Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Consolidation of the IEEE 802.16h Working Document – marked version**
Date Submitted	**2005-07-11**
Source(s)	Mariana Goldhamer Alvarion Tel Aviv, 21 HaBarzel Street Israel Voice: +972 3 6456241 Fax: +972 3 645 6204 mailto:marianna.goldhammer@alvarion.com
Re:	Call for Contributions, IEEE 802.16h Task Group on License-Exempt Coexistence, IEEE 802.16h-05/014
Abstract	The consolidation had been done in order to bring together principles from different parts, put all the networking / messages together, same for messages, delete overlapping text and figures.
Purpose	
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.
Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chair@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

~~Draft IEEE Standard for~~

~~Local and Metropolitan Area Networks~~

Part 16: Air Interface for Fixed 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 Society

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~~ is to be carried out by the Working Group's License-Exempt Task Group ~~h~~:
~~TGh Officers~~

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]*~~

Contents

List of Figures

List of Tables

Part 16: Air Interface for Fixed Broadband Wireless Access Systems

Amendment for Improved Coexistence Mechanisms for License-Exempt Operation

Acronyms

CIS Coexistence Identification Server
DRRM Distributed Radio Resource Management
DSM Distribution System Medium
ESP IP Encapsulating Security Payload
IETF Internet Engineering Task Force
IANA Internet Assigned Numbers Authority
RADIUS Remote Authentication Dial-in User Service
SAP Service Access Point
TCP Transmission Control Protocol
UDP User Datagram Protocol

1 Overview

1.1 General

1.2 IEEE 802.16h 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.

1.3 IEEE 802.16h applicability

This amendment is applicable for un-coordinated frequency operation in all bands in which 802.16-2004 is applicable, including bands allowing shared services.

2 Interference detection and prevention – general architecture

2.1 ~~Shared Radio Resource Management~~

2.1 Operational Principles and Policies

2.1.1 General Principles

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

There is country/region data base, which includes, for every Base Station:

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

There is a Server that manage the write/reading of this Data Base, using the 802.16h standardized procedures;

Every Base Station includes a data base, open for any other Base Station; the BS data-base contains information necessary for spectrum sharing, and includes the information related to the Base station itself and the associated SSs; a Base Station and the associated SSs form a System. Other Base Stations can send queries related to the information in the database to the DRRM entity, located in a Base Station (see ;

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

A community of BSs is formed in an ad-hoc mode; in this community are included Base Stations, if at least two of the Base Stations interfere; every Base Station maintains the list of the Base Stations forming the community. Supplementary, when using the IP-based communication approach:

- An SS will not communicate directly with a foreign BS;
- It is no need to register the SS location.

All the Base Stations forming a community will have synchronized MAC frames

A community will be limited to a reasonable size; the size limitations and interactions between different neighborhoods: t.b.d. ~~in further meetings~~

Every network will have a guaranteed minimum access time for the interference free use of the radio resource, being able to transmit at the needed powers for allowing communication between its Base Station and the remote subscribers

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

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

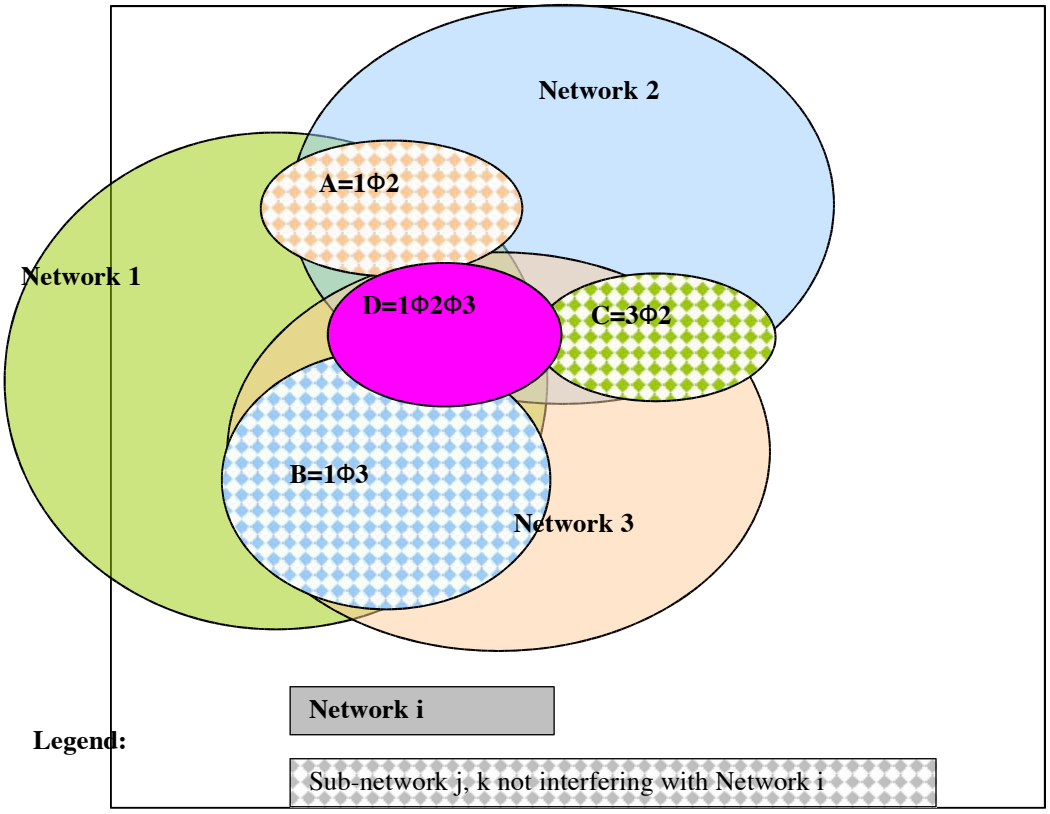


Figure 1 Interference due to overlapping networks

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

Zones in which the networks 1,2,3 do not interfere;

Zone A: Networks 1 and 2 interfere;

Zone B: Networks 1 and 3 interfere;

Zone C: Networks 3 and 2 interfere;

Zone D: Networks 1 and 2 and 3 interfere.

Now lets suppose that we split a time frame in 3 sub-frames (being 3 different networks), and every network will receive an interference free interval for operation.

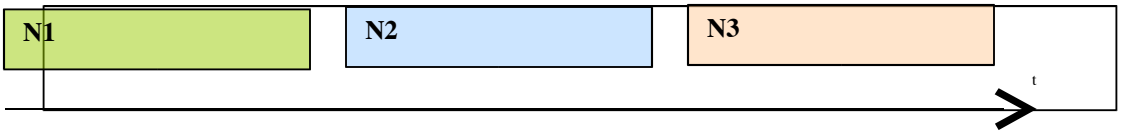


Figure 2 Equal splitting of radio resource between networks

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

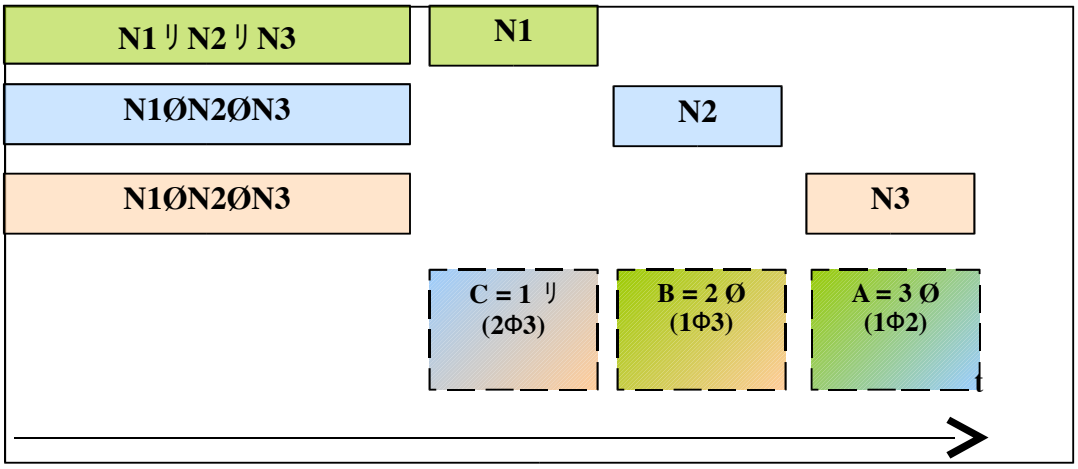


Figure 3 Usage of the spectrum by every system

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

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

Cooperation with other networks

A network may need more time 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 network may request from one or more adjacent networks to reduce their interference free transmission intervals. The other networks will consider the request, and when possible will accept the request, by indicating the agreed new interference-free operating interval. The duration of each sub-frame may be negotiated through inter-network communication and using the common DRRM policy.

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. Same approach is valid for Rx intervals.

~~For every community of Base Stations is created a repetitive pattern, based on one of the following possibilities, mentioned in 802.16h Working Document, chapt. 7.2.2.1.3.2:~~

- *Type 1* ~~*(par.* 7.2.2.1.3.2.1):~~ The MAC frame, for each Tx and Rx part, is split in N+1 sub-frames:
  - One for non-interfering traffic
  - Every other one to be used by a single BS or more non-interfering BSs which are assuming the Master role
- *Type 2* ~~*(par.* 7.2.2.1.3.2.2)~~: The MAC frame, for each Tx and Rx part, is split in N sub-frames, every one to be used by a single BS or more non-interfering BSs which are assuming the Master role during a sub-frame
- *Type 3*: ~~*(par.* 7.2.2.1.3.2.3)~~ The MAC frame is split in two sub-frames: one for non-interfering traffic and one in which a single BS or more non-interfering BSs are assuming the Master role; 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: ~~(here down are some of possible relations and corresponding MAC frames notation):~~

for type 1:

- $T_{Tx\_sub\text{-}frame} = T_{TxMAC} / (N+1)$
- $T_{Tx\_sub\text{-}frame} = (T_{TxMAC} - T_{Txsh}) / N$
- $T_{Rx\_sub\text{-}frame} = T_{RxMAC} / (N+1)$
- $T_{Rx\_sub\text{-}frame} = (T_{RxMAC} - T_{Rxsh}) / N$

