# ~~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**

~~Copyright © 2005 by the Institute of Electrical and Electronics Engineers, Inc.~~
Three Park Avenue
New York, New York 10016-5997, USA
All rights reserved.

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

~~IEEE Standards Activities Department~~
~~Standards Licensing and Contracts~~
~~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]*~~

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change.~~

## Contents

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change.~~

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change.~~

~~Copyright © 2005 IEEE. All rights reserved.~~
~~This is an unapproved IEEE Standards Draft, subject to change.~~

~~Copyright © 2005 IEEE. All rights reserved.~~
~~This is an unapproved IEEE Standards Draft, subject to change.~~

**List of Figures**

~~Copyright © 2005 IEEE. All rights reserved.~~
~~This is an unapproved IEEE Standards Draft, subject to change.~~

**List of Tables**

~~Copyright © 2005 IEEE. All rights reserved.~~
~~This is an unapproved IEEE Standards Draft, subject to change.~~

**Draft Amendment to 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

*NOTE-The editing instructions contained in this corrigendum define how to merge the material contained herein into theexisting base standard IEEE Std 802.16-2004.*
*The editing instructions are shown bold italic. Four editing instructions are used: change, delete, insert, and replace. Change is used to make small corrections in existing text or tables. The editing instruction specifies the location of the change and describes what is being changed by using strike through (to remove old material) and underscore (to add new material). Delete removes existing material. Insert adds new material without disturbing the existing material. Insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. Replace is used to make large changes in existing text, subclauses, tables, or figures by removing existing material and replacing it with new material. Editorial notes will not be carried over into future editions because the changes will be incorporated into the base standard.*

## 1 Overview

### 1.1 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.

### 1.2 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 References

## 3 Definitions

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

# 4 Abbreviations and acronyms

***[Insert the following abbreviations at appropriate location:]***

| | |
|---|---|
| AH | Authentication Header |
| BSIS | Base Station Identification Server |
| CNTI | Cognitive Network Time Interval |
| CoNBR | Coexistence Neighbor |
| CR | Cognitive Radio |
| CR_NOC | Cognitive Radio Network Operations Centre. |
| CTS | Coexistence Time Slot |
| DRRM | Distributed Radio Resource Management |
| DSM | Distribution System Medium |
| ESP | IP Encapsulating Security Payload |
| IANA | Internet Assigned Numbers Authority |
| IBS | Initializing Base Station |
| IETF | Internet Engineering Task Force |
| IPBC | IP address Broadcast |
| IPsec | Internet Protocol Security |
| NOC | Network operation center |
| OBS | Operating Base Station |
| PKM | Private Key Management |
| PLE | Path Loss Exponent |
| PSD | power spectrum density |
| RADIUS | Remote Authentication Dial-in User Service |
| SAP | Service Access Point |
| SSURF | Subscriber Station Uplink Radio Frequency |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| UTC | Universal Coordinated Time |

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

# 5 Service-specific CS

# 6 MAC common part sublayer

## 6.3 Data/Control plane

## 6.3.2 MAC PDU Format

### 6.3.2.3 MAC management messages

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

***[change the section into the following text in 802.16 primary standard:]***

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

If the BS, operating in bands below 11 GHz, requires RSSI and CINR channel measurement reports, or requires neighbor detection reports,  it shall send the channel measurements Report Request message. The Report Request message shall additionally be used to request the results of the measurements the BS has previously scheduled. Table 62 shows the REP-REQ message.

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

### 6.4 MAC enhancement for coexistence

***[tbc for deriving the appropriate part from clause 15 here ]***

***[Notes: the “[WirelessHUMAN]” in section 6.4 indicate renaming is required according to meeting #40]***

### 6.4.1 Extension to [WirelessHUMAN] operation

This section describes extensions to [WirelessHUMAN] operation beyond that which is described in the sections above. Extended operation includes capability negotiation, extended channel numbering, and reporting. These aspects are discussed in the sections below.

#### 6.4.1.1 Capability Negotiation

A mechanism is provided on how [WirelessHUMAN] and non-[WirelessHUMAN] devices are to inter-work. This is an important mechanism for deployment scenarios where regulatory designation of [WirelessHUMAN] operation is required. Some examples of how the capability negotiation can be used:

- A device with [WirelessHUMAN] functionality will need to interact with infrastructure that knows nothing of [WirelessHUMAN].
- A non-[WirelessHUMAN] device will need to interact with [WirelessHUMAN] compliant infrastructure.
- A non-[WirelessHUMAN] device shall have the ability to be barred from working in a [WirelessHUMAN] network – deployment specific.
- A [WirelessHUMAN] device shall work in a non- [WirelessHUMAN] network as ‘normal’ non-[WirelessHUMAN] device.

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

#### 6.4.1.2 Extended channel numbering structure

Extended channel numbering provide an enhancement to channelization and definition of channel number in section 8.5.1. This extension provides channelization references beyond the limits of 5-6GHz as defined in that section. The channelization is defined accordingly.

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

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

*Channel Centre Frequency [MHz] = BaseChRef [MHz] + (ExChNr [MHz]. ChSp [10kHz]) [xxx]*

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

#### 6.4.1.3 Reporting

Reporting enhancements provide the ability to:

- Enhance details on environment knowledge for license-exempt operation.

# 7 Privacy sublayer

# 8 PHY

# 9 Configuration

# 10 Parameters and constants

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

# 11 TLV encodings

## 11.7 REG-REQ/RSP management message encodings

***[Insert the following row into table 369a:]***

| Type | Parameter |
|---|---|
| 45 | [WirelessHUMAN] capability |
| 46 | Base Channel Reference (BaseChRef) |
| 47 | Channel Spacing (ChSp) |

***[Notes: the "[WirelessHUMAN]" in section 11 indicate renaming is required according to meeting #40]***

### 11.7.8 SS capability encodings

***[insert new subclause 11.7.8.14:]***

### 11.7.8.14[WirelessHUMAN] capability

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

## 11.11 REP-REQ management message encodings

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

| | | | |
|---|---|---|---|
| Coexistence neighbor Interference Report | 1.9 | 1 | Bit #0: 1-include IP address received in IPBC<br>Bit #1: 1-include RSSI of CTS symbols(only valid when bit#0 is set to one)<br>Bit #2: 1-include frame number that start to receive IPBC<br>Bit #3~7: reserved, shall be set to zero |
| ExChNr | 1.10 | 2 | Physical extended channel number ([WirelessHUMAN] only) |
| Extended report type | 1.11 | 1 | Bit #0 = 1: Include extended report type A<br>Bit #1 = 1: Include extended report type B<br>Bits #2 - #7: Reserved |

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

### 11.12 REP-REQ management message encodings

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

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

***[insert the following table into 11.12 as indicates:]***

| Coexistence neighbor Interference Report type | Name | Type | Length | Value |
|---|---|---|---|---|
| all | CoNBR count /New NDS | 7.1 | 1 | Bit #0:1-New CoNBR Discovered by IPBC received<br>Bit #1-7:The number of CoNBR that interference to this SS |
| bit #0=1 | CoNBR IP address | 7.2 | 4 | 4bytes IP address of CoNBR interference to this SS,<br>255. 255. 255. 255 indicate the fail of CRC check. |
| bit #1=1 | CoNBR IP address with RSSI | 7.3 | 2 | 1byte RSSI mean (see also 8.2.2, 8.3.9, 8.4.11) for details)<br>1byte standard deviation |
| Bit #2=1 | Starting Frame Serial Number of IPBC | 7.4 | 3 | Bit# 0-24: frame number of IPBC starting frame |

| REP-REQ Extended report type | Name | Type | Length | Value |
|---|---|---|---|---|
| Bit #0 = 1 OR<br>Bit #1 = 1 | *ExChNr* | 8.1 | 2 | Extended physical channel number to be reported on. |
| Bit #0 = 1 OR<br>Bit #1 = 1 | [WirelessHUMAN] interference indicator | 8.2 | 1 | Bit #0: Low interference indication<br>Bit #1: Medium interference indication<br>Bit #2: High interference indication<br>Bit #3: Primary user detected on the channel<br>Bit #4: Channel not measured. |
| Bit #1 = 1 | Zone specific CINR report | 8.3 | 2 | 1 byte: mean<br>1 byte: standard deviation |
| Bit #1 = 1 | Zone specific RSSI report | 8.4 | 2 | 1 byte: mean<br>1 byte: standard deviation |

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

# 12 System profiles

# 13 802.16 MIB structure for SNMP

# 14 Management Interfaces and Procedures

***[insert new clause 15:]***

# 15 Mechanism for improved coexistence

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

## 15.1 General

## 15.2 Interference detection and prevention – general architecture

### 15.2.1 Operational Principles and Policies

#### 15.2.1.1 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:

- *In some circumstances,*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 not including 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; the Server and the country/region data base can be hostedby one of the operators or a trusted entity, like the local Radio Administration. Otherwise, if the region/country database is not available, the base stations should try to find its neighbor and the community topology in a coordinatively distributed fashion.
- 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

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

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 <XREF>Figure h14);

- A community of BSs is formed in an ad-hoc mode; in this community are included Base Stations, if any two of the base stations form a neighborhood or have a successive neighborhood relationship between each other;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 in IP-based communication;
  - It is no need to register the SS location.
- All the Base Stations forming a community will have synchronized MAC frames and frame number.
- A community will be limited to a reasonable size; the size limitations and interactions between different coexistence neighborhoods: t.b.d.
- All Base Stations and their networks will as a first step seek the avoidance of co-channel utilization of the same spectrum, and will be equipped with a spectrum detection and monitoring capability which will allow this.
- All base stations are synchronized to a GPS clock. The start of all MAC frame and other transaction are referenced to the rising edge of this clock.
- All base stations and their networks, operating in the LE bands, will provide the opportunity to other non-IEEE 802.16h systems to communicate their coexistence requests to the IEEE 802.16h networks.
- The IEEE 802.16h systems will recognize the use of radar and other systems having higher priority to LE spectrum.
- Every network will have a guaranteed minimum access time for the interference free use of the radio resource, being able to receive with minimum interference and to transmit at the needed powers for allowing communication between its Base Station and the remote subscribers
- ***Coexistence Neighbor (CoNBR) BSs****: The base stations could create interference to each other or that have valid SSs in the common coverage area are called Coexistence neighbor (CoNBR) BSs, and shall form a coexistence neighborhood. There are 2 basic conditions to form a coexistence 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.*
- ***Coexistence Neighbor** Networks: Coexistence Neighbor BSs & their SSs are called Coexistence Neighbor Network, and shall form a network coexistence neighbor hood.*

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

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. As example of BS to SS interference,, the radio receivers in Zone A, in the figure below, suffer from the interference (noted with ) between Network 1 and Network 2. Interference Zone B includes also the Base Station of the Network B.

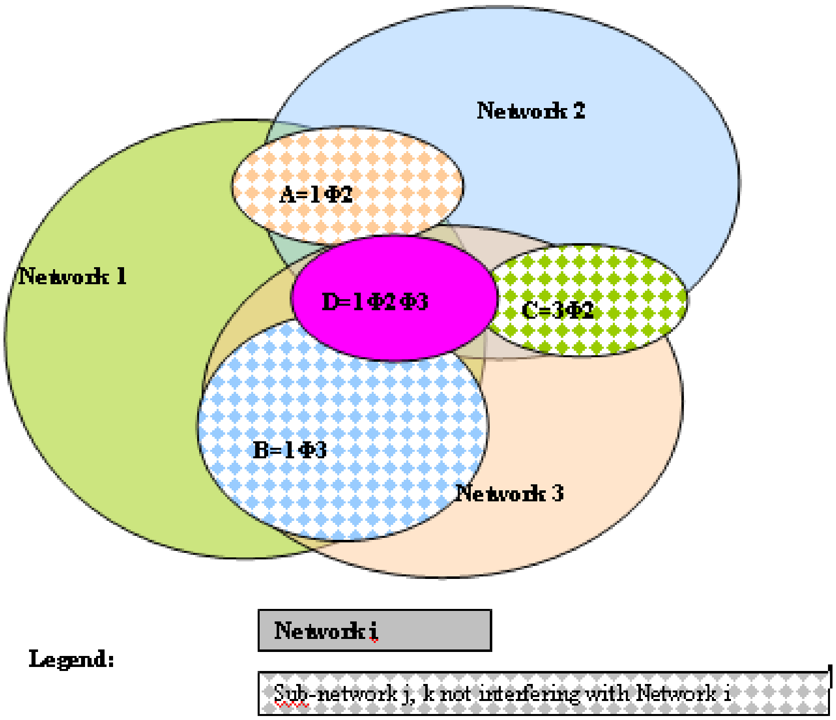


Figure h1.Interference due to overlapping networks

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.

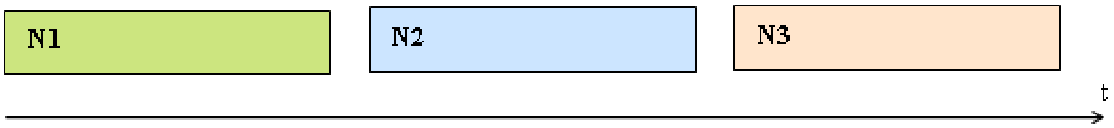


Figure h2.Equal splitting of radio resource between networks

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

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.

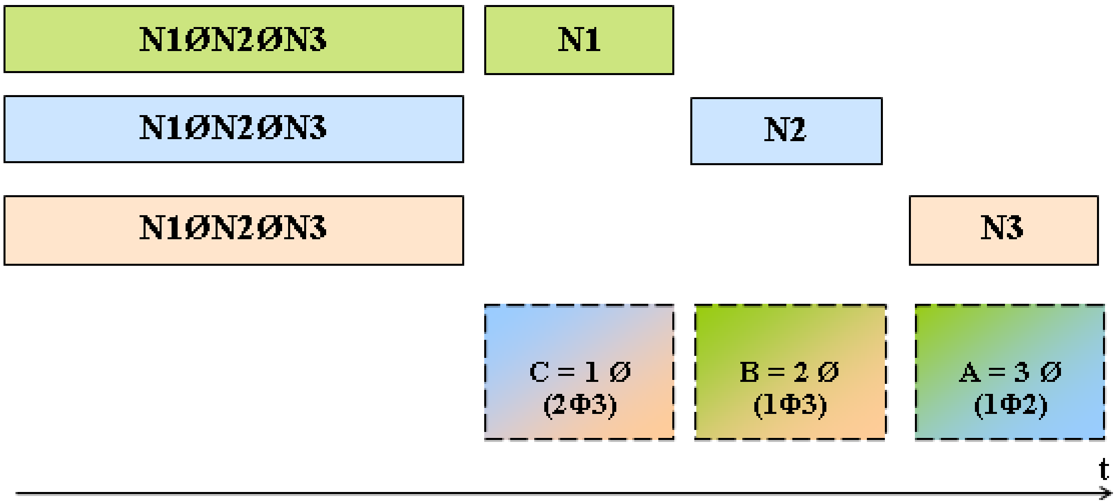


Figure h3.Usage of the spectrum by every system

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.

#### 15.2.1.1.1 Cooperation with other networks

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

#### 15.2.1.1.2 Scheduling of interference free intervals in the context of IEEE 802.16 MAC

A number of repetitive scheduling approaches are presented below, for Tx synchronized intervals. 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

~~Copyright © 2005 IEEE. All rights reserved.~~

- *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:

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

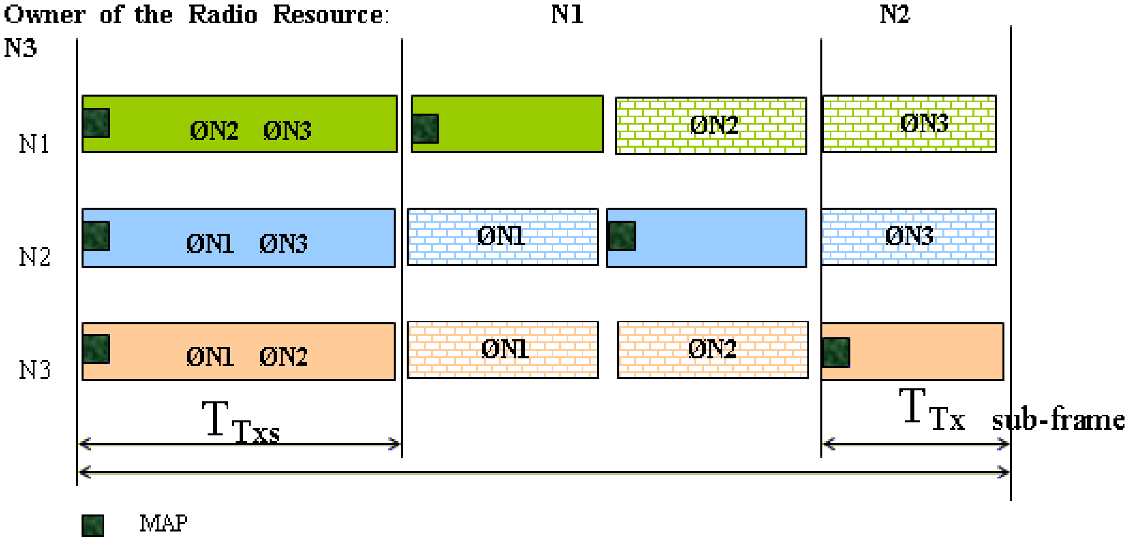


Figure h4.Sub-frame structure type1

for type 2:

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

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

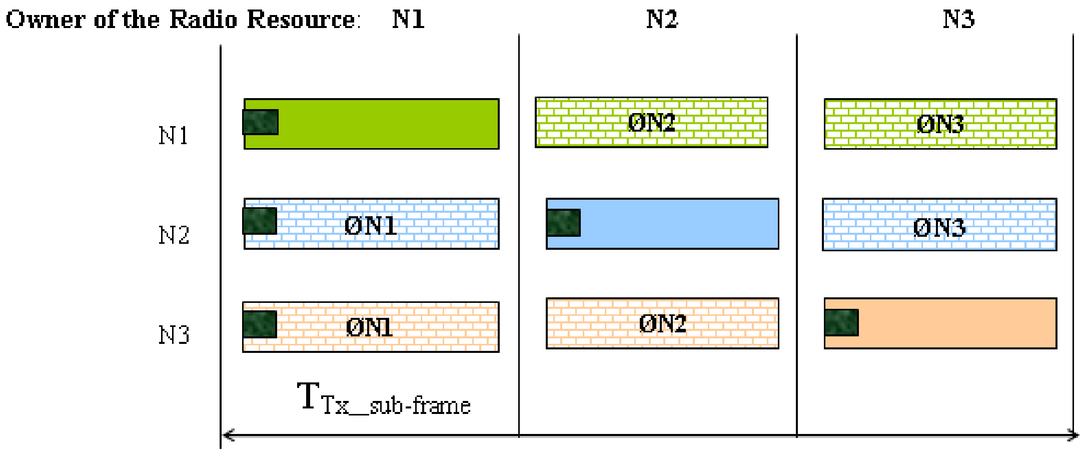


Figure h5.Sub-frame structure type 2

for type 3:

- $T_{Tx\text{–}sub\text{-}frame} = T_{TxMAC} / 2$
- $T_{Tx\text{–}sub\text{-}frame} = T_{TxMAC} - T_{Txsh}$
- $T_{Rx\text{–}sub\text{-}frame} = T_{RxMAC} / 2$
- $T_{Rx\text{–}sub\text{-}frame} = T_{RxMAC} - T_{Rxsh}$

repetition interval = $N*T_{MAC}$,

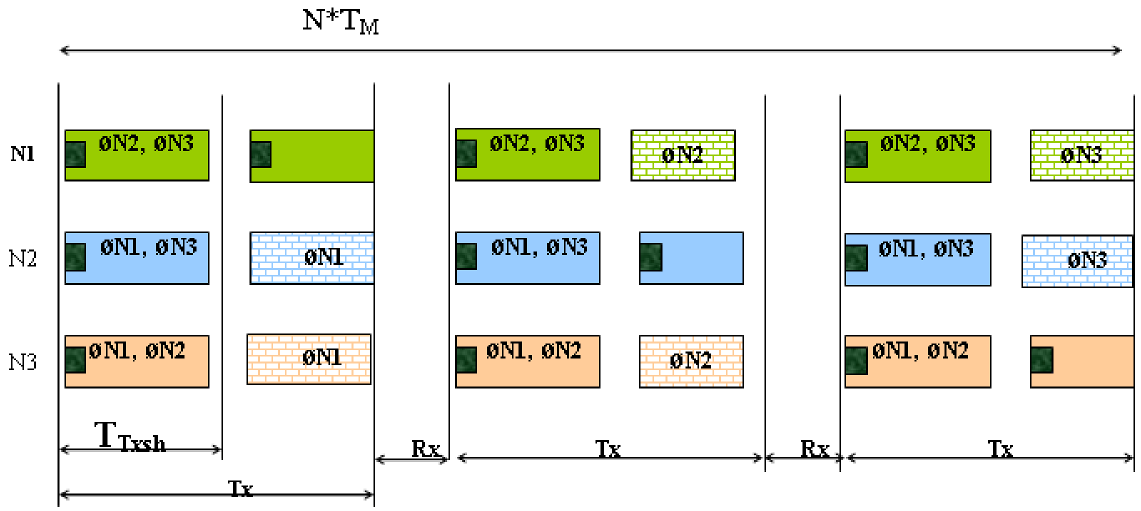


Figure h6.Sub-frame structure type 3

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.

