Frame_Request message.

3 Code:26

4 Parameters: tbc.

5 **6.1.27 Reduce_Power_Request message**

6 A message between a BS and an interfering BS requesting to reduce the power of the specified transmitter
7 (identified by frame_number, sub-frame, time-shift) by P dB

8 Code: 27

9 Parameters: tbc.

10 **6.1.28 Reduce_Power_Reply message**

11 A message by an interfering BS in response to the Reduce_Power_Reply message.

12 Code: 28

13 Parameters: tbc.

14 **6.1.29 Stop_Operating_Request message**

15 A message sent by a Master BS to the BSs operating in its Master sub-frame, but not being Masters for this
16 sub-frame, requesting to cease using this sub-frame in parallel

17 Code: 29

18 Parameters: tbc.

19 **6.1.30 Stop_Operating_Reply message**

20 A message sent by the BSs operating in its Master sub-frame,in response to the Stop_Operating_Request
21 message.

22 Code: 30

23 Parameters: tbc.

24 *[Note: the following part "RADIUS Protocol Messages" is from contribution C802.16-05/012r1, calling*
25 *for comments, as all the security issues]*

26 **6.2 RADIUS Protocol Messages**

27 RADIUS protocol message exchange sequence is shown in Figure 13. Most message content descriptions
28 follow the method in RFC2865:2000. Four messages are introduced to complete RADIUS client egistration
29 and the establishment of SAs with other RADIUS clients. Note that TBD means To Be Defined

1 **6.2.1 Radius-BS/CIS-Registration-Request (BS/CIS → RADIUS server)**

2 A startup BS/CIS sends this message for authentication purpose.

3 **Table 14 Table RADIUS-BS/CIS-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".
2	User-Password	RADIUS BSID Secret.
4	NAS-IP-Address	BS's IP Address
6	Service-Type	CRN-Register (value = TBD, ex. IAPP-Register, value = 15)
26	Vendor-Specific-Attribute (VSA)	
26-TBD	Supported-ESP-Authentication-Algorithms	The list of ESP Authentication IDs corresponding to the ESP Authentication algorithms supported by this BS (See Table A3)
26-TBD	Supported-ESP-Transforms	The list of ESP Transform IDs corresponding to the ESP transforms supported by this BS (See Table A2)
32	NAS-Identifier	BS's NAS Identifier
80	Message-Authenticator	The RADIUS message's authenticator

4

5 According to RFC 2865:2000, other RADIUS attributes may be included in the RADIUS-BS/CIS-
6 Registration-Access-Request packet in addition to the ones listed in Table 14.

7

8 **Table 15 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	12	[Leech]
Reserved for private use	249-255	[RFC2407]

1

2

3

Table 16 ESP Authentication algorithm identifiers

Transform identifier	Value	Reference
RESERVED	0	[RFC2407]
HMAC-MD5	1	[RFC2407]
HMAC-SHA	2	[RFC2407]
DES-MAC	3	[RFC2407]
KPDK	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 private use	61440-65535	

4

5

6.2.2 Radius-BS/CIS-Registration-Accept (RADIUS server → BS/CIS)

6

After RADIUS server verifies the valid membership, it will respond with this accept message.

7

8

9

Table 17 RADIUS-BS/CIS-Registration-Access-Accept

Attribute number	Attribute name	Value
1	User-Name	BSID.
6	Service-Type	CRN-Register (value = TBD, ex. IAPP-Register, value = 15)
26	Vendor-Specific-Attribute (VSA)	
26-TBD	RADIUS-ESP-Transform-ID RADIUS-ESP-	ESP Transform ID of the algorithm to use when encrypting/decrypting the Security Block in the next RADIUS messages

26-TBD	Authentication-ID RADIUS-ESP-SPI	ESP Authentication ID of the algorithm to use when encrypting/ decrypting the Security Block in the next RADIUS messages SPI used to identify ESP SA (between the BS and RADIUS server)
26-TBD		
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

