IEEE P802.15
Wireless Personal Area Networks

Project	IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)	
Title	**TG3 LB12 Comment resolution working document**	
Date Submitted	[11 February, 2002]	
Source	[James P. K. Gilb] [Appairent Technologies] [9921 Carmel Mountain Rd. #247, San Diego, CA 92129]	Voice: [858-538-3903] Fax: [858-538-3903] E-mail: [gilb@ieee.org]
Re:	[]	
Abstract	[This document is an additional record of comment resolution of LB12.]	
Purpose	[To provide a record of comment resolution, particularly for comments that are resolved based on the resolution of prior comments.]	
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

a) Coexistence - Response in 1728, “The proposed informative Annex (00000r0P802-15-3-Annex_Coexistence.pdf) has a description of the coexistence methods that are available in the draft. Also see 02/041r2 for a presentation and additional text on this issue. For 802.15.4 compatibility see subclause 6.9 in 00000D13P802-15-4__Draft_Standard.pdf. TG2 has been consulted and they will help with analysis.”
Also resolved: 1850 (Dydyk, T), 1765 (Callaway, E)

b) Security - Response in 781, “The 802.15.3 committee is going to issue a CFP, evaluate and choose a mandatory cipher suite for DEVs that implement security.”
Also resolved: 1845 (Dydyk, T), 894 (Roberts, TR), 904 (Roberts, TR), 1015 (Roberts, TR), 1233 (Roberts, T), 1293 (Roberts, TR), 1725 (Rofheart, TR), 1682 (Shvodian, TR, Add response: “Since there are no shalls, shoulds or mays, this section is informative and needs to be moved to the informative Annex. The commenter is invited and encouraged to provide additional text that describes other methods that provide the function of the certificate authority.”), 1689 (Shvodian, TR), 1767 (Y-C Chen, TR), 1741 (Maa, TR), 1785 (Liu, TR), 802 (Kinney, T), 1750, (H-K Chen, TR), 727 (Herold, T)

c) TBD’s - For page 107, response in 296 “Bit has been removed.”, for page 133, response in 294 “Security is applicable on a piconet basis, not a stream-by-stream basis. Delete the sentence and the associated bits in figure 76 (b4-b6). Reassign the bits as reserved and move the other bits foward so that the reserved bits are contiguous.”, for page 175, response in 1744 “Clause 9 has been deleted. TBD has been removed.”
Also resolved: 1674 (Shvodian, T), 1097 (Roberts, TR), 1119 (Schrader, T), 52 (Bain, T), 1846 (Dydyk, T)

d) Power managment -

2. Comment resolution order

2.1 February 5, 2002

768 (Huckabee, T): 1 second connect time, suggest accept in principle: “1 second connect time is a goal, not a requirement. Clause 5 is a qualitiative overview that does not place any requirments on devices. The authentication time required depends on the security suite that is selected. The security suite selection criteria indicates that a total connect time including authentication of less than one second is desired.”

Accept.

1663 (Shvodian, T): suggest accept, 0 length fields should be OK.

Accept.

1517 (Shvodian, TR): Add security parameters IE to association repsonse. Suggest accept.

Accept, OID goes into the association response rather than the beacon.

1513 (Shvovdian, TR): Add error code for security required to association. Suggest accept.

Accept.

308 (Gilb, T), 964 (Roberts, TR): No separate security information in data frame anymore. Suggest accept 308, accept in principle 964.

Accept as indicated above.

894 (TR), 904 (TR), 1015 (TR), 1233 (T), 1725 (TR), 1682 (TR), 1689 (TR): Various security related items. Suggest accept in principle with the response for other security suite comments “The 802.15.3 committee is going to issue a CFP, evaluate and choose a mandatory cipher suite for DEVs that implement security.”

894 - will accept if the following is appended to the response in 781
In clause 6.3.6.2.2, reference is made to the security subclauses that present the details on how the challenge commands are used.
904 - will accept if the following is appended to the response in 781
In clause 6.3.8.1.1, reference is made to the security subclauses that present the details on how the PNC does the security manager function.
1015 - will accept if the following is appended to the response in 781
In clause 7.5.3, reference is made to the security subclauses that present the details on how the PNC does the security manager function.
1233 - accept as per the response in 781
1293 - accept as per the response in 781
1725 - accept as per the response in 781
1097 - accept as per the response in part 1.c of doc 02/075r0

Accepted as indicated above.

