

Project	IEEE 802.16 Broadband Wireless Access Working Group < http://ieee802.org/16 >	
Title	Corrections to DES XOR.	
Date Submitted	June 25, 2004	
Source(s)	Baraa Al-Dabagh	mailto:baraa.al.dabagh@intel.com
	Intel Corporation CHP3-105 350 East Plumeria Dr. San Jose, CA 95134	
Re:	Supporting document for recirculation ballot #14b.	
Abstract	In P802.16 REVd/D5 [1], the text indicates that you have to XOR the IV of the DES encryption key with the PHY sync field from the map. But that SYNC field is missing. This contribution proposes an alternative to fix that	
Purpose	Adoption	
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.	
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.	
Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures < http://ieee802.org/16/ipr/patents/policy.html >, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair < mailto:chair@wirelessman.org > as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site < http://ieee802.org/16/ipr/patents/notices >.	

Corrections to DEX XOR

Baraa Al-Dabagh

Intel Corporation

1. Introduction

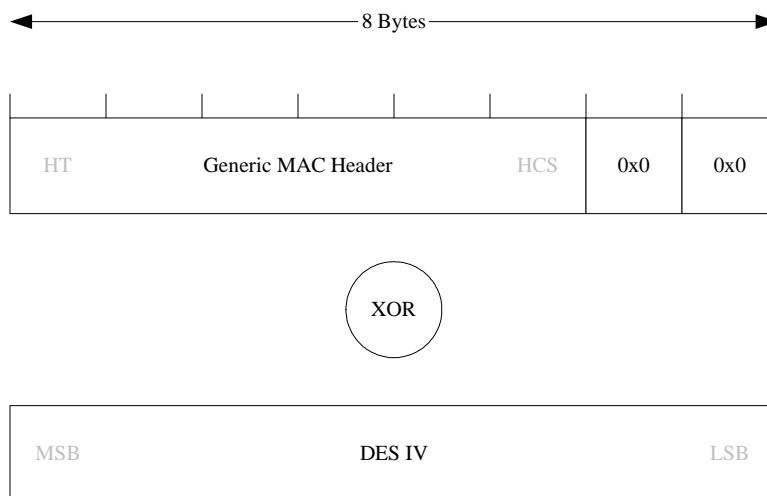
In P802.16 REVd/D5 [1], the text indicates that you have to XOR the IV of the DES encryption key with the PHY sync field from the map. But that SYNC field is missing. This contribution proposes an alternative to fix that.

2. Proposed fix

Rather than doing the XOR with the PHY sync field we can do the XOR with the Generic MAC Header of the received / transmitted packet. In this case the operation will be done as follows:

CBC IV computation on the transmitter :

1. Compute the HCS
2. XOR the generic MAC header padded by zeros as shown in the figure below with the appropriate IV, to produce the final IV to be used by the encryption engine.



3. proceed to encryption

CBC IV computation on the receiver:

1. Compute the HCS on the received generic MAC header
2. XOR the Generic MAC Header padded by zeros as shown in the figure above with the appropriate IV., to produce the final IV to be used by the decryption engine
3. proceed to decryptions

4. Proposed text changes

[Section 7.5.1.1 change the second paragraph accordingly]

The CBC IV shall be calculated as follows: in the downlink **and uplink**, the CBC shall be initialized with the exclusive-or (XOR) of (1) the IV parameter included in the TEK keying information, and (2) ~~the content of the PHY Synchronization field (right justified) of the latest DL-MAP~~ **the Generic MAC Header of the MAC PDU being transmitted or received as shown in the following diagram.**

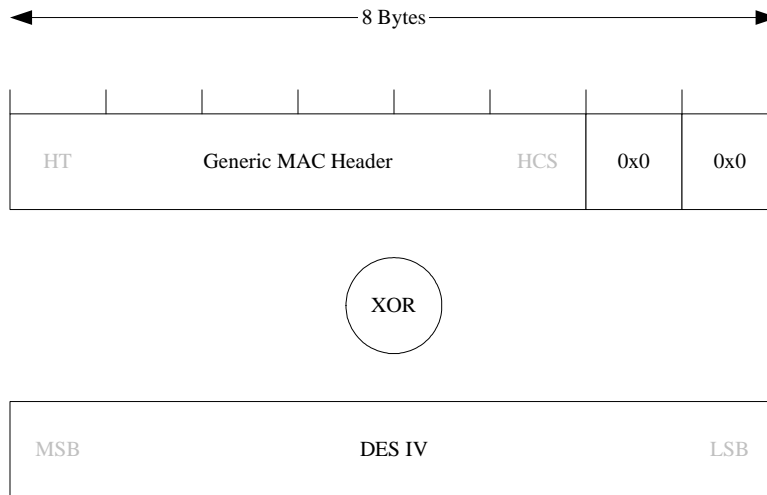


Figure NNN. CBC IV computation