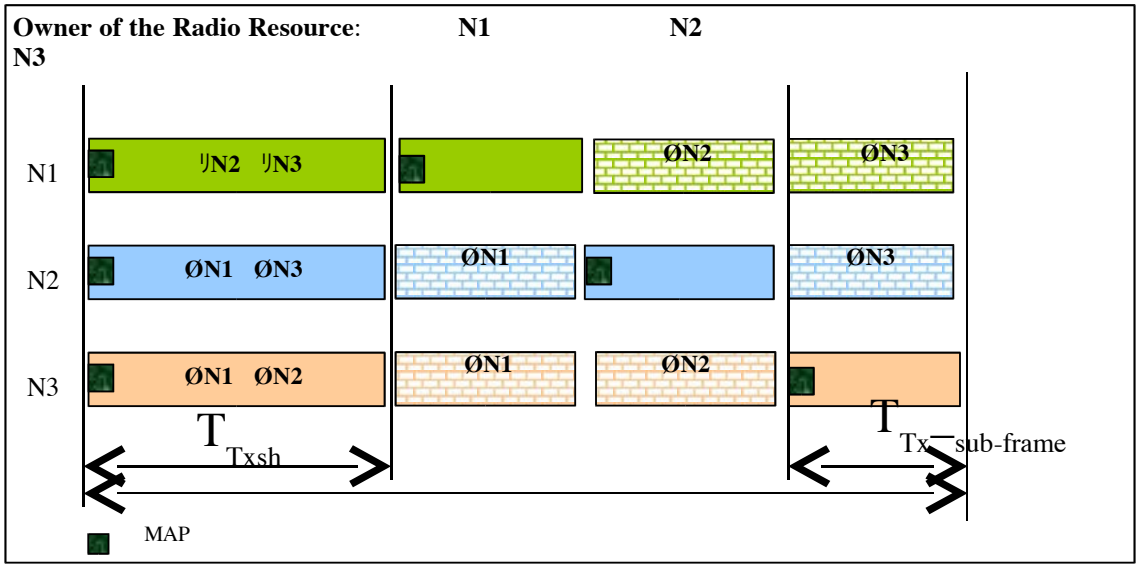


Figure 4 Sub-frame structure type1

for type 2:

- $T_{Tx\_sub\text{-}frame} = T_{TxMAC} / N$
- $T_{Rx\_sub\text{-}frame} = T_{RxMAC} / N$

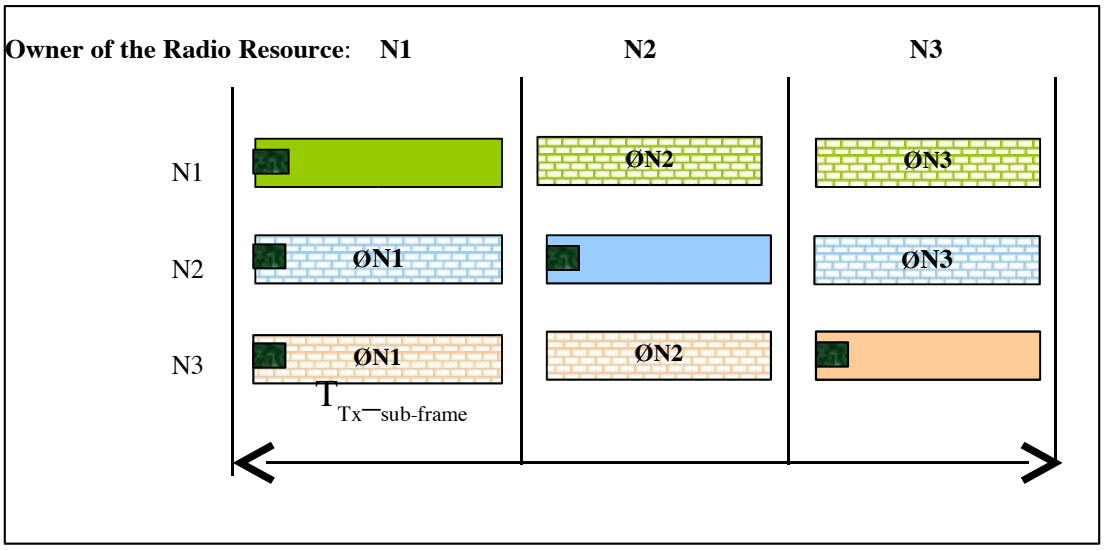


Figure 5 Sub-frame structure type 2

for type 3:

- $T_{Tx\_sub\text{-}frame} = T_{TxMAC} / 2$
- $T_{Tx\_sub\text{-}frame} = T_{TxMAC} - T_{Txsh}$
- $T_{Rx\_sub\text{-}frame} = T_{RxMAC} / 2$
- $T_{Rx\_sub\text{-}frame} = T_{RxMAC} - T_{Rxsh}$
- repetition interval = $N*T_{MAC}$,

$N*T_M$

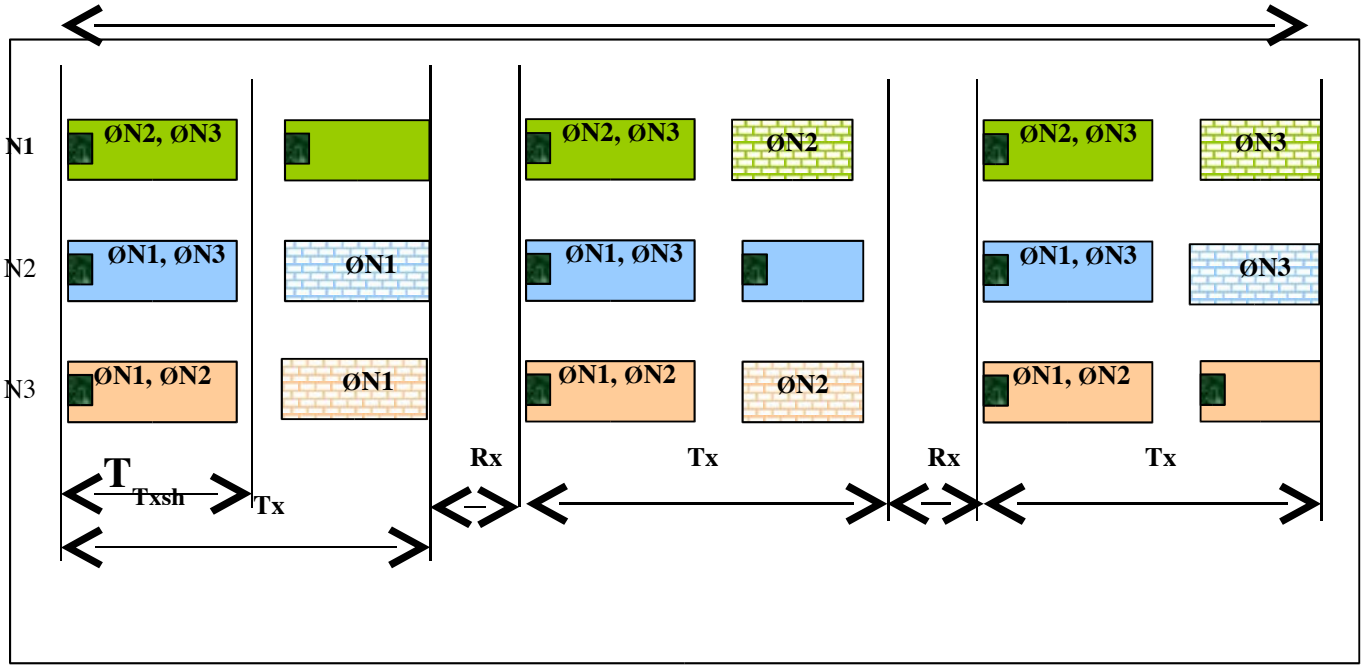


Figure 6 Sub-frame structure type 3

where T_{MAC}, T_{TxMAC}, T_{RxMAC}, T_{Txsh}, T_{Rxsh} are the durations of the respectively the MAC frame, Tx interval and Rx interval of the MAC frame or of the sub-frame used for shared used in the non-interfering sub-frame.

In the above relations, the meaning of Tx or Rx is relative to the usage of the MAC Frame by a Base Station.

During the Master sub-frame the Base Stations assuming Master role may use their maximum power

During every Master sub-frame, the Base Stations will create a slot, possibly not overlapping with another slot of a neighbor Base Station, during each 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"* ~~*shall be defined :*~~ *are t.b.d.*
- During "radio signature" intervals, all the other BSs and SSs shall use a GAP interval;
- The Base Station shall take care to provide enough transmit opportunities for the active SSs.

The figure below 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 Network 2.

The Network 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 solely one Base Station. Base Stations using the same MAC sub-frame as Master sub-frames shall schedule the transmission of their "radio-signatures" in such a way that will not interfere one with the 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 Data Base. The active SSs will provide a signature for every used power/OFDMA/sub-channelization/ direction partition.

~~The Base Station shall take care to provide enough transmit opportunities for the active SSs.~~

~~During "radio signature" intervals, all the other BSs and SSs shall use a GAP interval.~~

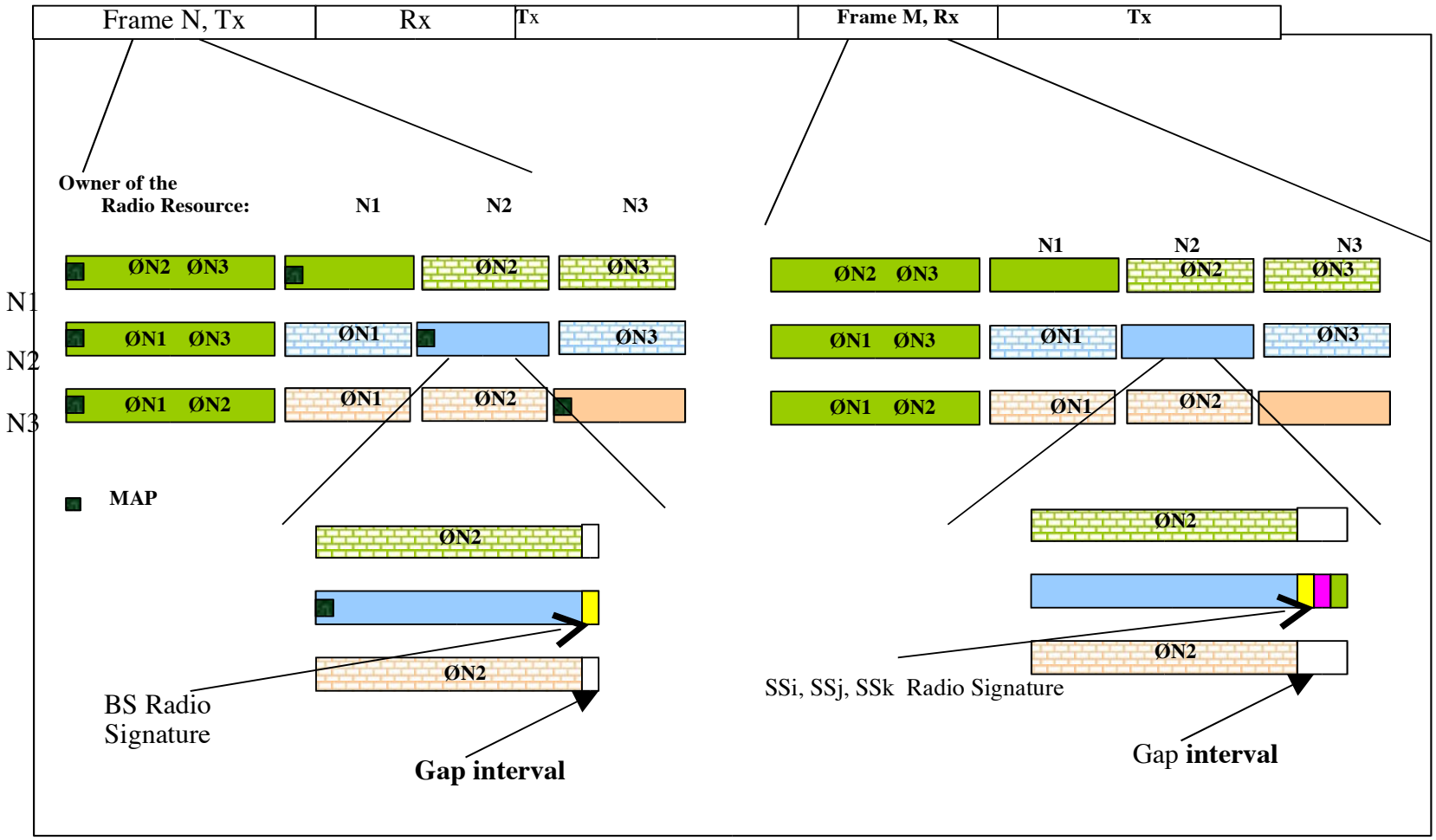


Figure 7 Allocation of slots for BS and SS radio signature

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.

