IEEE P802.15
Wireless Personal Area Networks

Project	IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)	
Title	**TG3 SB1 comment resolution**	
Date Submitted	[21 February, 2003	
Source	[James P. K. Gilb] [Appairent Technologies] [15373 Innovation Drive, #210, San Diego, CA 92129]	Voice: [858-485-6401] Fax: [858-485-6406] E-mail: [gilb@ieee.org]
Re:	[]	
Abstract	[This document is a record of comment resolutions for SB1.]	
Purpose	[To provide a record of the comment resolution for SB1.]	
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. Conference calls

1.1 Tuesday, 18 February 2003

Attendees: Jay Bain, Mark Schrader, Allen Heberling, Bill Shvodian, James Gilb, John Barr, Jim Allen

Concatenation (left/right, new figures, etc.) for AES-CCM

> Put in the changes proposed by Ari Singer.

Do we keep a security information command to take the place of the old authentication, challenge and de-authentication commands?

> Add security message command, formatted like vendor specific, with .request, .indication and .confirm, ACK with timeout gives the confirm. (COMPLETED, TIMEOUT)

When to we send an MLME-yyy.confirm for assocaition and channel time requests

> Move MLME-ASSOCIATION.confirm to just after the ACK is sent for the association request. Move the MLME-STREAM-CREATE.confirm (and MODIFY) to just after the ACK for the Channel Time Response command.

Other issues

Page 202, line 51: What is a SECID IE?

> Change to just SECID

Page 42, Table 11: SECID: As defined in 7.2.7.2, but 7.2.7.2 just says it is a 2 octet field. The actual contents of the field are described in 9.3.6. On page 113, line 31 change "protect the frame." to "protect the frame, {xref 9.3.6}.".

> Either xref to 9.3.6 or move the explict definition to clause 7

Page 43, line 7, 6.3.7.1: The SECID is not required in the request. It is not sent in the frame and does not appear in the indication. Remove "SECID,". Need to also remove the "designated key" from line 16. Replace with "shared key"?

> Delete SECID from 6.3.7.1 because it isn't in the frame format.

6.3.9: KeyType implies that BOTH keys can be sent with this command, but KeyInfo only passes one key. Suggest that we make it only possible to update one key at a time and when the Management key is updated, MembershipStatus is used to determine whether authenticated or not. Until the data key is received, only frames using the Management key are allowed.

> Suggest, delete BOTH, change the text to indicate that when the management key is deleted, the data key is deleted as well. Add text to clause 9 that indicates the way that this MLME is used.

Schedule: Draft is ready to go out on the 20th, possible SB start on the 21st, last comments for changes are due midnight PST on February 19.

Meeting adjourned at 9:04 am PST.

1.2 Thursday, 13 February 2003

Agenda

- Roll call
- Resolution for CID 45, 82 (see below)
- Security issues
  - Starting value of SECID (CID 18)
  - Other security issues (see below).
- Draft status
- Assignments for review
- Adjourn

Attendees: James Gilb, Ari Singer, John Barr, Allen Heberling, Bill Shvodian, Dan Bailey, Jay Bain, John Sarallo

Meeting called to order at: 9:08 am, PST.

CID 45 - A total of three octets would be used for DEV capabilities. Part of one would include the fragmentation preference (as for the 2.4GHz PHY). The other two would have additional PHY characteristics. For now, the rate bits would be aligned to the right of the 16 bits available. The three octets would be in 7.4.12, 7.5.1.1, and 7.5.4.2. For 7.4.4, the octet with the frag preference would not be present so the total there would be two octets instead of the current single octet.

I believe the change is only within clause 7.

> OK, current fields stay the same number of bits, the rest are reserved.

CID 82 - The change for the remote scan remains that text in clause 7 would allow for an IE to be located within the remote scan result command. It would not be present for this PHY. Again, the change is local to clause 7.

> Add an IE, specified to be used for future extensions. Currently ignored by the PNC and set to the undefined element ID, xref table 50, with zero length.

1.3 Security issues

CID 18 - What is the SECID when the piconet starts? What about the key? What if no one is in it?

> Add text that says when the piconet is started and it is operating in mode 1, the PNC selects a SECID and key to be used for beacon protection, even though this key is not sent to any other DEV. Add to end of 9.3.9 Selecting SECID for new keys.

From John Barr:

Page 231, lines 3-7: Delete "Recognizing the diversity ... cryptography." and "The instantiation ... suite." and "The background ... Annex C.1." Replace with "This standard supports the implementation of an authentication protocol between DEVs and between a DEV and the PNC. It also supports protection of command and data frames using an 128-bit AES security suite, and the distribution of keys for command and data frame protection." You might want to elaborate, but this is better than what is there.

> Wireless networks face unique security challenges and piconets are no exception. Recognizing the diversity of piconet applications and entities, this standard supports two different modes of security,

no security and the use of strong cryptography. The standard support the protection of command and data frames using an 128-bit AES security suite, and the distribution of keys for command and data frame protection.

The background assumptions used in designing this security solution are outlined in Annex B.1.

Change 9.1 "Security services" to "Security Mechanisms". Change "services are protections offered on communications" to "mechanisms are available for use".

Accept.

Delete section 9.1.1 entirely

Accept.

Lines 23-24: Change "An authentication protocol ... within a piconet. This protocol" to "The authentication and challenge commands".

Subclause deleted.

Line 33: Change "Authentication methods" to "Authentication protocols and policies".

Subclause deleted

Lines 37-38: Change "of a shared key or keys" to "of management and payload protection keys".

Subclause deleted.

Page 232, Line 26: Change "key(s)" to "key". Only the management key is used to protect commands.

Accept. Fixed everywhere it occurs in the draft where appropriate.

Delete last paragraph, lines 47-51. No such thing as an ACL any longer in the MAC.

Accept.

Page 233, lines 1-7: The new MAC does not differentiate between security suites. Only mode that is really defined is symmetric security for command and data protection. We don't get into how a security suite/system performs authentication.

Accept in principle, only ref symmetric key security operations.

Delete sections 9.2.2.1 and 9.2.2.2.

Put information from 9.2.2.1 into Annex C, if not already there.

Line 26: Change "Security policies" to "Security Support"

Accept.

Line 29: Change "requirements and recommendations for the use of security in the piconet." to "now this standard can be used to support specific security policies."

‘The following sub-clauses specify the methods that are provided in this standard to support specific security policies.’

Line 33: Delete "provided by this standard"

Accept

Line 49: Change "Sound security practice indicates that only" with "Only"

Accept.

Line 49: Change "piconet would be" to "piconet should be"

Accept in principle ‘piconet are’

Page 234, lines 7-11: Is this policy or a mechanism.

Text OK as is, this behavior is required.

Lines 13-20: No more ACL. We have security information instead.

Accept. Change to Security Information, Security Information Request and security information.

Line 42: Not sure "device shall be associated" is correct. What does this have to do with setting the SEC field to 0?

Sentence deleted.

Line 49: Change "the DEV should initiate" to "the DEV shall initiate"

Accept in principle, see new text: ‘After the DEV has associated and exchanged the desired information with the PNC, the DEV shall establish secure membership. The process by which secure membership is established is outside of the scope of this standard.’

Section 9.3.6: Most of this paragraph seems right, but at the end I am left with the question of just what does the standard provide for implementation of an authentication protocol. I think we should be answering "What can be done by an external DME to implement an authentication protocol?" We have the authentication request/reply and the challenge request/reply messages that can be used as part of the authentication protocol.

Accept in principle, Vendor Specifics commands have been allowed for this process.

Page 239, line 47: Is it a "Security suite" or a "Security system" that is identified by an OID? Two DEVs need to agree on which security system they are going to use for a security relationship. Once decided, the two security systems communicate via the authentication/challenge commands. If a DEV supports more than one security system, the OID will need to be included in those commands to make sure the MAC passes the command frame information to the right security system manager.

Subclause 9.4 deleted.

Page 240, lines 3-23: Are these sections really needed? They don't really define how the MAC interoperates. If we think of just providing what a security system requires as a special communications path, we don't really need to know what the data formats, protocol operations, and cryptographic implementations are. We just provide a container to carry information between the client and server parts.

Subclause 9.4 deleted.

Why is more than one key implied? Page 142, Line 49: "The integrity code is generated using the management keys that are shared ..." Page 143, Line 20: "This command shall be protected using the management keys that are shared ..." Page 143, Line 36: ibid. In the definition of the symmetric security suite the management key (singular) is the only key defined. Change all occurrences of keys and key(s) regarding management key usage to be singular instead of plural.

Accept. In some locations both keys (data and management) are referred to and in others it refers to keys in a general fashion.

Page 240, line 42: "The protocols in this clause are algorithm independent and may be used for any security suite". This sentence is left over from earlier. It is my understanding that we are using AES-128 symmetric keys as the management key and the data protection key. Delete the line.

Accept.

Page 240, Line 52-53: Delete ", but it does not need to store the public keys of these DEVs". Change "keys" to "key" in the first part of this sentence as well.

Accept.

Page 241+: Using "key(s)" in various places. I think we need to clearly state which key is used for what if "key(s)". It is not clear which keys are being use. We only have a management key and a data protection key.

Accept.

Pages 240-244: Delete clauses 9.5, 9.6, and 9.7. Update clause 9.8 to use same notation as in clauses 6, 7, and 8 instead of introducing an extremely confusing and possibly incorrect intermediate notation.

Delete 9.5, 9.6, 9.7, 9.8.4, 9.8.5, Table 70, Table 71, Table 72, Table 73, Figure 157, Figure 160

Page 244: Delete lines 29-33: Again the setup tables and capabilities tables are redundant and not required. Just confusing.

Deleted as above.

Page 244, Lines 40-43: Delete sentence "Therefore it is assumed ... in the MAC PIB." Implementation specific which is out of our scope.

Delete ‘through information stored in the MAC PIB.’
(all edits up to this point have been applied).

Page 245, clause 9.8.2.1: Figure 152 has an interface to the MLME and the state machines. This clause talks about frames, but there are no connections in Figure 152 to obtain frames. I think we have a much simpler architecture now and clause 9 does not reflect this simplicity. For example:

Unassociated -> associated/unauth upon completion of association protocol (clause 8)

associated/unauth -> associated/authenticated upon receipt of successful authentication response and SECID_UPDATE command from MLME.

associated/authenticated -> associated/unauthenticated upon receipt of valid

deauthentication command.

All commands are formed based on current associated and authenticated state using the management (SECID_UPDATE) or data protection (Distribute_Key or Request_key response) key information maintained in the MAC.

A new data protection key is established upon receipt of a Distribute_Key command from a valid key originator. The MAC has the management key from a SECID_UPDATE. A new data protection key can also be established using the Request_Key protocol when a SECID gets changed.

The changes required should be easy for someone familiar with the secure exchange of keys and such. Right now I think it is much too complicated and it needs to be rewritten before final approval.

Stopped here, meeting adjourned at 10:40 am PST.

Page 244, Lines 23-25: Delete "The algorithm choices for each operation in the protocols are determined by the selected security suites, which are specified in clause 10." We only have a single symmetric security suite defined.

Page 274, Lines 43-45: Delete "All of the sub-suites defined in this standard perform symmetric operations in the same manner as specified in this subclause." No sub-suites defined any more, just the symmetric suite.

Page 61+, clause 6.3.14: "ACL information retrieval" should be changed to "Security Information Exchange". Please correct as agreed in Ft. Lauderdale.

Clause 4: Remove ACL Acronym from list.

Page 16, Lines 9-11: Change "The PNC is allowed to use an access control list (ACL) to admit or deny entry to the piconet. The PNC uses the address of the DEV to determine if it will be allowed access to the piconet." to "The PNC allows the DME to determine whether any DEV is allowed to be a member of the piconet."

Page 55, Line 7: We no longer have an ACL, only a table of SECIDs. Change "find the designated key in the ACL" to "resolve the SECID".

Page 56, line 18: Change "find an appropriate key in the ACL" to "match the received SECID with a known SECID".

Page 56, Line 20-21: Change "according to the security suite or for which the DEV is unable to find the designated key in the ACL" to "or for which the DEV does not have a known SECID matching the received SECID".

Page 137, table 52: Update to replace ACL with Security Information.

Page 147, clauses 7.5.4.3 and 7.5.4.4 need to be updated to remove ACL and replace with the agreed on security information formats.

Page 168, line 13-14: Change "ACL handover" to "Security information handover"

Page 175, lines 3-7: Change "The PNC may maintain an access control list (ACL) of DEV addresses that are allowed to join the piconet. If the ACL is in use, when the PNC receives an association request command, the PNC shall consult the ACL to determine if the DEV address in the request is included in the ACL. If the DEV address is not in the ACL, the PNC shall send an association response command with the reason code set to "association denied", 7.5.1.2, indicating that the association failed." to "The PNC allows the DME to selectively deny association of any DEV. If the DME denies the association of any DEV, the PNC shall send an association response command with the reason code set to "association denied", 7.5.1.2, indicating that the association failed."

Clauses 9.2.2, 9.3.4, 9.8.3 also contain references to ACL that need to be changed to Security Information.

Page 351, lines 40-21: ACL information request and ACL information need to be changed to security information in table E-3.

page 355, line 44-45: ACL info handover should be Security info handover in table E-5.

1.4 Tuesday, 11 February 2003

Agenda:

- Roll call
- Editorial issues
- New probe command
  - Security issues (ref 03/032r11 and email from A. Singer)
    -References to security suites and OIDs in the draft, without making any statements about what they are or how they work exactly.
    - Changes proposed in 334 and 336, right/left first/last in describing bit ordering.

- There are some security policies that are included with the words "may" or "should" in clause 9 to give some guidance to implementers on how to use the MAC commands. Are these appropriate?
- Text CID 340.
- Is CID 342 resolved the way the group wants? The sections describing security analysis for the public-key stuff were removed.
- The resolution for CID 345 should be changed to indicate that the entire sub-clause was removed.
- Merge Annex B and Clause 10 since they are both reasonably small now and cover related topics?
- Draft status and schedule
- Next meeting
- Adjourn

Attendees: James Gilb, Ari Singer, Jay Bain, Bill Shvodian, Allen Heberling, Rene Struik, Dan Bailey, John Sarallo.

Meeting called to order at 8:10 am PST.

1.4.1 Editorial issues: (all E comments)

CID 440 - Rename MLME-ASIE-CREATE to MLME-ASIE-UPDATE?

Reject, keep current naming.

CID 217 - Apparently, IntServ - type QoS might be able to be supported, beyond 802.1p. Please state such.

‘802.15.3 only has the priorities as a parameter. It doen’t specify a bandwidth manager nor does it have policing, shaping or other IntServ stuff. It doesn’tt even specify the jitter for reasons that are fairly obvious in wireless design.

It is true that it is possible to pass IntServ data packets over a piconet, but so you can with any other data, be it Diffserv, RSVP, 1394....

Accept in principle: ‘An implementer is allowed to send IntServ packages and define IntServ policy functions in the FCSL, but that it would be out of scope of the standard. Other QoS services would also be supported, e.g. Diffserv, RSVP, 1394, etc.’”

1.4.2 New probe commands?

CLAUSE 3 CHANGES

Page 6 Line 5:

Replace

“A beacon followed by one or more broadcasted probe commands from the piconet controller.”

with

“A beacon followed by one or more broadcasted Announce commands from the piconet controller.”

CLAUSE 5 CHANGES

Page 16 Line 33:

Replace

"The beacon consists of the beacon frame, 7.3.1, as well as any Probe commands sent by the PNC as a beacon extension, 8.6.3."

with

"The beacon consists of the beacon frame, 7.3.1, as well as any Announce commands sent by the PNC as a beacon extension, 8.6.3."

Page 18 Line 32:

Replace

"This standard supports three methods for discovering information about other DEVs in the piconet: the PNC information request command, the Probe command and the piconet services information element."

with

"This standard supports four methods for discovering information about other DEVs in the piconet: the PNC Information Request command, the Probe Request command, the Announce command and the Piconet Services IE."

Page 18 Line 46:

Replace

"A DEV uses the Probe command, 8.9.2, to find out more detailed information about other DEVs in the piconet. This command allows the originating DEV to retrieve any valid information element, 7.4, from a target DEV in the piconet. In addition, the target DEV is able to request information from the originating DEV during this process."

with

"A DEV uses the Probe Request command, 8.9.2, to find out more detailed information about other DEVs in the piconet. This command allows the originating DEV to retrieve any valid information element, 7.4, from a target DEV in the piconet."

CLAUSE 6 CHANGES

Table 3:

Replace

MLME-PROBE	6.3.16.1	6.3.16.2	6.3.16.3	6.3.16.4

with

Page 66 Line 24:

MLME-PROBE	6.3.16.1	6.3.16.2	6.3.16.3	6.3.16.4
MLME-ANNONUCE	{xref}	{xref}		{xref}

Replace

"If the request fails, the PNC DME may decide to send the ASIE with the Probe command, 7.5.4.5. It also may try to send the ASIE in another beacon."

with

"If the request fails, the PNC DME may decide to send the ASIE with the Announce command, 7.5.4.5. It also may try to send the ASIE in another beacon."

Page 67 Line 1:

Replace Clause 6.3.16 with the following:

(begin new text)

1.4.3 Peer information retrieval

The MLME-PROBE primitives are used to request information about other DEVs in the piconet. The parameters used for the MLME-PROBE primitives are defined in Table 1.

Table 1—MLME-PROBE primitive parameters

Name	Type	Valid range	Description
TrgtID	Integer	Any valid DEVID as defined in 7.2.3.	Specifies the DEVID of the target of the MLME request.
OrigID	Integer	Any valid DEVID as defined in 7.2.3.	Specifies the DEVID of the DEV that initiated the MLME request.
InformationRequested	4 octets	As defined in {xref}.	Indicates which information elements are requested as defined in {xref}.
InformationElements	Variable number of octets.	As defined in {xref}.	The information elements sent or received in the Probe command, as defined in {xref}.
ProbeTimeout	Duration	0-65535	The time in milliseconds by which the operation initiated by the MLME request needs to be completed before responding with a ResultCode of TIMEOUT.
ResultCode	Enumeration	SUCCESS, TIMEOUT	Indicates the result of the MLME request.

1.4.3.1 MLME-PROBE.request

This primitive initiates a request for a list of selected information elements from a target DEV. The semantics of this primitive are:

```
MLME-PROBE.request      (
                        TrgtID,
                        InformationRequested,
                        ProbeTimeout
                        )
```

The primitive parameters are defined in Table 1.

1.4.3.1.1 When generated

The originating DME sends this primitive to its MLME when it wants to request information from another DEV in the piconet.

1.4.3.1.2 Effect of receipt

The MLME, upon receiving this primitive, sends the Probe Request command, {xref}, to the target DEV specified by the TrgtID. The use of the Probe Request command is described in {xref}.

1.4.3.2 MLME-PROBE.indication

This primitive indicates the reception of a request for a list of selected information elements. The semantics of this primitive are:

```
MLME-PROBE.indication   (
                        OrigID,
                        InformationRequested
                        )
```

The primitive parameters are defined in Table 1.

1.4.3.2.1 When generated

This primitive is sent by the MLME to its DME upon receiving a Probe Request command, {xref}.

1.4.3.2.2 Effect of receipt

The DME upon receiving this primitive sends an MLME-PROBE.response to its MLME.

1.4.3.3 MLME-PROBE.response

This primitive initiates a response to an MLME-PROBE.indication. The semantics of this primitive are:

```
MLME-PROBE.response     (
                        OrigID,
                        InformationElements
                        )
```

The primitive parameters are defined in Table 1.

1.4.3.3.1 When generated

The DME sends this primitive to its MLME in response to an MLME-PROBE.indication.

1.4.3.3.2 Effect of receipt

The MLME upon receiving this primitive sends a Probe Response command, {xref}, to the requesting DEV specified by the OrigID.

1.4.3.4 MLME-PROBE.confirm

This primitive informs the originating DME that its request for DEV information elements from a target DEV is complete. The semantics of this primitive are:

```
MLME-PROBE.confirm      (
                        TrgtID,
                        InformationElements,
                        ResultCode
                        )
```

The primitive parameters are defined in Table 1.

1.4.3.4.1 When generated

The MLME sends this primitive to its DME upon receiving a Probe Response command, {xref}, or a TIME-OUT.

1.4.3.4.2 Effect of receipt

The originating DME upon receiving this primitive is informed whether the request for the list of information elements from the target DEV was successful or unsuccessful. If unsuccessful, the DME may resend the MLME-PROBE.request with the same list of requested information elements. If successful, the DME will have acquired the information it requested from the target DEV and may initiate another MLME-PROBE.request to either the same target DEV or a different target DEV.

1.4.3.5 Information announcement to peers

The MLME-ANNOUNCE primitives are used by a DEV to send information about itself to other DEVs in the piconet. The parameters used for the MLME-ANNOUNCE primitives are defined in Table 2

1.4.3.6 MLME-ANNOUNCE.request

This primitive initiates a request to send selected information elements to a target DEV. The semantics of this primitive are:

```
MLME-ANNOUNCE.request   (
                        TrgtID,
                        InformationElements
                        )
```

The primitive parameters are defined in Table 2.

Table 2—MLME-PROBE primitive parameters

Name	Type	Valid range	Description
TrgtID	Integer	Any valid DEVID as defined in 7.2.3.	Specifies the DEVID of the target of the MLME request.
OrigID	Integer	Any valid DEVID as defined in 7.2.3.	Specifies the DEVID of the DEV that initiated the MLME request.
InformationElements	Variable number of octets.	As defined in {xref}.	The information elements sent or received in the Probe command, as defined in {xref}.
AnnounceTimeout	Duration	0-65535	The time in milliseconds by which the operation initiated by the MLME request needs to be completed before responding with a ResultCode of TIMEOUT.
ResultCode	Enumeration	SUCCESS, TIMEOUT	Indicates the result of the MLME request.

1.4.3.6.1 When generated

The originating DME sends this primitive to its MLME when it wants to request to send information to another DEV in the piconet.

1.4.3.6.2 Effect of receipt

The MLME, upon receiving this primitive, sends the Announce command, {xref}, to the target DEV specified by the TrgtID. The use of the Announce command is described in {xref}.

1.4.3.7 MLME-ANNOUNCE.indication

This primitive indicates the reception of selected information elements from a DEV. The semantics of this primitive are:

```
MLME-ANNOUNCE.indication    (
                            OrigID,
                            InformationElements
                            )
```

The primitive parameters are defined in Table 2.

1.4.3.7.1 When generated

This primitive is sent by the MLME to its DME upon receiving a Announce command, {xref}.

1.4.3.7.2 Effect of receipt

The DME upon receiving this primitive obtains selected information from the originating DEV.

1.4.3.8 MLME-ANNOUNCE.confirm

This primitive informs the originating DME that its request to send information elements to a target DEV is complete. The semantics of this primitive are:

```
MLME-ANNOUNCE.confirm    (
                         TrgtID,
                         ResultCode
                         )
```

The primitive parameters are defined in Table 2.

1.4.3.8.1 When generated

This primitive is sent by the originating MLME to its DME after sending an Announce command, {xref}, and either receiving an ACK or an ACK_TIMEOUT. The result code is set to SUCCESS if an ACK was received, and to ACK_TIMEOUT if successful reception of the command is never acknowledge by the TrgtID.

1.4.3.8.2 Effect of receipt

The originating DME upon receiving this primitive is informed whether the request to send information elements to the target DEV was successful or unsuccessful. If unsuccessful, the DME may resend the MLME-ANNOUNCE.request with the same list of information elements. If successful, the DME will have successfully sent the requested information elements to the target DEV and may initiate another MLME-ANNOUNCE.request to either the same target DEV or a different target DEV.

(end new text)

CLAUSE 7 CHANGES

Table 50:

Remove CTA Status Request IE from the table and renumber remaining IEs.

Page 131 Line 44:

Remove Clause 7.4.10.

Page 135 Line 35:

Replace

“If multiple security suite OID information elements are present in the same Probe command, they shall be considered to be listed in order of preference with the first OID transmitted being the highest preference and the last OID transmitted being the lowest preference.”

with

“If multiple security suite OID information elements are present in the same Probe Response command or Announce command, they shall be considered to be listed in order of preference with the first OID transmitted being the highest preference and the last OID transmitted being the lowest preference.”

Table 52:

Replace

0x0013	Probe	7.5.4.5	X	

with

0x0013	Probe request	7.5.4.5	X	
0x0014	Probe response	{xref 7.5.4.6	X	
0x0015	Announce	{xref 7.5.4.7}	X	

and adjust the Command Type values for the remainder of the Command names.

Page 145 Line 43:

Replace

"This set of commands is used to obtain information about another DEV in the piconet. The PNC information commands are used to retrieve data about any or all of the currently associated DEVs in the piconet. The Probe command deals with the information elements of a specific DEV."

with

"This set of commands is used to obtain information about another DEV in the piconet. The PNC information commands are used to retrieve data about any or all of the currently associated DEVs in the piconet. The ACL information commands are used to retrieve authentication data about any or all of the currently associated DEVs in the piconet. The Probe commands are used to retrieve information elements from a specific DEV in the piconet."

Page 148 Line 4:

Replace Clause 7.5.4.5 with the following text:

(begin new text)

1.4.3.9 Probe request

The Probe Request command is used to request information about a DEV or to see if a DEV is still present in the piconet. The Probe Request command shall be formatted as illustrated in Figure 1.

1	4	1	2
Stream index	Information requested	Length (=5)	Command type

Figure 1—Probe request command format

The Information Requested field shall be formatted as illustrated in Figure 2.

bits: b31-b1	b0
IE(s) requested	IE request type

Figure 2—Information requested field format

The IE Request Type field indicates how to interpret the IEs requested field. This field shall be set to 0 if the IEs Requested field is a bit map and shall be set to 1 if the IEs Requested field is a binary encoding of the information element's ID.

If the IE Request Type field indicates that the IEs Requested field is a bit map, then the sender shall set a value of 1 in a bit to request the information element that corresponds to the bit position. Otherwise, the sender shall set the bit to 0. The bit position for an information element is same as the value of the element-ID for that information element. That is, the bit position of *n* in information request field corresponds with the information element whose element ID, Table 50, is *n*.

If the IE Request Type field indicates that the rest of the bits are binary coded, then the IEs Requested field contains the element ID of the information element that is being requested by the sender of this command from its intended recipient.

Both the IE Request Type field and the IEs Requested field shall be set to 0 when the source DEV is not requesting any information from the destination DEV.

If the Information Requested field indicates that the CTA Status IE, {xref 7.4.11}, is being requested from the destination DEV, the Stream Index field is set to the stream index of the stream for which CTA information is requested. If the Stream Index field is set to 0, the DEV is requesting information about all isochronous streams directed to the requesting DEV and to the BcstId and McstId. If the Information Requested field indicates that the CTA Status IE is not being requested from the destination DEV, the Stream Index field has no meaning and shall be set to 0.

Table 4 lists the rules that shall apply to requesing an IE from another DEV based on the sender of the request.

Table 3—Rules for requesting IEs in a Probe Request command

Information element	Subclause	PNC allowed to request	DEV allowed to request
Channel time allocation	7.4.1	Shall not request	Shall not request
BSID	7.4.2	Shall not request	May request
Parent piconet	7.4.3	Shall not request	May request
DEV association	7.4.4	Shall not request	Shall not request
PNC shutdown	7.4.5	Shall not request	Shall not request
Piconet parameter change	7.4.6	Shall not request	Shall not request
Application specific	7.4.7	May request	May request
Pending channel time map (PCTM)	7.4.8	Shall not request	May request
PNC handover	7.4.9	Shall not request	Shall not request
CTA status	7.4.11	Shall not request	May request
Capability	7.4.12	May request	May request
Transmit power parameters	7.4.13	May request	May request
PS status	7.4.14	Shall not request	Shall not request
Continued wake beacon (CWB)	7.4.15	Shall not request	Shall not request
Security suite OID	7.4.16	May request	May request
Overlapping PNID	7.4.17	May request	Shall not request
Piconet services	7.4.18	May request	May request
Vendor specific or reserved	7.4	May request	May request

1.4.3.10 Probe response

The Probe Response command is used to return information about a DEV to a requesting DEV. The individual information elements used in this frame are described in 7.4. The Probe Response command shall be formatted as illustrated in Figure 3.

octets: n	2	2
IEs Provided	Length (=n)	Command type

Figure 3—Probe response command format

The IEs Provided field contains the information elements, 7.4, that the source DEV of this command is providing to the destination. The elements themselves may be placed in any order.

Table 5 lists the rules that shall apply to responding to a request for an IE based on the sender of the request.

Table 4—Rules for sending IEs in a Probe Response command

Information element	Subclause	DEV received request from DEV	DEV received request from PNC	PNC received request from DEV
Channel time allocation	7.4.1	Shall ignore	Shall ignore	Shall ignore
BSID	7.4.2	Shall ignore	Shall ignore	Shall respond
Parent piconet	7.4.3	Shall ignore	Shall ignore	Shall respond
DEV association	7.4.4	Shall ignore	Shall ignore	Shall ignore
PNC shutdown	7.4.5	Shall ignore	Shall ignore	Shall ignore
Piconet parameter change	7.4.6	Shall ignore	Shall ignore	Shall ignore
Application specific	7.4.7	May respond	May respond	May respond
Pending channel time map (PCTM)	7.4.8	Shall ignore	Shall ignore	Shall respond
PNC handover	7.4.9	Shall ignore	Shall ignore	Shall ignore
CTA status	7.4.11	Shall ignore	Shall ignore	May respond
Capability	7.4.12	Shall respond	Shall respond	Shall respond
Transmit power parameters	7.4.13	Shall respond	Shall respond	Shall respond
PS status	7.4.14	Shall ignore	Shall ignore	Shall ignore
Continued wake beacon (CWB)	7.4.15	Shall ignore	Shall ignore	Shall ignore
Security suite OID	7.4.16	Shall respond	Shall respond	Shall respond
Overlapping PNID	7.4.17	Shall ignore	May respond	Shall ignore
Piconet services	7.4.18	May respond	May respond	May respond
Vendor specific or reserved	7.4	May respond	May respond	May respond

Page 151 Line 1:

Replace Clause 7.5.4.6 with the following text:

1.4.4 Information announcement commands

This set of commands is used to announce information about a DEV or DEVs to one or all of the DEVs in the piconet. The Piconet Services command is sent by the PNC to provide information about the application layer capabilities of all of the DEVs in a piconet. The Announce command is used to send information about a DEV to one or more DEVs in the piconet.