1

2 The RADIUS-ESP-Transform-ID, RADIUS-ESP-Authentication-ID and RADIUS-ESP-SPI attributes are
3 encrypted as described for the MS-MPPE-Send-Key attribute in RFC 2548:1999

4 **6.2.3 Radius-BS/CIS-Access-Request (BS/CIS → RADIUS server)**

5 The BS sends this message to request for inter-communication with another neighbor BS or a regional CIS.

6

7

Table 18 RADIUS-BS/CIS- Access-Request

Attribute number	Attribute name	Value
1	User-Name	Regional CIS's WM address or neighbor BS's BSID.
2	User-Password	NULL.
4	NAS-IP-Address	Original BS's IP Address (the BS sending this request message)
6	Service-Type	CS/CIS-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

8

9 **6.2.4 Radius-BS/CIS-Access-Accept (RADIUS server → BS/CIS)**

10 After verifying that the neighbor BS is valid member, RADIUS server will respond with the security
11 parameters necessary for establishing a secure connection between the neighbor BS and requesting BS or
12 between CIS and requesting BS.

13

Table 19 RADIUS-BS/CIS- Access-Accept

Attribute number	Attribute name	Value
1	User-Name	Regional CIS's WM address or neighbor BS's BSID.
8	Framed-IP-Address	IP Address of Regional CIS or neighbor BS.
26	Vendor-Specific-Attribute (VSA)	
26-TBD	Originating-BS-Security-Block	Security Block encrypted using original BS's RADIUS BSID secret, to be decrypted and used by the original BS.

26-TBD	Terminating-BS/CIS-Security-Block	to be decrypted and used by the original BS Security Block encrypted using neighbor BS's RADIUS BSID secret (or CIS's), to be decrypted and used by the neighbor BS (or CIS)
80	Message-Authenticator	The RADIUS message's authenticator

1

2

Table 20 Information elements in the Originating-BS-Security-Block

Element ID	Length	Information
2	8	Security lifetime in seconds.
3	32	ACK nonce.
4	1	ESP transform number.
5	1	ESP authentication number.
6	4	SPI used to identify ESP SA to the regional CIS or neighbor BS
7	Variable	Key used by ESP Transform for ESP packets to the regional CIS or neighbor BS
8	Variable	Key used by ESP Authentication for ESP packets to the regional CIS or neighbor BS
9	4	SPI used to identify ESP SA from the regional CIS or neighbor BS
10	Variable	Key used by ESP Transform for ESP packets from the regional CIS or neighbor BS
11	Variable	Key used by ESP Authentication for ESP packets from the regional CIS or neighbor BS

3

4 6.3 Association

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

8

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

12 6.4 Sequencing and Retransmission

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

16 The initiator sets the Message ID in the header to any value in the first message of the CP
17 association, and increases the Message ID by one for each new request using serial

1 number arithmetic. Retransmissions do not increment the Message ID. The responder sets
2 the message ID in the response to the value of the message ID in the request.

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

6 The retransmitted requests/responses are exact duplicates of previous requests/responses.

7
8 The initiator must not send a new request until it receives a response to the previous one.
9 Packets with out-of-sequence Message IDs are considered invalid packets and are
10 discarded.

11
12 The initiator must retransmit after a configurable interval until either it gets a valid
13 response, or decides after a configurable number of attempts that the CP association has
14 failed. (Since the retransmission algorithm is implementation-dependent, it is not defined
15 here.)

16 6.5 Message Validity Check

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

- 18
- 19 - Message version field = 1.
- 20 - Association ID must match a current association
- 21 - All messages received by peer have R bit in flag set to zero
- 22 - All responses received by authenticator have R bit in flag set to one.
- 23 - Message opCode is valid
- 24 - Message length equals size of payload
- 25 - Message ID must match the expected sequence number
- 26 - The payload contains only those TLVs expected given the value of the opCode
- 27 - All TLVs within the payload are well-formed, TLVs marked as mandatory are
28 recognized.