2.2 February 7, 2002

547 (Gubbi, TR), 892, 895, 897, 1037, 1125, 1231, 1234, 1239, 1244, 1246, 1296 (Roberts, TR), 1247 (Roberts, T), 1682 (Shvodian, TR), 1689 (Shvodian, TR): Various security related items. Suggest accept in principle with the response for other security suite comments “The 802.15.3 committee is going to issue a CFP, evaluate and choose a mandatory cipher suite for DEVs that implement security.” For 1682, suggest adding “Since there are no shalls, shoulds or mays, this section is informative and needs to be moved to the informative Annex. The commenter is invited and encouraged to provide additional text that describes other methods that provide the function of the certificate authority.”

Email from Rick Roberts:

LB12 Comment Resolutions from Rick Roberts. All acceptances are based upon text presented in doc 02/075r1.

1. On the comments that deal with security ... I accept the technical editors suggested resolution for the following items

892, 895, 897, 1037, 1231, 1239, 1246, 1296 and 1247

2. I reject the editors suggested resolution for the following items

1125, 1234, 1244

Both 1125 and 1234 are comments on security policy during a PNC handover. Basically the question is does the authentication list transfer during a PNC handover, or do all DEV's have to re-authenticate with the new PNC. In my mind, this is a security policy issue and not a security suite issue (unless someone can convince me that they are one in the same). I lack technical expertise in this area otherwise I would generate text. I prefer that the certificates transfer (old PNC vouches for all authenticated DEVs) but I understand that some of the security experts believe this is a bad idea. So I am confused and want to defer to the experts.

On item 1244, the question is where is the list of authenticated DEV's maintained. It seems it should be in the PSM which is co-located with the PNC. If this is true then a simple resolution would be to add the following text.

"In all scenarios, the security manager, which is co-located with the PNC, shall update the list of authenticated piconet DEVs to exclude the disassociating DEV."

3. For comment 1131 ... I accept the suggested resolution as proposed by the technical editor.

Committee

Accept, as above 547, 892, 895, 897, 1037, 1231, 1239, 1246, 1296, 1247, 1682, 1689 (and 1694)
Skip 1125, 1234, 1244

1299 (Shvodian, TR): Do we need de-authenticate? Why not just disassociate? Suggest accept, “Delete the deauthentication command, frame formats and MLME’s.”

Accept

1127 (Roberts, TR): When is PNC handover required? Suggest accept in principle. The intention, lost in the words, is that handover always occurs if the Des-Mode bit is set and may occur otherwise. Either change last sentence to read: “Therefore, if re-authentication is not desirable and the PNC Des-Mode bit is not set in the new DEV, a PNC running security in the piconet should not perform PNC handover unless it is leaving the piconet.” or simply delete the last sentence.

Accept

1574 (Shvodian, TR): The PNC should wait until after the authentication if authentication is required for the piconet before broadcasting the Dev-Info (now PNC-Info) table. Suggest accept.

Accept

1131 (Roberts, TR): Authentication sub-clause in Clause 8 is considered silly, please delete. Suggest accept.

Accept

1832 (Rasor, TR), 1803 (Rasor, TR): PSM and PNC as separate entities: Suggest reject, reason as follows: “The task group previously considered this option and instead chose to co-locate the PSM and PNC. The main reason for requiring the PNC to also be the PSM is to prevent having two points of failure in the piconet. If the PSM and PNC reside in separate DEVs, then all of the DEVs in the piconet need to be able to hear both DEVs rather than just the PNC. With the current architecture, the piconet is defined as all devices that are able to hear the PNC. Another reason for co-locating the two functions is that it reduces the communications overhead and complexity of the security suite.”

Skip

1837 (Rasor, TR): Security and communication with child and neighbor piconets. Suggest accept in principle. “The draft already states (see 8.2.5 and 8.2.6) that the child and neighbor piconets are autonomous and do not share authentication or security. Add a note to the end of the first paragraph in 10.2 that says ‘These requirements apply only to the piconet and are not transferred to child or neighber piconets, which have distinct security requirements.’”