1.4.4.1 Piconet services

The piconet services command is sent by the PNC to provide information about the application layer capabilities of all of the DEVs in a piconet. The piconet services command shall be formatted as illustrated in Figure 4

octets: L_n	…	L_2	L_1	2	2
Piconet services IE n	…	Piconet services IE-2	Piconet services IE-1	Length (=sum of L_1-L_n))	Command type

Figure 4—Piconet services command format

The Piconet Services IE is defined in 7.4.18.

1.4.4.2 Announce

The Announce command is used to send unrequested information about a DEV to one or more DEVs in the piconet. The individual information elements used in this frame are described in 7.4. The Announce command shall be formatted as illustrated in Figure 5.

octets: n	2	2
IEs Provided	Length (=n)	Command type

Figure 5—Announce command format

The IEs Provided field contains the information elements, 7.4, that the source DEV of this command is providing to the destination. The elements themselves may be placed in any order.

Table 5 lists the rules that shall apply to sending an unrequested IE based on the sender of the request.

Table 5—Rules for sending IEs in an Announce command

Information element	Subclause	PNC sends	DEV sends
Channel time allocation	7.4.1	Shall not send	Shall not send
BSID	7.4.2	Shall not send	Shall not send
Parent piconet	7.4.3	Shall not send	Shall not send
DEV association	7.4.4	May send	Shall not send
PNC shutdown	7.4.5	May send	Shall not send
Piconet parameter change	7.4.6	May send	Shall not send
Application specific	7.4.7	May send	May send
Pending channel time map (PCTM)	7.4.8	May send	Shall not send

Table 5—Rules for sending IEs in an Announce command

Information element	Subclause	PNC sends	DEV sends
PNC handover	7.4.9	May send	Shall not send
CTA status	7.4.11	May send	Shall not send
Capability	7.4.12	May send	May send
Transmit power parameters	7.4.13	May send	May send
PS status	7.4.14	May send	Shall not send
Continued wake beacon (CWB)	7.4.15	Shall not send	Shall not send
Security suite OID	7.4.16	May send	May send
Overlapping PNID	7.4.17	Shall not send	May send
Piconet services	7.4.18	May send	May send
Vendor specific or reserved	7.4	May send	May send

CLAUSE 8 CHANGES

Page 177 Line 10:

Replace

"DEVs that are members of the piconet may place their own piconet services IE in the PNC's record of piconet services by sending the piconet services IE to the PNC using the Probe command. When the PNC receives this IE from a DEV, it adds it to its internal record of piconet services. The PNC then sends a Probe command with DestID set to the BcstID containing the piconet services IE that it has added to its internal record of piconet services. If the PNC supports this capability, it retains the piconet services IEs of DEVs that have sent them via the Probe command. The PNC will only save piconet services IEs for which it has space. Thus it is possible that the PNC would not retain a DEVís piconet services IE.
If a DEV sends a Probe command to the PNC requesting the piconet services IE, the PNC responds with Probe commands that contain all of the piconet services IEs that it has in its internal record. If a DEV has not provided a piconet services IE to the PNC, the PNC sends the piconet services IE in the Probe command with the DEVID, a zero vendor ID and zero length piconet services field. If the PNC did not have enough space to save the piconet services IE that a DEV provided, it shall send in the Probe command a piconet services IE with length 1, i.e. it only contains the DEVID."

with

"DEVs that are members of the piconet may place their own Piconet Services IE in the PNC's record of piconet services by sending the Piconet Services IE to the PNC using the Announce command. When the PNC receives this IE from a DEV, it adds it to its internal record of piconet services. The PNC then sends an Announce command with DestID set to the BcstID containing the Piconet Services IE that it has added to its internal record of piconet services. If the PNC supports this capability, it retains the Piconet Services IEs of DEVs that have sent them via the Announce command. The PNC will only save Piconet Services IEs for which it has space. Thus it is possible that the PNC would not retain a DEV's Piconet Services IE.

If a DEV sends a Probe Request command to the PNC requesting the Piconet Services IE, the PNC responds with Probe Response commands that contain all of the Piconet Services IEs that it has in its internal record. If a DEV has not provided a Piconet Services IE to the PNC, the PNC sends the Piconet Services IE in the Probe Response command with the DEVID, a zero Vendor OUI field and zero length Piconet Services field. If the PNC did not have enough space to save the Piconet Services IE that a DEV provided, it shall send in the Probe Response command a Piconet Services IE with length 1, i.e. it only contains the DEVID."

Page 177 Line 51:

Replace

"All DEVs in the piconet shall send frames to the PNC often enough to assure that the association timeout period (ATP) is not reached. If the PNC does not receive any frame originating from an associated DEV within this timeout duration, the PNC shall disassociate the DEV. The DEV may send a Probe command without requesting any information to cause the PNC to reset the ATP if the DEV does not have any other traffic that it needs to send to the PNC."

with

"All DEVs in the piconet shall send frames to the PNC often enough to assure that the association timeout period (ATP) is not reached. If the PNC does not receive any frame originating from an associated DEV within this timeout duration, the PNC shall disassociate the DEV. The DEV may send a Probe Requst command without requesting any information to cause the PNC to reset the ATP if the DEV does not have any other traffic that it needs to send to the PNC."

Page 181 Line 1

Replace

"If the PNC indicates that it is using an extended beacon, 8.6.2, then the DEV shall wait until a SIFS after the last Probe command sent by the PNC as a part of the extended beacon before beginning the backoff procedure."

with

"If the PNC indicates that it is using an extended beacon, 8.6.2, then the DEV shall wait until a SIFS after the last Announce command sent by the PNC as a part of the extended beacon before beginning the backoff procedure."

Page 187 Line 20

Replace

"A DEV transmitting in the CAP shall start transmitting no sooner than the end of the beacon plus a SIFS. If the PNC is using an extened beacon, 8.6.2, the CAP does not begin until after the last Probe command is sent that is part of the beacon."

with

"A DEV transmitting in the CAP shall start transmitting no sooner than the end of the beacon plus a SIFS. If the PNC is using an extened beacon, 8.6.2, the CAP does not begin until after the last Announce command is sent that is part of the beacon."

Page 200 Line 42

Replace

"If the PNC determines that the beacon frame is too large or if it wishes to split the information in the beacon frame, it may send one or more Probe commands with the SrcID set to the PNCID and the DestID set to the BcstId following the beacon. This is called an extended beacon. Unless it is specified otherwise, the term beacon applies to both the beacon frame and the Probe commands that make up the extended beacon. If the PNC has allocated time for the CAP, then the first Probe command shall be sent one MIFS following the beacon with any additional Probe commands following one MIFS after the the prior Probe command. If the PNC is using MCTAs instead of the CAP, then the Probe command shall be sent in the first MCTA assigned in the superframe. This MCTA shall have the SrcID set to the PNCID and the DestID set to the BcstID. If the PNC sends some of the beacon information in the broadcast probe frames, it shall set the more data bit to indicate 'more data' in the frame control field of the beacon frame and in all but the last Probe command frame used to communicate the information elements. The PNC shall send CTA IEs, piconet BSID, SECID IE or the parent BSID IE only in the beacon frame and not in any of the broadcast probe frames. The probe frames are sent to the BcstID and so the ACK policy shall be set to no-ACK in these frames."

with

"If the PNC determines that the beacon frame is too large or if it wishes to split the information in the beacon frame, it may send one or more Announce commands with the SrcID set to the PNCID and the DestID set to the BcstId following the beacon. This is called an extended beacon. Unless it is specified otherwise, the term beacon applies to both the beacon frame and the Announce commands that make up the extended beacon. If the PNC has allocated time for the CAP, then the first Announce command shall be sent one MIFS following the beacon with any additional Announce commands following one MIFS after the the prior Announce command. If the PNC is using MCTAs instead of the CAP, then the Announce command shall be sent in the first MCTA assigned in the superframe. This MCTA shall have the SrcID set to the PNCID and the DestID set to the BcstID. If the PNC sends some of the beacon information in the broadcast Announce command frames, it shall set the more data bit to indicate 'more data' in the frame control field of the beacon frame and in all but the last Announce command frame used to communicate the information elements. The PNC shall send CTA Status IEs, BSID IE, or Parent Piconet IE only in the beacon frame and not in any of the broadcast Announce command frames. The Announce command frames are sent to the BcstID and so the ACK policy shall be set to no-ACK in these frames."

Page 205 Line 45:

Replace

"Each DEV that is a member of the piconet may use the PNC information request command, 7.5.4.1, to obtain information about other DEVs in the piconet. In addition the DEV may use the Probe command, 7.5.4.5, to obtain other information required for peer-to-peer communication. The remote scan procedure is used by the PNC to determine channel conditions. All DEVs in the piconet are able to use the channel status command to gather information about the quality of their link with another DEV."

with

"Each DEV that is a member of the piconet may use the PNC Information Request command, 7.5.4.1, to obtain information about other DEVs in the piconet. In addition the DEV may use the Probe Request command, 7.5.4.5, to obtain other information required for peer-to-peer communication. The remote scan procedure is used by the PNC to determine channel conditions. All DEVs in

the piconet are able to use the channel status command to gather information about the quality of their link with another DEV."

Page 206 Line 34:

Replace Clause 8.9.2 with the following text:

(begin new text)

1.4.5 Probe request

The Probe Request command provides the ability to request information elements from a target DEV. If the target DEV receives the Probe Request command, it shall respond to the originator with a Probe Response command that shall have the IEs requested by the originator.

A DEV may request information about an isochronous stream by sending a Probe Request command requesting the CTA Status IE, {xref 7.4.11}, with the Stream Index field set to the stream index of the stream for which CTA information is requested. If the Stream Index field is set to 0, the DEV is requesting information about all isochronous streams directed to the requesting DEV and to the BcstId and McstId. The PNC shall respond to a Probe Request command containing a request for the CTA Status IE by sending a Probe Response command containing the appropriate CTA Status IE(s).

Any DEV may send the Probe Request command with the Information Requested field set to zero and ACK Policy field set to Imm-ACK to any other DEV in the piconet to determine if the destination DEV is still present in the piconet and is within range of the sending DEV.

A DEV that is going to send a Probe Request command to a DEV operating in a power save mode should consider the operation of those modes as described in {xref 8.13} to determine when to send the Probe Request command and when to expect a response.

Figure 6 illustrates the sequence of messages involved in acquiring DEV IEs from a target DEV using the Probe Request command.

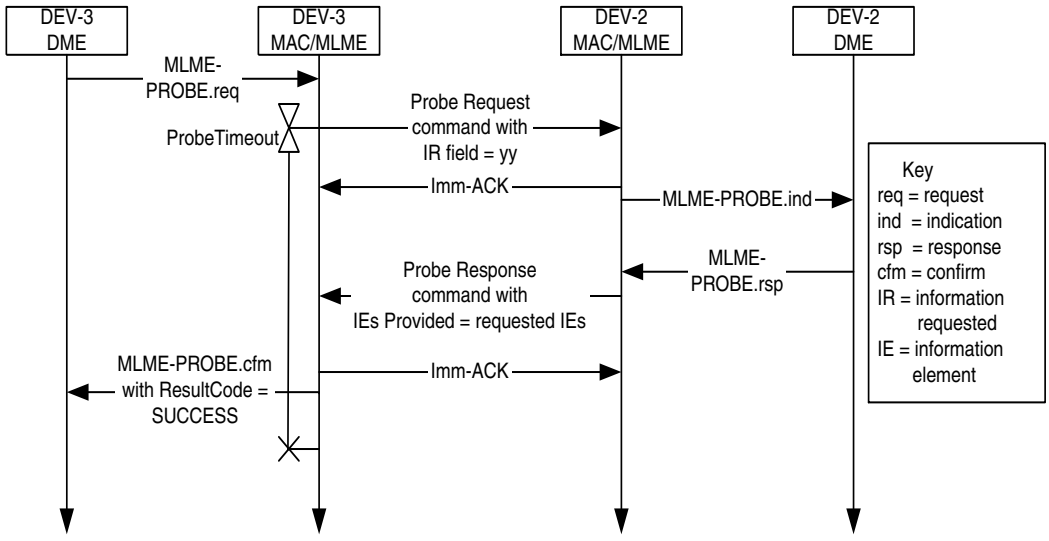

Figure 6—MSC for acquiring DEV IEs using the Probe Request command.

The types of information elements that are allowed to be requested depend on the status of the originator as either a DEV or PNC. The rules for requesting a specific IE are listed in Table 3.

1.4.6 Announce

The Announce command provides the ability to send unrequested information elements to a target DEV. This command shall have one or more IEs that the originator wants to send to the target.

A DEV that is going to send an Announce command to a DEV operating in a power save mode should consider the operation of those modes as described in 8.13 to determine when to send the Announce command.

Figure 7 illustrates the sequence of messages involved in using the Announce command for sending information.

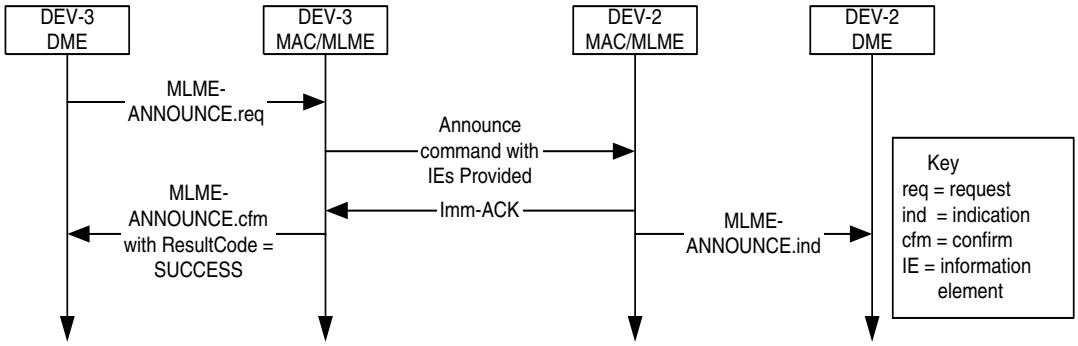

Figure 7—MSC showing sending of information using Probe command

The types of information elements that are allowed to be sent depend on the status of the originator as either a DEV or PNC. The rules for sending a specific IE are listed in Table 5.

(end new text)

Page 212 Line 41:

Replace

"If a DEV detects a piconet within its range on any channel with the same PNID, it shall send an Probe command to the PNC including an Overlapping PNID IE, 7.4.17, that contains the current PNID and channel index. Once this command has been sent successfully, the DEV shall not send this information again until after the current PNID has been changed by the PNC."

with

"If a DEV detects a piconet within its range on any channel with the same PNID, it shall send an Announce command, {xref}, to the PNC including an Overlapping PNID IE, 7.4.17, that contains the current PNID and channel index. Once this command has been sent successfully, the DEV shall not send this information again until after the current PNID has been changed by the PNC."

Page 217 Line 3:

Replace

"Send a Probe command, 7.5.4.5, to the target DEV to request its capability information element, 7.4.12;"

with

"Send a Probe Request command, 7.5.4.5, to the target DEV to request its Capability IE, 7.4.12;"

CLAUSE 9 CHANGES

Page 233 Line 39:

Replace

"If no secure frames are being transmitted by the previously authenticated DEV, the PNC or requesting DEV may send a secure Probe command requesting an information element (such as the DEV address) from the previously authenticated DEV."

with

"If no secure frames are being transmitted by the previously authenticated DEV, the PNC or requesting DEV may send a secure Probe Request command, {xref}, requesting an information element (such as the DEV address) from the previously authenticated DEV."

Page 234 Line 47:

Replace

"Before the authentication process is initiated, the DEV or PNC may choose to send probe commands to each other to request or transmit preferred OIDs. 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 security 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."

with

"Before the authentication process is initiated, the DEV or PNC may choose to send Probe Request commands to request or Announce commands to transmit preferred OIDs. 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 security turned off. In the Authentication Request command, the DEV should select either the security suite OID received in the Association Response command or an OID received in an Announce command after associating."

Table 62:

The "Probe" entry needs to be replaced with three entries; "Probe Request", "Probe Response", and "Announce".

Clause 10 Changes

Page 273 Line 18:

Replace

"The DEV or PNC may also send probe commands to each other before the authentication process to determine which OIDs are mutually supported."

with

"The DEV or PNC may also send Probe Request commands or Announce commands to each other before the authentication process to determine which OIDs are mutually supported."

Appendix D Changes

Page 334 Line 34:

Replace

"DEVs are also able to change their transmit power based on their own estimation of the channel. The Probe command, 8.9.2, allows DEVs to request information from other DEVs in the piconet to assist in getting this information."

with

"DEVs are also able to change their transmit power based on their own estimation of the channel. The Probe Request command, 8.9.2, allows DEVs to request information from other DEVs in the piconet to assist in getting this information."

Appendix E Changes

Table E.3: The "Probe" entry needs to be replaced with "Probe Request", "Probe Response", and "Announce".

Table E.4: The "Probe" entry needs to be renamed "Probe Request". An entry for "Announce" needs to be added with a reference to the new Announce clause of clause 8.

Accept in principle: Change the Stream Index field to be the Request Index field, 2 octets long and is the stream index when requesting the CTA Status IE, set to 0 otherwise.

1.4.7 Security issues:

1) We have still left obtuse references to security suites and OIDs in a couple of places in the draft, without making any statements about what they are or how they work exactly. The reason for this is that in order to ensure interoperability of implementations that use the authentication-related MAC commands, the standard needs to specify an unambiguous way for them to be distinguished. I think we may want to remove clause 9.4 as this discusses security suites exclusively, although it might be useful information for security suite writers. Note that all specific OIDs and security suites have already been removed from the standard.

Delete all references to OID, change OID in the Authentication request command to be an OUI. Delete Authenticate request, Authenticate response, Challenge Request, Challenge Response, De-authenticate command and their associated MLMEs and any MSCs.

Add an enumeration to MLME-SECID-UPDATE (now called MLME-MEMBERSHIP-UPDATE) that is either 'MEMBER', or 'NON-MEMBER' which indicates the membership status of the TrgtID for that SECID. When 'NON-MEMBER', the key length is zero. Add type 'BOTH'. Change 'MANAGMENT' to be 'MANAGEMENT'.

Delete security suite references in the draft, only keep locations where it refers to ‘symmetric key security operations’.

2) I was unable to incorporate the changes proposed in 334 and 336 as indicated while having it make any sense. I was as true to the proposed changes as I thought I could be, but I would love any other proposed wording. Perhaps it is best to include in the database the exact desired sentences, rather than just including the replacement phrases for the words that we want to change.

Ari will put together some text and pictures to clarify this.

3) There are some security policies that are included with the words "may" or "should" in clause 9 to give some guidance to implementers on how to use the MAC commands. John made some comments about security policies needing to be removed, but I am not certain which policies should be removed.

Delete subclause 9.4, the formal language can remain when in reference to key distribute and request. Edit 9.3.6 to reflect new lack of commands. Move 9.3.1, 9.3.2, 9.3.3 to Annex C. Replace 9.1.2 and 9.1.3 with “‘Security membership and key establishment’ with text ‘The method by which a DEV becomes a member of a security relationship and obtains the apppriate keys is outside of the scope of this standard. It can be achieved with higher layer protocols that are not specified in this standard. The MAC/MLME is informed of changes to the membership of a security relationship and the keys for that relationship with the MLME-MEMBERSHIP-UPDATE primitive.’

4) I need text for CID 340. I included the following text to satisfy the comment, but I am not sure if this satisfied the group or the commenter. "For extended network topologies, the number of DEVs that a DEV maintains a secure relationship with may be greater than 255." Note new text: ‘Although there is a fixed upper bound of fewer than 255 DEVs in a piconet, the security solution will need to scale to arbitrary sets of devices, rather than to a fixed set of limited size: devices may join and leave the network in an ad-hoc fashion and may not have met before at all.’

Use new text. ‘Although there is a fixed upper bound of fewer than 255 DEVs in a piconet, the security solution might need to scale to arbitrary sets of DEVs, rather than to a fixed set of limited size. DEVs join and leave the network in an ad-hoc fashion and in some cases, will not have previously communicated with the other DEV(s).’

5) Is CID 342 resolved the way the group wants? I simply removed the sections describing security analysis for the public-key stuff.

The resolution is OK as is.

6) The resolution for CID 345 should be changed to indicate that the entire sub-clause was removed.

Change resolution to be: ACCEPT IN PRINCIPLE. The security suites have been removed. This subclause was removed as a result of this and so this change no longer needs to be made.

7) I think that we should combine Annex B and Clause 10 since they are both reasonably small now and cover related topics.

Combine clauses.

Next meeting is conference call on Feb 12, 2003.

Potential agenda items: New text from Ari on concatenation and issues from John Barr.

Meeting adjourned 9:36 am PST.

1.5 Thursday, 6 February 2003

Agenda

- Roll call
- Resolution of CIDs 204, 254, 323
- Renaming of security manager
- Probe MLMEs, do we add MLME-PUSH or just live with what we have?
- Association MLME uses PiconetType to indicate if the DEV is associating as a neighbor PNC instead of 'Neighbor PNC'
- Use distinct fields in MLMEs (e.g. spell out every subfield as a parameter).
- Updates to CID 682.
- Other editorial requests
- Schedule future calls?
- Adjourn

Attendees: James Gilb, Dan Bailey, Ari Singer, Mark Schrader, Jim Allen, Rene Struik, Allen Heberling, Bill Shvodian, Knut Odman, John Sarallo, John Barr.

CID 323 (Shvodian, assigned to Schrader) - Collecting channel status for each source DEV in the piconet will add a substantial burden to any simple DEV and it will provide questional benefits. Any DEV using ImmACK or Del-ACK will know if the frames are getting through. A DEV should be able to respond that it doesn't provide channel response statistics. Add the following sentence: A measurement window size of zero indicates that the responding DEV does not provide channel status statistics.

> Accept in principle: “Add the following sentence to line 29, page 154 ‘The minimum measurement window size for a valid measurment for this command shall be 2 superframes. A Measurement Window Size field of zero indicates that the responding DEV does not provide channel status statistics.’”

CID 204 (Heberling, assigned to Heberling), CID 254 (Odman, assigned to Heberling) - [MCTA] We need a little better specification on how often MCTA are allocated to assure that the PNCRespTime can be met. Please add this new text, starting after the sentence beginning: "When MCTA are used...": "The PNC shall allocate MCTA assigned to a DEV, open MCTA or both. The frequency of assigned MCTA shall be at least CTRRespTime, as defined in the beacon. If only open MCTA are used, the PNC shall allocate at least one open MCTA per DEV and CTRRestTime. The PNC may reduce the MCTA allocation frequency for power save DEVs, and for DEVs requesting a longer interval between assigned MCTA using the CTR command, 7.5.5.1. Special rules power save DEVs is listed in 8.13.1, 8.13.2.2 and 8.13.3"

> Accept in principle “Change the name of PNCRespTime to be MCTAAllocRate with a new meaning, the frequency that the PNC assigns open MCTAs or directed uplink CTAs for each of the ACTIVE mode DEVs in the piconet. It means 'At least one open MCTAs in N superframes.' ‘If if the CAP isn’t used for commands, the PNC shall also allocate downlink CTAs to a DEV or the BcstID in response to commands by a DEV to the PNC within MCTAAllocRate superfames. A value of 15 means the PNC is not giving any guarantees about when it will allocate either MCTAs. A value of 0 indicates that the PNC be using only the CAP to provide access to the PNC.’”

Renaming the role of security manager. Suggest changing ‘security manager’ to be ‘key originator’ where it occurs in the draft.

> Accept suggested resolution.

Probe MLME’s and figure 128: Suggestion from John Sarallo (originally via email)

All,

I suggested the current implementation to make the DEV functionality easier. If a DEV receives a Probe Command with IEs in it, it sends a PROBE.cfm to the DME. If a DEV receives a Probe Command with a request for IEs, it sends a PROBE.ind to the DME. If it receives a Probe Command with both, it sends both primitives to the DME.

With the suggested change to figure 128 and the PROBE.ind MLME, a DEV will need logic to remember what has occurred in the past. For example, a DEV receives a Probe Command with IEs in it. What it sends to the DME depends on whether or not the DME previously requested the IEs. If the DME previously sent a PROBE.req, the DEV should pass the IE's back in a PROBE.cfm. If the DME didn't previously request the IEs, or if the Probe Command also contains Requested IEs, the DEV should pass up a PROBE.ind.

The current method overloads only the MLME-PROBE.request and MLME-PROBE.response primitives. By overload I mean used to both request and deliver IEs. As Bill indicates, if we change figure 128 as suggested, the MLME-PROBE.indicate primitive would need to be overloaded as well, making the PROBE mess even more complicated.

This change also introduces some races conditions that could lead to unexpected behavior. I won't go into the details, but it involves requesting IE's and getting unsolicited IEs at the same time.

If we go ahead with this change, please note that figure 127 would need to be modified as well. In figure 127, after DEV-3 DME sends the MLME-PROBE.req, it would only need to receive an MLME-PROBE.ind, and not both a MLME-PROBE.cfm and MLME-PROBE.ind. Again, the DEV MLME would require smarts to know it sends an .ind instead of a .cfm in this situation.

As an alternative, I suggest we bite the bullet and split up probe into two mlme sets and multiple command frames:

```
MLME-PROBE.request -->
        Probe Request Command --->
                MLME-PROBE.indication -->
                <-- MLME-PROBE.response
        <-- Probe Response Command
<-- MLME-PROBE.confirm
```

and

```
MLME-PUSH.request --->
        Push Command ---------->
                MLME-PUSH.indication --->
        <---------- Imm-Ack
<--- MLME-PUSH.comfirm
```

MLME-PROBE.request, Probe Request Command, and MLME-PROBE.indication contain only Requested IEs.

MLME-PROBE.response, Probe Response Command, and MLME-PROBE.confirm contain only Information Elements.

MLME-PUSH.request, Push Command, MLME-PUSH.indication contain only Information Elements.

NONE OF THE MLMEs OR COMMANDS WOULD CONTAIN BOTH REQUESTED IEs AND INFORMATION ELEMENTS.

Time to clean up the mess?

John

Minimal suggestion from James Gilb: In figure 128, change .cfm to .ind to match figures above and add a MLME-PROBE.cfm to DEV-3 after the Imm-ACK is received. It doesn't fix the probe mess, but it is consistent with the other figures.

John Sarallo, Mark Schrader and James Gilb to produce suggestion for the new text.

Problems with field naming in association request command: Suggestion (originally on email from John Sarallo)

The Issue:

The MLME-ASSOCIATE.request primitive also contains a parameters named PiconetType to indicate if the DEV is associating as a neighbor PNC or as a member of the piconet. However, this information is actually contained in the PNCCapabilities field as defined in 7.4.12 as the Neighbor PNC bit.

Furthermore, the PNC Capabilities field seems like an odd place to put the Neighbor PNC bit as it is not really a capability as much as an indication of the type of association request being made.

Here are some options to resolve this:

Option 1: Remove the PiconetType parameter from the MLME-ASSOCIATE.req and MLME-ASSOCIATE.ind primitives, as the information is already contained in the PNCCapabilities parameter. With this option, the method of associating as a Neighbor PNC is somewhat obscured.

Option 2: Leave the PiconetType parameter (perhaps rename NeighborPNC). Remove the Neighbor PNC bit from PNC Capabilities (figure 41) and add it to the DEV Utility field (figure 51) of the Association Request command. With this option there are more changes but the standard is clearer.

Thoughts?

John

Implement option 2, in clause 6 rename to be NeighborPNCRequest, rename to Neighbor PNC Request field in clause 7 and where it occurs in clause 8.

Issues with association MLMEs (originally in email from Knut Odman).

Clause 6.3.5, association.

It has been a policy to if possible avoid frame formats
in clause 6. Clause 6 is an informative interface description
and should have the logical paramters listed, not their
exact type or detailed implementation.
The number in paranthesis is affected CID's)
To pass all parameters needed for association, we need to
have the following in Table 9:
and
(297,401) Remove CapabilityField.
(297,401) Add PreferredFragmentSize, ref 7.5.1.1 and Table 138
(297,401) Rename MaxAssociations to MaxAssociatedDEV (as in 7.5.1.1)
(297,401) Rename TxPowerLevel to MaxTxPower (as in 7.5.1.1)
(297,401) leave SupportedDataRates as is.
(297,401) The two primitives would be:
6.3.5.1 MLME-ASSOCIATE.request (
  PiconetType,
  AssociationTimeoutPeriod,
  SupportedDataRates,
  PreferredFragmentSize,
/* PNC Capabilities, except neighbor, are assumed to come from PIB,
   if not put them in. */
/* In the same manner DEV Address have always been assumed to come
   from PIB. Table 9 could list params that are sent in the command
   that are not passed in the primitive, such as DevAddress, as long
   as the real source is listed */
  MaxAssociatedDEV,
  MaxCTRB,
  MaxTxPower,
  PiconetServicesInquiry,
  AssocTimeout
)
For 6.3.5.2, in addition we need to pass the parameters that
was members of the CapabilityField that originated from the PIB
on the requesting side (see 7.4.12)
6.3.5.2 MLME-ASSOCIATE.indication (
  OrigID,
  DEVAddress,
  AssociationTimeoutPeriod,
  SupportedDataRates,
  PreferredFragmentSize,
  PNC-Capable,
  PNC-DesMode,
  SEC,
  PowerSource,
  PiconetType,
  MaxAssociatedDEV,
  MaxCTRB,
  MaxTxPower,
  PiconetServicesInquiry
)
Summary: No technical change. Only discrete informal parameters used.