29 6.6 Fragmentation

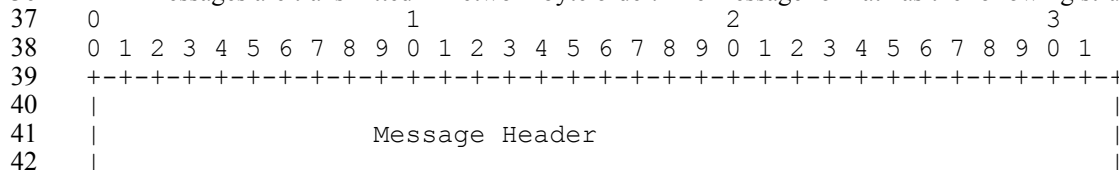
30 CP does not provide support for fragmentation.

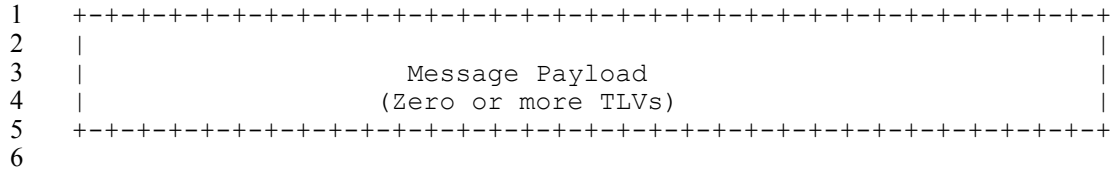
32 6.7 Transport Protocol

33 CP uses UDP as the transport protocol with port number TBD. All messages are unicast.

35 6.8 Message Format

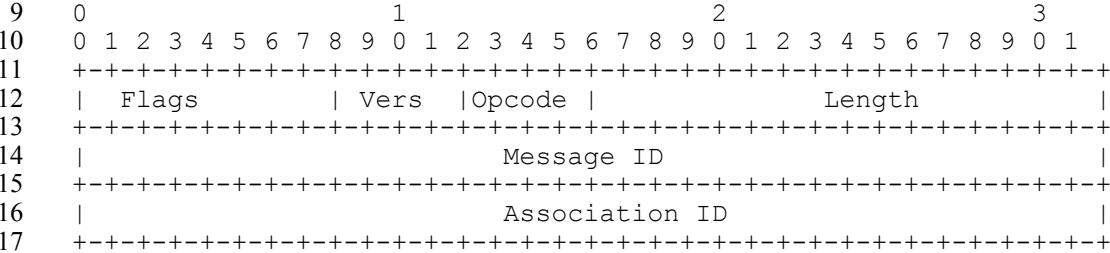
36 All messages are transmitted in network byte order. The message format has the following structure:



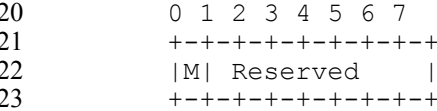


7 The subsection below describes the format of the header and payload.

8 **6.8.1 Header Format**



19 **Flags - 8-bit field indicating options**



24 **Response Flag (R).**

25 Set to 1 when message is a response to a request (same message ID). R must be zero in
26 all request messages.

27 **Reserved Flags:** Reserved. Must be zero. MUST be cleared on sending and ignored on
28 receipt

29
30 **Version - 4-bit field indicating the version of this protocol. This specification = 1**

31 **OpCode - 4 bit field indicating CP message type**
32 tbc

33 **Length - Length of CP payload in octets excluding header**

34 **Message ID - Used to ensure ordered delivery and detect retransmissions.**

35 **Association ID - Uniquely identifies association in authenticator and peer.**

