Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Storage of identification information and Coexistence Protocol**	
Date Submitted	**2005-04-29**	
Source(s)	Chi-Chen Lee, Keng-Ming Huang, Hung-Lin Chou, Han-Chiang Liu, Industrial Technology Research Institute, Computer and Communications Research Labs, Taiwan Bldg. 11, 195 Sec. 4, Chung Hsing Rd. Chutung, HsinChu, Taiwan 310, R.O.C.	Voice: +886-3-5914579 Fax: +886-3-5829733 mailto: jjlee@itri.org.tw
	Rina Nathaniel Alvarion Tel Aviv, 21 HaBarzel Street Israel	Voice: +972 3 7674287 Fax: +972 3 645 6204 mailto: Rina.Nathaniel@alvarion.com
Re:	Call for Contributions, IEEE 802.16h Task Group on License-Exempt Coexistence, IEEE 802.16h-05/007	
Abstract	Propose the architecture of storage of identification information and Coexistence Protocol.	
Purpose	Information.	
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.	
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.	
Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chair@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.	

Storage of identification information and Coexistence Protocol

Chi-Chen Lee, Keng-Ming Huang, Hung-Lin Chou, Han-Chiang Liu
Computer & Communications Research Labs, ITRI, Taiwan
Rina Nathaniel
Alvarion, Israel

1. Introduction

The scope of the paper is to provide text for the IEEE 802.16h standard, to be inserted under the section "*Storage of identification information*" – see [1]. This proposal is based on contribution IEEE S802.16h – 05/006 [2] which has been discussed in session#35. The *database* can facilitate the coexistence resolution between 802.16 LE systems of different networks. For instance, a BS relies on it to construct its *neighbor topology*. With the neighbor topology it can perform coexistence avoidance and Shared RRM negotiation as needed. Besides, in order to get the neighbor topology, perform registration to the database and registration to peer, negotiation for Shared RRM etc. we propose a *Coexistence Protocol* and this protocol is intended to be inserted under section "*2.1.2.2 Inter-network communication*". In order to secure the inter-network communication and to distribute the IP addresses of 802.16 LE BSs belonging to different networks in secure manner we propose general security architecture in another contribution [3]. Analogous design refers to IEEE 802.11F-2003 [4] due to the similar purpose of solving inter-network communication problems. This paper also refers to another contribution [5] for harmonization.

2. Storage of identification information

2.1 Regional LE database and Coexistence Identification Server (CIS)

Regional LE database (LE DB) (see [2]) is primary for facilitating the coexistence detection, avoidance and resolution. There is country/region database, which includes, for every Base Station:

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

Every Base Station also includes a database, called *Shared DB* [1], open for any other Base Station [5]. The BS data-base contains information necessary for spectrum sharing, and includes the information related to the Base station itself and the associated SSs. A Base Station and the associated SSs form a System. Other Base Stations can send queries related to the information in the Shared DB to the DRRM entity.
The BS Shared DB includes [5]:

1. Operator ID
2. Base Station ID
3. MAC Frame duration
4. Frame and sub-frame number chosen for the Master sub-frame
5. Repetition interval between two Master sub-frames, measured in MAC-frames

6. List of other used sub-frames, in the interval between two Master sub-frames
7. Time_shift from the Master sub-frame start, when a transmitter will transmit its radio signature
8. Slot position for network entry of a new Base Station, which is evaluating the possibility of using the same Master slot

The LE BSs can, therefore, have knowledge about the possible interferers such as coexisting BSs and SSs from neighbor BSs by querying the regional LE DB with its geographic position as well as by querying the Shared DBs of its neighbors. Another functionality of the regional LE DB is to deliver the BSIDs of neighbor BSs to the BS who looks up its neighbors in secure manner. As opposed to broadcast IP address over the air, one LE BS uses BSIDs acquired from LE DB to request the corresponding IP addresses by utilizing Remote Authentication Dial-in User Service (RADIUS) protocol. Contribution [3] will provide a detailed account of how IP addresses being delivered securely across 802.16 LE systems.