Update only these two MLMEs

Definitions of capabilites: (originally in email from Knut Odman)

Clause 7.4.12. Definitions of capabilities.

(453,465,177) Figure 39. Combine PNC Capabilities and DEV Capabilities
to "overall capabilities". Move Figure 50 from 7.5.1.1 here, since
this is the first place we use all combined capabilities.
Remove ATP from Figure 50. It will be included separately in the
two frames were it's used (6.5.1.1 and 6.5.4.2)
Length = 5. Overall Capabilities = DEV Cap. + PNC Cap.
Effective change from D15: MaxTxPower, MaxAssociatedDEV and
MaxCTRB will now be passed in Capability IE. Only used with probe.
(177) Figure 41. Add MaxTxPower, MaxAssociatedDEV, and MaxCTRB to
PNC Capabilities. Length = 4.

(the above have already been done)

The capability fields will be used for several commands, however nowhere
is listed where the source of the fields of the frame comes from.
Please by each definition add text:
Figure 40, DEV capabilities:
Preferred fragment size: MLME-ASSOCIATE.request, param PreferredFragmentSize
(6.3.5.1 Table 9) [new parameter, currently only table 138 ref:ed]
Supported data rates: MLME-ASSOCIATE.request, param SupportedDataRates
(6.3.5.1 Table 9)
PNC capabilities:
PNC capable: PIB param MACPIB_PNCCapable (6.5.1 Table 33)
PNC des-mode: PIB param MACPIB_PNCDesMode (6.5.1 Table 33)
SEC: PIB param MACPIB_SecurityOptionImplemented (6.5.3 Table 35)
PSRC: PIB param MACPIB_PowerSource (6.5.2 Table 34)
Neighbor PNC: MLME-ASSOCIATE.request, param PiconetType (6.3.5.1, Table 9)
Max Tx power: MLME-ASSOCIATE.request, param MaxTxPower (6.3.5.1, Table 9)
Max CTRBs: MLME-ASSOCIATE.request, param MaxCTRB (6.3.5.1, Table 9)
Max associated DEVs: MLME-ASSOCIATE.request, param MaxAssociatedDev
(6.3.5.1, Table 9)
Summary: all capability definitions and where the parameters come from
are collected in 7.4.12. One technical change: MaxTxPower, MaxAssociatedDEV
and MaxCTRB are passed in the Capability Information IE, which is used
with the Probe command.

(no action on the above, leave it as it is).

Clause 7.5.1.1, association request command

(453,176) Figure 50 moved to 7.4.12.
Figure 49: rename Capabilities to 'Overall Capabilities'.
Add ATP to Figure 49 (removed from Figure 50).

(already done)

Just like with 7.4.12, some parameters come from unknow sources.
Spell them out!

ATP: MLME-ASSOCIATE.request, param AssociationTimeoutPeriod
(6.3.5.1, Table 9)
DEV-Utility/Piconet services inquiry: MLME-ASSOCIATE.request,
param PiconetServicesInquiry (6.3.5.1, Table 9)
(299) This bit may only be set to 1 in an association
request command with the source DEVID set to the DEVID
previously assigned by the PNC. Otherwise it shall be set to 0.
DEV address: PIB param MACPIB_DEVAddress (6.5.2, Table 34)

(no action on the above, leave it as is).

Clause 7.5.4.2, PNC information command

Figure 50 moved to 7.4.12. Change name (text page 145, line 27)
(465) Figure 69: rename capability to 'Overall Capabilities'.
Add ATP to Figure 69. Definition in 7.5.1.1.
(ATP removed from Figure 50)

(already done)

Dynaminc length for PNC capabilities

---

(45) Resolution for 45 suggested adding length field to
"PHY Capabilities". Assuming this means "PNC Capabilities".
This is a case where the field will be used in other fields
and eventually in frames. I would urge the the committee to examine
the possibility to add a reserved octet for future use into
the PNC capabilities, or a new field "PHY Capabilities" into the
Overall Capabilities field, preferrably 1 octet long, all bits
reserved, if that is the intended use.

(waiting for Jay to propose, starting today)

Incorrect use of the word "capability" in other clause 5 and 8.

The word "capability" is used both in informal descriptions of
features and also referring to specific frame fields. The following
places need an update:
5.3.1.2, page 14, line 25: capabilities => PNC Capabilities {xref 7.4.12}
5.3.3, page 15, line 48: capabilities => PNC Capabilities {xref 7.4.12}
5.3.8, page 18, line 14: capabilities => Overall Capabilities {xref 7.4.12}
8.2.3, page 164, line 23: capability field => PNC Capabilities
8.2.3, page 164, line 24: capabilities information => PNC Capabilities
8.2.3, page 167, line 19: capabilities field => PNC Capabilities
8.2.5, page 169, line 34: capabilities field => PNC Capabilities
8.3.1, page 173, line 25: capabilities field => DEV Characteristics {xref 7.4.4}
??? [Do we really need to send only SupportedRAtes without fragmentation
preference? Couldn't we just send the one octet DEV Capabilites?]
8.7, page 199, line 37: capabilities information IE => DEV Capabilities field
{xref 7.4.12} of the association request command
{xref 7.5.5.1}.
8.12, page 214, line 1: capabilities => Supported Data Rates in the
DEV Characteristics field ... (see also comment above).

Technical editor will review and correct as necessary.

8.3.2 Services...
---
(299) remember to fix page page 175, line 6.

(Comment is ready to be applied here).

CID 682 - Needed to add one more figure, see also 03/059r0 for complete section. The new figure and text are:

Figure 8 shows a multi-frame CTRq with the CTRq TU MIFS field set to 1.

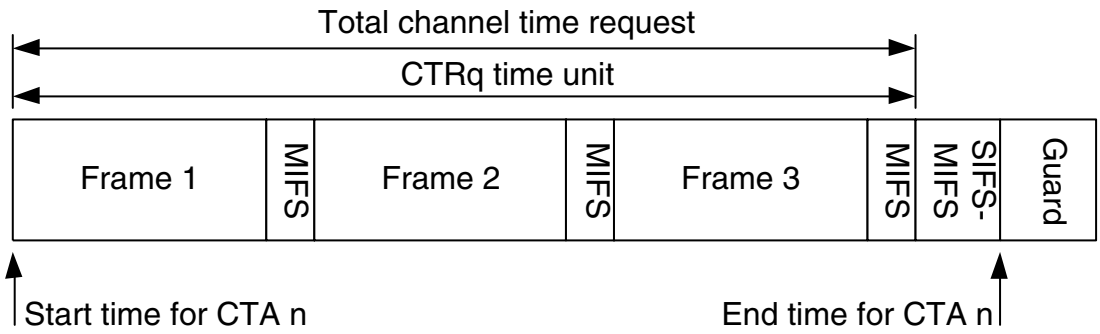

Figure 8—CTRq time unit covering multiple frames with CTRq TU MIFS = 1

Other editorial fixes to resolutions:

CID 59: 8.6.4, page 198, line 35: "If any DEV is in PSPS or SPS mode, the first IE announcement shall be made in a system wake beacon." Comment: SPS devices don't (necessarily) listen to system wake beacons. Resolution: delete "or SPS" from text. Problem: the original text describes the PNC policy. The PNC must decide somewhere to start putting the IE. Hibernation and SPS DEV may ignore the announcements made in the system wake beacon, but at least all DEVs should know where to look for such an announcement. A better solution: "If any DEV is in power save mode, the first IE announcement shall be made in a system wake beacon." This doesn't change any requirement on the DEVs, it is still only the PSPS DEVs (and ACTIVE of course) that shall listen, all others may.

Jay to provide suggested text.

CID 606: 8.2.3, page 165, line 23: "The parent PNC shall not hand over to a DEV that is currently operating as a dependent PNC." Comment: Remove restriction Resolution: Resolve as CID 139. Problem: CID 139, CID 215 and CID 352 deals with handover inside the dependent network, i.e. a dependent PNC handing over to a dependent DEV. The mentioned restriction has nothing to do with that. It says that the parent PNC cannot handover to the dependent PNC. This must still be true, because you have no way of merging the parent and dependent piconets. You will most likely get collisions in DEVID, StreamId, SPS Id, etc. A better solution: Leave this line as is. It is not related to the things you are trying to solve.

Knut to try at some text to explain that this does not mean merging.

Next meeting will be to discuss security, 8 am PST, John Barr to host.

Meeting adjourned at 10:42 am PST.

1.6 Tuesday, 4 February 2003

Agenda

> Roll call
> Resolve comments, reference 03/32r9
> Adjourn

Attendees: James Gilb, John Barr, Ari Singer, Jay Bain, Mark Schrader, Bill Shvodian, Knut Odman, Allen Heberling.

Meeting called to order at 8:09 am PST.

CID 576 (Ho, assigned to Schrader) - Ambiguous definition in lines 5-6: How would this command be responded when the DestID is set to the BcstID? Describe the response or delete the statement. **Suggest reject:** The section 7.5.6.2 Channel status response command provides an adequate explanation about what to do in each situation. The only knowledge that a DEV receiving the command must know is if the request came from the PNC or another DEV. From line 18 on page 154: "When the DestID of this command is the PNCID, the values in the command shall correspond to all frames exchanged by the DEV with other DEVs in the piconet. When the DestID of this command is a non-PNC DEVID, the values in the command shall correspond to the frames exchanged between the requesting DEV and the target DEV."

> Accept in principle: On page 154, line 6, change 'to the BcstID' to be 'to the BcstID with the ACK Policy field set to no-ACK.' Add to page 205, line 45 'If the PNC sends a broadcast Channel Status Request command, i.e. the DestID is the BcstID, it is requesting that all DEVs that receive the command respond with a Channel Status Response command sent to the PNCID. Each DEV sends the response command when they get an opportunity, either in the CAP or in an MCTA.'

CID 476 (Ho, assigned to Schrader) - Ambiguous statement in lines 15-16: What is an "ACTIVE channel time allocation" and what is an "SPS (not just PS?) channel time allocation"? Clarify the ambiguity. **Suggest accept in principle:** "In 7.5.5.1, page 152, after lines 15-16, add the following text:

> 'For subrate allocations, an ACTIVE allocation (specified by CTA type = 0) puts no restriction on the superframe of the first CTA specified by CTR interval. A DSPS allocation (specified by CTA type = 1) synchronizes all CTAs specified by the CTR interval with the DSPS set awake superframes of the DSPS set specified by the DSPS index. The value of the CTR interval shall be no smaller than the DSPS set's awake beacon interval.
>
> The DSPS set index field is used to identify the DSPS set with which the CTR is associated, if the CTR is for a DSPS allocation. Only valid DSPS set indices, {xref 7.5.7.2}, are allowed for a DSPS allocation request. Otherwise, the field shall be set to 0 and shall be ignored on reception.'
>
> Accept suggested resolution.

CID 275 (Rudnick, assigned to Schrader) - The CTRB's CTR interval field is currently unused for async requests. It should probably be put to use. A couple of possibilities are suggested below. Other uses may also be useful. 1) One possibility is that for async CTRBs, the CTR interval type field be required to be 0 (super-rate), and the CTR interval field be interpreted in the usual super-rate fashion. 2) Another possibility is to use the CTRB's CTR interval field to encode the maximum amount of time the requestor can use during any single superframe. **Suggest accept in principle:**

"In 7.5.5.1 page 152, lines 22-31 change:

'The CTR interval type field shall be set to 0 when the CTR interval field represents the number of super-rate CTAs, and shall be set to 1 when the CTR interval field represents the number of sub-rate CTAs. Superrate allocation includes the case where the CTR interval type is equal to 1, i.e. only one allocation requested every beacon. A sub-rate CTA is one where the allocation occurs once every N superframes while a superrate CTA is one where the allocation occurs N times in every superframe, including the case where it occurs once per superframe.

If the CTR interval type field is set to 1, the value contained in the CTR interval field shall be a power of 2. A PNC shall support at least 8 slots per stream in the same superframe.

Regardless of the value present in the CTR interval type field, the CTR interval field shall not be set to zero.'

to be

'For an isochronous channel time allocation request, the CTA Rate Type field is used to select whether the CTA Rate Factor field specifies the frequency of super-rate CTAs, or the frequency of sub-rate CTAs.

If the CTA Rate Type field is set to zero, indicating a super-rate CTA request, and the value of the CTA Rate Factor field is "N", then the CTA request is for N CTAs in every superframe. For example, if the CTA Rate Factor field is equal to 1, there will be one CTA block in each beacon, and one corresponding CTA in each superframe. The only restriction on CTA Rate Factor field is that it shall not be zero.

If the CTA Rate Type field is set to one, indicating a subrate CTA request, and value of the CTA Rate Factor field is "N", the subrate CTA request is for one CTA every N superframes with no CTAs in the remaining N-1 superframes. An additional restriction on CTA Rate Factor field when the CTA Rate Type field is set to one is that it shall be limited to powers of 2 (i.e. 2, 4, 8...), and because the value 65536 cannot be represented with 2 octets, an CTA Rate Factor field value of 0 shall be interpreted as 65536.

For an asynchronous channel time request, i.e. the Stream Index field is set to 0, the CTA Rate Factor field is set to the maximum number of TUs (amount of time) that the requestor can utilize during a single superframe. The PNC may limit the asynchronous CTAs in a single superframe for the requestor to this value.'"

Accept suggested resolution.

CID 174 (Heberling, assigned to Heberling) - [FrmFrmt] Figure 7 (Frame payload) and Figure 8 (Secure payload) indicate two different types of payloads, yet only the secure payload is partially described. Add a definition for the frame payload field. Also, add information to the secure payload definition to clarify the difference between the Frame payload and the secure payload. **Suggest accept in principle:** "Add a new subclause prior to the existing 7.2.7.1, '

1.6.0.1 Frame payload

The Frame Payload field is a variable length field that carries the information that is to be transferred to a DEV or group of DEVs in the piconet. In the case of a secure frame, it also includes the required security information, {xref Figure 8}.'

Rewrite the paragraph on page 113, line 24 to read ‘The Secure Payload field is a variable length field that contains the information, protected by the symmetric key security operations as defined in {xref 9.x}, that is to be transferred to a DEV or group of DEVs in the piconet. As illustrated in {xref Figure 8}, the Secure Payload field does not include the SECID, SFC or Integrity Code fields.’”

Accept suggested resolution

CID 299 (Sarallo, assigned to Bain) - The sentence "The association process does not wait for the piconet services command to complete." can result in problems. For example, if the association process completes before the PNC transmits the piconet services command, the newly associated dev would not receive the command because the command is addressed to the UnsssocID and not the associated DEVs newly aquired DEVID. Change: "If the DEV sets the piconet services inquiry bit, the PNC shall send the piconet services command, 7.5.4.6, with DestID set to UnassocID. The association process does not wait for the piconet services command to complete." To: "If the DEV sets the piconet services inquiry bit, the PNC shall send the piconet services command, 7.5.4.6, with DestID set to UnassocID before it allocates a DEVID to the associating DEV via the association response command." **Suggest accept in principle:** “Change: ‘If the DEV sets the piconet services inquiry bit, the PNC shall send the piconet services command, 7.5.4.6, with DestID set to UnassocID. The association process does not wait for the piconet services command to complete.’ To: ‘If the DEV sets the piconet services inquiry bit, the PNC shall send the piconet services command, 7.5.4.6, with DestID set to UnassocID before it allocates a DEVID to the associating DEV via the association response command.’ Also, add a new paragraph to 8.3.1 at line 51 on page 172. ‘If the PNC is going to send the piconet services command, {xref 8.3.2}, it shall do so prior to sending the association response command.’ In figure 103, insert a message after MLME-ASSOCIATE.rsp and before association response command. This message is in the direction of PNC MLME to DEV-2 MLME . ‘Piconet services command with DestID=UnassocID (note: this command is only sent if PNC is to provide this command)’. There is no ack.”

Accept in principle “Change to ‘If the DEV sets the piconet services inquiry bit, the PNC shall send the piconet services command, 7.5.4.6, with DestID set to newly assigned DEVID after that PNC

has received the second Association Request command from the DEV, {xref }. This process is illustrated in {figure xx}.' and add new MSC as shown in 03/032r10."

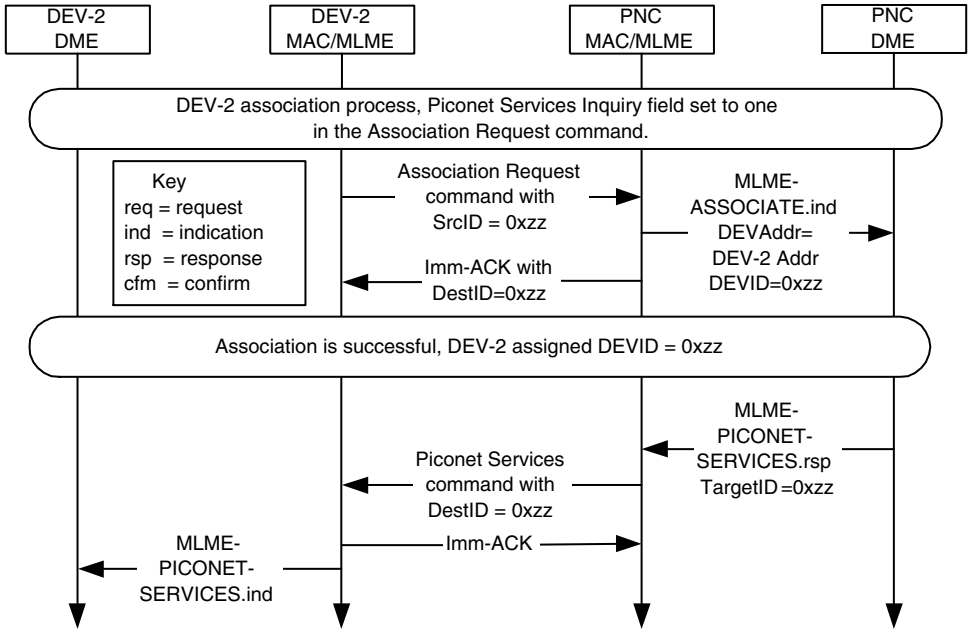

Figure 9—PNC sending the piconet services command to a newly associated DEV in response to a request in the association proces.

CID 172 (Heberling, assigned to Heberling) - [PiconetService] Seems there is a need for an MLME-PICONET-SERVICES.indication/response set of primitives. During association a DEV can set its PiconetServiceInquiry bit to request a list of piconet services from the PNC. The response to the services request bit is independent of the association response. Also I'm assuming that since the Services database is not managed by the MAC or MLME, that the PNC DME or some other protocol layer needs to receive some sort of notification that a request for services information has been received. Consequently, the current description of the piconet services functionality is incomplete and not acceptable. Add the missing MLME primitives regarding piconet services or delete all references to piconet services. S**uggest accept in principle:** Add the following MLME-PICONET-SERVICES.indication and .response.

(begin new MLME-PICONET-SERVICES primitives)

1.6.1 Piconet services

These primitives are used to transfer information regarding the services offered by DEVs in an piconet. The parameters used for these primitives are defined in Table 6

Table 6—MLME-PICONET-SERVICES primitive parameters

Name	Type	Valid range	Description
TargetID	Integer	Any valid DEVID as defined in {xref 7.2.3}	The target of the MLME command.
PiconetServicesIESet	Set of Piconet Services IEs	0 to N Piconet Services IE(s), {xref 7.4.19}.	The set of Piconet Services IEs in the Piconet Services command, {xref 7.5.4.6}

1.6.1.1 MLME-PICONET-SERVICES.response

This primitive is used to send the Piconet Services command, {xref 7.5.4.6}. The semantics of the primitive are:

```
MLME-PICONET-SERVICES.response(
                                    TargetID
                                    PiconetServicesIESet
                                    )
```

The primitive parameter is defined in Table 6.

The PNC MLME upon receiving this primitive will send a Piconet Services command to the TargetID.

1.6.1.2 MLME-PICONET-SERVICES.indication

This primitive is used to indicate the reception of the Piconet Services command, {xref 7.5.4.6}. The semantics of the primitive are:

```
MLME-PICONET-SERVICES.indication(
                                    PiconetServicesIESet
                                    )
```

The primitive parameter is defined in Table 6.

This DEV MLME generates this primitive when it receives a Piconet Services command.

(end new MLME-PICONET-SERVICES primitives)

Accept suggested resolution.

CID 53 (Bain, assigned to Gilb) - It is presumed that the DME should have the values of rates for the PHY to allow calculation of CTRs. The PHY-PIB should have a list of actual rates cooresponding to the indexed data rate that the MAC relates to the PHY for each frame sent. make the requested changes. **Suggest accept in principle:** “After line 49 on page 341, add the following new paragraph and table ‘The encoding of the TXDataRate and RXDataRate used in the PHY SAP, {xref 6.7}, is based on the value for the data rate sent in the PHY header, {xref Table 128} and is given in Table 7.’”

Table 7—Encoding of the 2.4 GHz PHY data rates for the PHY SAP

Modulation	Data rate	TXDataRate/ RXDataRate value
QPSK TCM	11 Mb/s	0x00
DQPSK	22 Mb/s	0x01
16-QAM TCM	33 Mb/s	0x02
32-QAM TCM	44 Mb/s	0x03
64-QAM TCM	55 Mb/s	0x04

Accept suggested resolution.

CID 721 - (Ho, assigned to Odman) Is the receiving MAC supposed to wait for any missing frames? If so, for how long? For instance, the sender sent 5 consecutive frames, of which frame 1 was not received by the recipient but was discarded by the sender after its last transmission (due to exceeding delay limit. Should the recipient hold all the received frames after frame 1 in waiting for frame 1? The issue is resolved in a similar mechanism defined in the latest 802.11e draft, which introduces a field in the frame requesting a Dly-ACK to indicate a Sequence Control value such that all frames with a smaller Sequence Control value have been discarded by the sender and hence should not be awaited by the recipient. This expedites the delivery of received frames to the upper layer in the case of missing frames at the recipient. Resolve this synchronization issue. **Suggest accept in principle:** 'On page 199, line 50 add the following at the end of the paragraph: 'MSDUs shall be delivered to the destination MAC's FCSL in ascending MSDU number order.' On page 201, line 25 add the following as a new paragraph: 'The destination MAC shall deliver MSDUs in ascending MSDU number order to its FCSL. If necessary to accomplish this, a destination MAC using Dly-ACK may discard correctly received (and potentially acknowledged) frames.'"

Accept in princple: "On page 201, line 25 add the following as a new paragraph: 'The destination MAC shall deliver MSDUs for each isochronous stream in ascending MSDU number order to its FCSL. If necessary to accomplish this, a destination MAC may discard correctly received (and potentially acknowledged) frames. Asynchronous MSDUs shall be delivered to the FCSL in the order of reception.'"

Also revise CIDs 286, 290, 720 to match this resolution.

CID 350 (Struik) - Incorporate proper security notions throughout the Draft, defined in line with well-established cryptographic practice. We give an example of improper usage: in Clause 3, Page 5, line 21, 'authentication' is confused with 'authorization', since 'authentication' refers to 'evidence as to the true source of information or the true identity of entities' (see, e.g., the Handbook of Applied Cryptography, or Slide 2 of 02/114r5), whereas 'authorization' refers to 'assurance that an entity may perform specific operations'. This improper/sloppy use of terminology leads to misleading claims regarding security services offered. The following terms in Clause 3 need more accurate definitions: authentication, authentic data, integrity code, key establishment, key management, key transport, nonce, symmetric key. I am - again - prepared to offer help, but this would assume flexibility and an open mind from the assistant security editor as well. Let us try again. **Suggest accept in principle:**

1.7 authentication: Process or protocol whereby one party obtains assurances as to the true identity of another party (entity authentication) or as to the true origin of data (data authentication).

1.8 authentic data: Data with assurances as to the true origin hereof.

1.9 key establishment: Process or protocol whereby a shared secret becomes available to two or more parties for subsequent cryptographic use.

1.10 key management: Set of techniques and procedures supporting the establishment and maintenance of keying relationships between authorized parties.

1.11 key transport: Key establishment technique where one party creates or otherwise obtains a secret value, and securely transfers it to the other(s).

1.12 nonce: A value that is used no more than once for the same purpose. It typically serves to prevent (undetectable) replay.

> Accept in principle “Delete definitions for key management, key establishment, key transport, authentication, access control, authentic data, nonce, confidentiality, private key, public key, public-key certificate, signature verification, signed data, trusted third party.”

CID 821 (Ho, assigned to Schrader) Spec does not define what determines a "Lost Beacon". Is it just not receiveing a beacon frame type at the expected time? Or if data within the beacon is wrong or unexpected (such as PNID, DestID, SrcID, Time Token), such that the beacon be ignored and lost beacon counter incremented? Some of this is implied but not explicitly specified. Add table or text to describe which info within a beacon must be valididated. Section 8.6.3, "Beacon Reception," would be a good location for such info. Suggest accept in principle: A lost beacon is defined as one for which the HCS is not valid or when a DEV has not received a beacon for a period significantly greater than one superframe.’

> Accept in principle “Add to page 197, line 53 ‘A lost beacon is defined as one for which the FCS is not valid or when a DEV has not received a beacon at the expected time.’”

CID 323 (Shvodian, assigned to Schrader) - Collecting channel status for each source DEV in the piconet will add a substantial burden to any simple DEV and it will provide questional benefits. Any DEV using ImmACK or Del-ACK will know if the frames are getting through. A DEV should be able to respond that it doesn't provide channel response statistics. Add the following sentence: A measurement window size of zero indicates that the responding DEV does not provide channel status statistics.

> Table, consider internally.

CID 204 (Heberling, assigned to Heberling), CID 254 (Odman, assigned to Heberling) - [MCTA] We need a little better specification on how often MCTA are allocated to assure that the PNCRespTime can be met. Please add this new text, starting after the sentence beginning: "When MCTA are used...": "The PNC shall allocate MCTA assigned to a DEV, open MCTA or both. The frequency of assigned MCTA shall be at least CTRRespTime, as defined in the beacon. If only open MCTA are used, the PNC shall allocate at least one open MCTA per DEV and CTRRestTime. The PNC may reduce the MCTA allocation frequency for power save DEVs, and for DEVs requesting a longer interval between assigned MCTA using the CTR command, 7.5.5.1. Special rules power save DEVs is listed in 8.13.1, 8.13.2.2 and 8.13.3"

> Table, take to email for suggestions.

Meeting adjourned at 10:04 am PST.

1.13 Thursday, 30 January 2003

Agenda

Roll call
Resolve comments, reference 03/032r7.
Status of comments that still need text written.
Adjourn

Meeting called to order at 9:09 am PST

Attendees: Ari Singer, Allen Heberling, Knut Odman, Bill Shvodian, Jay Bain, James Gilb, Mark Schrader.

CID 72 - (change dynamic/static to read only/write only/read-write) **Suggest accept in principle:** Remove the content and header of the "Type" column for each table and make the header be "Access." The content is as follows:

Table 33- MAC PIB PNC group parameters - All are read-only. Is MACPIB_CFPDuration a PIB parameter we desire. It requires a calculation by the DEV to subtract the start time of the first CTA fromt the SF duration.
Table 34 - MAC PIB characteristic group parameters - All are read-only except MACPIB-Power-Source and it is read-write .
Table 35 - MAC PIB authentication group parameters - Both managed objects are read-only.
Table 36 - MAC PIB association group parameters - the two managed objects are read-write.
Table 37 - MAC PIB piconet security group parameters - all managed objects are to be read-only. Note a comment to add another table is pending resolution.
Table 140 - PHY PIB implementation group parameters --- all managed objects are to be read-only. Note that another comment changes PHYPIB-RangeList. The part remaining is read-only. {Ed note: definitions on the two xmit power parms point to 7.5.6.5. That may not be a good pointer for their definition and the naming of the PHYPIB_TxMaxPower and PiconetMaxTXPower doesn't match. }
Table 141 - PHY PIB characteristics group parameters -- all managed objects are to be read-only. Note that other comments resolved or pending remove PHYPIB_RSSIVector, PHYPIB_LQIBVector, and PHYPIB_CCA_Treshold (there shouldn't be an underscore between A_T by the way)

Accept in principle: Remove the content and header of the "Type" column for each table and make the header be "Access." The content is as follows:

Table 33- MAC PIB PNC group parameters - All are read-only. Change MACPIB_CFPDuration to be MACPIB_CAPEndTime with a definition, 'The end time time of the CAP interval in the super-frames, {8.6}'.
Table 34 - MAC PIB characteristic group parameters - All are read-only except MACPIB-Power-Source and it is read-write .
Table 35 - MAC PIB authentication group parameters - Both managed objects are read-only.
Table 36 - MAC PIB association group parameters - the two managed objects are read-write.
Table 37 - Will be deleted per other comment.
Table 140 - PHY PIB implementation group parameters --- all managed objects are to be read-only. Note that another comment changes PHYPIB-RangeList. Change PHYPIB-TXMaxPower to be PHYPIB_MaxTXPower and change xref to be 7.5.1.1. For PHYPIB_TXPowerStepSize, replace cross-reference for the definitions to be a definition that it is 2's complement representation in dB.
Table 141 - PHY PIB characteristics group parameters -- all managed objects are to be read-only. , and PHYPIB_CCA_Threshold (there shouldn't be an underscore between A_T by the way). Note that other comments resolved or pending remove PHYPIB_RSSIVector, PHYPIB_LQIBVector.'