2.1.2 Interference Control

Interferer identificationer

- A receiver will listen to the media and will find out which are the strongest interferes; by scanning the BS data bases will be possible to identify, due to the knowledge of the frame number, sub-frame number and offset, to which BS is the interferer associated; based on time-shift information, the Base Station will be able to identify the Subscriber Station ID. During the allocated radio-signature transmit opportunity no other radio transmitters will operate.

Interference reduction

- A BS has the right to *request an interferer to reduce its power by P dB*, for transmissions during the time in which a Base Station is a Master; if the requested transmitter cannot execute the request, it has to cease the operation during the Master sub-frame of the requesting Base Station; this applies also for systems using the sub-frame as a Master

Sharing the Master time

- A Base Station will indicate in the data base *what portion of the sub-frame time, separately for Tx and Rx, is actually used*
- Other systems, which do not interfere one with each other, may use that time interval

Target acceptable interference levels during Master sub-frames:

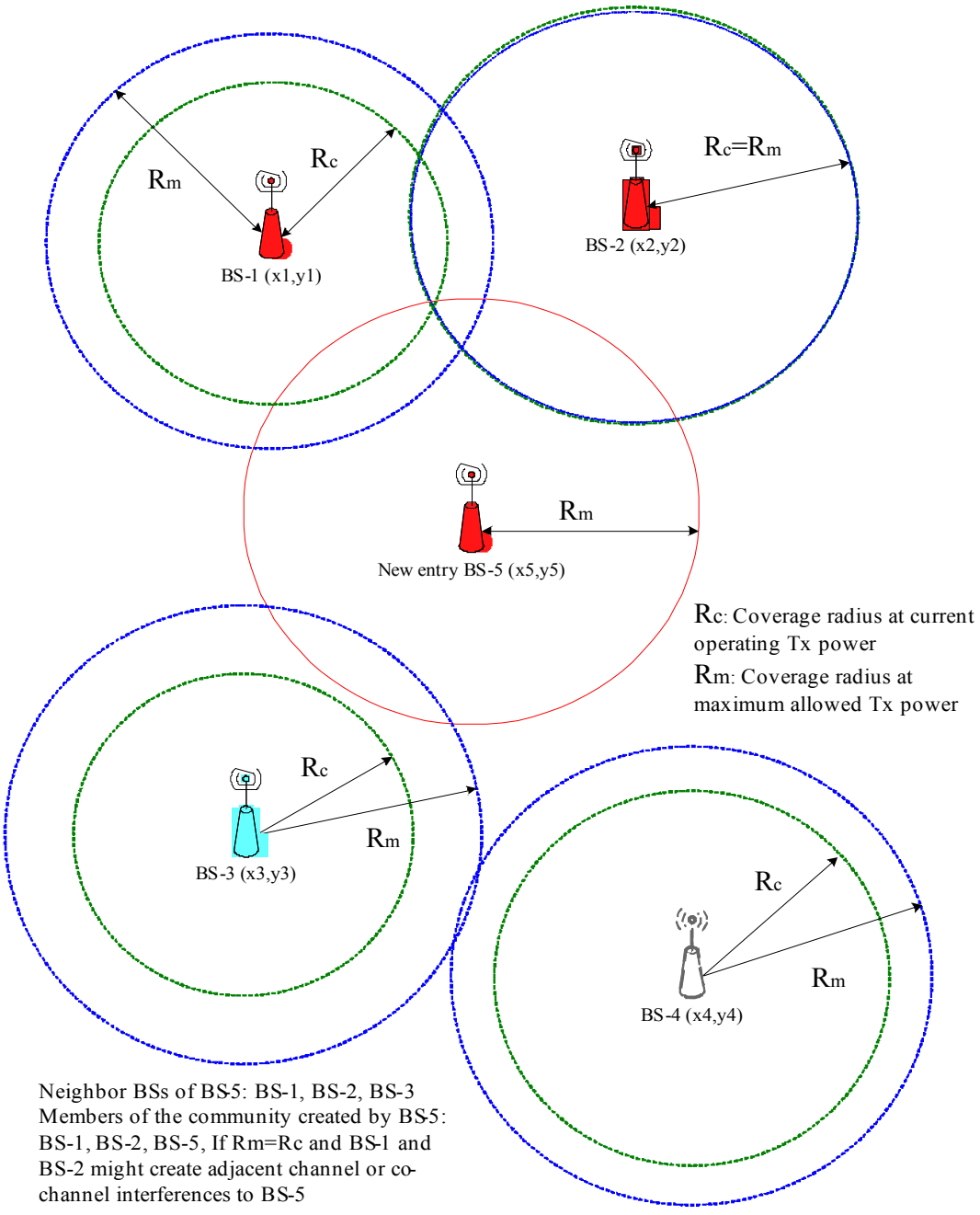
- For the Base Station and its SS, using the Master sub-frame: min. 14dB above the noise + interference level (16QAM 1/2 *(note: we should define the interference criteria; the existing one may be too stringent and not necessary for short links)*

2.1.3 Community Entry of new BS

Figure 8 explains how one new entry BS discovers its neighbor BSs. The new entry BS-5 uses its GPS coordinates (x5, y5) and its maximum coverage radius, Rm, at allowed maximum transmission power to query the LE DB. A BS is neighbor BS of another BS means their maximum coverages at allowed maximum transmission power overlaps. As depicted in Figure 8, the regional LE DB will return BS-1, BS-2 and BS-3 as the neighbor BSs of the new entry BS.

Once a LE BS has learnt its neighbor topology from the regional LE DB, it evaluates the coexisting LE BSs and identifies which BSs might create interferences. While it decides its working frequency after scanning, the *community* to which the LE BS belongs is determined. Each LE BS tries to form its own community. The members of community come from the neighbor BSs of one BS, i.e. the members of community are the subset of neighbor BSs. Those neighbor BSs that might create interferences to the BS or to the associated SSs under current working frequency are the members of its own community. For example, BS-1 and BS-2 are the members of the community create by BS-5 if Rm=Rc and BS-1 and BS-2

might create adjacent channel or co-channel interferences to BS-5. One BS creates and maintains one community of it at the same time. The members of community will change when its working frequency changes or new interfering neighbor BS comes in. Every BS maintains the list of the member BSs forming the community. An SS will not communicate directly with a foreign BS and there is no need to register the SS location. All the Base Stations forming a community will have synchronized MAC frames.



Neighbor BSs of BS-5: BS-1, BS-2, BS-3
Members of the community created by BS-5: BS-1, BS-2, BS-5, If Rm=Rc and BS-1 and BS-2 might create adjacent channel or co-channel interferences to BS-5

Figure 8 802.16 LE Neighbor BSs discovery and definition of neighbor and community

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

(1) *Initialization stage*

In initialization stage the LE BSs may avoid the co-channel or adjacent channel interference by scanning the available frequencies. But this method cannot avoid the *hidden* LE BS problem, i.e. the BS that cannot be heard directly but may have overlapping service coverage. Thus, with the knowledge of neighbor topology the LE BSs can detect the *hidden* LE BSs and can, therefore, avoid the possible interferences from coexisting neighbors. The procedures are described in Figure 9. If the LE BS finds that there is no "free" channel, the neighbor topology provides the guidelines of with whom it should negotiate.

(2) *Operating stage*

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

Figure 9 shows the proposed initialization procedures for the 802.16 LE BSs. Note that the procedures that BS tries to create a Master slot are also applicable for operating stage. The detailed negotiation and update procedures are described in section 2.2.3.

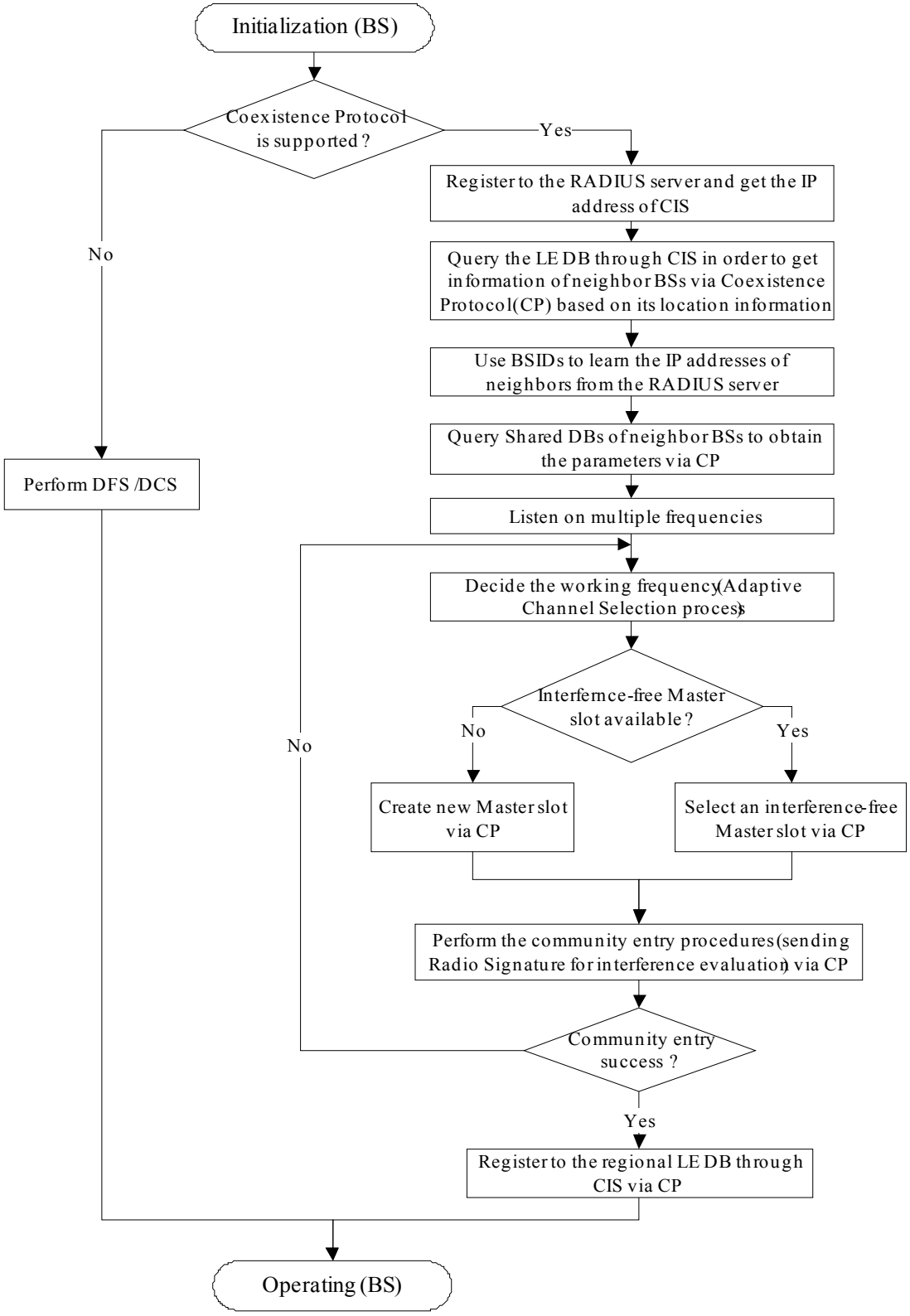


Figure 9 Initialization procedures — BS

The first phase of the Community Entry process uses the country/region (FCC) data base:

