Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Letter Ballot 14 Comment Addendum**	
Date Submitted	**2004-03-01**	
Source(s)	Robert Nelson MacPhy Technologies 1104 Pittsburgh Landing Richardson, TX 75080	Voice: 972-239-9224 Fax: 972-671-1455 bob_nelson@ieee.org
Re:	Letter Ballot 14 on document ***IEEE P802.16e/D1-2004***	
Abstract	Editorial reorganization to align clause 11 references in the TGe ammendment to match the section definitions and content of the current base document REVd/D3	
Purpose	Proposed remedy to LB 14 comment on Clause 11 changes	
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>.	

Letter Ballot 14 Comment Addendum

Bob Nelson
MacPhy Technologies

The following text is proposed as replacement for the current contents of P802.16e/D1 covering Clause 11 (Page 60, Line 1 through Page 68, Line 51). The text is an editorial reorganization and cleanup of the portion of the document to be replaced. The proposal aligns the draft amendment contents with Clause 11 of the base document, REVd/D3. TLV type values are assigned (if listed as TBD) or reassigned (if the current values are inconsistent with the numbering scheme in D3).

Portions of text that appears to duplicate other text in the draft or the base document, that describes entities that are no longer relevant due to the current contents of D3, or that is not referenced by other parts of the draft document have been removed from the proposed updates but are logged at the end of this document for reference.

11. TLV Encodings

11.1.2 HMAC Tuple

[Change the contents of table 274 as indicated:]

Table 274—HMAC Tuple definition

Type	Length	Value	Scope
149	21	See Table 275	DSx-REQ, DSx-RSP, DSx-ACK, REG-REQ, REG-RSP, RES-CMD, DREG-CMD, TFTP-CPLT, MOB_HO-IND

11.3.3 UCD channel encodings

[Insert the following rows at the end of Table 276:]

Table 276a—UCD channel encodings

Name	Type (1 byte)	Length (1 byte)	Value (Variable-length)
HO_ranging_start	7	1	Initial backoff window size for MSS performing initial ranging during hand-over processs, expressed as a power of 2. Range: 0-15 (the highest order bits shall be unused and set to 0).
HO_ranging_end	8	1	Final backoff window size for MSS performing initial ranging during hand-over process, expressed as a power of 2. Range: 0-15 (the highest order bits shall be unused and set to 0).

11.5 RNG-REQ management message encodings

[Insert the following row to the end of Table 292:]

Table 292a—RNG-REQ message Encodings

Name	Type (1 byte)	Length	Value (Variable-length)
Serving BS ID	5	6	The unique identifier of the former Serving BS

11.6 RNG-RSP management message encodings

[Insert the following row to to the end of Table 293:]

Table 293a—RNG-RSP message encodings

Name	Type (1 byte)	Length	Value (Variable-length)
Service Level Prediction	14	1	This value indicates the level of service the MSS can expect from this BS. The following encodings apply: 0 = No service possible for this MSS 1 = Some service is available for one or several Service Flows authorized for the MSS. 2 = For each authorized Service Flow, a MAC connection can be established with QoS specified by the AuthorizedQoSParamSet. 3 = No service level prediction available.

[Insert the following immediately before section 11.8:]

11.7.8 CID update encodings

This field provides a translation table that allows an MSS to update its service flow and connection information so that it may continue service after a hand-over to a new serving BS.

Name	Type (1 byte)	Length| (1 byte)	Value (Variable-length)
CID_update	16	variable	Compound

The following TLV values shall appear in each CID_update TLV.

Name	Type (1 byte)	Length (1 byte)	Value (Variable-length)
New_CID	16.1	2	New CID after hand-over to new BS.
Old_CID	16.2	2	Old CID before hand-over from old BS.

The following TLV element may appear in a CID_update TLV.

Name	Type (1 byte)	Length (1 byte)	Value (Variable-length)
Connection Info	16.3	Variable	If any of the service flow parameters change, then those service flow parameters and CS parameter encoding TLVs that have changed will be added. Connection_Info is a compound TLV value that encapsulates the Service Flow parameters and the CS parameters that have changed for the service. All the rules and settings that apply to the parameters when used in the DSC-RSP message apply to the contents encapsulated in this TLV.

11.7.9 Method for allocating IP address

Type	Length	Value
17	1	bit #0: DHCP bit #1: Mobile IPv4 bit #2-7: reserved; shall be set to zero

11.7.10 Mobility parameters support

The following parameters are associated with mobile operations.

11.7.10.0.1 Sleep-mode supported

This field indicates whether or not the MSS supports sleep-mode. A bit value of 0 indicates “not supported” while 1 indicates it is supported.

Type	Length	Value
18	1	Bit #0: Mobility (handover) support Bit #1: Sleep-mode support

11.7.10.0.2 Sleep-mode recovery time

This field indicates the time required for an MSS which is in a sleep-mode to return to awake-mode. This parameter is optional and may be used by the BS to determine sleep interval window sizes when initiating sleep-mode with an MSS.

