IEEE P802.15
Wireless Personal Area Networks

Project	IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)	
Title	**TG3 LB12 St. Louis comment resolution**	
Date Submitted	[8 July, 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 a record of comment resolutions for LB17.]	
Purpose	[To provide a record of the comment resolution for LB17.]	
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, Vancouver to Schaumburg

1.1 Tuesday, 16 July, 2002

909 (Bain, T) - Piconet Maximum transmit power is a beacon parameter that as suggested in the text (as a means of working with interference), may change during the duration of a piconet. It is not clear, how this parameter is adjusted after the initial configuration with MLME-START.request. Many of the operations regarding channels involve the DME so there should be a means to reflect a DME choice into the IE of 7.4.7. I recommend that we overload the existing MLME-PICONET-PARM-CHANGE.request and create a duplicate of the parameter PiconetMaxTxPower. Suggest accept in principle, "Add a new MAC PIB element to 6.5.1 as follows:"

Managed Object	Octets	Definition	Type
MACPIB_MaxTXPower	1	The maximum TX power allowed in certain times of the superframe as defined in 8.13.1.	Dynamic

826 (Bain, TR) - The text of 8.5.2.1 pg 181 line 40-43 on no guarantee of what delay will be between the time of request and a beacon indicating the time should also be placed in 8.5.1. Place the text mentioned above into 8.5.1 with a change that noting the change from async to isosync. Suggest accept.

3 (Heberling, TR) - A stream with del-ACK policy cannot be used with any other ACK-Request. Neither can the policy be changed, because enqueued frames with different ACK-Policy (del-ACK and other) will create unresolvable protocol conflicts. Consequently if del-ACK is declined by the destination, the stream must be terminated. 8.8.3, Insert line 9: Delayed Acknowledgement can only be used with isochronous data. Insert line 23, before "The destination DEV may change the max burst..." Upon reception of an imm-ACK frame after sending a data frame with the ACK request field set to del-ACK, the source DEV MAC shall: - issue a MLME_TERMINATE_STREAM.indication to DME - send a Channel Time Request frame to PNC with the terminate bit set to 1 and the desired CT to 0." Suggest accept in principle, "Change 'shall be used only for directed stream data frames where' to be 'shall be used only for directed stream data frames, i.e. isochronous connections, where' Add text to the section that says 'The source DEV may change the ACK policy in a stream from Dly-ACK to Imm-ACK or no ACK by sending a frame with the ACK policy set to one of those values. This has the effect of canceling the Dly-ACK policy and the souce shall use the Dly-ACK negotiaion procedure before restarting the Dly-ACK mechanism. The receiver shall no longer maintain the ACK status of any previous frames sent with the Dly-ACK policy set.'"

819 (Shvodian, TR) - CCA should not be used for retransmission. In a poor channel the sending DEV may not hear the other DEV. It needs to wait for an ACK time. 802.11 does not use CCA. It uses an ACK timeout. (p84 of 802.11 1999). Replace CCA with ACK time. Suggest accept, "Fix the text to indicate that the DEV waits for the length of time required for the appropriate ACK, either Dly-ACK or Imm-ACK."

340 (Heberling, TR) - The rules for association and authentication with PNC are inconsistent. < add text> In a piconet operating in security mode 0 or 1, an association shall also imply authentication. No authentication frame exchange shall be done with PNC in these modes. Suggest accept in principle, "A DEV will become a 'member of the piconet' or have 'membership in the piconet' when it is associated for mode 0 or completes authentication for mode 1, 2 or 3. Text will be added to specify this and the draft modified to use 'membership' instead of 'associated, and if required authenticated'. Note that the authentication process for mode 1 will be resolved as a part of another comment. If a null security suite is used, then the authentication process will be required. Otherwise, it will have the status of mode 0, i.e. that association is equivalent to authentication."

202, 204, 402 (Heberling, TR) - Services broadcast not standardized, thus not interoperable and must be removed from standard. Remove MLME_ASSOCIATE.request parameter DEVPiconetServicesIE. Suggest accept in principle, “Adding the vendor IE to the associate request and response commands as outlined in 02/276r0 will take care of problems with standardization. Since this information is needed to provide a fast response time, the DEVPiconetServicesIE will remain in the associate request command.”

109 (Heberling, TR) - No need to broadcast piconet information after association. Instead the newly associated DEV should ask for the information it desires. The PNC may still broadcast information at intervals of its own choice. If nothing has changed in the piconet, no broadcast is necessary. Delete first sentence "The PNC shall broadcast ... after a DEV associates" Delete "In addition" <Change from> The PNC shall send the piconet information for each of the associated DEVs at least once every aBroadcastDEVInfoDuration via a PNC information command. <to> The PNC may broadcast the piconet information for each of the associated DEVs when any change of association status has occured or at intervals of the PNCs own choice via a PNC information command. Suggest reject “A new DEV joining the piconet is unable to do anything until it finds out information about the other DEVs in the piconet. The information about the DEVs in the piconet is the first thing that the new DEV will likely require. It also allows other DEVs to update their own information in case they have missed the indication of a previous DEV joining or leaving the piconet. The broadcast of the DEV information table after association is unchanged since D09.”

372 (Heberling, TR) - This whole clause raises the question of why does the PNC info command get broadcast unsolicited? When a DEV associates, its Association IE info is broadcast via the beacon. If the Associating DEV needs the DEV association list from the PNC it can request directed frames from the PNC. There is no need to clog the medium with an unsolicited broadcast. Consequently, remove this clause. Please make the requested deletion. Suggest reject “A new DEV joining the piconet is unable to do anything until it finds out information about the other DEVs in the piconet. The information about the DEVs in the piconet is the first thing that the new DEV will likely require. It also allows other DEVs to update their own information in case they have missed the indication of a previous DEV joining or leaving the piconet. The broadcast of the DEV information table after association is unchanged since D09.”

105 (Heberling, TR) - Timeouts only works in the client in the vertical direction. A client cannot set a timeout for its server, less the entire distributed state machine in the scheduler is completely specified (RTOS theory). Delete the sentence: "The time difference between sending an ACK..." Suggest accept in principle, “The timeout is a requirement only for the PNC to enable fast join times for the network. However, the current sentence does not state that clearly. Change ‘The time difference between sending an ACK to an association request and sending an association response command meant for the same DEV shall not exceed aAssocRespConfirmTime.’ to be ‘The time difference between when the PNC sends an ACK to the association request command from a DEV and when it sends an association response command meant for the same DEV shall not exceed aAssocRespConfirmTime.’”

625 (Gilb, TR) - It is not likely but it is possible that this information element could be longer that 256 bytes long if enough devices associate/disassociate at the same time. Indicate that the PNC may use multiple DEV association IEs in the beacon too many DEVs are associating than will fit in the beacon. Suggest accept.

777 (Shvodian, TR) - DEV association IE does not belong in the beacon. There is no guarantee that the associating DEV will get the beacon anyway. The beacon is big enough as is. Other DEVs cannot talk to that DEV until it authenticates if it is a secure piconet anyway. The PNC info table is broadcast when the DEV associates (or authenticates in a secure piconet). If the DEV does not receive the PNC info table and has not MTS assigned to it, it will shall to associate again. Suggest accept.

920 (Bain, T) - It seems that information on what type of CAP/MTS used by piconet is not returned as part of a scan. Since MTS is optional in PICS a DEV may not support this and thus consider joining a different piconet. Add the CAP information from the channel timing IE to the MLME-SCAN.indicate primitive. Place as additional field in piconetdescriptionset in table 5. Suggest accept.

361 (Heberling, TR) - The current wakeup mechanisms are not sufficient to wake up a DEV when a major system change occurs. Examples are channel change, PNC handover, beacon duration or location change and PNID change. A method is needed to allow all APS and SPS devices to easily check if a system change is in progress. The intervals for such checks must be decided by PNC. See resolution [13] in 02276r0P802-15_TG3-commentsD10_KO.doc A system change bit is added to the mode field of the PNC synchronization IE. All DEVs are required to check this bit at minimum intervals. The bit is unrelated to any APS and SPS wakeup method. Suggest reject “There is no way to both guarantee that sleeping DEVs will see system change and make changes quickly. In fact it is not possible to to guarantee that DEVs that are ACTIVE will see the system change. The only way to guarantee that DEVs are aware of the change before it happens is to send directed frames to each DEV with Imm-ACK policy. When a system change happens and a DEV, for whatever reason, misses it, the DEV will begin to scan for its piconet. If it finds it before the ATP expires, it will re-join the piconet. If not, it will re-associate with the piconet when it finds it.”

418 (Heberling, TR) - Doc: 02/276r0 provides an argument for the persistence of the PiconetBSID. Consequently, change this sentence frag. from: "...PNID, BSID, and ChannelChangeTimeOut parameters." to "...PNID, and NmbrOfChangeBeacons parameters." Please make the indicated change. Suggest reject “The setting of the BSID is under use control and provides a human friendly manner to identify the piconet (i.e. a text string instead of list of hex numbers). Because of this, the user will want to be able to set this value from time to time without re-starting the entire piconet and re-program every DEV in thier net. However, since it is intended for use control, it is unlikely that it will change very often.”

210 (Gilb, TR) - The LQI gives better information if it is for the entire frame rather than for just the last CAZAC. In fact, the results for the CAZAC are not that good relative to checking the results of the TCM demodulator. Change "The LQI SNR shall be measured in the last CAZAC sequence of the PHY preamble, 11.4.2." to be "The LQI SNR shall be reported as the value for the received frame after the FCS for frames that have a frame length longer than 100 octets." Suggest accept in principle, “Change the the last two sentences in 11.6.7 from ‘The LQI SNR shall be measured ... via the PHY-RX-START.indication, 6.7.4.3.’ to read ‘The LQI SNR shall be measured during the TCM frame body and shall be reported after the last FCS symbol. This number shall be reported via the PHY-RX-END.indication, {xref 6.7.4.6.}.’ Change subclause 6.7.4.3 to remove LQI from the parameter list. Change subclause 6.7.4.6 to add LQI before the RXERROR parameter. Modify subclause 6.7.4.6.1 to include LQI in the list of parameters that are described, with the description ‘LQI is a 5 bit field that represents an SNR estimate from the receiver, {xref 11.6.7}.’”

