IEEE P802.15
Wireless Personal Area Networks

Project	IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)	
Title	**TG3 SB2 comment resolution**	
Date Submitted	[11 March, 2003]	
Source	[James P. K. Gilb] [Appairent Technologies] [15373 Innovation Drive, #210, San Diego, CA 92129]	Voice: [858-485-6401] Fax: [858-485-6406] E-mail: [gilb@ieee.org]
Re:	[]	
Abstract	[This document is a record of comment resolutions for SB2.]	
Purpose	[To provide a record of the comment resolution for SB2.]	
Notice	This document has been prepared to assist the IEEE P802.15. 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 acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15.	

1. Comment resolution in Dallas

1.1 Wednesday, 12 March 2003

Meeting called to order at 8:52 am CST.

CID 60 - REJECT. The FCSL will communicate the presence of a new stream to the DME when it first receives data with that stream index. This synchronizes the DME to the stream status in the piconet.

CID 142

Comment: Transmission time may vary from frame to frame due to data rate (and potentially preamble) changes, the variable bit rate nature of the stream, and throughput considerations. For instance, an 1394 ISO packet may contain 0, 1, or 2 small MPEG cells (188 bytes). Such variable length packets themselves may be further aggregated either at the so-called FCSL or right at the MAC (even though the current spec has no such aggregation mechanism) to make efficient use of the 100 Mb/s plus data rates being specified in 802.15.3a which is to be using this MAC. On the other hand, a retry does not occur right after a prefixed CTR time unit. Note that if CTA is not specified correctly, this MAC will just fall apart.

Suggested Remedy: Delete the newly introduced MIFS CTRq TU field and use natural time units, instead of "CTR time unit" to define the duration of each CTA (but not per "CTA Rate Factor") being requested. Suggest to rename "CTA Rate factor" as "CTA Repetition".

Response: ACCEPT IN PRINCIPLE. Delete MIFS CTRq TU and all references. However, the CTR time unit was unchanged from D16 and D17. They are free to use natural time (microsecond) units for the CTR TU. However, CTR time units allow a DEV to specify a unit of time allocation so that the PNC can efficiently allocate time beyond the minimum required for the DEV, or to breack a channel time allocation into multiple CTAs in the superframe if needed.

CCID 152:

Comment: The standard clearly states that the DEV is responsible for calculating it's needed channel time and also to make sure it stays within it. The decision to use MIFS or SIFS is DEV internal and the DEV should also take that into consideration when figuring out it's own internal guardtime at CTA start and end. The new MIFS CTRq TU bit puts extra calculation efforts on the PNC for no good reason. Let the DEVs handle this like they do with all other CTA related calculations. The PNC should be allowed to allocate adjacent CTA at its leasure and trust that the DEVs leave enough space at the CTA boundries.

Suggested Remedy: Remove the MIFS CTRq TU bit.

Response: ACCEPT.

CID 157:

Comment: The standard clearly states that the DEV is responsible for calculating it's needed channel time and also to make sure it stays within it. The decision to use MIFS or SIFS is DEV internal and the DEV should also take that into consideration when figuring out it's own internal guardtime at CTA start and end. The new MIFS CTRq TU bit puts extra calculation efforts on the PNC for no good reason. Let the DEVs handle this like they do with all other CTA related calculations. The PNC should be allowed to allocate adjacent CTA at its leasure and trust that the DEVs leave enough space at the CTA boundries.

Suggested Remedy: Delete page 188 line 33-39 and page 189 all reference to MIFS CTRq TU. The figures can stay to illustrate what the DEV needs to calculate. The PNC only allocates raw CTA and the DEV has to figure out how to use it.

Response: ACCEPT.

CID 101:

Comment: Undesirable specification. The use of the MIFS CTRq TU field for calculating the channel time is based on fixed frame transmission boundaries which do not hold in the case of retries.

Suggested Remedy: Remove the MIFS CTRq TU field from the draft and all references to it.

Response: ACCEPT.

CID 165 and CID 169

Comment: It would be helpful for DEVs to have a way to continuously monitor the channel quality between itself and other DEVs in the piconet. Monitoring the MCTAs would be a good way, but DEVs are not required to always transmit in their MCTAs.

Response: CID 165: Withdrawn, 12 March 2003. CID 169: Withdrawn, 12 March 2003.

1.2 Authenticate purge comments (CID 3, CID 39, CID 43, CID 45, CID 47 and CID 48)

On page 15, line 10, change ‘Association, authentication, and security’ to be ‘Association and security membership.’