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

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

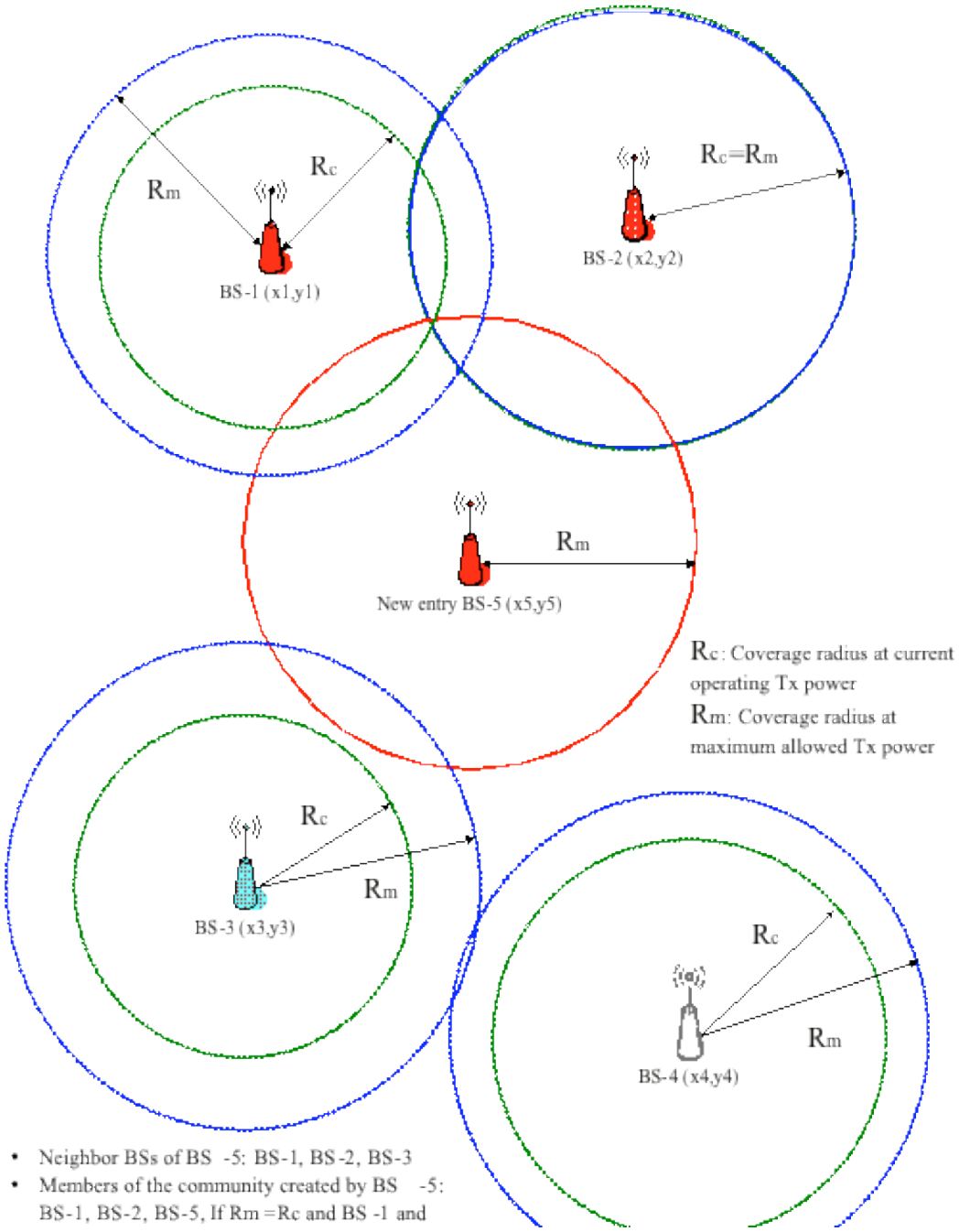

Figure 1_802.16 LE Neighbor BSs discovery and definition of neighbor and community

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

(1) *Initialization stage*

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

(2) *Operating stage*
In operating stage the LE BS has SS associated with it, however, even the operating system parameters has decided, the co-channel or adjacent channel interference from LE BSs of different network may still have a chance to happen due to the detection of interference from primary user, channel switching of neighbor BS or the entry of new neighbor BS makes the community so crowded that there is no enough channels. If the LE BS finds that there is no “free” channel at that moment, the neighbor topology provides the guidelines of with whom it should negotiate. [detailed procedures are to be defined]
Figure 2 shows the proposed initialization procedures for the 802.16 LE BSs. Note that the procedure that BS tries to create a Master slot [5] is also applicable for operating stage. The detailed negotiation and update procedures are described in section 2.1.2.2.1.