- *Read the Regional/country (FCC) data base;*
- Identify which Base Stations might create interference, based on the location information;
- Learn the IP identifier for those Base Stations;

Build the local image of the relevant information in the community BS's, *by copying the info in those BSs*
Listen on multiple frequencies

- Identify the level of interference on each frequency channel;

Decide the working frequency (ACS – Adaptive Channel Selection process);
If available, select an interference-free Master sub-frame; if not, use the procedure for creating new Master sub-frames;
Search the Base Station data base for finding the BSs using the selected Master sub-frame;
Request those Base Stations, by sending IP unicast messages, to listen during the BS_entry slot in order to evaluate the interference from the new Base Station;
Use the allocated slots for transmitting the "radio signature" at maximum power, maximum power density and in all the used directions;
Ask for permission of the Base Stations, using the sub-frame as Masters, *to operate in parallel and use the same sub-frames;*
If all of them acknowledge, the Base Station acquires a "temporary community entry"status; the final status will be achieved after admission of the SSs;
If no free Master slot sub-frame is found, use the procedure for creating new Master slotssub-frames.

2.1.4 Network and Community Entry for SS

- 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, s*end 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.*

2.1.5 BS regular operation

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

2.1.6 Operational dynamic changes

2.1.7 Creation of a new sub-frame

If none sub-frame 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 interfere with the new Base Station. However, all the others, that do not interfere one with each other and with the new one, may work in parallel and use the same operating time.

A Base Station will request the creation of a new sub-frame by:
Sending IP messages to all BS members of the community, and indicating:

- *The interfering operator ID and BS ID*

- *The MAC frame-number in which the addition of a new sub-frame will take place.*

All the requested *BSs will acknowledge the request*, by

- *Sending back a message having as parameters:*
  - *Frame-number for the change (must be the same as the requested one*
  - *Master sub-frame number for the new BS (SF = Sfold+1).*
- If are missing acknowledges, those BS will be asked again, for another M attempts, after that will be considered that they are not working;
- At the above specified MAC frame number, a new sub-frame partition will take place, by inserting in the sub-frame calculation relation:
  - N=N+1
- *The BSs will up-date the own SSs about the change*

Start to use the created Master sub-frame.

2.1.8 Controlling interference during master sub-frame

2.1.8.1 Interferer identification

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 arrival.

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.

2.1.8.2 Interference to BS

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

2.1.8.3 Interference to SS

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

2.1.9 Power Control

Every network will strive to reduce its transmit powers 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 network is operating during its interference-free period. The power control mandatory algorithm will be defined in chap. [t.b.c.]

2.1.10 Coexistence with non-802.16 wireless access systems

The above principles are also applicable to non-802.16 systems, like 802.11. During every 802.16 MAC frame, a 802.11 system 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 Coexistence Protocol, working at IP level, will allow the communication between systems using different PHY/MAC standards.

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

2.2 Shared distributed system architecture

2.2.1 Architecture

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

Every Base Station includes a Distributed Radio Resource Management entity, to apply the 802.16h spectrum sharing policies, and a Data Base 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 in 802.16h context.

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

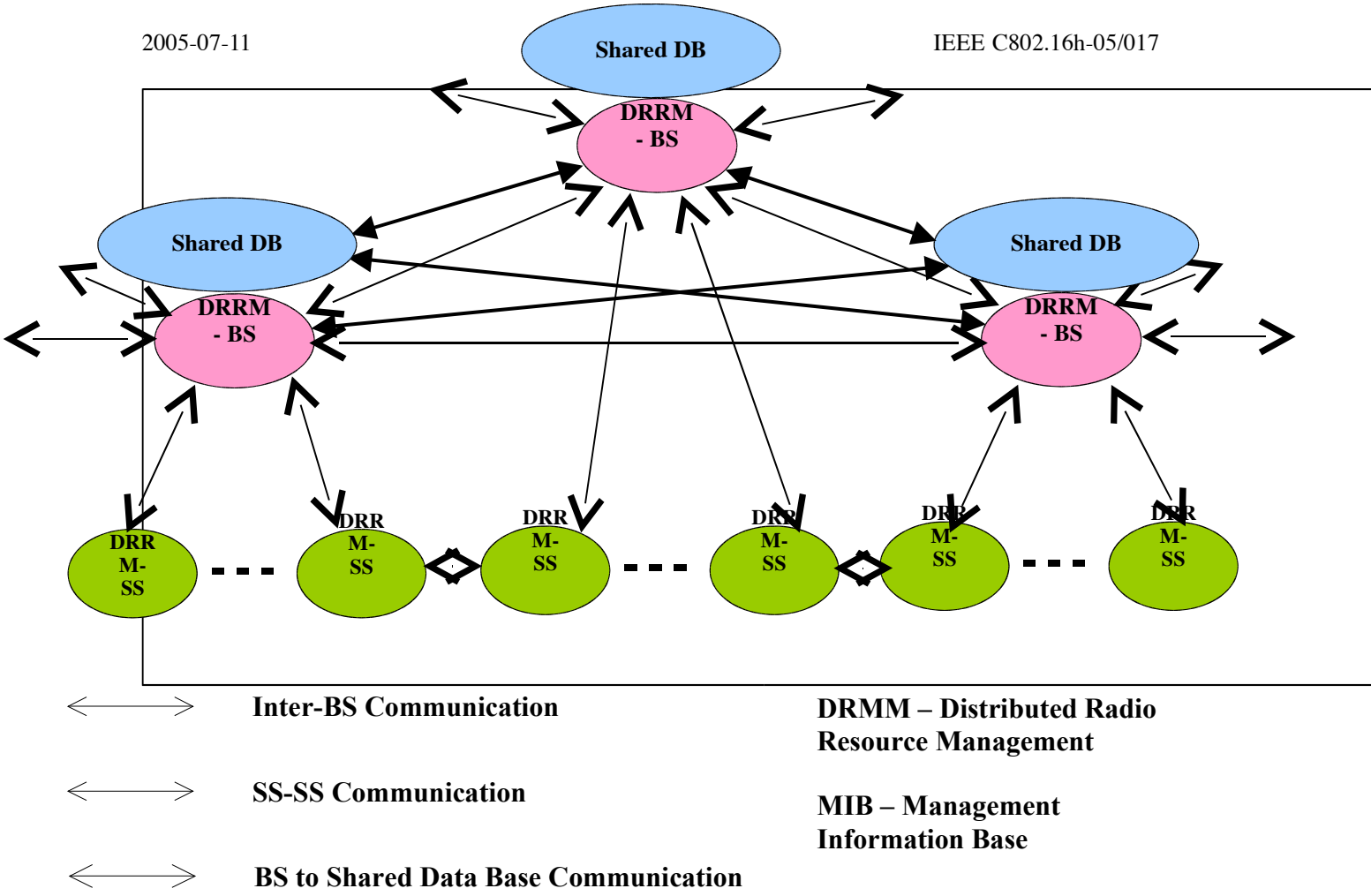
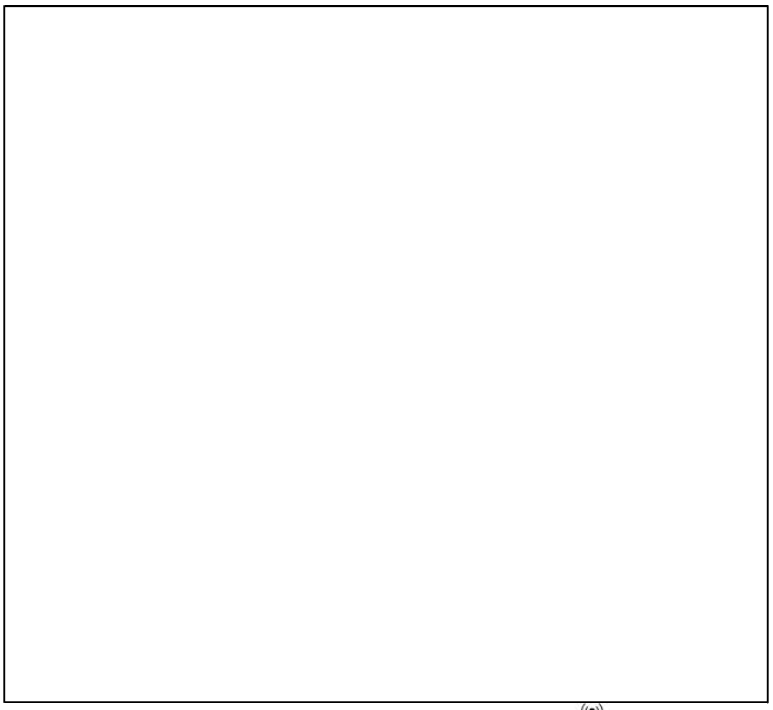


Figure 10 System Architecture

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

Figure 11 shows the IEEE 802.16 LE inter-network communication architecture:



General architectu

- The RA

- The C ction xxx ~~(detail descriptio~~

- The BS .M) procedure

RADIUS server p LE BSs and CIS. Keyed-Hashing fo RFC2869:2000) is adopted for authe wireless medium addresses of BSs his mapping is to distribute the keys

CIS maintains the d the BSID of LE BSs. BSs operatin while starting up, following the Co ription in section *x.x.x*). After the ie neighbor BSs. Intercommunicati the BS acquires coexisting neighbor's authentication key and encryption key for LSF as well as IP address by querying RADIUS server.

2.2.2 Inter-network communication

The inter-network communication consists in:

- Inter-network messages
    - Base Station to/from Base Station

- Base Station to/from Subscriber Station to/from foreign Base Station; the subscriber Station is used as relay, if the two Base Stations are hidden one from the other

- Open access to DRRM Data Base:
  - To read the parameters of the hosting Base Station
  - To request change of the hosting Base Station operating parameters.

