

Project	<b>IEEE 802.16 Broadband Wireless Access Working Group</b> < <a href="http://ieee802.org/16">http://ieee802.org/16</a> >	
Title	<b>MBS AES-CTR text change</b>	
Date Submitted	<b>2004-08-17</b>	
Source(s)	JUNHYUK SONG, YONG CHANG, JICHEOL LEE  Samsung Electronics	Voice: +82-31-279-3639 <a href="mailto:junhyuk.song@samsung.com">junhyuk.song@samsung.com</a>  Voice: +82-31-279-3639 <a href="mailto:jicheol.lee@samsung.com">jicheol.lee@samsung.com</a>
Re:	IEEE P802.16e/D4-2004	
Abstract	Proposal for MBS AES-CTR text change	
Purpose	Review and Adopt the suggested changes into P802.16e/D4	
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 < <a href="http://ieee802.org/16/ipr/patents/policy.html">http://ieee802.org/16/ipr/patents/policy.html</a> >, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair < <a href="mailto:chair@wirelessman.org">mailto:chair@wirelessman.org</a> > as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site < <a href="http://ieee802.org/16/ipr/patents/notices">http://ieee802.org/16/ipr/patents/notices</a> >.	

## AES-CTR clarification

JUNHYUK SONG, YONG CHANG, JICHEOL LEE  
Samsung Electronics

### Introduction

AES-CTR has defined in addition to DES-CBC and AES-CTR, however in current text there is inconsistency with overall assumption that needed to be cleared up. In this contribution we propose to change following

- “Little-endian” byte ordering specified for nonce to big-endian order

### Byte Ordering

802.16 specified big-endian byte ordering in Generic MAC header (see figure 1), and it is a basic assumption for packet format and other attribute has more than one octet. However AES-CTR specified little-endian ordering for nonce. It is desirable to have big-endian byte ordering for nonce transmission for sake of consistency with GMH and other packet formats

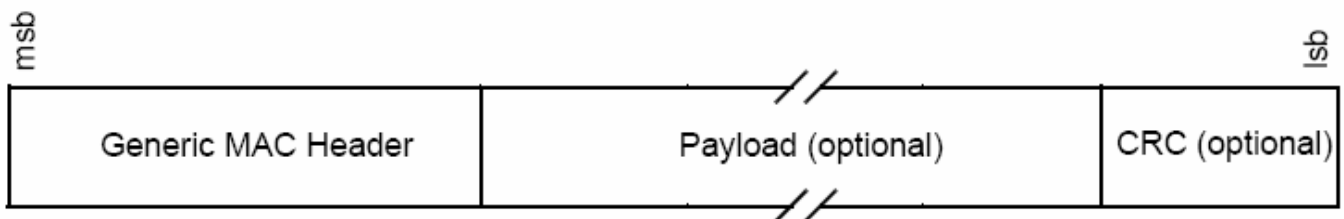


Figure 21—MAC PDU formats

Figure-1 MAC PDU formats

### Proposed Text

#### 7.8.2.1 Data encryption with AES in CTR mode

The PDU payload shall be appended with 32bits nonce randomly generated by base station. The nonce shall be transmitted in ~~big~~little endian byte order. The nonce shall not be encrypted.