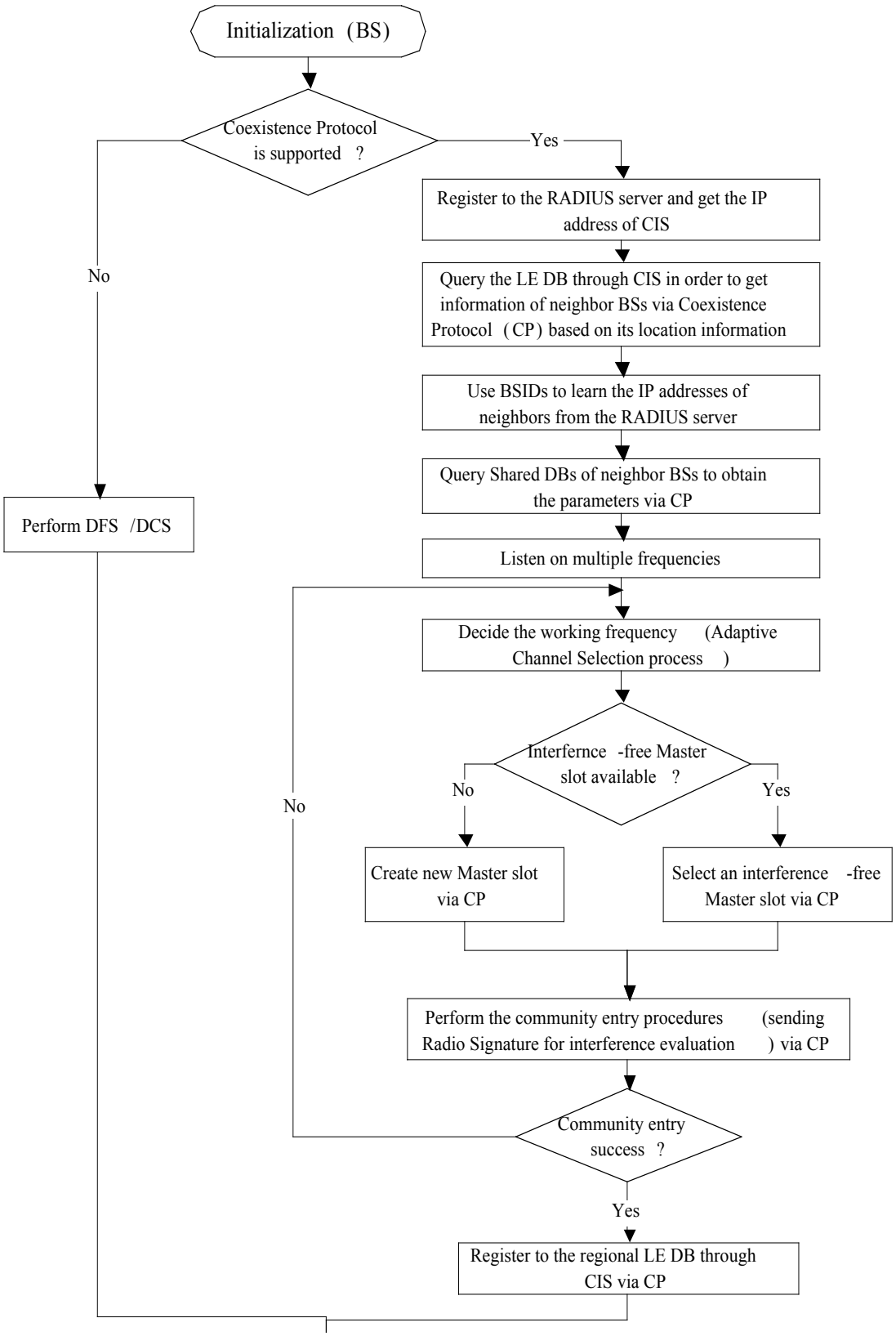

Figure 2 _Initialization procedures — BS

The coexistence resolution will rely on a regional LE DB but there should be an entity between the LE BSs and the regional LE DB in order to let the coexistence resolution processes to be independent of the database technologies. Therefore, we propose an entity named *Coexistence Identification Server* (CIS) 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. CIS converts the query results from the regional LE DB to the proper format, e.g. TLV encodings, and replies to the requested BSs. Figure 3 shows the general architecture of inter-network communication across 802.16 LE systems (for more details see [3]). In this architecture, the 802.16 LE systems (BSs and CIS) from different networks set up security association (including BS and BS, BS and CIS) with each other by utilizing the services provided by the RADIUS server. CIS 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 CIS is well known among the LE operators. The LE BSs can use the MAC address of CIS, which may be provisioned, to acquire the IP address and keys for Encapsulating Security Payload (ESP) (RFC2406:1998) operation of the CIS by utilizing RADIUS protocol. As shown in figure 3, the RADIUS server maintains the BSID and IP mapping. In summary, ESP with RADIUS can discover a Rogue BS or CIS. The messages exchanged between the LE BSs and the CIS will be revealed in the next section. Note that the interface between CIS and regional LE DB is out of scope.

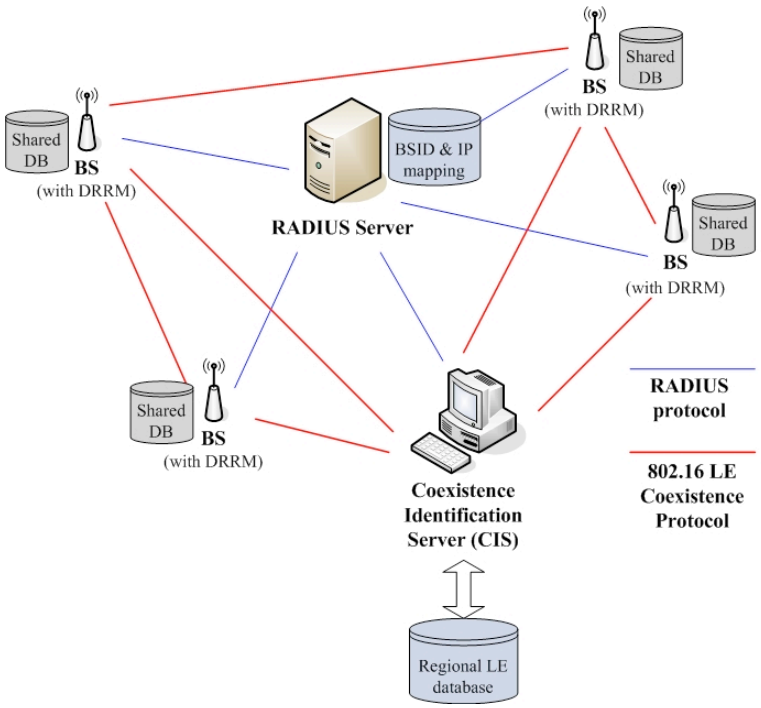

Figure 3 _general architecture of inter-network communication across 802.16 LE systems

3. Coexistence Protocol

In order to get the neighbor topology, perform registration to the database and registration to peer, negotiation

for Shared RRM etc. we propose a Coexistence Protocol. Figure 4 reveals the 802.16h protocol architecture based on the architecture described in 802.16g [6]. The protocol architecture indicates that DRRM, Coexistence Protocol and Shared DB belong to LE Management Part located in management plane and the messages will be exchanged over IP network. Thus, DRRM in LE Management Part uses the Coexistence protocol to communicate with other BSs and with Regional LE DB and interact with MAC or PHY. Figure 5 is LE BS architecture with Coexistence Protocol, which is akin to the AP architecture with IAPP proposed in [4]. The grey area indicates area where there is an absence of connection between blocks. DSM is Distribution System Medium which is another interface to the backbone network. Note that is architecture is only for reference. Similarly, Figure 6 is the CIS architecture with co-located regional LE database. Other architectures are not being illustrated. The Coexistence Protocol services are accessed by the LE Management Entity through CP SAP. But the service primitives will not provided in this contribution due to the Coexistence Protocol is incomplete at this stage. This proposal only provides the definition of PDUs exchanged between peer Coexistence Protocol entities. A BS uses the Coexistence Resolution and Negotiation (CP) Protocol, which is similar to PKM protocol, to perform the coexistence resolution and negotiation procedures. There are two types of messages to support Coexistence Protocol:
(1) LE_CP-REQ: BS→BS or BS→CIS
(2) LE_CP-RSP: BS→BS or CIS→BS

Similar to PKM messages, there is one byte CP message code in the message body to identify the type of CP packet. Table 1 shows LE_CP-REQ message format and Table 2 shows LE_CP-RSP message format. Table 3 is the proposed CP message codes in this contribution. Figure 7 shows an example message flow of Coexistence Protocol. It demonstrates how the CIS and the regional LE DB work.