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

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 coexistence 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.

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

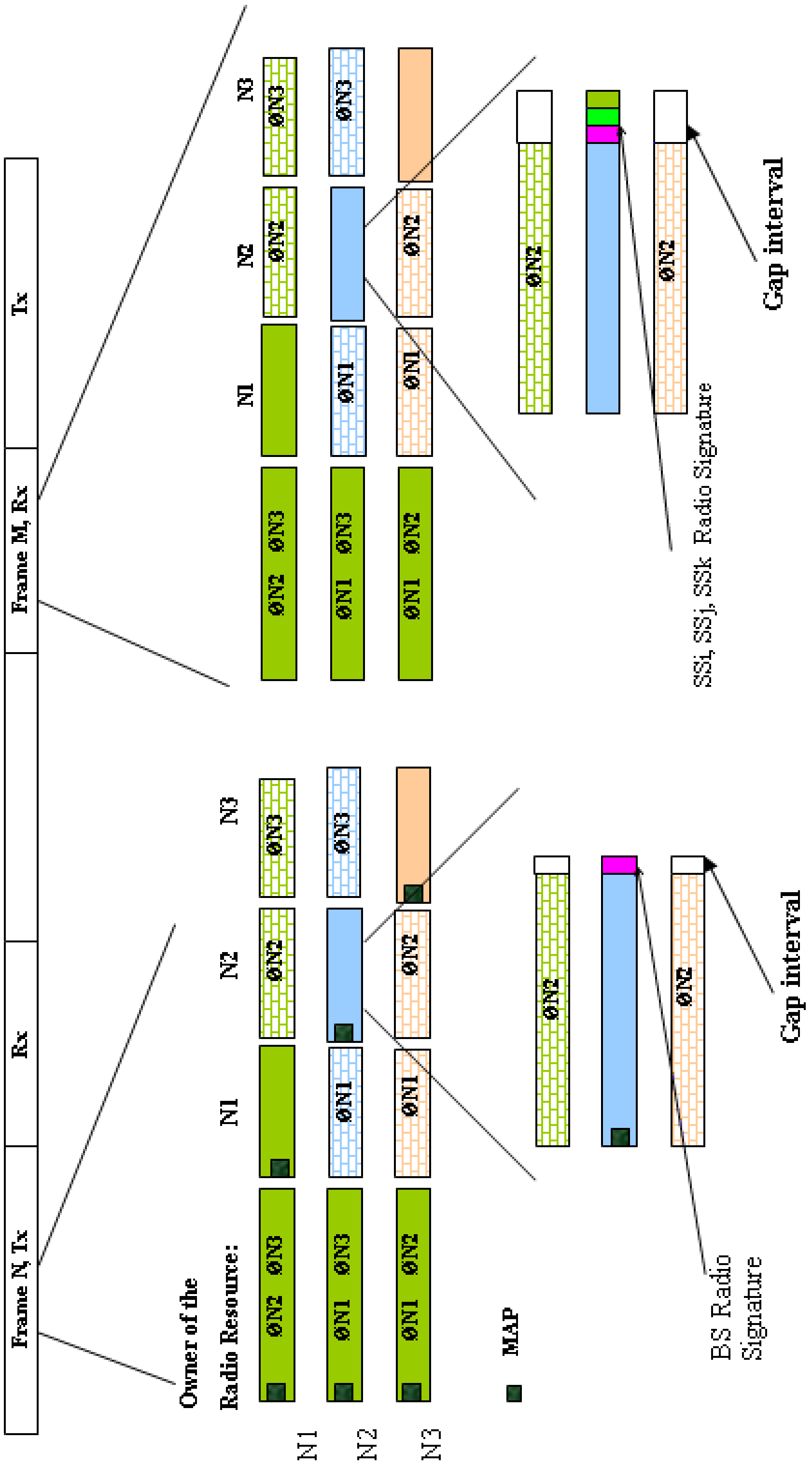


Figure h7.Allocation of slots for BS and SS radio signature

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

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

### 15.2.1.1.3 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 coexistence neighbor operating BS through one or more coexistence neighbor SSs in the common coverage area.

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

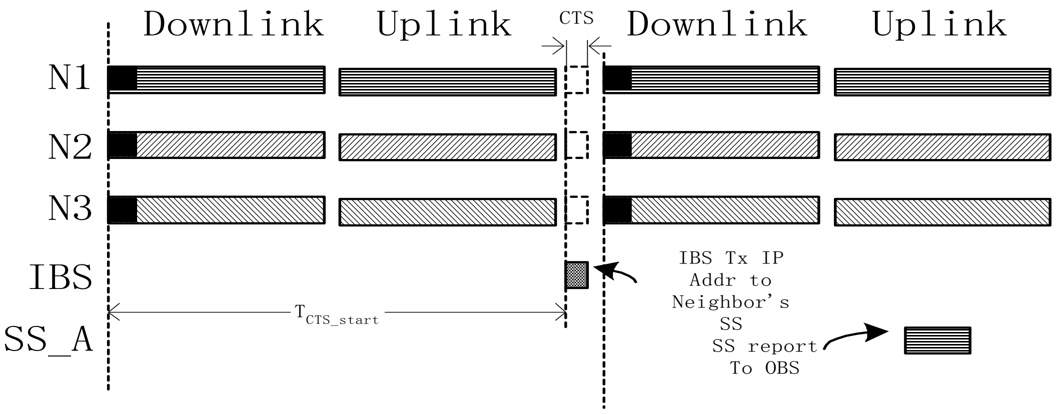


Figure h8.Timing of Coexistence Time Slot

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

Not to break the downlink PDU, and to prevent overhead of more preamble and gaps. CTS slots shall be located before RTG/TTG in TTD frame structure or before the preamble of downlink frame in FDD frame structure .To unify the location in these two kind of duplexing frame , CTS slots in FDD frame shall be put into the downlink structure right before the preamble, and shall be located right before RTG in TDD frame.

The broadcasting procedure is unidirectional, only from the IBS to the SSs in IBS/OBS's common coverage, and the SSs shall report all the useful information to their OBSs they registered to. The SSs that succeed in receiving the message should report the IP address of IBS and the frame number of the starting frame of IBS_IPBC, the SSs failed to received the broadcasting message but got IBS_IPBC like interference in the CTS should report the error status and the starting frame number of receiving the CTS interference. By the IBS IP address reported from the SSs, the OBSs will then find the IBS in the IP network, and go further signaling using IP network. And by checking the frame number in the report, OBS need to find out if the SSs that report the error status in IBS_IPBC receiving have got the same interference source, then OBS will update the database and reply to the SSs which send the error report.

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

- $T_{CTSstart}$ *CTS starting time from the beginning of the frame (ms)*
- $T_{CTSdurat}$*CTS duration time (ms)*
- $N_{CTSstart}$*CTS starting frame number frames*

- $N_{CTSintv}$ CTS interval framesframes

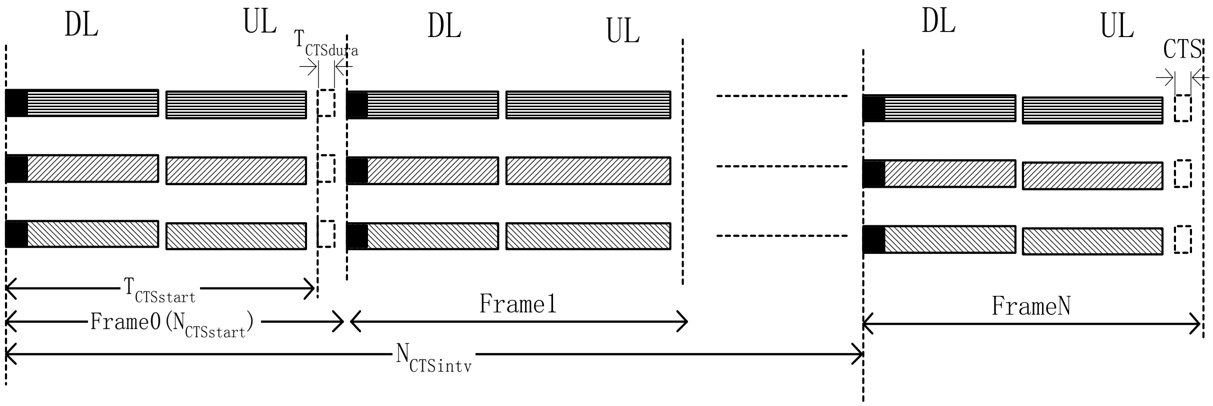


Figure h9.CTS parameters

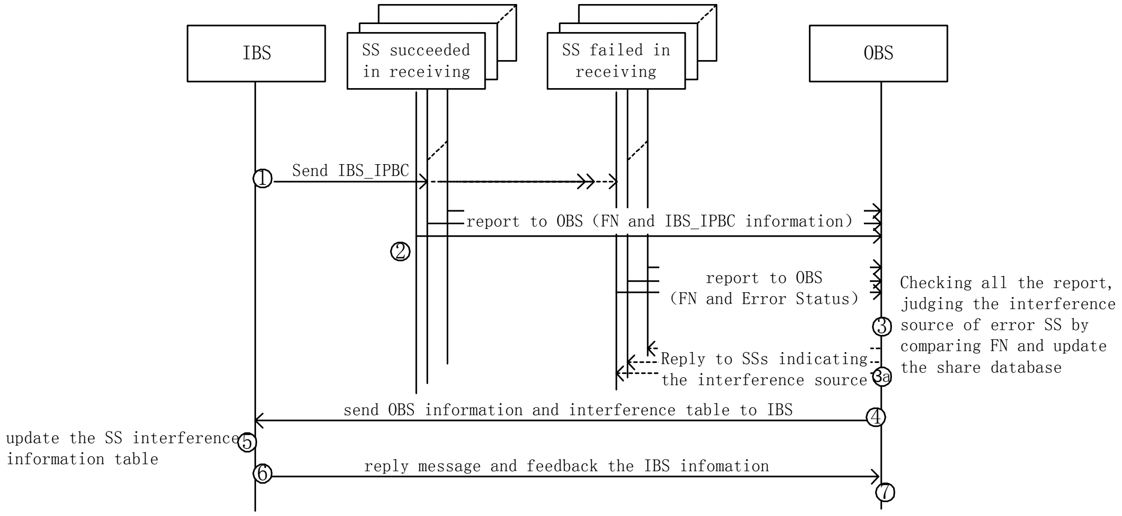

IBS
SS succeeded in receiving
SS failed in receiving
OBS
1 Send IBS_IPBC
report to OBS (FN and IBS_IPBC information)
2
report to OBS (FN and Error Status)
Checking all the report, judging the interference source of error SS by comparing FN and update the share database
3
Reply to SSs indicating the interference source
3a
send OBS information and interference table to IBS
4
update the SS interference information table
5
6 reply message and feedback the IBS infomation
7

Figure h10.CTS usage example- IBS broadcast IP address to CoNBR's SS

***[Notes: 15.2.1.1.4 & 15.2.1.1.5 is provisional, taken from C80216h-05_029 and call for comments and futher contribution]***

### 15.2.1.1.4 Energy Symbols Used in the CTS

The symbols used in the CTS slots is used to broadcast by the BS and received by the SS in coexistence neighbor network. The modulation technology on both side should be one of the3 following: SCa, OFDM or OFDMA, and could be different on two side. The band of the two side shall have overlapped part, and the bandwidth of two side could be different.

The symbol is defined only in the power and time aspect, and could use any one of the modulation technology and any band that have been used in the equipment. The length of the energy symbol shall be 1/N of the CTS length, here N is a natural number and to be consolidated in region/country regulator.

There is 4 kinds of symbols:<SOF>,0/null,1,<EOF>, to be used to form any frame in CTS.

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

Each symbol is divided into two equal length parts. And for each part, there is 2 kinds of power keying level defined, H (high) and L (low). High power level part need  the BS to use the maximum power to transmit and the SS will detect higher RSSI at that part, and the low power level part need BS to be silent and SS will detect lower RSSI at that time.

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

Table h1. CTS symbol Format

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

The receiving SS shall follow up the CTS timing and detect each symbol continuously in every symbol space. The SSs shall verdict the symbol by this aspect of RSSI and time.  One CTS consists of several symbols with the same length, the number of symbols in each CTS slot is standardized in region/country.

### 15.2.1.1.5 CTS Frame Structure

CTS frame is broadcasted from the base station to coexistence neighbor’s subscriber station. They are loaded into serialized CTS slots. It consists of power keying energy symbols as basic element and carry the information from BS to the coexistence neighbor’s SS. The CTS frame has the <SOF> symbols and <EOF> symbols as the boundary of slots, and two consecutive <SOF> and <EOF> indicate the message boundary, it shall be filled with symbol one in the rest part of last slots which have not enough payload and checking appendant.CTS frame should be continuously carried in the serialized CTS slots during the whole CTS frame structure. Each CTS frame shall have 8 bits cyclic redundancy check (Polynomial “X8+X2+X+1”) appendant to check the validity of the information carried in the CTS frame. The basic structure is shown below:

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

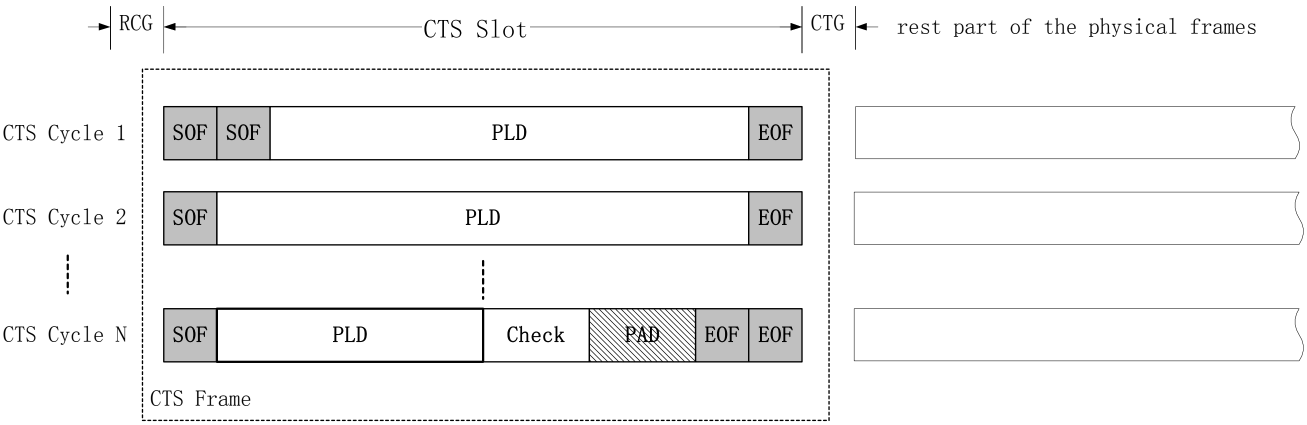


Figure h11.CTS frame construction

The PLD (payload) part of the CTS frame should be divided into TLV aspect. TYPE indicate the type of the payload, LENGTH correspond to the number of symbols/bits contained in the VALUE portion. (TYPE and LENGTH is 1 octet each.)

