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

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

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, *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

BSIS Base Station 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
PSD power spectrum density

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 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*
- The local Radio Administration may use, for light licensing procedure, its own database, generally notincluding the Base Station ID and IP identifier information.
- There is a Server that manage the write/reading of this Data Base, using the 802.16h standardized procedures including secure access procedures; the Server and the country/region data base can be hostedby one of the operators or a trusted entity, like the local Radio Administration.
- 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 Figure12);
- 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.
- 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
- ***Neighbor BSs:*** *The base stations that have valid SSs in the common coverage area are called neighbor BSs, and shall form a neighborhood.*
  There are 2 basic conditions to form a neighborhood:
  1) Common coverage area: base stations need to be close enough in geography;
  2) Valid SSs exist in the common coverage area: When SS transfer data with one BS at a time, it shall consider other BSs as an interference source at the same time.
  Neighbor Networks: *Neighbor BSs & their SSs are called Neighbor Network, and shall form a network neighbor hood.*

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.

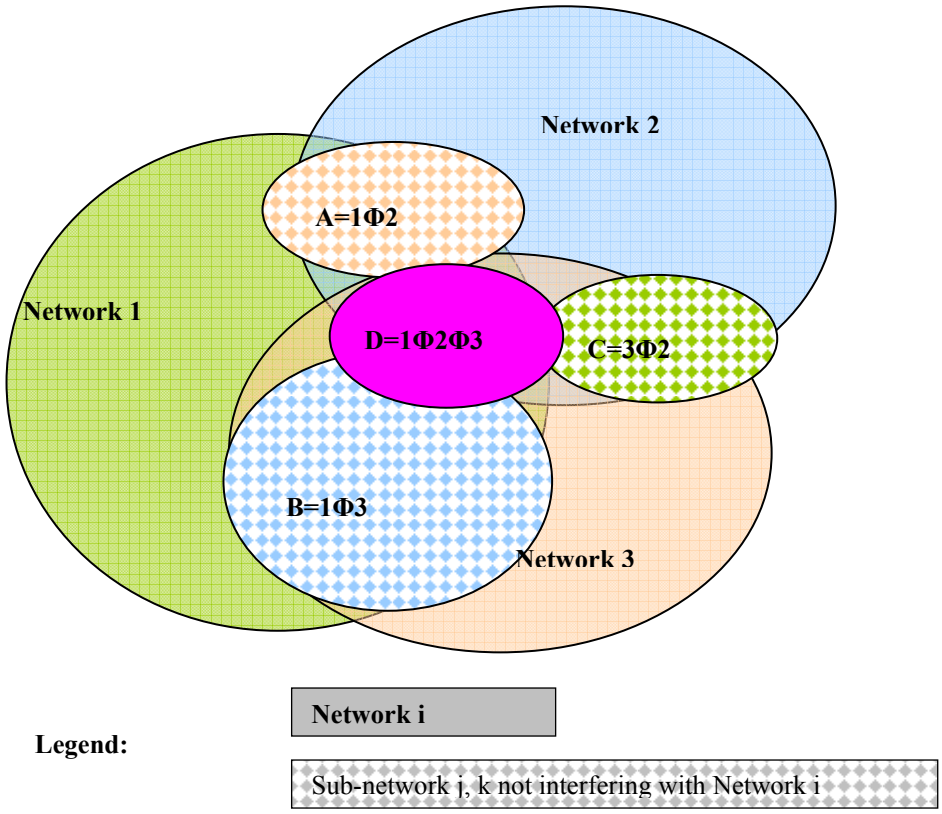


Figure 1. Interference due to overlapping networks

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.

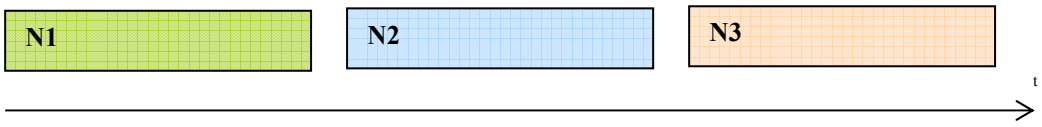


Figure 2. Equal splitting of radio resource between networks

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.

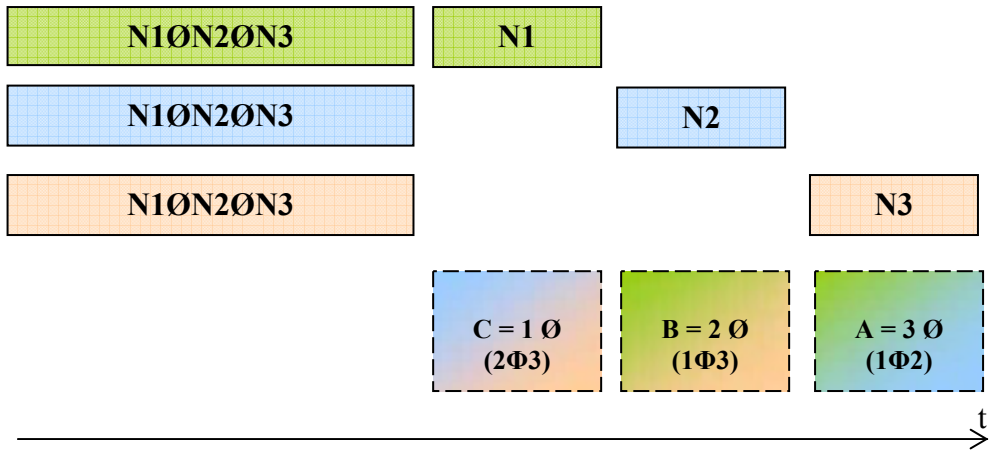


Figure 3. Usage of the spectrum by every system

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.

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

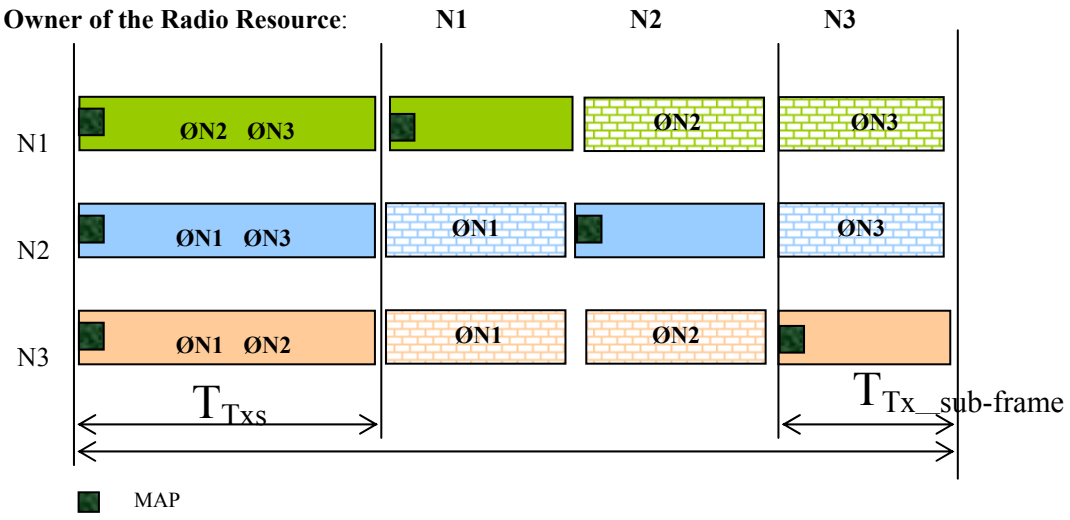


Figure 4. Sub-frame structure type1

- for type 2:
  - $T_{Tx\_sub\text{-}frame} = T_{TxMAC} / N$
  - $T_{Rx\_sub\text{-}frame} = T_{RxMAC} / N$

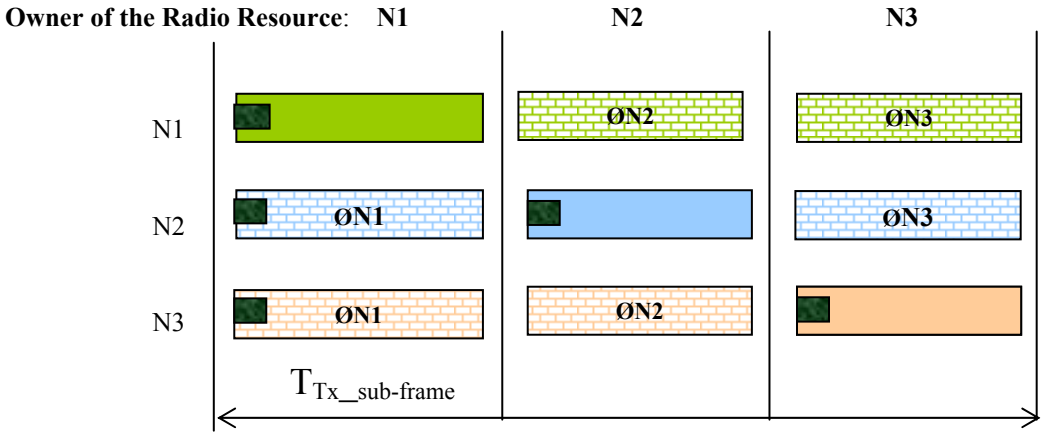


Figure 5. Sub-frame structure type 2

- 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 = $N*T_{MAC}$,

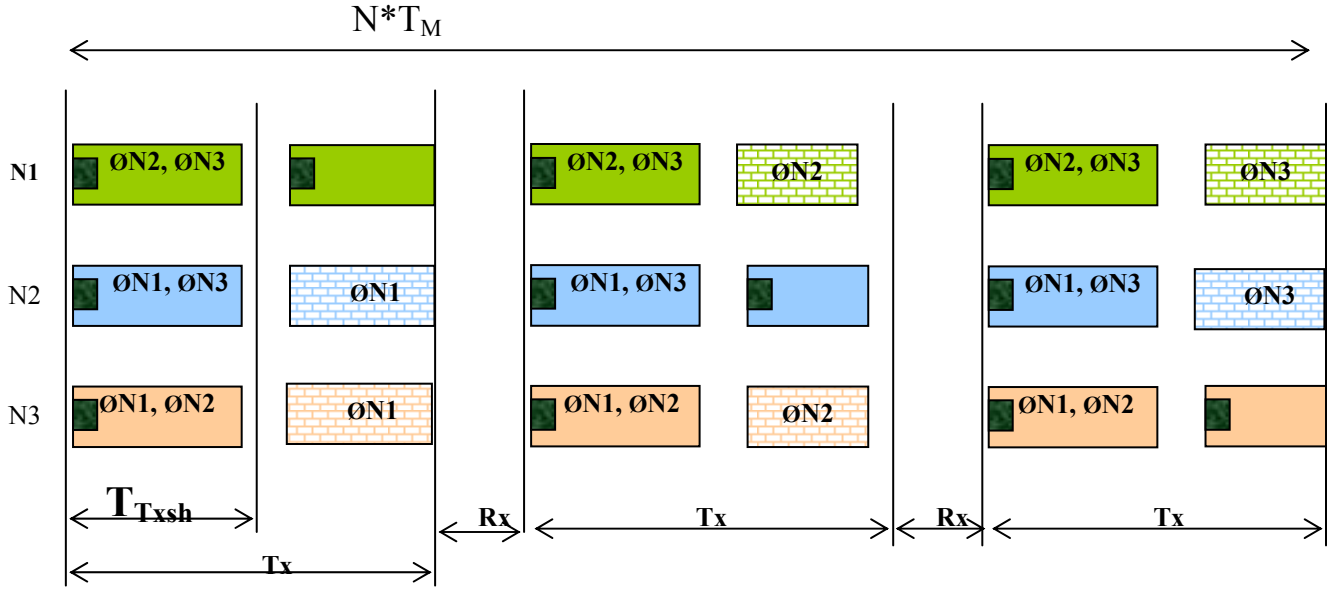


Figure 6. Sub-frame structure type 3

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" 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.