CID 91 (Gilb) - I have a problem with this standard. I believe 15.3 should have been completely interoperable with 15.1, 15.3 and 11b. Although it seems that 15.3 has put some effort towards that goal, it did not take

the last steps, whic are essential. The result is that 802 is now sending quite a confused message to the market. What device should the portable/mobile computer be equipped with? 11g? 15.1? 15.3? All of the above? Neither? Does 802.15 have any roadmap towards some kind of unification? Despite of that, I voted "approve", because I appreciate the effort put into the standard. However, I would like to see, or more importantly, I want RevCom to see the group rebuttal, and I hope some effort towards a more interoperable WPAN standard is going to be made. Make the change as requested. **Suggest reject:** "The PAR for 802.15.3 did not require 802.15.3 to be interoperable with any other standard. Different application requirements lead to solutions that are not necessarily interoperable. Within the 802.11 standard there are a total of 5 PHY layers, only two of which are interoperable with each other. The PAR for 802.15.3 identified a class of applications that required a MAC that was fundamentally different from 802.11's MAC, and so interoperability with 802.11 at a MAC level was not possible without seriously compromising the performance of 802.15.3. Although interoperability with other wireless standards is not required in the 802.15.3 PAR, Annex D in the standard does address the issue of interoperability with other IEEE wireless standards. The Annex indicates that it is possible for an implementer to build a DEV that could switch between 802.11b and 802.15.3, i.e. a dual-mode device. Not only that, specific choices in the selection of the PHY characteristics were made that make interoperability easier. In addition, some companies already have dual-mode solutions that can do both 802.15.1 and 802.11b with only a modest increase in the cost of the solution. These same techniques can be used to create dual-mode 802.15.3/802.15.1 implementations."

> Reject "The PAR for 802.15.3 identified a class of applications that required a MAC that was fundamentally different from 802.11's MAC, and so interoperability with 802.11 at a MAC level was not possible without seriously compromising the performance of 802.15.3. Although interoperability with other wireless standards is not required in the 802.15.3 PAR, Annex D in the standard does address the issue of interoperability with other IEEE wireless standards. The Annex indicates that it is possible for an implementer to build a DEV that could switch between 802.11b and 802.15.3, i.e. a dual-mode device. Not only that, specific choices in the selection of the PHY characteristics were made that make interoperability easier. In addition, some companies already have dual-mode solutions that can do both 802.15.1 and 802.11b with only a modest increase in the cost of the solution. These same techniques can be used to create dual-mode 802.15.3/802.15.1 implementations."

CID 510 - Unspecific Valid range and Description in Tables 29 and 30. "Replace "As defined in…" with specific valid range or description." **Suggest accept in principle:** "It is extremely difficult to keep normative definitions synchronized between separate sections of the standard. To avoid this problem, the standard tries to define any given requirement only once and to then cross reference to it in the text where appropriate. This makes the standard easier to maintain and less likely to have errors. However, there is one problem with the valid range cross-references in Table 29 and 30. Add to 7.5.7.2 'The PS set indices are defined as:

> 0x00 -> APS set
> 0x01 -> PSPS set
> 0x02-0xFD -> DSPS sets
> 0xFE-> Unallocated SPS set
> 0xFF -> Reserved'
>
> Also add a xref to 8.13 to all of the 7.5.7 xrefs that don't have it already.'
>
> Accept suggested resolution.

CID 313 - The low EVM values for the QAM modes will require very flat amplitude and group delay responses from the transmit filters - and hence greater cost. It seems likely that any demodulator that implements the QAM modes will include an equaliser quite capable of correcting moderate amounts of distortion in the transmitter anyway. Allow the ideal receiver used to measure these parameters to include an equaliser - perhaps also specify some larger EVM values for an unequalised measurement to keep some limits on the level of distortion allowed. **Accept in principle:** The PHY subcommitte discussed allowing an equalizer to for the ideal receiver, but it was felt that the current definition is sufficient. The equalizer in the receiver will

be much more limited that what can be created in lab equipment, yet the radio still needs to be able to adjust for both the channel and the transmitter imperfections. In reviewing the values for the EVM, the task group determined that they could be relaxed somewhat. Change the EVM table in 11.5.2 to be:

Table 8—EVM values for various modulations

Modulation	EVM (%)
64 QAM	3.3
32 QAM	4.8
16 QAM	7.5
DQPSK	9.2
QPSK-TCM	20.0

Accept suggested resolution.

CID 216 - The paragraph seems to assume behaviors of equipment which don't exist- and can't exist without some kind of a PAR in 802.11. 802.11 AP's (not 11b AP's) do not have any optional or normative ability to request neighbor piconet status. And, change the paragraph to "802.11 overlapping with 802.15.3..." Remove the paragraph. However, coexistence in timeCAN be accomdated if the INFORMATION element that was approved (see 802.15.2 coexistence) is used by the 2.4GHz AP. Please state something to that effect. **Suggest accept in principle** "Add to the end of the paragraph the following text: 'This capability is not specified in the 802.11 standard and so this would require an AP that had additional functionality that is outside of the current 802.11 standard. The IEEE 802.15.2 draft recommended practice has proposed an information element and extra functionality that, if added the 802.11 standard, would make it possible to build a standards compliant AP that could then support the 802.15.3 neighbor piconet capability.'"

Accept suggested resolution.

1.13.1 Handover of a dependent PNC.

CID 1, CID 215, CID 352 and CID 139

(begin resolution text)

Add a new field to PNC Handover Response:

.

octets: 1	2	2
Reason Code	Length(=1)	CommandType

Figure 10—PNC handover response command format

The Reason Code field indicates that the new PNC is either ready to take over as the new PNC or that it will be unable to become the PNC. The valid Reason Code values are:

0x00 -> Success, ready for handover
0x01-0xEC -> Success, member of parent piconet with DEVID equal to Reason Code value

0xED-0xF6 -> Reserved
0xF7-0xFC -> Success, associated in parent piconet with NbrID equal to Reason Code value
0xFE -> Handover refused, unable to join parent piconet
0xFF -> Handover refused, unable to act as PNC for more than one piconet

(end new text for 7.5.3.2)

Add new text to 8.5.1.2,

(begin new text for 8.5.1.2)

A dependent PNC, the originator DEV, may handover control of the dependent piconet's CTA to another DEV, the target DEV, in the parent piconet. The target DEV shall either be a member of the piconet or a DEV that has associated as a neighbor PNC, {xref association}. To handover control of the dependent piconet's CDA, the originator DEV shall send a Channel Time Request command to the parent PNC with the following parameters:

— The Num Targets field set to one.
— The Target ID List field containing the DEVID of the target DEV that is to receive control of the CTA
— The Stream Request ID set to zero.
— The Stream Index of a CTA that has already been allocated to the dependent PNC as a private, pseudo-static CTA.
— All other fields set to the same values as in the last successful Channel Time Request for this Stream Index.

If the target DEV indicated in the Target ID List is either a member of the parent piconet or is a associated neighbor PNC and the Channel Time Request command has the correct entries as indicated above, the parent PNC shall grant the request to change the source and destination for the stream and shall send a Channel Time Response command to the originator with the Reason Code set to 'Success'. The PNC shall continue to place the CTA block for the allocation in the beacon but shall change the SrcID and DestID to be equal to the target's DEVID. Once the PNC has changed the SrcID and DestID in the CTA block, the target DEV will have gained control of the CTA and will be allowed to request modifications or the termination of the allocation.

If the target DEV is not a member of the piconet and it is not an associated neighbor PNC, the parent PNC shall reject the request and shall send a Channel Time Response command to the originator with the Reason Code set to either 'DEV unassociated' or 'DEV unauthenticated' depending on the status of the Target DEV.

If the Channel Time Request command has improper entries, e.g. the Stream Index does not exist or the Stream Index is not associated with a private, pseudo-static CTA, then PNC shall reject the request and shall send a Channel Time Response command to the originator DEV with the Reason Code set to 'Request denied'.

The MSC for the handover of the control of a private, pseudo-static CTA is illustrated in Figure 11.

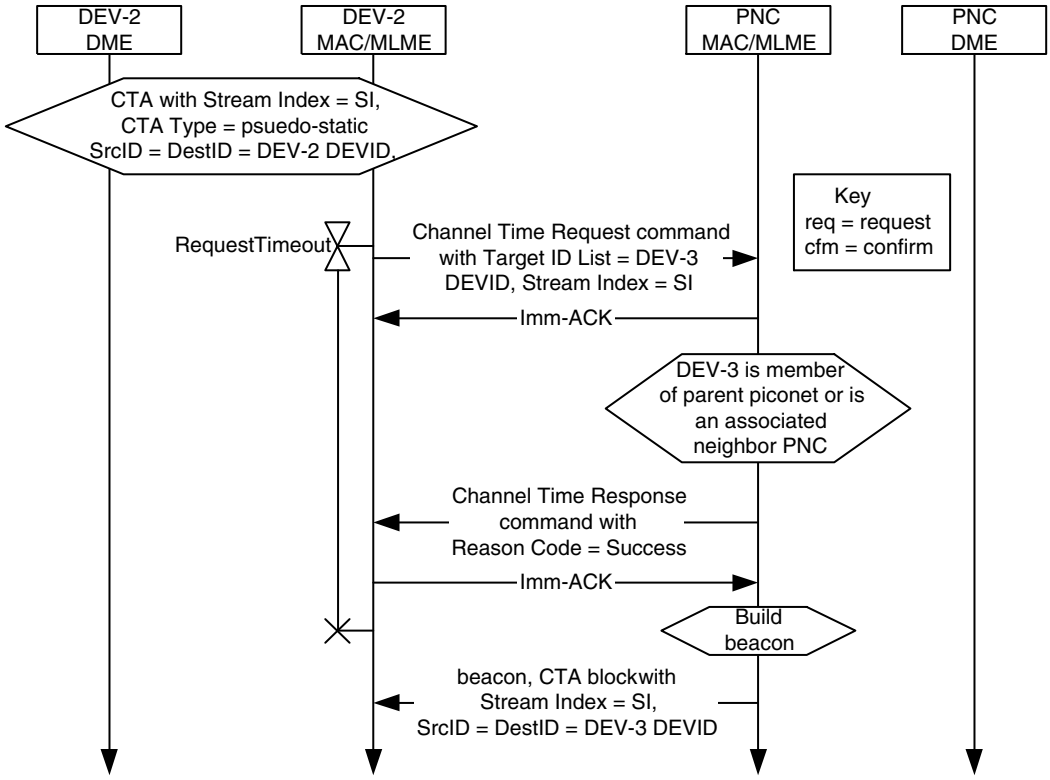

Figure 11—MSC for the handing over control of a private, pseudo-static CTA

(end new text for 8.5.1.2)

Replace pages 164, line 28 last line on the paragraph becomes: 'If the piconet is not a dependent piconet, the DEV shall accept the nomination and be prepared to receive the piconet information records. If the DEV is currently the PNC of a dependent picoent, it may refuse the request by sending PNC Handover Response command to the PNC with the Reason Code field set to 'Handover refused, unable to act as PNC for more than one piconet'. If the piconet is a dependent piconet, then the DEV shall accept the handover request unless it is unable to join the parent piconet as either a regular DEV or as a neighbor PNC. In this case the DEV sends the PNC Handover Response command to the PNC with the Reason Code field set to 'Refused, Handover refused, unable to join parent piconet.'

(begin new text for new subclause, 8.2.4 Depending PNC handover)

8.2.4 Dependent PNC handover

The dependent PNC handover process begins in the same manner as a regular PNC handover, {xref 8.2.3}, with the current PNC sending the PNC Handover Request Command to the target DEV that it has selected to become the new PNC, as shown in Figure 12. In this and the two subsequent figures, the identities PNC, DEV-2 and DEV-3 are all relative to the dependent piconet and not the parent piconet. If the target DEV is not a member of the parent piconet, then that DEV shall begin the association process to join the parent pico-

net and, if required, authenticate with the parent PNC. The target DEV may request to associate with the parent piconet as either a neighbor PNC or as a member of the piconet. While target DEV is attempting to join the parent piconet, the current dependent PNC shall send the target DEV the information about all of the DEVs with the PNC Information command, all of the current channel time requests with the PNC Handover Information command and the power save information, if any, using the PS Set Information Response command. The target DEV may also request the transfer of any ACL data at this point using the ACL Information Request command. Note that the transfer of this information will not interfere with the tareget DEV's association and authentication process because the former occurs only during time reserved for the dependent piconet while the latter only occurs during time reserved for the parent piconet.

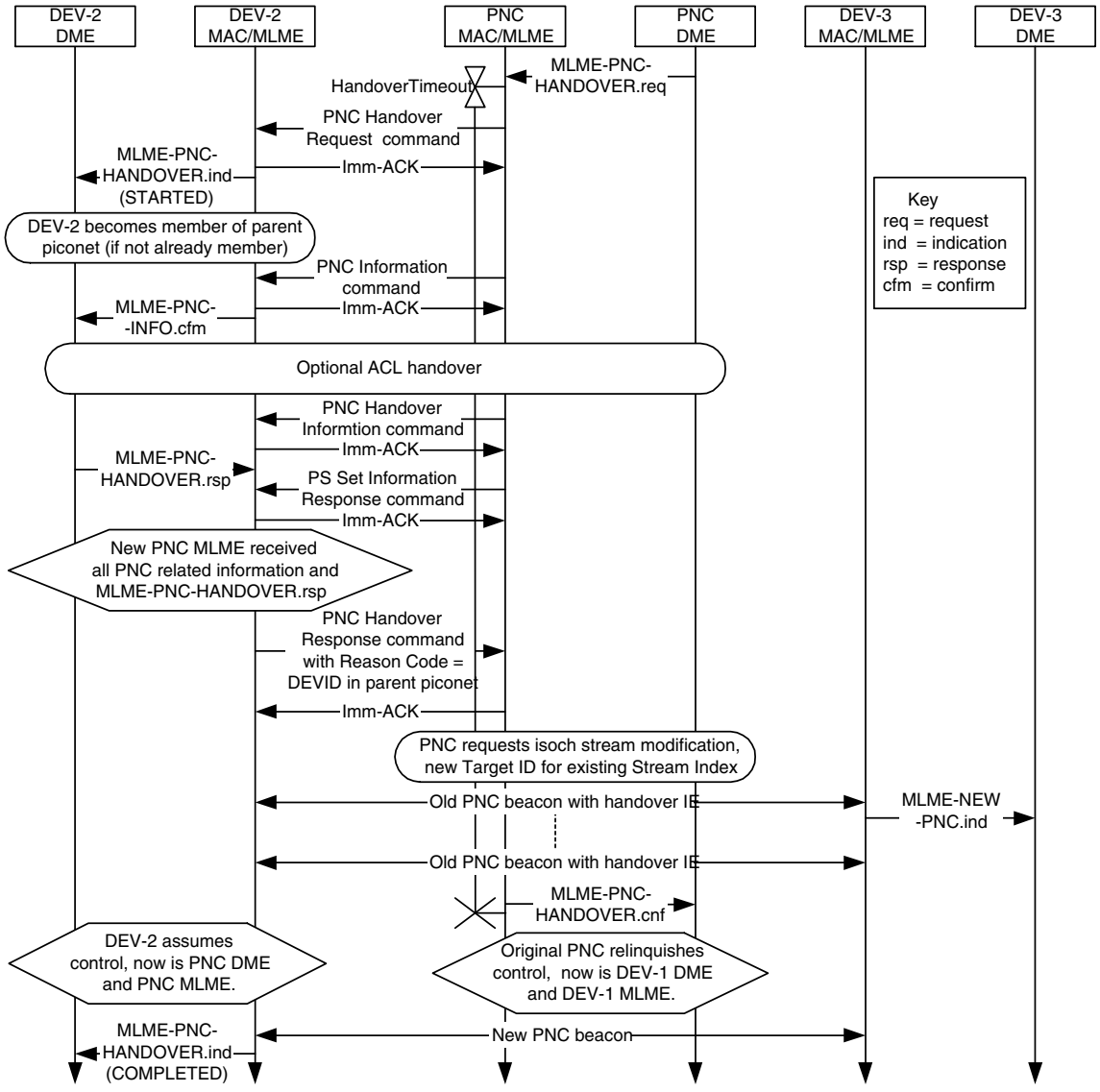

Figure 12—Successful PNC handover in a dependent piconet.

Once the transfer of the information is complete and target DEV has joined the parent piconet, the target DEV shall send a PNC Handover Response command to the dependent PNC with a Result Code set to the

DEVID that was assigned to it by the parent PNC. This lets the dependent PNC know that the target DEV is ready take over control of the piconet. At this point, the dependent PNC shall send a Channel Time Request command to the parent PNC to handover the control of the dependent piconet CTA to the new dependent PNC, {xref 8.5.1.2 stream modification}. Once the parent PNC changes the SrcID and DestID of the dependent piconet CTA, the current dependent PNC shall either complete the handover process to the new PNC or it shall shutdown the dependent piconet because it will not be able to regain control of the CTA.

After the dependent PNC receives a beacon from the parent PNC with the change in the SrcID of the dependent piconet CTA, the current dependent PNC shall begin placing the Handover IE in its beacon with a countdown to indicate the last superframe that it will be the PNC using the procedure indicated in {xref 8.2.3}. The last superframe controlled by the current dependent PNC will be the one in which the Handover Countdown field is zero. The following superframe will begin when the target DEV, now the new dependent PNC, sends its first beacon.

There are multiple points in the handover process where it can fail. The current dependent PNC may cancel the handover process up until the time that it requests that the parent PNC handover control of the dependent piconet CTA to the new dependent PNC. The dependent PNC cancels the process by sending PNC Handover Request command to the target DEV with the Handover Status field set to 1 to indicate that the process has been cancelled.

The handover process will also fail if the target DEV fails to join the parent piconet. If the target DEV attempts to join as a neighbor PNC and the parent PNC does not support neighbor PNCs or does not wish to allow any more neighbor PNCs, then the association request by the new dependent PNC will be rejected. In that case, the DEV may also try to join as a regular DEV, in which case the dependent piconet would become a child piconet after the handover process.

If the target DEV fails to join the parent piconet as either a regular DEV or as a neighbor PNC, it shall send the PNC Handover Response command to the dependent PNC with the Reason Code set to ‘Handover

refused, unable to join parent piconet' as illustrated in Figure 13. The target DEV may refuse the handover at any time while the dependent PNC is sending over the information about the piconet.

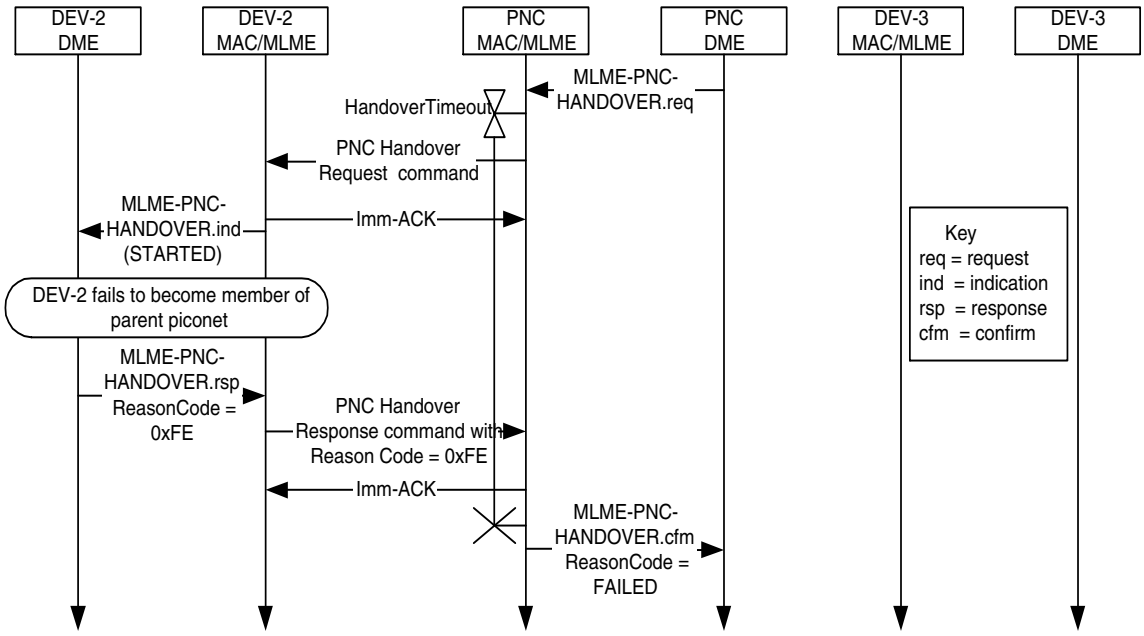

Figure 13—Failed dependent PNC handover when target DEV fails to join parent piconet.

If the parent PNC rejects the request to handover control of the CTA to the new dependent PNC, the dependent PNC shall send a PNC Handover Request command to the target DEV with the Handover Status field set to 1 to indicate that the handover process is being cancelled, as illustrated in Figure 14.

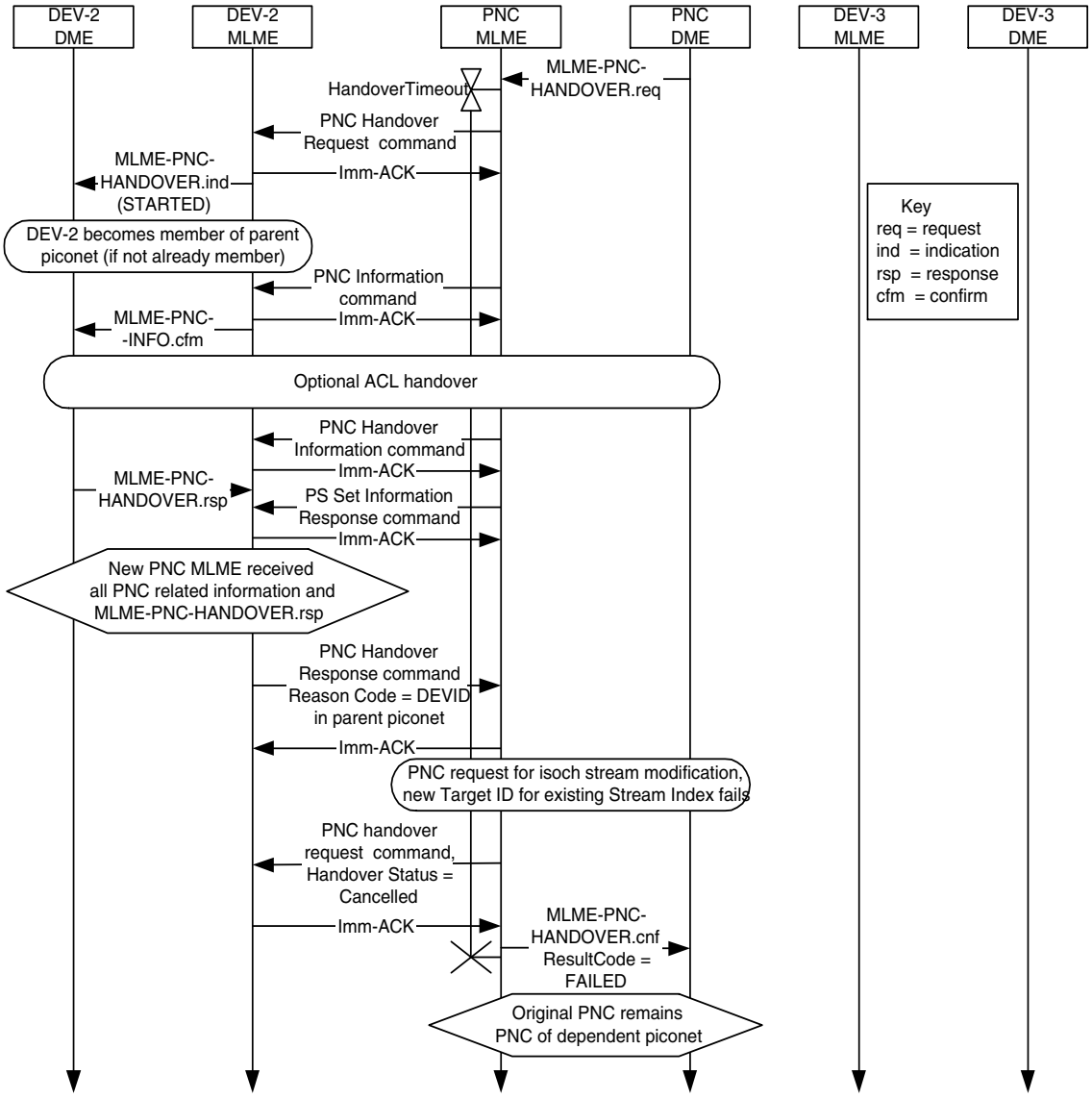

Figure 14—Failed dependent PNC handover when control for the dependent piconet CTA is handed over in the parent piconet.

If the dependent PNC cancels the handover process, the target DEV may disassociate from the parent picoent. If DEV-2 joined the parent picoent as a neighbor PNC, it should disassociate from the parent piconet if the handover process is cancelled to free up that resource for other DEVs that may want to form a neighbor piconet.

(end of new text for new subclause 8.2.4)

Resolve CIDs 1, 215, 352 and 139 as Accept in principle “Add the ability to handover the dependent PNC as indicated in 03/032r8.”

Meeting adjourned at 10:04 am PST.

1.14 Tuesday, 28 January 2003

Agenda

Roll call
Resolve comments, CIDs 357, 14, 21, 425, 677, 682, 331
Adjourn

Attendees: John Barr, James Gilb, Allen Heberling, Bill Shvodian, John Sarallo, Jay Bain, Ari Singer, Rene Struik, Mark Schrader.

Meeting called to order at 8:07 am.

CID 357 - (comment text and suggested resolution appears elsewhere in this document, suggestion is to reduce the fragmentation field by one octet). **Suggest reject:** "The current fragment fields allow a receiver of a fragment to know exactly how many fragments are in a fragmented MSDU no matter which fragment of the MSDU is received first. This allows an implementation the flexibility to be able to reassemble an MSDU in order in contiguous memory if that is desired. In the proposal in this comment, a receiver will not know how many total fragments are in the MSDU unless the first fragment is received first. Fragments can be received out of order when delayed ACK is used."

Resolution is to Reject as indicated above.

CID 14 (Bailey, TR) The MAC currently has no PIB group for peer to peer relationships. Replicate Table 37 for peer to peer relationships. **Suggest accept in principle.** Add the following subclause after 6.5.5.

(begin new text)

1.14.1 MAC PIB peer security group

The MAC PIB peer security parameters group, Table 9, describes the security relationship that the DEV has with a peer DEV and the current status of the keys and security parameters that are in use for that security relationship. The DEV shall maintain one set of MAC PIB peer security group parameters for each DEV with which it shares a security relationship. The DEV shall not maintain more than one MAC PIB peer security group parameters table with the same MACPIB_PeerDEVAddress and first byte of the MACPIB_ManagementSECID, which corresponds to the security manager in the relationship, see {xref 9.3.9}.

Table 9—MAC PIB peer security group parameters

Managed object	Octets	Definition	Type
MACPIB_PeerDEVAddress	6	DEV address for the peer DEV.	Dynamic
MACPIB_ManagementSECID	2	The security session ID that is currently active for the management key.	Dynamic
MACPIB_DataSECID	2	The security session ID that is currently active for the data key.	Dynamic

Table 9—MAC PIB peer security group parameters

Managed object	Octets	Definition	Type
MACPIB_ManagementKeyInfo	Variable	The keys agreed upon during authentication that are used for protecting commands.	Dynamic
MACPIB_DataKeyInfo	Variable	The keys that are currently active that are used for protecting data.	Dynamic

(end new text)

Accept in principle "Delete subclause 6.5.5 and table 37. This information is passed by the MLME-SECID-UPDATE.primitive."

CID 21 (Bailey, TR) Impact of child/neighbor piconets on security needs further definition. Update clause 9.3.2 to detail that a child PNC is handled just like any other DEV and a neighbor PNC is allowed to send a subset of commands without security. **Suggest accept in principle.** In table 66, add an 'X' to the 'None' column for channel time request and channel time response and add the following text in the 'Comment' column: 'If the communicating parties are the PNC and a neighbor PNC, the channel time request (resp. channel time response) command shall not be protected with any key. Otherwise, the PNC-DEV management key shall be used.' In 8.2.5, add the following text at the end of the first paragraph: 'Note that a neighbor PNC does not authenticate with the PNC, so a PNC operating in mode 1 may reject the request for the neighbor piconet for security reasons.'