508 (Gilb, TR) - The CCA only detects the CAZAC, but doesn't tell you to keep signalling busy until the end of the frame, up to the max frame length. Add text that says the CCA shall be maintained as busy until the end of the frame for which the inverted CAZAC was detected. Suggest accept.

512 (Gilb, T) - Incorrect sentence: "At the end of SLEEP state in APS mode, the DEV shall wakeup sufficient time before the expiration of the maximum sleep time in order to inform the PNC that it is in the ACTIVE mode."Change to "When transitioning from APS mode to ACTIVE mode, the DEV shall enter the AWAKE state sufficient time before the expiration of the maximum APS time in order to inform the PNC that it is in the ACTIVE mode." Suggest accept.

510 (Gilb, T) - When a dev is in APS mode, it can be in either the AWAKE or SLEEP state. Therefore, the following sentence is not correct: "The DEV shall be allowed to enter SLEEP state for a maximum sleep time duration indicated by the PNC in the APS sleep response command,..." Change to Replace with: "The DEV shall be allowed to enter APS mode for a maximum APS time duration indicated by the PNC in the APS response command,..." Suggest accept.

729 (Gilb, T) - Related to switching to ACTIVE mode, can't the DEV send ANY PDU to the PNC that requires an Imm-ACK, not just a command? Change to ..."the DEV shall send any directed frame, which may be an MSDU or MPDU with no payload, that requires"... Also change "wakeup" to "wake up" in this paragraph. Suggest accept.

313, 353 (Heberling, TR) - SPS set is not defined. Please define. Also, the structure of the DEVID list is not defined either. Please define. Please provide the requested definitions. Suggest accept “Add text that says ‘The SPS set field is defined in {xref 7.5.7.4}.’ Also, change the DEVID list to be formatted in the same way as the PCTM field, i.e. a starting DEVID and a bitmap that is as long as is required. Copy over the text, figure and description. This gives us a uniform method of listing DEVIDs in the standard.”

347 (Heberling, TR) - What is the difference between ACTIVE PS mode and the Awake state? Please clarify. Please provide the requested clarification. Suggest accept, “Resolve as in comment 456, Add text that says something similar to ‘There are three modes and 2 states in each mode. The modes are ACTIVE, APS and SPS. Within each mode, a DEV is either awake or sleeping.’ Gather up all of the modes and state references and put them in the beginning of 8.12 rather than spread out throughout the sublcause.”

335 (Heberling, TR) - The first sentence of this paragraph is and incomplete sentence. Please rewrite the sentence so that it expresses a complete thought. Please provide the requested rewrite of the indicated sentence. Suggest accept, “Change the first sentence to read ‘SPS mode allows a DEV that is sensitive to power utilization to reduce its power usage while remaining synchronized with the SLEEP states of other selected DEVs.’”

1.2 Email, due Friday, 19 July, 2002

464 (Gilb, T) - We should have an informative annex with sample calculations and examples of frame headers, commands, IEs, beacons, etc. Assign each person one item to create and assign 2 people to review their work. Suggest accept in principle “If there is time left when all other tasks are completed, we will try to put together some examples.”

632 (Gilb, T) - Delete the word "can". Suggest accept in principle, change “The CCM ideas can easily be extended to other block sizes, but this will require further definitions.” to “The CCM ideas are easily extended to other block sizes, but this would require further definitions.”

502 (Gilb, TR) - Cross reference to parameter missing. Add: "The parameter used in this primitive is defined in {xref Table 35}."(in 6.7.3.5) Suggest accept.

5, 131 (Heberling, TR), 786, 818 (Shvodian, TR) - Implied ACK policy is no longer needed since we have support for asynchronous time slots. Remove this sub clause and andy reference to implied ACK. Suggest accept. For 5 and 131, suggest accept in principle. “Implied ACK and all references to it will be removed from the draft.”

424 (Heberling, TR) - A 20 day Letter Ballot is much to short an interval to adequately review the volume of new text that was incorporated into D10. Particularly, all the material associated with security. There are major integration issues that need to be addressed that I did not have time to consider. Also given the PICs is now included in this document, there was no time to properly review the decisions made by the various editors to determine if they were in agreement as to what should be mandatory or optional. Recommend that the next LB for 802.15.3 be extended to 30 days minimum. Suggest reject “While we all appreciate the hard work that goes into reviewing a document for letter ballot, neither the ballot resolution committee nor the task group has the power to set the length of the letter ballot. The working group voted to set that duration.”

688 (Gilb, TR) - Withdraw

279 (Gilb, TR) - Meaning? I think you want to set the SrcID to the PNCID. Change to "The SrcID shall be set to the PNCID." Suggest accept.

48 (Heberling, TR) - The clause title: "Changing channels" is too restrictive given the change in primitive name. Rename clause 6.3.17 Changing Channels to "Changing Piconet parameters. Suggest accept.

209 (Gilb, TR) - PHYPIB_CCAThreshold is an 802.11 holdover and is not used in this standard. Delete this PIB entry. If it stays, however, it should be -55 dBm, but better still, just xref where it is defined. Suggest accept in principle, “Change the value of the PIB entry to indicate that it is implementation dependent but no more than the value listed in {xref 11.6.5}. Also remove ‘For the 2.4 GHz PHY’ text where found in the PIB tables in this subclause.”

1169 (Shellhammer, T) It is quite common for an 802.11b network to utilize all three channels. In addition to the adjacent and alternate channels plot the co-channel FER in figure D.2. Also, add a figure on 802.11b co-channel operation (like figures D.3 and D.4). Accept in principle, “While 802.11b networks will use all three channels in an infrastructure environment, it is not likely in the home environment targeted by 802.15.3. In addition, the APs for these channels will be widely spread (> 50 m distance) so that they do not interfere with each other. However, we will add additional results for co-channel interference with the note that this case is unlikely due to the ability of the 802.15.3 network to find the ‘quietest’ channel.”

1168 (Shellhammer, T) - The theoretical BER curves from 802.15.2 need some work. Modify to new formula once new 802.15.2 draft becomes available. Also, replot figure D.1 so that it is possible to determine which curve is for which system. Accept in principle “If the new formulas are available in time, the coexistence curves will be re-calculated. If not, it will be considered for revision at a future time.”

1170 (Shellhammer, T) - In clause D.3.3 it is not clear the separation between the two nodes in the system under evaluation. For example, the separation between the two 802.15.3 nodes is not specified in clause D.3.3.1 as far as I could tell. Please add text to state the separation between node of the system under evaluation. Do similar for the other systems under evaluation (i.e. 802.11b and 802.15.1). Suggest accept in principle, “Add text to D.3 that states that the separation of the members of the desired system is implied by the receive signal power, which is 10 dB above sensitivity. Add to the assumptions section that the received power is 10 dB above sensitivity since at sensitivity the channel fading cause >> 10% FER.”

1167 (Shellhammer, T) Receiver sensitivity does not effect coexistence performance. What does effect it is the signal-to-interference ratio (SIR) of the various standards. Remove clause D.3.2. section "a" and replace it with a section on SIR. Suggest accept in principle “None of the standards discussed have a SIR performance specified for other systems. SIR performance depends on the modem design and so would vary among implementations. However, the SNR performance is a reasonable approximation of the SIR peformance of the system since the SIR is not known. Add text to D.3.2 that discusses why SNR was used instead of SIR for the analysis.”

1164 (Shellhammer, T) - Since CSMA/CA is often based on frame detection it is not clear why this is the "best method" of coexistence. State that a method of detecting frames from the other standard would be required to use this method for coexistence. Suggest accept in principle “Some CCA detection is done purely on an energy detection basis (this optional for 802.11 and required for 802.15.3). In addition, the timing parameters used in the CSMA/CA affects the peformance of the systems. Add text that better describes the situations under which CSMA/CA would be an appropriate coexistence method, mentioning timing and the requirement for either energy detection or frame detection.”

1165 (Shellhammer, T) - It is not clear what happens if one Piconet chooses the four-channel plan and another Piconet selects the three-channel plan, since the first Piconet was already established. It looks like you could never effectively use the four-channel plan. Explain. Suggest accept in principle “Add text to clause D that explains what happens in this situation.”

1166 (Shellhammer, T) - References to collaborative coexistence mechanism states that "no on-air signaling is required." This is true of PTA, however, AWMA uses signaling over 802.11 to manage the coexistence mechanism. Please remove the phase "no on-air signaling is required." Suggest accept.

1163 (Shellhammer, T) - IEEE 802.11 not only uses CDMA/CA but is also uses a poling mechanism in Point Coordination Function. Mention PCF to prevent comments in sponsor ballot. Suggest accept.

1139 (Roberts, TR) - I missed this on the first letter ballot but specification of the EVM test seems to be incomplete. Below is suggested text to complete the specification. 11.5.2 EVM Calculated Values A compliant transmitter shall have EVM values of less than those given in Table 104 for all of the modulation levels supported by the PHY when measured for 1000 symbols. The error vector measurement shall be made on baseband I and Q data after recovery through an ideal reference receiver system.The ideal reference receiver shall perform carrier lock, symbol timing recovery and amplitude adjustment while making the measurements. The ideal reference receiver shall have a data filter impulse response whose cross-correlation is within 0.5 dB referenced to the impulse response of an ideal root raised cosine, 35% excess bandwidth, Fc=5.5 MHz (3 dB point) filter. Suggest accept in principle, “Add text to the end of 11.5.2 that says ‘The ideal reference receiver shall have a data filter impulse response that approximates that of an ideal root raised cosine filter with 30% excess bandwidth.’”

507 (Gilb, TR) - Need to add HCS to list of things in the frame. Change "... PHY preamble, PHY header, MAC header and the FCS." to be "... PHY preamble, PHY header, MAC header, HCS and FCS." Suggest accept.

506 (Gilb, TR) - HCS needs to be scrambled as well. Change "... MAC header and frame body." to be "... MAC header, HCS and frame body." Suggest accept.