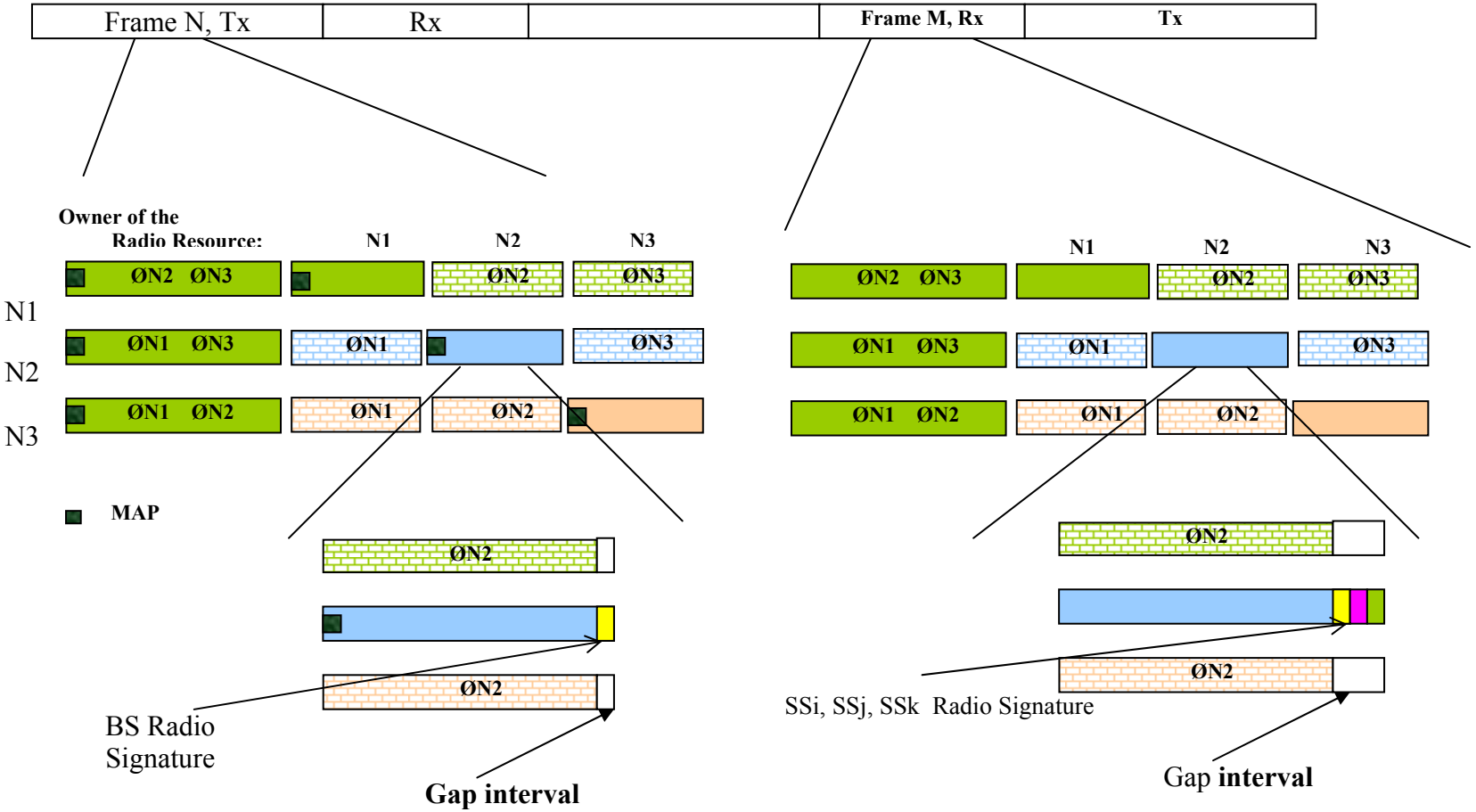


Figure 7. Allocation of slots for BS and SS radio signature

- 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.
  - BS power relative to radio-signature, in the used sub-frames, in the interval between two Master subframes;
  - For every active SS: SSID and its attenuation relative to radio-signature power, in the used subframes,in the interval between two Master sub-frames;

Coexistence Time Slot

CTS (Coexistence Time Slot): a predefined time slot for the coexistence protocol signaling purpose, especially for the initializing BS to contact its neighbor operating BS through the SS in the common coverage area.

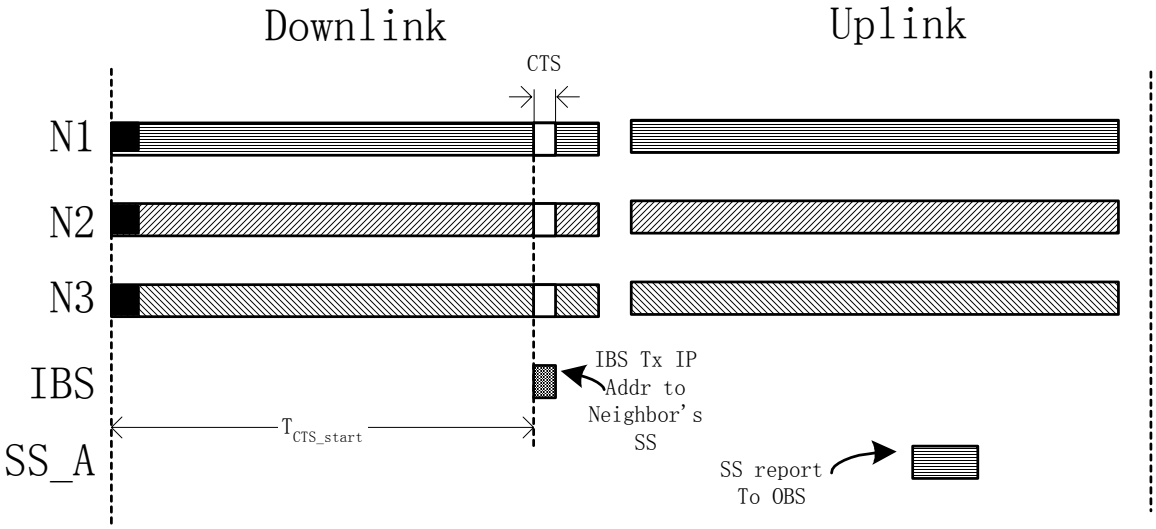


Figure 8. Timing of Coexistence Time Slot

CTS must not be used for other purpose by all the BSs, so that it will be an interference free slot for the neighbor discovery purpose. Initializing BS (IBS) shall use this slot to broadcast its IP identifier, so that the neighbor operating BS (OBS) could find the new neighbor in IP network after the SS report the message. Then the IBS and OBS begin further negotiation for coexistence protocol.

The broadcasting procedure is unidirectional, only from the IBS to the SSs in IBS's coverage, and the SSs shall report all the useful information to their OBSs they registered to. If the message be forward correctly to the OBSs, the OBSs will then find the IBS in the IP network, and go further signaling using IP network.

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

TCTSstart： CTS starting time from the beginning of the frame (ms)
TCTSdurat：CTS duration time (ms)
NCTSstart：CTS starting frame number（ frames）
NCTSintv： CTS interval frames（frames）

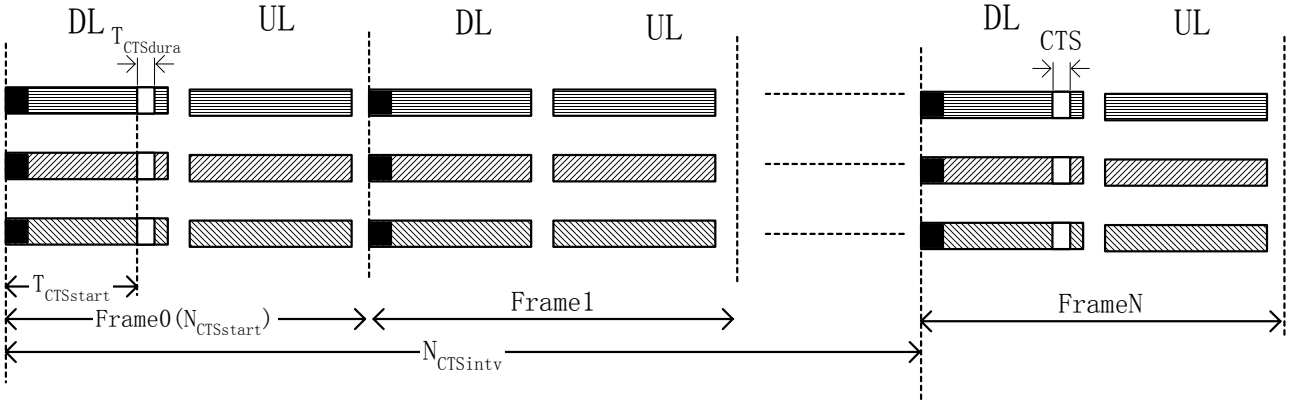


Figure 9. CTS parameters

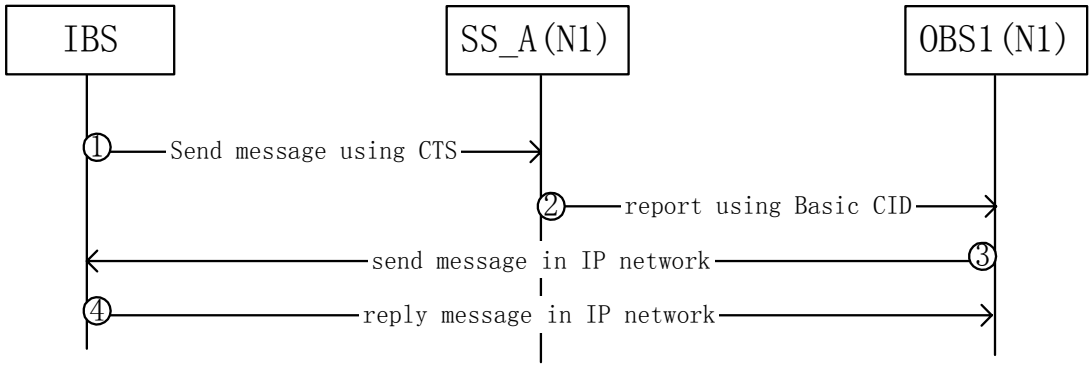


Figure 10. CTS usage example- IBS broadcasting IP address to neighbor's SS

2.1.2 Interference Control

- Interferer identification
  - 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

