IEEE P802.15
Wireless Personal Area Networks

Project	IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)	
Title	**TG3 LB22 comment resolution**	
Date Submitted	[11 November, 2002]	
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 LB22.]	
Purpose	[To provide a record of the comment resolution for LB22.]	
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 Kauai

1.1 Monday, 10 November, 2002

1.1.1 Security comments

Meeting called to order at 7:00 pm HAST.

CID 194 (Rasor, TR) - At the Vancouver plenary, in the agreeded upon security resolution regarding security models, the GROUP was told that the architecture presented by NTRU and adopted in St. Louis as the baseline would support both piconet wide data protection and smaller groups beginning at the peer to peer level. The current text does not support that model. The suggested text supports the current model as well as a sub-group starting at 2 DEVs and going up to the nmaximum allowable number of DEVs in the piconet - 1. Delete section 9.1.6 and insert the following text: Data encryption uses a symmetric cipher to protect data from being read by parties without the cryptographic key. Data may be encrypted either by using a key shared by all piconet DEVs or by using a key shared between two or more DEVs. **Suggest reject:** Do not have a remedy. For starters, the nonce and logic to determine which key to use must change. Appears to be a major technical change.

> Reject, “Group authentication mechanisms (other than the piconet group) is outside of the scope of the standard. In addition, the changes required for the current draft to implement this have not been presented to the task group. A mechanism does exist in the standard to accomplish sub-group security. The method that is available to do this is to start a dependent piconet with the members of that piconet as members of the dependent piconet.”

CID 195 (Rasor, TR) - At the Vancouver plenary, in the agreeded upon security resolution regarding security models, the GROUP was told that the architecture presented by NTRU and adopted in St. Louis as the baseline would support both piconet wide data protection and smaller groups beginning at the peer to peer level. The current text does not support that model. The suggested text supports the current model as well as a sub-group starting at 2 DEVs and going up to the nmaximum allowable number of DEVs in the piconet - 1. Data integrity uses an integrity code, often referred to as a message authentication code, to protect data from being modified by parties without the cryptographic key. It further provides assurance that data came from a party with the cryptographic key. Integrity may be provided using a key shared by all piconet DEVs or using a key shared between two or more DEVs. All secure data frames that fail integrity checks are discarded. **Suggest reject:** Do not have a remedy. For starters, the nonce and logic to determine which key to use must change. Appears to be a major technical change.

> Reject, “Group authentication mechanisms (other than the piconet group) is outside of the scope of the standard. In addition, the changes required for the current draft to implement this have not been presented to the task group. A mechanism does exist in the standard to accomplish sub-group security. The method that is available to do this is to start a dependent piconet with the members of that piconet as members of the dependent piconet.”

CID 196 (Rasor, TR) - The current text in 9.2.2 attempts to implement a very loose heartbeat function that closes teh set of authenticated DEVs in an established piconet. The problem is that security, in the sense of a wireless network, cannot be "mushy." In more definite terms, the text of 9.2.2 is indefinite and cannot be used to implement a method that securely, reliably closes teh network set. Replace the exsiting text with the following text: Current rememdy lacks notion of frequency. Even with "shall," DEV can simply choose to never do this. The PNC or another DEV shall request that each DEV with which it has authenticated (previously authenticated DEV) periodically transmit a secure frame using the management key to be certain that that DEV is still in the piconet. If no secure frames are being transmitted by the previously authenticated DEV, the PNC or requesting DEV shall send a secure probe command requesting an information element (such as the DEV adress) from the previously authenticated DEV. If the previously authenticated DEV does

not respond with a secure frame within a predetermined period of time, the previously authenticated DEV's authentication is revoked and the PNC or requesting DEV shall disassociate or deauthenticate the previously authenticated DEV. By definition, dissassociation of an authenticated DEV results in deauthentication. **Suggest accept in principle:** Rene and Gregg to clarify use of "periodically." Also Gregg to massage text slightly to clarify.

> Reject, "The current text allows DEVs to keep track of when other DEVs are still within the piconet. If the security manager wants to ensure that the DEVs are still available it can send frames to those DEVs. The security manager could also change the key periodically to ensure that DEVs that are part of the relationship are still current."

CID 242 (Shvodian, TR) - It needs to be made clear if authentication is required for a neighbor piconet. If so, a separate table is needed for neighbor authentication where the sym_keys_D are not passed. Create a table for neighbor authentication. **Suggest accept in principle:** Update 8.2.5, last paragraph. Change "The neighbor PNC is not a member of the parent piconet and shall only send the association request com-mand, the dissassociation command, the CTR command, authentication commands or any required Imm-ACK frames to the parent PNC. The parent PNC is not a member of the neighbor piconet." to "The neighbor PNC is not a member of the parent piconet and shall only send the association request command, the dissassociation command, the CTR command, or any required Imm-ACK frames to the parent PNC. The parent PNC is not a member of the neighbor piconet. In particular, the neighbor PNC shall not send authentication commands to the parent PNC."

> Accept in principle, "While the Neighbor PNC is allowed to request authentication from the parent PNC, it is unlikely that this would be successful based on the security policy of the parent PNC. However, it is not prohibited in the draft, so the text in 8.2.5 is correct."

CID 241 (Shvodian, TR) - The fact that a public key is in the ACL is not what provides theat the public key belongs to the intended DEV. The trust is established by the fact that the DEV can respond to the challenge and prove that it has the private key that accompanies the public key in the ACL. The fact that the public key and dev address are in the ACL provides the authorization that the DEV should be allowed into the piconet, provided it can authenticate by proving that it has the private key. Change to: In order to use a public key to achieve mutual authentication, it is necessary to trust that the received public key belongs to the intended DEV. This trust shall be indicated by a certificate or by a DEV rsponding sucessfully to a challeng, proving that it has the private key that corresponds to the public key in the ACL. the key's representation in an ACL or by the DEV verifying a digital certificate at the time of authentication. **Suggest reject:** Section 9.1.3 is addressing accepting trust in a public key. For this operation, verification of a certificate or the key's representation in the ACL is adequate.