36 **6.8.2 Payload Format**

37 The payload consists of zero or more type-length-value 3-tuples (TLVs).

38 Note: TLVs may not always start on a 4-byte boundary.

1 **6.9 Using dedicated messages**

2 **6.9.1 Common PHY**

3 **6.9.2 Between BS and SS**

4 **6.9.3 BS to BS**

5 **6.9.4 Connection sponsorship**

6 **6.9.5 Using a common management system**

7 **6.9.6 Higher layers communication**

8 **6.9.7 Decentralized control**

9 **6.9.8 Information sharing**

10 **6.9.9 IP / MAC address dissemination**

11 **7 Common policies**

12 **7.1 How to select a “free” channel (for ACS and DFS)**

13 **7.1.1 Acceptable S/(N+I)**

14 **7.1.2 Acceptable time occupancy**

15 **7.1.3 Capability of sharing the spectrum**

16 **7.2 Interference reduction policies**

17 **7.2.1 BS synchronization**

18 **7.2.1.1 GPS**

19 **7.2.1.2 Ad-hoc**

20 **7.2.2 Shared Radio Resource Management**

21 **7.2.2.1 Fairness criteria**

22 The elements of the fairness criteria are addressed below.

23 **7.2.2.1.1 Guaranteed radio resource**

24 Every network will have a guaranteed minimum access time for the interference free use of the radio
25 resource, being able to transmit at the needed powers for allowing communication between its Base Station
26 and the remote subscribers; the guaranteed minimum access time will be basically the same for all the
27 networks sharing the radio resource.

1 **7.2.2.1.2 Power control**

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

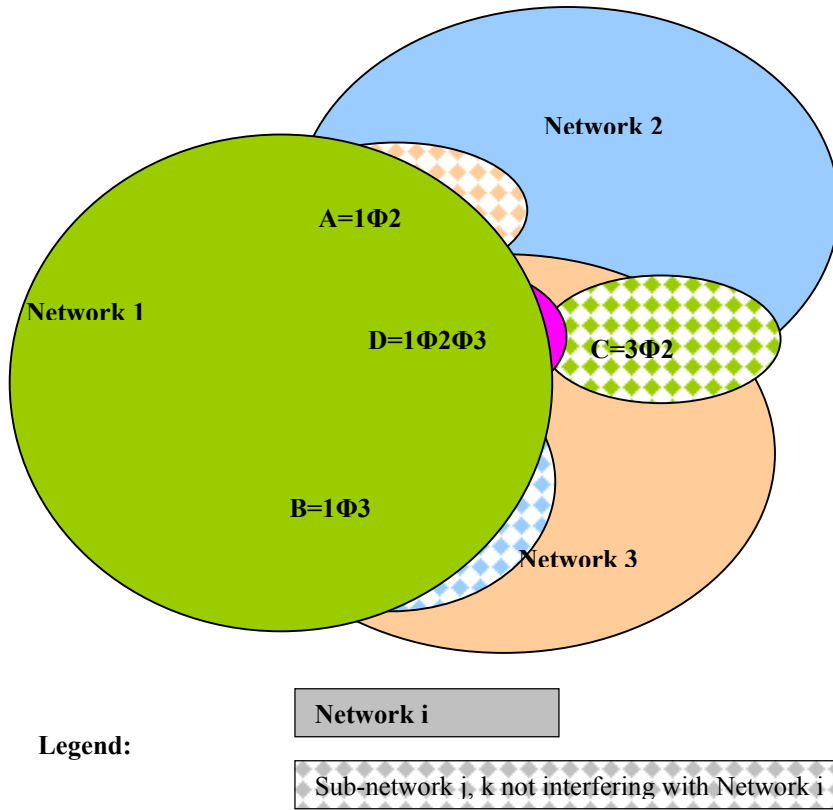
6 **7.2.2.1.3 Mutual tolerance**

7 A network may operate during the time designated for interference – free operation of other master
8 network, with the condition that:

- 9 - The network operating in its interference-free period perceives an interference level equal with the
10 noise level (3dB RSL degradation);
- 11 - The network operating in its interference-free period perceives an interference level higher than
12 the noise level (3dB RSL degradation), but explicitly agrees to operate at the created interference
13 level; this may be the case of a small cell size or reduced traffic
- 14 - If the interference level is higher than the acceptable level, the master network may request the
15 links operating in parallel to reduce their transmitting powers; if such a link enters the situation
16 that will not be able to operate anymore, the link transmitter will have to operate in another sub-
17 frame in which will not cause harmful interference.