2.2.3 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 neighbor topology, perform registration to the database and registration to peer, negotiation for Shared RRM etc. ~~we propose~~will be used a Coexistence Protocol (CP). Figure 12 ~~reveals~~ describes the 802.16h 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 13 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 14 is the CIS 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. ~~But the service primitives will not be provided in this contribution due to the Coexistence Protocol is incomplete at this stage. This proposal only provides the definition of PDUs exchanged between peer Coexistence Protocol entities.~~ 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) LE_CP-REQ: BS→BS or BS→CIS

(2) LE_CP-RSP: BS→BS or CIS→BS

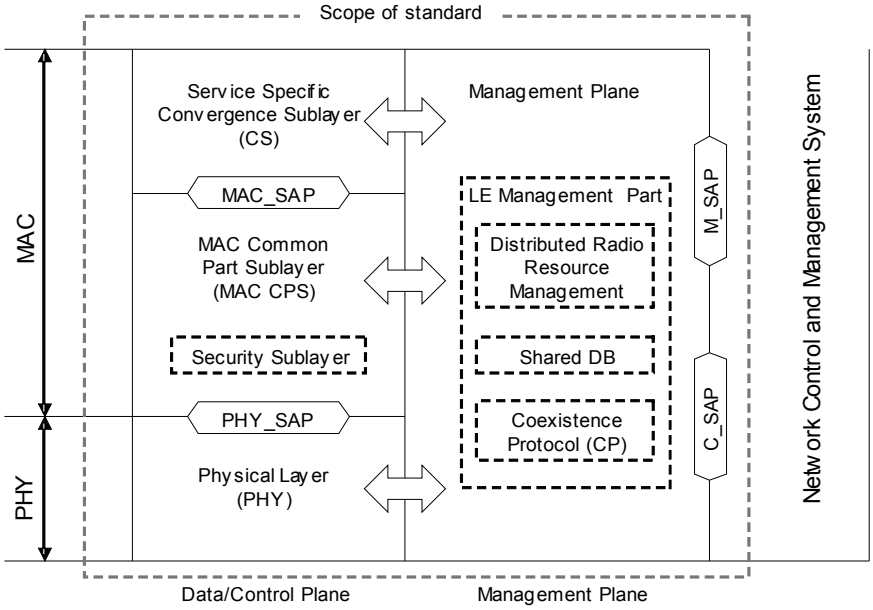


Figure 12 802.16h BS Protocol architecture Model

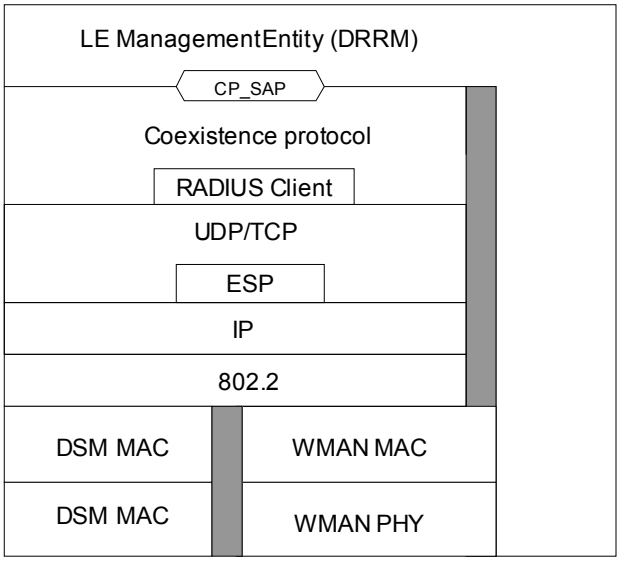


Figure 13 LE BS architecture with Coexistence Protocol

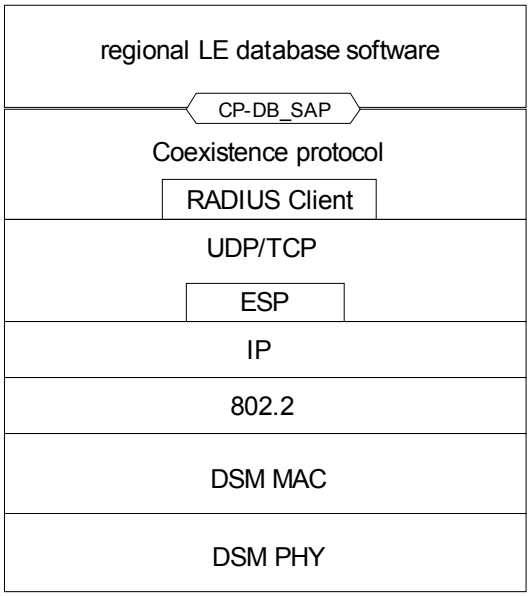


Figure 14 CIS architecture with co-located regional LE database

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

Before any data can be exchanged between BS and BS/CIS, 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 CIS shall first send a *RADIUS Access-Request* to request the establishment of the security association between originated BS and terminated BS/CIS. 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 LE_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 CIS. The peer returns LE_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 CIS.

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

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

2.2.3.1.1 Same PHY Profile

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

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

the inter-network communication may be done using 802.16 messages over the air, including messages defined by 802.16h amendment. The procedures for sending these messages are described in t.b.d.

2.2.3.1.2 Mixed-PHY Profile communication

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

~~Every system will:~~

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

3 Interference victims and sources

3.1 Identification of the interference situations

3.1.1 Interferer identification

3.1.2 Grouping of interfering/not-interfering units

3.2 Identification of spectrum sharers

3.2.1 Regulations

3.2.2 Messages to disseminate the information

3.2.3 Avoid false-identification situations

3.2.4 ~~Storage of identification information~~

Note: overlapping chapter

3.2.4.1 ~~Regional LE database~~

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

1. ~~Operator ID~~
2. ~~Base Station ID~~
3. ~~Base Station GPS coordinates~~
4. ~~IP address (TBD)~~

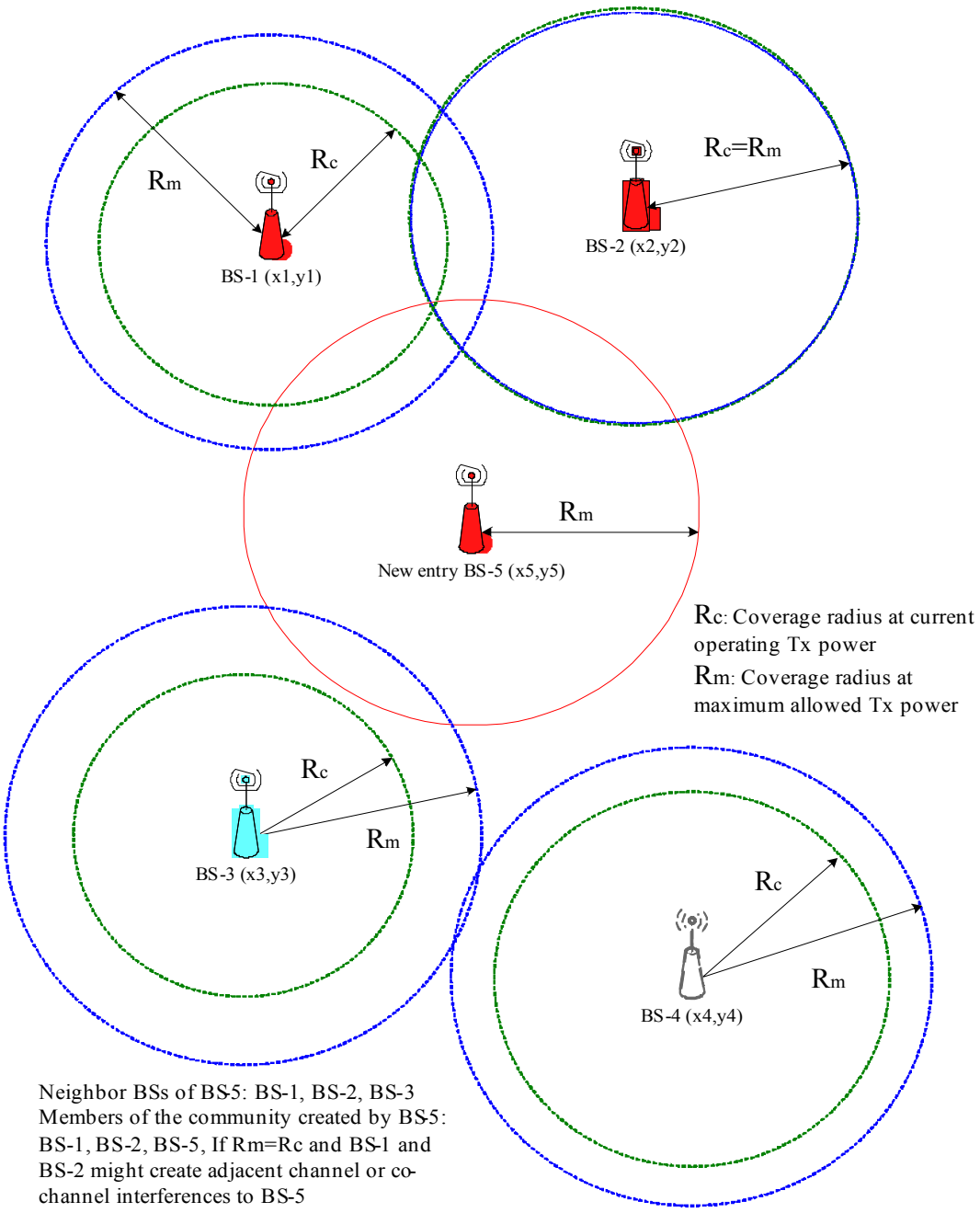
~~Every Base Station also includes a database, called *Shared DB*, open for any other Base Station. The BS data-base contains information necessary for spectrum sharing, and includes the information related to the Base station itself and the associated SSs. A Base Station and the associated SSs form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

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

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

~~explains how one new entry BS discovers its neighbor BSs. The new entry BS-5 uses its GPS coordinates (x5, y5) and its maximum coverage radius, Rm, at allowed maximum transmission power to query the LE DB. A BS is neighbor BS of another BS means their maximum coverages at allowed maximum transmission power overlaps. As depicted, the regional LE DB will return BS-1, BS-2 and BS-3 as the neighbor BSs of the new entry BS.~~

