Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**MBS refinements**
Date Submitted	**2005-03-15**
Source(s)	Rubin Amir, Yigal Eliaspur **Intel Corp**. amir.rubin@intel.com yigal.eliapsur@intel.com
Re:	IEEE P802.16e/D6
Abstract	.Refinements and clarifications for MBS
Purpose	Adoption of proposed changes into P802.16e /D6
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.
Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures (Version 1.0) <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, if there is technical justification in the opinion of the standards-developing committee and provided the IEEE receives assurance from the patent holder that it will license applicants under reasonable terms and conditions for the purpose of implementing the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:r.b.marks@ieee.org> as early as possible, in written or electronic form, of any patents (granted or under application) that may cover technology that is under consideration by or has been approved by IEEE 802.16. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

MBS Refinements

Amir Rubin, Yigal Eliaspur

1 Motivation

As for the major changes and enhancement for the MBS in the last sessions, a capability negotiation and text refinements are needed:

1. MBS security
2. MBS Time diversity
3. MBS MAP

.

2 Overview of the proposed solution

[change the following in section 11.13.20]

11.13.20 MBS service

This TLV indicates the type of ~~whether or not the~~ MBS ~~service~~ that is being requested for the connection that is being setup.
A value of 1 in bit 1 indicates Multi-BS-MBS and a value of 0 in bit 1 indicates Single-BS-MBS is requested. In bit 2, a value of 1 indicates that the ~~and a value of 1 indicates Multi-BS-MBS~~ Time_Diversity option is requested for the MBS whereas A value of 0 indicates that the MBS should not be Time_Diversity. If MS or BS ~~want~~wants to initiate MBS service, DSA-REQ with MBS service type and subtype shall be used. The DSA-RSP message shall contain the acceptance or rejection of the request in bit 0. If there is no available MBS service with the requested features, ~~MBS service value~~ bit 0 will be 0, otherwise it would be 1. ARQ shall not be enabled for this connection.

Type	Length	Value	Scope
[145/146].4	1	~~0: No available MBS~~ ~~1: Single-BS-MBS~~ ~~2: Multi-BS-MBS~~ Bit #0: MBS Available on this connection Bit #1: Multi_BS_MBS Bit #2: MBS Time_Diversity_Data	~~DSx-REQ~~ ~~DSx-RSP~~ ~~DSx-ACK~~ DSA-REQ DSA-RSP

[change the following in table 14]

Table 14—MAC Management messages (continued)

60	MOB_SCANREPORT	Scanning result report message	primary management
61	MOB_PAG-ADV	BS broadcast paging message	broadcast
62	MBS_MAP	MBS MAP message	broadcast
63	PMC_REQ	Power control mode change request message	Basic
64	PMC_RSP	Power control mode change response message	Basic
65	PRC-LT-CTRL	Setup/Tear-down of long term MIMO precoding	Basic
66~~-255~~223		*reserved*	

[change the following in section 6.3.2.3.56]

6.3.2.3.56 Multicast Broadcast Service Map (MBS-MAP) message

The BS may send an MBS-MAP message on an MBS portion to describe the MBS connections serviced by the MBS portion. When a MBS-MAP is sent, the connections~~-need~~should not be described in the DL-MAP, ~~but a~~and the MBS_MAP_IE() shall be substituted instead.

Table 108r—MBS-MAP

Syntax	Size	Notes
MBS-MAP Message Format (){		
Management Message Type =	8 bits	0x62
Frame number	8 ~~4~~ bits	The frame number is identical to the 8 LSB of the frame number in the DL-MAP
MBS_DIUC_Change_Count	8 bits	
#MBS_DATA_IE	4 bits	Number of included MBS_DATA_IE
#MBS_DATA_Time_Diversity_IE	4 bits	Number of included MBS_DATA_Time_Diversity_IE
For (i = 0; i<~~n~~N; i++){	12 bits	N=#MBS_DATA_IE
MBS_DATA_IE	Variable	
}	8 bits	
~~#MBS_DATA_Time_Diversity_IE~~	~~4 bits~~	~~Number of included MBS_DATA_Time_Diversity_IE~~
For(i=0; i<~~n~~M; i++){		M = #MBS_DATA_Time diversity_IE
MBS_DATA_Time_Diversity_IE	Variable	
}		
TLV encoding element		
If(!byte boundary){		
Padding Nibble		
}	8 bits	
}-		