Figure11 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 in LOS, Rm, at allowed maximum transmission power. A BS is neighbor BS of another BS if:

- In co-channel operation the LOS maximum coverage area resulting for the allowed maximum transmission power overlaps one with each other. As depicted in Figure11,the regional LE DB will return BS-1, BS-2 and BS-3 as the neighbor BSs of the new entry BS.

- in first or alternate adjacent channels operation, the BS should consider the attenuation of the transmitted power, corresponding to the actual operation channels of different Base Stations

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. The Adaptive Channel selection will select the actual operating frequency, such that the probability of interference will be minimized. Each LE BS tries to form its own community. By including the neighbor BSs that might create interferences to the associated SSs The members of community will change when the working frequency of any BSs changes or new interfering neighbor BS comes in.

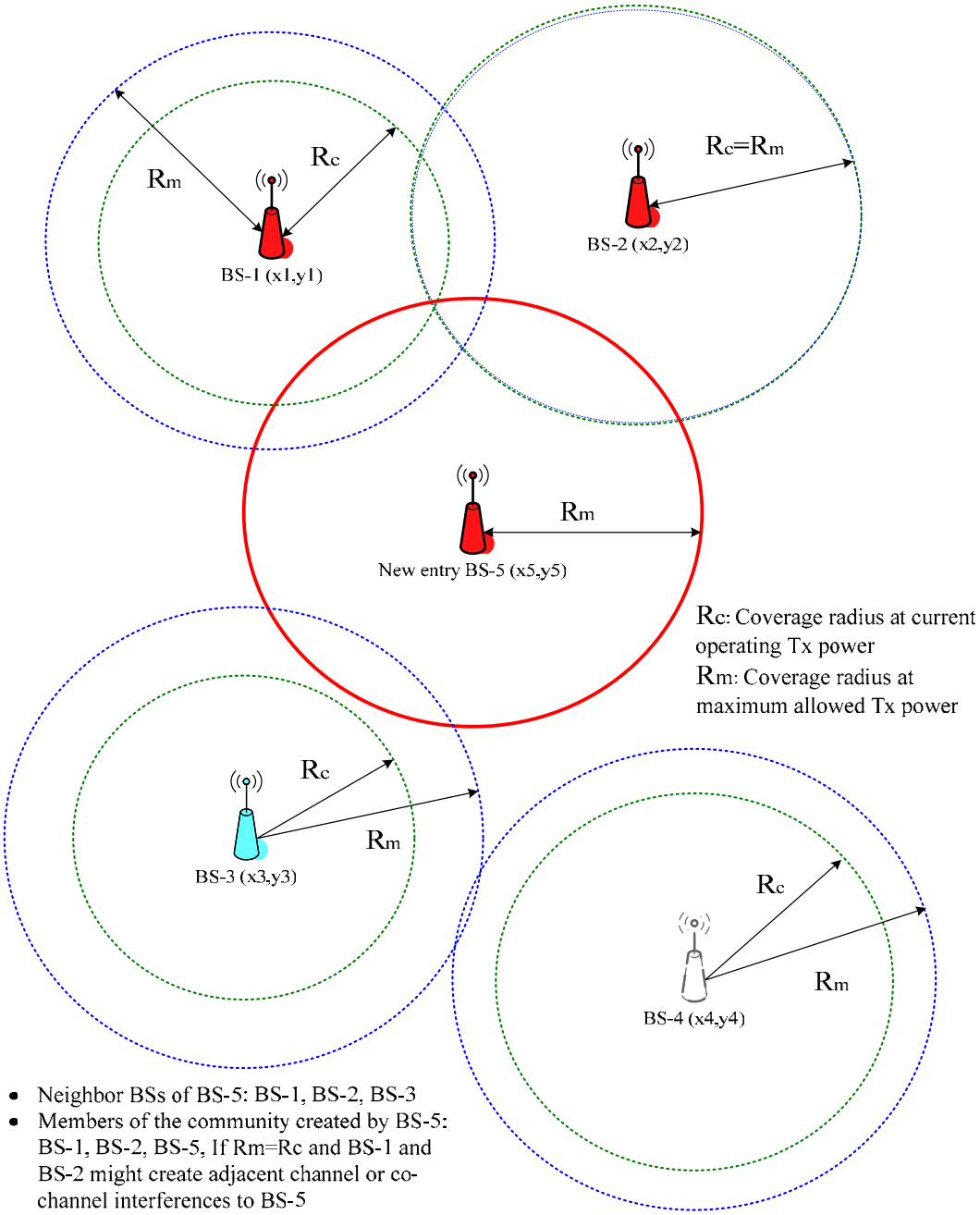


Figure 11. 802.16 LE Neighbor BSs discovery and definition of neighbor and community

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 inFigure12. 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]

Figure12 shows the 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.

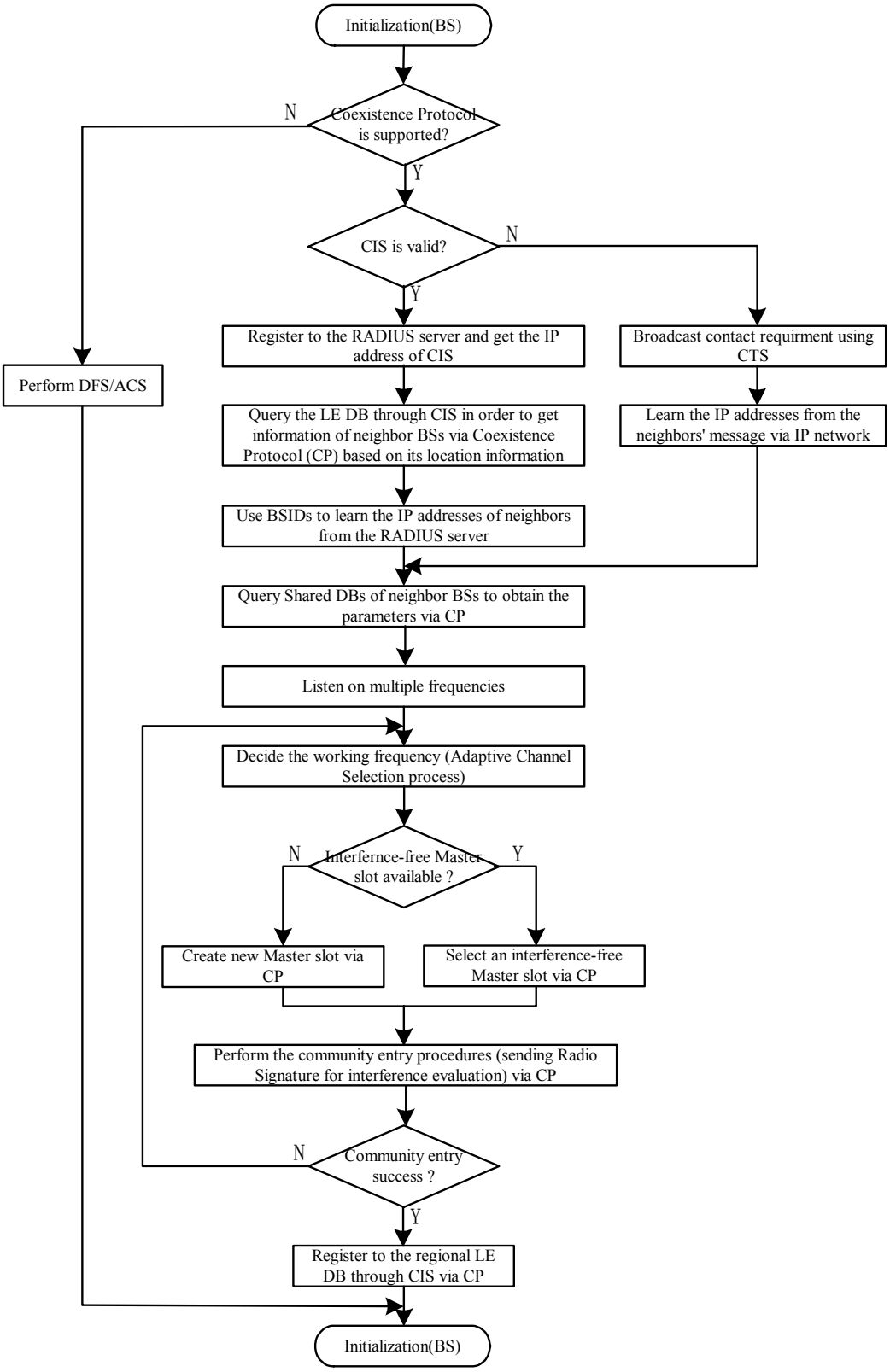


Figure 12. Initialization procedures — BS

- *The first phase of the Community Entry is to judge the validity of country/region data base. If the country/region database is valid, 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;

  Otherwise:
  - *New BS uses the interference free slot to broadcast the contact request*
  - *The SS in the common coverage will forward the information to its operating base station.*
  - *The operating neighbor BS send feedback information using IP network*
  - *learn the IP identifier By the message from neighbor BS via IP network*
- 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 Controlling interference during not-interfering traffic sub-frames

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

- BS power, relative to the radio signature power, when using each of the sub-frames;

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

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

2.1.10 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.]