> Accept in principle, "Change 'that the received public key belongs to the intended DEV.' to be 'that the received public key belongs to the intended DEV associated with the DEV address.'"

CID 199 (Rasor, TR) - The reference "While the security suites are interoperable," is inaccurate and misleading. Interoperation implies exactness in purpose, operation and results. In our case, the purpose of all security suites is the same, but the operation and results are different. For example, the ECMQV suite establishes a 128 bit key, while the NTRU and RSA suites establish only 80 bit keys. Repair the text to accurately reflect the defined operation of any current or future security suite. **Suggest accept in principle:** Change 9.4, line 49 from "While the security suites are interoperable, it is possible that there are differences in the levels of security provided as described in C.3" to "While the security suites all establish symmetric keys, it is possible that there are differences in the levels of security provided as described in C.3."

> Accept suggested resolution.

CID 198 (Rasor, TR) - In reading this clause, an implementer will certainly be confused. The Access Control List is said to contain information "about which devices are authorized to authenticate with the DEV using

their corresponding public key." The implemener then see the "manner in which the ACL is used depend[ing] on the application and the security suite in use." This is very confusing for the following reason. In the 802.15.3 ad-hoc network, DEVs are openly admitted (associated), and admitted DEVs then request authentication, and if successful, the PNC will add the authenticated DEV to the ACL. Does the current text preclude this operation? The text must be modified to address the correct issue. That issue is the binding of a DEV's identity to its public key, then the subsequent addition of the DEV's public key, or other representation into the ACL to control future group membership in the piconet. **Suggest accept in principle:** Change 9.3.2, 2nd paragraph to move the last sentence "See C.4 for further details on authorization of public keys." to be the second sentence in the paragraph.

Accept suggested resolution.

CID 201 (Rasor, TR) - The SRF - Security requirements field, defined as being included in the authentication response command used to indicate the authentication policies of the security manager. This should be more fully discussed with respect to the operation and establishment of data keys. It needs to be able to establish a required bit level of security in a system. Reference to current sections:

7.5.2.2 Authentication response command

If the certificates required bit is set to 1, the security manager shall only authenticate DEVs with a security suite that uses certificates, 1.2.1 and Table 96, while it operates as the security manager. If the 128-bit security required bit is set to 1, the security manager shall only authenticate DEVs with a security suite that is stated to provide 128-bit security in Table 96 while it operates as the security manager. The auth response field is the integrity code generated by the security manager and associated with the authentication protocol, 10.2. 10.3.1.3 ECMQV key agreement protocol The optional parameter Text2 as specified in sections 6.11.1 and 6.11.2 of ANSI X9.63-2001 shall be the one-byte value of the security requirements field included in the authentication response command,7.5.2.2.

Suggest reject: The Security Requirements Field allows a PNC to require 128-bit security suite and/or certificate usage. It currently suffices.

Reject “The security requirements field allows the PNC to require an 128-bit security suite and/or certificate usage. It does not adversely affect the security of the piconet to allow higher levels of security.”

CID 18 (Barr, TR) - When mode 2 was removed, implementation of any of the defined security suites for the remaining security mode is required. This sentence limits the suites to the non-certificate security suites which was not the intention of the BRC when this was accepted. Change "ECMQV manual, NTRUEncrypt raw 1, or RSA-OAEP raw 1" with "ECMQV manual, ECMQV implicit, ECMQV X.509, NTRYEncrypt raw 1, RSA-OAEP Raw 1, or RSA-OAEP X.509 1" **Suggest accept in principle:** Change "ECMQV manual, NTRUEncrypt raw 1, or RSA-OAEP raw 1" to "ECMQV manual, ECMQV implicit, ECMQV X.509, NTRYEncrypt raw 1, RSA-OAEP Raw 1, or RSA-OAEP X.509 1"

Accept in principle “The text has an incorrect set of cross references and a sentence that is not clear. Change ‘one of the following sub-suites: ECMQV manual, NTRUEncrypt raw 1, or RSA-OAEP raw 1. All other defined security subsuites may be implemented by a compliant DEV.’ to be ‘one of the sub-suites listed in {xref Table 95}. A DEV may implement more than one of the defined security subsuites.’ This matches the requirements in the PICS clause.”

CID 120, 121 (Heberling, T) - [SEC/Auth] Not clear whether PublicKeyObjectLength parm is required in the MLME-AUTHENTICATE.request/indication primitive's parm list since this parameter does not get used in the Authentication request command,7.5.2.1. Either add the parameter to the Authentication request command or delete the parm from the MLME-AUTHENTICATE.request primitive's parm list. Please make the

indicated change. **Suggest accept in principle:** Remove PublicKeyObjectLength parameter from MLME-AUTHENTICATE.request, 6.3.7.1 and MLME-AUTHENTICATE.indication, 6.3.7.2.

Reject “While the PublicKeyObjectLength is not sent explicitly over the air, it is used to calculate the length of the command frame by the MLME.”

CID 122, 123 (Heberling, T) - [SEC/Auth] It is not clear whether the "Key" parm in the MLME-REQUEST-KEY.response/confirm primitive's parm list needs to be listed as "EncryptedKey" since that is how it is named in the request key response command, 7.5.2.6. Please clarify which name is correct and make the appropriate change in either clause 6 or clause 7. Please make the requested clarification and change. **Suggest accept in principle:** Change 6.3.8.3.2 from "The MLME generates a request key response command, 7.5.2.6, and sends it to the specified DEV." to "The MLME generates a request key response command, 7.5.2.6 ,and sends it to the specified DEV. The MLME encrypts the key before transmission." Change the last sentence of 6.3.8.4.1 from: "Otherwise, the ResultCode is SUCCESS." to "Otherwise,the ResultCode is SUCCESS and the MLME decrypts the key."