[change the following in table 108s]

Table 108s—MBS_MAP_Type

MBS_MAP_Type	Description
0	MBS_DATA_IE
1	MBS_DATA_Time_Diversity_IE
2~~-255~~15	Reserved

[change the following in section **11.13.26** *]*

11.13.26 MBS zone identifier assignment

The DSA-RSP message may contain the value of this parameter to specify a MBS Zone identifier. This parameter indicates a MBS zone through which the connection or virtual connection for the associated service is valid.

Type	Length	Value	Scope
[145/146]33	~~8~~1	MBS zone identifier	DSA-REQ/RSP

[add the following section]

11.8.X MBS Support

This field indicates the MBS supporting features of the SS. bit value of 0 indicates "not supported" while 1 indicates "supported".

Type	Length	Value	Scope
XXX	1	Bit #0: MBS feature Bit #1: MBS security Bit #2: MBS Time_Diversity_Data Bit #3 _Multi_BS_MBS~~MBS_MAP~~	~~MBS~~SBC-REQ MBS-RSP

[change the following in section **6.3.2.3.9.20***]*

6.3.2.3.9.20 SA-TEK-Request message

The MSS transmits the SA-TEK-Request message after receipt and successful HMAC/OMAC verification of an SA-Challenge from the BS. The SA-TEK_Request proves liveliness of the SS and its possession of the AK . If this message is being generated during initial network entry, then it constitutes a request for SADescriptors identifying the primary and static SAs and optionally GSAs the requesting SS is authorized to access and their particular properties (e.g., type, cryptographic suite). If this message is being generated upon HO, then it constitutes a request for establishment (in the target BS) of TEKs, GTEKs and GKEKs at the MSS and renewal of active primary, static and dynamic SAs and associated SAIDs used by the MSS in its previous serving BS.

[change the following in section **7.8.3***]*

7.8.3 Multicast Broadcast Service (MBS) support

MBS is an efficient and power saving mechanism that when ~~requires~~ using PKMv2 to send multimedia broadcast information, it provides subscribers with strong protection from theft of service across broadband wireless mobile network by encrypting broadcast connections between SSs and BSs.

[change the following in section **7.8.4.1.1***]*

7.8.4.1.1 PDU payload format

Counter mode requires unique initial counter and key pair across all messages. This section describes the initialization of the 128-bit initial counter, constructed from the 24-bit PHY synchronization field or frame number and a new 8-bit Rollover counter (ROC). The PDU payload for AES-CTR encryption shall be prepended with the 8-bit ROC , i.e., the ROC is the 8 MSBs of the 32 bit nonce.. The ROC shall be transmitted in little endian order. The ROC shall not be encrypted. Any tuple value of {AES Counter, KEY} shall not be used more than once for the purposes of encrypting a block. MS and BS shall ensure that a new MTEK is requested and transferred before the ROC reaches 0xFF. The 32bit nonce made out of ROC and 24bits frame number shall be repeated four times to construct 128- bit counter block required by the AES-128 cipher. (e.g.,. NONCE|NONCE|NONCE|NONCE). This mechanism can reduce per-PDU overhead of transmitting the full counter. In other words, at the most 232 PDUs can be encrypted with a single MTK. The plaintext PDU shall be encrypted using the active MBS_Traffic_key (MTK) derived from MAK and- MGTEK, according to CTR mode specification. A different 128-bit counter value is used to encrypt each 128-bit block within a PDU. This can be achieved by only incrementing the lowest 32-bits by 1; the lowest 32-bit value may rotate to 0 and counted up. The processing yields a payload that is 8 bits longer than the plaintext payload. When MBS PDU is part of no security MBS connection, the nonce should not be part of the PDU and the MBS stream should not be encrypted.

Figure 137a—MBS MAC PDU ~~Ciphertext~~ payload format