2.1.11 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:[editorial note: add 2 lines between shareDB to DRRM BS]

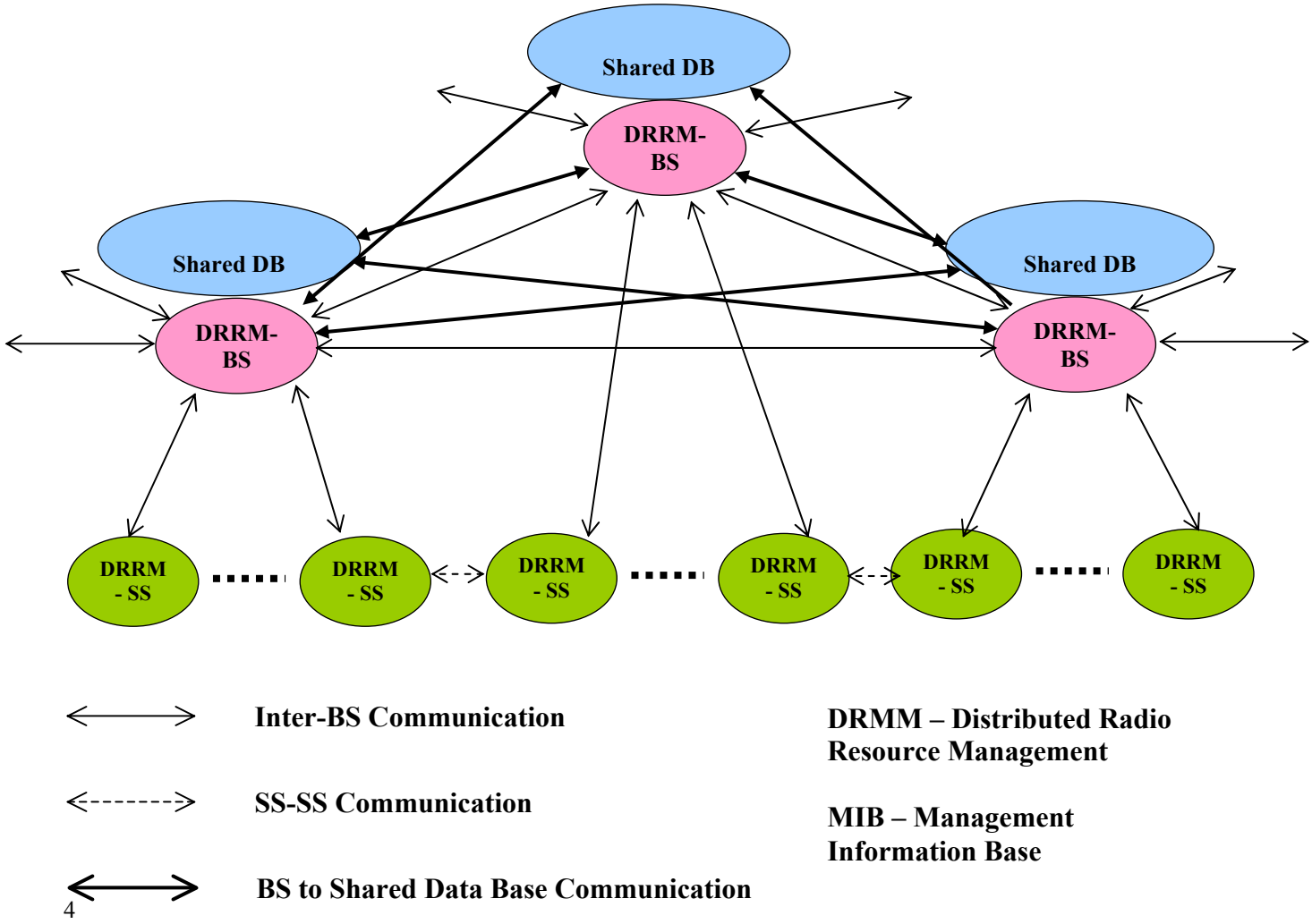


Figure 13. System Architecture

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

Figure14 shows the IEEE 802.16 LE inter-network communication architecture:

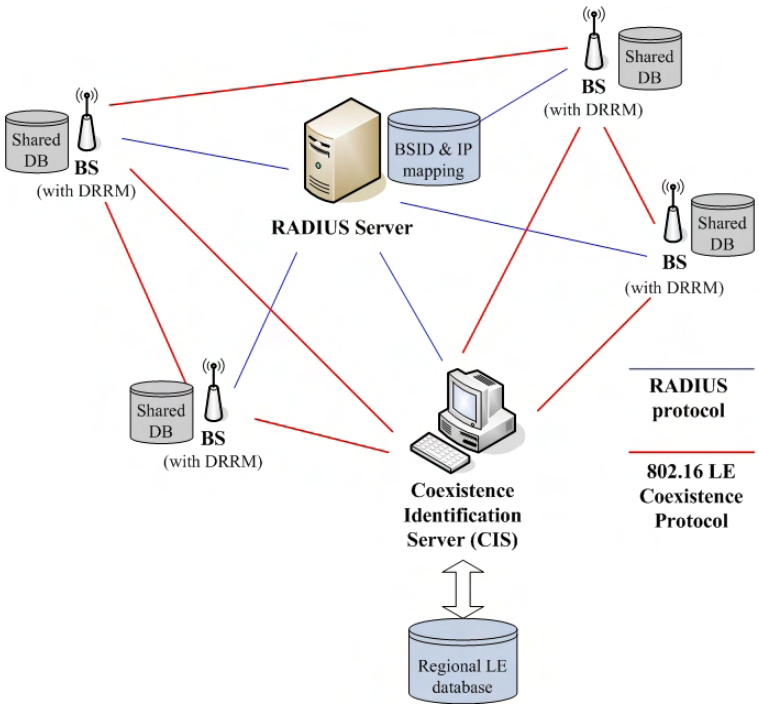


Figure 14. Network Architecture

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

- The RADIUS Server- The Base Station Identification Server (BSIS), described in detail in section xxx - The BSs cooperating with the Distributed Radio Resource Management (DRRM) procedure

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

BSIS maintains the geographic and operational information such as latitude, longitude and the BSID of LE BSs. BSs operating under LE system shall first query the BSIS and find the neighbor BSs while starting up, following the Coexistence Resolution and Negotiation (CRN) protocol (detailed description in section *x.x.x*). After the successful query procedure, the BS can obtain the BSIDs of the neighbor BSs. Intercommunication between BSs belonging to different networks is permitted after the BS acquires coexisting neighbor's authentication key and encryption key for ESP 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. will be used a Coexistence Protocol (CP). Figure15 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. Figure16is 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, Figure17 is the BSIS architecture with co-located regional LE database. Other architectures are not being illustrated. The Coexistence Protocol services are accessed by the LE Management Entity through CP SAP. The service primitives are described in t.b.d A BS uses the Coexistence Protocol, which is similar to PKM protocol, to perform the coexistence resolution and negotiation procedures. There are two types of messages to support Coexistence Protocol:

(1) LE_CP-REQ: BS→BS or BS→BSIS

(2) LE_CP-RSP: BS→BS or BSIS→BS

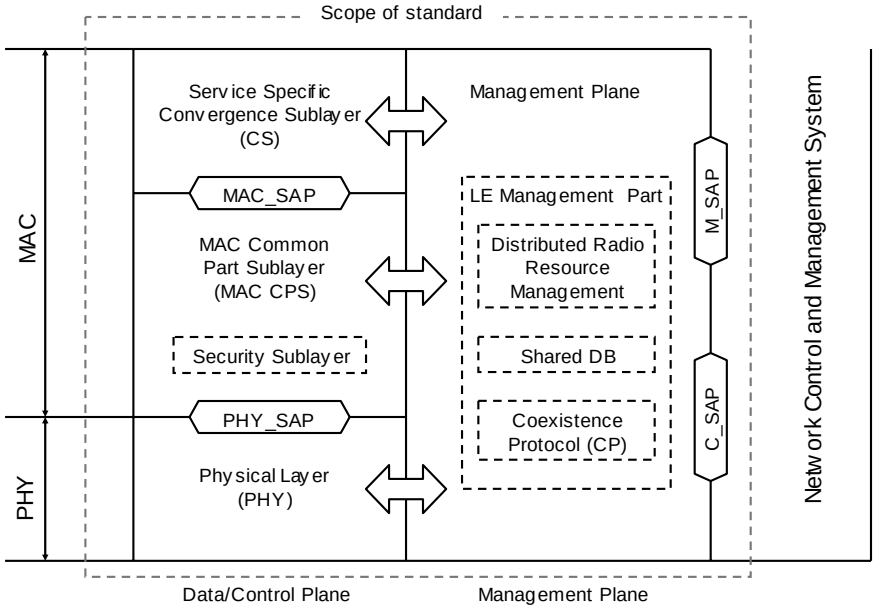


Figure 15. 802.16h BS Protocol architecture Model

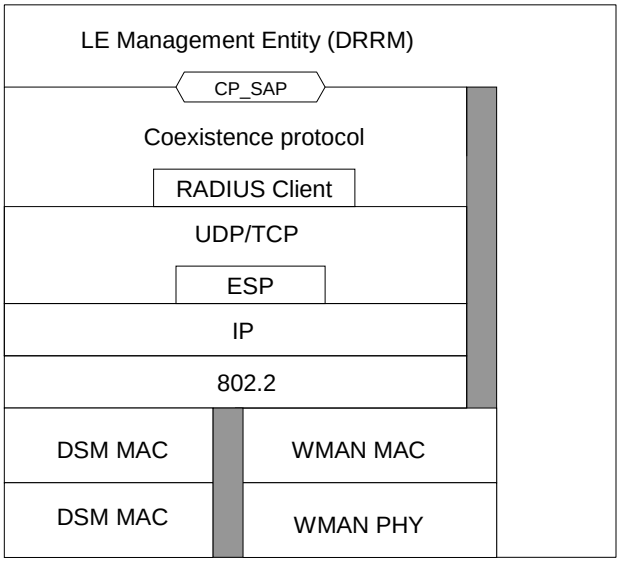


Figure 16. LE BS architecture with Coexistence Protocol

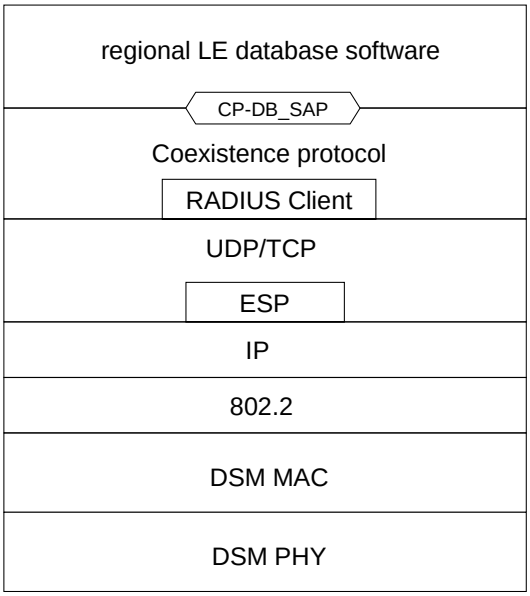


Figure 17. BSIS architecture with co-located regional LE database

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

Before any data can be exchanged between BS and BS/BSIS, security association must be setup first. IEEE 802.16 LE security associations between peers are established through RADIUS server. Any BS wants to communicate with another BS or BSIS shall first send a *RADIUS Access-Request* to request the establishment of the security association between originated BS and terminated BS/BSIS. RADIUS server replies a *RADIUS Access-Accept*, which includes security information for ESP operation, to the BS. At this point, only *virtual* security association is established between the peers. The BS sends the Security Block for the peer, which it received from the RADIUS Server, as a 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 BSIS. 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 BSIS.