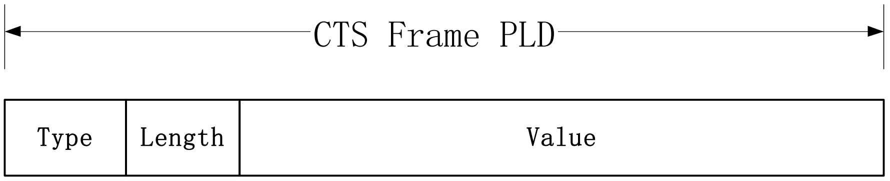


Figure h12.CTS frame PLD

### 15.2.1.2 Interference Control

Interferer identification using the radio signature

- A receiver will listen to the media during the radio signature slot 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

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

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]***

### 15.2.1.3 Community Entry of new BS

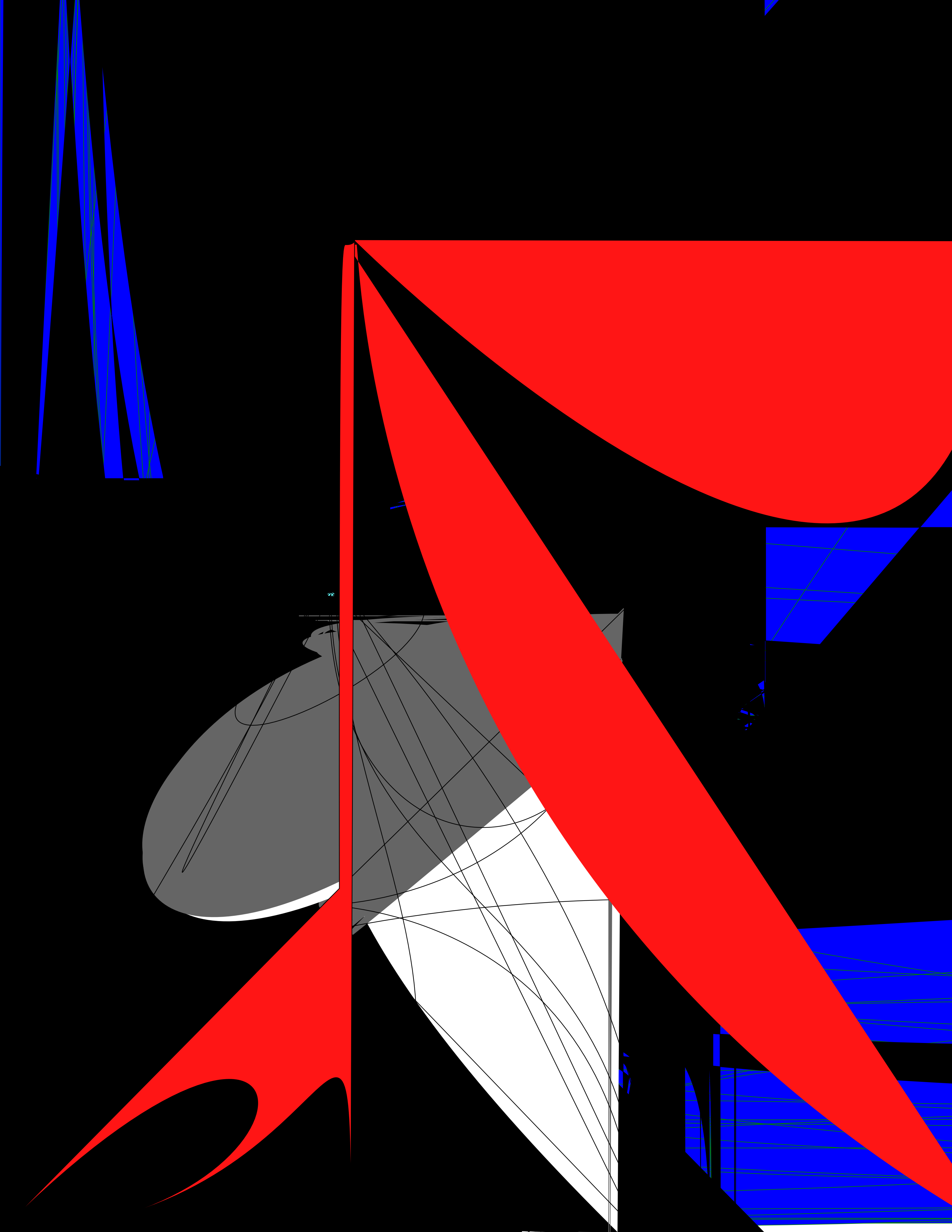
<XREF>Figure h13 explains how one new entry BS discovers its coexistence neighbor BSs. The new entry BS-5 uses its GPS coordinates (x5, y5) and its maximum coverage radius in LOS, Rm, at allowed maximum transmission power. A BS is *potential* coexistence neighbor BS of another BS if:

- In co-channel operation the LOS maximum coverage area resulting for the allowed maximum transmission power overlaps one with each other. As depicted in <XREF>Figureh 13,the regional LE DB will return BS-1, BS-2 and BS-3 as the *potential* coexistence neighbor BSs of the new entry BS.
- In first or alternate adjacent channels operation, the BS should consider the attenuation of the transmitted power, corresponding to the actual operation channels of different Base Stations

Once a LE BS has learnt its *potential* coexistence neighbor topology from the regional LE DB, it evaluates the coexisting LE BSs and identifies which BSs might create 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 coexistence neighbor BSs that create interferences to the associated SSs The members of community will change when the working frequency of any BSs changes or new interfering coexistence neighbor BS comes in.

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~



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

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 coexistence neighbor topology the LE BSs can detect the *hidden* LE BSs and can, therefore, avoid the possible interferences from coexisting coexistence neighbors. Alternatively, if the country/region database is not valid in this phase, the initializing BS will use the coexistence time slot to broadcast its IP address to its coverage using its maximum power. In this way, the SSs in the reachable zone of the new BS's interference will receive the message and forward the address to its serving BS. And after the neighbor BSs get the address via the SSs' reports, they will contact with their new coming neighbor via IP network and updating the database on both side. Thus, in ad-hoc fashion, it will avoid the hidden neighbor BS issue by the SSs in the neighbor network. If the LE BS finds that there is no "free" channel, the coexistence neighbor topology in the share database provides the information of with whom it should negotiate. LE BS may decide whether a "free" frequency can be allocated for itself by channel reallocation within community,  If IBS can figure out optimized channel distribution in the community, which made every member in the community could occupy a exclusive channel, IBS should contact the BSs in the community which need to reallocate the channel in the new distribution and negotiate, after admitted by each BS, IBS should send a message to the candidate BS to indicate the switch time and the target channel, all the candidate BS should then follow the indication and switch to the target channel synchronously. Otherwise, if IBS can't get a "free" frequency whatever reallocation executed, that means IBS should have to share a frequency with one or some of its neighbors. The procedures are described in Figure12.

(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 coexistence neighbor BS or the entry of new coexistence 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, synchronous channel switching maybe executed, or the coexistence neighbor topology provides the guidelines of with whom it should negotiate to share the channel. ***[detailed procedures are to be defined]***

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

<XREF>Figureh14 shows the initialization procedures for the 802.16 LE BSs. Note that the procedures that BS tries to create a Master slot or channel switching are also applicable for operating stage. The detailed negotiation and update procedures are described in section Coexistence Protocol and 15.7.1.4.

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

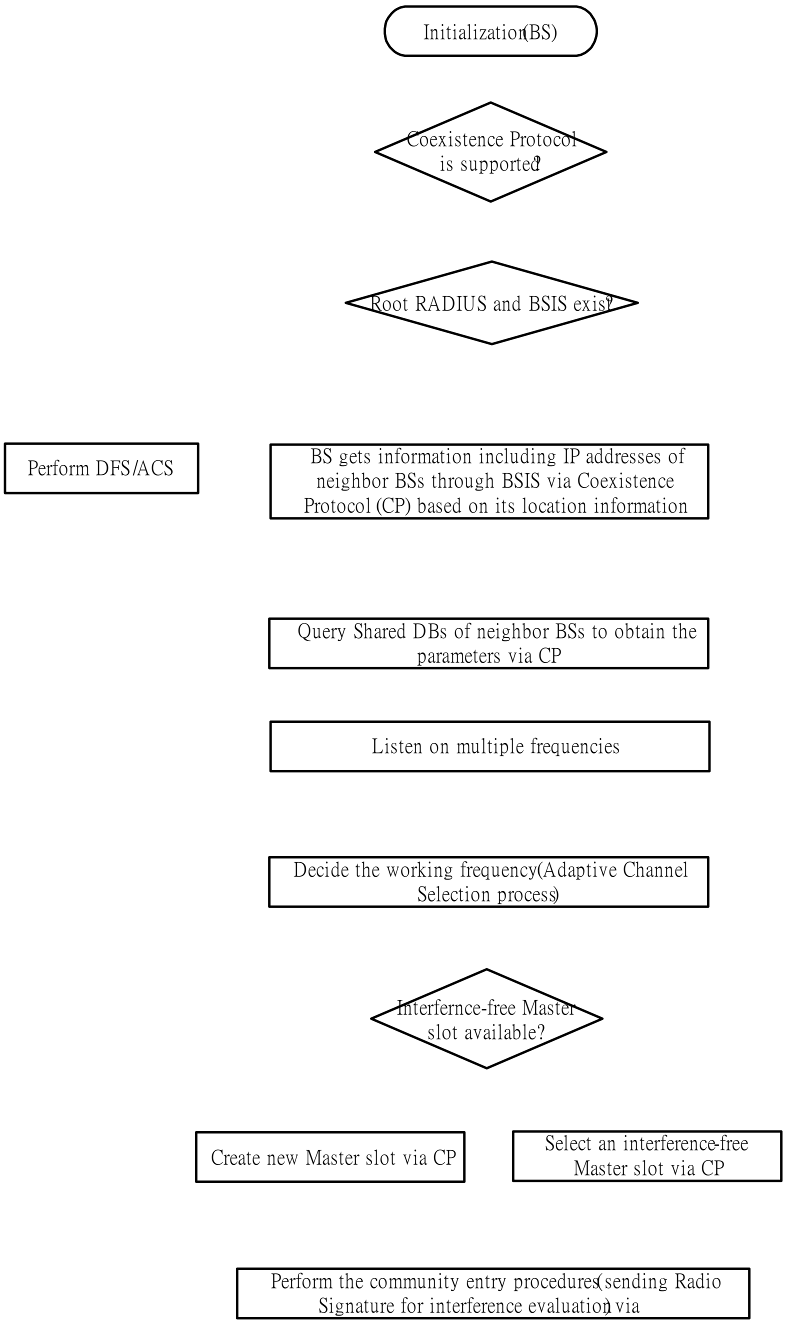

Initialization(BS)
Coexistence Protocol is supported?
Root RADIUS and BSIS exist?
Perform DFS/ACS
BS gets information including IP addresses of neighbor BSs through BSIS via Coexistence Protocol (CP) based on its location information
Query Shared DBs of neighbor BSs to obtain the parameters via CP
Listen on multiple frequencies
Decide the working frequency(Adaptive Channel Selection process)
Interfernce-free Master slot available?
Create new Master slot via CP
Select an interference-free Master slot via CP
Perform the community entry procedures(sending Radio Signature for interference evaluation) via

Figure h14.Initialization procedures — BS

***[Note: the following text needs further consideration]***

- *The first phase of* the Community Entry is to judge the validity of  country/region data base. If the country/region  Root RADIUS serveris valid(t.b.c: what means valid?),, the processfurther  queries Root RADIUS server::
  - *Get the BSISs from the country/region Root RADIUS server;*
  - *Read the data base maintained by BSIS via Coexistence Protocol;*
  - Identify which Base Stations might create interference, based on the location information;
  - The IBS learn the IP identifier  for those Base Stations;

  *Otherwise:*
  - *New BS uses the interference free slot to broadcast the message containing the contact request and/or the cognitive radio signal transmitting the IP address*
  - *The SS in the common coverage will forward the information to its operating base station. using REP_RSP message*
  - *The operating BS update its database and send feedback informationto the IBS, using the IP network*
  - *learn the IP identifier of the coexistence neighbor BS  from  the message sent by the coexistence 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 no interference detected on  some channels, select one randomly as working channel;
  - If interference detected by IBS or OBS network on all channels, then IBS should decide whether an optimized channel distribution can allocate an exclusive channel for each BSs including IBS in community.
  - If every BS in community can be allocated an exclusive channel without interfering with others, that means  default interference-free Master slot is available for this initializing BS.
- 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;*

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

- 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.

### 15.2.1.4 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.*

### 15.2.1.5 BS regular operation

- Schedule SS traffic:The traffic of each served SS should be schedule into corresponding sub-frame/resource based on the SSs’ interference situation. Traffic of SSs in the interference free zone could be scheduled into any available sub-frame/ resource of the serving BS, and traffic of SSs in the interference zone should take only corresponding master subframe/resource of the serving BS.
- 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.
- The BS need to keep updating the information of all the BS in the community including the coexistence neighbor BS, and the information of the served SSs in the own network. The information include the profile and the interference situation of the stations. The interference situation information include the interference status, the interference source and corresponding RSSI, the interference victims founded. Etc.

### 15.2.1.6 Operational dynamic changes

### 15.2.1.7 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.

### 15.2.1.8 Controlling interference during master sub-frame

#### 15.2.1.8.1 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.

In IBS’s coexistence neighbor discovery phase, the IBS’s IP address shall be broadcast using the IPBC frame with pulse energy keying. And this shall be detected by coexistence neighbor’s SS in the IBS’s reachable range and reported to its serving BS.

The IP address is used to identify the coexistence neighbor BS by the receiver SS in the IBS’s coexistence neighbor discovery phase. And also be the identifier of the IBS for the coexistence neighbor BS before the coexistence neighbor got in touch with the IBS in the IP network.

#### 15.2.1.8.2 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.

#### 15.2.1.8.3 Interference to SS

- *Report* to BS about experienced interference

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

- List of frame_number, sub-frame, offset, IP address of source BS (if detected)
- BS start process for interference reduction with *feedback from the SS.*

### 15.2.1.9 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.

### 15.2.1.10Power 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.]***

### 15.2.1.11Coexistence 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.

## 15.2.1 Shared distributed system architecture

### 15.2.1.1 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:

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

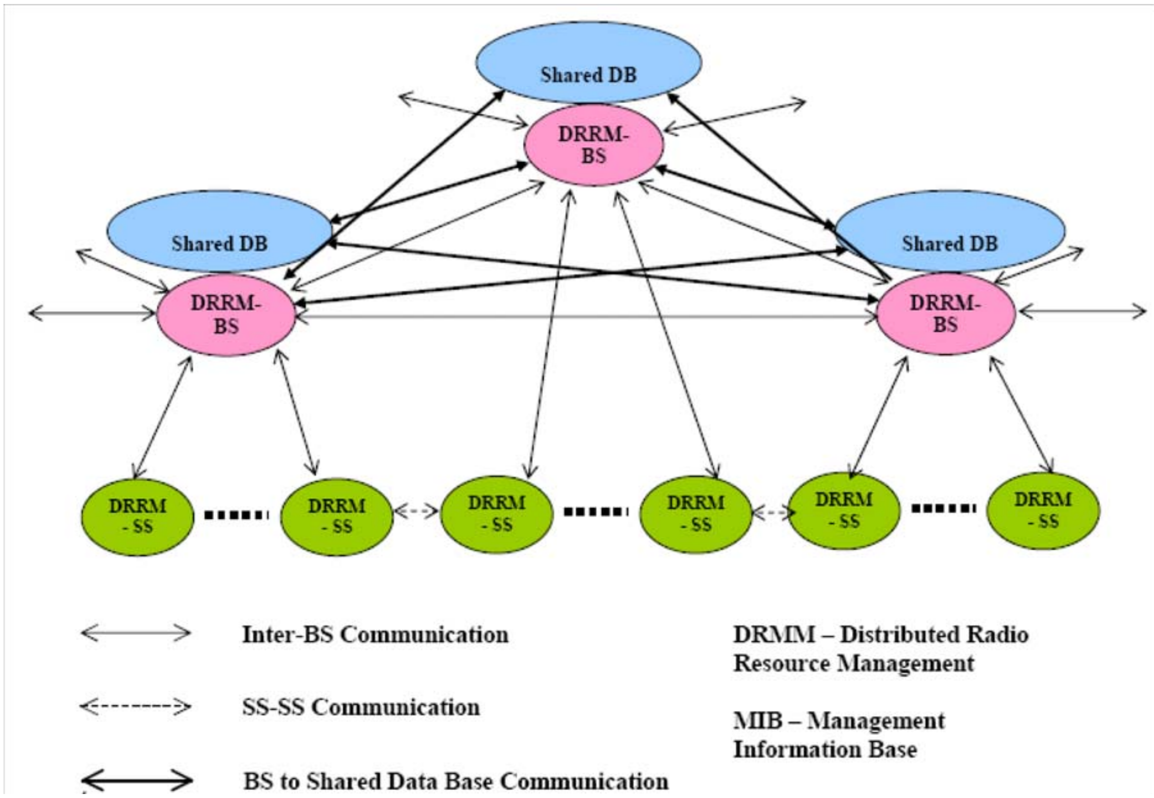
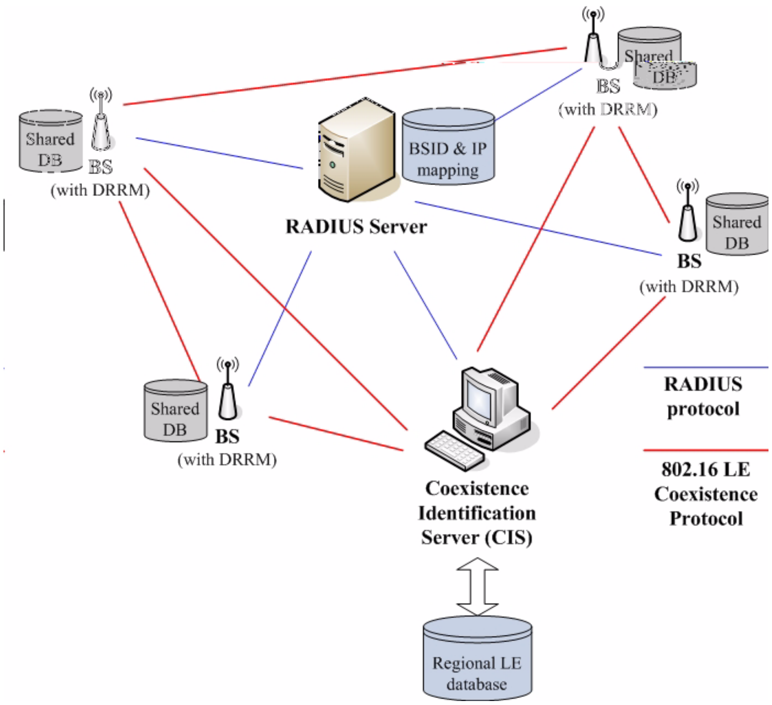


Figure h15.System Architecture

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

<XREF>Figureh14 shows the IEEE 802.16 LE inter-network communication architecture:



~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

Figure h16.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 to maintain the address mapping of wireless medium addresses of BSs (their BSID) and medium addresses of BSIS to their IP addresses.

### 15.2.1.2 Inter-network communication

The inter-network communication consists in:

- Inter-netwo*rk messages*
    - o *Base Station to/from Base Station*
    - o *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:*
    - o *To read the parameters of the hosting Base Station*
    - o *To request c*hange of the hosting Base Station operating parameters.