18 The figures below explain possible ways of implementing the Guaranteed radio resource principle, using a
19 example of three overlapping radio networks.

20 The overlapping radio networks create different interference zones, based on spatial distance between
21 transmitters and receivers. For example, the radio receivers in Zone A, in the figure below, suffer from the
22 interference (noted with Φ) between Network 1 and Network 2. Interference Zone B includes also the Base
23 Station of the Network B.



1

2

3

Figure 14 Interference due to overlapping networks

4 The operation of the 3 networks assume the following different situations:

5

6 Networks 1,2,3 do not interfere

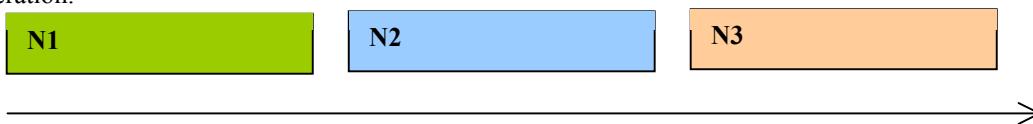
7 Zone A: Networks 1 and 2 interfere

8 Zone B: Networks 1 and 3 interfere

9 Zone C: Networks 3 and 2 interfere

10 Zone D: Networks 1 and 2 and 3 interfere

11 Now lets suppose that we split a time frame in 3 sub-frames (being 3 different networks), such that we
12 apply the fairness criteria defined above, and every network will receive an interference free interval for
13 operation.



14

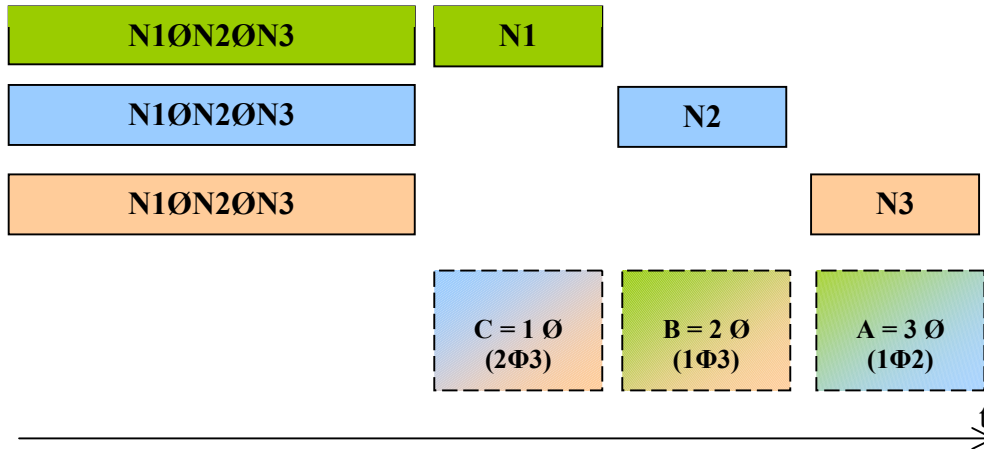
15 Figure 15 Equal splitting of radio resource between networks

1

2 In the figure above we resolved the interference problem, but we did not use optimally the radio resource.

3 Another possible approach will be to set an operating time for not interfering (noted \emptyset) situations, and split
4 equally between the 3 networks the remaining resource, like shown below. It can be seen that non-
5 interfering traffic may be scheduled in parallel, resulting in a much better radio resource usage.

6



7

8

9

Figure 16 Usage of the spectrum by every system

10 Taking as example Network 1, it can be seen that this network operates in all the sub-frames, achieving in
11 the same time interference-free operation and good spectral efficiency.

12 However, the networks working in the same time with the network having the control of the radio resource,
13 shall use power control, sectorization or beam-forming in order to not create interference to that network.