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 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.

2.2.3.2 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 approach

3 Interference victims and sources

3.1 Identification of the interference situations

3.1.1 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.

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

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

Note: overlapping chapter

3.2.4.1 Base Station Identification Server

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

The *Base Station Identification Server* (BSIS) acts as an interface between 802.16 LE BSs and the regional LE DB which stores the geographic and important operational information, e.g. latitude, longitude, BSID etc., of the LE BSs belonging to the same region. It converts the actions carried in PDUs received from the 802.16 LE BSs to the proper formats, e.g. SQL (Structured Query Language) string, and forwards the strings to the regional LE DB, which can be any available database software. BSIS converts the query results from the regional LE DB to the proper format, e.g. TLV encodings, and replies to the requested BSs. Figure14 shows the general architecture of inter-network communication across 802.16 LE systems. In this architecture, the 802.16 LE systems (BSs and BSIS) from different networks set up security association (including BS and BS, BS and BSIS) with each other by utilizing the services provided by the RADIUS server. BSIS acts as a peer of 802.16 LE BSs in this architecture, therefore, it also needs to register to the RADIUS server as the LE BSs do. The MAC address of BSIS is well known among the LE operators. The LE BSs can use the MAC address of BSIS, which may be provisioned, to acquire the IP address and keys for Encapsulating Security Payload (ESP) (RFC2406:1998) operation of the BSIS by utilizing RADIUS protocol. As shown inFigure14, the RADIUS server maintains the BSID and IP mapping. In summary, ESP with RADIUS can discover a Rogue BS or BSIS. The messages exchanged between the LE BSs and the BSIS will be revealed in the next section. Note that the interface between BSIS and regional LE DB is out of scope.

3.2.4.2 RADIUS Protocol Usage

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

Secure exchange of 802.16 LE signaling information can be achieved after successful procedures of the RADIUS protocol. To include RADIUS support, the RADIUS server and the BS/BSIS RADIUS client must be configured with the shared secret and with each other's IP address. Each BS/BSIS 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/BSIS.

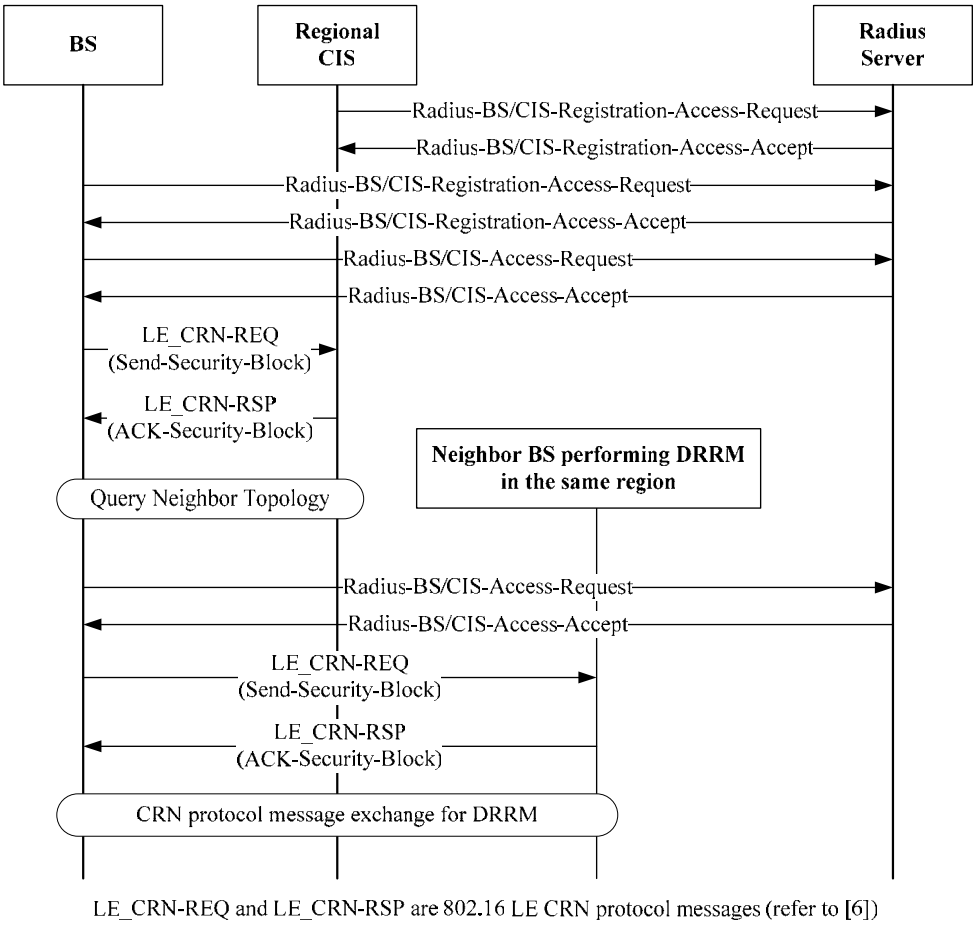


Figure 18. RADIUS protocol example – between BS and RADIUS server

Figure18 shows the RADIUS protocol message exchange sequence. At starting up, each BS or BSIS must send a Radius-BS/BSIS-Registration-Access-Request (shown inTable14) to the RADIUS server for authentication purpose and leave the address mapping (BSID to IP) information in the server. At this time, the RADIUS server will retain the following information of registered BS or BSIS:

(a) Wireless medium address of BS (BSID) or medium address of BSIS,
(b) RADIUS BSID Secret at least 160 bits in length,
(c) IP address or DNS name, and
(d) Cipher suites supported by the BS or BSIS 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/BSIS-Registration-Access-Accept message (shown inTable17), is used for encrypting the security parameters (named as Security Block, shown inTable4) 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/BSIS-Access-Request message (shown inTable3) to the RADIUS server in order to acqure the regional BSIS's IP

address, and also to deliver the ESP Security Blocks necessary for establishing a secure connection with the BSIS. The wireless medium addresses of regional BSIS, similar to BSID, well known by all BSs supporting LE operation, is sent in the Radius-BS/BSIS-Access-Request message to the RADIUS server for looking up IP address of the BSIS. Upon receiving the request message, the RADIUS server will respond with a Radius-BS/BSIS-Access-Accept message (shown inTable4) if the BSIS is a valid member which is allowed to perform inter-communication.

After succeeded query process between the BS and the regional BSIS the BSIS 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/BSIS-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/BSIS-Access-Accept messages is authenticated using the ESP authentication algorithm (indicated from the previous Radius-BS/BSIS-Registration-Access-Accept messages) and encrypted/decrypted using the ESP transform cipher (also indicated from the previous Radius-BS/BSIS-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 BSIS, or BS and BS.

The Radius-BS/BSIS-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 BSIS 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 BSIS, 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 BSIS 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

[*Note: the cognitive signalling may have effect on the power amplifier and on the PAPR. Call for contribution to investigate if there are any such effects.*]

5.1.1 Ad-hoc systems - operating principles using Cognitive Radio signaling

In order to reduce the interference situations, in deployments in which may exist a combination of 802.16 systems using a Coexistence Protocol and 802.16 ad-hoc systems, the 802.16 ad-hoc systems will apply the Adaptive Channel Selection procedures and use cognitive radio signaling procedures to interact with systems wising a Coexistence Protocol. The ad-hoc systems obtain a temporary Community registration status, that has to be renewed from time to time.

5.1.2 Registration

The 802.16h pro-active cognitive radio approach defines signals and procedures for the reservation of the activity intervals and registration of ad-hoc systems. The operational procedures are described below:

- 802.16h Community registered systems, using a Coexistence Protocol, will reserve the MAC frame Tx/Rx intervals by using, during the MAC Frame N, cognitive signals to indicate the MAC Tx_start, MAC Tx_end, MAC Rx_start, MAC Rx_end. These signals are transmitted by Base Stations and Repeaters. The specific MAC frame N is indicated in the BS data-base and these procedures will repeat after Ncogn MAC frames;;
- During the MAC frame N+1, cognitive signals will indicate the beginning and the end of Master sub-frames, by transmitting signals indicating by their transmission start the Tx_start, Tx_end, Rx_start, Rx_end for the specific sub-frame; these signals are transmitted by Base Stations, Repeaters and those SSs which experiences interference, at intervals equal with N_{cog} MAC Frames;
- During the MAC frame N+2, will be indicated the position of the time-slots, in each Master sub-frame, to be used starting with the MAC Frame N+3 for registration using cognitive signaling. The start of the "Rx_slot" signal will indicate the start of the slot.

- The start of the MAC frame N+4 is the start of a registration interval using the cognitive signaling; the registration interval has the duration of $T_{cr\_reg\ seconds}$;
- The ad-hoc transmitters shall use during the MAC frame N+4, the marked slot for sending their radio signature. The radio signature will be used for the evaluation of the potential interference during the Master slot, to systems which use the sub-frame as Master systems.
    - An ad-hoc radio unit (BS, Repeater or SS) will send this signal using a random access mode for T_{cr_reg1} seconds, using the sub-frame intended for their regular transmission (BSs and SSs use different sub-frames for transmission).
    - The ad-hoc transmitters will have to use the registration procedures every T_{ad_reg} seconds.
  - Registration replay
    - The radio units using the Master sub-frame will send a NACK signal, to be sent in a random mode during the next $T_{cr\_reg\_ack}$ seconds, if they appreciate that the ad-hoc transmitter will cause interference. Typically, to a registration signal sent during a DL sub-frame, the NAK will be sent by one or more SSs, while to a registration signal sent during UL sub-frame, the NACK signal will be sent by a Base Station. The radio units using the Master sub-frame will send their response in random mode.
    - The NACK signal indicates that the requesting ad-hoc device cannot use the specific sub-frame, while using the requesting radio signature
      - Same device may try again, if using a different radio signature (for example, lower power).
    - Lack of response, for $T_{cr\_reg\_ack}$ seconds, indicates that the registration is accepted for transmission during the specific sub-frame.