On page 16, line 20, change ‘No authentication is required’ to ‘No security membership is required.’

On page 16, line 23, change ‘Authentication and payload protection: DEVs authenticate’ to ‘Secure membership and payload protection: DEVs establish secure membership.’

On page 16, line 26, delete the last sentence beginning ‘Optionally, DEVs are allowed....’

On page 16, line 29-33, replace this entire paragraph with ‘When security is enabled, i.e. the piconet is using security mode 1, then DEVs that wish to join the piconet are required to establish secure membership with the PNC. The DEVs may also establish a secure relationship with other DEVs with whom they wish to communicate. DEVs have established secure membership or a secure relationship when they get a management key. The process of establishing secure membership or a secure relationship is outside of the scope of this standard. The PNC or DEV that generates and distributes the key is called the key originator.’

On page 16, line 35-36 replace this paragraph with ‘The payload protection protocol, {xref 9.4.7}, uses a symmetric key that is generated by the key originator and is securely distributed to DEVs that have established secure membership or a secure relationship with the key originator, {xref 9.4.4}.’

On page 43, line 28 replace ‘This mechanism supports the process of an authenticated DEV requesting and receiving a key from the key originator in the authentication relationship’ with ‘This mechanism supports the process of a DEV requesting and receiving a key from a key originator.’

On page 44, line 15-16 replace ‘This primitive is generated by the DME for a DEV to obtain the designated key from the key originator in an authentication relationship’ with ‘This primitive is generated by the DME for a DEV to obtain the designated key from the key originator.’

On page 44, line 24 replace ‘an authenticated DEV’ with ‘a DEV.’

On page 45, line 3 replace ‘an authenticated DEV’ with ‘a DEV.’

On page 45, line 16-17 replace ‘as a result of the receipt of an MLME-REQUEST-KEY.indication’ with ‘as a result of the receipt of an MLME-REQUEST-KEY.indication from a DEV that has established secure membership or a secure relationship with the key originator.’

On page 46, line 3 replace ‘This mechanism supports the process of an authenticated DEV acting as key originator sending a key to an authenticated DEV.’ with ‘This mechanism supports a DEV acting as key originator sending a key to another DEV.’

On page 46, line 31 replace ‘an authenticated DEV’ with ‘another DEV.’

On page 46, line 45 replace ‘an authenticated DEV’ with ‘a DEV that has established secure membership or a secure relationship with the key originator.’

On page 47, line 3 replace ‘an authenticated DEV’ with ‘a DEV.’

On page 47, line 28 replace ‘an authenticated DEV’ with ‘a DEV.’

On page 48, line 3 replace ‘an authenticated DEV’ with ‘another DEV.’

On page 48, line 17 replace ‘an authenticated DEV’ with ‘another DEV.’

On page 48, line 17 replace ‘the authenticated DEV’ with ‘the DEV.’

On page 49, Table 13, KeyInfo row, Description column replace ‘The key agreed upon during authentication or key update process that are used’ with ‘The key used’

On page 135, line 5ff, replace ‘Authenticated (if required)’ with ‘Secure membership (if required)’

Change ‘and authentication is required for the piconet,’ to be ‘and secure membership is required for the piconet.’

Change ‘Since a neighbor PNC is not a member of the piconet, it sends commands without authentication.’ to be ‘Because a neighbor PNC is not a secure member of the piconet, it sends only non-secure commands.’

Page 135, line 12, rewite paragraph as ‘For peer-to-peer communications, if a DEV has established a secure relationship with a peer DEV, and the ‘Secure membership (if required)’ column is marked with an ‘X’, that command shall be sent to the peer DEV using a secure command using the key specified in Table 61.’

Page 135, line 21, replace ‘Authenticated (if required)’ with ‘Secure membership (if required)’

Page 136, line 31, replace ‘authenticated’ with ‘be a secure member of the piconet’

Page 138, line 39, replace ‘authenticated in the piconet’ with ‘is a secure member of the piconet’

Page 139, line 12, replace ‘in an authenticated relationship’ with ‘in an secure relationship’

Page 141, line 38, replace ‘authentication data’ with ‘security information’

Page 142, line 40, replace ‘not authenticated’ with ‘is not a secure member of the piconet’

Page 142, line 41, replace ‘authenticated’ with ‘a secure member of the piconet’

Page 143, line 3, replace ‘authentication’ with ‘security’

Page 165, line 35, replace ‘authenticate with the parent PNC.’ with ‘establish a secure relationship with parent PNC.’