14 7.2.2.1.3.1 Cooperation with other networks

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

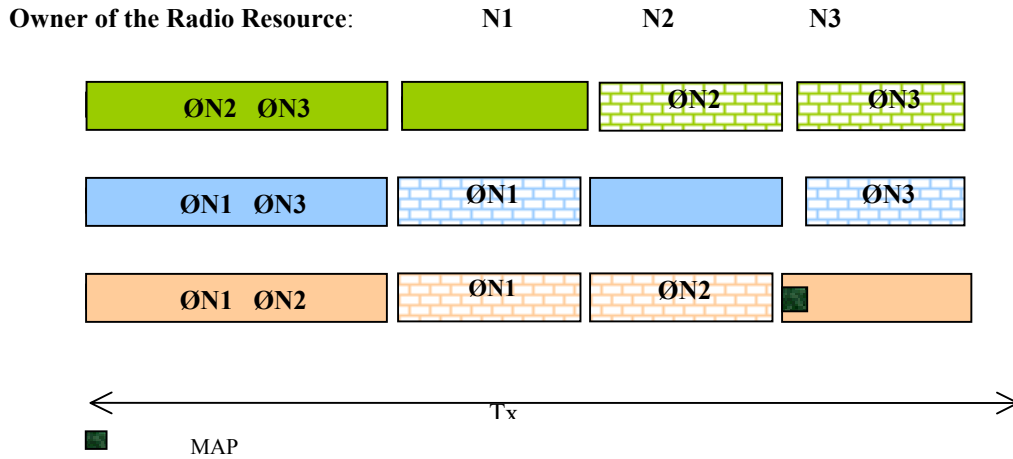
21 7.2.2.1.3.2 Scheduling of interference free intervals in the context of IEEE 802.16 MAC

22 A number of scheduling approaches may be considered, some of them being presented below, for Tx
23 synchronized intervals. Same approach is valid for Rx intervals.

24 7.2.2.1.3.2.1 Sharing same MAC Frame

25 This approach considers the possibility of including sub-frames for addressing all the systems suffering
26 from interference in the same MAC frame. The disadvantage of this approach is that the duration of the
27 MAC frame may be high and all the BS-SS links will suffer from the possible relatively high delay.

- 1 The advantage of this approach is that allows flexibility in changing the duration of different sub-frames, to
- 2 use the radio resource in accordance to traffic load or interference level.
- 3 The possible traffic scheduling is presented in fig. 4. If, for example, the common sub-frame has a
- 4 reservation of 40% of Tx duration and all the other sub-frames are 20% each, the maximum time-frame to
- 5 be used is 80%.

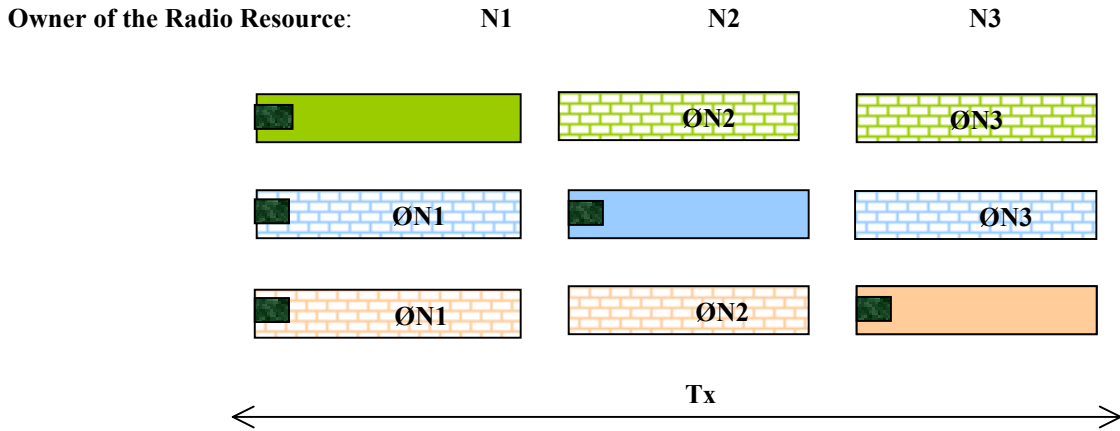


6

Figure 17 Sharing same MAC frame

7.2.2.1.3.2.2 Sharing the same MAC Frame – alternative mode

An alternate possibility for sharing the same MAC Frame is shown below. The MAPs are inserted at the beginning of the transmit frame for compatibility with the existing PHY/MAC.