Skip

1798 (Rasor, TR): Delete reference to IEEE MAC address. This is a re-definition of the Device ID (now Device Address), so deleting the reference to the IEEE MAC address is actually a good thing, suggest accept.

Accept

1679 (Shvodian, T): Clean up text in security requirements to reflect choices: Suggest accept.

Accept

1805 (Rasor, TR): Editorial change to the introduction text to include the mention of roles of the DEVs. Recommend accept (doesn't change implementation anyway).

Accept

1681 (Shvodian, TR): Allow for keys to be entered by the user. Suggest accept deletion of sentence and parenthetical comment.

Accept

1810 (Rasor, TR), 1811 (Rasor, TR): The PNC is PSM connection is listed twice, it can be removed from the first reference. Suggest accept in principle, "Delete the sentence in 10.3.2.1, line 25, and change "assumes" to be "shall assume" in 10.3.2.2, lines 15 and 16 (two places total)."

Accept

1817 (Rasor, TR): Specify what happens when group structure and role change simultaneously. Suggest accept in principle. "Add the following sentence after the enumerated points in 10.3.3.1 'Simultaneous changes of the group structure and of the role are conceptually thought of as taking place sequentially."

Skip

1819 (Rasor, TR): Add new security event for handover. Suggest accept in principle. "Add an enumeration item as "2) PNC promotion. This refers to a PNC-capable DEV assuming the role of PNC.'"

Accept

1821 (Rasor, TR), 1829 (Rasor, TR): Should changing the PNC require re-authentication (note that this does change the PSM): Suggest accept in principle, reason "The requirement for re-authentication when the PNC handover occurs will be specified by the security suite implementation. The 802.15.3 committee is going to issue a CFP, evaluate and choose a mandatory security suite for DEVs that implement security. Changes to the current description will be made when the security suite is selected."

Skip

1692 (Shvodian, TR): Make the cipher suite (now security suite) requirements normative. Suggest accept in principle with "The 802.15.3 committee is going to issue a CFP, evaluate and choose a mandatory security suite for DEVs that implement security. The description of the requirements for the security suite would be listed in an annex."

Accept

291 (Gifford, T): Review the use of shall/should/may/can/will/must throughout the document to be sure they are used in accordance with IEEE's style. Suggest accept, reason "The editor (and others) have closely

reviewed the document for proper usage. The word must occurs only in the copyright information on the first page, the word can does not appear at all. The technical editor has been trully annoying in enforcing the no must or can rule."

Accept

583, 588, 590 (Heberling, T): Reason code for disassociation is unnecessary: Suggest reject, reason "The committee reviewed the reason codes for the disassociate command in Dallas and felt that there was still useful information that could be passed using this reason code. Therefore, the reason code needs to stay in the MLME-DISASSOCIATE.xxx commands as well."

Withdrawn

2.3 Tuesday, 12 February, 2002

455 (Gilb, T): Should have been closed with 74, now closed with 74's resolution.

123 (DuVal, T) - Why is the neighbor piconet needed? Suggest accept in principle, add text as described in documet 02/060r1 for clause 5.3.7, 5.3.8.

1664, 1665, 1667 (Shvodian, T): Allow 0 length fields in MLME. Same comment that we accepted for 1663 on 5 Feb, 2002, suggest accept.

458 (Gilb, T): Add reason code. Closed this issue with 907 (Roberts, TR) and 1419 (Shvodian, TR), but we have different reason codes and no description. Suggest close all with following:.

Table 1—MLME-REQUEST-KEY primitive parameters

Name	Type	Valid Range	Description
ReasonCode	Enumeration	SUCCESS, FAILURE, TIMEOUT	The result of the key request command.

460 (Gilb, T): No reason code for MLME-DISTRIBUTE-KEY. Closed with 913 (Roberts, TR) and 1421 (Shvodian, TR), suggest accept as in 1421, result is below:

Table 2—MLME-DISTRIBUTE-KEY primitive parameters

Name	Type	Valid Range	Description
ReasonCode	Enumeration	SUCCESS, TIMEOUT	The result of the key distribution attempt.

463, 464 (Gilb, T): Add reason code for deauthenticate: Suggest accept in principle, reason "De-authenticate command has been removed, so reason code is not needed."