Page 165, line 45, replace ‘security data’ with ‘security information’.

Page 166, line 3, delete ‘and authentication process’

Page 170, line 34 Figure 99, change ‘authentication proces’ to be ‘establishes secure relationship’

Page 170, line 52, delete ‘authentication,‘

Page 171, line 8, replace ‘authenticate with the parent PNC.’ with ‘establish a secure relationship with parent PNC.’

Page 173, line 2, delete ‘authentication,‘

Page 173, line 13, delete ‘required for the authentication process’

Page 174, line 28, replace ‘upon successful completion of the authentication process.’ with ‘upon receipt of the MLME-MEMBERSHIP-UPDATE.request with MembershipStatus set to MEMBER.’

Page 178, line 11, replace ‘authentication’ with ‘security’

Page 178, line 12, replace ‘authentication is complete’ with ‘secure membership has been established’

Page 218, line 40, replace ‘associate and authenticate’, with ‘establish membership’

Page 232, line 7, replace ‘the key agreed on during mutual authentication.’ with ‘the PNC-DEV management key.’

Page 232, line 26, delete ‘an authentication protocol verify the authenticity of other DEVs in the piconet and’

Page 232, line 42, replace ‘authentication’ with ‘security’

Page 232, line 44, replace ‘authenticated’ with ‘associated’

Page 232, line 48, replace ‘performed the authentication protocol’ with ‘established secure membership’

Page 232, line 49, replace ‘authenticated DEVs to perform the authentication protocol with the new PNC.’ with ‘associated DEVs to establish secure membership with the new PNC.’

Page 233, line 1, replace ‘all of the authenticated DEVs’ with ‘the piconet’

Page 233, line 2, replace ‘authenticated DEV’ with ‘member of the piconet’

Page 233, line 4, replace ‘If the DME of each DEV chooses to accept this security information, the authentication process between the new PNC and each authenticated DEV may proceed without any interruption of service.’

Page 233, line 10 and 11, replace ‘authenticated DEVs’ with ‘members of the piconet’, 2 places.

Page 233, line 27 replace paragraph with ‘If a DEV wishes to join a secure piconet, it should associate with the PNC in order to be assigned a local DEVID. Once the DEV is associated, the PNC shall allocate an MCTA if commands are not allowed in the CAP. The DEV or PNC may choose to send Probe Request and/ or Announce commands to each other to either request or transmit IEs, including Vendor Specific IEs. The DEV and PNC may also exchange additional data frames, Security Message comamnds. After the DEV has associated and exchanged the desired information with the PNC, the DEV shall establish secure membership. The process by which secure membership is established is outside of the scope of this standard.’

Page 233, line 41, replace ‘authentication process’ with ‘establishment of a security relationship’

Page 234, line 49, delete ‘key agreed on with the PNC during the authentication process.’

Page 235, line 22, delete ‘authenticated to the PNC and’

Page 235, line 24, replace ‘been authenticated,’ with ‘received the piconet group data key’

Page 237, line 10, replace ‘is authenticated with the PNC’ with ‘establishes secure membership in the piconet.’

Page 237, line 47, page 238, line 10 and line 20, replace ‘authentication’ with ‘the DEV becomes a secure member of the piconet’

Page 240, line 1, replace ‘three state machines; one state machine that controls the authentication operations, another state machine that controls the key management operations and a third that controls the processing of other secure frames.’ with ‘two state machines; one state machine controls the key management operations and another that controls the processing of other secure frames.’

Page 240, line 9, replace ‘the state machines about changes in authentication status and communicates the authentication status information between’ with ‘the MLME about changes in membership status and communicates the membership status information to’

Page 242, delete subclauses 9.4.1, 9.4.2. Delete the second paragraph on 9.4.

Page 245, line 24.5, delete ‘In order to facilitate the authentication process,’ and capitalize the ‘a’.

Page 246, line 24, delete ‘A DEV may use the Security Message command to support security related communications, e.g. authentication processes.’

Page 246, line 52, replace ‘authenticated DEV before changing the key using the distribute key protocol.’ with ‘member of the piconet.’

Page 247, line 53, delete ‘The DEV should initiate this protocol ... the current payload protection key.’

Delete clause 9.4.6 and 9.4.7.

Change ‘CCM authentication and encryption’ to be ‘CCM encryption and data authentication’ everywhere. Also search for ‘CCM encryption’ to be safe.