Accept suggested resolution.

CID 124, 125 (Heberling, T) - [SEC/Auth] It is not clear whether the "Key" parm in the MLME-DISTRIBUTE-KEY.request/indication primitive's parm list needs to be listed as "EncryptedKey" since that is how it is named in the distribute key request command, 7.5.2.7. Please clarify which name is correct and make the appropriate change in either clause 6 or clause 7. Please make the requested clarification and change. **Suggest accept in principle:** Change 6.3.9.3.2 from "The MLME generates a distribute key response command, 7.5.2.8, and sends it to the specified DEV." to "The MLME generates a distribute key response command, 7.5.2.8, and sends it to the specified DEV. The MLME encrypts the key before transmission." Change the last sentence of 6.3.9.4.1 from: "Otherwise, the ResultCode is SUCCESS." to "Otherwise, the ResultCode is SUCCESS and the MLME decrypts the key."

Accept suggested resolution.

CIDs with no resolution:

Table until 1:00 pm Tuesday, November 12, 2002.

CID 16 (Barr, T) - A DEV must associate in order to be assigned DEVID and CTAs. Change 'should' to 'shall' Suggest accept?

CID 15 (Barr, T) - Since the new PNC must authenticate with all of the DEVs in the piconet. It must allocate time for this to happen. If the PNC does not allow commands in the CAP, then the PNC SHALL set up CTAs for authentication. Change 'should' to 'shall' and note that this is only necessary when commands are not allowed in the CAP. Suggest accept in principle: Change 9.2.4, line 20 from "When the PNC role has been handed over,the new PNC should set up CTAs for each of the authenticated DEVs to perform the authentication protocol with the new PNC." to "When the PNC role has been handed over, the new PNC shall set up CTAs for each of the authenticated DEVs to perform the authentication protocol with the new PNC if commands are allowed in the CAP. Otherwise it should set up CTAs for each of the authenticated DEVs to perform the authentication protocol with the new PNC."

CID 200 - No agreement among security participants.

CID 9 - Tabled for clarification by commenter.

CID 245 (Shvodian, T) - It looks like certificate use has been added for Ntru and RSA. WHy are these not listed as sub-suites in Table 95 as they are for ECMQV. Be consistent. Either add sub-suites for Ntru and RSA or delete them for ECMQV. Table to discuss with commenter.

CID 243 - Tabled for discussion with Rene.

CID 244 - Tabled for discussion with Rene.

CID 19 - Tabled for discussion with Rene.

CID 229 - Tabled for discussion with Rene.

1.1.2 Miscellaneous

CID 56 (Gubbi, TR) - Same as comment #537 in LB12 and Comment 387 in LB19 ORIGINAL COMMENT (LB12): What is the point in having slotted aloha access in addition to the backoff in CAP, TDMA in CFP? Why is this complexity being thrusted on the implementors of this "low cost", "low complexity" and "low power" standard?I don;t see any justification in having yet another access scheme with WPAN. ORIGINAL SUGGESTED REMEDY Remove slotted aloha scheme in 8.4.3.4 and all references to it from the draft. RESPONSE: REJECT. Slotted Aloha was added to make the MAC more versatile so that more PHYs that could use the 802.15.3 MAC. While it could be added at a later date, that would make the MACs incompatible.REBUTTAL: SAME AS THAT FOR COMMENT 536 in LB12 Commenter's response (LB22) If slotted aloha is added so that the MAC is used in other PHYs, since DEVs using different PHYs can not directly communicate with each other why should it cause incompatibility? The new mechanisms in MAC must be added only when a defined PHY needs it, all of which we may not know today. At the time of addition of new mechanism, it has to be overlaid on the existing mechanism. and there is definitely a way to do the same with slotted aloha as and when it is needed. For example, a set of stream indices can be left reserved and used at that time for the purpose desired. Regarding MCTA, specifically, what is not objected to is the open and association MCTAs. What prevents these things to be done in CAP insteadof devicing a new mechanism altogether for such a relatively low probability events? -- Remove open/association MTS/MCTA mechanism and slotted aloha mechanism and all references to them from the draft (Applicable to 8.4.4.4 and 8.4.4.5 in LB22/D14) Reserve a group of stream indices in 7.2.5 for future enhancements like the slotted aloha so that it can be added if and when it is really needed. **Suggest reject:** "The open and association MCTAs were added to handle two concerns, the first was that new PHYs may not support efficient CCA detection. In this case, slotted aloha provides a contention access method that provides for the needs of the piconet. Another reason to used slotted aloha is that under certain conditions, it can be more efficient than using the CAP. Adding a new contention method to the MAC when a PHY group has been formed is probably not the best venue. At this time, the TG has many members who have expertise in the MAC available to review draft. In the future, when a new PHY is down-selected, there may not be as many people available who have the experience and knowledge of the TG3 MAC to be able to add a new contention method. Adding slotted aloha does not add much, if any complexity, the DEV needs the random number generatora and exponential increasing backoff for any contention based method. The DEV is already required to be able to send frames and look to see if it gets an ACK. Depending on the parameters used for either the CAP or the open and association MCTAs, the power usage may actually be lower using MCTAs for the DEVs in the piconet than using the CAP. MCTAs have an advantage over the CAP in that they can be put into multiple locations in the superframe allowing the PNC to potentially use the time more efficiently."

Reject as indicated above.