### 15.2.1.3 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 coexistence neighbor topology, perform registration to the database and registration to peer, negotiation for Shared RRM etc. will be used a Coexistence Protocol (CP). <XREF>Figureh20 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. <XREF>Figureh20 is LE BS architecture with Coexistence Protocol. The gray area indicates area where there is an absence of connection between blocks. DSM is Distribution System Medium which is another interface to the backbone network. Note that is architecture is only for reference. Similarly, <XREF>Figureh20 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

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

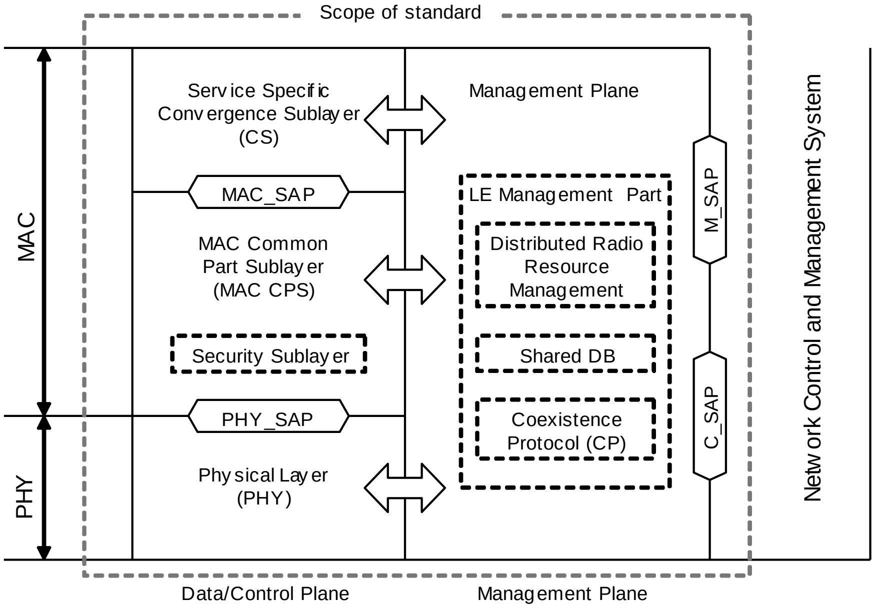


Figure h17.802.16h BS Protocol architecture Model

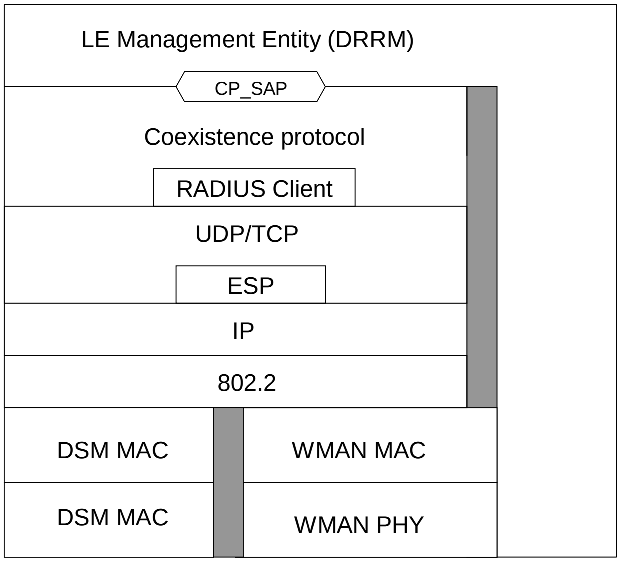


Figure h18.LE BS architecture with Coexistence Protocol

~~Copyright © 2005 IEEE. All rights reserved.~~
~~This is an unapproved IEEE Standards Draft, subject to change~~

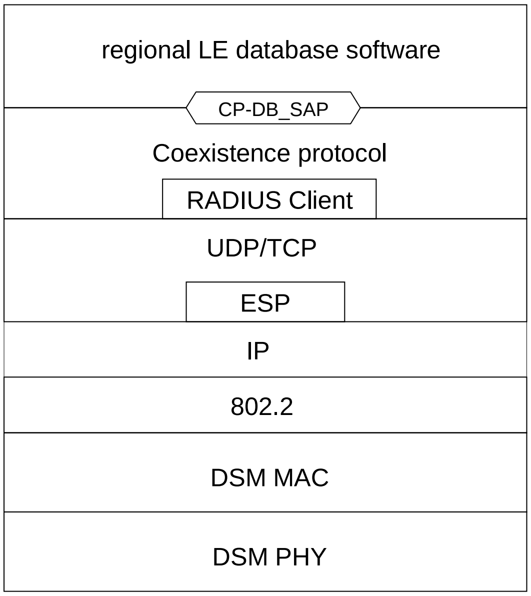


Figure h19.BSIS architecture with co-located regional LE database

### 15.2.1.3.1 Same PHY Profile

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

- Mandatory channel spacing for LE system in TBD MHz will be TBD MHz*;*
- *PHY mode:*
    - *WirelessMAN-OFDM (256 FFT points)*

      *Mandatory profiles for operation in the LE  5725-5850 MHz band will be:*
        - *profM3_pmp,profP3_10,profC3_23,TDD,profR13*
    - *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.

### 15.2.1.3.2 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 or/and by using cognitive radio signaling.

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

### 15.2.1.4 Information table in share database

Table h2. This BS information table

| Syntax | Size | Notes |
|---|---|---|
| This BS information table(){ | | |
| BSID | 48bits | |
| Operator ID | ?bits | |
| IP address | 32bits | IPv4 address |
| Master resource ID | 8bits | Sub-frame number |
| Negotiation status | 8bits | Bit0: get communication in the IP network<br>Bit1: be registered in<br>Bit2: registered to<br>Bit3: done for resource sharing(if neighboring)<br>Bit4-7: tbc. |
| CTS parameter(){ | | Regulated by region/country |
| Tcts_start | 16bits | In microseconds |
| Tcts_duration | 8bits | In microseconds |
| Period of frames | 8bits | frames |
| Starting frames offset | 16bits | frame serial number of the first frame that CTS presented |
| Length of Symbols | 8bits | In microseconds, need to be 1/n of Tcts_duration |
| } | | |
| Number of CoNBRs | 8bits | m:The number of coexistence neighbors of this BS |
| for (i= 1; i <= m; i++) { | | |
| BSID | 48bits | |
| (Tbc.) | (Tbc.) | (Tbc.) |
| } | | |
| Profile(){ | | |
| Band | | |
| PHY mode(){ | | |
| Modulation | | |
| (Tbc.) | | |
| } | | |
| Maximum power | 8 bits | dbm |
| Number of registered SS | 12bits | n |
| for (i = 1; i <= n; i++) { | | |
| SSID | 48bits | |
| (tbc.) | (tbc.) | (tbc.) |
| } | | |
| (tbc.) | (tbc.) | (tbc.) |
| } | | |
| } | | |

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

Table h3. BS information table

| Syntax | Size | Notes |
|---|---|---|
| BS information table(){ | | |
| Index | 16bits | |
| BSID | 48bits | |
| Operator ID | ?bits | |
| IP address | 32bits | IPv4 address |
| Sector ID | 8bits | |
| Master resource ID | 8bits | Sub-frame number |
| Negotiation status | 8bits | Bit0: get communication in the IP network<br>Bit1: be registered in<br>Bit2: registered to<br>Bit3: done for resource sharing(if coexistence neighboring)<br>Bit4-7: tbc. |
| Coexistence neighboring | 1bit | Coexistence neighbor with this BS?<br>1-yes<br>0-no |
| If (Coexistence neighbor){ | | |
| Number of victim SSs | 16bits | n:The number of victim SSs of this coexistence neighbor, in this network |
| for (i = i; i <= n; i++) { | | |
| SSID | 48bits | |
| RSSI | 16bits | 1byte RSSI mean (see also 8.2.2, 8.3.9, 8.4.11) for details)<br>1byte standard deviation |
| } | | |
| (Tbc.) | (Tbc.) | (Tbc.) |
| } | | |
| Number of Coexistence neighbors | 8bits | m:The number of coexistence neighbors of this BS |
| for (i= 1; i <= m; i++) { | | |
| BSID | 48bits | |
| (Tbc.) | (Tbc.) | (Tbc.) |
| } | | |
| Profile(){ | | |
| Band | | |
| PHY mode(){ | | |
| Modulation | | |
| (Tbc.) | | |
| } | | |
| Maximum power | 8 bits | dbm |
| Number of registered SS | 12bits | |
| (tbc.) | (tbc.) | (tbc.) |
| } | | |
| (tbc.) | (tbc.) | (tbc.) |
| } | | |

Table h4. SS information table

| Syntax | Size | Notes |
|---|---|---|
| SS information table(){ | | |
| Index | 16bits | |
| SSID | 48bits | |
| Interference status | 1bit | Interfered by coexistence neighbor?<br>1-yes<br>0-no |
| If (Interfered){ | | |

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

| | | |
|---|---|---|
| Number of source BSs | 8bits | n:The number of interference source of coexistence neighbor |
| for (i = 1; i<= n; i++) { | | |
| BSID | 48bits | |
| IBS_IPBC detected | 1bits | 1-yes 0-no |
| If (IBS_IPBC detected){ | | |
| IP address | 32bits | If the IBS_IPBC message detected, the IP address report by the SS will add here, and updating the bit above |
| Sector ID | ?bits | Reported by SS |
| Frame number | 24bits | Reported by SS |
| Error Status | ?bits | 0 -no error<br>1 - not capable to decode the energe pulse symbol.;<br>2 - not able to find the eligible <SOF>;<br>3 - not able to find the eligible <EOF>;<br>4 - not able to pass the CRC check for message; |
| (tbc.) | (tbc.) | (tbc.) |
| } | | |
| RSSI | 16bits | 1byte RSSI mean (see also 8.2.2, 8.3.9, 8.4.11 for details)<br>1byte standard deviation |
| (tbc.) | (tbc.) | (tbc.) |
| } | | |
| (tbc.) | (tbc.) | (tbc.) |
| } | | |
| (tbc.) | (tbc.) | (tbc.) |
| } | | |

## 15.3 Interference victims and sources

### 15.3.1 Identification of the interference situations

#### 15.3.1.1 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.

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

#### 15.3.1.2 Grouping of interfering/not-interfering units

### 15.3.1 Identification of spectrum sharers

#### 15.3.1.1 Regulations

#### 15.3.1.2 Messages to disseminate the information

#### 15.3.1.3 Avoid false-identification situations

#### 15.3.1.4 Using centralized server

***[Note: overlapping chapter]***

##### 15.3.1.4.1 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. <XREF>Figureh14 shows the general architecture of inter-network communication across 802.16 LE systems. BSIS acts as a peer of 802.16 LE BSs in this architecture. The BSID of regional BSIS is well known among the 802.16 LE systems within certain domain. The messages exchanged between the LE BSs and the BSIS will be revealed in the next section. ***Note that the interface between BSIS and regional LE DB is out of scope.***

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

## 15.4 Interference prevention

### 15.4.1 Adaptive Channel Selection – ACS

#### 15.4.1.1 Between 802.16 systems

### 15.4.1 Dynamic Frequency Selection – DFS

#### 15.4.1.1 Frequency selection for regulatory compliance

## 15.5 Pro-active cognitive approach

### 15.5.1 Signaling to other systems

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

#### 15.5.1.1 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 using a Coexistence Protocol. The ad-hoc systems obtain a temporary Community registration status, that has to be renewed from time to time.

#### 15.5.1.2 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 $N_{cogn}$ 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 Tcr_reg seconds; The ad-hoc transmitters shall use during the MAC frame N+4, the marked slot for sending

~~Copyright © 2005 IEEE. All rights reserved.~~
~~This is an unapproved IEEE Standards Draft, subject to change~~

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 Tcr_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 Tad_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 Tcr_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 Tcr_reg_ack seconds, indicates that the registration is accepted for transmission during the specific sub-frame.

### 15.5.1.3 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.

### 15.5.1.4 Signaling procedures for Cognitive Radio applications

The signaling and message exchange between an ad-hoc system and systems using a Coexistence Protocol is done as detailed below:

- 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

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

with at least 5dB higher for a bin marked in Tablex 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.

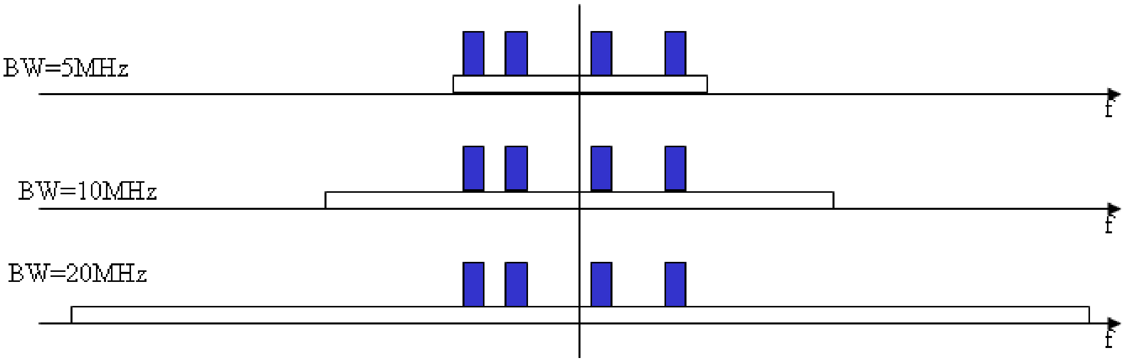


Figure h20.Desired spectral densities for different channel BWs

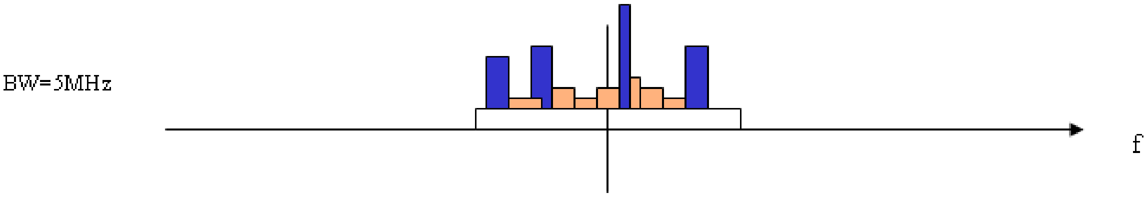


Figure h21.Obtainable spectral densities with MAC PDU approach

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. The MAC PDUs, having the spectral characteristics defined in the Table x, are defined in Chap. t.b.d for each of the 3 802.16 PHY modes.

In <XREF>Table x 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.

~~Copyright © 2005 IEEE. All rights reserved.~~
~~This is an unapproved IEEE Standards Draft, subject to change~~

Table h5. 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 (CTS_Start) | H | L | L | L | H | L | H | L | L | H |
| 8 (CTS_Continuation) | L | H | H | L | L | H | L | H | L | L |
| 9 | L | L | H | H | L | L | H | L | H | L |
| | | | | | | | | | | |

***[Note: 15.5.1.5 is provisional, taken from C80216h-05_032r1 and call for comments and further contribution]***

### 15.5.1.5 Using the coexistence slot for transmitting the BS IP identifier

The cognitive radio signaling described above may be also used for the transmission of the BS IP identifier, when there is no installed Base Station Identification Server.

The transmission is done in consecutive coexistence time slots, every NIptx MAC frames. The first CTS in the series starts with CTS start signal, the last CTS contains the Tx_end signal, the continuation in sequential MAC frames starts with the CTS_Continuation, as defined in Table x. Between these signals is transmitted the IP identifier of the BS and a 8bit CRC, the L.S.B (least significant bit) for each field being transmitted first. The transmission of the above information uses only the bins 6,8,10,12,14,18,20,22,24,26 (10bits / symbol), the L.S.B. corresponding to the lowest frequency.

The transmission of a IPV4 address will request 1+ (32+8)/10 + 1 = 6 symbols and the transmission of a IPv6 address will request 1+ceil((128+8)/10) +1 = 16 symbols.

### 15.5.1 Recognition of other systems

## 15.6 Transmission of information

### 15.6.1 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 x.

Table h6. LE_CP MAC messages

| **Type Value** | **Message name** | **Message description** |
|---|---|---|
| 0 | LE_CP-REQ | LE Coexistence Resolution and Negotiation Request |
| 1 | LE_CP-RSP | LE Coexistence Resolution and Negotiation Response |

These MAC management messages are exchanged between peers, e.g. BS and BSIS or BS and BS or BS and SS., and distinguish between CP requests (BS -> BS/BSIS/SS or SS-> BS)

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

and CP responses (BS/BSIS/SS -> BS or SS->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 or between BS and SS shall use the form shown in<XREF>. Table x.

Table h7. LE_CP message format

| Syntax | Size | Notes |
|---|---|---|
| CP _Message_Format() { | | |
| Version of protocol in use | *4* bits | *1 for current version* |
| | | |
| Code | 8 bits | See table x |
| Management Message Type | 16bits | 0-LE_CP-REQ<br>1-LE_CP-RSP |
| Length of Payload | *16*bits | |
| Confirmation Code | 8 bits | 0-OK/success<br>1-Reject-other<br>2-Reject-unrecognized-configuration-setting<br>3-Reject-unknow-action<br>4-Reject-authentication-failure<br>5-255 Reserved |
| Alignment | 4 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 in Table x.

**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

An Association ID is a parameter used to uniquely assign or relate a response to a request.

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

The association identifier used on the responder and initiator MUST be a random number greater than zero to protect against blind attacks and delayed packets.
When the initiator sends subsequent messages, it uses the responder's association identifier in the Association ID field; when the responder sends a message it uses the initiator's association identifier in the Association ID field.

**Confirmation Code**

The 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.

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

Table h8. LE_CP message codes

| Code | CP Message type | MAC Message Type | Protocol type | Direction |
|---|---|---|---|---|
| 0 | *Reserved* | — | — | — |
| 1 | Identify Coexistence Request | LE_CP-REQ | TCP | BSIS->BSIS |
| 2 | Identify Coexistence Response | LE_CP-RSP | TCP | BSIS->BSIS |
| 3 | CoNBR Topology Request | LE_CP-REQ | TCP | BS-> BSIS |
| 4 | CoNBR 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 | Channel Switch Negotiation Request | LE_CP-REQ | TCP | BS->BS |
| 38 | Channel Switch Negotiation Reply | LE_CP-RSP | TCP | BS->BS |
| 39 | Channel Switch Request | LE_CP-REQ | TCP | BS->BS |
| 40 | Channel Switch Reply | LE_CP-RSP | TCP | BS->BS |
| 41-255 | *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/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.]***

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

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

Table h9. 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 |
| Tbc | Country Code |
| Tbc | Operator contact - phone |
| Tbc | Operator contact – E-mail |
| Tbc | PHY mode |
| Tbc | Maximum coverage at Max. power |
| Tbc | Current Tx power |

### 15.6.1.1 Identify Coexistence Request message

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

Code: 1

Attributes are show in Table x

Table h10. Identify Coexistence Request message attribute

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

### 15.6.1.2 Identify Coexistence Reply message

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

Code: 2

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

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

Table h11. Coexistence neighbor Topology Parameter Set

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

### 15.6.1.3 Coexistence Neighbor Topology Request message

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

Code: 3

Attributes are shown in Table x.

Table h12. Coexistence Neighbor Topology Request message attribute

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

### 15.6.1.4 Coexistence neighbor Topology Reply message

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

Code: 4

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

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

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

Table h13. Coexistence neighbor Topology Parameter Set

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

### 15.6.1.5 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 <XREF>Table x.

Table h14. Registration Request message attributes

| Attribute | Contents |
|---|---|
| BSID | The BSID of the requested BS. |
| BS IP | 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. |
| Country code | The country code of the BS |
| PHY mode | The PHY modes of the requested BS. |
| Latitude | The latitude information of the BS. |
| Longitude | The longitude information of the BS. |
| Altitude | The altitude information of the BS. |
| Operational Range at Max. Power | The maximum operational radius of the BS at Max. power. |

### 15.6.1.6 Registration Reply message

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

Code: 6

No Attributes.