5.1.3 Selection of suitable reception sub-frames

An ad-hoc unit will find his suitable reception sub-frames, by using the ACS and Registration process in a repetitive way, searching for a suitable operation frequency. The practical interference situations, with synchronized MAC Frames are BS-SS and SS-BS interference. Assuming similar transmit powers, the above mentioned process will have as result finding Master sub-frames in which the path attenuation between interfering units is maximal.

5.1.4 Signaling procedures for Cognitive Radio applications

For signaling and message exchange between an ad-hoc system and systems using a Coexistence Protocol, it is:

- Split the narrowest channel to be used (as defined in 802.16 Profiles) into 32 energy bins, as follows:
    - For 256FFT, to 8 sub-carriers/bin
    - For 512 FFT, to 16 sub-carriers/bin
    - For 1024FFT, to 32 sub-carriers/bin
    - For 2048FFT, to 64 sub-carriers/bin.

- Send an 802.16h MAC message, at a suitable rate, such that the MAC header will use 1 symbol and the MAC PDU will use another symbol; the MAC header and the data field will be built in such a way that the power distribution for different bins will be with at least 5dB higher for a bin marked in Table 1 with “H” than for bin marked with “L”.

The data field for both transmit and receive operations, taking into account possible FFT sizes, channel widths and the defined PHY modes, is defined in chap. t.b.d.

The following figures show the desired spectral density for cognitive signaling and the possible outcome of the MAC PDU approach, introducing some distortions in time or frequency domain, but still detectable by non-802.16 systems.

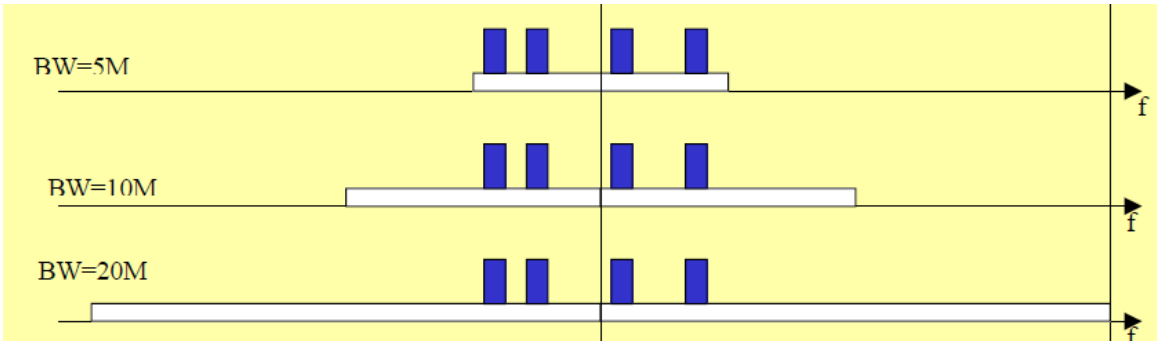


Figure 19. Desired spectral densities for different channel BWs

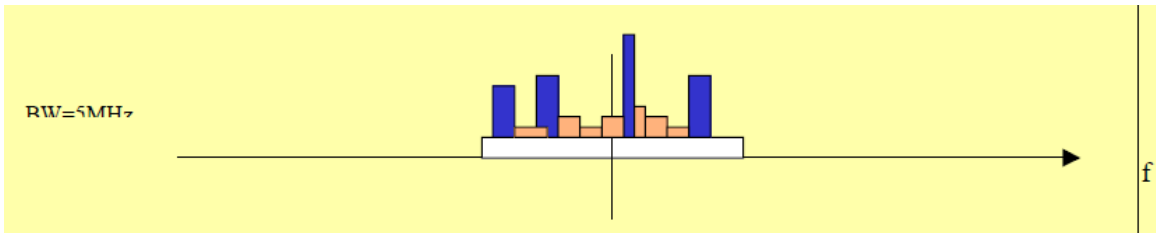


Figure 20. Obtainable spectral densities with MAC PDU approach

Due to the FFT guard sub-carriers, not all the bins are usable; we will use in continuation, from the bins numbered 0…31, where the bin#0 corresponds to the lowest frequency, only the bins 6…26.

In Table1 were defined a number of cognitive signals, having low inter-correlation properties. The energy on the not-used bins can take any value, but not more than the energy on a bin marked with "H". This tolerance will allow finding adequate data mapping for each PHY mode. Obviously, if the energy on not-used bins will be minimal, the detection process will be easier.

Table 1. Cognitive signal definition

Bin number /Signal number	6	8	10	12	14	18	20	22	24	26
1 (802.16h Cognitive MAC Header)	H	L	L	H	H	L	L	L	H	L
2 (Tx_start)	L	H	L	L	H	H	L	L	L	H
3 (Rx_start or Rx_slot)	H	L	H	L	L	H	H	L	L	L
4 (Tx_end)	L	H	L	H	L	L	H	H	L	L
5 (Rx_end)	L	L	H	L	H	L	L	H	H	L

6 (NACK)	L	L	L	H	L	H	L	L	H	H
7	H	L	L	L	H	L	H	L	L	H
8	L	H	H	L	L	H	L	H	L	L
9	L	L	H	H	L	L	H	L	H	L

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 inTable2.

Table 2. LE_CP MAC messages

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

These MAC management messages are exchanged between peers, e.g. BS and BSIS or BS and BS, and distinguish between CP requests (BS -> BS/BSIS) and CP responses (BS/BSIS -> 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 BSIS shall use the form shown in. Table3.

Table 3. LE_CP message format

Syntax	Size	Notes
CP _Message_Format() {		
Version of protocol in use	? bits	*1 for current version*
Code	8 bits	
Management Message Type	?bits	0- LE_CP-REQ 1- LE_CP-RSP
Length of Payload	??bits	

AssociationID	??bits	
CP Message Seq_ID	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

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 inTable4.

Length of payload

The length of payload descript the length of payload in bytes .

CP Message Sequence Identifier (CP Message Seq_ID)

The **CP Message Sequence** Identifier field is one byte. A BS/BSIS uses the identifier to match a BS/BSIS response to the BS's requests. The BS shall increment (modulo 256) the Identifier field whenever it issues a new CP message. The retransmission mechanism relies on TCP. The Identifier field in a BS/BSIS's CP-RSP message shall match the Identifier field of the CP-REQ message the BS/BSIS is responding to.

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

Code	CP Message type	MAC Message Type	Protocol type	Direction
0	*Reserved*	—	—	—
1	Send-Security-Block	LE_CP-REQ	TCP	BS->BS/BSIS
2	ACK-Security-Block	LE_CP-RSP	TCP	BS/BSIS->BS
3	Neighbor Topology Request	LE_CP-REQ	TCP	BS-> BSIS
4	Neighbor Topology Reply	LE_CP-RSP	TCP	BSIS->BS
5	Registration Request	LE_CP-REQ	TCP	BS-> BSIS
6	Registration Reply	LE_CP-RSP	TCP	BSIS->BS
7	Registration Update Request	LE_CP-REQ	TCP	BS-> BSIS
8	Registration Update Reply	LE_CP-RSP	TCP	BSIS->BS
9	De-registration Request	LE_CP-REQ	TCP	BS-> BSIS
10	De-registration Reply	LE_CP-RSP	TCP	BSIS->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	BS_CCID_IND	LE_CP-REQ	UDP	BS->BS
32	BS_CCID_RSP	LE_CP-RSP	UDP	BS->BS
33	SS_CCID_IND	LE_CP-REQ	UDP	BS->BS
34	SS_CCID_RSP	LE_CP-RSP	UDP	BS->BS
35	PSD_REQ	LE_CP-REQ	UDP	BS->BS
36	PSD_RSP	LE_CP-RSP	UDP	BS->BS
37-255	*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/BSIS shall silently discard all requests that do not contain ALL required attributes. The BS shall silently discard all responses that do not contain ALL required attributes.

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

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

Table 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/BSIS. 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/BSIS to decrypt and encrypt ESP packets.

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

Code: 1

Attributes are shown inTable6.

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

Code: 2

Attributes are shown inTable7.

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/BSIS-ACK-Authenticator	48 Octets.

6.1.3 Neighbor Topology Request message

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

Code: 3

Attributes are shown inTable8.

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 BSIS 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 BSIS 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 inTable9.

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 BSIS 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 inTable9.

6.1.8 Registration Update Reply message

The BSIS 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 BSIS to perform de-registration.

Code: 9

Attributes are shown inTable10.

Table 10. De-registration Request message attributes

Attribute	Contents
BSID	The BSID of the request BS.

6.1.10 De-registration Reply message

The BSIS 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 inTable11.

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 BSIS 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 inTable12.

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 BSIS 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 Table13.

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 BSIS 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.

6.1.31 BS_CCID_IND message

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

Code: 31

This is a message sent by a SS to CR_NMS when co-channel interference is detected at SS. This message shall contain the following minimum information to help determine the source and victim of co-channel interference:

- BS_NUM: total number of base stations from which CCI interference is detected.
- BS_ID: the base station IDs causing CCI
- Sector_ID: the sector IDs of the base stations causing CCI
- SS_ID: the SS that sent this message.

Essentially, this message will contain a table of co-channel interference sources for this SS.

Table 14. table of co-channel interference source for SS

Base station ID	Sector ID
123456	2
234534	4
…	…

6.1.32 BS_CCID_RSP message

A "set" message to BS.

Code: 32

This is a "set" message; it is to set the emission or reception qualities of the specified SS. Upon receiving co-channel interference notification, the algorithm in CR-NMS will determine an appropriate CCI mitigation decision and forward

This message to the victim SS.

SS_CCID_RSP can contain the following information for example:

- SS_ID: the ID of subscriber station that causes/receives co-channel interference. It is the receiver of this message.
- EIRP for the specified SS. This is a reduced/increased EIRP value for this SS based on algorithm.
- Downlink/uplink frequency change.
- Reregistration request to a new BS
- Specification of allowable uplink timing slots.
- Adaptive antenna configuration parameters for reception/transmission.