902 (Roberts, TR): Add two acronyms: Suggest, add "DEK - data encryption key and DIK - data integrity key. SEED will be changed to lower case, 'seed' and a definition added 'seed: initial small key stream used as input by an algorithm to generate a (usually bigger) key stream."

900 (Roberts, TR): What are KEK, DEK, DIK and SEED? Suggest, accept in principle, "Add 'KEK - key encryption key' to the acronyms clause. The other acronyms will be defined as in the resolution for comment

902. The items will be defined with the proposals for the security suite. The 802.15.3 committee is going to issue a CFP, evaluate and choose a mandatory cipher suite for DEVs that implement security."

905, 906, 909 (Roberts, TR): Suggest accept in principle, "The 802.15.3 committee is going to issue a CFP, evaluate and choose a mandatory cipher suite for DEVs that implement security."

459 (Gilb, T): Device ID description is incorrect (cut 'n paste error) in Table 16, page 42. Suggest accept.

461 (Gilb, T): Cut 'n paste error, there is no MLME-DISTRIBUTE-KEY.response command. The response is the ACK, not a separate command. Suggest accept.

462 (Gilb, T): Fix de-authenticate table. Suggest accept in principle: reason "De-authenticate command has been removed, so reason code is not needed."

465 (Gilb, T): Already accepted in 592, 593 (Heberling, T), suggest accept.

595 (Heberling, T): Add that the DEV sends a disassociation request to the PNC. Suggest accept in principle, "The DEV MLME, upon receiving this primitive, sends a disassociation request command frame to the PNC, if it is currently associated, sets the MAC to its initial conditions and clears all of its internal variables to their default values."

596, 597, 598 (Heberling, T): We don't need MLME-RESET.confirm, and its description is incomplete. Suggest accept, "Delete sub-clause as specified in comment 598."

293 (Gilb, T): The capability information element does not need to be passed in the primitive, it is derived form the PIB. Suggest accept.

466 (Gilb, T) The primitive parameters for MLME-STREAM-CTA.indication are not defined, solution is to copy them from table 25 into table for this sub-clause. Suggest accept.

467 (Gilb, T): Missing reason code. Suggest accept, would look like below:

Table 3—MLME-TERMINATE-STREAM primitive parameters

Name	Type	Valid Range	Description
ReasonCode	Enumeration	SUCCESS, TIMEOUT	Indicates the result of the stream termination command.

468 (Gilb, T): The RequestorDEVAddress is missing a definition. Also add TIMEOUT to the valid range of the reason code. Suggest accept.

Table 4—MLME-CHANNEL-STATUS primitive parameters

Name	Type	Valid Range	Description
RequestorDEVAddress	MAC address	Any valid MAC address	The MAC address of the DEV which is requesting the channel status.

607, 610 (Heberling, T), 470 (Gilb, T): Don't need ChannelIndex for this command, everyone is on the same channel. Suggest accept.

469 (Gilb, T): Change DestinationDEVAddress to RequestorDEVAddress to match the definition in table 28. Suggest accept.

616 (Heberling, T): Change from ACK_TIMEOUT to RESPONSE_TIMEOUT. Suggest accept in principle "Make change as indicated and add RESPONSE_TIMEOUT to the valid range of the ReasonCode in Table 28."

617 (Heberling, T): Add a response timer to the MSC. Suggest accept.

619 (Heberling, T): Add MLME-CHANNEL-STATUS and MLME-CREATE-REPEATER message sequence chart clause and diagram just after the last clause of the MLME-CREATE-REPEATER.confirm primitive. Text and diagram are in clause 6.3.1.12 of doc 01/410r1. Suggest accept.

621 (Heberling, T): Change NewChannelIndex data type from octet to integer on page 64. Suggest accept.

622 (Heberling, T): Change timeout type to duration on page 64. Suggest accept.

624 (Heberling, T): Add MLME-PNC-HANDOVER.request, indication, response and confirm clauses into the space just before current D09 clause 6.3.18. Based on doc 01/410r1? Suggest accept if 01/410r1 has been posted with the new MLME.