504 (Gilb, TR) - CCIT CRC-16 implementation, the description doesn't say that it needs to be set to all 1s when initialized and the figure doesn't really show how to get the data out. Add text that says that the register shall be set to all 1s before beginning the process and show how the data is xor'ed and shifted out of the registers when it is done. Suggest accept.

580 (Gilb, TR) Errors in 802.11's description of the CRC calculation. 1. The text states "consider the following 48-bit length sequence" but in fact the sequence is only 32-bits. 2. The text identifies bits as follows "b0.....b48", but it seems that "b0.....b31" would be correct. Again, it is only a 32-bit stream. 3. The text identifies the HCS output sequence as follows "b0..... .....b16" but in fact, since it is only 16-bits, it should be "b0..... .....b15". Suggest accept.

943 (Bain, TR) - The text solution does not match the comment on LB12. The first value is to be the means to return the PHY to a operational state (not in a power save state). "Vector number 0 is the entry used by the MAC to instruct the PHY to return from a reduced power state, or off state, to a state where it is ready to receive command. Other values are implementation dependent." Suggest accept in principle, “The table is only times, not the instruction. PSLevel in 6.7 and 6.7.5 controls the PHY’s on/off state. Add text to the description of PSLevel in Table 35 that says ‘PSLevel value 0 is used by the MAC to instruct the PHY to return from a reduced power state, or off state, to a state where it is ready to receive command. Other values are implementation dependent.’”

505 (Gilb, TR) - The status of the scrambler with respect to the second PHY header is ambiguous. In order to ensure that the FER of the 11 Mb/s mode remains low, the scrambler will need to be reset so that losing one of the first two bits does not cause an FER failure. Add text that states that the PHY header of the second repetition of the PHY + MAC header + HCS is unscrambled and that the scambler is re-initialized with the same seed used for the first header when it begins scrambling the second header. The scrambler continues for the frame body following the second header structure as normal. Suggest accept.

456 (Gilb, TR) - Need to add a better explanation of the power save modes here. Add text that says something similar to "There are three modes and 2 states in each mode. The modes are ACTIVE, APS and SPS. Within each mode, a DEV is either awake or sleeping." Gather up all of the modes and state references and put them in the beginning of 8.12 rather than spread out throughout the sublcause. Suggest accept.

947 (Bain, T) - "enable DEVS to completely ...." may be how many implementations will operate but this is implementation specific as to how deep the DEV will "turn off". Change to ‘to turn off completely or reduce power...’. Suggest accept.

2. Comment resolution in Vancouver

2.1 MLME policy

— Change MLME-CREATE-CTA parameters to pass only those things needed to verify the functioning of the standard. Since the channel time parts are not going to be verified, only that a CTA.

2.2 Channel time management (CTM/Async*, CTM/Isoch*)

IDs: 15, 16, 34, 368, 813, 370, 614, 195, 906, 652, 914, 907, 917, 155, 411, 364, 366, 120, 410.

For asynchronous data, initial command comes from FCSL via MAC SAP with the MAC-ASYNC-DATA.request. Then the DEV MLME decides if it needs more time (hexagon decision). If so, it sends the frame over the air. The PNC MLME decides what to do and in the case of rejection responds with channel time status command, otherwise it is a beacon. Neither the PNC DME nor the DEV-2 DME are involved.

Asyncrhonous termination: Do we allow the destination to terminate. PNC is allowed to terminate and the source is allowed to terminate (this simply means that it sets the request to zero).

Now we don’t need MLME-CREATE-CTA.indication or MLME-CREATE-CTA.response, just let the PNC MLME do the response over the air. Also we don’t need MLME-MODIFY-CTA.indication or MLME-MODIFY-CTA.response

Note: Perhaps we want to rename MLME-xxx-CTA to be MLME-xxx-STREAM?

20, 21 , 411 (Heberling, TR) Terminations can never be unsuccessful. The command can only originate from the client and the PNC cannot refuse termination. If the PNC wishes to initialize a termination it will just remove the CTA.

For the ResultCodes on negative actions, allow timeout but do not refer to it as unsuccessful, instead refer to it in the text as indicating that the ACK was not received.

20 - Reject: The ResultCode indicates if the ACK was received for the command. The DEV may consider this to be success or it may take other action depending on the implementation. However the text associated with this is incorrect since it refers to the lost ACK as "unsuccessful" rather than that the ACK was not received.

21 - Accept in principle. Change "The originating DME, when it receives this primitive, is notified whether its CTA termination request was successful or unsuccessful." to be "The originating DME, when it receives this primitive, is notified of the result of its CTA termination request."

411 - Accept in principle. The ResultCode indicates if the ACK was received for the command. The DEV may consider this to be success or it may take other action depending on the implementation. Retain the result code, change the text in clause 6.3.14.11.1 to say: "The originating DEV MLME sends this primitive to its DME after the DEV MLME either has received an ACK to its CTA request command or the RequestTimeout has expired." and change the text in clause 6.3.14.11.2 as indicated in the resolution of comment number 21.

Ed note: This probably applies to other comments, particularly disassociation and deauthentication.

123 (Heberling, TR) - Many issues

Beacon confirmation of synchronous request. Suggest stream creation information element. IDs 123, which really is a reference to [06] in 02/276r0. Asked for straw poll, do we require ACK before building the beacon, result was 4/1/5 (y/n/a). So action is for WMS to create new text in 8.5.1.1, page 175, line 50 that indicates this and send it to the reflector by COB 10 July 2002.

Resolution for 123: Accept in principle: Detailed resolution is in document 02/273r2.

(Beginning of resolution for comment #123)

Don't use new IE, other edits that will be made are (based on 02/276r0 notation):

8.5 Channel Time management, <Page 175, line 3, TR> Accept as written
8.5.1 Isochronous Stream management, <Page 175, line 13-15, Editorial> Accept as written.
<Page 175, line 19-20, TR> (needs work, but seems like the right direction)
<Page 175, line 24, Ed> Accept as written.
8.5.1.2 Isochronous stream modification, <change two last bullets , TR>
Change to implement:
The CTR type field shall be set to the same value as in the original request for that stream index.
All the other channel time request command parameters are set to appropriate values as defined in 7.5.5.1.
Minimum number of TUs field is set to either the original value requested or a new value if the DEVs requirements have changed.
Desired number of TUs field is set to a value that is greater than or equal to the minimum number of TUs.
Note: This allows a DEV to change from every beacon to subrate and vice-versa. Does this cause enough problems that we should require a tear-down and re-establishment?
<page 177, line 46, TR> Accept as written.
Figure 115 – MSC for modifying a stream <revert to old, TR> Accept as written
8.5.1.3 Isochronous stream termination, <Page 179, line 40-42, TR > Withdraw this issue.
Figure 117 – MSC of source DEV-2 requesting termination of its stream <TR>: Withdraw this issue.
New issue: Make sure that we mention somewhere that only the source or the PNC of a broadcast or multicast stream shall be able to terminate the stream. Page 179, line 30, Add text "In the case of multicast or broadcast streams, only the source DEV or the PNC may terminate the stream."
Figure 118 – MSC for a target DEV-2 disassociating causing a source DEV-3 stream termination <delete whole MSC, TR>. Accept as written, also delete lines 23-24 on page 180. Add text that says "When either the source or destination of a stream is disassociated from the network the streams are terminated as indicated in {xref disassociation}.
8.5.2.1 Asynchronous channel time creation and modification reservation <Page 181, line 26, TR> Accept as written.
<Page 181, line 37, TR> Change "and the same destination" to be "and the same source"
<Page 181, line 40, E> JPKG to check grammar, otherwise it is probably OK.
<Page 181, line 49, E> Accept as written.
Figure 119 – MSC for reserving asynchronous data channel time. Discussed earlier, new MSC is below:

