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	
Release	
Patent Policy and Procedures	

Corrections to DEX XOR

Baraa Al-Dabagh
Intel Corporation

1. Introduction

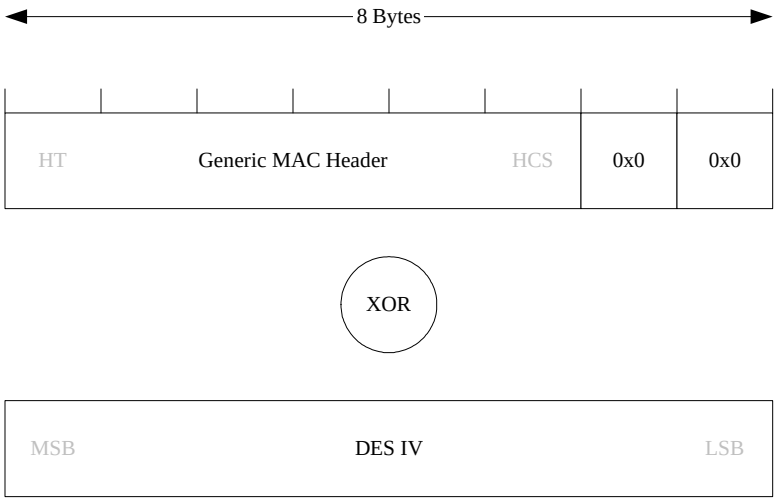
In P802.16 REVd/D5 [1], the text indicates that you have to XOR the IV of the DES encryption key with the PHY sync field from the map. But that SYNC field is missing. This contribution proposes an alternative to fix that.

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.**

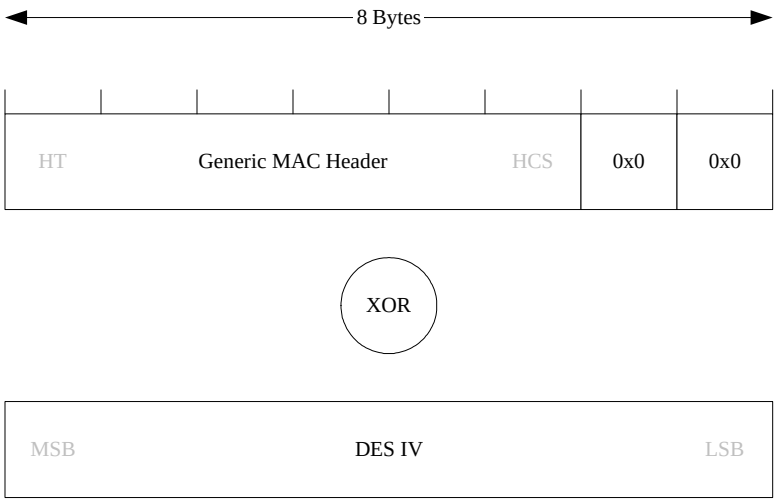


Figure NNN. CBC IV computation