Accept suggested resolution. In table 66, add an 'X' to the 'None' column for channel time request and channel time response and add the following text in the 'Comment' column: 'If the communicating parties are the PNC and an un-authenticated neighbor PNC, the channel time request (resp. channel time response) command shall not be protected with any key. Otherwise, the PNC-DEV management key shall be used.' In 8.2.5, add the following text at the end of the first paragraph: 'A neighbor PNC is not required to authenticate with the PNC, and so a PNC operating in mode 1 may reject the request for the neighbor piconet.' Add to page 171, line 31, 'any probe commands required for the authentication process' (Ed. note: Consider making this a list)

CID 425 (Ho, TR) Definition for MLME-SECID-UPDATE.confirm missing! Create a subclause to define the MLME-SECID-UPDATE.confirm primitive. **Suggest reject.** No frames are sent or received as a result of the MLME-SECID-UPDATE.request primitive and the only information that might need to be passed back to the DME would be if there was a memory failure of some kind that prevented the DME from being able to update or add the data, which is outside the scope of the MLME commands.

Resolution is to reject as indicate above.

However, if the group disagrees with this assessment, add the following entry to Table 15 and the following sub-clause after 6.3.11.1. Note that if we decide that this kind of thing is worth mentioning, we might also want to add a command that securely deletes a security relationship. This is an important function that either the DME or MAC needs to be able to implement anyway to protect keys from being compromised and to free up memory.

Table 10—MLME-SECID-UPDATE primitive parameters

Name	Type	Valid range	Description
ResultCode	Enumeration	SUCCESS, MEMORY-FAILURE	Indicates the result of the MLME-SECID-UPDATE.

(begin new MLME text)

1.14.1.1 MLME-SECID-UPDATE.confirm

This primitive reports whether the appropriate authentication relationship was included or updated. The semantics of the primitive are as follows:

```
MLME-SECID-UPDATE.confirm    (
                             TrgtID,
                             SECID,
                             KeyType,
                             SecurityManager,
                             ResultCode
                             )
```

The primitive parameters are defined in Table 10.

1.14.1.1.1 When generated

The MLME sends this request to the DME after attempting to add a new authentication relationship or update an existing authentication relationship.

1.14.1.1.2 Effect of receipt

The DME is notified whether the authentication relationship was successfully added or updated.

(end new MLME text)

CID 677 - Incorrect illustrations in Figure 107, Figure 108, and Figure 109. Change "SIFS" to "MIFS" in Figure 107 (3 occurrences). Delete "CTR time unit" (which does not necessarily cover a whole frame plus MIFS due to variable frame sizes) from all the three figures. Change "SIFS" to "MIFS" after "Frame 1" and "Frame 2", respectively, in Figure 109. **Suggest accept**

> Accept in principle ‘Change "SIFS" to "MIFS" in Figure 107 (3 occurrences). Change "SIFS" to "MIFS" after "Frame 1" and "Frame 2", respectively, in Figure 109’

CID 682: - **Suggest accept in principle:** The inclusion of MIFS changed the CTR calculations, but the changes were not reflected in 8.4.4.6. ‘1)Change b3 in Figure 79 from “stream termination” to “MIFS CTRq TU”. 2)Replace page 152, line 12 with:

> ‘The MIFS CTRq TU bit indicates that the CTRq TU includes MIFS, not SIFS as described in 8.4.4.6. When the MIFS CTRq TU bit is set to one the PNC shall allocate SIFS-MIFS additional time to the CTA so that there is at least a SIFS duration between the last transmission in one CTA and the first transmission in the next. Otherwise, the SIFS is included in the CTRq TU.’

3)Move 8.4.4.6 after 8.4.4.7 since 8.4.4.6 refers to guard time. 4)Modify 8.4.4.6 as follows:

1.14.1.2 Calculating channel time requests

Each DEV sends channel time requests to the PNC to indicate the amount of channel time required for transmission.

The requesting DEV shall include the frame transmission time, if known *a priori*, and the ACK transmission time, if used, and MIFS or SIFS time as appropriate per frame or ACK when calculating channel time

requests. Figure 15 (was #108) shows an example of channel time being requested for a CTA where Imm-ACKs are used.

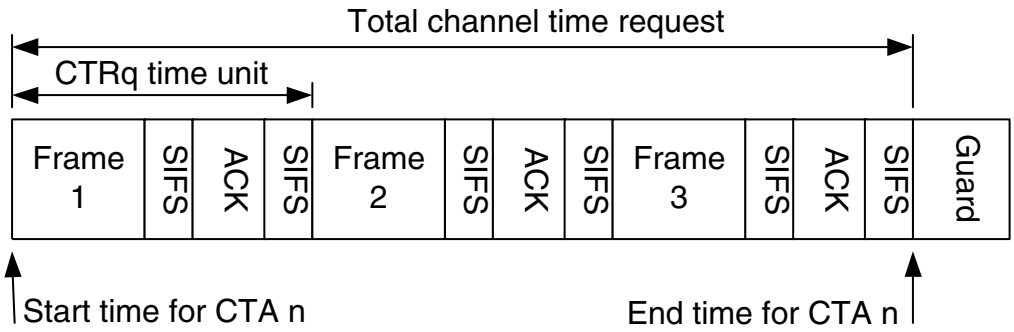

Figure 15—Channel time request for frames with immediate ACKs

When No-ACK is used, the channel time request is calculated differently because there is a MIFS in between each frame in the CTA instead of a SIFS. A channel time request that uses a CTRq TU with MIFS instead of SIFS shall set the CTRq TU MIFS bit to one to inform the PNC that it must add a time equal to SIFS-MIFS to the end of the CTA. This ensures that there is a SIFS between the end of transmission in one CTA and the start of the next. Figure 16 shows an example of a channel time request when no-ACK is used and the MIFS bit is set in the Channel Time Request command.

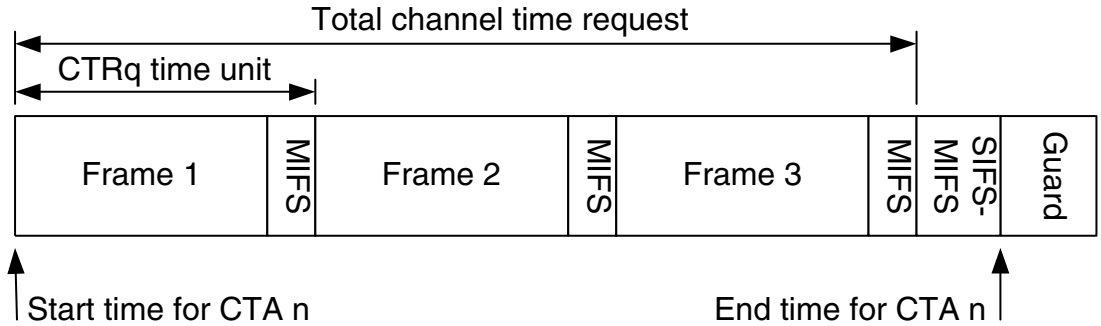

Figure 16—Channel time request with no ACKs

A CTRq TU in the CTA may cover more than one frame as shown in Figure 17. If the requesting DEV included SIFS-MIFS following the last MIFS as shown in Figure 17 it shall set the CTRq TU MIFS in the

Channel Time Request to “0.” IF SIFS-MIFS is not included in the CTRq TU, the CTRq TU MIFS bit shall be set to “1” and the PNC shall add SIFS-MIFS to the CTRq TU to calculate the duration of the CTA.

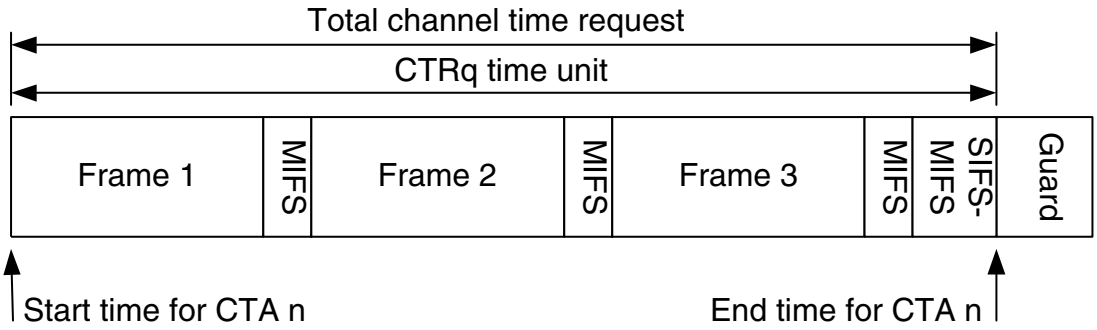

Figure 17—CTRq time unit covering multiple frames with no-ACK policy

(end new text for CID 682)

Accept in principle with the text above and an additional figure for the time when the CTRq TU does not include the SIFS.

CID 331 - (the I’m awake bit). Suggest accept in principle: “1) Add add an octet to the DEV capabilities field in Figure 39. 2) Add an octet to the DEV capabilities field in Figure 40.

1 bit is the "Always AWAKE" bit

1 bit is the "Listen to Source" bit

1 bit is the "Listen to Multicast" bit

5 reserved bits

3) Add the following text to 7.4.12

When set to "1", the "Always AWAKE" bit indicates that when the DEV is in ACTIVE mode it will listen to all CTAs, regardless of the DestID or SrcID. The bit shall be set to zero otherwise.

When set to "1" the "Listen to Source" bit indicates that when the DEV is in ACTIVE mode it will listen to all CTAs with the SrcID equal to the DEVID of a DEV that is currently the source of a stream to that DEV regardless of the DestID of that CTA. The bit shall be set to zero otherwise.

When set to "1" the "Listen to Multicast" bit indicates that the DEV will listen to all multicast CTAs regardless of the SrcID or the Stream Index. The bit shall be set to zero otherwise.

4) Add the following text to 8.4.4.2

All AWAKE DEVs shall listen to CTAs with the BcstID as the DestID and shall receive frames with the BcstID as the DestID. All DEVs shall listen to CTAs with their DEVID as the DestID and shall receive frames with their DEVID as the DestID. (Replace the first two with some sort of xref to the table in 8.1.2) DEVs with the "Always AWAKE" bit set in the DEV Capabilities field shall listen to all CTAs in the superframe.

DEVs with the "Listen to Source" bit set shall listen to all CTAs with the SrcID equal to any DEVID that is currently the source of a stream for that DEV. DEVs with the "Listen to Multicast" bit set shall listen to all CTAs with the destID equal to the McstID.

5) As below:

While we're at it, the sentence before Table 63 (line 5, page 215) says:

"Figure 63 lists the rules for the four modes of operation defined in this standard. Each cell indicates the state required, either WAKE or SLEEP, for the DEV."

This should say AWAKE, not WAKE

(end new text for CID 331).

Accept in principle, the two sentences need some work.

Dly-ACK, out order reception. Use option d) (see Knut's email) for simplicity. The destination decides when to pass up the frames and discards any newly received frames that would create an out of order delivery problem.

Change the definitions of SECID to be 'two octets' instead of integer in clause 6.

Update section 7.2.7.1 to include the definition of the octets in the SECID:

The SECID field shall be included in the frame body of all secure frames. The SECID field contains a 2-octet identifier for the key that is being used to protect the frame. The first octet of the SECID for all keys except the piconet-wide group data key shall be set to the DEVID of the security manager in the relationship. The SECID for the piconet-wide group data key shall have the first octet set to the BcstID, 7.2.3. The second octet shalldesignate a unique value for the key associated with the securityrelationship. The SECID for a given key is selected by the security manager in the secure relationship, 9.2.9. The SECID for management keys is communicated to a DEV in a successful authentication protocol by the security manager in the challenge request command 7.5.2.3. The SECID for data keys is communicated to a DEV by the security manager in a distribute key request command, 7.5.2.7, or a request key response command, 7.5.2.6.

Change section 9.2.9 to read:

For each management and payload protection key used in the piconet, the security manager in the relationship shall select the 2-octet SECID that identifies the key following the definition of a SECID {xref 7.2.7.1}.

Meeting adjourned at 9:22 am, PST.

1.15 Thursday, 23 January 2003

Agenda

Roll call
Assign orphan CIDs 821, 576, 510, 172,
Resolve comments, CIDs 546, 528, 350
PM/PS mode naming: CIDs 394, 511, 586, 769, 477, 509
Fixes: CIDs 35, 47, 347, 342, 774, 59, 606, 820.
Adjourn.

Meeting called to order at 9:08 am PST.

Roll call: Allen Heberling, Bill Shvodian, Rene Struik, James Gilb, Mark Schrader, John Sarallo, Jay Bain, Dan Bailey, Ari Singer.

CID 546 **Suggest reject.** The two fields 'max burst' and 'max frames' have two different uses. 'Max burst' indicates how many frames of the pMaxFrameSize length the destination can handle in one dly-ACK burst sequence. This value represents a buffering limitation in the destination DEV, i.e. what is the total storage capacity for data frame payloads that can be alloted before the destination MAC needs to get chance to process a burst. The destination may also be designed to arbitrate memory between different streams, e.g. every stream get a limited amount of memory, or every stream gets access to more memory for a limited time. The source DEV may send more frames than 'max burst' if their total frame body lengths are shorter than or equal to pMaxFrameSize * max burst. The 'max frames' field indicates another limitation in the destination DEV. The receiver function may only be able to store a certain amount of the 16 bit MPDU-IDs. There may also be a limitation of storage capacity for headers. These two limitations may also be per stream, totally, or any other implementation dependent limitation. A common application domain for 802.15.3 is low cost, low power, limited footprint devices with very limited amount of memory, so the protocol must provide a method to communicate such restrictions between the destination and source devices.

Resolution is to reject as above.

CID 528 (Barr) - Incorrect specification in line 17. Delete the last statement of the 3rd paragraph. **Suggest accept in principle.** "This text replaces the 3rd paragraph of clause 7 on page 107 lines 14-17:

> 'For a frame to be correctly received by the MAC it shall pass the frame check sequence, have a protocol revision supported by the MAC, have a DestID equal to DEVID, BcstID, McstID or when applicable the PNCID or UnassocID, and have a PNID equal to the PNID of the piconet with which the DEV is synchronized. The MAC shall ACK all correctly received frames with ACK policy set to either Imm-ACK or Dly-ACK and DestID is the DEVID or when applicable the PNCID. If a DEV correctly receives a frame from an unassociated DEV it may ignore the frame and may choose not to respond to the frame. If authentication is required and a DEV correctly receives a frame from an unauthenticated DEV, it shall ignore the frame and shall not respond to the frame, except for the ACK, if the ACK policy is set to either Imm-ACK or Dly-ACK.'"

Accept in principle as indicated above.

CID 350 (Struik) - Incorporate proper security notions throughout the Draft, defined in line with well-established cryptographic practice. We give an example of improper usage: in Clause 3, Page 5, line 21, 'authentication' is confused with 'authorization', since 'authentication' refers to 'evidence as to the true source of information or the true identity of entities' (see, e.g., the Handbook of Applied Cryptography, or Slide 2 of 02/114r5), whereas 'authorization' refers to 'assurance that an entity may perform specific operations'. This improper/sloppy use of terminology leads to misleading claims regarding security services offered. The following terms in Clause 3 need more accurate definitions: authentication, authentic data, integrity code, key establishment, key management, key transport, nonce, symmetric key. I am - again - prepared to offer help, but this would assume flexibility and an open mind from the assistant security editor as well. Let us try again. **Suggest accept in principle:**

1.16 authentication: Process or protocol whereby one party obtains assurances as to the true identity of another party (entity authentication) or as to the true origin of data (data authentication).

1.17 authentic data: Data with assurances as to the true origin hereof.

1.18 key establishment: Process or protocol whereby a shared secret becomes available to two or more parties, for subsequent cryptographic use.

1.19 key management: Set of techniques and procedures supporting the establishment and maintenance of keying relationships between authorized parties.

1.20 key transport: Key establishment technique where one party creates or otherwise obtains a secret value, and securely transfers it to the other(s).

1.21 nonce: A value that is used no more than once for the same purpose. It typically serves to prevent (undetectable) replay.

1.22 symmetric key: key (=secret value) in a symmetric key cyptographic system.

Table for email discussion and suggestions. For definition of authentication, need understand impact in the draft.

1.22.1 PM/PS naming

CID 394, 511, 586, 769, 477, 509

Use PM for the four modes. Use PS for the three modes, SPS for the two modes, PSPS and DSPS (DEV synchronized power save). Use APS for HIBERNATE, asynchronous power save.

CID 394 - Incorrect statement in the last paragraph in line 47. Replace "In addition to the power save modes" with "Regardless of the power management mode"

ACCEPT.

CID 511 - Naming inconsistencies: The names of some parameters in Tables 29 and 30 and the following primitives are different from those of the corresponding fields defined in 7.5.7 for the related commands. Throughout 6.3.24, change 'PSSwitchOperation" to "NewPMMode", "PSSetOperation" to "OperationType", "PSStructureSet" to "PSSetStructureSet" (this change is especially essential since it means a set of sets), "DEVIDMapLength" to "BitmapLength", and "DEVIDMap" to "DEVIDBitmap".

ACCEPT IN PRINCIPLE “Throughout 6.3.24, change 'PSSwitchOperation" to "PMMode", "PSSetOperation" to "OperationType", "PSStructureSet" to "PSSetStructureSet" (this change is especially essential since it means a set of sets), "DEVIDMapLength" to "BitmapLength", and "DEVIDMap" to ‘DEVIDBitmap’”

CID 586 - Incorrect naming: As noted by this commenter earlier, the term "PS mode" is used to mean "PM mode" (power management mode), which includes ACTIVE mode and other modes (i.e., PS modes), and truly PS mode. Change PS to PM (power management) when it references all power management modes.

ACCEPT.

CID 769 - Confusing and incorrect definitions for power management modes, power save modes, power states, and their relationships: ACTIVE mode is NOT a power save mode as is often confused throughout this draft. A DEV may be in "AWAKE" state beyond the time when it is either transmitting or receiving. For instance, a DEV may be in "AWAKE" state when the channel is idle. A DEV may not be in a "SLEEP" state even if it is neither transmitting nor receiving. Rewrite the first paragraph as follows: ‘There are four power management (PM) modes defined in this standard, ACTIVE, HIBERNATE, PSPS, and SPS modes. The latter three modes are collectively referred to as power save (PS) modes. A DEV that is in ACTIVE, HIBERNATE PSPS, or SPS mode is said to be an ACTIVE DEV, a HIBERNATE DEV, a PSPS DEV, or an SPS DEV, respectively. In any given PM mode, a DEV may have two power states, AWAKE and SLEEP states. A DEV in AWAKE state is able to transmit and receive and is fully powered, while a DEV in SLEEP state is not able to transmit or receive and consumes very low power. A DEV, regardless of its PM mode, is

allowed to enter the SLEEP state during a CTA for which it is neither the source nor the destination, and between CTAs other than the beacon times and CAPs. A DEV is allowed to enter the AWAKE state during any time when it is in a power save mode.'

ACCEPT IN PRINCIPLE "Rewrite the first paragaph in 8.13 as follow: 'There are four power management (PM) modes defined in this standard, ACTIVE, APS, PSPS, and DSPS modes. The latter three modes are collectively referred to as power save (PS) modes. A DEV that is in ACTIVE, APS, PSPS, or DSPS mode is said to be an ACTIVE DEV, an APS DEV, a PSPS DEV, or a DSPS DEV, respectively. In any given PM mode, a DEV may be in one of two power states, either AWAKE or SLEEP states. AWAKE state is defined as the state of the DEV where it is either transmitting or receiving. SLEEP state is defined as the state in which the DEV is neither transmitting nor receiving. A DEV, regardless of its PM mode, is allowed to enter the SLEEP state during a CTA for which it is neither the source nor the destination. A DEV is also allowed to enter the AWAKE state during any time when it is in a power save mode.' The AWAKE and SLEEP states in the standard are defined based on their affect the operation of the piconet. The operation of the piconet is only affected by the DEV either transmitting or receiving. The state where the DEV is neither transmitting nor receiving but is still powered up is equivalent to the state where the DEV is completely turned off from the point of view of the other DEVs in the piconet. The only charactertistics that affect the piconet operation are that the DEV is either receiving or transmitting."

CID 477 - Confusing naming. "Rename "CTR type" to "Power Type" throughout the draft."

ACCEPT IN PRINCIPLE. "Rename "CTR type" to "CTA PM Type" throughout the draft."

CID 509 - Change "PS mode" to "PM mode", "PS modes" to "PM modes" and "PS-MODE" to "PM-MODE" throughput this subclause, including the tables therein.

ACCEPT IN PRINCIPLE. "Throughout sub-clause 6.3.24 and its tables, when the term 'PS mode' refers to all four modes use 'PM mode' instead, including in the naming of the MLMEs. This will affect the MSCs and some of the text in clause 8 as well."

1.22.2 Fixes

CIDs 35, 47, 347, 342

35 - Accept in principle: The security suites will be removed so this change no longer needs to be made.
47 - Accept in principle: The security suites will be removed so this change no longer needs to be made.
347 - Accept in principle: The security suites will be removed so this change no longer needs to be made.
342 - Accept in principle: The security suites will be removed so this section will be deleted.

CID 774 - "All other CTAs and intervals" What interval? CTR, SPS, beacon, ... I suggest "All other CTAs and unallocated time"

Resolution is to update the resolution as indicated above.

CID 59: 8.6.4, page 198, line 35: "If any DEV is in PSPS or SPS mode, the first IE announcement shall be made in a system wake beacon." Comment: SPS devices don't (necessarily) listen to system wake beacons. Resolution: delete "or SPS" from text. Problem: the original text describes the PNC policy. The PNC must decide somewhere to start putting the IE. Hibernation and SPS DEV may ignore the announcements made in

the system wake beacon, but at least all DEVs should know where to look for such an announcement. A better solution: "If any DEV is in power save mode, the first IE announcement shall be made in a system wake beacon." This doesn't change any requirement on the DEVs, it is still only the PSPS DEVs (and ACTIVE of course) that shall listen, all others may.

Jay to provide suggested text.

CID 606: 8.2.3, page 165, line 23: "The parent PNC shall not hand over to a DEV that is currently operating as a dependent PNC." Comment: Remove restriction Resolution: Resolve as CID 139. Problem: CID 139, CID 215 and CID 352 deals with handover inside the dependent network, i.e. a dependent PNC handing over to a dependent DEV. The mentioned restriction has nothing to do with that. It says that the parent PNC cannot handover to the dependent PNC. This must still be true, because you have no way of merging the parent and dependent piconets. You will most likely get collisions in DEVID, StreamId, SPS Id, etc. A better solution: Leave this line as is. It is not related to the things you are trying to solve.

Knut to try at some text to explain that this does not mean merging.

CID 820 8.5, page 187, line 23: "Each DEV shall support at least one isochronous stream." PICS, page 393, Table E.4: MLF13 - Isochronous stream in a dynamic CTA - at least one - 8.5 - M Comment: Get rid of requirement in 8.5 Resolution: ACCEPT. Also delete from the PICS. Problem: Deleting requirement on DEV is OK, the problem is that if we delete the MLF 13 in the PICS we have no requirement that the PNC can allocate a single stream! We have the requirement that PNC cal understand a CT request command, but not that it can allocate a stream. Better solution: Change PICS from M to FD2:M

Should OK as is.

1.22.3 Dependent handover

CID 352 (Gilb) - What happens in the event of a handover of the child PNC, where the new child PNC is not part of the parent piconet?

CID 139 (Gilb) - The current draft does not provide support by the Parent PNC for the handover of the dependent PNC to another DEV in the dependent piconet. For example, the DEV chosen for handover may not be a member of the parent piconet. It may not be possible, due to security or physical limitations, for the DEV to join the parent piconet. Fix handover of dependnet PNCs or delete dependnet networks from the draft.

CID 215 (Gilb) - Is PNC handover permitted within dependent piconets? If "yes," should not the handover procedure incorporate the parent piconet? If it weren't permitted, how would, e.g., the new PNC get apprised of the parent PNC's change, if one were to happen? So it would seem that some form of communicability requirement within the dependent piconet is required with the parent PNC ... Please clarify- either explicitly state that such behavior is permitted or forbidden & provide parental PNC approval if permitted.

CID 1 (Gilb) - This paragraph (clause) does not clearly specify how dependent piconets are handled during a PNC handover. Is CTRB information for a child piconet transferred to the new PNC? Is the new PNC obligated to determine where the CTA for the child piconet should go even though CTA information is not transferred to the new PNC? Is CTRB information for a neighbor piconet transferred to the new PNC even though the neigher PNC is not a member of the piconet that is being handed over? Is the new PNC obligated to determine where the CTA for a neighbor piconet should go even though CTA information is not transferred to the new PNC?

Add ‘Reason Code’ to PNC Handover Response command, reasons are ‘0 - Success, 1 - Refused, unable to join parent piconet, 2 - Refused, unable to operate an additional piconet’

In clause 8, need to say ‘only refuse if it is a dependent piconet and DEV is unable to join the parent piconet as a member or if the DEV is a dependent PNC already and is unable to simultaneously operate two piconets.’
Handing over channel time, restrict it to private CTAs, request must sent by the originator/source of the private CTA. It does it by sending an Channel Time Request command with the stream ID and a different TrgtID.’

Assign orphan comments:

510 - Jay, 172 - Heberling, 576 - Schrader, 821 - Schrader

Meeting adjourned at 10:30 pm.

1.22.4 CIDs still pending

CID 821 (??) Spec does not define what determines a "Lost Beacon". Is it just not receiveing a beacon frame type at the expected time? Or if data within the beacon is wrong or unexpected (such as PNID, DestID, SrcID, Time Token), such that the beacon be ignored and lost beacon counter incremented? Some of this is implied but not explicitly specified. Add table or text to describe which info within a beacon must be valididated. Section 8.6.3, "Beacon Reception," would be a good location for such info.

CID 576 (??) - Ambiguous definition in lines 5-6: How would this command be responded when the DestID is set to the BcstID? Describe the response or delete the statement.

CID 510 (??) Unspecific Valid range and Description in Tables 29 and 30. Replace "As defined in…" with specific valid range or description."

CID 172 (??) - [PiconetService] Seems there is a need for an MLME-PICONET-SERVICES.indication/response set of primitives. During association a DEV can set its PiconetServiceInquiry bit to request a list of piconet services from the PNC. The response to the services request bit is independent of the association response. Also I'm assuming that since the Services database is not managed by the MAC or MLME, that the PNC DME or some other protocol layer needs to receive some sort of notification that a request for services information has been received. Consequently, the current description of the piconet services functionality is incomplete and not acceptable. Add the missing MLME primitives regarding piconet services or delete all references to piconet services.

CID 721 (Odman) - Is the receiving MAC supposed to wait for any missing frames? If so, for how long? For instance, the sender sent 5 consecutive frames, of which frame 1 was not received by the recipient but was discarded by the sender after its last transmission (due to exceeding delay limit. Should the recipient hold all the received frames after frame 1 in waiting for frame 1? The issue is resolved in a similar mechanism defined in the latest 802.11e draft, which introduces a field in the frame requesting a Dly-ACK to indicate a Sequence Control value such that all frames with a smaller Sequence Control value have been discarded by the sender and hence should not be awaited by the recipient. This expedites the delivery of received frames to the upper layer in the case of missing frames at the recipient. Resolve this synchronization issue.

CID 72 (Bain) - Other specifications of management attibutes typically call out not only the static vs. dynamic nature but also include the characteristic of "read", "write", and read/write. This standard should apply this to all PIB tables in clauses 6 and 11. make requested change.

CID 91 (Gilb) - I have a problem with this standard. I believe 15.3 should have been completely interoperable with 15.1, 15.3 and 11b. Although it seems that 15.3 has put some effort towards that goal, it did not take the last steps, whic are essential. The result is that 802 is now sending quite a confused message to the market. What device should the portable/mobile computer be equipped with? 11g? 15.1? 15.3? All of the above?

Neither? Does 802.15 have any roadmap towards some kind of unification? Despite of that, I voted "approve", because I appreciate the effort put into the standard. However, I would like to see, or more importantly, I want RevCom to see the group rebuttal, and I hope some effort towards a more interoperable WPAN standard is going to be made. Make the change as requested.

CID 216 (Gilb) - The paragraph seems to assume behaviors of equipment which don't exist- and can't exist without some kind of a PAR in 802.11. 802.11 AP's (not 11b AP's) do not have any optional or normative ability to request neighbor piconet status. And, change the paragraph to "802.11 overlapping with 802.15.3..." Remove the paragraph. However, coexistence in timeCAN be accomdated if the INFORMATION element that was approved (see 802.15.2 coexistence) is used by the 2.4GHz AP. Please state something to that effect.

CID 323 (Schrader) - Collecting channel status for each source DEV in the piconet will add a substantial burden to any simple DEV and it will provide questional benefits. Any DEV using ImmACK or Del-ACK will know if the frames are getting through. A DEV should be able to respond that it doesn't provide channel response statistics. Add the following sentence: A measurement window size of zero indicates that the responding DEV does not provide channel status statistics

CID 476 (Schrader) - Ambiguous statement in lines 15-16: What is an "ACTIVE channel time allocation" and what is an "SPS (not just PS?) channel time allocation"? Clarify the ambiguity.

CID 204, CID 254 (Heberling) - [MCTA] We need a little better specification on how often MCTA are allocated to assure that the PNCRespTime can be met. Please add this new text, starting after the sentence beginning: "When MCTA are used...": "The PNC shall allocate MCTA assigned to a DEV, open MCTA or both. The frequency of assigned MCTA shall be at least CTRRespTime, as defined in the beacon. If only open MCTA are used, the PNC shall allocate at least one open MCTA per DEV and CTRRestTime. The PNC may reduce the MCTA allocation frequency for power save DEVs, and for DEVs requesting a longer interval between assigned MCTA using the CTR command, 7.5.5.1. Special rules power save DEVs is listed in 8.13.1, 8.13.2.2 and 8.13.3"

CID 275 (Schrader) - The CTRB's CTR interval field is currently unused for async requests. It should probably be put to use. A couple of possibilities are suggested below. Other uses may also be useful. 1) One possibility is that for async CTRBs, the CTR interval type field be required to be 0 (super-rate), and the CTR interval field be interpreted in the usual super-rate fashion. 2) Another possibility is to use the CTRB's CTR interval field to encode the maximum amount of time the requestor can use during any single superframe.