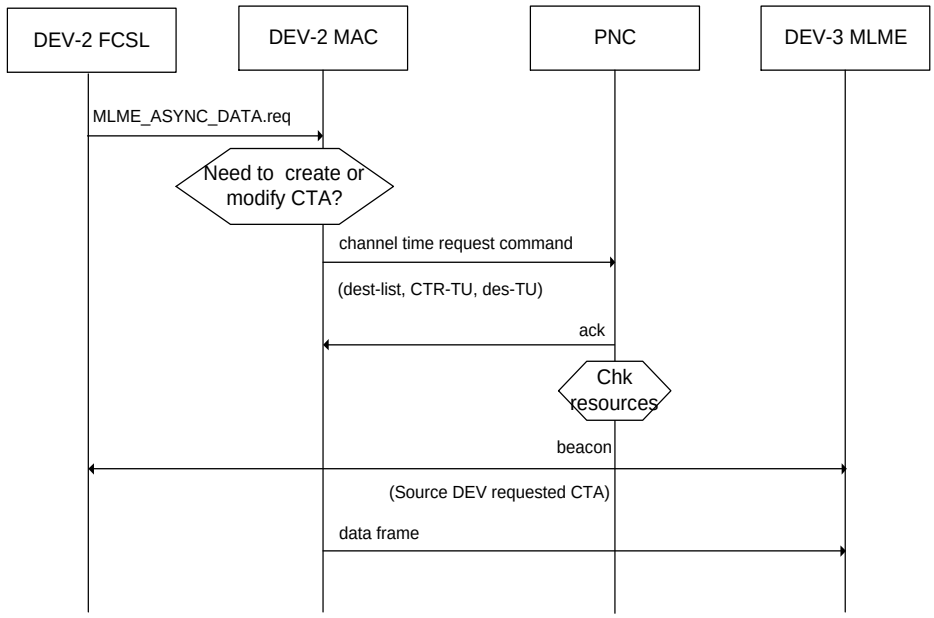

Figure 1—MSC for a approved asynchronous channel time request

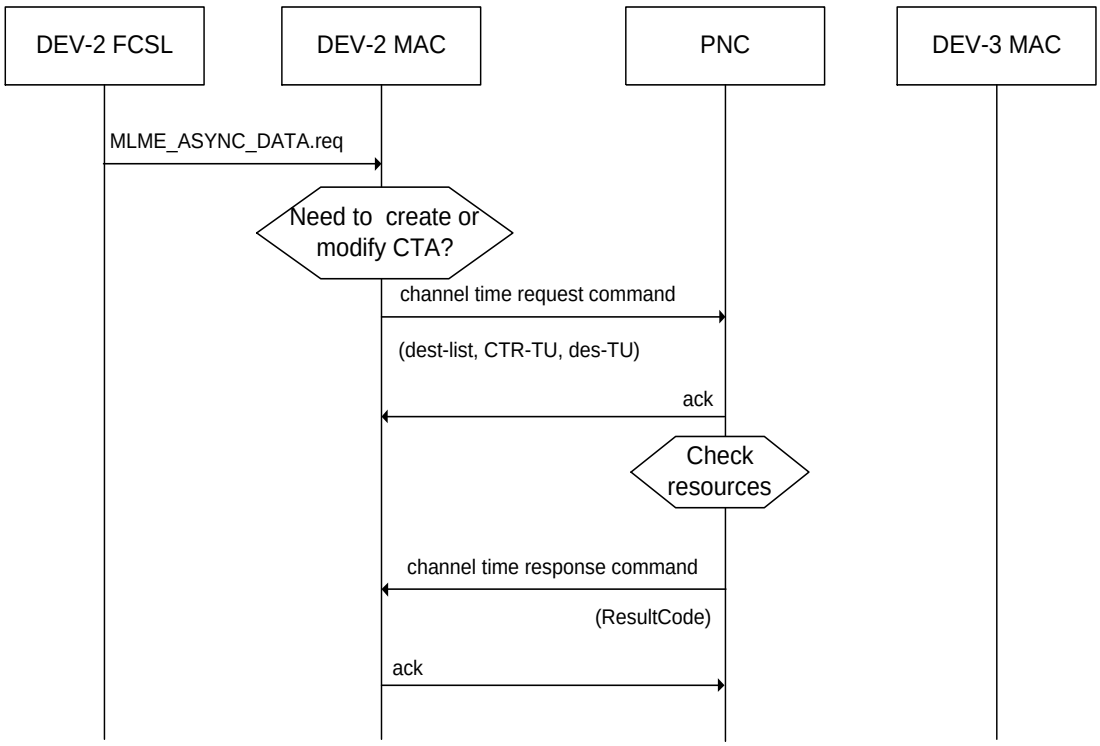

Figure 2—MSC for a denied asynchronous channel time request

8.5.2.1 Asynchronous GTS termination: Change it to only allow the source and PNC to terminate.

Change “Only the PNC, the originating DEV, or the target DEV shall be able to” to be “Only the PNC or the originating DEV shall be able to”
(end of resolution of comment #123)

2.3 Child/neighbor handover ()

2.4 Handover

779, 785 (Shvodian, TR) - Add a new handover handover IE to be used to announce the beacon number where handover will take place.

785 ACCEPT IN PRINCIPLE. The new IE will be added as indicated in the resolution of comment #779.

779 ACCEPT IN PRINCIPLE. Add an PNC Handover information element. It only needs to be 4 octets total (IE number, Length=2, handover countdown, PNC response) . The last beacon sent by that PNC shall have counter number 0.

Note: the PNC response field depends on the resolution of the comments relative to this field.

24 (Heberling, TR) - Withdrawn

154 - Withdrawn

797 - ACCEPT IN PRINCIPLE. Add a beacon countdown in the new PNC handover IE.

22 - ACCEPT IN PRINCIPLE. Add new subclause as follows:

6.3.11.5 MLME-PNC-HANDOVER-INFO.indication This primitive indicates the reception by the DEV of an unsolicited DEVInfo list sent by the PNC as part of the PNC handover procedure, 8.2.3. The semantics of this primitive are: MLME-PNC-HANDOVER-INFO.indication(DEVInfoSet) 6.3.11.5.1 When generated The MLME sends this primitive to its DME upon receiving a complete DEVInfo list via the PNC info command. 6.3.11.5.2 Effect of receipt The new PNC's DME is provided with a copy of the complete DEVInfoSet.

160 ACCEPT IN PRINCIPLE. Change the indication to be initiated by the PNC handover information element in the beacon as opposed to the broadcast PNC handover command. This now passes one element, the PNC response value.

98 - ACCEPT. Delete all other references to it in the draft, replacing it, where appropriate with the PNC handover IE.

154 - Withdrawn

14 (Heberling, TR) - Add these parameters to the MLME-PNC-HANDOVER.request parameter list: NmbrHndOvrBcns, DEVInfolist. Delete NmbrOfDEVs from the parm list since it can be determined from the DEVInfoList. Also add these new parameters to Table 15 with these type/range and defs. NmberHndOvrBcns: Type:Integer; Range: 4-255; Def: The number of beacons, containing the PNC handover IE, the old PNC will transmit before control of the piconet by the old PNC is turned over to the new PNC.

606 - ACCEPT IN PRINCIPLE. The new PNC timeout has been replaced by the number of beacons.

162 - ACCEPT IN PRINCIPLE. Add new clause 6.3.11.3 which describes the MLME-PNC-HANDOVER.response primitive. The text of which is included here. 6.3.11.3 MLME-PNC-HANDOVER.response This primitive is used to initiate a response to an MLME-PNC-HANDOVER.indication. The semantics of this primitive are: MLME-PNC-HANDOVER.response()

6.3.11.3.1 When generated This primitive is sent by the new PNC's DME to its MLME after receiving these two primitives in succession, MLME-PNC-HANDOVER.indication, MLME-PNC-INFO.indication and the DME is ready to take over as the new PNC of the piconet.

6.3.11.3.2 Effect of receipt When the new PNC's MLME receives this primitive from its DME it is informed that its DME is ready to become the new PNC of the piconet.

399 - Withdrawn.

381 - ACCEPT IN PRINCIPLE. Delete the HandoverTimeout from the MLME-PNC-HANDOVER.indication parameter list

100 - ACCEPT IN PRINCIPLE. Change the PNC handover information command to PNC handover CTRB command. Also change the title of figure 64 as well. Delete the "Last" field from the command body and its descriptive text.

43 - ACCEPT IN PRINCIPLE. The new handover will use the number of beacons to avoid this problem.

323 - Accept.

319 - ACCEPT IN PRINCIPLE. Change this sentence fragment from "... and obtain the DEV information from the current PNC within ..." to "... and be prepared to receive the list of DEV information list, {xref 7.5.4.2}, and CTRB records from the current PNC."

317 - ACCEPT. Change this sentence fragment from "...with an indication of the hand-over time out." to "... with the parameters specified in the PNC handover request command, 7.5.3.2."

325 - Please delete the sentence starting with these words: " The PNC shall indicate that the transfer is complete..." Also delete the first two sentences of the last paragraph and insert these sentences: " The chosen AC after receiving the PNC handover request command, the list of DEV information, and the CTRB records shall respond to the PNC with a PNC handover response command. This will signal to the PNC that the chosen AC is ready to commence the handover beacon sequence. The PNC upon receiving the PNC handover response shall ACK the received command and then put the PNC handover IE, {xref 7.4.x}, in the beacon. (additional text is provided in 02/276r0 Page8, Clause 8.2.3 paragraph 3 and page 9 paragraph 1.) Meanwhile the chosen AC after receiving an ACK to its PNC handover response command will prepare to broadcast its first beacon as the new PNC after the last beacon received from the current PNC. The current PNC shall decrement the beacon countdown field in the PNC handover IE with each beacon broadcast until the field is zero. After sending the last handover beacon, the old PNC relinquishes control of the piconet, generates an MLME-PNC-HANDOVER.confirm to its DME, and stops generating beacons. The new PNC shall broadcast its first beacon as close to the start time of what would have been the old PNC's next beacon."

382 - The PNC MLME sends this primitive to its DME The PNC MLME sends this primitive to its DME after it has sent its last beacon as PNC or if it fails to receive the PNC handover response command within the HandoverTimeout interval.

For effect of recipt, The ResultCode is set to SUCCESS when the PNC sends its last beacon as PNC before the HandoverTimeout interval expires. The ResultCode is set to HANDOVER_FAILED if the PNC fails to

receive the PNC handover response command before the HandoverTimeout interval expires, then the Result-Code is set to TIMEOUT.

677 - ACCEPT IN PRINCIPLE. The old sentence was deleted.

172 - ACCEPT IN PRINCIPLE. The proposed text for these changes are below: 7.5.3.1 PNC handover request command keep the first two sentences intact. Make these changes to figure 63: |Cmd-Type|Length=2|NmbrDevs(1)|NmbrCTRBs(1)|. NmbrDevs is the same defintion as is currently defined in this clause. NmbrCTRBs is the number of CTRBs, excluding requests for asynchronous channel time, currently being served by the PNC that will be transferred from the current PNC to the new PNC using the PNC handover CTRB command. 7.5.3.2 PNC handover response command This command is used to inform the current PNC that the DEV selected to become the new PNC is ready to assume PNC responsibilities. The structure of this command shall be as ilustrated in figure xxx |Command type|Length=0|(PNC response, if it survives, xref to where it is defined).|

400 - Accept.

192 - Withdrawn

2.5 ACK (ACK*)

1024 (Rasor, TR) - Figure 11: the non-secure Immediate ACK Frame Format does not contain a FCS, which is incompatible with practice with all other frame formats.

> Reject, There is no need for an FCS if there is no payload. The Imm-ACK has an HCS on the header, so all of the information in the packet is protected by a CRC. Depending on the what is done with an FEC in a future PHY, there may be a minimum packet size for interleaving and additional latency. Furthermore, this is an item that has been unchanged since before D09. (accepted by Rasor).

421 (Heberling, TR) - <change from> If an Imm-ACK is expected for that frame, the remaining time in the time slot needs to be large enough to accomodate the current frame, 2 SIFS periods and the Imm-ACK frame at the same PHY rate as the transmitted frame. <to> If an Imm-ACK or del-ACK is expected for that frame, the remaining time in the time slot needs to be large enough to accomodate the current frame, 2 SIFS periods and the Imm-ACK or del-ACK frame at the same PHY rate as the transmitted frame.

> Accept

3 (Heberling, TR) - Del-ACK policy: 1) Once you request Dly-ACK policy on a stream, can you change it? If so, is it required to do a Dly-ACK request? If Dly-ACK is declined, you should be able to keep sending Dly-ACK policy, change to Imm-ACK policy or No-ACK, but you cannot mix them up. Can we pass up the decline to the higher layers? If so, it can re-negotiate the time.