CID 63 (Gubbi, TR) Same as comment 513 in LB19 Comment: same as comment #536 in LB12 ORIGINAL COMMENT (LB12)If SA is broadcast and anybody could start tx, how's collision handled? What is the point in getting devices to collide here instead of making this MTS part of CAP and letting devices freely use CAP as alreadydefined. This is useless and adds unnecessary complexity ORIGINAL SUGGESTED REMEDY (LB12): Remove lines 8:22 on page 151 and all references to "MTS/GTS with BC/MC-SA"from the draft Response: REJECT. The slotted aloha access method is used to provide access to theseslots just as CSMA/CA is used in the CAP. The TG has decided to allow bothaccess methods, CSMA/CA in the CAP and slotted aloha in the MTSs so thatthe 802.15.3 MAC is capable of supporting different types of PHYs. REBUTTAL (LB19): The response does not resolve the issue of having COLLISION based transmissions

under COLLISION FREE PERIOD, instead of making this part of CAP. I do not see 802.15.3 PHY or applications listed in PAR requiring it. I do not see how CSMA/CA mechanism used in CAP and TDM mechanism used in CFP fail in achieving whatever the slotted-aloha cheme is achieving. I do not see any reason or justification to add extra complexity resulting from having one another channel access mechanism. Suggested Remedy: Remove MTS mechanism and slotted aloha mechanism and all references to them from the draft. (This is applicable to section 8.4.4.4 and 8.4.4.5 in the current draft) Response: ACCEPT IN PRINCIPLE. Add new subclause 11.2.10, 'Channel access methods' with text 'A PNC-capable DEV compliant to this standard shall allow the use of the CAP for contention based access for association, data and commands, {xref 7.3.1} when using the 2.4 GHz PHY. A DEV compliant to this standard shall support the use of the CAP when using the 2.4 GHz PHY.'Use 1 bit from the reserved bits to the 'Piconet mode field', 'MCTAs used' with definitions 'The MCTAs used bit shall be set to 1 if the PNC will be using open or association MCTAs.' Delete the sentence on page 111, lines 1-2, 'If the CAP end time indicates no available time and no message types are permitted during the CAP, then MTSs are implied.' (note this deletion is in response to CID 407). Expand MLF13 in the PICs (note this will become MLF13.1 and MLF13.2 due to another comment.)MLF13.1; Open and association MCTA operations; 8.4.4.4, 8.4.4.5; O.1MLF13.2; Regular MCTA operations; 8.4.4.4; M{ed. note: the CAP stuff is like MLF13.3 now}Commentor's response: Response to this comment do not address the core issue of an additional access mechanism (MTS and slotted aloha) in the standard. The proposal does not justify why they are needed in802.15.3. Hence the resolution is unacceptable. -- Remove MTS mechanism and slotted aloha mechanism and all references to them from the draft. (This is applicable to section 8.4.4.4 and 8.4.4.5 in the current draft) **Suggest reject:** "The open and association MCTAs were added to handle two concerns, the first was that new PHYs may not support efficient CCA detection. In this case, slotted aloha provides a contention access method that provides for the needs of the piconet. Another reason to used slotted aloha is that under certain conditions, it can be more efficient than using the CAP. Adding a new contention method to the MAC when a PHY group has been formed is probably not the best venue. At this time, the TG has many members who have expertise in the MAC available to review draft. In the future, when a new PHY is down-selected, there may not be as many people available who have the experience and knowledge of the TG3 MAC to be able to add a new contention method. Adding slotted aloha does not add much, if any complexity, the DEV needs the random number generatora and exponential increasing backoff for any contention based method. The DEV is already required to be able to send frames and look to see if it gets an ACK. Depending on the parameters used for either the CAP or the open and association MCTAs, the power usage may actually be lower using MCTAs for the DEVs in the piconet than using the CAP. MCTAs have an advantage over the CAP in that they can be put into multiple locations in the superframe allowing the PNC to potentially use the time more efficiently."

Reject as indicated above.

CID 58 (Gubbi, TR) Same as CID 410 in LB22 Original comment: The new field "Num max frame size" is mostly useless. What if all the frames are (aMaxFrameSize-1) octets long? Instead of that, it is useful to includethe total number of octets as sum of number of octets in the payload of all frames sent in the dly-ack-window. this total number of octets is helpfulin buffer management at the receiver which is supposed to hold all theframes (in some corner cases) until a delayed-ack-frame is sent.Suggested Remedy:1. Remove "Num max frame size" from Figure-15 and all its references from the fraft2. Include total number of octets as sum of number of octets in the payload of all frames sent in the delayed-ack-windowResponse: REJECT. Two variables are needed, the total amount that can be sent as well as the number of frames that the destination DEV is able to handle. The number of frames is important because there are physical limitations in the Dly-ACK generation. The other reason is that there are physical limitations in the buffer implemention, e.g. addressing. Commentor's response: The commenter agrees that there are two variables needed and it is evident by the suggestion. But what is not clear is the intention in providing number of frames of size aMaxFrameSize, instead of providing a direct bound of max on total number of octets that is entertained in the burst. The implementations can make use of this information in a useful way while the current info does not given any cluse on the size of the (MAxNumFrames - NumMAxFrameSize) of the frames. How do you expect the implementations to guess those sizes? If all of them are (aMaxFrameSize-1), they are not indicated to the rx-DEV in this frame and the rx-DEVis supposed to handle them properly. In the worst case if all of the NumMaxFrames areof the size (aMaxFrameSize-1), then NumMAxFrameSize will be indicated as

zero although the rx-DEV has the pain of dealing with these mega-burst!! -- Remove "max frames" from Figure-17 and instead include a two-octet wide "total number of octets" as sum of number of octets in the payload of all frames sent in the burst. **Suggest reject:** “The TG has considered the new suggestion, but feels that ther are two different numbers that are required, one that gives the total amount of space available for frames and another that indicates the number of frames of any size that the DEV is able to receive. Both of these values have direct implications in terms of the capabilities of the implementation. An implementation will likely need to keep track of each of the frames received individually, e.g. assign them some space and a ‘pointer’ that indicates the start point and either a length or another ‘pointer’ to the end of the buffer. This places a specific requirement on an implementation that is not communicated with a single number of the total buffer space. In addition, using aMaxFrameSize is an abstraction that allows this to be used for future PHYs that may use much larger frame sizes as opposed to using only the number of bytes.”