CID 677 (Shvodian) - Incorrect illustrations in Figure 107, Figure 108, and Figure 109. Change "SIFS" to "MIFS" in Figure 107 (3 occurrences). Delete "CTR time unit" (which does not necessarily cover a whole frame plus MIFS due to variable frame sizes) from all the three figures. Change "SIFS" to "MIFS" after "Frame 1" and "Frame 2", respectively, in Figure 109.

CID 357 (Shvodian) - One can save 1 byte in each MAC header, by encoding information for the Fragment Control Field differently. The current encoding is unnecessarily wasteful. Suggested remedy: The Frame Control Field consists of 3 bytes, including the last fragment number, say N (7 bits), the current fragment number, say i (7 bits). Obviously, one has 0 £i£N. One uses the natural ordering of fragments: 0,1,2,3,...,N. Since, if a frame is lost in a stream, the whole stream is discarded, one can use the following more economical encoding for the Fragment Control Field: (a) Fragment number, say i (7 bits); (b) Indication as to whether a fragment is the first one (1 bit). Natural ordering of fragments: N,N-1, N-2, ..., 2, 1, 0. The 1-bit indicator (b above) indicates whether one is dealing with the first frame in a fragmented message or not. If so, one knows that the corresponding frame number is the highest one to expect. Then one just counts down. Note that the fragment number i now indicates the number of fragments one still has to receive. Adopting this encoding would save 6 bits compared to the current encoding. Moreover, one does not need to firmly now the total frame size in advance, only an estimate. So, accidental out-of-order receipt of the first fragment does not really hurt. The Frame Control Field (Clause 7.2.1) has 5 reserved bits. The Fragment Control Field

(Clause 7.2.4, with my suggestion) would have 7 reserved bits. Combining both the frame and the fragment control field and pooling reserved bits would yield 12 reserved bits. It seems reasonable to cut down this number of reserved bits by 1 byte (12 ® 4 reserved bits), thus cutting down the total number of bytes that has to be communicated in EVERY frame header (thus in every frame) by 1, from 10 to 9 bytes. Suggested remedy: Change the draft in line with the more economical representation given above and adapt all impacted text. The Frame Control Field consists of 3 bytes, including the last fragment number, say N (7 bits), the current fragment number, say i (7 bits). Obviously, one has 0 £i£N. One uses the natural ordering of fragments: 0,1,2,3,...,N. Since, if a frame is lost in a stream, the whole stream is discarded, one can use the following more economical encoding for the Fragment Control Field: (a) Fragment number, say i (7 bits); (b) Indication as to whether a fragment is the first one (1 bit). Natural ordering of fragments: N,N-1, N-2, ..., 2, 1, 0. The 1-bit indicator (b above) indicates whether one is dealing with the first frame in a fragmented message or not. If so, one knows that the corresponding frame number is the highest one to expect. Then one just counts down. Note that the fragment number i now indicates the number of fragments one still has to receive. Adopting this encoding would save 6 bits compared to the current encoding. Moreover, one does not need to firmly now the total frame size in advance, only an estimate. So, accidental out-of-order receipt of the first fragment does not really hurt. The Frame Control Field (Clause 7.2.1) has 5 reserved bits. The Fragment Control Field (Clause 7.2.4, with my suggestion) would have 7 reserved bits. Combining both the frame and the fragment control field and pooling reserved bits would yield 12 reserved bits. It seems reasonable to cut down this number of reserved bits by 1 byte (12 ® 4 reserved bits), thus cutting down the total number of bytes that has to be communicated in EVERY frame header (thus in every frame) by 1, from 10 to 9 bytes. Suggested remedy: Change the draft in line with the more economical representation given above and adapt all impacted text.

CID 174 (Heberling) - [FrmFrmt] Figure 7 (Frame payload) and Figure 8 (Secure payload) indicate two different types of payloads, yet only the secure payload is partially described. Add a definition for the frame payload field. Also, add information to the secure payload definition to clarify the difference between the Frame payload and the secure payload.

CID 313 (Gilb) - The low EVM values for the QAM modes will require very flat amplitude and group delay responses from the transmit filters - and hence greater cost. It seems likely that any demodulator that implements the QAM modes will include an equaliser quite capable of correcting moderate amounts of distortion in the transmitter anyway. Allow the ideal receiver used to measure these parameters to include an equaliser - perhaps also specify some larger EVM values for an unequalised measurement to keep some limits on the level of distortion allowed.

CID 53 (Gilb) - It is presumed that the DME should have the values of rates for the PHY to allow calculation of CTRs. The PHY-PIB should have a list of actual rates cooresponding to the indexed data rate that the MAC relates to the PHY for each frame sent. make the requested changes.

CID 331 (Shvodian) - Early on, the power save text had a separate mode called reduced power save, wher a DEV didn't listen to slots (excuse me, CTAs) that were not assigned to him. At the time we decided that DEVs only ever listen to slots that are explicitly assigned to them. I now believe there is a case where it would be bemenficial to have DEVs that listen to all channel time regardless of the destination ID. Some have raised the issue of the ability to do statistical multiplexing between various streams effectively. There are some complicated ways to do this, but there is a simple way: have DEVs that are not power sensitive listen to all channel time, regardless of the assigned destination DevID.Add a capability bit to the PNC capabilities field (OK, this is not the best place for it but there are reserved bits) called "receive always." A DEV transmitting to another DEV that has the "receive always" bit set can send frames to that DEV in any CTA assigned to the transmitting DEV, regardless of the destination DEVID of the CTA.

CID 21 (Singer) - Impact of child/neighbor piconets on security needs further definition. Update clause 9.3.2 to detail that a child PNC is handled just like any other DEV and a neighbor PNC is allowed to send a subset of commands without security.

CID 299 (Bain) - The sentence "The association process does not wait for the piconet services command to complete." can result in problems. For example, if the association process completes before the PNC transmits the piconet services command, the newly associated dev would not receive the command because the command is addressed to the UnsssocID and not the associated DEVs newly aquired DEVID. Change: "If the DEV sets the piconet services inquiry bit, the PNC shall send the piconet services command, 7.5.4.6, with DestID set to UnassocID. The association process does not wait for the piconet services command to complete." To: "If the DEV sets the piconet services inquiry bit, the PNC shall send the piconet services command, 7.5.4.6, with DestID set to UnassocID before it allocates a DEVID to the associating DEV via the association response command."

CID 425 (Singer) - Definition for MLME-SECID-UPDATE.confirm missing! Create a subclause to define the MLME-SECID-UPDATE.confirm primitive.

CID 14 (Singer) - The MAC currently has no PIB group for peer to peer relationships. Replicate Table 37 for peer to peer relationships.

1.23 Tuesday, 21 January 2003

Attendees: James Gilb, Jay Bain, Allen Heberling, Bill Shvodian, Ari Singer, Knut Odman, John Sarallo, Mark Schrader, John Barr.

Meeting called to order at 8:09 am PST.

- Schedule for future calls and volunteers to host.
- Editing instructions
- Review of status of CIDs that need to be written.
- CIDs 721, 323, 204, 254, 357, 331 and 299
- - Assign responsible person
- - Assign due date.
- Drafting schedule for sponsor re-circulation.

Schedule will be 23 Jan. 2003 - ADH, 28 Jan. 2003 John Barr, 30 Jan. 2003 Ari Singer, 4 Feb. 2003 John Barr, 6 Feb 2003 James Gilb.

Editing instructions: James will mail out editorial instructions, schedule and spreadsheet.

John Barr will look into how TG4 mapped 48 bit to 64 bit (CID 117).

Review status - All CIDs assigned.

CID 416 - ACCEPT IN PRINCIPLE. Add the parameter here and add the SECID field to the frame formats in figure 59, 60, 61, 62. The SECID should not be included in the request key command nor appear in the request key indication MLME. A DEV is asking for the latest symmetric key from the security manager (PNID for shared key or DEVID for peer-to-peer key) when it issues the request key command. It does not know the current SECID for the peer-to-peer or piconet shared key, only the management key for the relationship. Section 7.2.7.1 describes the SECID field and how a security manager communicates new values of that key:

> "The SECID for management keys is communicated to a DEV in a successful authentication protocol by the security manager in the challenge request command 7.5.2.3. The SECID for data keys is communicated to a DEV by the security manager in a distribute key request command, 7.5.2.7, or a request key response command, 7.5.2.6."

The proper resolution of this comment should be:

ACCEPT IN PRINCIPLE. A DEV is always requesting the current symmetric key associated with a security relationship when using the request key command. By sending a request key command to the TrgtID DEV, the security manager will know which relationship (TrgtID-OrigID) to reference for the key. The request key indication provides the OrigID and should also provide the TrgtID contained in the frame so the DEV can determine whether this message if for the piconet security manager or the peer security manager. Add TrgtID following the OrigID parameter in the request key indication MLME. The target DEV must send back the current SECID with the latest symmetric key. For the distribute key command, the originating security manager must designate the SECID value along with the symmetric key. To complete the protocol, the receiving DEV needs to send back the SECID that it received. Add SECID field to the frame format in Figure 60, 61, and 62. On page 141, lines 38-39, remove the second sentence of the first paragraph of section 7.5.2.5, "The SECID is the unique identifier for the security relationship with which the distributed key is associated."

Accept.

The concern in CID 24 was that if a DEV fails to hear a beacon or chooses not to update its LastValidTimeToken when the key is changing, it will send a frame with a time token that doesn't match what other DEVs are using and the integrity code will fail. There is also the possibility of a DoS attack whereby an attacker inserts a beacon with a bogus SECID and a timetoken that is several seconds ahead of the current one. If it does this a few times, it might convince several devices that the time is far ahead of the actual time. When the device stops the attack, the beacon that the PNC is sending will have an "old" time token according to those devices and the beacon will be rejected until the time token catches up to the attacker's value (or the device gives up and disassociates). I think the following changes should solve the initial problem and make it so that the worst an attacker can do is trick a DEV into thinking the time token is aMaxTimeTokenChange - 1 away from the correct value.

Note that I also made a couple of additional fixes in the same area. I added a change in this text to point out that the beacon might be protected with the old piconet group data key, which will be the case after the PNC has sent the distribute key command but before the key is changed in the beacon (see 9.2.5). I also changed things so that the current time token is set when the device authenticates, not when it gets a valid beacon with a key it knows (this puts a time limit for the device to get a valid key within 65,000 superframes or so, but that shouldn't be a problem).

Otherwise, how can it verify the distribute key command? The risk is that an attacker might modify the time token in the beacon of the final authentication message, but if that time token value is integrity protected in the authentication protocol, the devices will detect it and the authentication will fail (which the attacker could cause anyway).

> (1) Page 233, lines 13-28: Change "An associated device that has not yet authenticated to the PNC and received the piconet group data key shall accept all secure beacons and ignore the integrity code, SECID and secure frame counter. After the DEV has received the piconet group data key, 9.8.6, and verified the integrity code on a beacon, it shall set the LastValidTimeToken to be the time token in that beacon. When a DEV receives a secure beacon frame (a beacon with the SEC field in the frame control field set to 1), the DEV shall determine if the received time token is greater than the LastValidTimeToken and less than the LastValidTimeToken + aMaxTimeTokenChange. If not, 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 beacon. The DEV shall also determine if the SECID matches the SECID of the piconet wide group data key stored in the MACPIB_DataKeyInfo field in the MAC PIB, see Table 37. If the SECID does not match, the DEV may set the LastValidTimeToken to the value in the beacon and send a key request command to the PNC to obtain the new piconet group data key. If both of these checks succeed, the DEV shall check the integrity code on the beacon using the piconet wide group data key .If this suc-

ceeds, the DEV shall accept the beacon and set the LastValidTimeToken to be the time token in the beacon."

to

"An associated device that has not yet authenticated to the PNC and received the piconet group data key shall accept all secure beacons and ignore the integrity code, SECID and secure frame counter. When the DEV has been authenticated, it shall set the LastValidTimeToken and CurrentTimeToken to be the time token in that beacon.

When a DEV receives a secure beacon frame (a beacon with the SEC field in the frame control field set to 1), the DEV shall determine if the received time token is greater than the CurrentTimeToken and less than the LastValidTimeToken + aMaxTimeTokenChange. If not, 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 beacon. The DEV shall also determine if the SECID matches the SECID of the piconet-wide group data key stored in the MACPIB_DataKeyInfo field in the MAC PIB, see Table 37, or the SECID of a valid old piconet-wide group data key, see 9.2.5. If the SECID does not match, the DEV may set the CurrentTimeToken to the value in the beacon and send a key request command to the PNC to obtain the new piconet group data key. If both of these checks succeed, the DEV shall check the integrity code on the beacon using the piconet wide group data key. If this succeeds, the DEV shall accept the beacon and set the LastValidTimeToken and CurrentTimeToken to be the time token in the beacon."

(2) Pg. 232, line 49: Change "current time token" to "CurrentTimeToken."

This still doesn't solve the problem if the DEV fails to hear a particular time token. I'm not sure if a DEV can operate properly in a superframe in which it misses a beacon anyway, but if it can, we could also add the following change:

3) Pg. 233, line 28: Add the following to the end of this paragraph. "If the DEV is able to determine that it missed a beacon or that the beacon was corrupted and if CurrentTimeToken is less than LastValidTimeToken + aMaxTimeTokenChange - 1, the DEV should increment the CurrentTimeToken to maintain synchronization with other DEVs in the piconet."

We might also add a note for clarity (if desired) after the second sentence of the second paragraph in the above text that says "Note that if the time token sent by the PNC is greater than LastValidTimeToken + aMaxTimeTokenChange, the DEV will never recover the correct time token and will need to re-authenticate in the piconet."

Resolution is to accept the changes.

CIDs 721 - Knut Odman due 1/24

CID 323 - Mark Schrader

CID 204, 254 - Allen Heberling, due 1/28

CID 357 - Bill Shvodian due 1/27,

CID 331 - Bill Shvodian due 1/27

CID 299 - Jay Bain due 1/24

Meeting adjourned at 90:12 am PST.

2. Comment resolution in Ft. Lauderdale

2.1 Thursday, 16 January 2003

Meeting called to order at 8:03 am EST

CID 152 - REJECT. Using the MIFS instead of the SIFS with no-ACK frames can provide an improvement in the throughput of 8%. One of the key applications of 802.15.3 is streaming applications such as music and video which typically would be sent with either a no-ACK or Dly-ACK policy. At 55 Mb/s this is equivalent to 4.4 Mb/s, almost enough for an additional SDTV stream. This does require that the receiver process unload its input queue somewhat faster, but this can be handled in hardware.

CID 154 - REJECT. The ASIE is intended to be included in the beacon as an announcement. A command cannot be sent in the beacon so the vendor specific command would not be applicable to solve this need. The ASIE was put in to enable new functionality for some DEVs without breaking compatibility for all DEVs. Since the TG cannot possibly forsee all uses that might be required, this is left to be defined by the vendors.

2.1.1 Dly-ACK

CID 544 - REJECT. The Max Burst refers to the size of the remaing buffer on the receiver, so therefore it would include frame 3 in the example. The Max Burst is re-negotiated each time Dly-ACK is used. In the example, if the buffer held 8 frames, after the first burst, 3 would be filed (frames 1, 3 and 5) and so the next Max Bust would be set to 5 instead of 8. If there no more space available, the DEV would set Max Burst would be equal to 1.

CID 545 - REJECT. While it would be clear to some implementers that this is for pMaxFrameSize, others may not make this interpretation. If it is obvious that these are all of pMaxFrameSize, then it doesn't change the specification to explicitly indicate that they are of that size here.

CID 546 REJECT. Two variables are needed, the total amount that can be sent as well as the number of frames that the destination DEV is able to handle. The number of frames is important because there are physical limitations in the Dly-ACK reception. The other reason is that there are physical limitations in the buffer implemention, e.g. addressing.

CID 333 - ACCEPT

CID 332 - ACCEPT. Resolve as indicated in CID 333.

CID 334 - ACCEPT IN PRINCIPLE. The terms 'right' and 'left' are ambiguous. Change 'concatenation' to be 'concatentated as the lower order octets' and 'appending' with 'appending as the lower order octets'

CID 335 - REJECT. The proposed resolution (in document 03/046r1) only replaces the equation with a sentence. Either are correct, but the equation is less likely to lead to misinterpretation. Finally, first M octets is unambiguous whereas 'left' and 'right' are open to interpretation.

CID 336 - ACCEPT IN PRINCIPLE. The terms 'right' and 'left' are ambiguous. Change 'concatenation' to be 'concatentated as the lower order octets'.

CID 337 - ACCEPT.

CID 340 - ACCEPT IN PRINCIPLE. Add text that indicates that the ACL will potentially contain more than 256 DEVs as you may want to keep track of DEVs that move in and out of the piconet.

CID 343 - Resolve in the same manner as other ‘remove Ntru comments’

CID 341 - REJECT. Annex C is an informative annex and information on the threat models is not required for proper implementation of the standard.

CID 342 - REJECT. Annex C is an informative annex to provide additional security considerations. They provide arguments that indicate why the present method was selected but are not part of the requirements for the standard. The security arguments are not required to ensure compliance with the standard.

CID 39 - Withdrawn, 16 January 2003.

CID 346 - REJECT. Annex C is an informatve annex. The analysis in Annex C is felt to be a proper analysis. The annex details the ways in which the present method differs from TLS and addresses those issues.

CID 20 - Withdrawn, 16 January 2003.

CID 15 - Resolve with ‘remove all security suites’

CID 16 - ACCEPT.

CID 409 - ACCEPT IN PRINCIPLE. Change the "Valid range" of "ResultCode" as follows: COMPLETED, TIMEOUT. Change the corresponding "Description" to "Indicates if the authentication request has received a response or timed out."

CID 410 - ACCEPT IN PRINCIPLE. "After "there is no" add "authentication". Replace "shall be set to" with "is" (2 occurrences). Change "SUCCESS" to "COMPLETED".

CID 518 - REJECT. There are only two security modes defined in the draft, modes 0 and 1.

CID 461 - ACCEPT.

CID 330 - Resolve as indicated in 21.

CID 47 - ACCEPT.

CID 35 - ACCEPT.

CID 345 - ACCEPT.

CID 413 - ACCEPT IN PRINCIPLE. "Replace "shall" with "is" (2 occurrences). Change "SUCCESS" to "COMPLETED"."

CID 416 - ACCEPT IN PRINCIPLE. Add the parameter here and add the SECID field to the frame formats in figure 59, 60, 61, 62.

CID 418 - ACCEPT.

CID 415 - ACCEPT.

CID 419 - ACCEPT.

CID 420 - ACCEPT.

CID 421 - ACCEPT.

CID 370 - REJECT. The request key response command will return only the key that was requested, see the resolution of CID 416. Freshness is ensure with the CCM nonce, Annex B.

CID 373 - REJECT. The DEVs know that they are sharing information with all of the DEVs in the piconet. If this is unacceptable, they can use peer-to-peer security. In some cases a group key for the piconet is sufficient security because only one entity will authorize access.

CID 27 - ACCEPT.

CID 13 - Withdrawn, 16 January 2003.

CID 444 - ACCEPT.

CID 399 - REJECT. The PNC is required in clause 8 to do a final scan prior to starting the piconet and so it may find all of the channels busy.

CID 400 - ACCEPT IN PRINCIPLE. Change 'If all of the channels for the PHY are occupied' to be 'If the requested channel is occupied'. The PNC is required to do a final scan before starting the piconet.

CID 305 - ACCEPT IN PRINCIPLE. Add text similar to below to clause 8.2.2, on page 163, around line 35 "When the piconet starts, the PNC allocates an additional DEVID to itself for the purposes of exchanging data with other DEVs that become members of the established piconet."

CID 601 - REJECT. The PNC may be required to scan multiple channels during the scan procedure. Thus selected channel may have not been scanned very recently and the new PNC could end up starting in a channel that has since become occupied. This takes a little longer but piconet startup is an infrequent event and scanning helps to prevent possible collision.

CID 41 - ACCEPT.

CID 566 - ACCEPT.

CID 764 - ACCEPT.

CID 767 - ACCEPT.

CID 508 - ACCEPT.

CID 56 - ACCEPT.

Meeting recessed at 10:04 am EST.

Meeting called to order at 10:34 am EST.

Removal of security suites.

What is required in the MAC?

- Symmetric key processing for payload protection
- Ability to ask the DME which DEVs are acceptable peers and members of a piconet.
- Ability to obtain and update symmetric keys.
- Provide security events to upper layer security manager.
- Processing of security events required to update how the MAC operates in a secure mode.

- Selective processing of commands and acceptance of frames based on security mode and state (which DEVs are authenticated).
- Definition of parameters used within the MAC that depend on a particular authentication security suite specification.
- Security command frames with undefined TLVs, auth, chal, dist key, req key.
- Add justification for why security related command frames are required in the MAC, e.g. request/distribute keys.
- Change ACL handover to be Security Information Handover.

What is not required in the MAC?

- ACL – The MAC should not maintain a separate list of authenticatable DEVs as this will be done in a higher layer.
- Any informative annex on possible security suites.
- Any protocol for authenticating peer or membership relationships.
- Any references to specific security suites.
- Any definition of 802.15.3 security suite ARC
- Define or modify authentication protocols.
- Specify parameters for a public key security suite used for authentication.
- Public key IE.

CID 375 - REJECT. This standard only deals with TG3 and the encryption specification is adequate for these data rates.

CID 64 - ACCEPT

CID 368 - ACCEPT IN PRINCIPLE. The ACL handover command will be changed to use LV elements so that no restrictions are placed on the data or verification methods. The command will be renamed to Security Information Exchange command.

CID 366 - ACCEPT IN PRINCIPLE. The ACL handover command will be changed to use LV elements so that no restrictions are placed on the data or verification methods. The command will be renamed to Security Information Exchange command.

CID 19 - ACCEPT IN PRINCIPLE. Remove the security suites and update the draft consistent with the criteria listed in 03/032r3.

CID 338 - ACCEPT IN PRINCIPLE. Remove the security suites and update the draft consistent with the criteria listed in 03/032r3.

CID 362 - ACCEPT IN PRINCIPLE. The public key IE will be removed from the draft.

CID 371 - ACCEPT IN PRINCIPLE. Remove the security suites and update the draft consistent with the criteria listed in 03/032r3.

CID 86 - ACCEPT IN PRINCIPLE. Remove the security suites and update the draft consistent with the criteria listed in 03/032r3.

CID 36 - ACCEPT IN PRINCIPLE. Remove the security suites and update the draft consistent with the criteria listed in 03/032r3.

CID 37 - ACCEPT IN PRINCIPLE. Remove the security suites and update the draft consistent with the criteria listed in 03/032r3.

CID 377 - ACCEPT IN PRINCIPLE. Remove the security suites and update the draft consistent with the criteria listed in 03/032r3.

CID 85 - ACCEPT IN PRINCIPLE. Remove the security suites and update the draft consistent with the criteria listed in 03/032r3.

CID 343 - ACCEPT.

CID 15 - ACCEPT IN PRINCIPLE. Remove the security suites and update the draft consistent with the criteria listed in 03/032r3.

CID 286 - ACCEPT IN PRINCIPLE. Add text to clause 8 that indicates that Dly-ACK frames are passed up as the MSDUs are correctly received.

CID 290 - ACCEPT IN PRINCIPLE. Add text to clause 8 that indicates that Dly-ACK frames are passed up as the MSDUs are correctly received.

CID 720 - ACCEPT IN PRINCIPLE. Add text to clause 8.7 and 8.8.3 that indicates that Dly-ACK frames are passed up as the MSDUs are correctly received.

CID 394 - Agree we are going to change names for power save mode and introduce a mode set that includes ACTIVE.

CID 388 - ACCEPT.

CID 118 - Withdrawn, 16 January 2003

CID 91 - JPKG will explain why interoperability was not required by our PAR and is out-of-scope.

CID 216 - JPKG will write text to explain that 802.11 APs do not support this behavior, but could if updates in 802.15.2 were adopted.

CID 101 - ACCEPT IN PRINCIPLE. The WG has adopted a motion to request a title change for the draft. When the title in the PAR is changed, the title in the draft will be changed to match.

CID 102 - ACCEPT IN PRINCIPLE. Change 'The Medium Access Control (MAC) sublayer protocol supports both isochronous and asynchronous data types and is designed to support additional physical layers as might be specified at a later time.' to 'The Medium Access Control (MAC) sublayer protocol supports both isochronous and asynchronous data types.'

CID 103 - REJECT. The current PAR only states that DEVs will support greater than 20 Mb/s, i.e. that the rate will be high enough, 20 Mb/s or more. All DEVs are required to support the 22 Mb/s mode so that this fulfills the requirment. Note that the quoted text says that 20 Mb/s is proposed to be the lowest rate, but it is not a requirement from the PAR.

Meeting recessed at 12:04 pm EST.

Meeting called to order at 1:11 pm EST

CID 266 - ACCEPT IN PRINCIPLE. Merging piconets is very complex and has been discussed in prior meetings. The group had decided not to provide this capability in the standard. The options that the DEV has are: Shutdown its piconet, join the new one. Handover control to another DEV, disassociate and join the new one. Join as a neighbor, etc.

CID 45 - ACCEPT IN PRINCIPLE. Add a length element wherever the PHY capabilities field occurs.

CID 294 - ACCEPT.

CID 140 - ACCEPT IN PRINCIPLE. Add the PNC address to the Piconet Synchronization Parameters and delete it from the Piconet IE. Rename the Piconet IE as the BSID IE. Change page 134, line 17 should say "e.g., the PNC MAC address is different,"

CID 821 - Write text that describes what is a valid beacon, i.e. it has the correct PNID and PNC MAC address and if security enabled it follows {9.x.x secure beacon reception}. Also define that 'Lost beacon' is not receiving a valid beacon at the expected time.

CID 713 - ACCEPT IN PRINCIPLE. After "recipient of" change "the IE" to "an IE" (2 occurrences). Change "IEs" before "shall" to "IE" (3 occurrences). Change "subsequent" to "consecutive" (3 occurrences). Use 'at least' in all the references to the number of repeated beacons. In line 42, change "the first IE announcement shall be made in a system wake beacon" to "the IE shall be announced in a System Wake beacon and at least the following mMinBeaconInfoRepeat-1 beacons". Line 43 is modified as indicated in CID 309.

Replace lines 46 and 47 as follows: "A CTA Status IE is considered to be intended for all DEVs if the DestID contained in that IE is the BcstID or McstID. Otherwise the CTA Status IE is intended for the DEV defined by the DestID."

The standard does not allow the BcstID or McstID to be used for SrcID except that the BcstID is allowed for an MCTA, but this CTA is not announced with a CTA Status IE. The SrcID of the CTA status IE is informed of this information with a directed Channel Status Response command that requires and ACK. The CTA Status IE main purpose is to inform the destination, not source.

CID 272 - ACCEPT IN PRINCIPLE. Allow the PNC to tx a command a SIFS following the terminating ACK for a non-PNC CAP PDU. Also mention that the PNC is allowed to use MCTAs to accomplish this.

CID 287 - ACCEPT IN PRINCIPLE. Delete 'Hence, once a DEV decrements its backoff counter to zero, it shall check whether there is enough time remaining in the CAP for the transmission of current frame and a SIFS interval.' Merge information from this page and 179 that deal with the same issue.

CID 324 - ACCEPT IN PRINCIPLE. Clarify that each transmission attempt, even for re-transmissions, is included in the total.

CID 576 - Add a description of the PNC using the BcstID as the destination for this command. Need to say that this is sent no-ACK and the PNC simply receives response from everyone who hears it, if they hear it, when they get chance to respond.

CID 449 - ACCEPT IN PRINCIPLE. Change 'The PNC or destination DEV shall not respond to any command from a DEV that is not allowed to be sent as indicated in Table 53. The PNC or destination DEV may transmit an ACK following reception of the frame if the ACK policy is set to Imm-ACK.' to be 'The PNC or destination DEV shall ignore any command from a DEV that is not allowed to be sent as indicated in {xref Table 53}. The PNC or destination DEV shall transmit an Imm-ACK following reception of the frame if the ACK policy is set to Imm-ACK.' Add a sentence to clause 7, 'A DEV shall not respond or ACK any frame that has a Protocol Version different from the one(s) that the DEV supports.'

CID 289 - ACCEPT IN PRINCIPLE. Defined in clause 5 "A Channel Time Allocation (CTA) is the channel time allocated by the PNC in response to a Channel Time Request Block (CTRqB) in a Channel Time Request." Change CTRB to CTRqB everywhere.

CID 570 - ACCEPT IN PRINCIPLE. Change the paragraphs as follows:

(note CTR Interval will change names due to the resolution of another comment.)

The CTR Interval Type field shall be set to one for a subrate CTA request and zero for a super-rate CTA request. A subrate CTA request indicates a need for a CTA every N superframes where N is greater than one, while a super-rate CTA request indicates a need for N CTAs in every superframe where N equals one or N greater than one.

The CTR Interval field specifies the value of N, as described above. For a subrate CTA request, the CTR Interval field value shall be a power of 2. A PNC shall support up to eight CTAs per superframe for each stream."