13 (Heberling, TR) - Dly-ACK negotiation, do we need to add more values? ACCEPT IN PRINCIPLE. The name of the field may need to change. Also need to delete aMaxDlyACKBurstSize from the end of clause 8 and change the reference to it to indicate that it is a value passed in the Dly-ACK frame.

768, 816, 817 (Shvodian, TR) - Dly-ACK policy/No-ACK explained: ACCEPT IN PRINCIPLE. The ACK stream policy is set with the stream, individual data packets set an ACK policy, the two bits in the frame field are back to ACK-policy and the one bit Dly-ACK is Dly-ACK request. (Note: we still need someone to write precise text).

819 - (Shvodian, TR) - Accept if Implied ACK goes away, probably accept anyway. The text needs some work and we need to say that you have to leave time for a Dly-ACK request as well. WMS to provide some text.

1 (Heberling, TR) - Does MAC or CL decide ACK policy for each packet? This depends in part on the resolution of 3. WITHDRAWN by Heberling.

806 (Shvodian, TR), 184 (Heberling, TR) - The recipient of Delayed ACK traffic is no longer responsible for obtaining channel time for sending the Dly-ACK frames

Accept 184, Accept 806 in principle, “Resolve as indicated in 184.”

820 (Shvodian, TR) - The retry bit is also used to detect duplicate frames.

ACCEPT IN PRINCIPLE. Change to "The source ID, stream index, fragmentation field and retry bit are used to detect multiple receptions of the same frame."

2.6 IEs (IE*)

73, 76 (Heberling, TR), 300 (Shvodian, TR) - Does this create interoperability problems?

Suggest accept in principle, use the suggestion in 02/276r1 (resolution [16] in the document), but we need to find a way to get unique manufacturer identifiers. Suggestions are:

— Use MAC address first 2 (or is it 3) octets
— String that is the trademarked manufacturer name.
— Have the RAC assign number
— Have 802.15 assign OIDs
— Have 802.15 assign number.

74 (Heberling, TR) - Remove DEV GTS status information element. The supposed benefits provided by this information element do not warrant chewing up 34 octets of beacon time. In its place introduce this new information element: StreamAnnouncement IE 7.4.10 Stream announcement The stream announcement information element shall only be sent by the PNC in the beacon. The stream announcement IE shall be formatted as illustrated in Figure 33. This IE is used to indicate in the beacon to a DEV that its requested CTA |Element ID|Length|= 2|SrcDEVID|StreamIndex| SrcDEVID is defined in 7.x.x Stream Index is defined in 7.x.x.

Accept in principle: Delete the DEV GTS Status IE. However, the stream announcement information element is not needed.

2.7 Implied ACK (ACK/Implied)

WMS will post to the list to see if someone still needs it. Comments 786, 131, 5 (withdraw if implied ACK is deleted), 818.

2.8 Starting child or neighbor piconets (DepPN)

968 -

2.9 Frame issues

255 (Heberling, TR)

Withdrawn

770 - accept.

444 - Rejected.

778 - ACCEPT IN PRINCIPLE. Delete the maximum transmit power IE, take the Max TX power level field and put it with the new piconet sycnrhonization field in the beacon. Add text that says that if the PNC does not want to limit the TX power it shall set the field to 0x7F.

432 - ACCEPT IN PRINCIPLE. The beacon ordering was resolved with comment #937 and 386.

937 - ACCEPT. Change the piconet synchronization IE into a field.

436 - Parent BSID?

500 - Withdrawn

70 - Accept: The pad bit has been removed, make the indicated change.

166 - Accept: The pad bit has been removed, make the indicated change.

1018 - ACCEPT IN PRINCIPLE. Change the text to "At the receiver, the initial remainder shall be preset to all ones. The serial incoming bits of the calculation fields and FCS, when divided by G(x), in the absence of transmission errors, results in a unique non-zero remainder value. The unique remainder value is the polynomial:"

64 - ACCEPT IN PRINCIPLE. The FCS field shall be transmitted in the order specified in {xref 7.1}. Change the text on page 101, line 47, from "Any field containing a CRC is an exception to this convention and is transmitted with the coefficient of the highest-order term first." to read "Any field containing a CRC is an exception to this convention and is transmitted msb first."

774 - ACCEPT IN PRINCIPLE. Modified as follows: "The frame body is a variable length field and contains information specific to individual frame types. The minimum frame body is zero octets. The maximum length frame body is aMaxFrameSize-4 octets. This maximum length includes the security fields, if present."

1020 - REJECT. The non-secure frames do not need a sequence counter. The secure frames probably don't need a sequence counter either, that will be resolved by another comment.

2.10 Security/authentication (SEC/Auth)

57 (Heberling, TR) The MAC address isn't needed as parameter in the Authentication exchange. The header carries the DevID of source and destination, and if either side is unknown to the other, they are not likely to accept authentication anyway.

Withdrawn

941 (Shvodian, T)

Dan is to figure this one out.

769, 890 (Shvodian, TR) Do we need a SEC pad - Yes, add an octet to secure frame formats. It is set to the number of octets that the encryption algorithm added. If the frame is unecrypted, the is field shall be set to 0. (unless the encryption already deals with this.)

48 (Gilb, TR) Withdrawn

834 (Shvodian, T) - Do we need to protect ACKs

Accept (deletes protected ACKs)

835 (Shvodian, T)

Accept in principle. PNC handover does not require ACL handover. (See clause 9.3.2).

831 (Shvodian, T)

Accept.

832 (Shvodian, T)

Accept in principle. PNC handover does not require ACL handover. (See clause 9.3.2).

836 (Shvodian, T)

Accept in principle. ACLs are needed, text needs to be added to mode 3 to clarify this requirement.

837 (Shvodian, T)

Accept.

836 (Shvodian, T)

Accept in principle. ACLs are needed, text needs to be added to mode 3 to clarify this requirement.

836 (Shvodian, T)

Accept in principle. ACLs are needed, text needs to be added to mode 3 to clarify this requirement.

872 (Shvodian, T)Withdrawn
875 (Shvodian, T)Reject
854 (Shvodian, T)ACCEPT IN PRINCIPLE. The security manager maintains a separate association/ authentication state for each of the DEVs with which it is willing to authenticate.
863 (Shvodian, T)ACCEPT IN PRINCIPLE. Text will be added (based on another comment) that describes what happens in this case.
853 (Shvodian, T)Accept.
866ACCEPT IN PRINCIPLE. None of the commands use the secure command format. Clause 7.5.2.x specifies that these commands are always sent in the non-secure format.

2.11 PNC Responsiveness

10, 12, 17, 86, 92, 94, 188, 191, 357 (Heberling, TR), 808 (Shvodian, TR)

17 and 94 have more than just PNC Responsiveness.

808 - Suggested remedy is to have JB add text that clarifies the usage of the PNC responsiveness, text is due by the morning of 11 July, 2002.

For the rest, ADH will review a prior document to see if there is a compromise available. 02/109, review will be later today.

2.12 Transmission sequence resync

41 (Heberling, TR), 478 (Gilb, TR), 787 (Shvodian, T) - Transmission sequence resync command is not needed.

Accept: The transmission sequence resync command and all references to it will be removed from the draft.

2.13 Misc

56 (Heberling, TR) Inconsistent DEVID naming conventions between clause 6 and clause 7. Which is it going to be: SrcID instead of OrigID, DestID instead of TrgtID? Lets be consistent.

Accept in principle. The BRC will closely review the use of OrigID, TargetID, SrcID and DestID to reduce the number of uses of OrigID and TargetID to the absolute minimum necessary.

423 (Heberling, TR) - Missing an MSC illustrating the primitives and signals needed during a de-authentication initiated by a DEV to the PNC.

Withdrawn

96 (Heberling, T) Missing a reason code for when the DEV disassociates from the piconet. Add this reason code 4-> DEV_LEAVING_PICONET.

Accept.

55 (Heberling, T) Disassociation cannot "fail". Both PNC and client shall regard a disassociate request as being completed when requested and proceed with the disassociation procedure. The PNC needs to get back the DevID from the confirm in case it has disassociated several DEVs. The reasonCode is not needed since the request cannot fail, and even if it did there is no recovery.

ACCEPT IN PRINCIPLE. The command is issued when it gets an ACK or the time out has occurred. The ResultCode is used to inform the DME of the result of the process. Change text in 6.3.6.3.1 to "This primitive is sent by the originating MLME to its DME after sending a disassociation request command, {xref 7.5.1.3}, and receiving either an ACK or an ACK_TIMEOUT." Change the text in 6.3.6.3.2 to "The originating DME, when it receives the MLME-DISASSOCIATE.confirm primitive, is notified of the result of the disassociation procedure."

158 (Heberling, TR) The MLME-DISASSOCIATION.confirm primitive has value only to the PNC. A DEV that requests to be disassociated from the piconet doesn't really care if it receives an ACK, since by the time it does receive an ACK it would most likely be shutdown. Consequently, the only entity that is interested in receiving a confirmation is the PNC, since it will still be in operation and therefore interested in knowing which DEV, it(PNC) had previously requested disassociate, responded with an ACK. Given this perspective please make these changes: Change this sentence from: "This primitive reports the results of a disassociation request." to "This primitive reports to the PNC the results of a PNC initiated disassociation request

directed to a DEV. The semantics of the primitive are: MLME-DISASSOCIATE.confirm(DEVID) 6.3.6.1 When generated This primitive is sent by the PNC MLME to its DME after receiving an ACK from the DEV to which the PNC had sent a disassociation request command 7.5.1.3. (Delete lines 35-37) 6.3.6.2 Effect of receipt The PNC DME, when it receives the MLME-DISASSOCIATE.confirm primitive, is notified as to which DEV has been disassociated.

> Accept in principle, Add to then end of 6.3.6.2 “The PNC DME, when it receives the MLME-DISASSOCIATE.confirm primitive, is notified as to which DEV has been disassociated.

1) IEs PNServices CID-63: This one will be handled with the vendor identification that will be used for the ASIE.