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



802.16 LE Neighbor BSs discovery and definition of neighbor and community

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

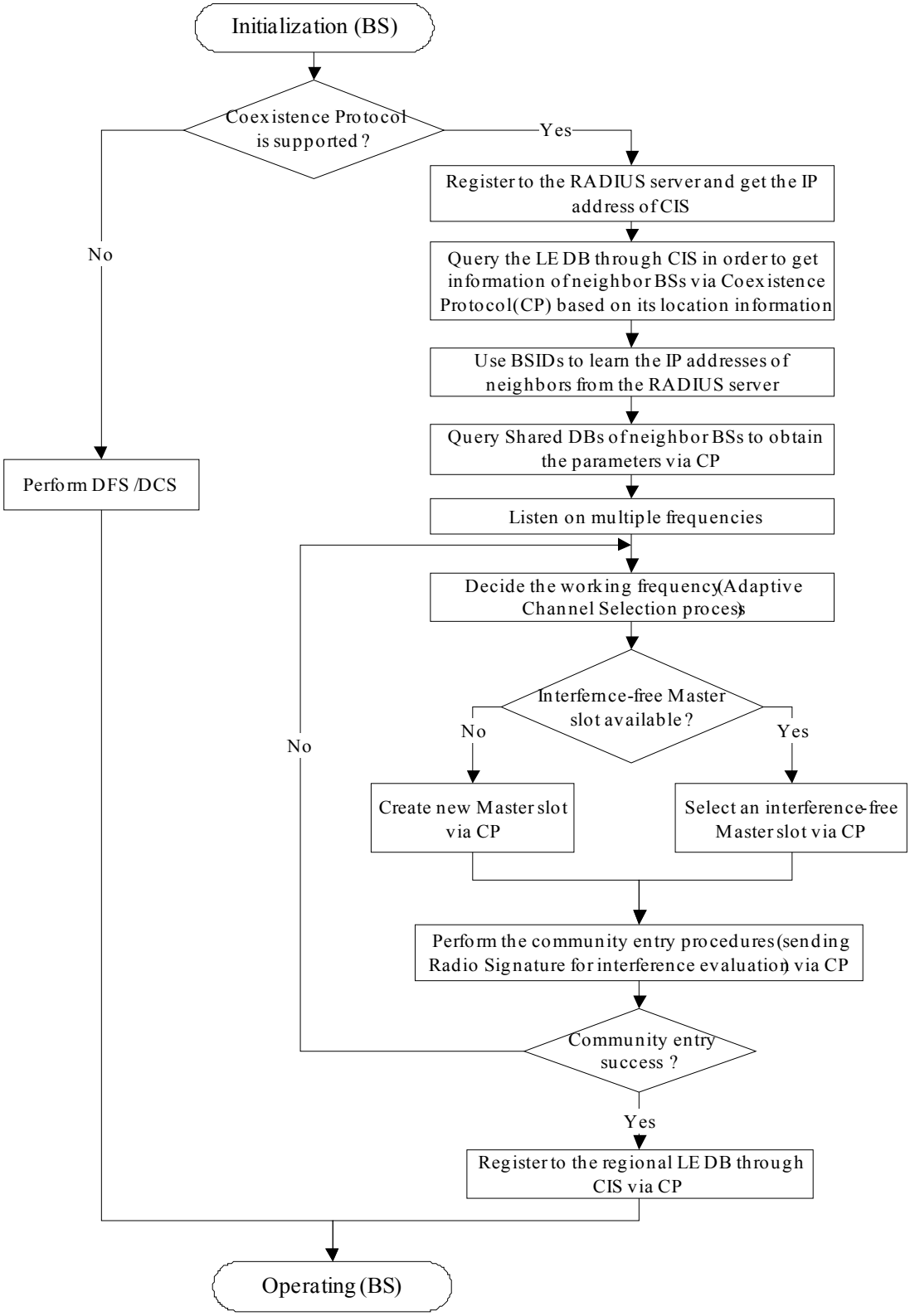
(1) *Initialization stage*

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

(2) *Operating stage*

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

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

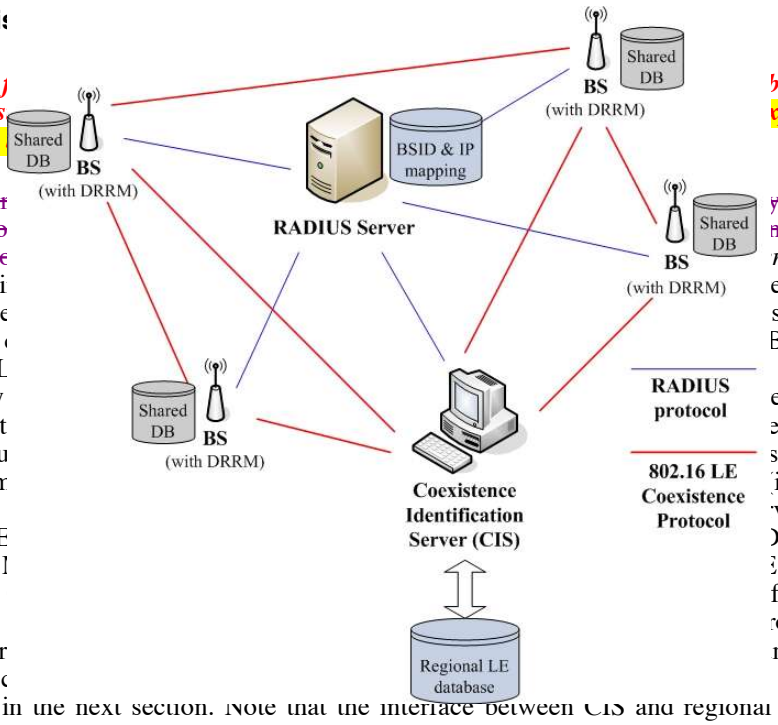


~~Initialization procedures – BS~~

3.2.4.2 Coexis

[Note: The j *bution C802.16h-05/11r1 and is s* *xperts is open to comment on this*

~~The coexistence r~~ ~~y between the LE BSs and the regio~~ ~~ndependent of the database technol~~ *ntification Server* (CIS) acts as an i es the geographic and important ope s belonging to the same region. It BSs to the proper formats, e.g. SQL regional LE DB, which can be any egional LE DB to the proper format e 11~~N6~~ shows the general architectu s architecture, the 802.16 LE system including BS and BS, BS and CIS) ver. CIS acts as a peer of 802.16 LE IUS server as the LE BSs do. The E BSs can use the MAC address of for Encapsulating Security Payload otocol. As shown in ~~figure N6~~Figur mmary, ESP with RADIUS can disc BSs and the CIS will be revealed in the next section. Note that the interface between CIS and regional LE DB is out of scope.



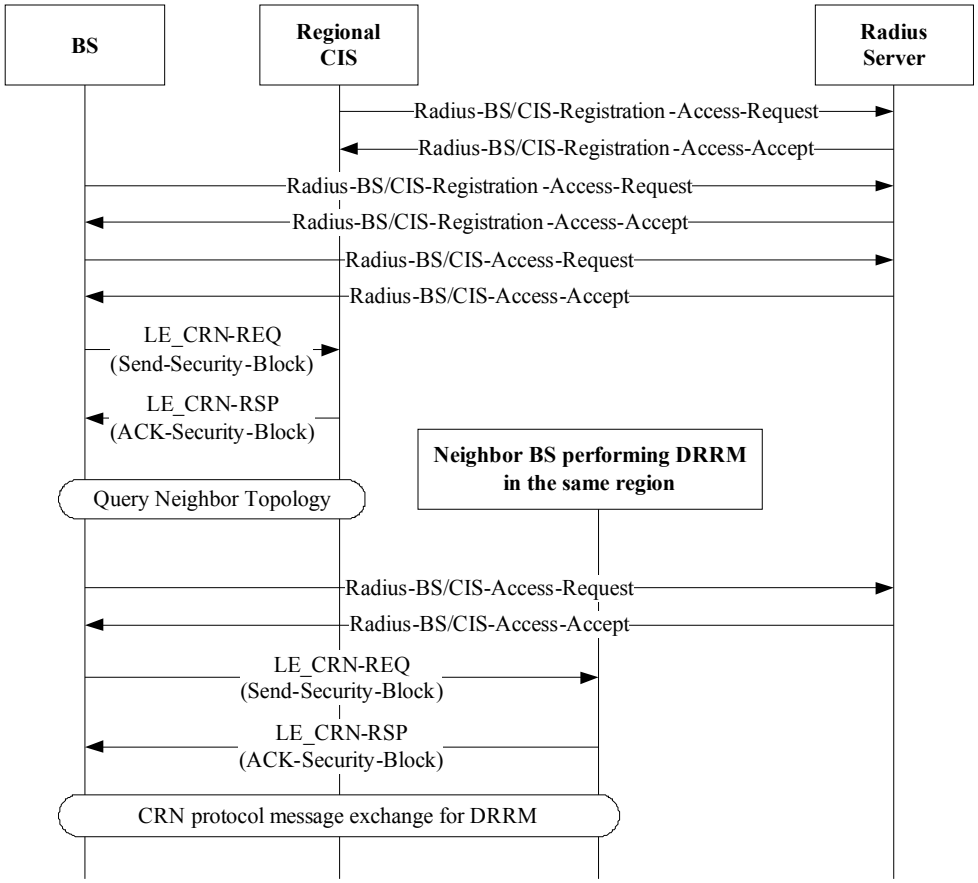
~~General architecture of inter-network communication across 802.16 LE systems~~

3.2.4.3 ~~Security~~

3.2.4.4 RADIUS Protocol Usage

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

For future interoperability consideration, mechanisms similar to [4] ? is proposed. 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/CIS RADIUS client must be configured with the shared secret and with each other's IP address. Each BS/CIS acts as a RADIUS client and has its own shared-secret with the RADIUS server. The shared secret may be different from that of any other BS/CIS.



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

Figure 15 RADIUS protocol example – between BS and RADIUS server

Figure 15 shows the RADIUS protocol message exchange sequence. At starting up, each BS or CIS must send a Radius-BS/CIS-Registration-Access-Request (shown in table 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 CIS:
(a) Wireless medium address of BS (BSID) or medium address of CIS,

(b) RADIUS BSID Secret at least 160 bits in length,
(c) IP address or DNS name, and
(d) Cipher suites supported by the BS or CIS for the protection of CRN protocol communications

RADIUS BSID Secret is used as decryption key for the security parameters, which will be described later. Same as [4], 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/CIS-Registration-Access-Accept message (shown in table B), is used for encrypting the security parameters (named as Security Block, shown in table D2) in the accept message. 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 neighbor topology, it must first send Radius-BS/CIS-Access-Request message (shown in table C) to the RADIUS server in order to acqure the regional CIS's IP address, and also to deliver the ESP Security Blocks necessary for establishing a secure connection with the CIS. The wireless medium addresses of regional CIS, similar to BSID, well known by all BSs supporting LE operation, is sent in the Radius-BS/CIS-Access-Request message to the RADIUS server for looking up IP address of the CIS. Upon receiving the request message, the RADIUS server will respond with a Radius-BS/CIS-Access-Accept message (shown in table D1) if the CIS is a valid member which is allowed to perform inter-communication.

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

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

secret1 = HMAC-SHA1 (null, secret)

secret2 = HMAC-SHA1 (null, secret || secret1)

secret3 = HMAC-SHA1 (null, secret || secret2)

…

…

secretN = HMAC-SHA1 (null, secret || secretN-1)

key = secret1 || secret2 || secret3 || … || secretN

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

The Radius-BS/CIS-Access-Accept message contains two Security Blocks. One is used for the original requesting BS, and the other is used for the neighbor BS or regional CIS performing the inter-communication. Therefore, the first CRN protocol message exchanged between them is of the CRN

message type “Send-Security-Block” sent by the original requesting BS. The second one is of the type “ACK-Security-Block”, sent by the neighbor BS or regional CIS, indicating the correct reception of the security parameters used for the following secure inter-communication.

An access reject message may be issued due to a BS or the regional CIS 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.

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

In this model, data traffic is protected by using IPsec.
The IP Security Protocol [IPsec] ? 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 [IKEv2] ?, but a key and security association (SA) management system with comparable features can be used instead.