Type	Length	Value
19	1	Number of freames required for the MSS to switch from sleep-mode to awake-mide

[Insert immediately before the start of section 11.9:]

11.8.3 Authorization policy support

This field indicates authorization policy sued by the SS and BS to negotiate and synchronize. A bit value of 0 indicates “not supported” while 1 indicates “supported.” If this field is omitted, then both SS and BS shall

use the IEEE 802.16 essential privacy method, constituting X.509 digital certificates and the RSA public key encryption algorithm, as authorization policy.

Type	Length	Value	Scope
4	1	Bit# 0: IEEE 802.16 essential privacy (Legacy PKM) Bit# 1-7: Reserved for open privacy. Set to 0.	SBC-REQ (see 6.4.2.3.23) SBC_RSP(see 6.4.2.3.24)

11.9 PKM-REQ/RSP management message encodings

[Change as indicated]

11.9.3 TEK

Description: This attribute contains a quantity that is a TEK key, encrypted with a KEK derived from the AK.

Type	Length	Value (string)
8	8 or 16	Encrypted TEK

When the TEK encryption algorithm identifier in the SA is 0x01, the length shall be 8 and the TEK shall be encrypted with 3DES in EDE mode according to the procedure defined in 7.5.2.1.

When the TEK encryption algorithm identifier in the SA is 0x03, the length shall be 16 and the TEK shall be encrypted with AES in ECB mode according to the procedure in 7.5.2.3

[Change as indicated]

11.9.8 TEK parameters

Description: This attribute is a compound attribute, consisting of a collection of subattributes. These subattributes represent all security parameters relevant to a particular generation of an SAID's TEK. A summary of the TEK-Parameters attribute format is shown below.

Type	Length	Value (compound)
13	*variable*	The compound field contains the subattributes as defined in table 298

Table 298—TEK-parameters subattributes

Attribute	Contents
TEK	TEK, encrypted with the KEK
Key-Lifetime	TEK Remaining Lifetime
Key-Sequence-Number	TEK Sequence Number
CBC-IV	CBC Initialization Vector

The CBC-IV attribute is required when the data encryption algorithm identifier in the SA ciphersuite is 0x01 (DES in CBC mode).

The CBC-IV attribute is not required when the data encryption algorithm identifier in the SA ciphersuite is 0x02 (AES).

11.9.14 Cryptographic suite

Type	Length	Value (uint8, uint8, uint8)
20	3	A 24-bit integer identifying the cryptographic suite properties. The most significant byte, as defined in Table 301, indicates the encryption algorithm and key length. The middle byte, as defined in Table 302 indicates the data authentication algorithm. The least significant byte, as defined in Table 303, indicates the TEK Encryption Algorithm.

Table 301—Data encryption algorithm identifiers

Value	Description
0	No data encryption
1	CBC-Mode, 56-bit DES
2	CCM-Mode, 128-bit AES
~~2~~ 3-255	*Reserved*

Table 302—Data authentification algorithm identifiers

Value	Description
0	No data authentication
1	CCM-Mode, 128-bit AES
~~1~~ 2-255	*Reserved*

Table 303—TEK encryption algorithm identifiers

Value	Description
0	Reserved
1	3-DES EDE with 128-bit key
2	RSA with 1024-bit key
3	ECB mode AES with 128-bit key
~~3~~ 4-255	*Reserved*

The allowed cryptographic suites are itemized in Table 290

Table 304—Allowed cryptographic suites

Value	Description
0x000001	No data encryption, no data authentication & 3-DES, 128
0x010001	CBC-Mode 56-bit DES, no data authentication & 3-DES, 128
0x000002	No data encryption, no data authentication & RSA, 1024
0x010002	CBC-Mode 56-bit DES, no data authentication & RSA, 1024
0x020103	CCM-Mode 128-bit AES, CCM-Mode, 128-bit AES, ECB mode AES with 128-bit key
All remaining values	*Reserved*

[Insert immediately before the start of 11.13 and renumber succeeding sections accordingly:]

11.13 MOB_NBR-ADV message encodings

The following TLV holds UCD and DCD information for an individual BS.l

Name	Type (1 byte)	Length (1 byte)	Value (Variable-length)
Encoded Neighbor Information	1	*Variable*	Compound

The following table defines the TLV elements that may appear in a Encoded Neighbor Information TLV.

Name	Type (1 byte)	Length (1 byte)	Value (Variable-length)
DCD_settings	1.1	*Variable*	The DCD_settings is a compound TLV that encapsulates an entire DCD message (excluding the generic MAC header). All the rules and settings that apply to the DCD message apply to the contents encapsulated in this TLV.
UCD_settings	1.2	*Variable*	The UCD_settings is a compound TLV value that encapsulates an entire UCD message (excluding the generic MAC header). All the rules and settings that apply to the UCD message apply to the contents encapsulated in this TLV.