6.1.33 SS_CCID_IND message

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

Code: 33

This is a message sent by a BS to CR_NMS when co-channel interference is detected at BS. This message shall contain the following information to help determine the source and victim of co-channel interference:

- SS_NUM: total number of subscriber stations that interference events were noted.
- SS_ID: the subscriber stations ID that causes the co-channel interference
- Sector_ID: the sector ID of the subscriber stations that cause interference
- Source basestation ID: the BS that sent this message.
- Source sector_ID: the antenna sector that detects the co-channel interference.

Essentially, this message will contain a table of co-channel interference sources for this BS.

6.1.34 SS_CCID_RSP message

A "set" message to SS.

Code: 34

This is a "set" message; it is to set the configuration of the BS. Upon receiving co-channel interference notification, the algorithm in CR-NMS will use this message to set the emission or reception qualities of the specified BS. It shall have the following information:

- BS_ID: Base station ID of Base Station receiving/causing interference. It is the receiver of this message.
- EIRP for the specified BS
- Downlink/Uplink frequency change.
- Adaptive antenna configuration parameters for reception/transmission.

6.1.35 PSD_REQ message

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

Code: 35

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

This is a "set" message, it is requests a BS or SS to sample PSD (power spectrum density) data for next "get" message. Since sampling PSD data will take some time, depending on environment, nature of bursty users, the following "get" message shall wait long enough for BS/SS to complete the PSD data sampling. There shall be only one scalar MIB object defined for this operation.

6.1.36 PSD_RSP message

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

Code: 36

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

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

Resolution bandwidth is scalar, it is used together with X-max and X-min to determine how many PSD values are collected and contained in the STRUF_REP message (i.e. $(X_{\max} - X_{\min})/(resolutionBandwidth) + 1$).

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

Here is an example of PSD display:

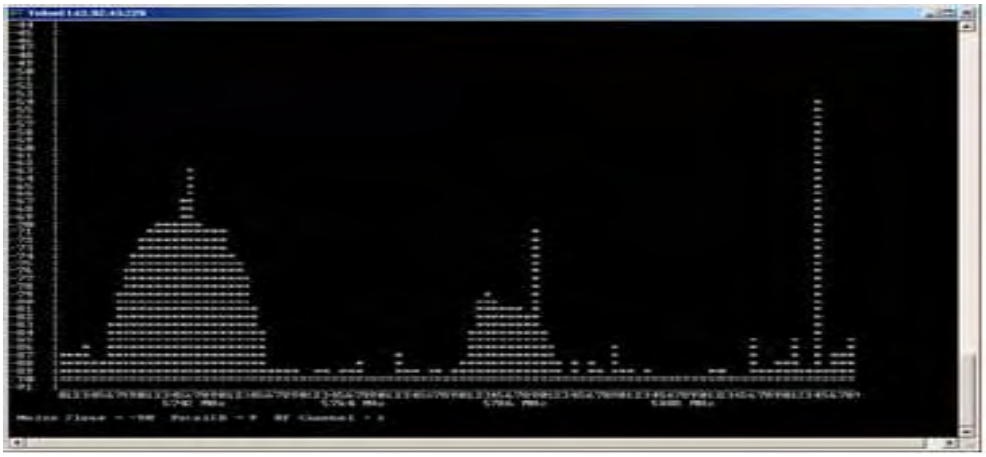


Figure 21. Example of PSD Display

[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 Figure18. 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/BSIS-Registration-Request (BS/BSIS → RADIUS server)

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

Table 15. Table RADIUS-BS/BSIS-Registration-Access-Request

Attribute number	Attribute name	Value
1	User-Name	BSID. The BSID should be represented in ASCII format, with octet values separated by a "-". Example: "00-10-A4-23-19-C0".
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 (SeeTable15)
26-TBD	Supported-ESP-Transforms	The list of ESP Transform IDs corresponding to the ESP transforms supported by this BS (SeeTable2)
32	NAS-Identifier	BS's NAS Identifier
80	Message-Authenticator	The RADIUS message's authenticator

According to RFC 2865:2000, other RADIUS attributes may be included in the RADIUS-BS/BSIS-Registration-Access-Request packet in addition to the ones listed inTable14.

Table 16. 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 17. 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/BSIS-Registration-Accept (RADIUS server → BS/BSIS)

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

Table 18. RADIUS-BS/BSIS-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/BSIS-Access-Request (BS/BSIS → RADIUS server)

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

Table 19. RADIUS-BS/BSIS- Access-Request

Attribute number	Attribute name	Value
1	User-Name	Regional BSIS'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/BSIS-Check (value = TBD, ex. IAPP-AP-Check, value = 16)
61	NAS-Port-Type	Wireless – Other (value = 18)
80	Message-Authenticator	The RADIUS message's authenticator

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

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 BSIS and requesting BS.

Table 20. RADIUS-BS/BSIS- Access-Accept

Attribute number	Attribute name	Value
1	User-Name	Regional BSIS's WM address or neighbor BS's BSID.
8	Framed-IP-Address	IP Address of Regional BSIS 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/BSIS-Security-Block	Security Block encrypted using neighbor BS's RADIUS BSID secret (or BSIS's), to be decrypted and used by the neighbor BS (or BSIS)

80	Message-Authenticator	The RADIUS message's authenticator

Table 21. 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 BSIS or neighbor BS
7	Variable	Key used by ESP Transform for ESP packets to the regional BSIS or neighbor BS
8	Variable	Key used by ESP Authentication for ESP packets to the regional BSIS or neighbor BS
9	4	SPI used to identify ESP SA from the regional BSIS or neighbor BS
10	Variable	Key used by ESP Transform for ESP packets from the regional BSIS or neighbor BS
11	Variable	Key used by ESP Authentication for ESP packets from the regional BSIS 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 Using dedicated messages

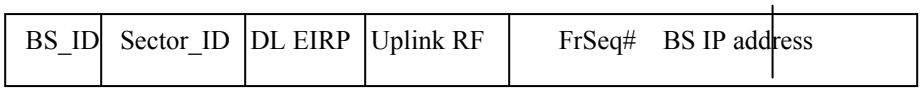
6.8.1 Common PHY

6.8.2 Between BS and SS

Two MAC messages are defined for use between the BS and SS. These messages are called “tags” since the tag the radio packet communication bursts which create co-channel interference

6.8.2.1 SS_MEM

The subscriber station membership (SS_MEM) message can be a new (or modified) MAC message for IEEE 802.16h FDD. The BS broadcasts a SS_MEM message in each RF sector at a periodic intervals, inserted within the DL MAC PDU. It defines the radio emission characteristics of the downlink of the sector, and provides information on uplink FDD channels utilized by the sector and could include channel width information as well. The message is encoded in the following format:

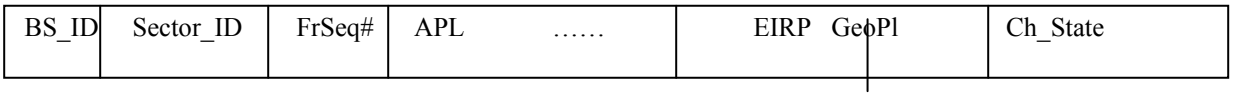


Parameters:

1. BS_ID: The base station ID. This information will help SS to determine which BS this message is received from. If it is not received from the home base station (it registered with), then it is co-channel interference caused by another BS downlink. In this case, a BS_CCID_IND message shall be send to Network Management System (CR_NMS) to indicate co-channel interference source and victim. Upon receiving this message, CR_NMS will initiate a response, which could access the CIS or be determined by the CR-NMS by itself, based on the SS_Mem contents.
2. Sector_ID: Identifies the Sector antenna broadcasting this SS_MEM message. This information will help SS to determine which BS sector this message is received from. This could contain the GPS location, height of sector antenna, beamwidth of sector and direction of sector antenna, etc.
3. DL EIRP: Down link EIRP of sector
4. Uplink RF: Uplink RF frequency channels used by this sector
5. FrSeq#: Frame sequence number
6. BS IP address: IP address of the base station that broadcasts this message.

6.8.2.2 SSURF

1. The subscriber station uplink radio frequency (SSURF) message shall be a modified (or new) MAC message for IEEE 802.16h. This message is periodically sent by SS as uplink tags, but could also contain interference and other event information experienced by the SS.



SSURF message fields are:

2. BS_ID: The base station ID to identify which base station this message is sent to. This information will help receiving BS to determine if received packet is CCI. If BS_ID it is different from the receiving base station ID, co-channel interference has occurred with another SS uplink. In this case, a SS_CCID_IND message shall be send to Network Management System (CR_NMS) to

indicate co-channel interference source and victim. Upon receiving this message, CR_NMS will, initiate a CR response, which could access the CIS or be determined by the CR-NMS by itself. A response could be based on the SSURF contents.

3. Sector_ID: Identifies the destination sector antenna of this message. In essence, it is the same field as used in the SS_MEM message. Contains information, that if this packet is received as CCI, can to transported to a CR_NMS within the SS_CCID_IND message.
4. FrSeq#: Frame sequence number.
5. APL: Antenna parameter list giving information on antenna type (adaptive w/parameters; beam width, polarization, diversity, etc) of SS
6. EIRP: EIRP of transmitted SSURF
7. GeoPl: Geographical placement of SS, Range from associated BS, GPS coordinates, etc.)
8. Ch_State: mean fade duration, mean fade depth, variance of DL signal strength, Bit Error Rate mean, Bit Error Rate Variance, RSSI mean, RSSI variance, etc.

Upon reception of this message, BS will stamp the message based on the arrival time and translate the information into internal format for construction of a SS_CCID_IND message.

6.8.3 BS to BS

6.8.4 Connection sponsorship

6.8.5 Using a common management system

6.8.6 Higher layers communication

6.8.7 Decentralized control

6.8.8 Information sharing

6.8.9 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

7.2.2.1.1 Power control

7.2.2.1.2 Mutual tolerance

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 Credit token based coexistence protocol

Spectrum sharing between several networks (NW) can be achieved through the sharing of a common MAC frame between the different NWs as exampled by Figure 22. In such a MAC frame structure, dedicated portions (denoted as “master NW sub-frames”) of the frame are periodically and exclusively allocated to a NW (denoted as the “master NW”) respectively in the forward and reverse link. The terminology used hereafter defines a slave NW as a NW that may operate during the other master NWs sub-frames. With respect to this definition, the slave NW sub-frames are the time intervals operating in parallel of the master NWs sub-frames.

Additional flexibility can be provided by such a frame structure if: (1) the length of each master sub-frame can be dynamically adjusted as a function of the spatial and temporal traffic load variations of each NW; (2) the slave NWs sub-frames can be allocated with the same sub-carriers (co-channel) as the master NW during the master NW sub-frames transmissions.