4 Interference prevention

4.1 Adaptive Channel Selection – ACS

4.1.1 Between 802.16 systems

4.2 Dynamic Frequency Selection – DFS

4.2.1 Frequency selection for regulatory compliance

5 Pro-active cognitive approach

5.1 Signaling to other systems

5.2 Recognition of other systems

6 Transmission of information

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

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

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

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	*[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]*
Code(opCode???)	8 bits	
(Length of Payload)	??bits	
(AssociationID???)	??bits	
CP Identifier(MessageID???)	8 bits	
TLV Encoded Attributes	*variable*	TLV specific
}		

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	*[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.]*
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
}		

The parameters shall be as follows:

Version of protocol in use

This specification of the protocol is version 1.

Code*(opCode???)*

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 D.

Length of payload

CP Identifier(Message ID???)

The Identifier field is one byte. A BS/CIS uses the identifier to match a BS/CIS 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. The Identifier field in a BS/CIS's CP-RSP message shall match the Identifier field of the CP-REQ message the BS/CIS is responding to.

Association identifier(Association ID)

For uniquely identifying an CP connection between a initiator and responder

Confirmation Code (see *x.xx*)

The appropriate CC for the entire corresponding LE_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 of the MAC PDU header.

Table 4 LE_CP message codes

	CP Message type	MAC Message Type	Protocol type	Direction
0	*Reserved*	—	—	—

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	*reserved*	LE_CP-REQ	UDP	—

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 *x.xx*.

Unknown attributes shall be ignored on receipt and skipped over while scanning for recognized attributes. The BS/CIS 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 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

6.1.1 Send-Security-Block message

The Send-Security-Block packet is sent using the Coexistence Protocol, over TCP and IP. This message is sent from the originated BS who initiates the protocol to the terminated BS/CIS. TCP is used instead of UDP because of its defined retransmission behavior and the need for the exchange to be reliable. The TLV encoded attributes of the Send-Security-Block message carries the security information needed by the terminated BS/CIS to decrypt and encrypt ESP packets.

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

Code: 1

Attributes are shown in Table 6.

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.

6.1.2 ACK-Security-Block message

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

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

Code: 2

Attributes are shown in Table 7.

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.

6.1.3 Neighbor Topology Request message

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

Code: 3

Attributes are shown in Table 8.

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.

6.1.4 Neighbor Topology Reply message

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

Code: 4

Query results of Neighbor Topology Encodings (see *xx.xx*)

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

6.1.5 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 9.

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.

6.1.6 Registration Reply message

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

Code: 6

No Attributes.

6.1.7 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.

6.1.8 Registration Update Reply message

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

Code: 8

No Attributes.

6.1.9 De-registration Request message

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

Code: 9

Attributes are shown in Table 10.

Table 10 De-registration Request message attributes

Attribute	Contents
BSID	The BSID of the request BS.

6.1.10 De-registration Reply message

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

Code: 10

No Attributes.

6.1.11 Add Coexistence Neighbor Request message

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

Code: 11

Attributes are shown in Table 11.

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.

6.1.12 Add Coexistence Neighbor Reply message

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

Code: 12

No Attributes.

6.1.13 Update Coexistence Neighbor Request message

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

Code: 13

Attributes are shown in Table 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.

6.1.14 Update Coexistence Neighbor Reply message

The CIS responds to the BS' to Update Coexistence Neighbor Request with an Update Coexistence Neighbor Reply message.

Code: 14

No Attributes.

6.1.15 Delete Coexistence Neighbor Request message

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

Code: 15

Attributes are shown in Table 13.

Table 13 Delete Coexistence Neighbor Request message attrubutes

Attribute	Contents
BSID	The BSID of the requested BS.

6.1.16 Delete Coexistence Neighbor Reply message

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

Code: 16

No Attributes.

6.1.17 Get_Param_Request message

Messages between BSs, used to request the list of parameters

Code:17

Parameters: list of the BS parameters

6.1.18 Get_Param_Reply message

Messages between BSs, reply to the Get_Param_Request

Code:18

Parameters: list of the BS parameters

6.1.19 Evaluate_Interference_Request message

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

Code:19

Parameters: tbc.

6.1.20 Evaluate_Interference_Reply message

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

Code:20

Parameters: tbc.

6.1.21 Work_In_Parallel_Request message

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

Code: 21

Parameters: tbc.

6.1.22 Work_In_Parallel_Reply message

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

Code: 22

Parameters: tbc.

6.1.23 Quit_Sub_Frame_Request message

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

Code:23

Parameters: tbc.

6.1.24 Quit_Sub_Frame_Reply message

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

Code:24

Parameters: tbc.

6.1.25 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: interfering BSIDs and the frame-number in which the change will take place

Code:25

Parameters: tbc.

6.1.26 Create_New_Sub_Frame_Request message

A message sent in response to the Create_New_Sub_Frame_Request message.

Code:26

Parameters: tbc.

6.1.27 Reduce_Power_Request message

A message between a BS and an interfering BS requesting to reduce the power of the specified transmitter

(identified by frame_number, sub-frame, time-shift) by P dB

Code: 27

Parameters: tbc.

6.1.28 Reduce_Power_Reply message

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

Code: 28

Parameters: tbc.

6.1.29 Stop_Operating_Request message

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

Code: 29

Parameters: tbc.

6.1.30 Stop_Operating_Reply message

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

Code: 30

Parameters: tbc.

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

6.2 RADIUS Protocol Messages

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

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

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

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

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

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]

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	

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

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

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

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

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

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

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

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

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

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	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

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

6.3 Association

An Association ID 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.

6.4 Sequencing and Retransmission

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.)

6.5 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
- All messages received by peer have R bit in flag set to zero
- All responses received by authenticator have R bit in flag set to one.
- Message opCode 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 opCode
- All TLVs within the payload are well-formed, TLVs marked as mandatory are recognized.

6.6 Fragmentation

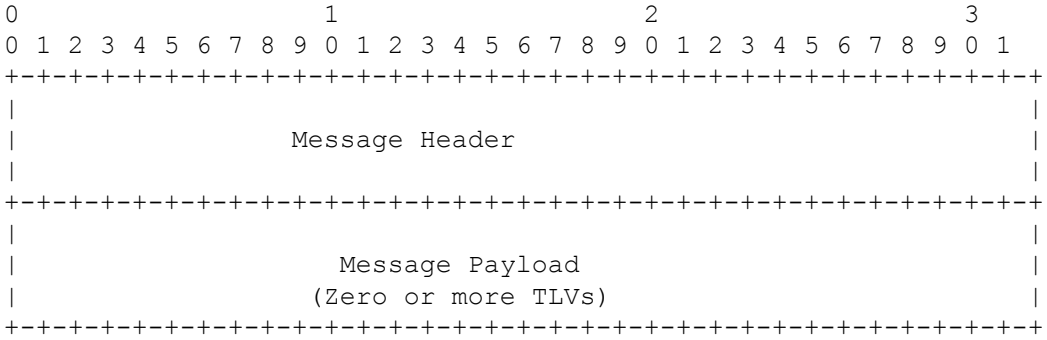
CP does not provide support for fragmentation.

6.7 Transport Protocol

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

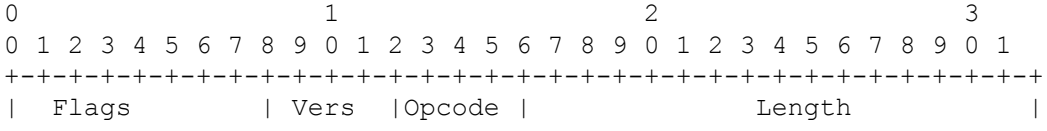
6.8 Message Format

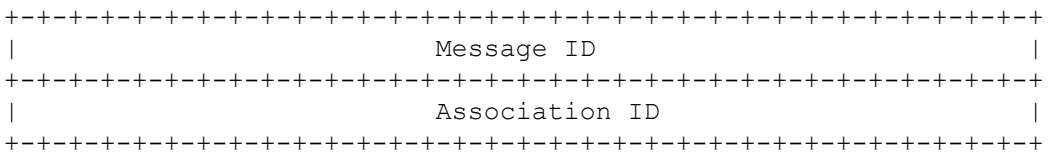
All messages are transmitted in network byte order. The message format has the following structure:



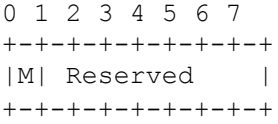
The subsection below describes the format of the header and payload.

6.8.1 Header Format





Flags - 8-bit field indicating options



Response Flag (R).
Set to 1 when message is a response to a request (same message ID). R must be zero in all request messages.
Reserved Flags: Reserved. Must be zero. MUST be cleared on sending and ignored on receipt

Version - 4-bit field indicating the version of this protocol. This specification = 1
OpCode - 4 bit field indicating CP message type
tbc
Length - Length of CP payload in octets excluding header
Message ID - Used to ensure ordered delivery and detect retransmissions.
Association ID - Uniquely identifies association in authenticator and peer.

6.8.2 Payload Format

The payload consists of zero or more type-length-value 3-tuples (TLVs).
Note: TLVs may not always start on a 4-byte boundary.

6.9 Using dedicated messages

6.9.1 Common PHY

6.9.2 Between BS and SS

6.9.3 BS to BS

6.9.4 Connection sponsorship

6.9.5 Using a common management system

6.9.6 Higher layers communication

6.9.7 Decentralized control

6.9.8 Information sharing

6.9.9 IP / MAC address dissemination

7 Common policies

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

7.1.1 Acceptable S/(N+I)

7.1.2 Acceptable time occupancy

7.1.3 Capability of sharing the spectrum

7.2 Interference reduction policies

7.2.1 BS synchronization

7.2.1.1 GPS

7.2.1.2 Ad-hoc

7.2.2 Shared Radio Resource Management

7.2.2.1 Fairness criteria

~~The elements of the fairness criteria are addressed below.~~

7.2.2.1.1 ~~Guaranteed radio resource~~

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

7.2.2.1.2 Power control

Every network will strive to reduce its transmit powers 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 network is operating during its interference-free period. The power control mandatory algorithm will be defined in chap. [t.b.c.]

7.2.2.1.3 Mutual tolerance

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

- The network operating in its interference-free period perceives an interference level equal with the noise level (3dB RSL degradation);

- The network operating in its interference-free period perceives an interference level higher than the noise level (3dB RSL degradation), but explicitly agrees to operate at the created interference level; this may be the case of a small cell size or reduced traffic

- If the interference level is higher than the acceptable level, the master network may request the links operating in parallel to reduce their transmitting powers; if such a link enters the situation that will not be able to operate anymore, the link transmitter will have to operate in another sub-frame in which will not cause harmful interference.