Page 318, line 28, change ‘authenticated’ to be ‘a secure relationship’

Page 318, line 30, replace ‘previously authenticated’ with ‘target’ (4 locations)

Page 318, line 33, replace ‘deauthenticate’ with ‘terminate the secure relationship with’

Page

Editorial: Security Session Identifier definition is no longer used in the draft.

Editorial: Page 48, line 28 replace ‘Primitive’ with ‘Primitives’

Editorial: Page 48, line 27 replace ‘is used’ with ‘are used’

CID 3 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/160r2.

CID 39 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/160r2.

CID 43 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/160r2.

CID 45 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/160r2.

CID 47 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/160r2.

CID 48 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/160r2.

1.3 Tuesday, 11 March 2003

Meeting called to order at 8:04 am CST.

CID 3 - Dan Bailey will provide detailed edits for changing this.

CID 166 - REJECT. The majority of the changes from Draft D15 to Draft D16 other than the removal of the optional public-key cryptography suites were editorial or clarification of the existing content. No major architectural changes were made to the MAC/PHY in the change from D15 to D16. It is the opinion of the Ballot Resolution Committee and other individuals that are in the process of implementing the draft standard that the changes made were not significant. In the closing plenary at Ft. Lauderdale, the working group approved the comment resolution results of the sponsor ballot committee and voted unanimously to send the revised draft to sponsor ballot recirculation. The working group was aware of the decision to remove the public-key security suites from the draft. The documents that provided the supporting information for the changes in the draft were made available to the sponsor ballot pool via the 802.15.3 web site.

CID 168 - REJECT. The SBRC voted 11 to 1 to remove the public-key cryptography suites, per the recommendation from the 802 SEC chair and the 802.15 working group chair. After discussion at the working group level, the 802.15 affirmed this decison and instructed the SBRC to proceed with sponsor ballot recirculation. The SBRC agreed that the inclusion of these suites could be seen as being outside of the scope of the PAR which limits the standard to the MAC and PHY only. The decsion to remove the security suites was affirmed by the working group in the closing plenary of the Ft. Lauderdale meeting as well. The issue of the inclusion of the public-key cryptography suites was not that there were more than one option, but rather that the authentication process took place in layers above the MAC and PHY. Removing all but one public-key suite would not resolve the issue of the public-key security suites being out of scope of the 802.15.3 PAR.

CID 167 - REJECT. The PAR of 802.15.3 limits the scope of our standard. There are many issues of an implementation that are outside of the scope of a MAC and PHY. For example, service discovery, network address resolution, routing and bridging are all outside of the scope of a MAC/PHY standard. The committee has used the experience with the public-key cryptography suites to ensure that the 802.15.3 MAC supports the use of these higher layer protocols to perform entity authentication and key establishment. There are higher layer protocols, e.g. 802.1x, that allow MAC/PHY standards to implement entity authentication and key establishment. The 802 leadership and the 802.15 working group chair both indicated that the inclusion of these security suites was outside of the scope of a MAC/PHY standard.

CID 54 - ACCEPT. (Ed note: JS to write clause 6, 7 and 8 text based on CID 54, due by Thursday)

CID 2 - ACCEPT IN PRINCIPLE. On page 233, line 20, delete ‘While waiting to obtain the ... valid beacon with the known key.’ On page 235, line 34, change ‘and send a Key Request command to the PNC to obtain the new piconet group data key.’ to be ‘and request a new piconet group data key, {xref 9.3.2}.’

CID 5 - Withdrawn 11 March, 2003.

CID 4 - ACCEPT.

CID 10 - ACCEPT IN PRINCIPLE. Change first sentence to "The key used to protect a particular frame depends on the purpose of the frame and the membership states of the DEV. If the DEV is a member of a secure piconet (i.e. the DEV is the PNC or the DEV is a secure member with the PNC), the DEV will have entries for the piconet group data key and for the PNC-DEV management key. If the DEV has a secure relationship with a peer-DEV (i.e. the DEV is a secure member with a peer DEV), the DEV will have entries for a peer-to-peer data key and a peer-to-peer management key that it shares with that DEV. For any given frame, the DEV shall either send the frame without security or with the single key that is required for that frame, as indicated in {xref Table 61}." (Ed. Note, look at this paragraph to see if it can read better).

CID 11 - ACCEPT.