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

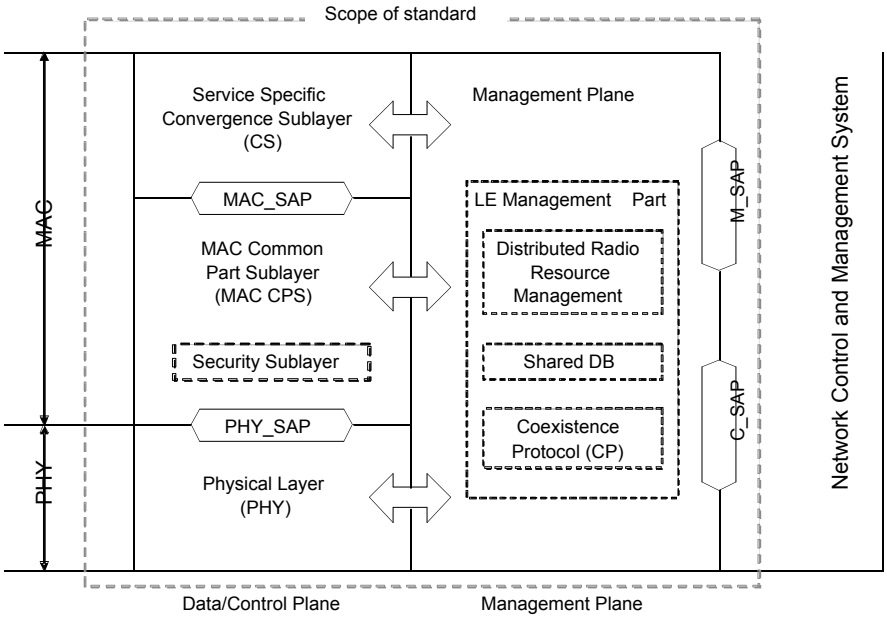

Figure 4 _802.16h BS Protocol architecture Model

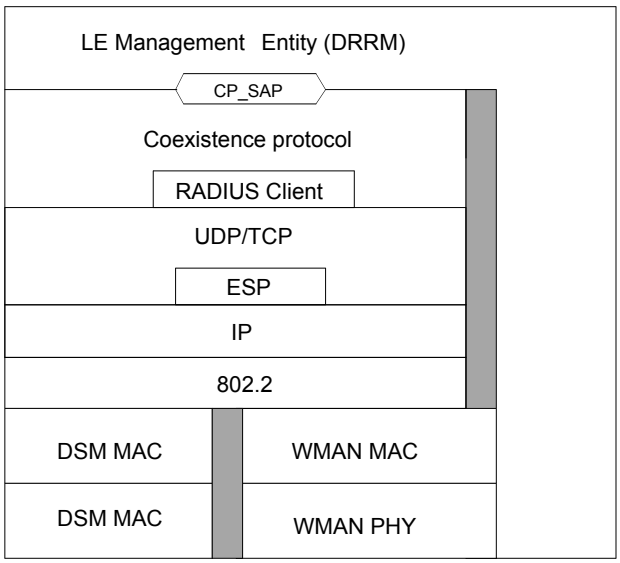

Figure 5 _LE BS architecture with Coexistence Protocol

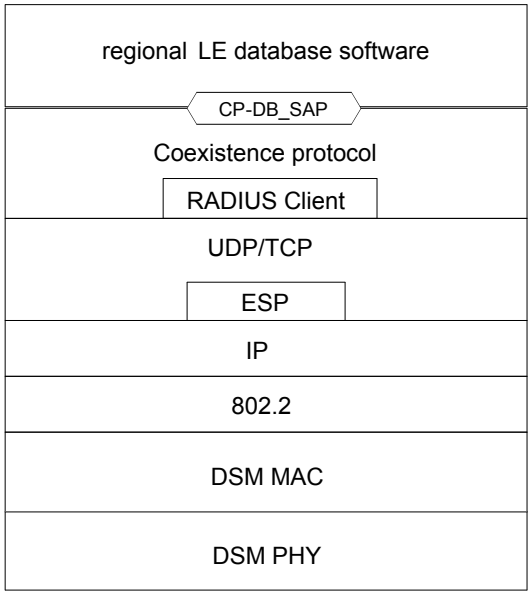

Figure 6 _CIS architecture with co-located regional LE database

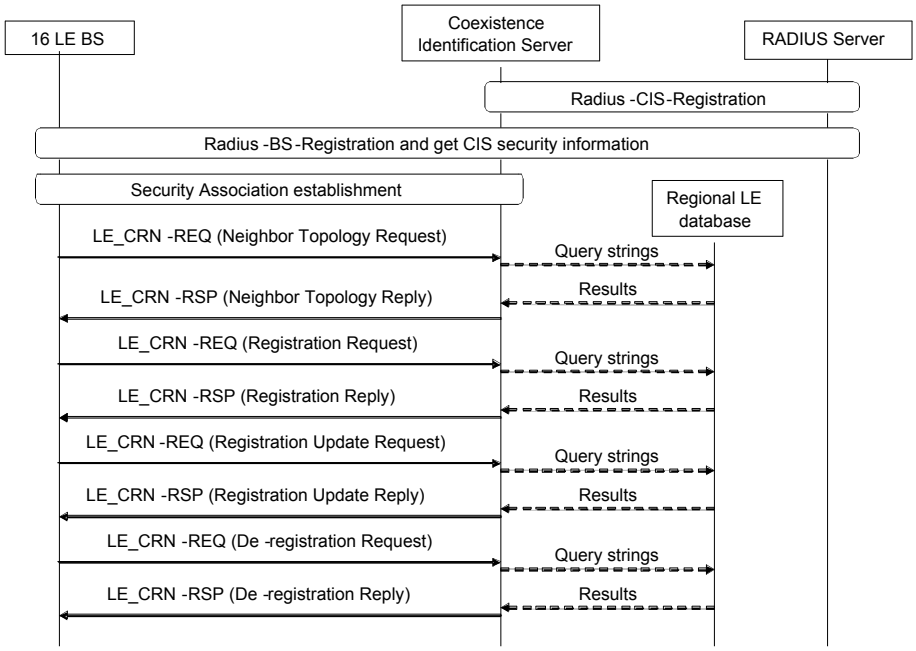

Figure 7 _Coexistence Protocol example — BS between CIS

Table 1—LE_CP request (CP-REQ) message format

Syntax	Size	Notes
CP-REQ_Message_Format() {		

Management Message Type = xx	8 bits	
Code	8 bits	
CP Identifier	8 bits	
TLV Encoded Attributes	*variable*	TLV specific
}		

Table 2—LE_CP response (CP-RSP) message format

Syntax	Size	Notes
CP-RSP_Message_Format() {		
Management Message Type = xx	8 bits	
Code	8 bits	
CP Identifier	8 bits	
Confirmation Code	8 bits	
TLV Encoded Attributes	*variable*	TLV specific
}		

Table 3—LE_CP message codes

	CP Message type	MAC Message Type
0	*Reserved*	—
1	Send-Security-Block	LE_CP-REQ
2	ACK-Security-Block	LE_CP-RSP
3	Neighbor Topology Request	LE_CP-REQ
4	Neighbor Topology Reply	LE_CP-RSP
5	Registration Request	LE_CP-REQ
6	Registration Reply	LE_CP-RSP
7	Registration Update Request	LE_CP-REQ
8	Registration Update Reply	LE_CP-RSP
9	De-registration Request	LE_CP-REQ
10	De-registration Reply	LE_CP-RSP
11	Add Coexistence Neighbor Request	LE_CP-REQ
12	Add Coexistence Neighbor Request	LE_CP-RSP
13	Update Coexistence Neighbor Request	LE_CP-REQ
14	Update Coexistence Neighbor Request	LE_CP-RSP
15	Delete Coexistence Neighbor Request	LE_CP-REQ
16	Delete Coexistence Neighbor Request	LE_CP-RSP
17-255	*reserved*	—