Requirements (2) can be envisaged if provided that the master NW perceives a co-channel interference level lower than an admissible interference threshold explicitly agreed with the slave NWs to ensure master NW's QoS (QoSMaster) is guaranteed. Similarly, parallel transmissions can be envisaged if the slave NWs can negotiate with master NW to be provided with a guaranteed QoS (QoSSlave) and if contention issues between slave NWs are resolved.

Given requirements (1) and (2), this contribution proposes the dynamic coordination of the frame structure sharing between BSs when several master and slave NWs compete to share this common shared MAC frame.

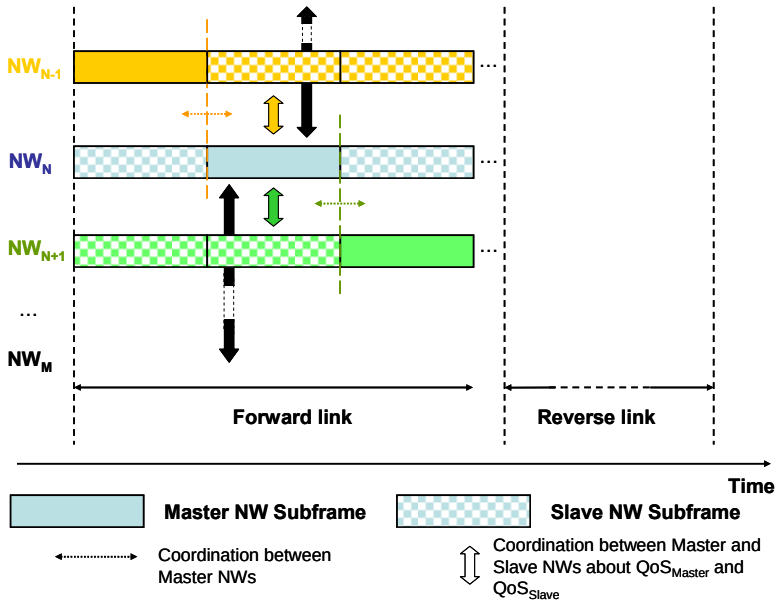


Figure 22. Example of TDD based MAC frame sharing structure between M NWs

7.2.2.6.1 General principle

The first step consists in defining credit tokens and designing appropriate reserve price auctioning and bidding mechanisms to solve contention access channel issues between NWs. Then, on the basis of the credit tokens based mechanisms usage, the second step consists in managing dynamically the bandwidth (in time and frequency) requests and grants mechanisms of the common shared MAC frame between BSs of master and slave NWs competing for spectrum sharing.

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

7.2.2.6.2 Credit tokens assignment and usage principles

- _ Each NW is initially allocated with a given credit tokens account.
- _ Negotiation for spectrum sharing between NWs is based on credit tokens transactions.
- _ Credit tokens transactions occur dynamically between a seller (master NW owner of the radio resources during the active master sub-frame) and one or several bidders (the other master NWs or slave NWs).
- _ The negotiation occurs dynamically either:
  - o Between master NWs (denoted "Case 1" in the following) to agree the length of each master sub-frame as a function of the spatial and temporal traffic load variations need of each master NW (refers to above requirement (1) of section 2).
  - o Between master and slave NWs (denoted "Case 2" in the following) to select the slave NWs allowed operating in parallel of the master sub-frame based on QoSSlave and QoSMaster (refers to above requirement (2) of section 2).

7.2.2.6.3 Negotiation between master NWs

Two sub-cases of "case 1" can be considered: the negotiation can be triggered by the master NW seller ("case 1a"), or can be triggered by the master bidder ("case 1b").

For "case 1a", the mechanisms are:

- The master NW_N (seller) advertises that its periodic assigned master sub-frame is open for renting (Figure23) from starting time $\boldsymbol{T_{Start}}$ to ending time $\boldsymbol{T_{End}}$ for a fraction ($\mathbf{T_{Renting}}/\mathbf{T_{Msf}}$) of its master sub-frame duration $\mathbf{T_{Msf}}$.
- The master NW_N proposes a reserve price auction ***RPA*** for this renting. The ***RPA*** is expressed as a number of credit tokens per time unit.
- The interested contiguous (NW_{N-1} and NW_{N+1}) and non contiguous (NW_{N-i} and $NW_{N+i,}$ $i>1$) master NWs of NW_N make bidding on this auction. The bid ($\boldsymbol{BID_k}$) of each bidder k is a vector including the following information:
  - o The amount of bided credit tokens per time unit ($\boldsymbol{CT_k}$),
  - o The fraction $\boldsymbol{x_k}$ of $\boldsymbol{T_{Renting}}$ his bid $\boldsymbol{CT_k}$ applies for,
  - o The time interval $[\boldsymbol{T_{Start\,k}}, \boldsymbol{T_{End\,k}}]$ his bid applies for. $[\boldsymbol{T_{Start\,k}}, \boldsymbol{T_{End\,k}}] \subset [\boldsymbol{T_{Start}}, \boldsymbol{T_{End}}]$. $\boldsymbol{BID_k} = \{\boldsymbol{CT_k}, \boldsymbol{x_k}, \boldsymbol{T_{Start\,k}}, \boldsymbol{T_{End\,k}}\}$
- Based on the different biddings $\boldsymbol{BID_k}$ received:
  - o The master NW_N partitions $[\boldsymbol{T_{Start}}, \boldsymbol{T_{End}}]$ into contiguous time segments $\{\mathbf{TS_m}\}$ on the basis of the time intervals set $\{[\boldsymbol{T_{Start\,k}}, \boldsymbol{T_{End\,k}}]\}$. Each $\mathbf{TS_m}$ corresponds to a time window (integer number of $\mathbf{T_{Frame}}$) in which a subset of intervals of $\{[\boldsymbol{T_{Start\,k}}, \boldsymbol{T_{End\,k}}]\}$ overlaps. In each $\mathbf{TS_{m,}}$ each involved bidder k competes with his respective $\mathbf{BID_k}$.
  - o For each $\mathbf{TS_{m,}}$ master NW_N calculates the payoff $\mathbf{P_k} = \boldsymbol{CT_k} * \boldsymbol{x_k} * \boldsymbol{T_{Renting}} * \mathbf{N_{Frame\ m}}$ for each bidder k. $\mathbf{N_{Frame\ m}}$ is the number of frames within $\mathbf{TS_m}$ ($\mathbf{N_{Frame\ m}} = \mathbf{TS_m}/\mathbf{T_{Frame}}$).
  - o The master NW_N searches the subset of {k} such as sum($\boldsymbol{x_k}$) = **1** and sum($\mathbf{P_k}$) is maximal.
- The clearing price auction ($\boldsymbol{CPA_{m,k}}$) is derived by the master NW_N for each $\mathbf{TS_m}$ and each k. $\boldsymbol{CPA_{m,k}}$ is expressed as a number of credit tokens per time unit. Different methods can be applied here to define $\boldsymbol{CPA_{m,k}}$ (more on that in section 9).
- Each k of the selected list {k} on $\mathbf{TS_m}$ pays the price $\boldsymbol{Pr_k} = \boldsymbol{CPA_{m,k}} * \boldsymbol{x_k} * \boldsymbol{T_{Renting}} * \mathbf{N_{Frame\ m}}$.
- Provided that $\boldsymbol{Pr_k}$ does not exceed the credit tokens account of user k, each winning bidder k is then assigned with the corresponding granted resources (all pool of frequencies) during $\boldsymbol{x_k} * \boldsymbol{T_{Renting}}$ time unit of NW_N and for $\mathbf{N_{Frame\ m}}$ frames.

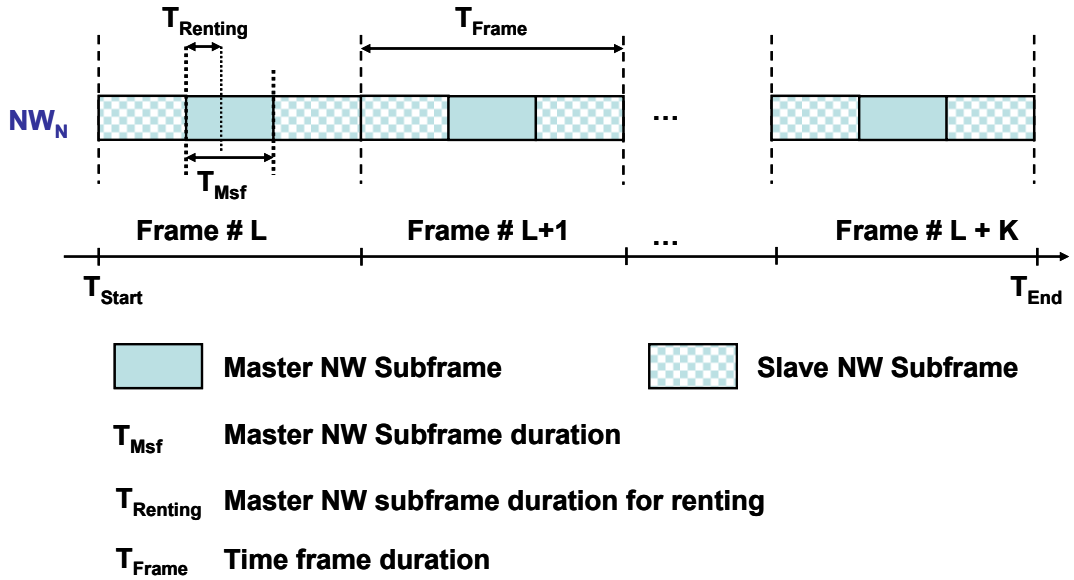


Figure 23. Simplified MAC frame structure illustrating master NW sub-frame renting principle and associated notations

Note: The same mechanisms as "case 1a" apply in "case 1b". In addition to "case 1a", in "case 1b" the master NWs bidder candidates can trigger themselves the other master NW that could potentially rent some spectrum. This triggering can be made by one of the approaches presented in section 7.2.2.6.4.

7.2.2.6.4 Inter BSs communication

The above mechanisms require inter BSs communication between different NWs. This inter BS communications is necessary to exchange the parameters related to the *Advertising phase,* the *Admissible co-channel interference control phase* and the *Auctioning/bidding phase.* It is assumed that these parameters are stored into the regional LE DB and into the local database of each LE BS. The information exchange between these databases and the RADIUS/BSIS servers can be either supported by secured over the air signalling, or by IP communication between the networks.