Resolution is to reject.

CID 59 (Gubbi, TR) Same as Comment 412 in LB19 Original comment:In D10 the start of Information element was adjusted to be from even pos(2 octets) to help implementations having to deal with octet levelsearching for the start of required IE. Complexity involved in octetlevel searching is too much for low-cost implementations. This will also halve the computations needed in implementations that use higher size ords (like 4-octet).Suggested Remedy:Put back the paragraph that mandated the start of an IE at evenposition of octets and hence the padding of a zero if an IE whenever thetotal size of that IE is odd number.Response: REJECT. The frame formats specified only shows the bits sent over the air. Implementations of the receiver functions of a DEV are free to pad and rearrange to any word length, endian or bit order they may choose to optimize the interface to their host. This issue was discussed multiple times before the TG agreed to make the change. Commentor's response: The comment itself is about the bits sent over the air, not some constructionwithin rx-DEV. The goal is to simplify, as much as possible, the processing of IEs. As noted in the comment, the even octet aligning of IEs does simplify the processing both in hardware and software implementations. By the time the frame arrives at therx-DEV, the damage is already done in the sense that the rx-DEV has to go through octet level processing of the frame. Hence the resolution is NOT acceptable. -- Put back the paragraph that mandated the start of an IE at even position of octets and hence the padding of a zero at the tx-DEV at the end of an IE whenever the total size of that IE is odd number of octets. **Suggest reject:** “The BRC has addressed this issues and believes that while it may help some implementations to use 16 bit alignment for IEs, other impementations may not be assisted with this. For example, a 32 or 64 bit implementation would not necessarily benefit from the 16 bit alignment.”

Resolution is to reject.

CID 60 (Gubbi, TR) same as CID 414 in LB19 Original comment: In this sentence what does "multiple beacons" actually mean? Multiple beacons in the same superframe, similar to fragementing beacon, OR IEbeing present in beacons sent at different TBTT but each time with differentcontents of association info. I think what is intended is to say thatif there are too many assoc/disassoc, the beacon at current TBTT may notbe big enough to carry them all, so the remaining Dev-assoc-IEs will befilled into the next beacon sent at next TBTTSuggested Remedy:If intended, do NOT allow fragementation of beacon. Alter the sentence inln42:43 to mean that the PNC may send IE corresponding to a recent assoc/deassoc in the beacon at next TBTT if the current beacon does nothave space for it.Response:ACCEPT IN PRINCIPLE. Delete the sentence "The PNC may use multiple beacons to broadcast successive DEV association IEs if too many DEVs are associating than will fit in a single beacon.." as it is confusing and does not add any new information. The PNC is able to choose when it sends any IE.Commentor's response (LB22)The response addresses the issue only partially. For interpretations towardsconformance, "The PNC is able to choose when it sends any IE" is not correct The interpretation by vendors can go either way. that is, a group of implementors might expect the Dev-Assoc-IE contianing the recently associated DEVs to appear immediately after assoc while the rest might tolerate it appearing anytime. Hence the inclusion of the suggested remedy is required. I have rephrased the same in thefollowing text for editor's peruse (Applicable after the removal of sentence asin the response)."The the DEV association IE corresponding to an association shall be included in thebeacon sent at the start of immediate next superframe, excepting the case where thatbeacon is already at its maximum

allowed size where the inclusion of IE is delayeduntil the space in the beacon permits the same." -- I have rephrased my earlier suggested remedy in the following text for editor's peruse (Applicable after the removal of sentence asin the response)."The the DEV association IE corresponding to an association shall be included in thebeacon sent at the start of immediate next superframe, excepting the case where thatbeacon is already at its maximum allowed size where the inclusion of IE is delayeduntil the space in the beacon permits the same." Suggest accept in principle – TBD need to review to determine if draft text is not clear on use IEs and Association IE in beacons.

> Accept in principle "The sentence was deleted for draft D14 as indicated in the resolution of CID 414 for LB19. The words "multiple beacons" occurs only once in D14 in the section describing ASIE and not for association/disassociation. The repetition of beacon announcements is now described in 8.6.4 for all of the announcements, including this one. Functional descriptions, such as when announcements belong in clause 8. The location of text is editorial and the repetition of these elements is already described in clause 8."

CID 61 (Gubbi, TR) Definition of wake beacon is vague and hence can cause confusion to theimplementors who are not part of TG3 -- A wake beacon is a beacon sent by PNC at a previously declared periodic interval at which time all the sleeping DEVs, except those in HIBERNATE mode, are expected to be awake and be able to receive. Wake beacons contains <TBD???> in addition to other fields/elements that can be present in beacons transmitted at other times. The BC/MC traffic in a piconet shall always be in the superframe in which a wake beacon was transmitted by the PNC.[NOTE: If beacon transmission time is defined (BTT), this can be defined as WBTT which makes the text flow naturally since wake beacon referred here is mostly to do with the time of its transmission than its contents] – Recommend accept in principle – the suggested resolution does not match the intent of the draft. Provide clarification in a single location in 8.13 to note the idea of wake beacons relationship to PS set.

> Reject, "The wake beacons are defined in 8.6.2 (for system wake beacons) and in 8.13 (for all of the wake beacons and in 8.13.2.1 (for SPS wake beacons). A wake beacon is when a DEV wakes up and otherwise is a normal beacon. It does not contain any special fields that are not present in any other beacon. The concept of the wake beacon is well defined for all power save modes and is used consistently in the draft."