9. Text to be inserted in the standard

Acronyms

CIS Coexistence Identification Server
DSM Distribution System Medium
ESP IP Encapsulating Security Payload
IETF Internet Engineering Task Force
IANA Internet Assigned Numbers Authority
SAP Service Access Point
TCP Transmission Control Protocol
UDP User Datagram Protocol

[*Insert the following section after section "6 Transmission of information"*]

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

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

Table A—LE_CP MAC messages

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

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

Table B—LE_CP request (CP-REQ) message format

Syntax	Size	Notes
CP-REQ_Message_Format() {		
Management Message Type = nn	8 bits	
Code	8 bits	
CP Identifier	8 bits	
TLV Encoded Attributes	*variable*	TLV specific
}		

Table C—LE_CP response (CP-RSP) message format

Syntax	Size	Notes
CP-RSP_Message_Format() {		
Management Message Type = nn	8 bits	

Code	8 bits	
CP Identifier	8 bits	
Confirmation Code	8 bits	
TLV Encoded Attributes	*variable*	TLV specific
}		

The parameters shall be as follows:

Code

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

CP Identifier

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

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 D—LE_CP message codes

	CP Message type	MAC Message Type	Protocol type	Direction
0	*Reserved*	—	—	—
1	Send-Security-Block	LE_CP-REQ	TCP	BS->BS/CIS
2	ACK-Security-Block	LE_CP-RSP	TCP	BS/CIS->BS
3	Neighbor Topology Request	LE_CP-REQ	TCP	BS-> CIS
4	Neighbor Topology Reply	LE_CP-RSP	TCP	CIS->BS
5	Registration Request	LE_CP-REQ	TCP	BS-> CIS
6	Registration Reply	LE_CP-RSP	TCP	CIS->BS
7	Registration Update Request	LE_CP-REQ	TCP	BS-> CIS
8	Registration Update Reply	LE_CP-RSP	TCP	CIS->BS
9	De-registration Request	LE_CP-REQ	TCP	BS-> CIS
10	De-registration Reply	LE_CP-RSP	TCP	CIS->BS
11	Add Coexistence Neighbor Request	LE_CP-REQ	TCP	BS->BS
12	Add Coexistence Neighbor Reply	LE_CP-RSP	TCP	BS->BS
13	Update Coexistence Neighbor Request	LE_CP-REQ	TCP	BS->BS
14	Update Coexistence Neighbor Reply	LE_CP-RSP	TCP	BS->BS
15	Delete Coexistence Neighbor Request	LE_CP-REQ	TCP	BS->BS
16	Delete Coexistence Neighbor Reply	LE_CP-RSP	TCP	BS->BS
17-255	*reserved*	—		—

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

6.1.1 Send-Security-Block message

The Send-Security-Block packet is sent using the Coexistence Protocol, over TCP and IP. This message is sent from the originated BS who initiates the protocol to the terminated BS/CIS. TCP is used instead of UDP because of its defined retransmission behavior and the need for the exchange to be reliable. The TLV encoded attributes of the Send-Security-Block message carries the security information needed by the terminated BS/CIS to decrypt and encrypt ESP packets.
The Security Block attribute is a series of TLV encodings. This block is encrypted with the terminated BS/CIS's RADIUS BSID Secret, using the BS's configured cipher. The terminated BS/CIS has to authenticate and decrypt it first before processing it.

Code: 1
Attributes are shown in Table E.

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

6.1.2 ACK-Security-Block message

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

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

Code: 2
Attributes are shown in Table F.

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

6.1.3 Neighbor Topology Request message

This message is sent by the BS to the CIS to request its neighbor topology with its geometric information.
Code: 3
Attributes are shown in Table G.

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

6.1.4 Neighbor Topology Reply message

The CIS responds to the BS' to Neighbor Topology Request with a Neighbor Topology Reply message.
Code: 4
Query results of Neighbor Topology Encodings (see *xx.xx*)
Specification of the query results of neighbor topology from CIS specific parameters.

6.1.5 Registration Request message

This message is sent by the BS to the regional LE DB to perform the registration.
Code: 5
Attributes are shown in Table H.

Attribute	Contents
BSID	The BSID of the requested BS.
BS IP [TBD]	The IP address of BS.
Operator identifier	The operator ID.
Operator contact - phone	The phone number in ASCII string of the operator.
Operator contact – E-mail	The E-mail address in ASCII string of the operator.
PHY mode	The PHY modes of the requested BS.
Latitude	The latitude information of the BS.
Longitude	The longitude information of the BS.
Altitude	The altitude information of the BS.
Operational Range at Max. Power	The maximum operational radius of the BS at Max. power.

6.1.6 Registration Reply message
The CIS responds to the BS' to Registration Request with a Registration Reply message.
Code: 6
No Attributes.

6.1.7 De-registration Request message

This message is sent by the BS to the CIS to perform de-registration.
Code: 7
Attributes are shown in Table I.

Attribute	Contents
BSID	The BSID of the request BS.

6.1.8 De-registration Reply message

The CIS responds to the BS' to De-registration Request with a De-registration Reply message.
Code: 8
No Attributes.

6.1.9 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: 9
Attributes are shown in Table J.

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.

6.1.10 Add Coexistence Neighbor Reply message

The CIS responds to the BS' to Add Coexistence Neighbor Request with an Add Coexistence Neighbor Reply message.
Code: 10
No Attributes.

6.1.11 Update Coexistence Neighbor Request message

This message is sent by the BS to the neighbor BS to request to update its neighbor list.
Code: 11
Attributes are shown in Table k.

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.

6.1.12 Update Coexistence Neighbor Reply message

The CIS responds to the BS' to Update Coexistence Neighbor Request with an Update Coexistence Neighbor Reply message.
Code: 12
No Attributes.

6.1.13 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: 13
Attributes are shown in Table L.

Attribute	Contents
BSID	The BSID of the requested BS.

6.1.14 Delete Coexistence Neighbor Reply message

The CIS responds to the BS' to Delete Coexistence Neighbor Request with a Delete Coexistence Neighbor Reply message.
Code: 14
No Attributes.