CID 8- ACCEPT IN PRINCIPLE. Change 'above' on line 9 to be '{xref 7.2.7.2}.' Insert ', {xref 7.2.7.2}' after 'SECID' on line 8.

CID 13 - ACCEPT IN PRINCIPLE. On page 266, line 5, change ‘Seed encryption operation’ to be ‘Key encryption operation’ change ‘seed for key transport’ to be ‘key for key transport’ On page 266, line 6, change ‘seed’ to ‘key’ Change ‘CCM authentication and encryption’ to be ‘CCM encryption and data authentication’ in 2 places and change ‘CCM authenticated encryption’ to be ‘CCM encryption and data authentication’, all in table 73. Change the definition of ‘source authentication: ...’ to be ‘data authentication: Authentication of the sender of the data and provision of data integrity.’

CID 60 - Is this fatal or just annoying, JPKG to find out.

CID 57 - ACCEPT.

CID 160 - Can we add some text to clarify that the DEV backdate’s its timer?

Meeting recessed at 10:02 am CST.

Meeting called to order at 10:48 am CST.

CIDs remaining

New Always TX bit, Bill Shvodian to write new text, due ???, CID 165, CID 169.

Change to Beacon number rather than Beacon countdown, Allen Heberling, due 11 March, 2003 3:30 pm, CST: CID 149 and CID 150.

Last fragment field, JPKG due 11 March, 2003 3:30 pm, CST: CID 129

Retry bit, JPKG with input from WMS, due 11 March, 2003 3:30 pm, CST CID 106.

MIFS CTRq bit, Bill Shvodian, due ??, CID 142, CID 152, CID 157, CID 101.

Clean up of authentication in the security clause, Dan Bailey, due 12 March, 2003 3:30 pm: CID 3, CID 39, CID 43, CID 45, CID 47 and CID 48.

MLME-CREATE-STREAM.indicate, JPKG to check if this is crucial or nice to have, due 11 March, 2003 at 3:30 pm, CID 60.

CTA block location, can we add some helping text? Allen Heberling, due 3:30 pm, CID 160.

Meeting recessed until 3:30 pm, 11 March, 2003.

Meeting called to order at 3:35 pm, 11 March 2003.

CID 129 - REJECT, The current fragment fields allow a receiver of a fragment to know exactly how many fragments are in a fragmented MSDU no matter which fragment of the MSDU is received first. This allows an implementation the flexibility to be able to reassemble an MSDU in order in contiguous memory if that is desired. The total Fragment Number field allows up to 128 fragments. It was felt that 64 might be too low and a full 8 bits wouldn't fit into 2 octets of the Dly-ACK frame with a 9 bit MSDU number. The definition of the Fragmentation Control field was not changed between D15 and D16.

CID 106 - REJECT. The retry bit is included specifically for the purpose of doing duplicate detection. Consider the following scenario (excerpted from an email exchange when the group considered removing the retry bit in an earlier working group letter ballot):

1) Dev A sends Dev B a frame with stream=0 and MSDU=0 and frag=0.

2) Dev B ACKs the frame

3) Dev A sends 511 stream 0 frames to other DEVs, none to Dev B.

(remember, we only have one sequence number counter for all stream 0 frames regardless of destination).

4) Dev A sends DEV B a frame with stream=0 and MSDU=0 and frag=0.

What does DEV B do? If there is no retry bit, DEV B will discard the frame even though it is not a retry. If there is a retry bit, DEV B will not discard the frame unless the retry bit is set to 1.

Note that this is not the same as using one more bit in the MSDU number field because the probability of a frame error is not 50%. It better be 10% or less. 1 retry bit is better than 3 bits of MSDU #.

The retry bit and its interpretation was unchanged between D15 and D16.

CID 149 and CID 150: ACCEPT IN PRINCIPLE:

P52, L13 and L45. Line 13: Change 'NmbrHndOvrBcns' to 'HndOvrBeaconNumber', change the valid range to be '0-65535', change the description to be 'The beacon number of the superframe when the new PNC will take over as PNC for the piconet.' Line 45: Change 'NmbrHndOvrBcns' to 'HndOvrBeaconNumber'

P79, L43: Change 'ChangeCountdown,' to be 'ChangeBeaconNumber'

P80, L7: Change ‘ChangeCountdown,’ to be ‘ChangeBeaconNumber’, change change the valid range to be ‘0-65535’, change the description to be ‘The beacon number of the superframe when the new piconet parameter will take effect.’