2) MTS CIDs 58 Trying to compromise, up to ‘Change this sentence fragment from"... 0x00 reserved for asynchronous data and 0xFE reserved for unassigned streams." to "...0x00 for asynchronous GTSs and asynchronous data, 0xFD reserved for MTSs, and 0xFE reserved for unassigned streams."‘

119, ACCEPT IN PRINCIPLE. Change the sentence to read "If commands are not allowed in the CAP, the PNC should assign an MTS with the new DEVs DEVID as the SrcID as soon as possible after a successful association, {xref 8.3.1}, preferably in the next superframe, in order to support fast connections."

190 Withdrawn.

3)PICs CID 1171 Although I did not have a personal comment regarding the PIC, I feel very strongly that this is an area of the Specification that I will definitely clobber during the next recirc. if we do not discuss in detail what functionality shall be mandatory and what should be optional.

1171 (Cypher, TR)

> ACCEPT. The BRC will closely review the PICS to ensure that it is correct before the next letter ballot.

4)PNCInfo CIDs 377 & 140

377 - This will be true when we fix the fragmentation of the commands for handover.

140 - This will be true when we fix the fragementation of the commands for handover.

5) Scan(BSID) CIDs 83, 795, 416; BSID CIDs420,51,419,50,52

83 - Withdrawn, except that need to make sure another comment addresses adding the BSID to the scan procedure.

795 - ACCEPT IN PRINCIPLE. Need to specify that we scan for both or one, the other or any. (need better text).

416 - Accept

420 - Withdrawn

51 - Withdrawn

419 - Withdrawn

50 - ACCEPT IN PRINCIPLE. Delete the ChannelChangeTimeout parameter. Replace the deleted parm with NmbrOfChangeBeacons. see doc: 02/276r0 Page 21 for further description.

52 - ACCEPT IN PRINCIPLE. Replace ChannelChangeTimeOut parameter with the NmbrOfChangeBeacons parm. Also make sure the definition of this parameter goes in the appropriate table, as indicated in 02/276r0, p21.

6) CTM CIDs 32,30,23,28,80,33,408,407,409,413,414,401

32 - Accept.

30 - Accept

23 - Accept

28 - ACCEPT IN PRINCIPLE. Remove NumTrgts and NumAsyncTUs from the all instances of MLME-CREATE-CTA, MLME-MODIFY-CTA, and MLME-TERMINATE-CTA. Rename the TrgtIDlist to TrgtDEVID in all the indicated primitives.

80 - Withdrawn

33 - ACCEPT IN PRINCIPLE. MLME-yyy-CTA.indicate and MLME-yyy-CTA.response do not go up or come down from to the PNC DME. Delete these MLMEs and fix the MSCs to reflect this change.

408 - Withdrawn, Resolution of 33 makes this unnecessary.

407 - Withdrawn, Resolution of 33 makes this unnecessary.

409 - Withdrawn, Resolution of 33 makes this unnecessary.

413 - ACCEPT IN PRINCIPLE. Move the Chk Resources and Evaluate request to the PNC MLME. Delete the MLME-CREATE-CTA.{ind,rsp} from the MSC. Delete the PNC DME from the MSC. Delete the Allocate Resource hexagon.

414 - ACCEPT IN PRINCIPLE. Move the Chk-Resources processes from the DME to the MLME. Delete the and Allocate Resources hexagon.

401 - Withdrawn

7) DEVID CID 56 - Resolution in process, agreement in principle.

8) DisAssoc/DeAuth CIDs

344 (Heberling, TR) - Withdrawn

348 (Heberling, TR) - Withdrawn

346 (Heberling, TR) - ACCEPT IN PRINCIPLE. Add text "The PNC does not use the de-authenticate command to remove a DEV from the piconet."

9) bit/byte ordering CID 150

150 (Heberling, TR) - Ask the reflector, BRC will vote, outcome either way is OK.

10) FrmFrmt/... CIDs 386, 385,66,68

386 (Heberling, TR) - Accept

385 (Heberling, TR) - ACCEPT IN PRINCIPLE. Move the table to 7.3.1 so that it is clear that it applies to both secure and non-secure beacon formats. Delete the SECID, integrity code and time token IEs since they are already in the frame format for the secure beacon.

425 (Gilb, TR) - Accept.

66 (Heberling, TR) - ACCEPT IN PRINCIPLE. Change the text to "At the receiver, the initial remainder shall be preset to all ones. The serial incoming bits of the calculation fields and FCS, when divided by G(x), in the absence of transmission errors, results in a unique non-zero remainder value. The unique remainder value is the polynomial:"

68 (Heberling, TR) - ACCEPT IN PRINCIPLE. "The FCS is the one's complement of the sum of the remainders in "a" and "b" below: a) The remainder resulting from ((xk*(x31+x30+...)) divided(modulo 2) by G(x)). The value k is the number of bits in the calculation field. b) The remainder resulting from the calculation field contents, treated as a polynomial, multiplied by X32 and then divided by G(x))." Note: add reference to ANSI X3.66 CRC-32 when we get a copy to review to get the correct reference.

11) ChnlTime change CID 194

194 - Accept in principle, DEVs may sleep and BSID stays.

12) System Change Bit CID 361 Possible withdrawn.

3. Status at closing in Vancouver

a) Ballot resolution committee formed, members are:
b)

.

Table 1—Ballot resolution as of close of St. Louis meeting

Type	LB17	Unresolved as of 12 July, 2002
T (technical)	131	?
TR (Technical required)	444	?
T and TR	575	?
E (editorial)	622	?
Total	1197	?

4. Suggested resolutions from JPKG

4.1 Clause 6 comments.

Comment (TR): (Clause 6, multiple locations) When the device is operating in security modes 1, 2 or 3, the MLME needs to be able to indicate to the DME what type of protection is used on a given received frame so that the DME can decide whether or not to accept the frame. This is important because some devices may want to choose to send unprotected frames to certain other devices and the DME needs to be able to determine whether its policy allows it to accept those frames. An indication needs to be added to each MLME.indication and each MLME.confirm in Clause 6, which indicates that a frame is received from another DEV, specifying whether the frame had security turned on and whether the frame came from a device in the ACL.

Author's note: The interfaces for the above described MLME messages should add the following entries to the semantics tables:

```
MLME-XXX.indication (or .confirm)    (
                                     SecurityUse,
                                     ACLEntry
                                     )
```

Author's note: The following table entries should be added to the above described MLME messages.

Table 2—MLME-XXX.indication (or MLME-XXX.confirm) parameters

Name	Type	Valid Range	Description
SecurityUse	Boolean	TRUE or FALSE	This indicates to the DME if the received data frame had the security suite applied to it.
ACLEntry	Boolean	TRUE or FALSE	This indicates to the DME if the sender was found in the ACL.

Comment (TR): (Clause 6, multiple locations) Devices need to have the capability of choosing when to send frames with security and when not to. The decision for when to send a frame with security and what key to use should be determined by the DME. An indication needs to be added to each MLME.request and MLME.response in Clause 6, which cause the DEV to send a frame to another DEV, specifying whether that frame should be protected by security.

Author's note: The interfaces for the above described MLME messages should add the following entry to the semantics tables:

```
MLME-XXX.request (or .response)    (
                                   KeySelection
                                   )
```

Author's note: Insert the following entry into Table 61 on page 86:

Table 3—MLME-GTS.request parameters

Name	Type	Valid Range	Description
KeySelection	Enumeration	PICONET-MGMT, PICONET-DATA, PEER-MGMT, PEER-DATA, NONE	Specifies the key that shall be used to protect the outgoing frame or that security shall not be used on the frame.

Comment (TR): (Clause 6) When devices are running in a secure mode, they need to be able to indicate to the DME when frames received or frames being sent cause security operation failures. These security operation failures could be caused by not having the specified key or by a failed integrity check or some other cryptographic failure.

Author's note: The following sub-clause should be added to Clause 6 to support the above comment.

4.1.1 Security management primitives

These primitives define how the MLME communicates security related events to the DME.

4.1.1.1 MLME-SECURITY-ERROR.indication

This primitive allows the MLME of any DEV to indicate a failed security processing operation to the DME.

4.1.1.1.1 Semantics of the service primitive

This primitive shall provide the following interface:

```
MLME-SECURITY-ERROR.indication (
                                    SrcID,
                                    DestID,
                                    SECID,
                                    ReasonCode
                                    )
```

Table 4 specified the parameters for the MLME-SECURITY-ERROR.indication primitive.

Table 4—MLME-SECURITY-ERROR.indication parameters

Name	Type	Valid Range	Description
SrcID	Integer	Any valid DEVID as defined in 7.2.3{xref}	The DEVID of the entity from which the frame causing the error originated.
DestID	Integer	Any valid DEVID as defined in 7.2.3{xref}	The DEVID of the device that the frame was intended for.
SECID	Octet string	Any valid security session identifier.	Specifies the unique security session identifier for the key that was used on the incoming frame or that was requested to be used on the outgoing frame.
ReasonCode	Enumeration	UNAVAILABLE-KEY, FAILED-SECURITY-CHECK, BAD-TIME-TOKEN	The reason for the security error.

4.1.1.1.2 When generated

This primitive is issued by the MLME when it receives an MLME.request message from a higher layer that requires security to be applied to a frame, but it is unable to find an appropriate key in the ACL or fails to be able to apply security to the frame. This primitive is also issued by the MLME when it receives a validly formatted frame from another device that induces a failed security check according to the security suite or for which the device is unable to find the designated key in the ACL. This primitive is also issued by the MLME when the time token received in a frame does not correspond to the current time token known by the DEV or if the last beacon was not valid.

4.1.1.1.3 Effect on receipt

On receipt of this primitive, the DME is notified of a security error and the reason for the security error.

Author's note: End of added text for that comment.

Comment (E): (Table 11, pg. 41) The entries for ChallengeType and ChallengeLength should be removed as they are not used any longer.

Comment (T): (6.3.8.1, pg. 46) The use of the SECID in the MLME-REQUEST-KEY.request and MLME-REQUEST-KEY.indication implies that the requesting device knows the SECID of the key it is requesting. This will be true for piconet-wide keys because the SECID will be included in the beacon, but for peer-to-peer keys, the DEV may not know the SECID of the current key, in which case it perhaps should be allowed to request the key without knowing its SECID.