### 15.6.1.7 Registration Update Request message

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

Code:7

Attributes are shown in <XREF>Table x.

### 15.6.1.8 Registration Update Reply message

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

Code: 8

No Attributes.

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

### 15.6.1.9 De-registration Request message

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

Code: 9

Attributes are shown  in<XREF>Table x.

Table h15. De-registration Request message attributes

| Attribute | Contents |
|---|---|
| BSID | The BSID of the request BS. |

### 15.6.1.10De-registration Reply message

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

Code: 10

No Attributes.

### 15.6.1.11Add Coexistence Neighbor Request message

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

Code: 11

Attributes are shown in <XREF>Table x.

Table h16. Add Coexistence Neighbor Request message attributes

| Attribute | Contents |
|---|---|
| BSID | The BSID of the requested BS. |
| BS IP | The IP address of requested BS. |
| Operator identifier | The operator ID. |
| Country code | The country code 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. |
| Current Tx power | Current Tx power of the BS. |
| Operational Range | The operational radius of the BS. |
| PHY specific parameters | The PHY specific encodings. |

### 15.6.1.12Add 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.

### 15.6.1.13Update Coexistence Neighbor Request message

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

Code: 13

Attributes are shown  in <XREF>Table x.

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

Table h17. Update Coexistence Neighbor Request message attributes

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

#### 15.6.1.14Update Coexistence Neighbor Reply message

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

Code: 14

No Attributes.

#### 15.6.1.15Delete Coexistence Neighbor Request message

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

Code: 15

Attributes are shown in <XREF>Table x.

Table h18. Delete Coexistence Neighbor Request message attrubutes

| Attribute | Contents |
|---|---|
| BSID | The BSID of the requested BS. |

#### 15.6.1.16Delete 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.

#### 15.6.1.17Get_Param_Request message

Messages between BSs, used to request the list of parameters

Code:17

Parameters: list of the BS parameters

#### 15.6.1.18Get_Param_Reply message

Messages between BSs, reply to the Get_Param_Request

Code:18

Parameters: list of the BS parameters

#### 15.6.1.19Evaluate_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

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

Parameters:  tbc.

### 15.6.1.20Evaluate_Interference_Reply message

A message sent by the existing Master BSs, reply to the Evaluate_Interference_Request.
Code:20
Parameters:  tbc.

### 15.6.1.21Work_In_Parallel_Request message

A message sent by a new BS to request the use an existing Master sub-frame
Code: 21
Parameters:  tbc.

### 15.6.1.22Work_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.

### 15.6.1.23Quit_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.

### 15.6.1.24Quit_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.

### 15.6.1.25Create_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.

### 15.6.1.26Create_New_Sub_Frame_Request message

A message sent in response to the Create_New_Sub_Frame_Request message.
Code:26
Parameters:  tbc.

### 15.6.1.27Reduce_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.

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

### 15.6.1.28Reduce_Power_Reply message

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

Code: 28

Parameters: tbc.

### 15.6.1.29Stop_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.

### 15.6.1.30Stop_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.

### 15.6.1.31BS_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 h19. table of co-channel interference source for SS

| **Base station ID** | **Sector ID** |
|---|---|
| 123456 | 2 |
| 234534 | 4 |
| … | … |

### 15.6.1.32BS_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:

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

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.

### 15.6.1.33SS_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.

### 15.6.1.34SS_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.

### 15.6.1.35PSD_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-

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

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.

### 15.6.1.36PSD_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:

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

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

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:

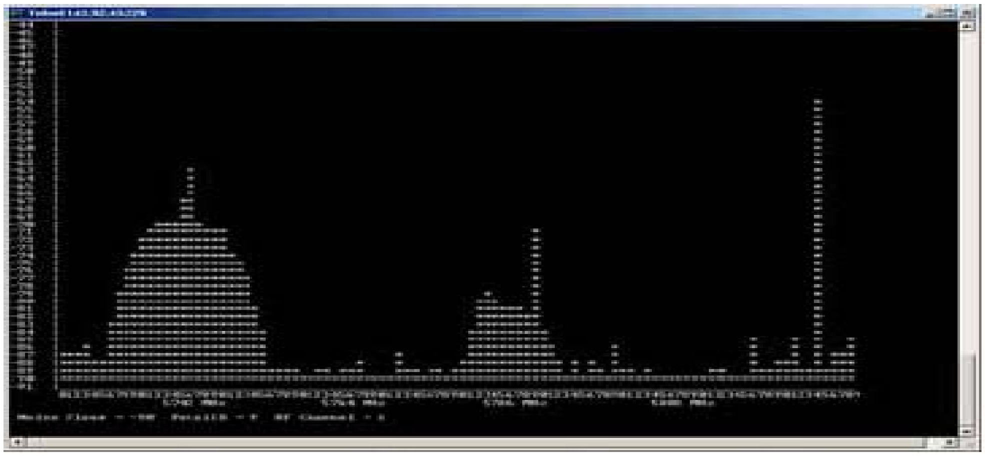


Figure h22.Example of PSD Display

### 15.6.1.37Channel Switch Negotiation Request message

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

Code: 37

Parameters: tbc.

### 15.6.1.38Channel Switch Negotiation Reply message

A message sent by BS, reply to Channel Switch Negotiation Request message about whether it agree or refuse to switch.
Code: 38
Parameters: tbc.

### 15.6.1.39Channel Switch Request message

This message is send by BS to another coexistence BS in the community to request to switch to a certain target channel.
Code: 39
Parameters: tbc.

### 15.6.1.40Channel Switch reply message

A message sent by BS, reply to Channel Switch Request message.
Code: 40
Parameters: tbc.

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

### 15.6.1 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.)

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

### 15.6.1 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-form*ed, TLVs marked as mandatory are recognized.

### 15.6.1 Fragmentation

CP does not provide support for fragmentation.

### 15.6.1 Transport Protocol

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

### 15.6.1 Using dedicated messages

#### 15.6.1.1 Common PHY

#### 15.6.1.2 Between BS and SS

***[Note: following 15.6.8.2.1 is provisional, taken from C80216h-05_029 and call for comments and further contribution]***

##### 15.6.1.2.1 IBS_IPBC

IBS_IPBC message is the message broadcasted by the initializing base station to the SS in the coexistence neighbor network. It use the CTS frame to carry the IP address information from the IBS to the SS, and the IP information shall be reported by the SS to the serving coexistence neighbor BS. And the serving coexistence neighbor BS will find the initializing BS in the IP network, and then start the further coexistence negotiation.

Table h20. IBS_IPBC messbor.72 T2(ah3IP 3Tranning)]TJ/TT8 1 Tf12 0 0 12 89.82 59.22 T

| | | | | |
|---|---|---|---|---|
| | | | IPBC_V4 0 4 | BS IP address(IPv4 |
| | | | IPBC_V6 1 16 | BS IP address(IPv6 |
| | | | | |

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

### 15.6.1.2.2 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:

| BS_ID | SECTOR_ID | DL EIRP | UPLINK RF | FRSEQ# | BS IP ADDRESS |
|---|---|---|---|---|---|
| | | | | | |

Parameters:

- 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.
- 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.
- DL EIRP: Down link EIRP of sector
- Uplink RF: Uplink RF frequency channels used by this sector
- FrSeq#: Frame sequence number
- BS IP address: IP address of the base station that broadcasts this message.

### 15.6.1.2.3 SSURF

- 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.

| BS_ID | SECTOR_ID | FRSEQ# | APL ...... | EIRP | GEOPL | CH_STATE |
|---|---|---|---|---|---|---|
| | | | | | | |

SSURF message fields are:

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

- 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.
- 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.
- FrSeq#: Frame sequence number.
- APL: Antenna parameter list giving information on antenna type (adaptive w/ parameters; beam width, polarization, diversity, etc) of SS
- EIRP: EIRP of transmitted SSURF
- GeoPl: Geographical placement of SS, Range from associated BS, GPS coordinates, etc.)
- 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.

#### 15.6.1.3 BS to BS

#### 15.6.1.4 Connection sponsorship

#### 15.6.1.5 Using a common management system

#### 15.6.1.6 Higher layers communication

#### 15.6.1.7 Decentralized control

#### 15.6.1.8 Information sharing

#### 15.6.1.9 IP / MAC address dissemination

## 15.7 Common policies

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

BS should listen on multiple frequencies during the selection of working frequency. If the interference’s level is greater than the detection threshold, which is the required strength level of a received signal within the channel bandwidth, the channel is considered as a interfered channel. If IBS can’t find a “free” channel by scanning, it should figure out whether an

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

indirect “free” channel can be found by optimized channel distribution, as described in 15.7.1.4.

Process of ACS is shown in Figure h35. ACS results two kinds of resolution, a “free” channel found with or without channel switching, or no “free” channel found.

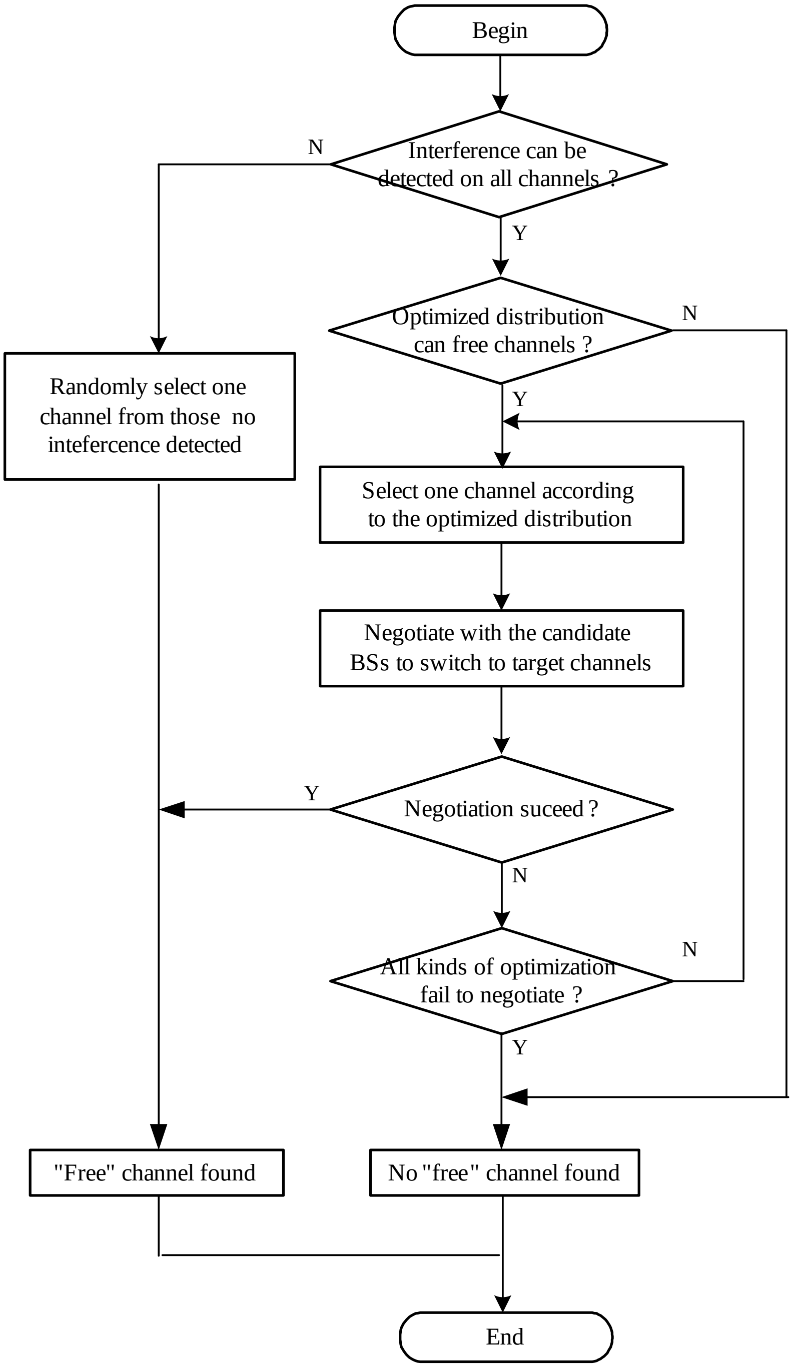

Begin
Interference can be detected on all channels ?
N
Y
Optimized distribution can free channels ?
N
Y
Randomly select one channel from those no intefercence detected
Select one channel according to the optimized distribution
Negotiate with the candidate BSs to switch to target channels
Y
Negotiation suceed ?
N
All kinds of optimization fail to negotiate ?
N
Y
"Free" channel found
No "free" channel found
End

Figure h23.Process of ACS

If a “free” channel found, means default interference-free Master slot is available, otherwise, IBS need to share the channel with coexistence neighbors, as described in 15.2.1.7.

~~Copyright © 2005 IEEE. All rights reserved.~~
~~This is an unapproved IEEE Standards Draft, subject to change~~

#### 15.7.1.1 Acceptable S/(N+I)

#### 15.7.1.2 Acceptable time occupancy

#### 15.7.1.3 Capability of sharing the spectrum

#### 15.7.1.4 Optimization of Channel Distribution

### 15.7.1 Interference reduction policies

#### 15.7.1.1 BS synchronization

##### 15.7.1.1.1 Synchronization of the IEEE 802.16h Networks

All base stations forming a community of users sharing common radio spectrum will use a common clock to synchronize their MAC frames. The common clock will be available to all outdoor IEEE 802.16h networks. Such a clock can be provided by global navigational systems such as GPS (Annex 2) or can be distributed by other mean . Every BS upon activation, will as a first step ensure the derivation of the common system clock.

###### 15.7.1.1.1.1 Network Time Interval

All synchronized IEEE 802.16h base stations will either synthesize or derive a 1 pps clock broadcast by a global navigational system or other means. The 1 sec duration is called the Network Time Interval (NTI). The rising edge of the 1 pps synchronization pulse will be considered as the start of the NTI. The 1pps pulse will have a stability of +/- 100 XX microseconds, as measured from rising edge to rising edge.

###### 15.7.1.1.1.2 Granularity of the NTI

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

###### 15.7.1.1.1.3 UTC Standard Time

The common clock specified in 15.7.2.1.1 will provide a Universal Coordinated Time (UTC) signal to all IEEE802.16h networks, making all networks synchronized to this referenced time stamp. IEEE 802.16h base stations will use the UTC time standard for coordinating and identifying specific NTI intervals.

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

##### 15.7.1.1.2 Ad-hoc

#### 15.7.1.2 Shared Radio Resource Management

##### 15.7.1.2.1 Fairness criteria

###### 15.7.1.2.1.1Power control

###### 15.7.1.2.1.2Mutual tolerance

##### 15.7.1.2.2 Distributed scheduling

###### 15.7.1.2.2.1Assignments

##### 15.7.1.2.3 Distributed power control

##### 15.7.1.2.4 Distributed bandwidth control

##### 15.7.1.2.5 Beam-forming

##### 15.7.1.2.6 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 <XREF>Figure h33. 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 The length of each master sub-frame(interference free sub-frame) can be dynamically adjusted as a function of the spatial and temporal traffic load variations of each NWas stated in section 15.2.1.1.1.
To achieve this, this section proposes the dynamic coordination of the frame structure sharing between BSs when several master NWs compete to share this common shared MAC frame.

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

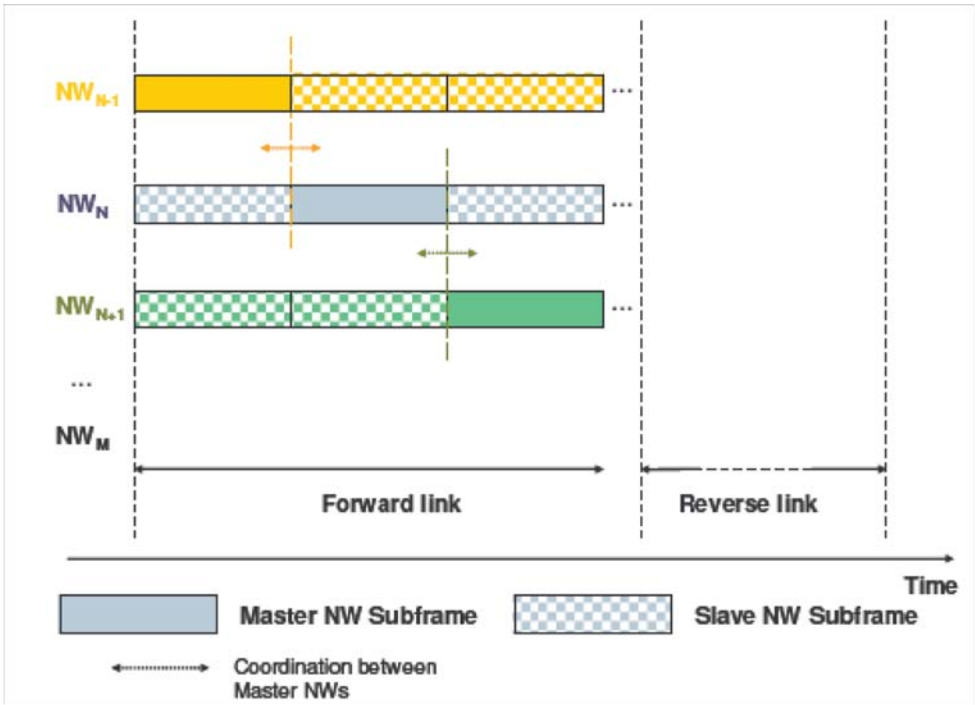


Figure h24.Example of TDD based MAC frame sharing structure between M NWs

### 15.7.1.2.6.1General principle

In order to solve contention access channel and resources scheduling issues between NWs, the first step consists in defining credit tokens and designing appropriate reserve price auctioning and bidding mechanisms. Then, on the basis of the credit tokens based mechanisms usage, the second step consists in managing dynamically(temporally) the bandwidthrequests and grants mechanisms for the sharing of the master sub frames within the common MAC frame.

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. The result is the dynamic shaping of the MAC frame structure sharing as a function of the space time traffic intensity variations, and the dynamic credit tokens portfolio account of the master NWs. The transaction mechanisms are detailed in the following sections.

### 15.7.1.2.6.2Credit 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).

~~Copyright © 2005 IEEE. All rights reserved.~~
~~This is an unapproved IEEE Standards Draft, subject to change~~

- The negotiation occurs dynamically between master NWs 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.

### 15.7.1.2.6.3Negotiation between master NWs

#### 15.7.1.2.6.3.1Definition and notation

- BSN denotes the BS belonging to the master NWN.
- BSk denotes the BS belonging to the slave NWk.
- Each BSk can dynamically make a bid BS_CT(n)k at the nth iteration. This bid corresponds to the amount of credit tokens per time unit corresponding to the BSk during the nth iteration of the auctioning/bidding phase.
- Resource scheduling is carried out by an auction like mechanism. The auction type used for the scheduling is dynamic in time. Starting from the reserved price auction RPA, the price of auction is successfully raised (at each iteration n) until the winning bidders remain.