[*Insert the following section before section "2.1.2.2.1 Same PHY Profile"*]

2.1.2.2.1 Coexistence Protocol

In order to get the neighbor topology, perform registration to the database and registration to peer, negotiation for Shared RRM etc. we propose a Coexistence Protocol (CP). Figure N1 reveals the 802.16h protocol architecture. The protocol architecture indicates that DRRM, Coexistence Protocol and Shared DB belong to LE Management Part located in management plane and the messages will be exchanged over IP network. Thus, DRRM in LE Management Part uses the Coexistence protocol to communicate with other BSs and with Regional LE DB and interact with MAC or PHY. Figure N2 is LE BS architecture with Coexistence Protocol. The grey area indicates area where there is an absence of connection between blocks. DSM is Distribution System Medium which is another interface to the backbone network. Note that is architecture is only for reference. Similarly, Figure N3 is the CIS architecture with co-located regional LE database. Other architectures are not being illustrated. The Coexistence Protocol services are accessed by the LE Management Entity through CP SAP. But the service primitives will not be provided in this contribution due to the Coexistence Protocol is incomplete at this stage. This proposal only provides the definition of PDUs exchanged between peer Coexistence Protocol entities. A BS uses the Coexistence Protocol, which is similar to PKM protocol, to perform the coexistence resolution and negotiation procedures. There are two types of messages to support Coexistence Protocol:
(1) LE_CP-REQ: BS→BS or BS→CIS
(2) LE_CP-RSP: BS→BS or CIS→BS

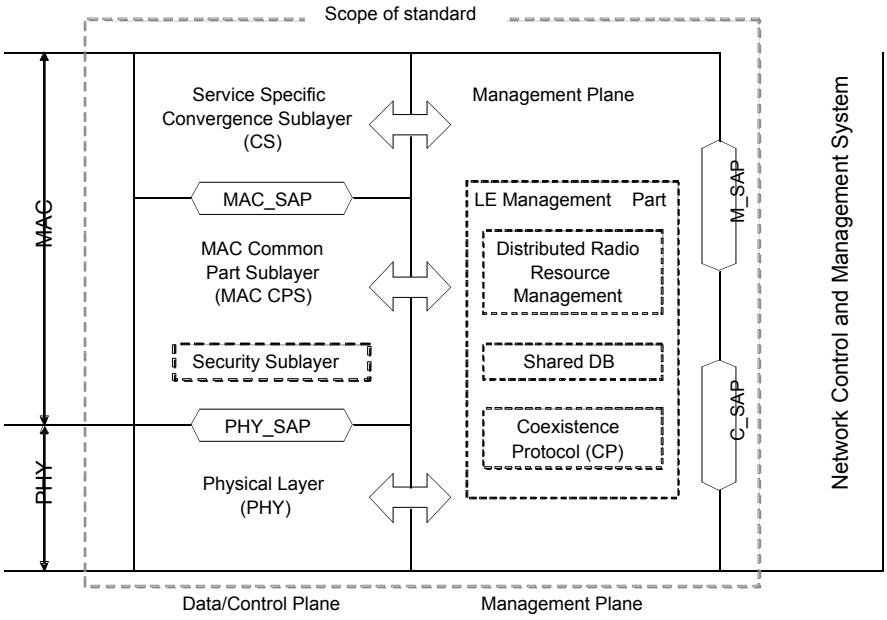

Figure N1_802.16h BS Protocol architecture Model

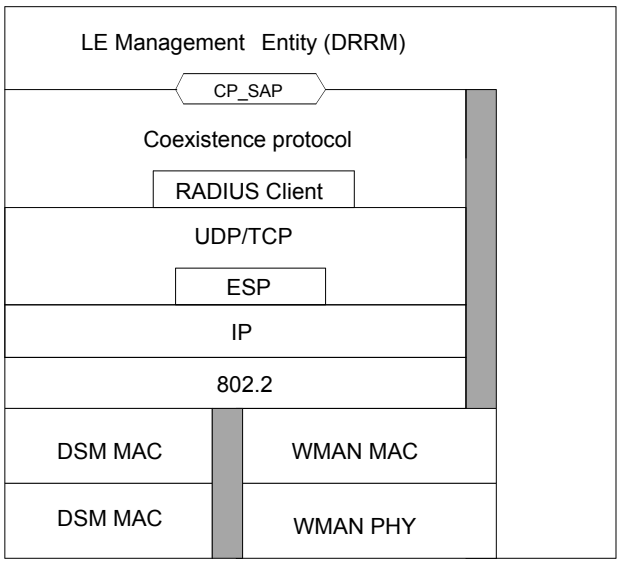

Figure N2_LE BS architecture with Coexistence Protocol

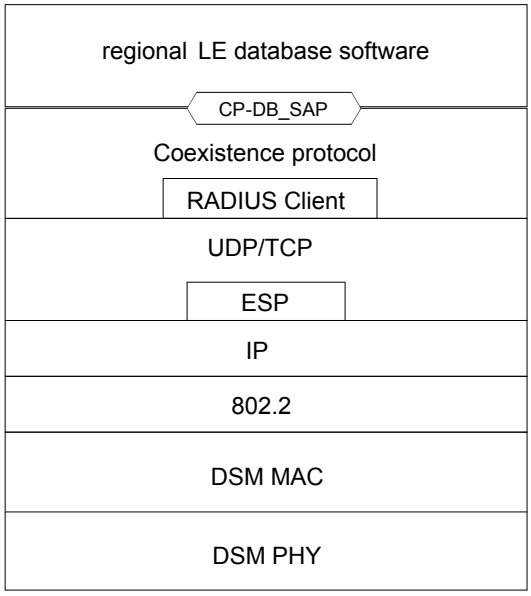

Figure N3_CIS architecture with co-located regional LE database

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

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

3.2.4 Storage of identification information

[*Replace the section "3.2.4.1 Registration data-base" with the following section*]

3.2.4.1 Regional LE database

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

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

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

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

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

Figure N4 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, R_m, at allowed maximum transmission power to query the LE DB. A BS is neighbor BS of another BS means their maximum coverages at allowed maximum transmission power overlaps. As Figure 1 depicted, the regional LE DB will return BS-1, BS-2 and BS-3 as the neighbor BSs of the new entry BS.

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

members of community will change when its working frequency changes or new interfering neighbor BS comes in. Every BS maintains the list of the member BSs forming the community. An SS will not communicate directly with a foreign BS and there is no need to register the SS location. All the Base Stations forming a community will have synchronized MAC frames.