11
12

Figure 18 Sharing same MAC frame – alternative mode

14

1 The disadvantage of this mode is that for interference-free traffic there is no guaranteed interval. As a
 2 result, all the N systems will have approximately $1/N$ from the frame duration. For example, if every sub-
 3 frame will be $1/3$ of the Tx time, every network will be able to use 66% of the time. The delay may be
 4 slightly lower than with the previous case. This mode may be useful in high interference environments.

5 7.2.2.1.3.2.3 Repetitive sharing approach

6 With this approach, a first option is to split every frame has two sub-frames:

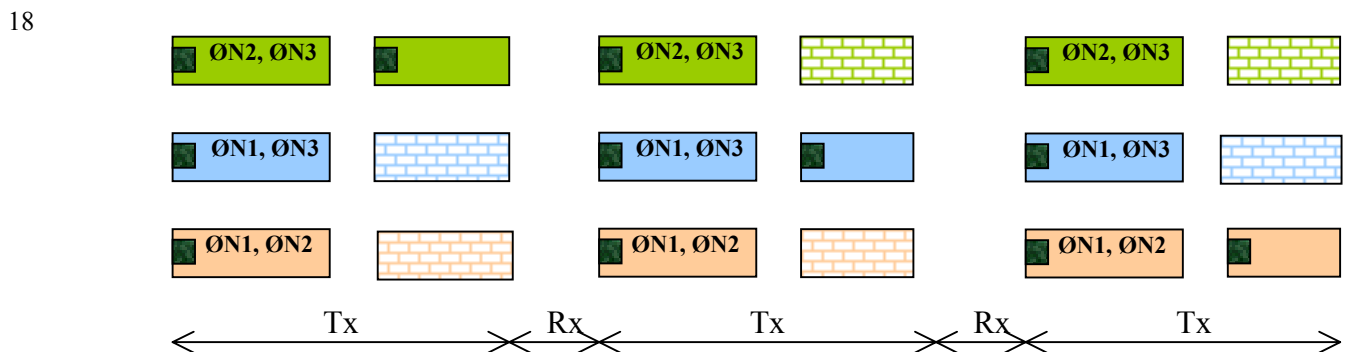
- 7 - one sub-frame is reserved for traffic not affected by interference
- 8 - one sub-frame is reserved for Network I and the traffic not affecting Network I.

9 The advantage of this scheduling mode are:

- 10 - the MAC frame duration may be small and users not affected by interference will have an optimal
 11 delay;
- 12 - some flexibility exists to trade between the duration allocated for Network i and the duration of
 13 the interference-free sub-frame.

14 The disadvantage is that subscribers affected by interference will suffer from higher delay than subscribers
 15 not affected by interference.

16 The repetitive scheduling for 3 networks, every network having its interference-free traffic in one of the
 17 frames, and repeating every 3 frames the interference-free sub-frame will be:



19
 20

21 **Figure 19 Repetitive scheduling**

22 The advantage of this approach is that it is easier, per Tx frame, to negotiate the splitting between the
 23 interference-free sub-frame and the sub-frame allocated to Network i. The delay remains minimal for SSS
 24 not affected by interference.

- 1 **7.2.2.2 Distributed scheduling**
- 2 **7.2.2.2.1 Assignments**
- 3 **7.2.2.3 Distributed power control**
- 4 **7.2.2.4 Distributed bandwidth control**
- 5 **7.2.2.5 Beam-forming**

- 6