Comment (E): (Table 31, pg. 84) The SECID, sequence numbers and time token should have lengths 2, 4 and 6 respectively.

Comment (T): (Table 31, pg. 84) There should be two SECIDs, one for the management key and one for the data key. Recommend inserting an additional entry for MACPIB_PNCManagementSECID that indicates the SECID of the management key. The MACPIB_PNCSECID should be called the MACPIB_PNCDataSECID and correspond to the data key only.

Comment (T): (Table 32, pg. 85) Each entry in the access control should be able to support keys shared with that particular device. For each access control list table, there should be ManagementKeyInfo, Management-SECID, DataSECID, DataKeyInfo, SMSeqNum and DEVSeqNum entries. Recommend adding these field to the table.

4.2 Clause 7 comments

Comment (TR): (Clause 7.3) A 2-byte secure frame counter needs to be added to the secure frame formats in Figure 10, Figure 12, Figure 17 and Figure 19. The entry should be called "Secure frame counter" and should be added directly after the Time token in each figure. Similarly, the following entry should be added to Table 38:

Table 5—Beacon frame body

Information element	Sub clause	Note	Present in beacon
Secure frame counter	{xref}	The secure frame counter used by the PNC in this superframe, which is used to ensure uniqueness of the nonce.	As needed

Comment (TR): (Clause 7.3.2) A secure delayed ACK frame should be specified. The same conventions used with the other frames should be implemented.

Comment (TR): (Clause 7.4) The 2-byte secure frame counter needs to be added as an information element. Insert the following text for the secure frame counter:

4.2.1 Secure frame counter

The secure frame counter is used to guarantee that the nonce used for CCM security in a given frame is unique. The secure frame counter information element shall be formatted as illustrated in Figure 3.

Figure 3—Secure frame counter information element format

octets: 2	**1**	**1**
Secure frame counter	Length (=2)	Element ID

The secure frame counter represents the number of times the selected key has been used during that superframe. This counter shall be included in the CCM nonce.

Author's note: End of added text for this comment

Comment (TR): (Clause 7.5) In each of the commands, the DME should control whether the SEC field is set to 1 or 0. In each case in which the SEC field is mentioned, the word "shall" should be changed to should or the sentence should be removed. For example, in 7.5.1.1, remove the second sentence or change it to "The SEC field in the frame control field should be set to 0."

Comment (T): (Clause 7.5.1.2) It appears that if the length of the OID is variable, it may not be possible to unambiguously parse the association response command. Recommend adding the length of the OID before the OID to make this unambiguous.

Comment (TR): (Clause 7.5.2.1) The RSA security suite should be added to the document and the following entries should be added to the list of public-key object types:

5 -> RSA 1024-1 key
6 -> RSA X.509 certificate

Comment (TR): (Clause 7.5.2.5-7.5.2.9) The sequence number in the request key, request key response, distribute key, distribute key response, and de-authenticate commands are not necessary, as the general format for commands specified in 7.3.3.2 includes the sequence number in the command already. The sequence number should be removed from all of these commands.

Comment (TR): (Clause 7.5.2.6-7.5.2.8) The security session ID (SECID) should be included before the Encrypted Seed (where the sequence number currently resides) in the request key response, distribute key request and distribute key response commands. This value is needed to uniquely identify the key that is being transmitted in the protocol. Note that the SECID should not be included in the request key command since the requesting party may not know the SECID of the key being requested. Recommend adding the following text to each of the three commands:

The SECID is the unique identifier for the seed (and corresponding key) that is being transported in this protocol.

4.3 Clause 8 comments

Comment (T): Many of the operational requirements used in clause 8 describe what the DME has to do in order to perform certain operations. The responsiveness of a DEV to operations performed by other devices tends to be based on what the DME does, but the standard doesn't really have any control over the DME.

Should the “shall” statements in clause 8 be made into “should” statements since they aren’t actually requirements on the MAC layer itself? If so, clause 8 should be changed accordingly to indicate that the requirements in this clause are only optional.

4.4 Clause 9 comments

Comment (T): (Clause 9.3) The security policies described in clause 9.3 are policies that must be implemented by the DME in order to provide the security intended by the security architecture. As such, they cannot be requirements that are placed on the DME. Recommend changing the text in clause 9.3 to:

Security policies determine the actions taken to preserve the security of the piconet. In general, these security policies are implemented by the DME and are thus outside the scope of this standard. However, proper implementation of the security policies is imperative to providing the security services and operational functionality claimed in this standard. It is therefore strongly recommended that implementers ensure that the DME implements the following security policies accurately.

Comment (T): (Clause 9.3) In order to help implementers clearly understand the security processes defined in this document, a description of the processes for implementing security should be included in the standard.

Author’s note: The following text should be added to clause 9 in the security policies sub-clause.

4.4.1 Secure frame generation

When a DEV wishes to send a secure frame, it shall obtain the appropriate keying material from the MAC PIB depending on the key indicated by the DME. If the DME indicates that the PICONET-MGMT key shall be used, the DEV shall use the key from the MACPIB_ManagementKeyInfo entry from the MAC PIB piconet security group parameters. If the DME indicates that the PICONET-DATA key shall be used, the DEV shall use the key from the MACPIB_DataKeyInfo entry from the MAC PIB piconet security group parameters. If the DME indicates that the PEER-MGMT key shall be used, the DEV shall use the key from the MACPIB_ManagementKeyInfo entry from the corresponding MAC PIB access control list group parameters table. If the DME indicates that the PEER-DATA key shall be used, the DEV shall use the key from the MACPIB_DataKeyInfo entry from the corresponding MAC PIB access control list group parameters table. If the DEV is unable to find the corresponding key that is to be used, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to UNAVAILABLE-KEY and shall not transmit the requested frame.

If the DEV is able to obtain the appropriate security suite and key from the MAC PIB, the DEV shall check to see if the last beacon was valid by obtaining the MACPIB_ValidBeacon value. If the last beacon was not valid, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to BAD-TIME-TOKEN and shall not transmit the requested frame. If the beacon was valid, the DEV shall apply the operations defined by the security suite using the key(s) to the frame. The time token included in the frame shall be the value found in the MACPIB_CurrentTimeToken and the SECID included in the frame shall be the value corresponding to the key being used.

The integrity code shall be computed on the entire frame up to the integrity code itself including the MAC header. The result of the integrity code computation shall be encrypted and placed in the integrity code field in the secure frame. The encryption operation shall be applied only to the integrity code, seeds that are being transmitted in a distribute key command or request key response command and the payload of data frames. The result of the encryption operation shall be inserted into the frame in the place of the data that was encrypted.

If any of the security operations fail, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to FAILED-SECURITY-CHECK and shall not transmit the requested frame.

If the security operations have been successfully performed and the payload field has been modified appropriately, the device shall then compute the FCS over the modified frame.

Comment (T): (Clause 9) The following table should be added at the end of the clause describing secure frame generation along with this text:

The key used to protect a particular frame depends on the purpose of the frame. In general, all secure commands between the PNC and other devices should be protected with the PNC management key. All secure data frames to or from the PNC, all secure broadcast frames and all secure beacons should be protected with the piconet group data key. For two DEVs that share a peer-to-peer security relationship, peer-to-peer management keys should be used for all secure commands and peer-to-peer data keys should be used for all secure data frames. If two DEVs in a secure piconet do not have a peer-to-peer security relationship, they may use the piconet group data key for secure commands and secure data frames transmitted between them. The following table summarizes which keys should be used for each type of frame.

Table 6—Key selection for secure frames

Frame type or command	None	PNC-DEV mgmt. key	Piconet group data key	Peer-to-peer mgmt. key	Peer-to-peer data key	Comment
Beacon frame			X			All secure beacon frames shall be protected by the group data key.
Immediate acknowledgement frame		X	X	X	X	Secure immediate acknowledgement frames should use the key used in the frame that is being acknowledged.
Delayed acknowledgement frame		X	X	X	X	Secure delayed acknowledgement frames should use the key used in the frame that is being acknowledged.
Data frame			X		X	Secure data frames between devices that share a peer-to-peer key shall use the peer-to-peer data key, otherwise they shall use the piconet group data key.
Association request	X					Association request commands shall not be secured with any key.
Association response	X					Association response commands shall not be secured with any key.
Disassociation request		X				
Disassocation response		X				

Table 6—Key selection for secure frames

Frame type or command	None	PNC-DEV mgmt. key	Piconet group data key	Peer-to-peer mgmt. key	Peer-to-peer data key	Comment
Authentication request	X					Authentication request commands shall not be secured with any key.
Authentication response	X					Authentication response commands shall not be secured with any key.
Challenge request	X					Challenge request commands shall not be secured with any key.
Challenge response	X					Challenge response commands shall not be secured with any key.
Request key		X		X		The management key for the relationship (peer-to-peer or PNC-DEV) shall be used for this command.
Request key response		X		X		The management key for the relationship (peer-to-peer or PNC-DEV) shall be used for this command.
Distribute key request		X		X		The management key for the relationship (peer-to-peer or PNC-DEV) shall be used for this command.
Distribute key response		X		X		The management key for the relationship (peer-to-peer or PNC-DEV) shall be used for this command.
De-authenticate				X		
New PNC announcement			X			
PNC handover		X				
PNC handover information		X				
PNC information request		X				
PNC information		X				
Probe		X	X	X		If the devices do not share an individual relationship, the piconet group data key shall be used. Otherwise, the management key (peer-to-peer or PNC-DEV) for the relationship shall be used.
Transmission sequence sync		X				

Table 6—Key selection for secure frames

Frame type or command	None	PNC-DEV mgmt. key	Piconet group data key	Peer-to-peer mgmt. key	Peer-to-peer data key	Comment
Channel time request		X				
Channel time status		X				
Channel status request		X	X	X		If the devices do not share an individual relationship, the piconet group data key shall be used. Otherwise, the management key for the relationship (peer-to-peer or PNC-DEV) shall be used.
Channel status response		X	X	X		If the devices do not share an individual relationship, the piconet group data key shall be used. Otherwise, the management key for the relationship (peer-to-peer or PNC-DEV) shall be used.
Remote scan request		X				
Remote scan response		X				
Transmit power change		X	X	X		If the devices do not share an individual relationship, the piconet group data key shall be used. Otherwise, the management key (peer-to-peer or PNC-DEV) for the relationship shall be used.
APS sleep request		X				
APS sleep response		X				
SPS change		X				
SPS configuration request		X				
SPS configuration response		X				
SPS inquiry		X				
SPS inquiry response		X				

4.4.2 Removing security from frames

When a DEV receives a secure frame, it shall obtain the appropriate keying material from the MAC PIB depending on the SECID and source address found in the frame. To find the correct key, the DEV shall first check the MAC PIB for an ACL entry that corresponds to a peer-to-peer relationship with the sending DEV

and that has a MACPIB_DataSECID or MACPIB_ManagementSECID that matches the received SECID. If no peer-to-peer ACL entry matches the received frame, the DEV shall check the MACPIB_PNCDataSECID and MACPIB_ManagementSECID to determine if it matches the received SECID. If either of these entries gives a match, the DEV shall use the security suite in the corresponding MACPIB_SecuritySuite and the key corresponding to the SECID. If an appropriate entry in the ACL cannot be found, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to UNAVAILABLE-KEY and shall not perform any additional operations on the received frame.