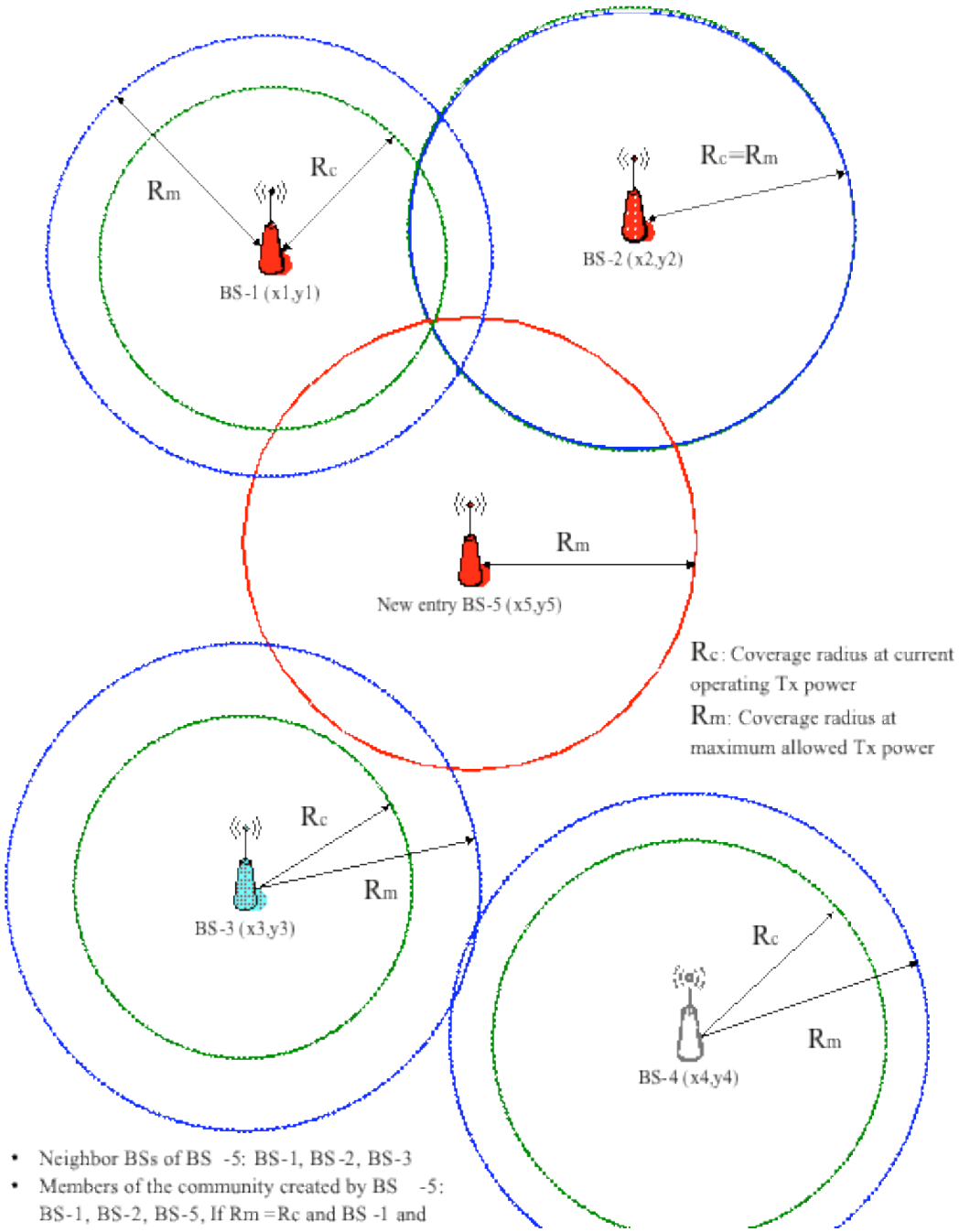

Figure N4_802.16 LE Neighbor BSs discovery and definition of neighbor and community

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

(1) *Initialization stage*
In initialization stage the LE BSs may avoid the co-channel or adjacent channel interference by scanning the available frequencies. But this method cannot avoid the *hidden* LE BS problem, i.e. the BS that cannot be heard directly but may have overlapping service coverage. Thus, with the knowledge of neighbor topology the LE BSs can detect the *hidden* LE BSs and can, therefore, avoid the possible interferences from coexisting neighbors. The procedures are described in figure N5. If the LE BS finds that there is no “free” channel, the neighbor topology provides the guidelines of with whom it should negotiate.

(2) *Operating stage*
In operating stage the LE BS has SS associated with it, however, even the operating system parameters has decided, the co-channel or adjacent channel interference from LE BSs of different network may still have a chance to happen due to the detection of interference from primary user, channel switching of neighbor BS or the entry of new neighbor BS makes the community so crowded that there is no enough channels. If the LE BS finds that there is no “free” channel at that moment, the neighbor topology provides the guidelines of with whom it should negotiate. [detailed procedures are to be defined]
Figure N5 shows the proposed initialization procedures for the 802.16 LE BSs. Note that the procedures that BS tries to create a Master slot are also applicable for operating stage. The detailed negotiation and update procedures are described in section 2.1.2.2.1.