[Insert the following entries to the end of Table 310:]

Table 310a—Service flow encodings

Type	Parameter
29	Type of Data Delivery Services
30	SDU Inter-arrival Interval
31	Time Base

[Insert the following immediately before the start of Clause 12:]

11.13.23 Type of Data Delivery Services

The value of this parameter specifies type of Data Delivery Service as defined in 6.4.16.

Type	Length	Value	Scope
[145/146].29	1	0: Continuing Grant Service 1: Real Time - Variable Rate Service 2; Non-Reql Time - Variable Rate Service 3: Best Efforts Service	DSA-REQ, DSA-RSP DSC-REQ, DSC-RSP REG-REQ, REG-RSP

11.13.24 SDU Inter-arrival Interval

This parameter specifies nominal interval between consequent SDU arrivals as measured at MAC SAP.

Type	Length	Value	Scope
[145/146].30	2	SDU Inter-arrival Interval in units of 0.5 ms	DSA-REQ, DSA-RSP DSC-REQ, DSC-RSP REG-REQ, REG-RSP

11.13.25 Time Base

This parameter specifies time base for rate measurement as defined in 6.4.16.

Type	Length	Value	Scope
[145/146].31	2	Time base in ms	DSA-REQ, DSA-RSP DSC-REQ, DSC-RSP REG-REQ, REG-RSP

==========

The following D1 text was excised from this proposal.

==========

11.1.4 RNG-RSP TLVs for re-establishment of Service Flows

[Insert the following rows at tne end of table 280:]

Table 280a—REG-RSP Encodings

Name	Type (1 byte)	Length (1 byte)	Value (Variable-length)
New CID	TBD	2	New CID after hand-over to new BS.
Old CID	TBD	2	Old CID before hand-over from old BS.
Connection_Info	TBD	Variable	The Connection_Info is a compound TLV value that encapsulates the **Service Flow Parameters** and the **CS Parameter** that have changed for the service. All the rules and settings that apply to the parameters when used in the DSC-RSP message apply to the contents encapsulated in this TLV.

==========

11.4 Common encodings

[Insert the following rows at the end of Table 295:]

Table 295a—MSS Capability encodings

Type	Parameters
23	Method for allocating IP address
24	Mobility parameters support

==========

[Apply the following changes to section 11.4.2:]

11.4.2 SS Capabilities encoding

[Add to table 306]

Table 296—SS Capability encodings

Type	Parameters
5.25	Authorization Policy Support

==========

[Insert new section 11.4.2.13:]

11.4.2.13 MSS Mobility parameters support

This field defines the parameters associated with the mobility support capabilities of the MSS.

Type	Length	Value
5.24	n	-

==========

11.4.9.9 Minimum reserved traffic rate

This parameter specifies the minimum rate reserved for this service flow.

Minimum Reserved Traffic Rate = R (bits/sec) with time base T(sec) means the following: Let S denote additional demand accumulated at the MAC SAP of the transmitter during an arbitrary time interval of the length T. Then the amount of data forwarded to PHY (in bits) during this interval should be not less than min {S, R * T}.

The BS should be able to satisfy bandwidth requests for a service flow up to its Minimum Reserved Traffic Rate. If less bandwidth than its Minimum Reserved Traffic Rate is requested for a service flow, the BS may reallocate the excess reserved bandwidth for other purposes. The aggregate Minimum Reserved Traffic Rate of all service flows may exceed the amount of available bandwidth. The value of this parameter is calculated from the byte following the MAC header HCS to the end of the MAC PDU payload. If this parameter is omitted, then it defaults to a value of 0 bits per second (i.e., no bandwidth is reserved for the flow by default).

==========

11.4.9.10 Minimum Tolerable Traffic Rate

"Minimum Tolerable Traffic Rate = R (bits/sec) with time base T(sec)" means the following. Let S denote additional demand accumulated at the MAC SAP of the transmitter during an arbitrary time interval of the length T. Then the amount of data forwarded at the receiver to CS (in bits) during this interval should be not less than min {S, R * T}.

In the case of DL connection, Minimum Tolerable Traffic Rate should be monitored by the BS to make decisions on rate change or deletion of the connection in the case SDUs' loss ratio is too high. So the MSS has to measure and report certain parameters to BS as specified in NNN .

==========

11.4.10 Minimum Tolerable Traffic Rate

This parameter specifies time base for rate measurement as defined in 6.4.16.

Type	Length	Value	Scope
[24/25].33	4	Minimum Tolerable Traffic Rate in bits per second.	DSA-REQ, DSA-RSP DSC-REQ, DSC-RSP REG-REQ, REG-RSP

==========

[Insert new sections 11.4.14:]

11.4.14 Mobility support capabilities

This field defines common parameters for mobility support..

Type	Length	Value
44	n	-