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

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

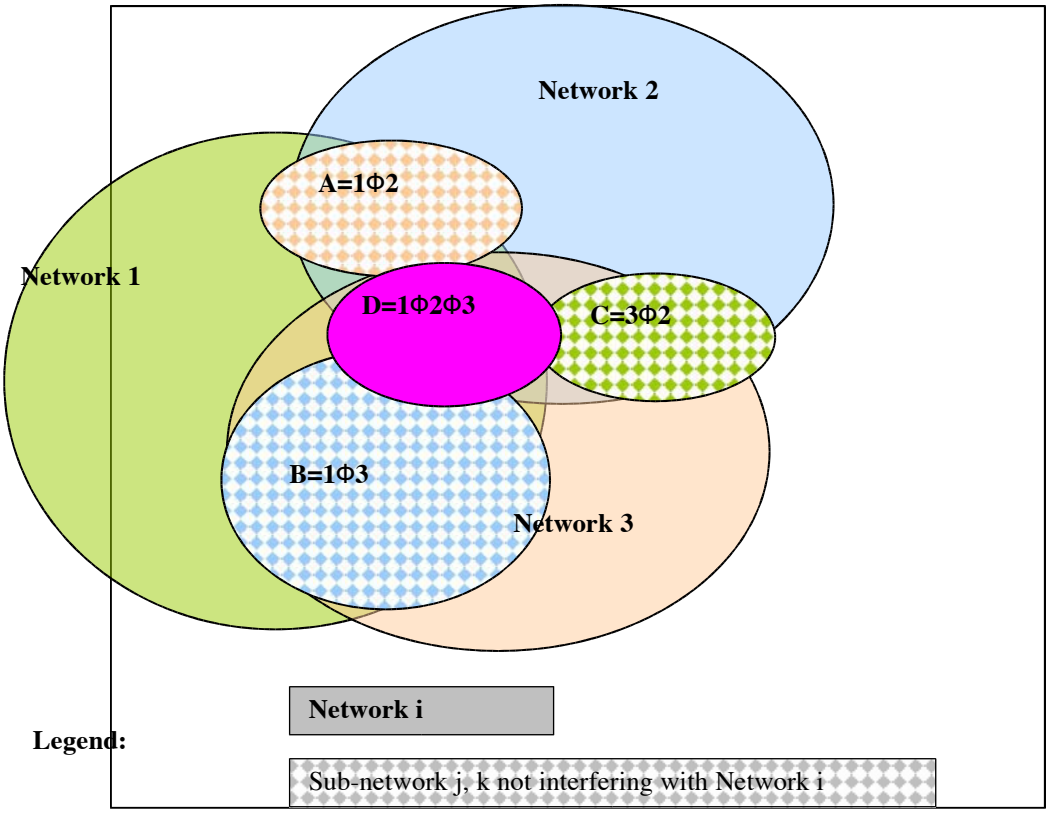


Figure 16 – Interference due to overlapping networks

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

Networks 1,2,3 do not interfere

Zone A: Networks 1 and 2 interfere

Zone B: Networks 1 and 3 interfere

Zone C: Networks 3 and 2 interfere

Zone D: Networks 1 and 2 and 3 interfere

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

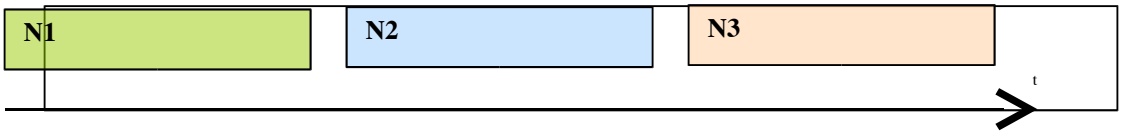


Figure 17 – Equal splitting of radio resource between networks

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

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

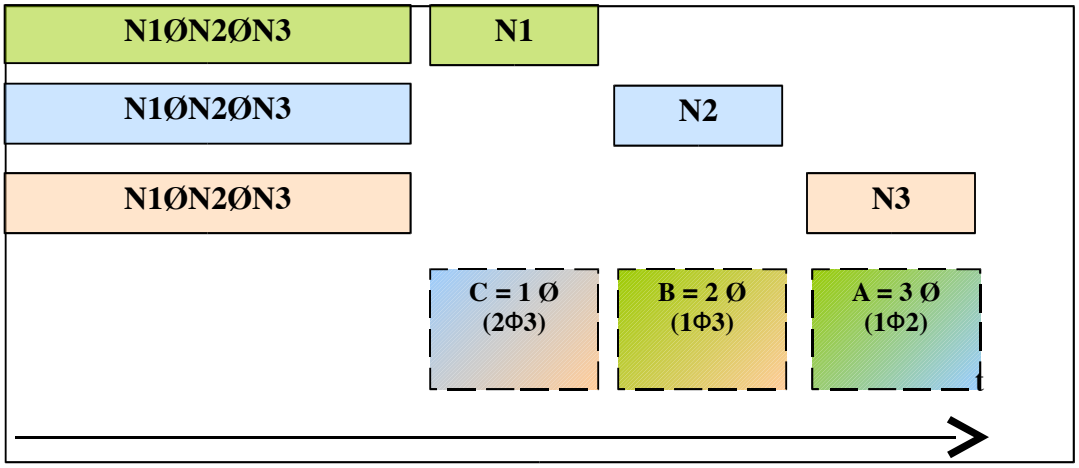


Figure 18 Usage of the spectrum by every system

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

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

7.2.2.1.3.1 Cooperation with other networks

A network may need more time 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 network may request from one or more adjacent networks to reduce their interference free transmission intervals. The other networks will consider the request, and when possible will accept the request, by indicating the agreed new interference-free operating interval. The duration of each sub-frame may be negotiated through inter-network communication and using the common DRRM policy.

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

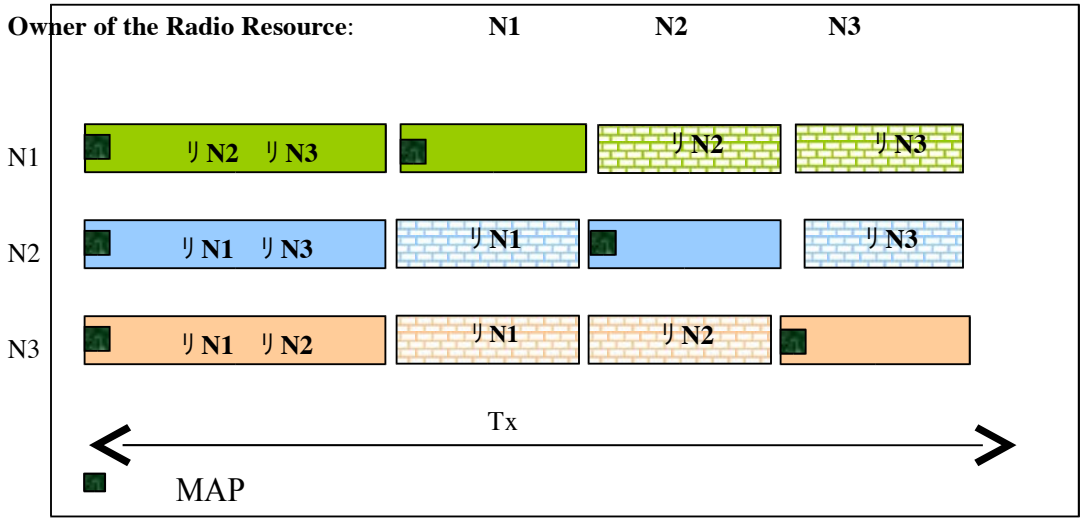
A number of scheduling approaches may be considered, some of them being presented below, for Tx synchronized intervals. Same approach is valid for Rx intervals.

7.2.2.1.3.2.1 Sharing same MAC Frame

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

~~The advantage of this approach is that allows flexibility in changing the duration of different sub-frames, to use the radio resource in accordance to traffic load or interference level.~~

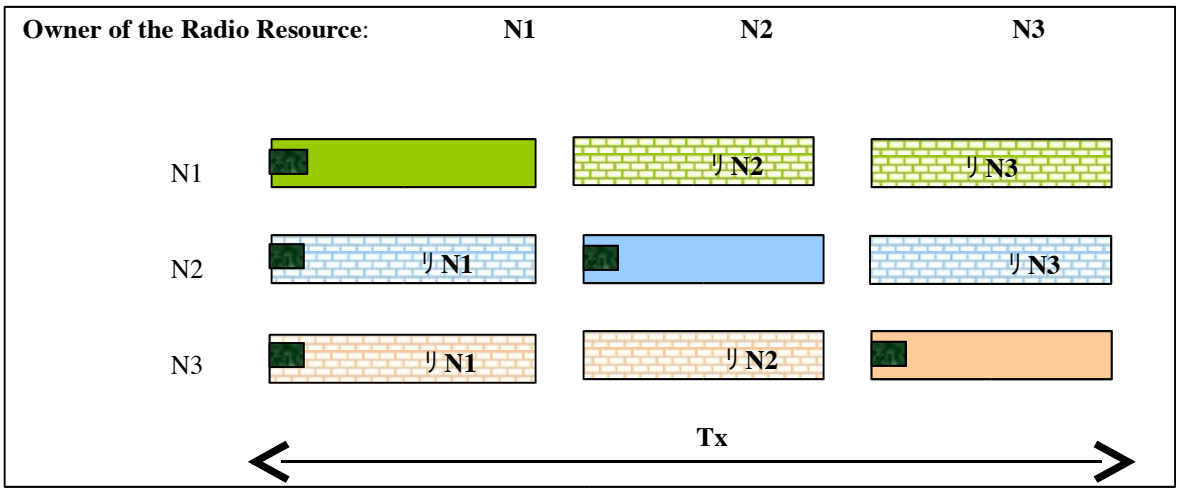
~~The possible traffic scheduling is presented in fig. 4. If, for example, the common sub-frame has a reservation of 40% of Tx duration and all the other sub-frames are 20% each, the maximum time-frame to be used is 80%.~~



~~Figure 19 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.~~



~~Figure 20 Sharing same MAC frame – alternative mode~~

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

7.2.2.1.3.2.3 Repetitive sharing approach

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

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

The advantage of this scheduling mode are:

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

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

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

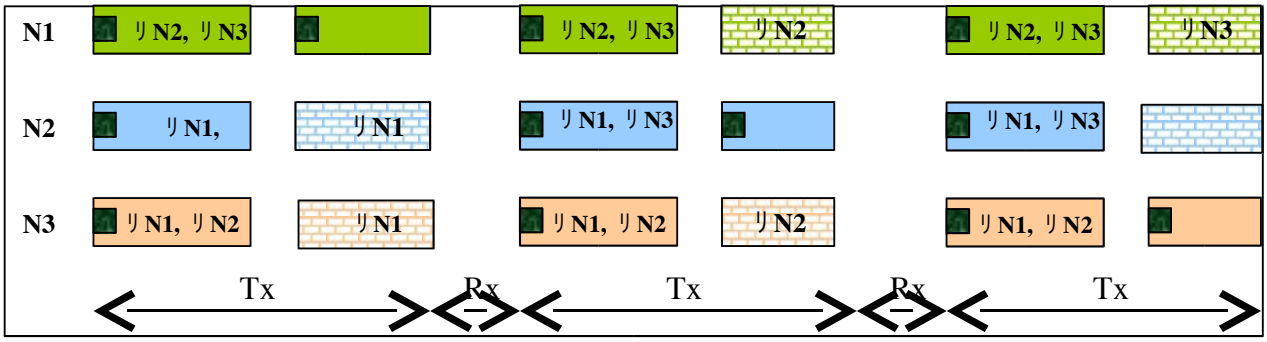


Figure 21 - Repetitive scheduling

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

7.2.2.2 Distributed scheduling

7.2.2.2.1 Assignments

7.2.2.3 Distributed power control

7.2.2.4 Distributed bandwidth control

7.2.2.5 Beam-forming

7.2.2.6