CID 62 (Gubbi, TR) Same as comment 509 in LB19 (Applicable for 8.13.2 also)PS status bit map has an issue and that is, let's say DEV-A and DEV-B aremembers of the same piconet managed by a PNC. If DEV-A sees the PS-status-bit corresponding to DEV-B as set in the beacon from PNC (meaning DEV-Bis in power save mode), but in the same superframe receives a frame (directed or not) from DEV-B, can DEV-A assume that the DEV-B is in AWAKEstate for that superframe? I think that should be allowed. it helps certainBC/MC traffic transactionsSuggested Remedy:1.If a DEV in in PSPS (SPS) mode in a superframe, but transmits a frame theDEV shall consider itself in AWAKE state and hence may enter SLEEPstate only after another succesful transaction of power-save-commands(s)with PNC.AND2. The DEV shall enter SLEEP state only at the start of superframefollowing the succesful transaction of power-save-commands(s) with PNC.Response:ACCEPT IN PRINCIPLE. 1. A DEV in PSPS keeps it's GTS and may transmit in them. This does not imply that the DEV wishes to change power save mode. 2. It is specified in 13.1 that a DEV may enter the SLEEP state only after having received an ACK from PNC on a PS mode change command with the PS Mode set to PSPS.Commentor's response (LB22) The comment exposes an ambiguity in the interpretation of PS-status bits and frame transmissions by a PSPS DEV as read in the draft (D11). But the resolution is just an explantory to the commentor with no clarification in the draft. Hence the ambiguity in the draft is still left remaining. -- 1.If a DEV in in PSPS (SPS) mode in a superframe, but transmits a frame the DEV shall consider itself in AWAKE state and hence may enter SLEEP state only after another succesful transaction of power-save-commands(s)with PNC. AND 2. The DEV shall enter SLEEP state only at the start of superframefollowing the succesful transaction of power-save-commands(s) with PNC. – Suggest reject The text seems to request the operation similar to APS where the DEV is required to request PS repeatedly. Is it a misunderstanding or a preference of operation?

> Reject: “It is clear in the text that AWAKE and SLEEP states are not the same as a power save mode. A DEV will be in AWAKE and SLEEP states when it is in a power save mode or even when it it ACTIVE. The draft clearly states this on page 214, line 54 ‘Regardless of the power save mode, a DEV is allowed to go to the SLEEP state during a CTA where it is neither the source or the destination. A DEV is also allowed to switch to the AWAKE state during any time when it is in a power save mode.’ Thus, the second sentence clearly states that a DEV may be AWAKE for some period of time without changing its power save mode. Since AWAKE means either transmitting or receiving, a DEV is allowed to send frames without changing its power save mode. This is an intended feature of 802.15.3’s power save modes that is an different from the 802.11 power save modes.”

CID 64 (Gubbi, TR) Change of GTS into CTA from D11 to D14 in clauses 5, 7 & 8:AT many places in clause-8, this has caused lot of confusion.For example pp-188, ln-17:18 where the first reader can easily confuse this with PNC listing the CTA information in the beacon as opposed to the GTS allocation in that superframe. To a vetern 802.15.3-WPANer this may seem same, but they are not. CTA is only a way of providing a GTS, there may be other ways in the future. change back all the GTS as they were in D11 in Clause 7 and 8. -- Revert back to the use of GTS when referring to time slot in super frame and CTA being limited to the component present in the beacon that is used to allocate a GTS to a DEV. Suggest accept in principle – Review draft and edit cases of CTA that are used without clarification of CTA IE vs CTA in CFP.

> Reject, “The name of an element in the standard is editorial decision, not technical one. A CTA is time allocated during the superframe. A CTA block is an element in an IE that tells a DEV when the CTA is allocated, the stream index, source DEVID and destination DEVID. A collection of CTA blocks is called a CTA IE that is put into the beacon. Thus the component in the beacon is either the CTA IE or the CTA block, but never the CTA. The technical editor is considering if a change to the name for the time allocation is appropriate, but any such change is editorial and not technical.”

CID 67 (Gubbi, TR) Lines 53-54 on pp-178 with lines 1-3 on pp-179 create an unnecessary special case for starting backoff algorithm at the start of CAP. The save is not worth the special case at the lowest level of MAC where Backoff algo is run. Added to that, applicability of this special case gets narrowed by another level by the probability of not-correctly-receiving the beacon and/or the last extended beacon by a DEV. Although this specail case has a "may" in it and hence does not enforce its applicability, it is worth the space in the standard given the above reasoning. -- Change "SIFS" to "BIFS" in Lines 53-54 on pp-178 and lines 1-3 on pp-179 Suggest table for group.

> Reject “If the DEV does not correctly receive the beacon, it cannot use the CAP anyway. If it correctly receives the beacon, it knows if there are extended beacons and it knows when the beacon eneded. If it is too complex for the DEV to implement this special case, it doesn’t have to do it. However, if the DEV can use this, it should be allowed to.”

CID 68 (Gubbi, TR) Table-120:Definition of MIFS and BIFS: Since MIFS is less than SIFS, make them same as SIFS. The channel time saving by the use of MIFS is very little given the probability of its use, but this is another unnecessary IFS that the MAC has to deal with and it is not optional. Making MIFS same as SIFS adds to uniformity at the lowest level of MAC. If the committee is so bent on saving channel time, please explore putting back the chaining of commands and similar options where the saving is huge and not just a few (at most 10+) microseconds. -- Change MIFS to SIFS in the draft Suggest reject – The Intent of MIFS is reduce overhead with a single CTA with multiple frames that to not entail a transmit/receive switch. The benefit with the 2.4GHz PHY of the draft is nominal but with increased data rates of alt-PHYs the overhead becomes pronounced.

> Reject “While the benefit with the 2.4GHz PHY of the draft is nominal, it is still about 5% at the highest data rate. With increased data rates of alt-PHYs the overhead becomes pronounced and is necessary to realize the promise of higher throughput. While chaining commands could save some overhead, commands are sent very infrequently while the vast majority of the traffic in the piconet is data. Thus, reducing the overhead for data is much more important than reducing the overhead for

commands. Currently, the draft defines four IFS, all of which are based on the characteristics of a PHY. The MIFS relates directly to a PHY's ability to send or receive multiple frame when it does not have to switch between sending or receiving. Thus it makes sense to keep this as a separate parameter."