623 (Heberling, T): Add MLME-CHANNEL-STATUS, MLME-REMOTE-SCAN, and MLME-CHANGE-CHANNEL MSCs to the MLME-SAP interface clause from 01/410r0. Suggest accept if 01/410r1 has been posted with the MSCs and with caveat that the remote scan has been updated with the changes agreed to in Dallas (i.e. removing the channel change from the MSC).

629, 635, 637 (Heberling, T): Change DevInfoSet to PNCInfoSet. Suggest accept in principle, "Change DevInfoSet to be DEVCTRSet."

472 (Gilb, T), 1670 (Singer via Shvodian, T): DEV does not need to be authenticated to use probe command so delete the word "authenticated" from line 19, 20, 36 and 37 all on page 66 (i.e. every occurance in 6.3.18.1). Suggest accept. For 1670, accept in principle, add "The command is used to request information about the current channel time requests from the PNC to enable faster PNC handover. However, authentication is not necessarily required, so the word "authenticated" has been deleted from this sub-clause."

1440 (Shvodian, T): Naming collision between probe and DEV-info commands. Suggest accept in principle, "The MLME-PROBE-PNC primitives (now renamed PNC Info primitives) are used to issue DEV Info commands (now renamed PNC Info commands.) The MLME-DEV-INFO primitives (now MLME-PROBE) are used to issue probe commands."

471 (Gilb, T): Add TIMEOUT to ReasonCode valid range. Suggest accept in principle, "Add RESPONSE_TIMEOUT to the valid range of the ReasonCode in Table 30 (see comment 639)."

639 (Heberling, T): Change from ACK_TIMEOUT to RESPONSE_TIMEOUT. Suggest accept in principle "Make change as indicated and add RESPONSE_TIMEOUT to the valid range of the ReasonCode in Table 30."

644 (Heberling, T), 473(Gilb, T): Type and valid range wrong for reason code. Suggets accept 644, accept in principle 473, "Change the valid range to be SUCCESS, RESPONSE_TIMEOUT as indicated in comment 644."

474 (Gilb, T): The sentence "The ReasonCode ... for failure." does not belong here since it has been put into the table, so delete it. Suggest accept.

652 (Heberling, T): Change from ACK_TIMEOUT to RESPONSE_TIMEOUT on page 70, line 37. Suggest accept.

653 (Heberling, T): Add MLME-NEW-PNC information from doc 01/410r1. Suggest accept if 01/410r1 has been posted with the new MLMEs.

654 (Heberling, T): Add clause 6.3.1.34 MLME-DEV-INFO, MLME-PNC-HANDOVER, MLME-PROBE-PNC, and MLME-NEW-PNC message sequence chart from doc 01/410r1. Suggest accept if 01/410r1 has been posted with the new MLMEs.

1438 (Shvodian, T): Should the requestor or responder choose the window size for channel status. Specifying a window size in the request will potentially force a delay of that amount of time while the responding DEV gathers the statistics. Suggest reject, “Having the requesting DEV specify a window size will either introduce delay in the response of the channel status request command or would require every DEV to keep a detailed history rather than simply a running count. While there are reasons why the requesting DEV might wish to specify the measurement window, the committee feels that the corresponding delay or added complexity to every DEV would be too much.”

2.4 Thursday, 14 February, 2002

1817 (Rasor, TR): Specify what happens when group structure and role change simultaneously. Suggest accept in principle. “Add the following sentence after the enumerated points in 10.3.3.1 ‘Simultaneous changes of the group structure and of the role are conceptually thought of as taking place sequentially.”

1125, 1234, 1244 (Roberts, TR), 1821, 1829 (Rasor, TR): Should changing the PNC require re-authentication (note that this does change the PSM): Suggest ?

2.5 Later dates

Power management (TBD date, tagged PM in database)

857, 859 (Roberts, T) - mode definitions.

Channel time request clean up (tagged as CTR in database)

1429, 1434 (Shvodian, TR): Clean up CTR, suggested remedy in 02/076r0?

1425 (Shvodian, TR): 48 or 8 bit addresses in the MLMEs? Did we already decide this one?

3. Schuamburg ad-hoc, Feb. 25-27

3.1 New association response proposal

(Tagged Association Info in the database)

576, 662 (Heberling, TR), 661 (Heberling, T)