If the DEV is able to obtain the appropriate security suite and key from the ACL, the DEV shall compare the received time token to the value in the MACPIB_CurrentTimeToken. If the frame is a beacon frame, the DEV shall determine if the received time token is greater than the MACPIB_CurrentTimeToken. If the frame is not a beacon frame, the DEV shall determine if the received time token is equal to the MACPIB_CurrentTimeToken. If either of these checks fail, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to BAD-TIME-TOKEN and shall not perform any additional operations on the received frame. If the time token matches, the DEV shall apply the operations defined by the security suite to the frame.

Before the security operations have been performed and the payload field has been modified, the DEV shall check the FCS. The DEV shall also check that the time token in the frame corresponds to the value in the MACPIB_CurrentTimeToken. If the time token does not match, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to UNAVAILABLE-KEY and shall not perform any additional operations on the received frame

The decryption operation shall be applied only to the integrity code, seeds that are being transmitted in a distribute key command or request key response command and the payload of data frames. The result of the decryption operation shall be replaced into the received frame in the place of the encrypted data. The integrity code shall be computed on the entire frame with the decrypted data replacing the encrypted data up to the integrity code itself including the MAC header.

If any of the security operations fail, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to FAILED-SECURITY-CHECK and shall not perform any additional operations on the received frame.

If the security operations have been successfully performed and the frame has been modified appropriately, the device may then continue to process the frame.

4.4.3 Joining a secure piconet

If a DEV wishes to join a secure piconet, it should associate with the PNC in order to be assigned a local DEVID and time slots to perform the authentication process. Since the device must be associated before the authentication process has taken place, the association command and response should have the SEC field in the frame control field set to 0.

Once the DEV is associated, the PNC should allocate an MTS to allow the DEV to proceed with the authentication protocol as described in 9.9.1{xref}. Before the authentication process is initiated, the DEV and PNC should ensure that they will be able to successfully implement the authentication protocol. Once the DEV is associated, the DEV or PNC may choose to send probe commands to each other to request or transmit public key objects or to request or transmit preferred OIDs. When a public key object is received in a probe command before authentication, the DEV may choose to determine whether that public key would be accepted in an authentication protocol and update its ACL if desired. The DEV and PNC may also exchange additional information before authentication if desired.

After the DEV has associated and exchanged the desired information with the PNC, the DEV should initiate the authentication protocol. The authentication and challenge commands are designed to be used with secu-

rity turned off. In the authentication request command, the DEV should select either the security suite OID received in the association response or an OID received in a probe command after associating. Once the authentication protocol has been initiated, the DEV should follow the states and state transitions specified in 9.9.1.1 and 9.9.1.2 {xref}. While in the authentication process, the authentication commands should have the SEC field in the frame control field set to 0. If during the authentication process there is a security check failure of any kind, the DEV or PNC should return the appropriate error in the challenge response command or authentication response command respectively and exit from the authentication protocol.

4.4.4 Secure beacon processing

4.4.4.1 Generating secure beacons

A PNC in a piconet using security should send secure beacons protected with the piconet protection key stored in the MACPIB_DataKeyInfo field in the MAC PIB. For each superframe, the PNC should increment the time token stored in the MACPIB_CurrentTimeToken in the MAC PIB and transmit a secure beacon with the SEC field in the frame control field set to 1.

4.4.4.2 Receiving secure beacons

In order to maintain secure and reliable operations in the piconet, a DEV shall use the beacon to help maintain the current time token and the current key. When the DEV receives a secure beacon (a beacon with the SEC field in the frame control field set to 1), it shall verify that the time token is greater than the MACPIB_CurrentTimeToken, that the SECID matches the MACPIB_PNCSECID stored in the MAC PIB and that the integrity code passes. If all of these checks succeed, the DEV shall set the MACPIB_CurrentTimeToken to the received time token value and set the MACPIB_ValidBeacon to valid. If the time token is greater than the MACPIB_CurrentTimeToken, but the SECID does not match the MACPIB_PNCSECID, the device may set the MACPIB_CurrentTimeToken to the value in the beacon and send a key request command to the PNC to obtain the new key.

Comment (T): (Clause 9.4) The following descriptive text should be added to clause 9.4.

The security mode indicates in what manner a DEV shall utilize the entries in the MAC PIB piconet security group parameter and MAC PIB access control list group parameters. The security mode in use is determined by the MACPIB_SecurityOptionImplemented entry in the MAC PIB.

Comment (T): (Clause 9.4.1) The description of security mode 0 is not descriptive enough and should refer to a DEV operating in the mode, not a piconet operating in the mode. Recommend replacing the text in 9.4.1 with the following text:

A device operating in security mode 0 shall not utilize the ACL entries and shall not perform any security related operations on MAC frames. While in this mode, if the MAC receives a frame with the SEC field set to 1, the MAC shall discard the frame and the MLME shall return an MLME-SECURITY-ERROR.indication to the higher layer with the ReasonCode set to UNAVAILABLE-KEY. If the MAC receives a frame with the SEC field set to 0, the MLME shall set the SecurityUse and ACLEntry fields to FALSE in the indication to the DME.

Comment (T): (Clause 9.4.2) The description of security mode 1 is not descriptive enough and should refer to a DEV operating in the mode, not a piconet operating in the mode. Recommend replacing the text in clause 9.4.2 with the following text:

Security mode 1 provides a mechanism for the MLME of a PNC to indicate to the DME if a received frame purportedly originated from a device in the ACL. The PNC may use this information as a criterion for allowing a device into the piconet. A device operating in security mode 1 shall not perform any security related operations on MAC frames. While in this mode, if the MAC receives a frame with the SEC field set to 1, the

MAC shall discard the frame and the MLME shall return an MLME-SECURITY-ERROR.indication to the higher layer with the ReasonCode set to UNAVAILABLE-KEY. If the MAC receives a frame with the SEC field set to 0, the MLME shall set the SecurityUse field to FALSE and the ACLEntry field to TRUE or FALSE depending on if the sender is in the ACL in the indication to the higher layer.

Comment (T): (Clause 9.4.3) The description of security mode 2 is not descriptive enough and should refer to a DEV operating in the mode, not a piconet operating in the mode. Recommend replacing the text in clause 9.4.3 with the following text:

Security mode 2 provides a mechanism for a device to perform cryptographic security on frames transmitted in the piconet. DEVs operating in security mode 2 use public-key cryptography to verify the authenticity of other DEVs in the piconet and symmetric-key cryptography to protect frames using encryption and integrity. The cryptographic operations used for secure frames exchanged with the PNC and with other members of the piconet security group shall be performed as specified by the security suite indicated in the MACPIB_SecuritySuite in the MAC PIB piconet security group parameters. The cryptographic operations performed for secure frames exchanged with a peer DEV shall be performed as specified by the security suite indicated in the MACPIB_SecuritySuite entry associated with that peer security relationship in a MAC PIB access control list group parameters table. While in this mode, the MAC may accept frames with the SEC field in the frame control field set to 1 or 0 and shall set the SecurityUse in the MLME message to the DME to TRUE or FALSE respectively.

Comment (T): (Clause 9.4.4) The description of security mode 3is not descriptive enough and should refer to a DEV operating in the mode, not a piconet operating in the mode. Recommend replacing the text in clause 9.4.4 with the following text:

Security mode 3 provides a mechanism for a device to perform cryptographic security on frames transmitted in the piconet. DEVs operating in security mode 3 use public-key cryptography and public-key certificates to verify the authenticity of other DEVs in the piconet and symmetric-key cryptography to protect frames using encryption and integrity. The cryptographic operations used for secure frames exchanged with the PNC and with other members of the piconet security group shall be performed as specified by the security suite indicated in the MACPIB_SecuritySuite in the MAC PIB piconet security group parameters. The cryptographic operations performed for secure frames exchanged with a peer DEV shall be performed as specified by the security suite indicated in the MACPIB_SecuritySuite entry associated with that peer security relationship in a MAC PIB access control list group parameters table. While in this mode, the MAC may accept frames with the SEC field in the frame control field set to 1 or 0 and shall set the SecurityUse in the MLME message to the DME to TRUE or FALSE respectively.

4.5 Clause 10 comments

Comment (TR): (Clause 10.2.2) The mandatory to implement sub-suite should be less expensive and easier to implement than the current mandatory to implement sub-suite (ECIES-prime-256 raw 1). A security suite based on the RSA algorithm should be made mandatory.

Comment (TR): (Clause 10) The RSA-OAEP based security suite proposed in document {xref} should be inserted into the draft and made the mandatory to implement algorithm.

Comment (TR): (Table 82, pg. 259) The challenge response generation entry and the authentication response generation entry should add the following sentence at the end:

The secure frame counter used in the CCM nonce shall be the 2-byte string 0x0000.

5. Notes

Are sub-rate slots allowed to be pseudo-static?

Clarify 3 modes, 2 state (should already be comment).