P127, L37; and L41; and L44; and L47; and L51,

Line 37: New text ‘The new PNID that will take effect beginning with the superframe which has the beacon number equal to the Change Beacon Number field.’

Line 41: New text ‘The new BSID that will take effect beginning with the superframe which has the beacon number equal to the Change Beacon Number field.’

Line 44: New text ‘The offset in milliseconds between the beacon’s expected transmission time and the time that it will be send by the PNC, {xref 8.x.x}. The change occurs with the beacon which has the beacon number equal to the Change Beacon Number field.’

Line 47: New text ‘The new superframe duration that will be used for the superframe which has the beacon number equal to the Change Beacon Number field.’

Line 51: New text ‘The New Channel Index field contains the channel index of the PHY channel that the piconet will begin using with the beacon that has the beacon number equal to the Change Beacon Number field.

P127, L24: Change ‘ChangeCountdown,’ to be ‘ChangeBeaconNumber’

P128, L1; and L6: Rewrite the paragraph:

‘The Change Beacon Number field is the beacon number of the superframe when the change will take effect. The difference between the beacon number of the beacon which first includes this IE and the Change Beacon Number field is defined to be the NbrOfChangeBeacons. For a piconet without pseudo-static CTAs, NbrOfChangeBeacons shall be at least two. For a piconet that has pseudo-static CTAs, NbrOfChangeBeacons shall be at least mMaxLostBeacons. For a piconet that has child or neighbor piconets, NbrOfChangeBeacons shall be at least eight. However, a child or neighbor PNC may set the NbrOfChangeBeacons to a different number based on the Change Countdown field in the parent PNC’s beacon as defined in 8.11.1.

P129, L8; L16 Line 8: Change ‘Handover Countdown’ to be ‘Handover Beacon Number’, on line 16, change it to read ‘The Handover Beacon Number field contains the beacon number of the first beacon that will be sent by the new PNC. The last beacon sent by the old PNC will have a beacon number one less than the Handover Beacon Number field.

P165, L29: Change ‘where the countdown is set to zero’ to be ‘which has a beacon number equal one less than the Handover Beacon Number field in the Handover IE’

P167, L3 and L5: Change ‘Handover Countdown field set to indicate the last superframe that it will be the PNC’ to be ‘Handover Beacon Number field set to indicate the first beacon that will be sent by the new PNC’ Change ‘will be the one in which the Handover Countdown field is zero.’ to be ‘will be the one in which the beacon number is one less than the Handover Beacon Number field.’

P211, L36: Change ‘change countdown value’ to be ‘the value of the Change Beacon Number field’

P211, L44: Change ‘change countdown’ to be ‘Change Beacon Number’

P212, L16; L36; In both lines, change ‘change countdown=1’ to be ‘beacon number = Change Beacon Number -2’, change ‘change countdown=0’ to ‘beacon number = Change Beacon Number -1’, change first ‘beacon' to be 'beacon number = Change Beacon Number', change second 'beacon' to be 'beacon number = Change Beacon Number + 1'

P213, L17: Change 'at the time of the first beacon after the beacon with the Change Countdown field equal to zero has been sent.' to 'at the time of the beacon with a beacon number equal to the Change Beacon Number field in the previous Piconet Parameter change IEs.'

P214, L43 and L45: Change 'change countdown after which the piconet DEVs shall switch to the new channel.' to be 'Change Beacon Number field that contains the beacon number of the first beacon that will be sent on the new channel.' change 'The channel change shall take effect starting with the first beacon sent after the Change Countdown field becomes zero.' to be 'The channel change shall take effect starting with the first beacon with a beacon number equal to the Change Beacon Number field in the previous Piconet Parameter Change IEs.'

CID 160 - REJECT. The start of the superframe has been set to be the first symbol of the beacon preamble since November of 2001. A DEV simply adjusts their timer to account for the fact that the frame synchronization event occurs after the first symbol of the preamble. The current definition indicates that the first energy that is sent on the wireless medium for the superframe occurs after time 0.

Meeting recessed at 4:55 pm, CST.

1.4 Monday, 10 March 2003

Meeting called to order at 4:25 pm CST.

CID 19 - ACCEPT.

CID 21 - ACCEPT.

CID 22 - ACCEPT.

CID 23 - ACCEPT.

CID 24 - ACCEPT IN PRINCIPLE. On page 232, line 8, change 'are discarded' to be 'is passed to the DME using the MLME-SECURITY-ERROR.indcate and no other action is taken on the frame by the MLME.' Also page 231 line 40 and all other occurances.