#### 15.7.1.2.6.3.2Dynamic credit tokens based scheduling cycle

The contribution proposes a dynamic scheduling cycle between one BSN of master NWN and several BSk of different slave NWk. For the sake of simplicity, the cycle is illustrated (Figure 1 and Figure 2) for one BSN and one BSk of a given slave NWk. The cycle is composed of different phases, and each phase can be composed of several sequences as follows.

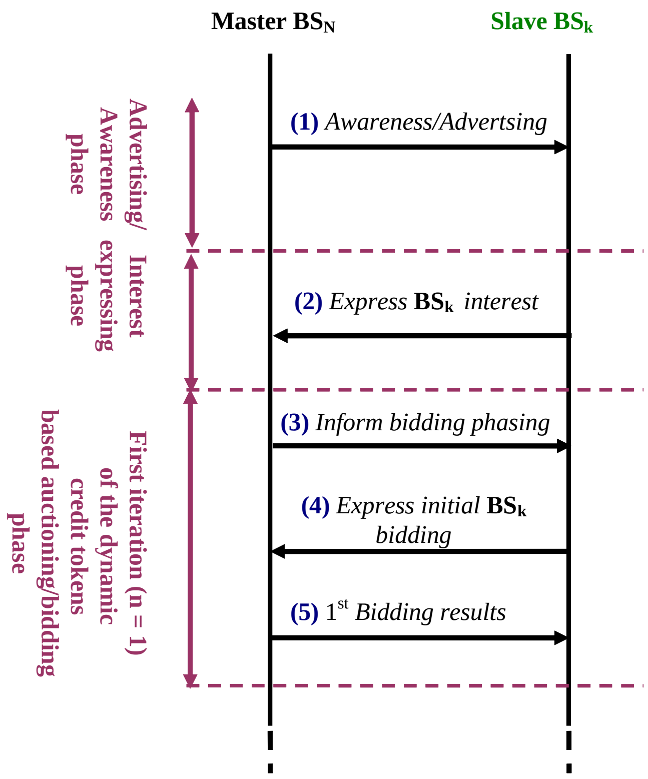

Master $BS_N$
Slave $BS_k$
Advertising/ Awareness phase
Interest expressing phase
First iteration (n = 1) of the dynamic credit tokens based auctioning/bidding phase
(1) Awareness/Advertsing
(2) Express $BS_k$ interest
(3) Inform bidding phasing
(4) Express initial $BS_k$ bidding
(5) 1st Bidding results

Figure h25.Dynamic (iterative) credit tokens based scheduling cycle – (sequences (1) to (5))

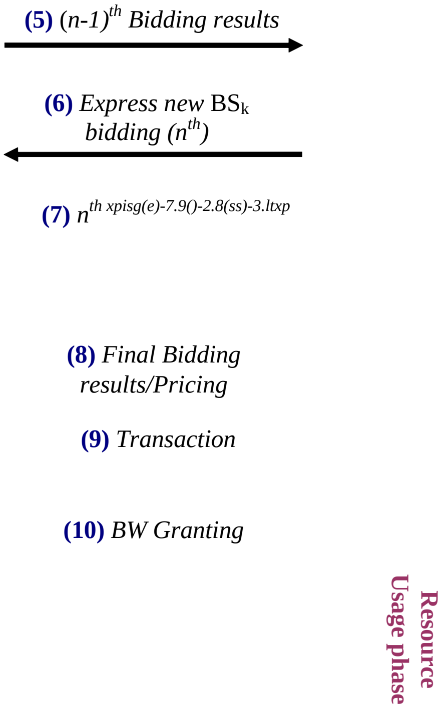

(5) (n-1)th Bidding results
(6) Express new BSk bidding (nth)
(7) nth xpisg(e)-7.9()-2.8(ss)-3.ltxp
(8) Final Bidding results/Pricing
(9) Transaction
(10) BW Granting
Resource Usage phase

Figure h26.Dynamic (iterative) credit tokens based scheduling cycle – (sequences (5) to (10))

### 15.7.1.2.6.3.3Negotiation mechanisms between master NWs

For each of the phase of the credit tokens based scheduling cycle presented in section 15.7.2.2.6.3.2, this section 15.7.2.2.6.3.3 describes the details of the enhanced mechanisms.

Figure h27.Simplified MAC frame structure illustrating master NW sub-frame renting principle and associated notations

~~Copyright © 2005 IEEE. All rights reserved.~~
~~This is an unapproved IEEE Standards Draft, subject to change~~

**Advertising/Awareness phase**

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

- The master $NW_N$ (seller) advertises that its periodic assigned master sub-frame is open for renting (Figure h34) from starting time $\mathbf{T_{Start}}$ to ending time $\mathbf{T_{End}}$ for a fraction ($\mathbf{T_{Renting}}/\mathbf{T_{Msf}}$) of its master sub-frame duration $\mathbf{T_{Msf}}$. $\mathbf{T_{Renting}} = \mathbf{T_{End\ Renting}} - \mathbf{T_{Start\ Renting}}$.
- 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.

**Interest expressing phase**

This phase is composed of the single sequence (2) as follows: each BSk informs the master BSN about its willingness (or not) to participate to the bidding. If the BSk is interested, it communicates its idk to the master BSN.

**First iteration (n = 1) of the credit tokens based auctioning/bidding phase**

This phase is divided into 3 sequences as follows:

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

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

($\{\mathbf{id}^{(1)}_{\mathbf{k,m}}\}_{\text{selected}}$ ) of $\{\mathbf{id}^{(1)}_{\mathbf{k,m}}\}$ such as sum($\mathbf{x_k}$) = **1** and sum($\mathbf{P}^{(1)}_{\mathbf{k}}$) is maximal. $\mathbf{N_{Frame\ m}}$ is the number of frames within $\mathbf{TS_m}$ ($\mathbf{N_{Frame\ m} = TS_m/ T_{Frame}}$).

- For each $\mathbf{TS_m}$, $BS_N$ informs all $\{\mathbf{id}^{(1)}_{\mathbf{k,m}}\}$ about $\mathbf{P}^{\mathbf{min,\ (1)}}_{\mathbf{m}}$ and $\mathbf{P}^{\mathbf{max,\ (1)}}_{\mathbf{m}}$ where $\mathbf{P}^{\mathbf{min,\ (1)}}_{\mathbf{m}}$ is the minimal payoff from $\{\mathbf{id}^{(1)}_{\mathbf{k,m}}\}_{\text{selected}}$ and $\mathbf{P}^{\mathbf{max,\ (1)}}_{\mathbf{m}}$ is the maximal payoff from $\{\mathbf{id}^{(1)}_{\mathbf{k,m}}\}_{\text{selected}}$ during the first iteration. With this approach, each $BS_k$ is directly informed whether it has been selected or not, and has some information on how far it is from $\mathbf{P}^{\mathbf{min,\ (1)}}_{\mathbf{m}}$ while still having some information on $\mathbf{P}^{\mathbf{max,\ (1)}}_{\mathbf{m}}$. This approach enables to keep the privacy of competing $\{\mathbf{id}^{(1)}_{\mathbf{k,m}}\}$ on $\mathbf{TS_m}$.

**n^th iteration of the credit tokens based auctioning/bidding phase**

This phase is composed of 2 sequences as follows:

- In sequence (6):
  - If $\mathbf{P}^{(1)}_{\mathbf{k}} < \mathbf{P}^{\mathbf{min,\ (1)}}_{\mathbf{m}}$, this means that $BS_k$ has not been selected for being granted the resources he has bided for during the first iteration n = 1. More generally speaking, for n>1, if $\mathbf{P}^{(n-1)}_{\mathbf{k}} < \mathbf{P}^{\mathbf{min,\ (n-1)}}_{\mathbf{m}}$**,** this means that $BS_k$ has not been selected for being granted the resources he has bided for during the (n-1)th iteration.
  - If $\mathbf{P}^{(n-1)}_{\mathbf{k}} < \mathbf{P}^{\mathbf{min,\ (n-1)}}_{\mathbf{m}}$ and if $BS_k$ is still interest to be allocated with the additional resources he initially requested for, it can propose a new $\mathbf{BS\_CT}^{(n)}_{\mathbf{k}}$ for the nth iteration. Then, $BS_k$ computes the new $\mathbf{P}^{(n)}_{\mathbf{k}} = \mathbf{BS\_CT}^{(n)}_{\mathbf{k}} * \mathbf{x_k} * \mathbf{T_{Renting}} * \mathbf{N_{Frame\ m}}$ where $\mathbf{x_k}$,$\mathbf{T_{Renting}}$ and $\mathbf{N_{Frame\ m}}$ are fixed for all n on $\mathbf{TS_m}$.
  - If $\mathbf{P}^{(n)}_{\mathbf{k}} > \mathbf{P}^{(n-1)}_{\mathbf{k}}$ and $\mathbf{P}^{(n)}_{\mathbf{k}} > \mathbf{P}^{\mathbf{min,\ (n-1)}}_{\mathbf{m}}$, $BS_k$ expresses its interest to keep on participating in the bidding with the new bid $\mathbf{P}^{(n)}_{\mathbf{k}}$. In that case, it informs $BS_N$ with its new (update) value of $\mathbf{BS\_CT}^{(n)}_{\mathbf{k}}$. In case $\mathbf{P}^{(n)}_{\mathbf{k}} = \mathbf{P}^{(n-1)}_{\mathbf{k}}$ or $\mathbf{P}^{(n)}_{\mathbf{k}} < \mathbf{P}^{\mathbf{min,\ (n-1)}}_{\mathbf{m}}$, $BS_k$ leaves the bidding phase and will not be granted with the additional resources he asked for.
- In sequence (7), $BS_N$ updates $\{\mathbf{id}^{(n-1)}_{\mathbf{k,m}}\}$ into $\{\mathbf{id}^{(n)}_{\mathbf{k,m}}\}$. Based on the new received biddings $\{\mathbf{BS\_CT}^{(n)}_{\mathbf{k}}\}$ for each $\mathbf{TS_m}$, the master $BS_N$ calculates the new payoff $\mathbf{P}^{(n)}_{\mathbf{k}} = \mathbf{BS\_CT}^{(n)}_{\mathbf{k}} * \mathbf{x_k} * \mathbf{T_{Renting}} * \mathbf{N_{Frame\ m}}$ for each bidder k who still participates to the bidding. Then, for each $\mathbf{TS_m}$, $BS_N$ searches the subset ($\{\mathbf{id}^{(n)}_{\mathbf{k,m}}\}_{\text{selected}}$) of $\{\mathbf{id}^{(n)}_{\mathbf{k,m}}\}$ such as sum($\mathbf{x_k}$) = **1** and sum($\mathbf{P}^{(n)}_{\mathbf{k}}$) is maximal. Next, $BS_N$ performs the

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

same actions as in sequence (5): for each $\mathbf{TS_m}$, $BS_N$ informs all $\{\mathbf{id^{(n)}_{k,m}}\}$ about $\mathbf{P^{min,\ (n)}\ _m}$ and $\mathbf{P^{max,\ (n)}\ _m}$ where $\mathbf{P^{min,\ (n)}\ _m}$ is the minimal payoff from $\{\mathbf{id^{(n)}_{k,m}}\}_{selected}$ and $\mathbf{P^{max,\ (n)}\ _m}$ is the maximal payoff from $\{\mathbf{id^{(n)}_{k,m}}\}_{selected}$ during the nth iteration.

### Final pricing and credit tokens transaction phase

This phase is composed of two sequences as follows:

- In sequence (8):
    - As long as $\mathbf{T_{End\ Bidding}}$ - $\mathbf{T_{Start\ Bidding}}$ > 0 (i.e. the bidding phase duration has not yet elapsed), n is increased and the credit tokens based bidding phase mechanisms of the previous paragraph "***nth iteration of the credit tokens based auctioning/bidding phase***" are applied.
    - When $\mathbf{T_{End\ Bidding}}$ - $\mathbf{T_{Start\ Bidding}}$ = 0, bidding phase is over. None $BS_k$ can propose a new bid. $\{\mathbf{id^{(n\ final)}_{k,m}}\}_{selected}$ is derived. At this point, $BS_N$ derives the clearing price auction $\mathbf{BS\_CPA_k}$ (expressed as a number of credit tokens per time unit) for each $\mathbf{TS_m}$ and each k from $\{\mathbf{id^{(n\ final)}_{k,m}}\}$. For each k and m, $\mathbf{BS\_CPA_k}$ can correspond to the $\mathbf{BS\_CT^{(final)}_k}$, or for example can follow another price auction method.
- In sequence (9), each $BS_k$ is requested to pay $\mathbf{Pr_k = BS\_CPA_k * x_k * T_{Renting} * N_{Frame\ m}}$ to be allowed to use the resources it won on its corresponding $\mathbf{TS_m}$. Provided that $\mathbf{Pr_k}$ does not exceed the credit tokens account of $BS_k$, the token transaction between $BS_N$ and each $BS_k$ is performed.

### Credit tokens based bandwidth granting phase

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

### Resource usage phase

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

### 15.7.1.2.6.4Inter 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.

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

#### 15.7.1.2.7 Legitimate Request for Bandwidth and Transmission Time

An IEEE 802.16h  network that is a member of a community of networks granted access to shared spectrum resources only if it forms an actual network comprised of at least one base station and one subscriber station and supports a bi-directional link.

#### 15.7.1.2.8 Coverage Area

#### 15.7.1.2.9 Direction of Coverage Area

#### 15.7.1.2.10Bandwidth Utilization

## ANNEX 1. Machanism of security in coexistence –reference

### A 1.1 General Principal

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

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

<XREF>Figureh14 shows the IEEE 802.16 LE inter-network communication architecture:

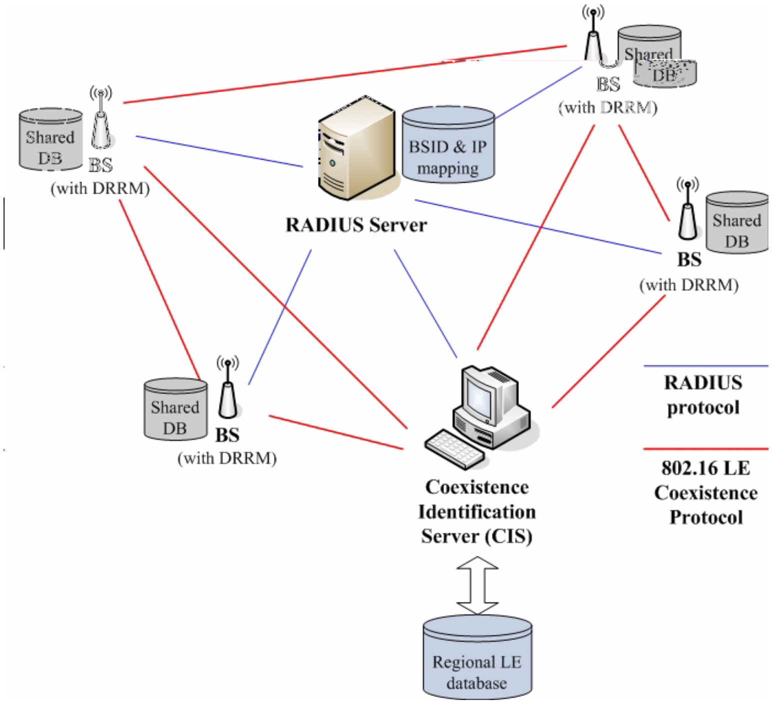


Figure h28.Network Architecture

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

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

- 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) procedureRADIUS 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 within certain management domain. BSs operating under LE system shall first query the foreign BSISs which are geographically close to the local BSIS and find the coexistence neighbor BSs while starting up, following the Coexistenceprotocol (detailed description in section 15.2.2.3). After the successful query procedure, the BS can obtain the BSIDs of the coexistence neighbor BSs. Intercommunication between BSs belonging to different networks is permitted after the BS acquires coexisting neighbor’s Pairwise Master-key. and PMK-index for ESP.

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

*Figureh15 shows the BSs/BSISs connections encrypted in IPSec. Based on IPSec, all data connections between BSs/BSISs could pass through firewalls and routers unless some firewalls block IPSec connections.*

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

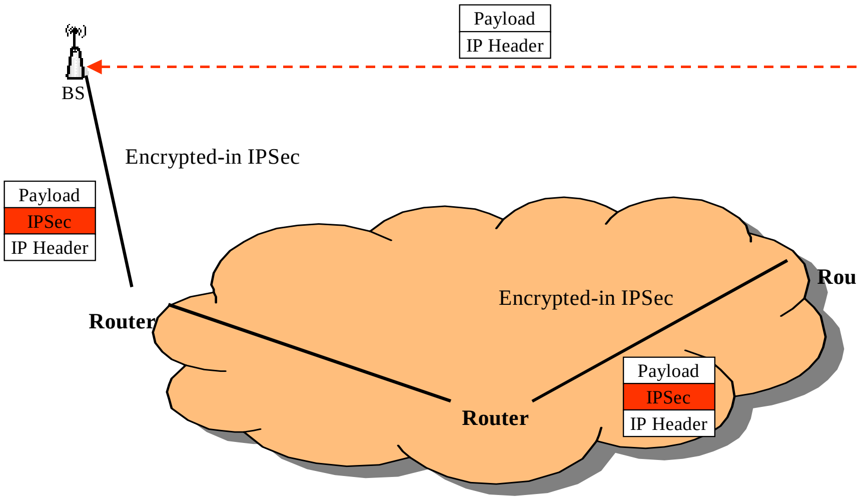


Figure h29.BSs/BSISs connection encrypted in IPSec

*Figure h15 demonstrates the IEEE 802.16 LE inter-network communication architecture under multi-Operators with multi-RADIUS Servers.*

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

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

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

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

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

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

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

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

~~Copyright © 2005 IEEE. All rights reserved.~~
~~This is an unapproved IEEE Standards Draft, subject to change~~

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

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

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

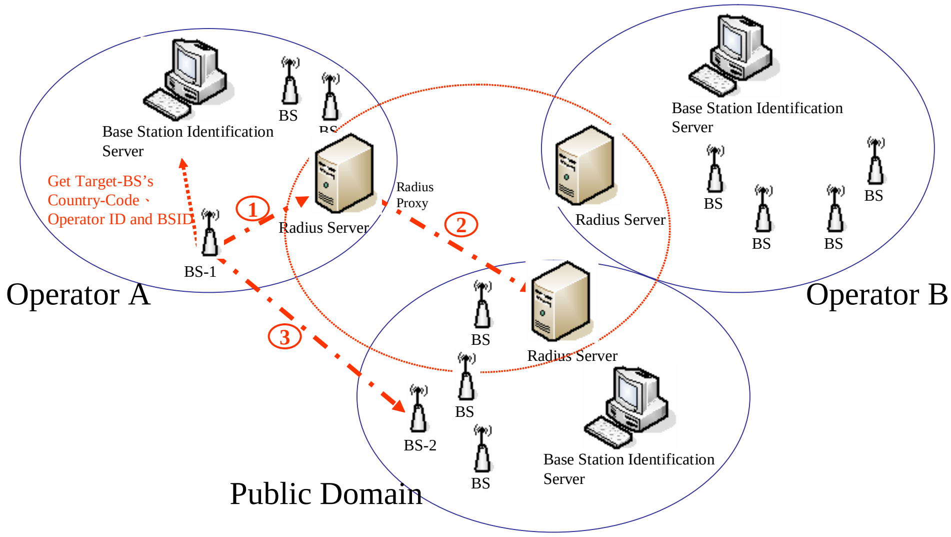

Base Station Identification Server
BS
BS
Get Target-BS's Country-Code 、 Operator ID and BSID
1
Radius Server
BS-1
Operator A
Radius Proxy
2
Base Station Identification Server
Radius Server
BS
BS
BS
BS
Operator B
3
BS
Radius Server
BS
BS-2
BS
Base Station Identification Server
Public Domain