CID 69 (Gubbi, TR) Table-120: PLEASE summarise all PHY parameters (aCCADetectTime, aPHYSIFSTime etc.) in a table at one place instead of spreading them all around the PHY clause (something on the lines of Table-64, for MAC, is very desirable from implementors' view). Although Table-65 provides a list of PHY parameters in a table, the values have to be searched through in those referred clauses, which can easily be avoided. -- Create a summary table of PHY parameters instead of spreading them all over the PHY clause(s). Suggest accept in principle – There is already a single table in d14 for interframe spacings. Text to provide a single location for all parameters should be provided by clause 11 editor.

Accept in principle "The location of the parameters in the draft is an editorial decision, not a technical decision (and this location did not change from draft D11 to D14). However, the technical editor will consider putting all of the parameters into a single table at the end of the PHY clause."

CID 70 (Gubbi, TR) 8.13 - Table-66. The cell corresponding to "Hibernate in wake superframe" column and "Beacon" row contradicts the text on pp-220, lines36-41 where the hibernating DEVs are allowed the liberty of sleeping through "any" beacon until they themselves change over to ACTIVE state (and it should be within ATP to retain the membership of Piconet) -- Change the referred entry from "AWAKE" to "May sleep" Recommend accept in principle – a note should be added for the table 63 cell regarding HIBERNATE wake superframe. Although the text is correct, distinguish the HIBERNATE from other PS wake superframes.

Accept in principle "The text above the table indicates that the HIBERNATE DEV only wakes up when it wants to listen to the beacon and that is called its wake beacon. Therefore, the table is correct since a HIBERNATE DEV's wake superframe is defined as any superframe where it listens to the beacon. The relevant text fro 8.13 is 'The wake beacon for a DEV in HIBERNATE mode occurs at times determined by the DEV and is unknown to the PNC and other DEVs in the piconet. Unlike the SPS and PSPS wake beacons, the wake beacon of the DEV in HIBERNATE mode is not periodic and is only guaranteed to happen once per ATP period for that DEV.'"

CID 71 (Gubbi, TR) 8.14 - See CID-446, 477, 478 and 479 in LB19 Use of Vendor specific command is the answer to the issue that is intended to be solved through this app-specific IE. -- Remove this subclause and references to ASIE from the draft. Recommend reject – This may not be resolvable.

Reject, "The ASIE is intended to be included in the beacon as an announcement. A command cannot be sent in the beacon so the vendor specific command would not be applicable to solve this need. The ASIE was put in to enable new functionality for some DEVs without breaking compatibility for all DEVs. Since the TG cannot possibly forsee all uses that might be required, this is left to be defined by the vendors."

CID 216 (Shvodian, TR) There should not be an MLME that is sent every beacon. Get rid of this MLME.

Accept in principle, "Change 'upon reception of a beacon containing an ASIE containing its DEVID.' to be 'upon reception of a beacon containing an ASIE containing its DEVID, as described in {xref 8.14}.'"

CID 78 (Heberling, TR) - [CTA] Range of AvailableNumTUs is wrong. CTR response carries only one octet for this parameter, see 7.5.5.2/KO. Valid range for AvailableNumTUs is 0-255.

Accept, “The requirements for this field are set out in clause 7.5.5.2, so the range in clause 6 should match. Change as indicated. After discussion, the commenter agreed that this comment is editorial and not technical.

CID 79 (Heberling, TR) - [CTA/Asynch] AvailableNumTUs never returned for asynchronous requests (neither is the primitive!)/KO. Change description to: "The number of TUs available to the requesting DEV for allocation"

Accept, “The description does not match the usage that is clearly defined in clause 8. Change as indicated in the comment. After discussion, the commenter agreed that this comment is editorial and not technical.”

CID 80 (Heberling, TR) - [CTA/Term] The source is not informed about termination via the NULL CTA, it's informed via the CTR response from the PNC. Ref Fig 120, page 193 and 8.3.4 page 176 line 16-17./KO Change sentence to: This primitive is used to inform the SrcDEV DME that the MLME has received a channel time response command indicating that the channel time that was previously allocated has been terminated by the PNC or the TrgtDEV. It may also be used to indicate to the TrgtDEV DME that the MLME has seen a null-CTA in the beacon with its DEVID, BcstId or McstID as the destination.

Accept in principle, “Change ‘This primitive is used to inform the source DEV that channel time that was previously allocated is no longer present in the most recently received beacon.’ to be ‘This primitive is used to inform the DEV DME that a stream has been terminated.’ After discussion, the commenter agreed that this comment is editorial and not technical.”

CID 218 (Shvodian, TR) - If conformant DEVs are not allowed to send reserved values in fields, how does a DEV receive a reserved value? Unsupported version? Clarify by changing the sentence to: "Reserved values in non-reserved fields shall not be transmitted by conformant DEVs. However, a DEV may receive frames of a different protocol version with values that it considers to be reserved values in non-reserved fields.

Withdrawn, 11 November, 2002.

CID 225 (Shvodian, TR) - What does "may be decoded" mean? Change to "may be ignored"

Accept in principle, “Change ‘may be decoded’ to be ‘may be ignored’ in two tables, 47 and 48 since the terms are technically equivalent. However, this needs to be changed for consistency in the draft. After discussion, the commenter agreed that this comment is editorial and not technical.”

CID 240 (Shvodian, TR) - WHy is there a MaxRetransmissionLimit? Does that mean that a DEV that tries to associate and gets no response must self destruct? Get rid of maximum retransmission limit. That should be left to the implementer.

Accept in principle, “The retry limit is defined in 8.8.4. The only location this parameter is referenced is in 8.4.3, page 179, line 22 which has to do with the backoff procedure and not the retry limit. Consequently, to clean up the organization, delete the sentence ‘The DEV ... is reported through the MAC-SAP interface.’ and delete the parameter in table 64 since the parameter is not used in the draft. After discussion, the commenter agreed that this comment is editorial and not technical.”