CID 27 - ACCEPT.

CID 28 - ACCEPT IN PRINCIPLE. Add sentence following "...not specified in this standard.", "The Security Message command has been included as a special command to assist in the implementation of vendor specific protocols for establishing security relationships and any related data.

CID 31 - ACCEPT.

CID 33 - ACCEPT.

CID 36 - ACCEPT IN PRINCIPLE. Change "authentication" to "secure membership" in two places.

CID 35 - ACCEPT.

CID 37 - ACCEPT IN PRINCIPLE. Change:Line 24: "such as a change in authentication state" to "such as a change in security relationship"Line 25: "transitions from being unauthenticated to authenticated or viceversa" to "changes membership status in a security relationship"Line 27: "change in authentication status" to "change in secure membership status"

CID 38 - ACCEPT.

CID 39 - Write new text for the security membership row that replaces authentication and deauthenticaion rows, change the table title as well. - Bailey, due 11/3/03 am.

CID 41 - ACCEPT.

CID 42 - ACCEPT.

CID 44 - ACCEPT.

CID 45 - Replace authentication and deauthentication with MLME-MEMBERSHIP-UPDATE.request in the figures and in the text in 9.4.6.1. Lots of text, could be 12 March 2003.

CID 43 - Resolve with CID 45.

CID 46 - ACCEPT IN PRINCIPLE. Change two occurances of "authentication complete" to "security membership established". Also change de-authenticate to "secure membership rescinded"

CID 47 - Replace authentication and deauthentication with MLME-MEMBERSHIP-UPDATE.request in the figures and in the text in 9.4.6.3. Lots of text, could be 12 March 2003.

CID 48 - Replace authentication and deauthentication with MLME-MEMBERSHIP-UPDATE.request in the figures and in the text in 9.4.6.4. Lots of text, could be 12 March 2003.

CID 49 - ACCEPT IN PRINCIPLE. Change text on right side of figure to read' to be 'Disassociate command sent or received, membership status rescinded or PNC handover.' Add text to page 233, line 54. ', i.e. the DEVs secure membership has been rescinded.' Add text to page 234, line 3 change "If the MembershipStatus is set to NON-MEMBER, the MLME shall ...' to be 'If the MembershipStatus is set to NON-MEMBER, the DEV's secure membership is rescinded and the MLME shall ...'.

CID 50 - ACCEPT IN PRINCIPLE. Change text on right side of figure to read' to be 'Disassociate command sent or received, membership status rescinded or PNC handover.'

CID 51 - ACCEPT.

CID 151 - REJECT. The symmetric key operations happen at the MAC level and so the updating and exchanging of these keys is appropriate for the standard. The symmetric key operations are fully defined in this standard and they are an integral part of the frame formats. There needs to be a way for the MAC to change a key to maintain its freshness.

Meeting recessed at 5:33 pm CST.

Meeting called to order at 7:10 pm CST.

CID 76 - ACCEPT IN PRINCIPLE. Add a .indicate to be generated after the reciept of the second Assocation Request command with the Piconet Services Inquiry bit set. Change the existing .indicate primitive to be a .confirm that carries the information back to the DEV that requested it. Add the When generated and Effect of Reciept. Update the MSC in figure 103 to be PNC MLME -> .indicate -> PNC DME, PNC DME -> .response -> PNC MLME, and DEV MLME -> .confirm -> DEV DME.

CID 59 - ACCEPT IN PRINCIPLE. Change text to indicate that the Association IE only indicates that a DEV is associated. Add text to the PNC information command using the old text from the Association IE to indicate that this command is used to communicate changes in a DEV's membership.

CID 58 - ACCEPT IN PRINCIPLE. Add a timer to the MSC that starts after the MLME-ASSOCIATE.response primitve. Add text that says that the associating DEV has until the ATP timer expires to send the response frame. If the DEV sends the second response command after the timeout expires, the PNC sends the disassociate command as described in 8.3.4.

CID 96 - ACCEPT IN PRINCIPLE. The backoff counter is suspended and then re-starts with the next CAP. This is stated on page 181, lines 38-42. Delete the xref to 8.4.2 on line 39, the text is now in the same subclause.

CID 169 and CID 165 - Sounds interesting, check for outside opinion.