Figure h30.Network Architecture under multi-Operators with multi-RADIUS Servers

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

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

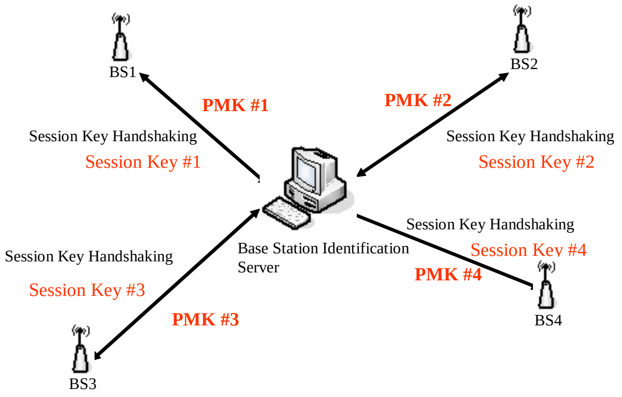


Figure h31.Individual Session-Key

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

### A 1.2 Coexistence Protocol

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

In order to get the coexistence neighbor topology, perform registration to the database and registration to peer, negotiation for Shared RRM etc. will be used a Coexistence Protocol (CP). <XREF>Figureh20 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. <XREF>Figureh20 is LE BS architecture with Coexistence Protocol. The gray area indicates area where there is an absence of connection between blocks. DSM is Distribution System Medium which is another interface to the backbone network. Note that is architecture is only for reference. Similarly, <XREF>Figureh20 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:

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

(1) LE_CP-REQ: BS→BS or BS→BSIS
(2) LE_CP-RSP: BS→BS or BSIS→BS

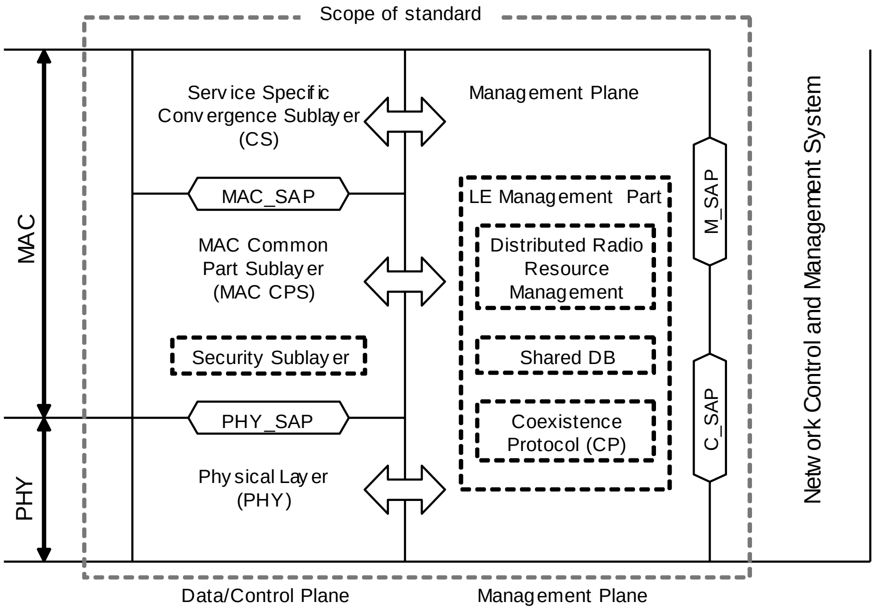

Scope of standard
MAC
PHY
Service Specific Convergence Sublayer (CS)
MAC_SAP
MAC Common Part Sublayer (MAC CPS)
Security Sublayer
PHY_SAP
Physical Layer (PHY)
Management Plane
LE Management Part
Distributed Radio Resource Management
Shared DB
Coexistence Protocol (CP)
M_SAP
C_SAP
Network Control and Management System
Data/Control Plane
Management Plane

Figure h32.802.16h BS Protocol architecture Model

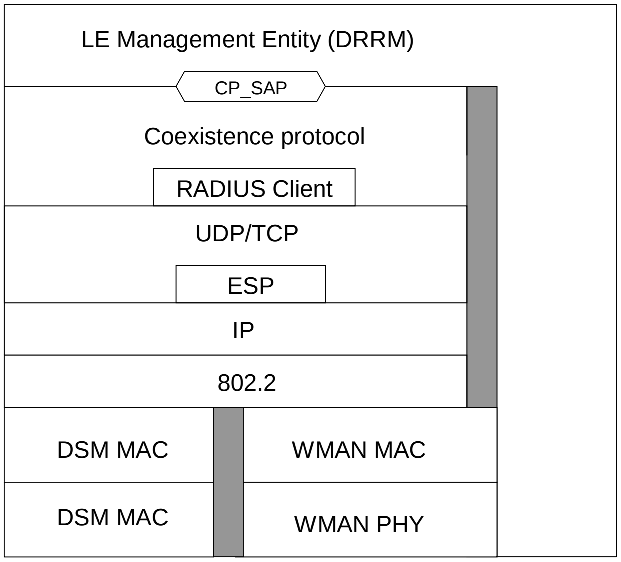


Figure h33.LE BS architecture with Coexistence Protocol

~~Copyright © 2005 IEEE. All rights reserved.~~
~~This is an unapproved IEEE Standards Draft, subject to change~~

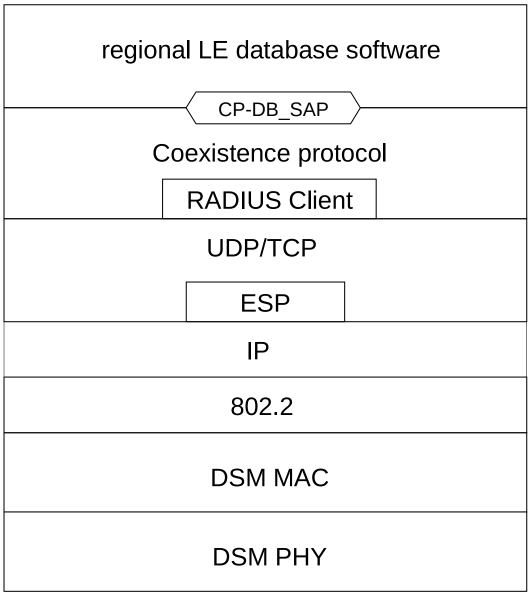


Figure h34.BSIS architecture with co-located regional LE database

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.

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

### A 1.3 Base Station Identification Server

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

The *Base Station Identification Server* (BSIS) acts as an interface between 802.16 LE BSs and the regional LE DB which stores the geographic and important operational information, e.g. latitude, longitude, BSID etc., of the LE BSs belonging to the same region. It converts the actions carried in PDUs received from the 802.16 LE BSs to the proper formats, e.g. SQL (Structured Query Language) string, and forwards the strings to the regional LE DB, which can be any available database software. BSIS converts the query results from the regional LE DB to the proper format, e.g. TLV encodings, and replies to the requested BSs. <XREF>Figureh14 shows the general architecture of inter-network communication across 802.16 LE systems. In this architecture, the 802.16 LE systems (BSs and BSIS) from different networks set up security association (including BS and BS, BSIS and BSIS) with each other by utilizing the services provided by the RADIUS server. BSIS acts as a peer of 802.16 LE BSs in this architecture. The BSID of regional BSIS is well known among the 802.16 LE systems within certain domain.In summary, ESP with RADIUS can discover a Rogue BS or BSIS. The messages exchanged between the LE BSs and the BSIS will be revealed in the next section. Note that the interface between BSIS and regional LE DB is out of scope.

### A 1.4 RADIUS Protocol Usage

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

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

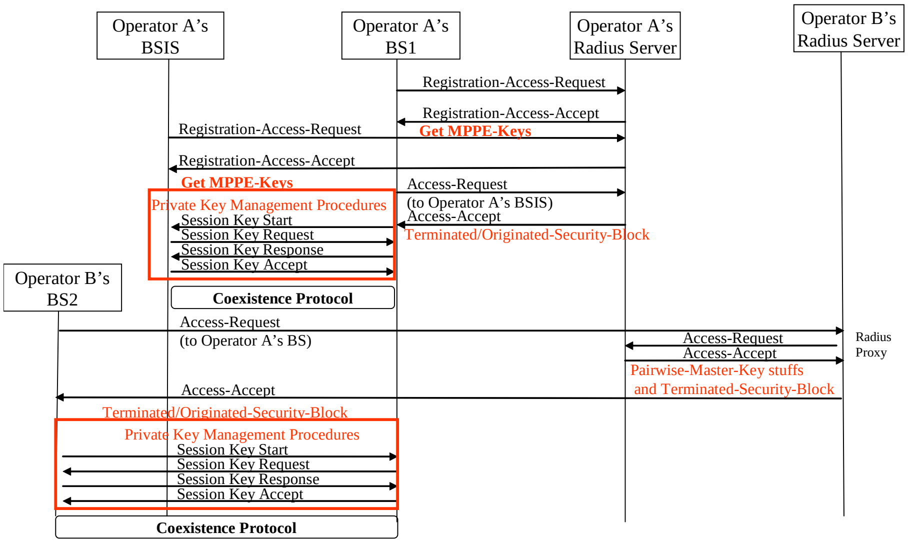


Figure h35.RADIUS protocol example

*Figure 4 shows the RADIUS protocol message exchange sequence. At starting up, each BS or BSIS must send a RADIUS-BS/BSIS-Registration-Access-Request (shown in table x) to the RADIUS server for authentication purpose and leave the address mapping (BSID to IP) information in the server. At this time, the RADIUS server will retain the following information of registered BS or BSIS:*

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

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

*Once a BS wants to get the knowledge of coexistence neighbor topology, it must first send RADIUS-BS/BSIS-Access-Request message (shown in table x) to the RADIUS server in order to acquire the regional BSIS's IP address. The wireless medium addresses of regional BSIS, similar to BSID, well known by all BSs supporting LE operation, is sent in the RADIUS-BS/ BSIS-Access-Request message to the RADIUS server for looking up IP address of the BSIS.*

~~Copyright © 2005 IEEE. All rights reserved.~~
~~This is an unapproved IEEE Standards Draft, subject to change~~

*Upon receiving the request message, the RADIUS server will respond with a RADIUS-BS/BSIS-Access-Accept message (shown in table x) if the BS is a valid member which is allowed to perform inter-communication. The RADIUS-BS/BSIS-Access-Accept message would contain Originated-BS-Security-Block(for BS encrypted in MPPE-Send-Key from current RADIUS-BS/BSIS-Access-Request/Accept message) and Terminated-BS/BSIS-Security-Block(for BSIS encrypted in MPPE-Send-Key from BSIS's RADIUS-BS/BSIS-Registration-Access-Request/Accept message). Security-Block (shown in table x) contains Pairwise Master Key IndexPairwise-Master-KEYKey Lifetimethe list of ESP Authentication/Transform IDs for initiator-send/receive for establishing a secure connection with the BSIS .*

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

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

Table h21. Security Block Format

| **Element ID** | **Length** | **Information** |
|---|---|---|
| 1 | 1 | Pairwise Master Key Index for BS/BSIS (0-255) |
| 2 | 32 | Pairwise-Master-KEY |
| 3 | 4 * number | The list of ESP Authentication IDs corresponding to the ESP Authentication algorithms for initiator-send |
| 4 | 4 * number | The list of ESP Transform IDs corresponding to the ESP transforms for initiator-send |
| 5 | 4 * number | The list of ESP Authentication IDs corresponding to the ESP Authentication algorithms for initiator-receive |
| 6 | 4 * number | The list of ESP Transform IDs corresponding to the ESP transforms for initiator-receive |
| 7 | 4 | Pairwise-Master-KEY Lifetime |

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

b(1) = MD5(MPPE-Send-Key+BSID) c(1) = p(1) xor b(1) C = c(1)
b(2) = MD5(MPPE-Send-Key+BSID + c(1)) c(2) = p(2) xor b(2) C = C + c(2)
. .
. .
. .
b(i) = MD5(MPPE-Send-Key+BSID + c(i-1)) c(i) = p(i) xor b(i) C = C + c(i)

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

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

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

### A 1.5 Privacy Key Management protocol usage

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

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

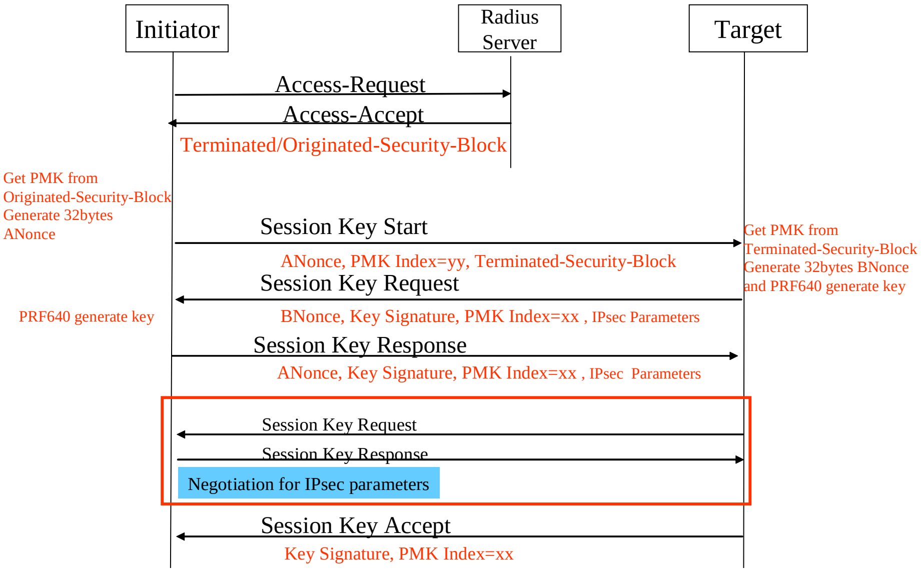

Initiator
Radius Server
Target
Access-Request
Access-Accept
Terminated/Originated-Security-Block
Get PMK from Originated-Security-Block Generate 32bytes ANonce
Session Key Start
Get PMK from Terminated-Security-Block Generate 32bytes BNonce and PRF640 generate key
ANonce, PMK Index=yy, Terminated-Security-Block
Session Key Request
PRF640 generate key
BNonce, Key Signature, PMK Index=xx , IPsec Parameters
Session Key Response
ANonce, Key Signature, PMK Index=xx , IPsec Parameters
Session Key Request
Session Key Response
Negotiation for IPsec parameters
Session Key Accept
Key Signature, PMK Index=xx

Figure h36.Figure 5 PKM Session-Key-Handshaking procedures

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

*(1) PKM-Initiator would get Pairwise-Master-Key-IndexPairwise -Master-KeyESP Authentication/Transform IDs and Key-Lifetime in originated Security-Block in RADIUS-BS/BSIS- Access-Accept message and then generate a random 32-bytes ANonce.*

*(2) PKM-Initiator would will send Session-Key-Start message to PKM-Target with "ANonce""Pairwise-Master-Key-Index" and "Terminated Security-Block".*

*(3) After receiving Session-Key-Start message, PKM-Target would generate a random 32-bytes BNonce. And perform the PRF640 algorithm to generate the 640-bits Key. Keep the first 512-bits ESP-Transform/Authentication Keys and use the last 128-bits M-Key as the HMAC-MD5 key to generate 16-bytes Key-Signature.*

*(4) PKM-Target would will send Session-Key-Request message to PKM-Initiator with "BNonce""Pairwise-Master-Key-Index" and " ESP Authentication/Transform IDs"(PKM-Target chosen).*

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

*(5) After receiving Session-Key-Request message, PKM-Initiator would perform the PRF640 algorithm to generate the 640-bits Key. Keep the first 512-bits ESP-Transform/ Authentication Keys and use the last 128-bits M-Key as the HMAC-MD5 key to generate 16-bytes Key-Signature to verify the Key-Signature field on the Session-Key-Request message. If it is wrong, PKM-Initiator would perform silent-drop and doesn't response any message. If it is correct, PKM-Initiator would prepare the Session-Key-Response message and use HMAC-MD5 generate Key-Signature filed.*

*(6) PKM-Initiator would will send Session-Key-Response message to PKM-Target with "ANonce""Pairwise-Master-Key-Index" and " ESP Authentication/Transform IDs"(PKM-Initiator chosen) .*

*(7) After receiving Session-Key- Response message, PKM-Target would check the ANonce value if equal to the previous ANonce value in Session-Key-Start message and use HMAC-MD5 generate Key-Signature filed to verify the Key-Signature field. Compare the values of "ESP Authentication/Transform IDs" to make sure the security parameters.*

*(8) After the above, PKM-Target will send Session-Key-Accept with Key-Signature filed to PKM-Initiator to verify.*

*(9) The following IPsec connection will use the first 512-bits ESP-Transform/Authentication Keys from PRF640 as keys and perform the ESP-Transform/Authentication algorithms from chosen ESP Authentication/Transform IDs.*