CID 275 - Allow the DEV to set this field to the max number of TUs it can use in a superframe as an asynchronous allocation. The PNC may ignore the field in creating its allocations. This is a request for a maximum number, not a requirement. 0 = as many as I can take, 1-255

CID 677 - Use MIFS where appropriate, add bit to the Channel Time Request command to indicate if MIFS or SIFS is included in the TU. PNC adds the difference between MIFS and SIFS to the end of the calculation.

CID 682 - ACCEPT.

CID 49 - ACCEPT.

CID 355 - REJECT. The symmetric key encryption is sufficient for the PAN space without adding additional complexity.

CID 528 - Sample text: Only correctly received frames shall be processed. Also add that the DestID needs to check. Add a definition of correctly received as FCS check, procotol revision check (see other comment on this), DestID is either DEVID, McstID, BcstID, PNID is the PNID of the piconet with which the DEV is synchronized. Shall ACK all correctly received frames with Imm-ACK and DestID is DEVID.

CID 227 - ACCEPT IN PRINCIPLE. Add the PNC address to the Piconet Synchronization Parameters and delete it from the Piconet IE. Rename the Piconet IE as the BSID IE. Change page 134, line 17 should say "e.g., the PNC MAC address is different,"

CID 356 - REJECT. This text is well accepted and is essentially the same as the text in 802.11.

CID 376 - REJECT. Authentication for multicast groups is outside of the scope of the PAR.

CID 129 - ACCEPT.

Meeting recessed at 3:05 pm EST.

Meeting called to order at 4:25 pm EST.

CID 313 - Lower the values, Jeyhan will provide reduction, currently at 30 dB, will reduce to at least 27 dB

CID 281 - ACCEPT IN PRINCIPLE. Change to 5 CAZAC sequences.

CID 132 - ACCEPT IN PRINCIPLE. Change from 4 to 5.

CID 282 - ACCEPT IN PRINCIPLE. Change from 4 to 5.

CID 131 - Withdrawn, 16 September 2003.

CID 52 - REJECT. The SIFS, MIFS and PHY header are low level timing information that would be required when the MAC was designed and therefore should be known to the DME as well.

CID 53 - Add information to the PIB

CID 510 - Names don't match with clause 7, change clause 6 names to match.

CID 511 - Change any names that don't match with clause 7 in clause 6.

CID 769 - Change PS names to new ones, however, for the purposes of the standard and interoperability AWAKE and SLEEP will keep the same definitions.

CID 263 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 225 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 321 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 162 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 512 - ACCEPT IN PRINCIPLE. Change the name from PSSwitchOperation to PSMode to match the frame formats. The frame formats in 7.5.7.1 only specify 3 states because PS is used to switch to PSPS, SPS or both SPS and PSPS.

CID 255 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 222 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 382 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 159 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 96 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 318 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 260 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 232 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 97 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 233 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 261 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 319 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 383 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 223 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 160 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 236 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 322 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 226 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 386 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 100 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 163 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 224 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 262 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 384 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 320 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 161 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 98 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 234 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 235 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 385 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 99 - ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

CID 71 - ACCEPT IN PRINCIPLE. The BSID is set with either the MLME-START, MLME-START-DEPENDENT or MLME-PICONET-PARM-CHANGE and we will set the BSID to be read only in the PIB. Read only applies to the MLME-GET and MLME-SET.

CID 605 - John Sarrallo will write text to define PNC and non-PNC related traffic.

CID 244 - ACCEPT.

CID 606 - ACCEPT IN PRINCIPLE. However, the DEV needs to have the opportunity refuse handover, see the resolution of CID 139.

CID 610 - ACCEPT.

CID 135 - REJECT. Security policies are out of scope. If a DEV wants high security it should set its Des-Mode.

CID 2 - ACCEPT IN PRINCIPLE. The move with superframe timing field set to 0 solves this so that the dependent piconets know to listen for the next beacon.

CID 437 - ACCEPT IN PRINCIPLE. The DENIED code is no longer necessary due to changes in the ACL handover command. Delete 'DENIED'.

CID 438 -ACCEPT IN PRINCIPLE. Change "that DEV" to "the DEV of TrgtID". The request command asks for all of the security information that is managed by the QueriedDEVID, not just information about the QueriedDEVID.

CID 431 - ACCEPT.

CID 429 - ACCEPT.

CID 265 - ACCEPT IN PRINCIPLE. While a DEV could send a frame with the wrong PNID, the new text will require that no DEV in the piconet will ACK the frame because it has the wrong PNID. Text has been added as a part of the resolution of CID 528 to require checking the PNIC for ACK.

CID 267 - ACCEPT IN PRINCIPLE. The IE is limited to help limit the memory space required by the PNC and also to limit the size of the Piconet services command.

CID 300 - ACCEPT IN PRINCIPLE. The IE is limited to help limit the memory space required by the PNC and also to limit the size of the Piconet services command.

CID 172 - Add MLME for Piconet servies that matches the frame formats.

CID 605 - ACCEPT IN PRINCIPLE. Change: "The new PNC shall begin using the PNCID for all PNC related traffic, but it shall continue to use its previously assigned DEVID for all non-PNC traffic." To: "The new PNC shall begin using the PNCID as the SrcID for all beacon frame or command frames transmitted. The new PNC shall use the PNCID or its previously assigned DEVID as the SrcID for all data frames transmitted."

CID 206 - Withdrawn, 16 January 2003

CID 173 - Withdrawn, 16 January 2003

CID 205 - Withdrawn, 16 January 2003

CID 637 - ACCEPT IN PRINCIPLE. Add to the end of line 19 'After a DEV disassoicates from the piconet, the PNC shall delete the DEV's Piconet Services IE from its own record.' Note: All of the other DEVs will see the disassoicate announcement and can update their own internal storage by deleting the entry if they kept it.

CID 469 -ACCEPT IN PRINCIPLE. Rename the field name "Information elements" to "IEs Provided". However, when bit 0 is equal to zero, the other 31 bits are a binary represenation of the IE number, thus you can request Ies (one at time) up to an index of about 2^31, which is more than sufficient.

CID 732 - ACCEPT.

CID 149 - ACCEPT.

CID 5 - ACCEPT.

CID 398 - REJECT. The DEV is required to scan through all of the requested channels before it returns the .confirm. One reason for this is that DEV might find multiple piconets with the same PNID or BSID and it should report to the DME all of the relevant piconets that it defines.

CID 79 - Withdrawn, 16 January 2003.

CID 600 - REJECT. The DEV stays on the channel after it receives a frame so it can find the beacon associated with the piconet. If no frame is found, it stays on the channel for the ChannelScanDuration specified in the MLME-SCAN.request.

CID 264 - REJECT. The remote DEV determines the length of time that is used to scan the channel. The DME then informs the MAC/MLME to perform the scan using MLME-SCAN.request.

CID 82 - ACCEPT IN PRINCIPLE. Replace DEV characteristics with DEV characteristics IE, this allows expandability.

CID 502 - ACCEPT.

James Gilb asked the BRC if they felt that the resolution process had completed sufficiently to go forward to Sponsor Ballot recirculation. Everyone present indicated that they felt that we were ready to finish the editing and go forward to Sponsor Ballot recirculation. There is also agreement that there is much work to do and that careful review will be required.

Meeting recessed at 7:34 pm EST.

James Gilb moved to adjourn, seconded by Jim Allen, no objections

802.15.3 adjourned at 7:34 pm EST.

2.2 Wednesday, 15 January 2003

Meeting called to order at 8:00 am EST.

CID 275 - Table, MKS to provide text by Thursday morning on how to use it to limit max allocated async slots in a superframe.

CID 353 - (add to existing resolution) add the following section:

> 8.2.6.3 Dependent PNC termination of a dependent piconet
>
> After stopping piconet operations for its own piconet {xref 8.2.6}, a child PNC shall inform its parent PNC that it no longer requires channel time for child piconet operations by sending the parent PNC a channel status request command terminating the CTA used for the child piconet.
>
> After stopping piconet operations for its own piconet {xref 8.2.6}, a neighbor PNC shall inform its parent PNC that it no longer requires channel time for neighbor piconet operations by sending a disassociation request command to the parent PNC. Upon receiving a disassociation request command from a neighbor PNC, a parent PNC shall remove the CTA used by the neighbor piconet.

CID 328 - ACCEPT IN PRINCIPLE:

> 7.2.1.7 More data
> The More Data bit shall be set to 0 if the DEV will not use the rest of the channel time in that CTA, {xref 8.4.4.1}. The More Data bit shall be set to 1 when the PNC is sending an extended beacon, {xref 8.6.2}. In all other cases it shall be set to 1.

New paragraph in 8.4.4.1:
The More Data bit is set to 1 to indicate that the source DEV could be sending more frames in the CTA. In order to save power at the destination DEV, a source DEV may indicate that it will not use the remaining time in the current CTA by setting the More Data bit to 0. The source DEV may retransmit a frame with More Data set to 0 if an ACK is expected but not received. If the destination DEV receives a frame with the More Data bit set to 0 with ACK policy set to Imm-ACK or Dly-ACK, it should continue to listen for an implementation specific time after sending the ACK to make sure that the source DEV is not going to retransmit the frame because it did not receive the ACK. The source DEV may choose to send a zero length frame with the More Data bit set to zero when it has no more frames to send in a CTA.

The More Data bit shall be ignored by the destination for all frames sent in the CAP.

CID 81 - ACCEPT.

CID 4 - Table, John Sarallo to write more text to include that the child PNC needs to change its superframe duration as well.

CID 213 - REJECT. The PAN environment is very dynamic. DEVs move in and out of coverage as a normal course of operation. Unlike the Aps in 802.11, the PNC may also be moving and so it may move out of range of DEVs in the piconet. Even in the case where the PNC does not handover, DEVs will occaisionally lose contact with the piconet. The 802.15.3 standard is designed to provide recovery mechanisms for the times that the DEVs lose contact with the piconet, e.g. scanning for new piconet, the ability to automatically start a piconet if the PNC disappears, fast association time using BSID and PNID, the requirement for a channel scan prior to starting a new piconet. The association timeout period is used by both the PNC and DEV to detect when they have lost contact.

In the case of a home, the user is allowed to designate a DEV to be the PNC via the Des-Mode bit in the capability field. Thus the user is able select a central DEV with sufficient range and power to be the PNC and force it not to handover responsibilities.

CID 352 - Table, JPKG to provide MSCs for fixes.

CID 430 - REJECT. The DME already knows the mapping between DEVID and MAC address, in fact it is the DME and FCSL that map MAC addesses into DEVIDs, not the MAC or MLME. The other proposed parameters are not used by the DME. The handovder countdown is a local timing requirement of the MAC. The number of CTRBs is not passed to the DME because the CTRBs are used only by the MAC/MLME, 8.5.1.1 and 8.5.2.1. The number of SPS sets is only used by the MAC/MLME and is not used by the DME, 8.13.

CID 433- REJECT. The MSC in figure 98 shows that the MLME-PNC-HANDOVER.indcation is only used at the beginning and end of the handover process. At the beginning of the handover, the NmbrHndOvrBcns and the DEVInfoSet are not known by the new PNC. At the end of the handover process, the NmbrHndOvr-Bcns has no meaning and the DEVInfoSet has already been passed to the new PNC. If the .indication says that the handover process has been canceled, then neither of these parameters are required either.

CID 436 - ACCEPT IN PRINCIPLE. Add NewPNCDEVID and NewPNCDEVAddress, the Handover-Countdown is a timing parameter local to the MAC/MLME and doesn't have significance here.

CID 177 - ACCEPT IN PRINCIPLE. Add three more octets be to the left end of figure 41, with these parameters:|MaxTxPwr|MaxCTRBs|MaxAssociatedDEVs| Also modify figure 39 so that the PNC capabilities field length is now four octets and the Length field of the IE is increased from 2 to 5.

CID 176 - ACCEPT.

CID 465 - ACCEPT. See also CID 453.

CID 468 - ACCEPT IN PRINCIPLE. Rephrase the definition as follows: 'The Sequence Number field specifies the number of frames that have been sent prior to this frame by this DEV in the response to the request. Thus the first frame has a Sequence Number of 0 while the last frame has a Sequence Number equal one less than the Total Number of Frames.'

CID 139 - Table, JPKG to provide MSCs for fixes. See also CID 352.

CID 215 - Table, JPKG to provide MSCs for fixes. See also CID 352 and 215.

CID 603 - ACCEPT.

CID 1 - Table, JPKG to provide MSCs for fixes. See also CID 352 and 215.

Meeting recessed at 10:05 EST.

Meeting called order at 1:04 pm EST.

CID 672 Comment:

> "Undesirable specification: The Aloha access algorithm defined in this subclause is undesirable in two folds: (1) The "binary backoff" nature of the contention algorithm, i.e., doubling the contention window after an inferred collision, in a PAN would unnecessarily increase the access latency, as an inferred collision could be a result of a non-collision event such as interference or bad channeling. Also, the backoff has a memory which could spread over a large number of superframes, and hence does not allow the PNC to adapt the CW to load changes for optimal channel throughput and access latency. Instead, re-randomizing the backoffs without doubling the CW among contending DEVs in every superframe would be more effective in avoiding collision, especially considering the generally low DEV population in a PAN, and hence in improving channel throughput and access delay. (2) Potentially each contending DEV may have to buffer a large number of MCTA definitions as announced in the beacon, and determine which of those MCTAs may be used for an initial transmission, a retransmission, and a retransmission again, ..., of a command frame, all within the same superframe. This would certainly increase the implementation cost."
>
> Remedy:
> "(1) The number "a" should not be individual functions of retransmission attempts by contending DEVs. Instead, it should be a parameter whose value is updated and annonced by the PNC in each beacon. To this effect, add two 1-octet subfields to the Piconet Synchronization Parameters field for encoding "a", one for use with Association MCTAs and one for use with Open MCTAs. "a" may be called Associaiton CW exponent and Open CW exponent, respectively. Eliminate the first branch of Equation (1) and the condition in the second branch. Each contending DEV shall redraw a backoff after receiving a beacon using the "a" value contained in that beacon, even if the previous backoff has not expired (and hence the DEV did not transmit in the previous superframe). A DEV shall regenerate a backoff for a retransmission within the same superframe using the same "a" value as in the initial transmission.
>
> (2) Add a statement to limit the number of MCTAs (for each type, Association or Open) that may be used by any given DEV to two within each superframe. That is, only one retransmission is allowed by each DEV following a failed transmission in the same superframe."
>
> Proposed Response:
> REJECT. The Slotted Aloha backoff algorithm is well documented in the literature. Just as an associating DEV won't know the difference between a collision and interference, the PNC likely won't be

able to tell the difference between a collision and interference either. In this case, the PNC won't know what value to set for the exponent of the back-off window, "a". Also, the suggested Remedy does not specify what algorithm the PNC will use to determine the parameter "a".

Resolution is to reject as indicated above.

CID 675 Comment:

"Incorrect specification in lines 13-16, page 183."

SuggRemedy:
"Change "broadcast or unassigned" to "Association or Open". Delete "the open or association MCTA with the number r=". Change "ACK" to "Imm-ACK". Delete the last statement "After receiving" if "a", and hence the "backoff", is to be updated every superframe, as suggested earlier by this balloter."

Response:
ACCEPT IN PRINCIPLE:
The comment that "broadcast or unassigned" should be changed to open or association. The rest of the suggested Remedy is not appropriate because it is based on a rejected suggestion from CID 672.

CID 338 - Table, Dan Baily to provide references for Ntru.

CID 19 - Table, wait for email ballot so the entire BRC can weigh in with their opinions.

CID 374 - REJECT. This subject is appropriate for a follow-on PAR when there is more experience with a standard. This is an efficiency issue only.

CID 349 - ACCEPT IN PRINCIPLE. Replace the sentence with 'At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed below.'

CID 347 - ACCEPT IN PRINCIPLE. Change '1' to '1.0', change 'SEC 1: Standards for Efficient Cryptography' to be 'Standards for Efficient Cryptography, SEC 1:'

CID 350 - Rene to provide new suggested definitions by January 22 via email. authentication, authentic data, integrity code, key establishment, key management, key transport, nonce, symmetric key. Clarify that any changes in the definitions will not impact the draft.

CID 425 - Dan Bailey to submit new MLME-SECID-UPDATE.confirm

CID 14 - Where do we prohibit using distribute key (or request key) to distribute a management key.

CID 362 - Table and solve with fragmentation field update if necessary.

CID 363 - Withdrawn, 15 January 2003.

CID 364 - ACCEPT IN PRINCIPLE. Add 'RSA X.509' and 'ECC X.509' above 'X.509'.

CID 361 - ACCEPT IN PRINCIPLE. Add a field '80 bit security required' with the definition 'If the 80-bit security required bit is set to 1, the security manager shall only authenticate DEVs with a security suite that

is stated to provide at least 80-bit security in Table 96 while it operates as the security manager.' Add a column to table 96 with title 'At least 80 bit claimed secuity' and put X's in all of the columns.

CID 24 - Table, Singer to provide paragraph by Jan 20.

CID 25 - Withdrawn, 15 January 2003.

CID 26 - ACCEPT IN PRINCIPLE. Add a sentence to the end of 9.2.9: 'A DEV shall reject any SECID that it receives where the first octet does not contain the correct DEVID as described above.'

Meeting recessed at 3:00 pm, EST.

Meeting called to order at 4:34 pm EST.

CID 372 - REJECT. There is no reference in the draft for scalable security suites. The working group felt strongly that certificates should be optional, not required, based on the application space that 802.15.3 is addressing.

CID 371 - Dan/Ari to provide references for claimed security levels and independent review, due Jan 20.

CID 365 - REJECT. The extra 8 octets over the air have an inconsequential effect on the overall throughput of the piconet because they are sent infrequently. Futhermore, there are techniques to efficiently store these in memory.

CID 367 - ACCEPT IN PRINCIPLE. Remove the field 'Security suite' from 'Verification Info Type field'. Add a new fields to the 'Verification Info Type field', 'OID Length' and 'OID' with the definitions 'The OID indicates the security suite of the ACL information, {xref 10.2.1}.' and 'The OID length is the length of the OID.' Add these definitions to 7.5.2.1 where they are missing as well.

CID 369 - ACCEPT IN PRINCIPLE. Delete 'Certificate chain URL' from page 147, line 15.

CID 86 - (also 19, 371,) Table, resolve with email ballot.

CID 85 - Need Dan to specify something (ITU-T) that says you can use X.509 for Ntru.

Meeting recessed at 5:54 pm EST.

2.3 Tuesday, 14 January 2003

Meeting called to order at 8:12 am EST.

CID 572 - ACCEPT.

CID 573 - ACCEPT

CID 478 - ACCEPT IN PRINCIPLE. Using 'rate' would be confusing with data rate. Rename "CTR interval type" to "CTA Rate Type" and "CTR Interval" to "CTA Rate" throughout the draft.

CID 651 - ACCEPT IN PRINCIPLE. Rename CFP to CTAP - channel time allocation period.

CID 652 - REJECT. The proposed text is too restrictive. A DEV may have data pending for stream index 5 that is lower priority than stream index 3. The DEV would want to send data from stream index 3 in a CTA assigned to stream index 5 to improve the performance of its highest priority applications.

CID 326 - ACCEPT.

CID 69 - ACCEPT IN PRINCIPLE. Change 'of type other than data' to be 'of any type'

CID 664 - ACCEPT IN PRINCIPLE. After the sentence on line 51, add to the paragraph. "However, it is possible that the target DEV will not be receiving during the CTA if it is in a power save mode, {xref 8.13} or if it is not receiving multicast traffic, {xref 6.3.19.1}"

CID 666 - ACCEPT IN PRINCIPLE. Change 'If the PNC ... additional channel time.' to be 'If the source DEV requires additional channel time it will need to use the stream modification procedure, 8.5.1.2.'

CID 278 - ACCEPT IN PRINCIPLE. Replace the sentence in D15p181L30-31 by "In any individual superframe, the PNC may allocate more time for a dynamic CTA than the amount indicated in the channel time response command."

CID 672 - Table, WMS to consider, possible reject.

CID 675 - Table pending resolutionof 672.

CID 144 - ACCEPT.

CID 817 - ACCEPT. The parameter will be deleted as indicated in CID 144.

CID 571 - ACCEPT IN PRINCIPLE. It is possible that the asynchronous request will not replace the previous requests. This is described in 8.5.2.1 and should have been cross-referenced here. Add a cross-reference to 8.5.2.1 after 'all previous asynchronous requests'

CID 124 - ACCEPT IN PRINCIPLE. Use 'group' and 'individual', change throughout the draft to match.

CID 274 - ACCEPT IN PRINCIPLE. Replace the paragraph with ‘The target ID list type field shall be set to 0 for group allocation requests and shall be set to 1 for individual asynchronous allocation requests, {xref 8.5.2.1}.’

CID 701 - ACCEPT.

CID 702 -ACCEPT IN PRINCIPLE. After "superframe" add ", with any such CTA again announced by multiple CTA blocks that overlap in time but have different DestIDs.'

CID 704 - ACCEPT.

CID 486 - REJECT. The participation of the PNC DME is not required to respond to this command as required by the draft standard. Thus the .indication and .response primitives are not required in this instance.

CID 488 - REJECT. The participation of the PNC DME is not required to respond to this command as required by the draft standard. Thus the .indication and .response primitives are not required in this instance.

CID 484 - ACCEPT IN PRINCIPLE. The probe command is always sent as a peer-to-peer command (i.e. as a 'side-stream'). If a DEV sends a probe to the PNC, the PNC responds with information about itself, not with information about another DEV. The only way to find probe information about a DEV is to send the probe command directly to the DEV. Therefore, the TargetID in this MLME will become the DestID in the first probe command frame that is sent.

CID 482 - ACCEPT

CID 483 - ACCEPT IN PRINCIPLE. Change the "Valid range" of "ResultCode" as follows: RESPONSE_RECEIVED, TIMEOUT. Change the corresponding "Description" to "Indicates if the request has received a response or timed out."

CID 487 - ACCEPT.

CID 489 - ACCEPT.

CID 657 - ACCEPT IN PRINCIPLE. On page 179, line 52 at the end of the paragraph add 'Dynamic CTAs may be used for both asynchronous and isochronous streams.'

CID 820 - ACCEPT. Also delete from the PICS.

CID 199 - ACCEPT.

CID 245 - ACCEPT.

CID 270 - ACCEPT IN PRINCIPLE. Add an xref to the paragaph, change 'the requested priority,' to be 'the requested priority {xref Annex A.1.2.1},'

CID 301 - ACCEPT IN PRINCIPLE. Change bullet text from:

> "The available number of TUs field shall be set to a value less than the minimum number of TUs requested."
> to:
> "The available number of TUs field shall be set to the number of TUs that the PNC had available for allocation to this request."

Meeting recessed 10:00 am EST

Meeting called to order at 10:30 am EST.

CID 690 - ACCEPT.

CID 312 - REJECT. The scheduler, including the allocation of left over time in the superframe is out of the scope of this standard. Implementers are free to create scheduling algorithms that best meet their combination of price and performance for their application.

CID 246 - ACCEPT IN PRINCIPLE. Change 'is in a power save mode, if the CTR type or

CTR interval is modified.' to be 'is in a power save mode. The PNC shall announce the modification of all streams where the CTR type or CTR interval is modified.'

CID 200 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 246.

CID 247 - ACCEPT IN PRINCIPLE. Delete the sentence, there is text in 8.13 now that handles this issue.

CID 691 - ACCEPT IN PRINCIPLE. In figures 114, 115 and 116, Change "ACK" to "Imm-ACK" (2 occurrences in each figure). Delete"with ResultCode = ???" in each of these three figures.

On page 183, line 8, change "presence" to "reception" and change 'association frame" to "Association Request command".

CID 697 - ACCEPT IN PRINCIPLE. In figures 117 and 118, Change "ACK" to "Imm-ACK" (2 occurrences in each figure). Delete"with ResultCode = ???" in each of these two figures. Add 'with Reason Code = success" to the channel time response command arrow in figure 117.

CID 699 - ACCEPT IN PRINCIPLE. Change "ACK" to "Imm-ACK" in both figures. Change "SUCCESS" to "RESPONSE_RECEIVED" in each of these two figures. Ed. Note coordinate this code with new clause 6 name.

CID 150 - REJECT. The open and association MCTAs were added to handle two concerns, the first was that new PHYs may not support efficient CCA detection. In this case, slotted aloha provides a contention access method that provides for the needs of the piconet. Another reason to used slotted aloha is that under certain conditions, it can be more efficient than using the CAP. Adding a new contention method to the MAC when a PHY group has been formed is probably not the best venue. At this time, the TG has many members who have expertise in the MAC available to review draft. In the future, when a new PHY is down-selected, there may not be as many people available who have the experience and knowledge of the TG3 MAC to be able to add a new contention method. Adding slotted aloha does not add much, if any complexity, the DEV needs the random number generatora and exponential increasing backoff for any contention based method. The DEV is already required to be able to send frames and look to see if it gets an ACK. Depending on the parameters used for either the CAP or the open and association MCTAs, the power usage may actually be lower using MCTAs for the DEVs in the piconet than using the CAP. MCTAs have an advantage over the CAP in that they can be put into multiple locations in the superframe allowing the PNC to potentially use the time more efficiently.

CID 151 - REJECT. The open and association MCTAs were added to handle two concerns, the first was that new PHYs may not support efficient CCA detection. In this case, slotted aloha provides a contention access method that provides for the needs of the piconet. Another reason to used slotted aloha is that under certain conditions, it can be more efficient than using the CAP. Adding a new contention method to the MAC when a PHY group has been formed is probably not the best venue. At this time, the TG has many members who have expertise in the MAC available to review draft. In the future, when a new PHY is down-selected, there may not be as many people available who have the experience and knowledge of the TG3 MAC to be able to add a new contention method. Adding slotted aloha does not add much, if any complexity, the DEV needs the random number generatora and exponential increasing backoff for any contention based method. The DEV is already required to be able to send frames and look to see if it gets an ACK. Depending on the parameters used for either the CAP or the open and association MCTAs, the power usage may actually be lower using MCTAs for the DEVs in the piconet than using the CAP. MCTAs have an advantage over the CAP in that they can be put into multiple locations in the superframe allowing the PNC to potentially use the time more efficiently.

CID 204 - Table, ADH to comminicate with KO to see if this allocates slots too often. Plus, are we overloading CTRRespTime which only has to do with the PNC’s current loading for channel time request. If the PNC is efficient, then it will take up a lot time in the superframe for MCTAs.

CID 254 - Table, resolve with CID 204.

CID 490 - REJECT. The participation of the PNC DME is not required to respond to this command as required by the draft standard. Thus the .indication primitive is not required in this instance.

CID 241 - ACCEPT.

CID 242 - ACCEPT.

CID 201 - ACCEPT.

CID 202 - ACCEPT.

CID 252 - ACCEPT.

CID 251 - ACCEPT.

CID 203 - ACCEPT.

CID 119 - ACCEPT.

CID 700 - ACCEPT.

CID 474 - ACCEPT IN PRINCIPLE. Change all CTR references to be "CTRq" to avoid confusion. If the response command needs an acronym, it will be ‘CTRsp’.

CID 275 - Table, JS to figure out what MR meant.

CID 121 - ACCEPT IN PRINCIPLE. After line 50 on page 152, add a paragraph that says 'For isochronous requests, the minimum number of TUs and the desired number of TUs are the number of TUs per CTR interval requested by the DEV. In the case of a super-rate allocation, it is the number of TUs requested in each superframe. In the case of a sub-rate allocation it is the number of TUs requested in each of the sub-rate superframes. For example, a request for a minimum number of TUs of 4 with a sub-rate CTR interval of 4 indicates that the DEV is requesting 4 TUs every fourth superframe.'

CID 677 - Table, WMS to propose solution.

CID 678 - REJECT. The DEVs need to have time to switch between transmit and receive between CTAs. A MIFS is not necessarily enough time to do this, therefore the SIFS time is required which is equal to the greater of the the TX/RX turnaround and the RX/TX turnaround times.

CID 679 - ACCEPT IN PRINCIPLE. The equation is confusing because it is missing parentheses. It should read:

MaxDrift = [clock accuracy (ppm)/1e6]*interval

A number in ppm is divided by 1e6 to get its fractional equivalent, thus 100 ppm is equal to 0.0001. The drift for a 10 ms interval with 100 ppm accuracy is 10 us.

Add parentheses to the equation to emphasize that the interval is multiplied by the fractional clock accuracy.

Recessed at 12:06 pm EDT.

Meeting called to order at 1:13 pm EDT

CID 45 - Tabled, Bain to work on it.

CID 682 - Tabled, WMS to suggest solution, resolve with CID 677

CID 684 - ACCEPT.

CID 49 - Tabled, WMS to suggest solution, resolve with CID 677

CID 120 - ACCEPT IN PRINCIPLE. On page 72, line 25, delete 'and a beacon containing the requested stream modification.'

CID 574 - ACCEPT IN PRINCIPLE. On page 153, line 18, add ‘In the case of a super-rate allocation, it is the number of TUs assigned in each superframe. In the case of a sub-rate allocation it is the number of TUs assigned in each of the sub-rate superframes.'

CID 329 - ACCEPT IN PRINCIPLE. Change 'super-rate' to be 'super-rate or subrate'

CID 353 - ACCEPT IN PRINCIPLE. On page 15, line 36 add 'A child piconet ends its piconet with the shut-down procedure and then uses the stream termination command to release the resources in the parent pico-net. When the child PNC shuts down its piconet, it is not required to leave the parent piconet.'