CID 149 and CID 150 - Probably a good idea, but we need to review the text to find all of the places where it will need to change, probably a few in clause 8 as well as the parameter names in clause 6. The beacon number will correspond to the superframe when the change takes effect. The beacon number - 1 superframe is the last superframe with the old status. ADH will review clause 8 text to find out where to change.

CID 93 - ACCEPT.

CID 120 - ACCEPT IN PRINCIPLE. Asynchronous data can't use the Dly-ACK because there is no guarantee that the MSDU numbers will be sequential because asynchronous data frame all share the same MSDU counter, regardless of destination. If the DEV is sending asynchronous data to more than one destination, there will be gaps in the MSDU numbers.

The text in 8.8.3 is confusing, move the sentence on page 205, line 27 to 8.1 on line 27, page 159.

CID 125 - ACCEPT IN PRINCIPLE. Use the yet unused bit combination in the ACK Policy subfield to indicate "Dly-ACK Policy with Dly-ACK Request", and merge reserved bits into a reserved subfield.

CID 129 - Will be reject, James to dig up the old reject text. Keep the same name.

CID 106 - Will be reject, WMS will dig up old email on why the retry bit is used. Also add an xref to 7.2.1.6 to the fragmentation and duplicate detection. 8.8.4 and 8.8.5.

CID 68 - ACCEPT IN PRINCIPLE. The RIFS was intended as guidance of when the DEV could start the retransmission, however in the current draft it incorrectly mandates when the DEV will start transmitting. Change "limit has been met) at the end of RIFS as long" to be "limit has been met) after the end of RIFS as long"

CID 142, CID 152, CID 157, CID 101 - MIFS CTRq? WMS will check with KO to get better explanation of why it should be deleted.

CID 143 - ACCEPT IN PRINCIPLE. Change the first sentence on line 20 to be "The Wake Beacon Interval field is defined in {xref 7.5.8.3}. This field is set to the system wake beacon interval for PS sets 0 and 1." Change the first sentence on line 24 to be "The Next Wake Beacon field is defined in {xref 7.5.8.4}. This field is set to the next system wake beacon for PS sets 0 and 1."

CID 98 - ACCEPT IN PRINCIPLE. Add a new sentence to the end of line 26 on page 183: ‘The source DEV may also send a frame to a destination DEV in any CTA assigned to that source even if the destination DEV is different that that indicated in the CTA block, provided the source DEV has determined that the destination DEV will be receiving in that CTA, {xref 7.4.11}.’

CID 148 - REJECT. Sending with the IE would save a total of 7 octets per DEV. However it would limit the total number of DEVs unless the Announce command could be fragmented. Alternatively, the number of DEVs in the piconet would have to be communicated if multiple Announce commands were used. The text on broadcasting the piconet information with the PNC Information command was unchanged between D15 and D16.

CID 156 - REJECT. Sending with the IE would save a total of 7 octets per DEV. However it would limit the total number of DEVs unless the Announce command could be fragmented. Alternatively, the number of DEVs in the piconet would have to be communicated if multiple Announce commands were used. The text on broadcasting the piconet information with the PNC Information command was unchanged between D15 and D16.

CID 158 - ACCEPT.

CID 155 - ACCEPT IN PRINCIPLE. In Figure 103, change ‘in the first Association Request command.’ to be ‘in the Association Request command with the SrcId set to the newly assigned DEVID.’ On page 177, line 1 change ‘in the Association Request command’ to be ‘in the Association Request command with the SrcID set to the newly assigned DEVID’ On page 177, line 3, change ‘PNC has received the second Association Request’ to be ‘PNC has received the second Association Request with the SrcID set to the newly assigned DEVID’

CID 53 - REJECT. The DEV will eventually timeout waiting for the IE if the DEV doesn't return it. This is sufficient for the state machines.

CID 54 - JPKG to ask JS how important this is. What if we put the received Overlapping PNID in the beacon. Can this be done by just sending it in piconet parameter change? How about letting it re-send it every 0x2A superframes. Also say that DEVs don’t send it if the Piconet parameter change is in the beacon.

Meeting recessed at 10:22 pm CST.

2. Unsatisfied technical comments from SB1

3. Status summary

3.1 Status at Dallas

.

Table 1—Ballot resolution at opening of Dallas meeting

Type	SB1	SB2
T (technical)	447	67
E (editorial)	379	104
Total	826	171

.

Table 2—Comment resolution at opening of Dallas meeting

Type	3/10/03	3/11/03
Unresolved T	31	
Resolved T	36	
Unresolved E	72	
Resolved E	32	
Total coments	171	171