Project	**IEEE 802.20 Working Group on Mobile Broadband Wireless Access** <**http://grouper.ieee.org/groups/802/20/**>	
Title	**802.20 Message Format**	
Date Submitted	**2003-03-07**	
Source(s)	Alan Chickinsky Northrop Grumman/TASC 4801 StoneCroft Blvd Chantilly, VA 20151	Voice: 703-633-8300 x 8554 Fax: 703-449-3400 Email: achickinsky@northropgrumman.com
Re:	MBWA Call for Contributions	
Abstract	Proposal for message format	
Purpose	Propose a message format	
Notice	This document has been prepared to assist the IEEE 802.20 Working Group. 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 802.20.	
Patent Policy	The contributor is familiar with IEEE patent policy, as outlined in Section 6.3 of the IEEE-SA Standards Board Operations Manual <http://standards.ieee.org/guides/opman/sect6.html#6.3> and in *Understanding Patent Issues During IEEE Standards Development* <http://standards.ieee.org/board/pat/guide.html >.	

802.20 Message Format

Alan Chickinsky

Northrop Grumman/TASC

March 10, 2003

Message Parts

- Header
  - Source and Destination Address
  - Options
  - Security Option Field
- Body
  - Message Text
- Trailer
  - Padding

Source and Destination Address

- Order is destination MAC address immediately followed by the source MAC address

Options

- The options section is composed of one or more optional fields
- The first byte is the option number
  - Option 0 is reserved to indicate end of list
  - Options 1 to 254 are reserved for this standard
  - Option 255 is used to indicate that the next byte contains a vendor specific option.
  - Vendor assignment is TBD

Options (continued)

- The most bit on in the option number indicates the next byte contains the field length of the option number
- The most bit off in the option number indicates the next byte contains the option value
- For option value 255, the next byte contains the length of the vendor specific data

Field Values

- Field values are composed of one or more consecutive bytes.
- If the remaining value is less than 254, then one byte is used
- If the value is greater than 254, then 255 is used and the next byte is added to the current byte to obtain the correct value

Security Option Field

- Option number 1
- The contents of this field and use are defined in the security section of the specification
- By making this an option, an implementer can use the same protocol for secure and non-secure networks
- Size changes to block codes or initialization vectors do not require a specification change
- Indicates where the security block starts

Security Section

- In presentation IEEE C802.20-03/06 it was shown that block security can be enhanced if the first block is random
- This first block is defined as an Initialization Vector
- Setting the security option value as the Initialization Vector for the enhanced security need
  - Initialization Vector is a fixed number of random bits
- The randomness of the Initialization Vector is determined by the vendor

Suggested Security Values

1	127 bit Initialization Vector for AES
2	512 bit Initialization Vector for AES

Advantages

- If you do not want encryption, do not use option 1
- If you want security to start after 10 other options, make option 1 the eleventh entry
- To add an different encryption algorithm, we either add a new value to option 1or create a new option number

Proposal #1

Motion-

The MAC layer message header contain in this order

- 48 bit destination field,
- 48 bit source field
- Option field(s)

Proposal #2

Motion-

Option fields contain in this order

- Option number
- Option value length
- Option value

Proposal #3

Motion-

Option values 0-127 are reserved for the standard

Options over 128 are assigned to vendors in groups of 10 upon request

Proposal #4

Motion-

Value for options are between 0 and 254 are one byte long

If any option byte is 255, then the following byte is added to current value to get actual value.

Proposal #5

Motion-

Option length between 0 and 254 are one byte long

If any length byte is 255, then the following byte is added to current value to get actual length.