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

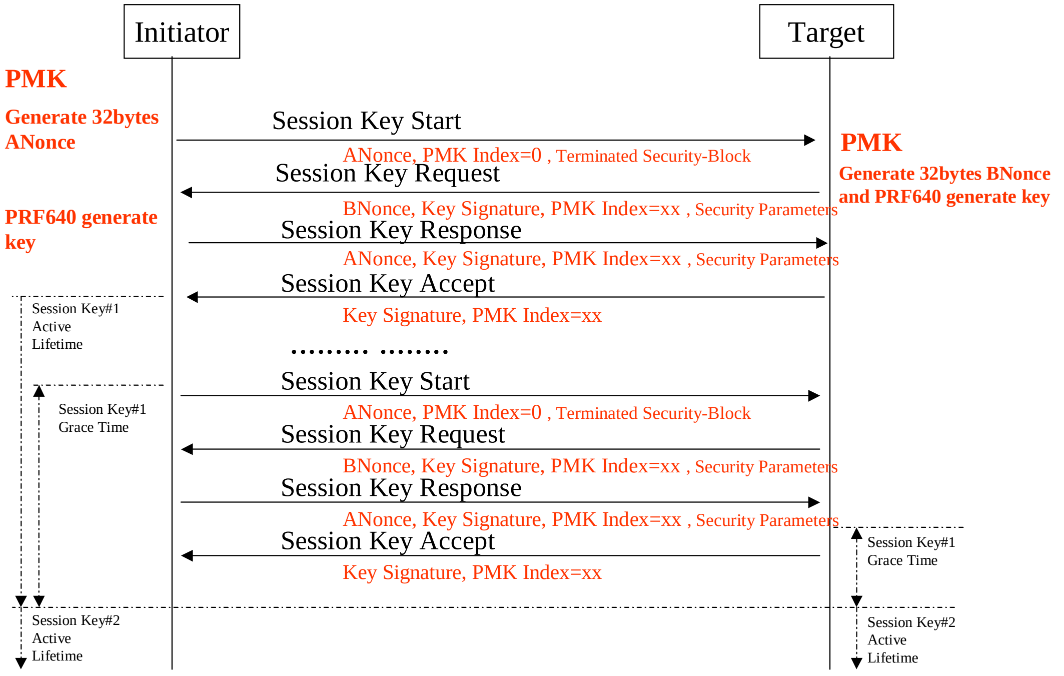

Initiator
Target
PMK
Generate 32bytes ANonce
PRF640 generate key
Session Key Start
ANonce, PMK Index=0 , Terminated Security-Block
PMK
Generate 32bytes BNonce and PRF640 generate key
Session Key Request
BNonce, Key Signature, PMK Index=xx , Security Parameters
Session Key Response
ANonce, Key Signature, PMK Index=xx , Security Parameters
Session Key Accept
Key Signature, PMK Index=xx
Session Key#1 Active Lifetime
......... ........
Session Key Start
ANonce, PMK Index=0 , Terminated Security-Block
Session Key#1 Grace Time
Session Key Request
BNonce, Key Signature, PMK Index=xx , Security Parameters
Session Key Response
ANonce, Key Signature, PMK Index=xx , Security Parameters
Session Key Accept
Key Signature, PMK Index=xx
Session Key#1 Grace Time
Session Key#2 Active Lifetime
Session Key#2 Active Lifetime

Figure h37.Figure 6 PKM Session-Key Re-Key procedures

*Each Session-Key would set a Key-Lifetime, and PKM-Initiator could set a Session-Key grace time to perform Session-Key-Handshaking for the next new Session-Key#2 to be*

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

*generated until the end of the key lifetime. The Session-Key#1 could use up its lifetime and then activate the Session-Key#2. If each side use the Session-Key#2 first in IPsec connection, it could also activate the Session-Key#2. If the lifetime of Session-Key#1 use up, the PKM-Initiator doesn't perform the Session-Key Re-Key procedures. PKM-Target would disconnect the IP connection until the Session-Key#2 generated.*

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

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

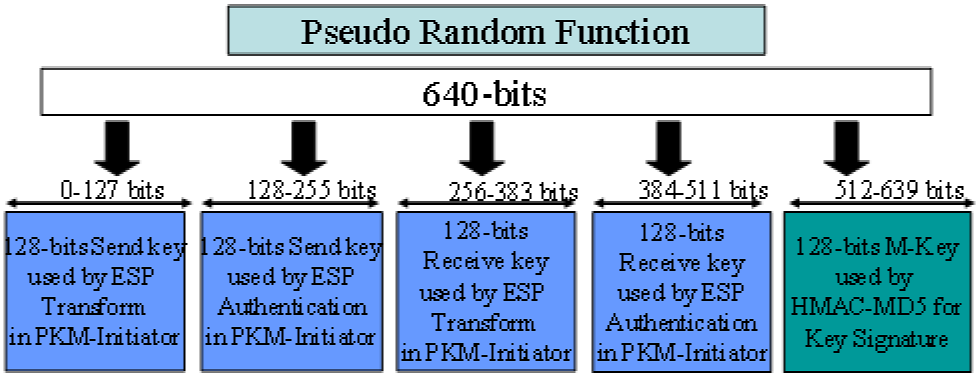

Pseudo Random Function
640-bits
0-127 bits
128-255 bits
256-383 bits
384-511 bits
512-639 bits
128-bits Send key used by ESP Transform in PKM-Initiator
128-bits Send key used by ESP Authentication in PKM-Initiator
128-bits Receive key used by ESP Transform in PKM-Initiator
128-bits Receive key used by ESP Authentication in PKM-Initiator
128-bits M-Key used by HMAC-MD5 for Key Signature

Figure h39.the 640-bits Key generated by PRF640

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

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

*Where*

```
PRF-640 (K,A,B) =
        for i=0 to 4 do
                R=R|HMAC-SHA-1(K, A|0|B|I)
        return LeastSignificant-640-bits( R )
```

*and "|" denotes bitstring concatenation*

### A 1.6 Security consideration

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

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

### A 1.7 RADIUS Protocol Messages

*The following messages are listed to support RADIUS protocol:*

*Note that TBD means To Be Defined.*

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

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

Table h22. RADIUS-BS/BSIS-Registration-Access-Request

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

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

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

Table h23. RADIUS-BS/BSIS-Registration-Access-Accept

| Attribute number | Attribute name | Value |
|---|---|---|
| 1 | User-Name | BSID. |
| 6 | Service-Type | Coexistence-Protocol -Register (value = TBD, ex. IAPP-Register, value = 15) |
| 26<br>26-TBD<br>26-TBD | Vendor-Specific-Attribute (VSA)<br>Supported-ESP-Authentication-Algorithms<br>Supported-ESP-Transforms | The list of ESP Authentication IDs corresponding to the ESP Authentication algorithms approved by Radius Server<br>The list of ESP Transform IDs corresponding to the ESP transforms approved by 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 |

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

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

~~This is an unapproved IEEE Standards Draft, subject to change~~

Table h24. RADIUS-BS/BSIS- Access-Request

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

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

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

Table h25. RADIUS-BS/BSIS- Access-Accept

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

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

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

Table h26. ESP Transform identifiers

| Transform identifier | Value | Reference |
|---|---|---|
| RESERVED | 0 | [RFC2407] |
| ESP_DES_IV64 | 1 | [RFC2407] |
| ESP_DES | 2 | [RFC2407] |
| ESP_3DES | 3 | [RFC2407] |
| ESP_RC5 | 4 | [RFC2407] |
| ESP_IDEA | 5 | [RFC2407] |
| ESP_CAST | 6 | [RFC2407] |
| ESP_BLOWFISH | 7 | [RFC2407] |
| ESP_3IDEA | 8 | [RFC2407] |
| ESP_DES_IV32 | 9 | [RFC2407] |
| ESP_RC4 | 10 | [RFC2407] |
| ESP_NULL | 11 | [RFC2407] |
| ESP_AES-CBC | 12 | [RFC3602] |
| Reserved for privacy use | 249-255 | [RFC2407] |

Table h27. 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 privacy use | 61440-65535 | |

### A 1.8 Privacy Key Management protocol messages

*The PKM protocol procedures contain 4 message actions, and each-side could check the code value of the begin of PKM message to recognize* which *action need to perform this moment. The meaning of codes for PKM message as follows*

- *0* = Session Key Start
- 1 = Session Key Request
- 2 = Session Key Response
- 3 = Session Key Acce*pt*

*The PKM message uses TLV* format *to add the following attributes*

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

Table h28. Session Key frame TLV

| Type | Length | Value Information |
|---|---|---|
| 1 | 32 | Nonce |
| 2 | 8 | Replay Counter |
| 3 | 8 | Key lifetime in seconds |
| 4 | 16 | Key Signature |
| 5 | 4 | Security Parameter Index |
| 6 | 4 * number | The list of ESP Authentication IDs corresponding to the ESP Authentication algorithms for initiator-send supported by this BS |
| 7 | 4 * number | The list of ESP Transform IDs corresponding to the ESP transforms for initiator-send supported by this BS |
| 8 | 4 * number | The list of ESP Authentication IDs corresponding to the ESP Authentication algorithms for initiator-receive supported by this BS |
| 9 | 4 * number | The list of ESP Transform IDs corresponding to the ESP transforms for initiator-receive supported by this BS |
| 10 | 33 + 4*n | Security Block |

*The Length field contains a 16-bits value to record the whole frames size starting from Code field, with the ESP-Transforms-and-Authentication-Algorithms-Codes field filled in if present.*

*The PMK-Index field contains a 8-bits value to record the current Pairwise-Master-Key-Index each PKM-side used. If the PKM-Target detects the PMK-Index different of PKM-Initiator, it must update the latest Pairwise-Master-Key.*

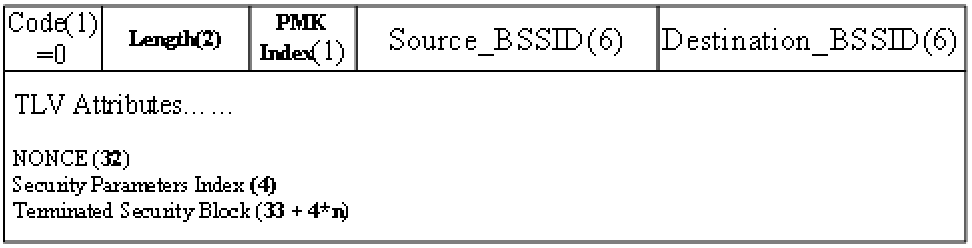
*The Replay-Counter field contains a 64-bits random number (such as 64-bit NTP timestamp) and does not repeat within the life of the Master-Key material.*

*The Key-Lifetime field contains a 64-bits value to record the Session-Key lifetime in seconds.*

*The Key-Signature field contains an HMAC-MD5 message integrity check computed over the Session-Key-Frame starting from Code field, with the ESP-Transforms-and-Authentication-Algorithms-Codes field filled in if present, but with the Key Signature field set to zero. The M-Key is used as the HMAC-MD5 key.*

*The Security-Parameters-Index field contains a 32-bits value to assign to the IPsec Security Association (including the encryption and authentication keys, the authentication algorithm for AH and ESP, the encryption algorithm for ESP, the lifetime of encryption keys…etc in this session). PKM-Initiator/Target could check the SPI value in ESP-Header to detect to use which SA for this IPsec connection.*

*The following figure shows the Session-Key-Start message format*



| Code(1) =0 | Length(2) | PMK Index(1) | Source_BSSID(6) | Destination_BSSID(6) |
|---|---|---|---|---|

TLV Attributes……

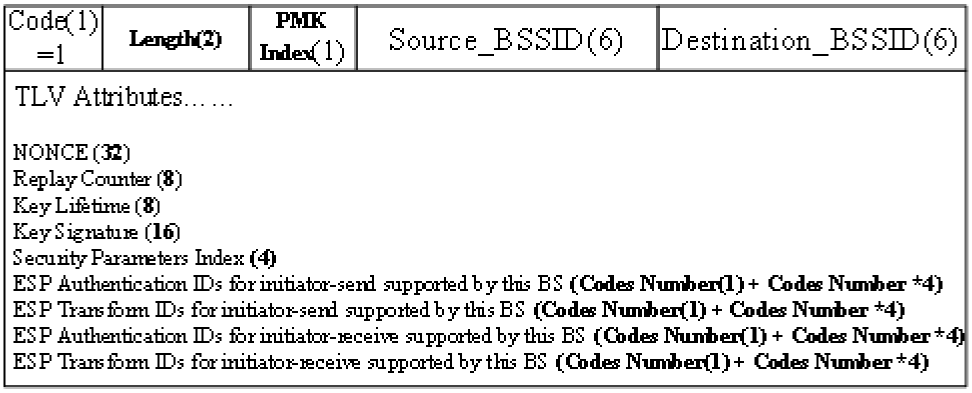
NONCE (32)
Security Parameters Index (4)
Terminated Security Block (33 + 4*n)

Figure h40.Session-Key-Start message format

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change~~

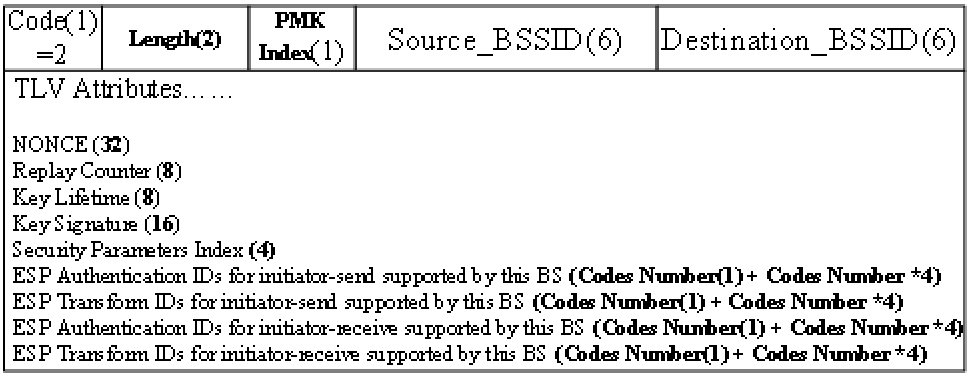
*The following figure shows the Session-Key-Request message format*



| Code(1)<br>=1 | **Length(2)** | **PMK**<br>**Index**(1) | Source_BSSID(6) | Destination_BSSID(6) |
|---|---|---|---|---|
| TLV Attributes……<br><br>NONCE (**32**)<br>Replay Counter (**8**)<br>Key Lifetime (**8**)<br>Key Signature (**16**)<br>Security Parameters Index **(4)**<br>ESP Authentication IDs for initiator-send supported by this BS **(Codes Number(1) + Codes Number *4)**<br>ESP Transform IDs for initiator-send supported by this BS **(Codes Number(1) + Codes Number *4)**<br>ESP Authentication IDs for initiator-receive supported by this BS **(Codes Number(1) + Codes Number *4)**<br>ESP Transform IDs for initiator-receive supported by this BS **(Codes Number(1) + Codes Number *4)** | | | | |

Figure h41.Session-Key-Request message format

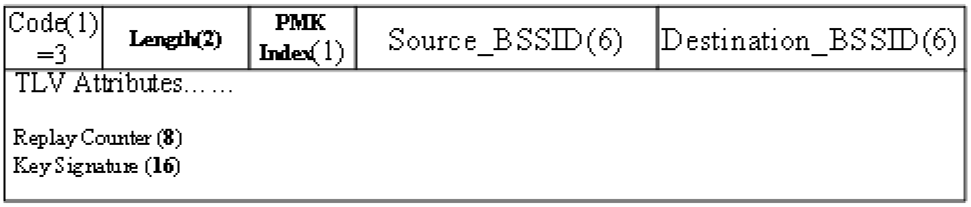
*The following figure shows the Session-Key-Response message format*



| Code(1)<br>=2 | **Length(2)** | **PMK**<br>**Index**(1) | Source_BSSID(6) | Destination_BSSID(6) |
|---|---|---|---|---|
| TLV Attributes……<br><br>NONCE (**32**)<br>Replay Counter (**8**)<br>Key Lifetime (**8**)<br>Key Signature (**16**)<br>Security Parameters Index **(4)**<br>ESP Authentication IDs for initiator-send supported by this BS **(Codes Number(1) + Codes Number *4)**<br>ESP Transform IDs for initiator-send supported by this BS **(Codes Number(1) + Codes Number *4)**<br>ESP Authentication IDs for initiator-receive supported by this BS **(Codes Number(1) + Codes Number *4)**<br>ESP Transform IDs for initiator-receive supported by this BS **(Codes Number(1) + Codes Number *4)** | | | | |

Figure h42.Session-Key-Response message format

*The following figure shows the Session-Key-Accept message format*



| Code(1)<br>=3 | **Length(2)** | **PMK**<br>**Index**(1) | Source_BSSID(6) | Destination_BSSID(6) |
|---|---|---|---|---|
| TLV Attributes……<br><br>Replay Counter (**8**)<br>Key Signature (**16**) | | | | |

Figure h43.Session-Key-Accept message format

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change.~~

## ANNEX 2. GPS Timing and Base Station Synchronization

Every IEEE 802.16h network will be synchronized to a globally distributed reference timing system that is capable of allowing the network Base Stations to synthesize a 1 pps NTI and a UTC time stamp. The Global Positioning System (GPS) is capable of providing such a temporal references to the Base Stations providing they are equipped with GPS receivers.

Every base station equipped with a GPS receiver would be capable of receiving a UTC synchronized 1 pps timing signal. The accuracy of the clock pulses derived from using GPS are accurate to +/- 100 usec and the pulses that are derived typically have rise times within +/- 2.5 nsec. Fig 1 shows a typical GPS 1 sec pulse and its duration (Trimble Inc. Palisade output).

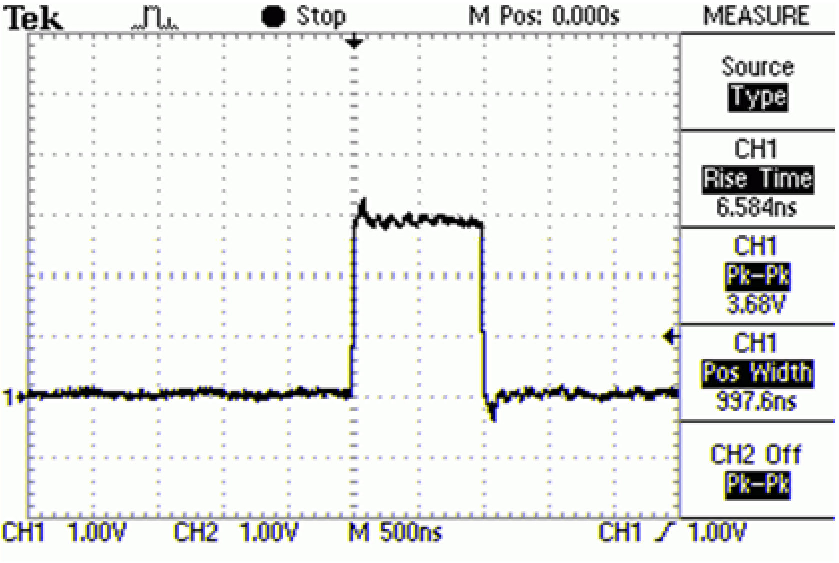


Figure h44.GPS 1pps Pulse

The availability of a globally distributed clock will result in a common temporal unit that can be used in negotiating access times to spectrum shared by a community of ad-hoc users. Non-IEEE 802.16h networks having different architectures and messaging signals could also use a common 1 sec interval for synchronization of their networks. This would conceivably allow communication between them and IEEE 802.16h networks in a synchronized manner, to facilitating the exchange of information related to coexistence and spectrum sharing.

The one second unit is considered ideal because it is distributed by the GPS as such and the length of the unit is seemingly appropriate. IEEE 802.16h networks typically have frames in the order of several to tens of milliseconds, which is of a granularity that could allow several to several tens of networks to negotiate coexistence subintervals within the 1 second span. Additionally, for IP networks, the 1 second interval is of a length sufficient to accommodate inter-router TCP/IP latency, especially over networks that are likely to be close to each other, such as ad-hoc LE networks.

~~Copyright © 2005 IEEE. All rights reserved.~~

~~This is an unapproved IEEE Standards Draft, subject to change.~~