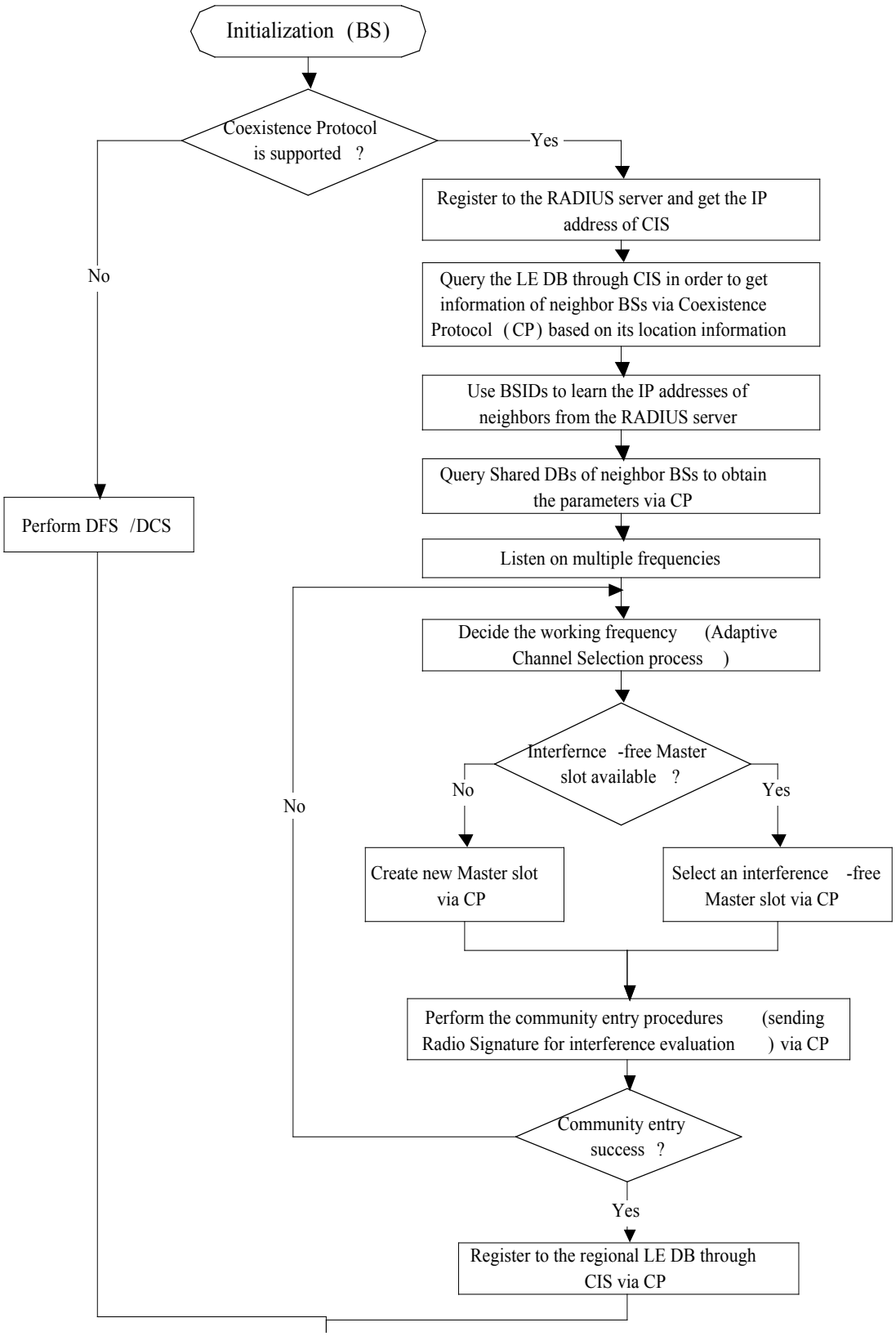

Figure N5_Initialization procedures — BS

[*Replace the section "3.2.4.2 Security" with the following section*]

3.2.4.2 Coexistence Identification Server

The coexistence resolution will rely on a regional LE DB but there should be an entity between the LE BSs and the regional LE DB in order to let the coexistence resolution processes to be independent of the database technologies. Therefore, we propose an entity named *Coexistence Identification Server* (CIS) 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. CIS converts the query results from the regional LE DB to the proper format, e.g. TLV encodings, and replies to the requested BSs. Figure N6 shows the general architecture of inter-network communication across 802.16 LE systems. In this architecture, the 802.16 LE systems (BSs and CIS) from different networks set up security association (including BS and BS, BS and CIS) with each other by utilizing the services provided by the RADIUS server. CIS 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 CIS is well known among the LE operators. The LE BSs can use the MAC address of CIS, which may be provisioned, to acquire the IP address and keys for Encapsulating Security Payload (ESP) (RFC2406:1998) operation of the CIS by utilizing RADIUS protocol. As shown in figure N6, the RADIUS server maintains the BSID and IP mapping. In summary, ESP with RADIUS can discover a Rogue BS or CIS. The messages exchanged between the LE BSs and the CIS will be revealed in the next section. Note that the interface between CIS and regional LE DB is out of scope.

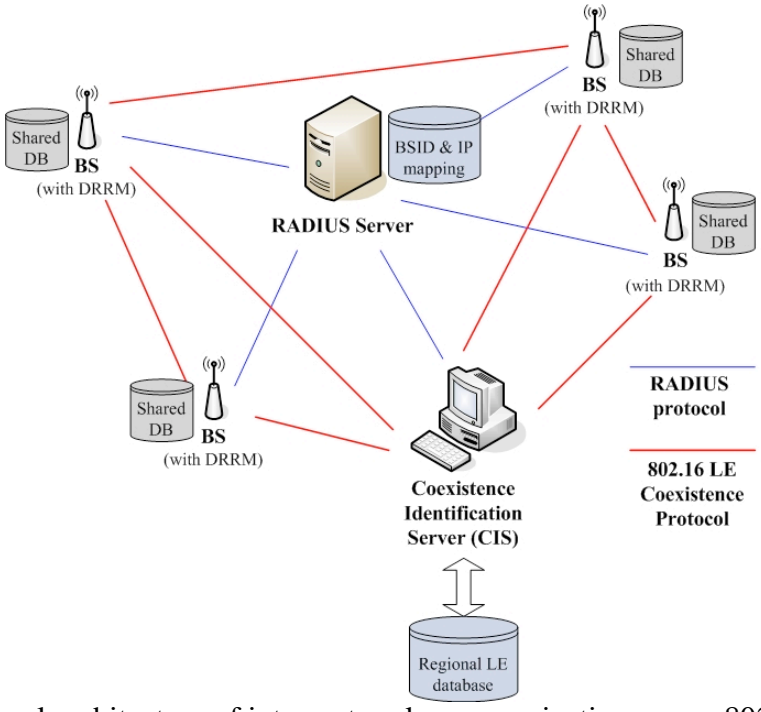

Figure N6_general architecture of inter-network communication across 802.16 LE systems

References

[1] IEEE 802.16h – 05/010 –Working Document for P802.16h, 2005-03-29
[2] IEEE S802.16h – 05/006 – Proposals for facilitating co-channel and adjacent channel coexistence in 802.16 LE, 2005-03-10
[3] IEEE C802.16h – 05/012r1 –General Architecture for Inter-network Communication Across 802.16 LE Systems, 2005-04-28
[4] IEEE Std 802.11F-2003, IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11™ Operation
[5] IEEE C802.16h – 05/008 –Proposal for 802.16h general operating principles, 2005-04-28
[6] IEEE 802.16g – 04/03r2 –Amendment to IEEE Standard for Local and Metropolitan Area Networks - Management Plane Procedures and Services (Baseline Document), 2005-04-01