CID 232 (Shvodian, TR) - What about unsupported sub-rate? Add "or unsupported sub rated"

REJECT. This error code was not changed from D11 to D14. The commenter is encouraged to resubmit this comment in sponsor ballot.
Suggest

Recessed at 10:06 pm HAST.

1.1.3 Working list of comments

216 - Suggest reject or withdraw.

186 - Suggest reject or withdraw.

230 - Editorial, add clarification - Dan Bailey to write

218 - Editorial, possibly add clarification.

225 - Editorial, possibly accept.

140 - Suggest reject or withdraw.

232 - Editorial, add clarification. KO to research.

86 - Suggest reject or withdraw

87 - Suggest reject or withdraw

238 - Fix if possible? Old comment?

92 - Editorial, move text around, add clarification in shutdown and handover that the beacon announcements are done as indicated in 8.6.4.

180 - Editorial, delete the sentence, it is handled by 8.6.4.

93 - Editorial changes: 20

21 - Accept in principle, Add optional ACL handover block to new PNC handover. Push on fixing the .ind

97 - Suggest reject or withdraw, probably fragment probe command?

192 - Is this implied already and therefore needs to be clarified here.

98 - Editorial, delete redundant text.

180 - Editorial, text no longer applies in this draft.

191 - Suggest reject or withdraw.

100 - Editorial, delete redundant sentence, timeouts for MAC-ISOCH-DATA are already described in 6.6.5.1

236 - Editorial, changed as indicated in CID 236.

101 - Suggest reject or withdraw

103 - Suggest reject or withdraw

106 - Editorial, clarify by saying that this for all streams.

181 - Editorial, change names, value is the same.

180 - Withdraw?

162 - Editorial, add clarification that the PNC is required to scan at least the new channel, not just any channel.

110 - Editorial, clause 7 says that the value shall be set to CHANNEL, so we should mention it here as well.

182 - Editorial, change names, value is the same. The count should always include the first one as it is stated elsewhere in the draft.

207 - Suggest reject or withdraw

165 - Suggest reject or withdraw

112 - Withdraw.

111 - Change sentence to “The valid range for requested system wake beacons is defined in {xref 7.5.7.2}.” Also add an xref to the appropriate place for SPS.

170 - Editorial, clarify the meaning of the sentence.

239 - Suggest reject or withdraw

241 - Editorial, is it possible to add clarifying text?

18 - Change xref to indicate the table to match the text in the PICS clause.

126 - Editorial accept, name change to match usage

129 - Editorial accept, name change to match usage.

7 - Editorial, change field length to match.

MCTA

190 - Suggest reject or withdraw

189 - Suggest reject or withdraw

CWB

84 - Suggest reject or withdraw, possibly withdraw?

204 - Suggest reject or withdraw

205 - Suggest reject or withdraw

206 - Suggest reject or withdraw

136 - Suggest reject or withdraw

139 - Suggest reject or withdraw

116 - Suggest reject or withdraw

172 - Suggest reject or withdraw.

175 - Suggest reject or withdraw.

119 - Suggest reject or withdraw

193 - Suggest reject or withdraw

89 - Suggest reject or withdraw? Or can we add a clarification as to how to set this.

177 - Suggest reject or withdraw.

208 - Suggest reject or withdraw.

117 - Editorial. Add rows to the PICS to reflect the text in clause 8.

PM/Wakeup

183 - Suggest reject or withdraw

184 - Suggest reject or withdraw

185 - Suggest reject or withdraw

115 - Suggest reject or withdraw

Frag

202 - Editorial, Add text that says that this it is maximum or less and that the source is allowed to choose the fragment size

137 - Resolve as in CID 202

208 - Resolve as in CID 202

203 - Resolve as in CID 202

154 - Resolve as in CID 202

PNC/Scan

118 - Suggest reject or withdraw

179 - Suggest reject or withdraw.

178 - Suggest reject or withdraw.

2. Editorial CIDs

CID 75, 86 (Heberling, E) - Parameter "ACLInfoSet" is called "ACL Record" in 7.5.4.4/KO. pick one “Replace ‘ACL record’ in 7.5.4.4 with ‘ACLInfoSet’”

CID 222 (Shvodian, E) - Change payload to Secure Payload Change payload to Secure Payload. Also show that everything in the figure but the FCS is part of the MAC payload. Accept.

CID 12 (Barr, E) - Verification info length(=L2) does not seem to be required since the length of the ACL record field will determine length of the Verification info. Remove Verification info length if not really required. Suggest reject.

CID 197 (Rasor, E) - The current text reads: "The authentication and challenge commands are designed to be used with security turned off." Is this an accurate statement? Withdrawn? Otherwise, Accept in principle: “The statement is accurate, the security for the authentication procedure comes from the protocol that is used not via an integrity code on any of the individual frames. The protocol calculates an integrity code for the entire authentication process which verifies the identity of the participants in the exchange.”

CID 20 (Barr, E) - Market suitability criteria seems to be incomplete. Change "The protocols have been reviewed by" to "The protocols have been reviewed by (whomever reviewed these protocols)" Accept in principle. “Delete the dashed item. ‘Market suitability: The protocols have been reviewed by to ensure that they satisfy the requirements of 802.15.3 applications.’”

3. Status summary

3.1 Status at opening of Kauai meeting

.

Table 1—Ballot resolution at opening of Kauai meeting

Type	LB22
T (technical)	34
TR (Technical required)	90
T and TR	124
E (editorial)	121
Total	245

3.2 Status at closing in Kauai

.

Table 2—Ballot resolution as of close of Kauai meeting

Type	LB22	Unresolved as of 15 November, 2002
T (technical)	34	
TR (Technical required)	90	
T and TR	124	
E (editorial)	121	
Total	245	