CID 209 - REJECT. The child piconet is a full member of the parent piconet and is able to communicate to other DEVs in the piconet. The neighbor, on the other hand, only communicates with the PNC and may not be a full 802.15.3 DEV, i.e. it could be a entity from another network that wants to request quiet time to share the channel. In addition, the neighbor could be a DEV that is not able to authenticate with the parent PNC, but would like to coordinate the channel resources to avoid collision. Wherever possible, the draft will be updated to use dependent piconet and a single description when discussing similarities of child and neighbor piconets.

CID 614 - ACCEPT

CID 208 - ACCEPT IN PRINCIPLE. Change 'If the piconet is not 802.15.3 compliant, it shall' to be 'If the network operated by the neighbor PNC is not an 802.15.3 piconet, the neighbor PNC shall ...'

CID 715 - ACCEPT IN PRINCIPLE. On page 199, line 30 change 'Fragmentation is performed ... stream or asynchronous data.' to be 'Fragmentation may be performed at the transmitting DEV on each MSDU.' On line 31 change 'commands' to be 'commands, i.e. MCDUs,'. On page 199, line 34 delete 'for any reason and all the retransmissions shall obey the original fragmentation threshold of the MSDU/MCDU.' Change 'aMin-FragmentSize' to be {xref pMinFragmentSize}.

CID 355 - Tabled, RS to provide more detailed information.

CID 292 - ACCEPT.

CID 528 - Table, J. Barr to work on it. If a DEV receives a frame from an unassociated DEV it may ignore the frame and may ACK the frame if the ACK policy is set to Imm-ACK. If authentication is required and a DEV receives a frame from an unauthenticated DEV, it shall ignore the frame and may ACK the frame if the ACK policy is set to Imm-ACK. If a DEV receives a frame from a PNID other than the PNID of the piconet with which the DEV is synchronized, it shall ignore the received frame.

CID 530 - ACCEPT

CID 357 - JS, WMS and KO to consider changing? What are the arguments to keep it this way?

Meeting recessed at 3:02 pm EST

Meeting called to order at 3:44 pm EST.

CID 174 - Table, ADH to present text.

CID 359 - Withdrawn, 14 January 2003.

CID 117 - WMS to ask the commenter.

CID 358 - Withdrawn, 14 January 2003.

CID 227 - Table, resolve with the other comment about putting the BSID up front (WMS?)

CID 325 - Withdrawn, 14 January 2003.

CID 360 - REJECT. This information is already passed to DEVs in the authentication process in the authentication response command. While it allows the DEV to know before it joins what is the level of security, this provides only part of the information that the DEV needs when selecting a piconet.

CID 240 - REJECT. While it is true that flipping the figure may be easier to read, it would be the only figure in the entire draft with octet 0 on the right.

CID 549 - ACCEPT IN PRINCIPLE. Delete 'consists of a single command block and'

CID 550 - ACCEPT IN PRINCIPLE. "Rename "Data" to "Data Payload" whenever it references the "Data" field of a Data frame."

CID 536 - ACCEPT IN PRINCIPLE. Change 'payload field' to 'Frame Payload field' in this subclause, 2 places lines 35, 37.

CID 356 - Table, ADH to look for rewritten text.

CID 531 - REJECT. Requiring the PNC to monitor all of the frames sent between devices is not feasible. Also, the use of the bits by the PNC is not clearly defined.

CID 551 - ACCEPT.

CID 328 - Table, WMS to describe how this can optional or used with a null data frame once last data frame has been sent.

CID 78 - ACCEPT.

CID 152 - JPKG to write REJECT.

CID 145 - ACCEPT.

CID 517 - ACCEPT IN PRINCIPLE. Change 'MaxAssociations' to be 'MaxAssociatedDEVs' to match the name in 7.5.1.1. Also change this name in 6.3.5 as well.

CID 147 - ACCEPT IN PRINCIPLE. Add to this section 'For each stream, all MSDUs that do not use Dly-ACK policy shall be transmitted in the order that they were received from the FCSL. This implies that it is possible that MSDUs from different streams will be transmitted in a different order than they were received from the FCSL. MSDUs that use Dly-ACK policy may be transmitted out of order by the MAC.'

CID 137 - ACCEPT.

CID 136 - ACCEPT.

CID 519 - ACCEPT.

CID 520 - ACCEPT.

CID 522 - ACCEPT.

CID 521 - ACCEPT.

Recessed at 5:33 pm EST.

Called to order at 6:58 pm EST.

CID 524 -ACCEPT IN PRINCIPLE. "Change "MSDU" to "MPDU" and "media" to "medium". Change 'If the StreamIndex for the request is not assigned to the DEV as a stream source,' to be 'If the StreamIndex for the request does not correspond to an existing stream with the DEV as the source.'

CID 597 - ACCEPT IN PRINCIPLE. Change 'SUCCESS' to be 'COMPLETED' in the figure and in the text.

CID 54 - ACCEPT IN PRINCIPLE. Change the description from 'Data rate in Mb/s.' to be 'PHY dependent index of the data rate' Add a note to the PHY section that this is the corresponds to the value that goes in the PHY header.

CID 148 - ACCEPT.

CID 129 - Table, JPKG to bring data.

CID 825 - ACCEPT.

CID 826 - ACCEPT IN PRINCIPLE. Change x^15 to be x^14 in table 126. Let n=15 in the xinit matrix and map x_(n-1) to x_14, etc. in the text.

CID 133 - ACCEPT.

CID 313 - Table, James will provide new numbers for EVM that are 5 dB relaxed and are more in line with 802.11a.

CID 134 - ACCEPT.

CID 281 - Table, JPKG to bring back result.

CID 132 - Table, same as CID 281.

CID 282 - Table, same as CID 282.

CID 280 - ACCEPT.

CID 130 - ACCEPT.

CID 131 - JPKG to check for efficiency.

CID 53 - Table, JPKG to suggest clause 11 text, don't need PIB

CID 50 - ACCEPT.

CID 55 - ACCEPT IN PRINCIPLE. Delete the PHYPIB_Range from the table.

CID 153 - ACCEPT IN PRINCIPLE. Make a table of all of the pZZZYyy parameters and their values, this will follow the format of table 65 in clause 8.

CID 594 - ACCEPT IN PRINCIPLE. Change "non zero value" to "than 0 or 1", This command returns a list of all the DEVs who are members of a particular PS set. It does not indicate that they are in a PS mode. The PS status IE(s) in the beacon contain the lists of the DEVs that are in PS mode for each of the sets. A DEV

shall first join a set before it can change to either SPS or PSPS mode. Thus a DEV can be a member of a set but not be in a power save mode.

CID 59 - ACCEPT IN PRINCIPLE. Delete 'or SPS mode,' because SPS DEVs do not make a special effort to hear beacon annoucements.

CID 309 - ACCEPT IN PRINCIPLE. Change 'subsequent' to be 'consecutive', 2 places, change the third dashed list items on line 43 from 'If the DEV is in SPS mode, the IEs shall be sent in mMinBeaconInfoRepeat subsequent SPS set wake beacons.' to be 'If the DEV is in SPS mode, the first IE announcement shall be made in one of the DEV's SPS set wake beacons.'

CID 249 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 309. This resolution removes the requirement that the PNC align the announcements to the SPS DEV's wake beacons. Instead it aligns it with one and sends the rest in the following beacons.

CID 248 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 309.

CID 774 - ACCEPT.

CID 560 - ACCEPT IN PRINCIPLE. The PCTM IE is placed in the beacon until the HIBERNATE DEV either a) repsonds to the IE with a PS mode change command or b) the ATP of the DEV expires and the PNC disassociates the DEV. Thus the DEV will either respond or it will be removed from the piconet.

CID 799 - REJECT. This standard only has positive acknowledgement, there is not an negative acknowledgement. Thus any acknowledgement is a positive one.

CID 806 - ACCEPT IN PRINCIPLE. The PCTM IE is placed in the beacon until the HIBERNATE DEV either a) repsonds to the IE with a PS mode change command or b) the ATP of the DEV expires and the PNC disassociates the DEV. Thus the DEV will either respond or it will be removed from the piconet.

CID 559 - REJECT. The PCTM bit is not used for PSPS DEVs because they listen to all of the system wake beacons and the beacons that follow any missed system wake beacons.

CID 777 - ACCEPT IN PRINCIPLE. Following line 51 on page 215, add 'The PNC uses the wake beacon interval information from all particpating PSPS DEVs to determine the system wake beacon interval. The actual system wake beacon interval may not correspond to any of the PSPS DEVs desired wake beacon interval.'

CID 778 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 777.

CID 771 - Change "A DEV that is in SPS mode may have multiple wake beacons" to "A DEV in SPS mode may be in multiple SPS sets and therefore may have multiple wake beacons because each of those SPS sets may have its own wake beacon."

CID 127 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 310

CID 250 - ACCEPT.

CID 793 - ACCEPT IN PRINCIPLE. Change 'field to ‘PS’ and shall request that the PNC terminate the stream, 8.5.1.3.' to be 'field to ‘PS’. The DEV shall also send a Channel Time Request command to terminate the stream, {xref 8.5.1.3}.'

CID 789 - REJECT. The sentence does not add any specifications (no shalls, mays or shoulds). This sentence was added to clarify the purpose of the MCTA and its length. It is intended as an aid to the implementers but does not place any restrictions on them.

CID 791 - ACCEPT.

CID 797 - ACCEPT IN PRINCIPLE. Change 'wake CTAs' to be 'CTAs'

Skip to Probe.

CID 480 - REJECT. The Probe command that is sent by the MLME-PROBE.response primitive can also contain a request for information. Therefore the .response command needs these two parameters.

CID 156 - ACCEPT IN PRINCIPLE. Delete the parameter and the paragraph on page 203, lines 40-47, ‘To accommodate ... describe above.’

CID 143 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 156.

CID 67 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 156.

CID 315 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 156.

CID 379 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 156.

CID 257 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 156.

CID 229 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 156.

CID 219 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 156.

CID 93 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 156.

CID 243 - ACCEPT IN PRINCIPLE. 0 -> Non-dependent piconet1 -> Dependent piconet2-255 -> Reserved.

CID 496 - REJECT. The remote piconet description set corresponds to the data that is passed in the Remote Scan Response command. Some of the data (beginning with SuperframeDuration) is not passed in the command and so cannot be passed up by the primitive.

CID 497 - REJECT. The remote piconet description set corresponds to the data that is passed in the Remote Scan Response command. Some of the data (beginning with SuperframeDuration) is not passed in the command and so cannot be passed up by the primitive.

CID 499 - REJECT. The DME controls the scan process and it happens after it receives the the MLME-REMOTE-SCAN.indication primitive as illustrated in Figure 131.

CID 500 - ACCEPT.

CID 498 - REJECT. The scan has not yet been performed when this primitve is issued, see Figure 131, so these parameters are not yet available.

CID 582 - REJECT. The purpose of the remote scan request is to determine the level of potential interference on the current channel and other channels without disturbing the coordination function of the PNC. It also gives the PNC a longer 'reach' in finding out who might be the potential interferers. The PNC does not

need this additional information to be able to determine the interferrence levels. This information is included in the scan process because the DEV might join one of the piconets that it finds.

Meeting recessed at 9:58 pm EDT. T = 225, E = 378

2.4 Monday, 13 January 2003

Meeting called to order at 1:14 pm EST.

PM/SPS-4 comments

CID 253 - Accept

CID 230 - Accept in principle, Resolve as indicated in CID 253

CID 258 - Accept in principle, Resolve as indicated in CID 253

CID 94 - Accept in principle, Resolve as indicated in CID 253

CID 316 - Accept in principle, Resolve as indicated in CID 253

CID 157 - Accept in principle, Resolve as indicated in CID 253

CID 220 - Accept in principle, Resolve as indicated in CID 253

CID 380 - Accept in principle, Resolve as indicated in CID 253

PM/SPS-4

CID 83 - Accept in principle, Delete item MLF 23.3 from Table E.4. In item MLF 23.2 Table E.4, remove “& - FD3” Remove item FD3 from Table E.1.

CID 84 - Accept in principle, Resolve as indicated in CID 83.

CID 259 - Accept in principle, Resolve as indicated in CID 83.

CID 317 - Accept in principle, Resolve as indicated in CID 83.

CID 381 - Accept in principle, Resolve as indicated in CID 83.

CID 221 - Accept in principle, Resolve as indicated in CID 83.

CID 95 - Accept in principle, Resolve as indicated in CID 83.

CID 231 - Accept in principle, Resolve as indicated in CID 83.

CID 158 - Accept in principle, Resolve as indicated in CID 83.

Misc PS issues:

CID 780 - ACCEPT IN PRINCIPLE. The terms power management and power save were used interchangeably but this is confusing. The TG has agreed to change all the occurances of 'power management' to be 'power save' for consistency.

CID 295 - ACCEPT IN PRINCIPLE. Add the CWB IE to the table with entries: 'shall ignore' for all three entries.

CID 296 - ACCEPT IN PRINCIPLE. Add the CWB IE to the table with entries: 'shall not request', 'shall not request', 'shall not send', 'shall not send'

CID 293 - Accept.

CID 128 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 293.

CID 122 - ACCEPT IN PRINCIPLE. Change the description to "The wake beacon interval is the number of superframes, including the current one, between wake beacons, {xref 8.13}. For example, a wake beacon interval of 8 indicates that the DEV is requesting a wake beacon every 8th beacon, {xref Figure 137}."

CID 44 - Accept.

CID 311 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 44.

CID 123 - Accept

CID 310 - ACCEPT IN PRINCIPLE. Add a reason code to 7.5.7.2 "Unique Wake Beacon Interval required." Add to 8.13.2.1 "The PNC may require that all PS sets have a unique Wake Beacon Interval. For example, the PNC may reject a request to create a PS set with a Wake Beacon Interval of 4 if there is a PS set that already has this value. If the DEV requires this Wake Beacon Interval, it may join the existing PS set."

CID 509 - Table: Do we rename PS mode as PM mode? Or do we use another name? DEV Mode? (DM)

CID 511 - Table: Rename some of the parameters? Resolve after CID 509.

CID 586 - Table: Resolve after CID 509

CID 503 - Accept

CID 818 - ACCEPT IN PRINCIPLE. Change "For a piconet that has pseudo-static CTAs, NbrOfChange-Beacons shall be at least four." to be "For a piconet that has pseudo-static CTAs, NbrOfChangeBeacons shall be at least {xref mMaxLostBeacons}."

CID 753 - ACCEPT IN PRINCIPLE. The CTA location does not change relative to the beacon and so the CTA does not change (CTAs only have meaning measured relative to the beacon). The location of the psuedo-static CTA relative to previous beacons will change, but the source and destination DEVs will be informed prior to that by the piconet parameter change IE. If there are pseudo-static CTAs, the piconet parameter IE will be sent at least mMaxLostBeacons prior to the change. Thus, even if the DEVs miss some of the announcements, they will either a) hear at least one of them or b) miss all but hear the first beacon with the new superframe duration. To clarify this, change "A PNC shall not change pseudo-static CTAs" to be "A PNC shall not change either the pseudo-static CTAs or the pseudo-static CTA blocks"

CID 71 - Table, resolution will be to add an MLME-PICONET-PARM-CHANGE.indicate that goes up to the other DEVs in the piconet after the change occurs. Add this to Figure 134. Change text in 10.3 to reflect the fact that the change of BSID value in the PIB occurs after the MLME-PICONET-PARM-CHANGE.request. Pass up the BSID, PNID, Channel index and superframe duration. Note: the BSID will become a read-only attribute. Need text for this.

Recessed at 3:47 pm EST for potential TG3 official business.

Called to order for comment resolution at 3:50 pm EST.

CID 510: Jay to check all of the xrefs to make sure that they point to the correct location. Due Tuesday afternoon at 3:30 pm.

CID 513: REJECT. The participation of the PNC DME is not required to respond to this command as required by the draft standard. Thus the .indication and .response primitives are not required in this instance.

CID 43: ACCEPT IN PRINCIPLE: “Add NumberOfPiconets to describe how many PiconetDescriptionSet fields are specified. Add a parameter for the "NumberOfPSStructureSet" to specify how many PSStructureSet fields are specified. Add needs a NumberOfDEVInfoFields, 'type: integer, valid range: 2 to mMaxNumValidDEVs', add mMaxNumValidDEVs to table 64 with a value of 256-3-10 = 243, add text to 7.2.3 ‘The maximum number of valid DEVs, mMaxNumValidDEVs includes the PNC and the NbrIDs but not the reserved IDs, the BcstID, McstID or the UnassocID.’, Add to 7.5.4.2, page 145, line 20, change ‘broadcast and multicast ID.’ to be ‘the BcstID, the UnassocID, the McstID or the reserved IDs, {xref 7.2.3}.’ in 8.3.3, change ‘In addition, the PNC shall send the piconet information for each of the DEVs that are a member of the piconet at least once every mBroadcastDEVInfoDuration via a PNC information command.’ to be ‘In addition, the PNC shall send the piconet information for each of the DEVs once every mBroadcastDEVInfoDuration via a PNC information command. When the PNC broadcasts this command, the PNC shall include all DEVs that are associated in the piconet, including the DEV personality of the PNC, as well as an entry for the PNCID.’, in 8.2.3, page 164 line 38 following ‘to the chosen PNC capable DEV.’ add ‘In the PNC information command, the PNC shall include all DEVs that are associated in the piconet, including the DEV personality of the PNC, as well as an entry for the PNCID.’ and a re-definition of the DEV InfoSet as follows:

> Name:Piconet Decription Set
> Type: Set of PiconetDescriptions as defined in Table 6.
> Valid Range: a set containing zero or more instances of a PiconetDescription
> Description: The PiconetDescriptionSet is returned to indicate the results of the scan request.
>
> Name: DEVInfoSet
> Type: A set of DEVInfo fields as defined in {xref 7.5.4.2}.
> Valid Range: a set containing 3 to mMaxNumbValidDEV instances of fixed length DEVInfo fields.
> Description: The DEVInfoSet is returned to indicate the results of a PNCInfo request.
>
> Name: ACLRecordSet
> Type: A set of ACLRecords as defined in {xref 7.5.4.4}
> Valid Range: a set containing 0 or more instances of variable length ACLRecords. The maximum number of instances depends on the size of the records, {xref pMaxFrameSize} and the length of the secure command security fields, {xref 7.3.3.2}
> Description: The ACLRecordSet is returned to indicate the results of a ACLInfo request.”

CID 514: REJECT. The participation of the PNC DME is not required to respond to this command as required by the draft standard. Thus the .indication and .response primitives are not required in this instance.

CID 515: REJECT. The participation of the PNC DME is not required to respond to this command as required by the draft standard. Thus the .indication primitive is not required in this instance.

CID 516: ACCEPT IN PRINCPLE. Replace the first sentence with ‘The DME is informed of the PS mode change to ACTIVE.’

CID 588: ACCEPT IN PRINCIPLE. Change 'PS mode' to be 'SPS mode' and change this in figure 144, also on page 216 line 4, page 217 line 19 and page 281, line 13.

CID 593: ACCEPT IN PRINCIPLE. Change "number PS set structures" to "number of current PS sets", and "The PS set structure" to "Each PS set structure". Change 'Number of supported PS sets' to be 'Maximum Supported PS Sets' in Figure 92 and the following text. Also replace where it occurs in clause 8. Add a new field, "Number of Current PS Sets" with definition, 'The Number of Current PS Sets field is a count of the number of PS set structures in this command as well as the number of currently active PS sets in the piconet.'

Recessed for dinner at 5:30 pm EST.

Meeting called to order at 6:41 pm EST

CID 824 - ACCEPT. Renumber 18.x as 17.x and update the rest of the numbers in the table accordingly.

CID 138 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 298.

CID 298 - ACCEPT

CID 719 - ACCEPT

CID 394 - PM renaming, table resolve after CID 509

CID 388 - Table, is there another way to do this.

CID 91 - Table, Gilb to write interoperability text

CID 154 - Table, Reject using old text, JPKG to do this.

CID 237 - ACCEPT IN PRINCIPLE. Add parameter to MLME-CREATE-ASIE.request:"ASIE-index", integer type, range is application specific, definition: 'Used to uniquely identify an ASIE.'

CID 168 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 237.

CID 238 - ACCEPT IN PRINCIPLE. Add parameter to MLME-CREATE-ASIE.confirm: "ASIE-index" (note type, range and definition defined in CID 237.)

CID 169 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 238.

CID 170 - ACCEPT IN PRINCIPLE. Add the ASIE index to the MLME's as indicated in CIDs 237 and 238.

CID 173 - Withdrawn, 13 January 2003.

CID 816 - ACCEPT IN PRINCIPLE. This field is no longer used (and hasn't existed for at least 3 drafts). Delete the sentences "If the application data identifier field was set to "0" in the request, the MAC shall assign a new application data identifier that is different from that assigned to other current ASIEs. The "0" value application data identifier shall not be assigned to any ASIE. If the requested application data identifier belongs to an existing ASIE, the MAC shall modify the persistence of that ASIE, and reply with the same application data identifier in the indicate. If the repeat field an existing ASIE is set to "0", the PNC shall terminate the existing ASIE."

CID 297 - ACCEPT.

CID 125 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 297.

CID 401 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 297.

CID 403 - ACCEPT IN PRINCIPLE. After a DEV gains membership in the piconet, i.e. after it associates if authentication is not required or after it authenticates if authenticationis required, the PNC broadcasts the PNC info command that contains not only the DEVID and DEV addresses of every DEV in the piconet, it also contains their capabilities. The complete list of DEVs in the piconet might make the beacon too long, so the standard uses the broadcast of the PNC info command, which can be fragmented, to communicate the list of DEVs in the piconet. This is described in 8.3.3. No change is required for the draft because this functionality is already provided.

CID 404 - ACCEPT IN PRINCIPLE. "Change the "Valid range" of "ResultCode" as follows: SUCCESS, TIMEOUT. Change the corresponding "Description" to 'Indicates if the primitive completed successfully or timed out.' In line 47, change "the result of the attempted association" to 'the reason why the attempted association failed as indicated in the association response command or indicates that the association was successful.'

CID 406 - REJECT. The list of active DEVs in the piconet is passed to the DME via the MLME-PNC-INFO.confirm, see also the resolution of CID 403. This MLME is used to notify DEVs that are already in the piconet that a new DEV has joined. The DEVs that are already in the piconet should already have the membership information, if not they can request in a directed frame from the PNC using the PNC Info Request command.

CID 555 - ACCEPT IN PRINCIPLE. This IE is only used to notify the existing members of the piconet about a new member that has just joined. DEVs that join the piconet after this DEV will find out about the existing DEVs in the piconet when the PNC broadcasts the PNC Info command after the new DEV joins the piconet. See also the resolution of CID 403. No change required for the draft since the requested capability is provided by the PNC Info command.

CID 453 - ACCEPT IN PRINCIPLE. In Figure 49 change "Capabilities" to "Overall Capabilities" and in lines 14-15 change "The capabilities" to "the Overall Capabilities"

CID 627 - ACCEPT IN PRINCIPLE. Change the name to mAssocRespConfirmTime which is defined in 8.15, Table 64.

CID 629 - REJECT. The PNC info command provides the requested functionality as described in 8.3.3. Thus the DEV association IE does not need to be expanded. See also the resolution of CID 403.

CID 75 - ACCEPT.

CID 630 - ACCEPT IN PRINCIPLE. Change 'ack with' to 'Imm-ACK with'. (2 places) The association IE is sufficient for this process as the PNC info command will be used to update the new DEV with the complete membership in the piconet as described in 8.3.3. See also the resolution of CID 403.

CID 634 - REJECT. The association IE serves two purposes. The first is to tell other DEVs in the piconet that a new DEV has joined. The second, perhaps more important purpose is that this IE is used to complete the association process for the requesting DEV. When the DEV receives this IE in the beacon, it knows that it has successfully associated.

CID 643 - ACCEPT.

CID 642 - REJECT. DEVs that remain associated already know the members of the piconet (or they can find out by requesting this information from the PNC with the PNC info command). They do need to know when a DEV is disassociated and the association IE provides this information.

CID 644 - ACCEPT IN PRINCIPLE. Change "ack" and "ACK" to "Imm-ACK", and "ASSOCIATE-INFO" to "ASSOCIATION-INFO" As indicated in the resolution of CID 642, the association IE is sufficient to

inform the DEVs in the piconet that a DEV has disassociated from the piconet. See also the resolution of CID 403.

CID 42 - ACCEPT IN PRINCIPLE. Define mAssocRespConfirmTime to be 4*mMaxSuperframeDuration.

CID 314 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 42.

CID 142 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 42.

CID 378 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 42.

CID 256 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 42.

CID 218 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 42.

CID 155 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 42.

CID 228 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 42.

CID 92 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 42.

CID 712 - REJECT. The source DEV finds out information about the CTA in channel time request process. Some of the information is sent by the source to the PNC with the channel time request command and some of the information is passed back by the PNC to the source DEV with the channel time response command. The only DEV not involved in the negotiation is the destination and so it is the only intended target of this information element.

CID 77 - ACCEPT IN PRINCIPLE. Change 'If the CAP is present in the superframe, ...' to be 'If the CAP is present in the superframe and the PNC allows data in the CAP, ...'.

CID 146 - ACCEPT.

CID 279 - ACCEPT.

CID 291 - ACCEPT.

CID 126 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 291.

CID 277 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 291.

CID 650 - ACCEPT. See also CID 291.

CID 493 - REJECT. The MAC/MLME does not perform any measurements, rather the DME responds via MLME-CHANNEL-STATUS.respone primitive with the numbers that it has been collecting over a previous measurement window size.

CID 492 - REJECT. These parameters are not coming from the requestor, rather the DME is keeping track of the channel status so that it can compute channel time requests and to determine which PHY data rates to use.

CID 554 - ACCEPT IN PRINCIPLE. Change to 'The stream index, 7.2.5, indicates the stream corresponding to the channel time allocation.'

CID 561 - ACCEPT IN PRINCIPLE. Change "about certain characteristics of the CTAs" to "of certain characteristics of a CTA". An allocated CTA would be an allocated channel time allocation, which would be redundant.

CID 476 - Tabled, M. Schrader to write a definition for SPS and ACTIVE CTAs

2.4.1 Waking up HIBERNATE mode DEVs

PM/Wakeup CID 262, CID 98, CID 384, CID 224, CID 234, CID 320, CID 161, CID 99, CID 235, CID 385, CID 321, CID 225, CID 162, CID 263, CID 255, CID 260, CID 382, CID 318, CID 96, CID 222, CID 232, CID 159, CID 97, CID 319, CID 261, CID 160, CID 233, CID 223, CID 383, CID 100, CID 386, CID 322, CID 163, CID 236, CID 226

Allow DEV to request CTAs with HIBERNATE DEV. PNC allows or rejects and responds with the channel time response command but doesn't allocate until the HIBERNATE DEV changes mode to ACTIVE. If it accepted, use Reason Code "Success, target DEV in HIBERNATE mode" When the DEV wakes up, begin allocating the CTAs as normal with a CTA status IE to notify people.

3. Text for resolutions

PM/Wakeup CID 262, CID 98, CID 384, CID 224, CID 234, CID 320, CID 161, CID 99, CID 235, CID 385, CID 321, CID 225, CID 162, CID 263, CID 255, CID 260, CID 382, CID 318, CID 96, CID 222, CID 232, CID 159, CID 97, CID 319, CID 261, CID 160, CID 233, CID 223, CID 383, CID 100, CID 386, CID 322, CID 163, CID 236, CID 226

Allow DEV to request CTAs with HIBERNATE DEV. PNC allows or rejects and responds with the channel time response command but doesn't allocate until the HIBERNATE DEV changes mode to ACTIVE. If it accepted, use Reason Code "Success, target DEV in HIBERNATE mode" When the DEV wakes up, begin allocating the CTAs as normal with a CTA status IE to notify people.

Attempt at merged text for requesting channel time with either an SPS DEV or a HIBERNATE DEV.

8.5.1.1

(new text)

If the target DEV is in either SPS or HIBERNATE mode and the PNC grants the channel time request, the PNC shall set the Reason Code in the Channel Time Response command to "Success, DEV in PS mode." The PNC shall place the PCTM IE in the beacon with a bit set for the target DEV, 7.4.8.

When the Target DEV in HIBERNATE or SPS mode receives a beacon with its bit set in the PCTM IE, it shall send a PS mode change command to the PNC. If the DEV wants to remain in a power save mode it shall set the PS mode field in the PS mode change command to the appropriate value, either 'PS' or 'HIBERNATE'. The PNC shall then terminate the stream, 8.5.1.3.

If the power save DEV wishes to listen to the new allocation, it shall set the PS mode field in the PS mode change command to 'ACTIVE'. The PNC shall then begin allocating the channel time in the beacon for the stream. The PNC shall no longer set the bits for the DEV in the PS status IEs.

If the PNC does not receive the PS change command from the power save DEV within a timeout determined by the PNC, the PNC shall terminate the channel time request, 8.5.1.3, and unset the power save DEV's bit in the PCTM IE.

If the Target DEV is SPS mode, after the PNC sets the SPS DEV's bit in the PCTM IE the PNC shall provide in the SPS DEV's next wake superframe a CTA with the SPS DEV as the source and the PNC as the destination that is long enough to handle a PS change command and a channel time request command with 4 isochronous CTRBs. This allows the SPS DEV to request a change to one of the current channel time allocations, to request new channel time or to request that a channel time allocation be terminated.

8.5.2.1

Same as above, but only for HIBERNATE DEV since async slots are aligned to the SPS wake beacons.

(new text)

If the target DEV is in either HIBERNATE mode and the PNC grants the channel time request, the PNC shall set the Reason Code in the Channel Time Response command to "Success, DEV in PS mode." The PNC shall place the PCTM IE in the beacon with a bit set for the target DEV, 7.4.8.

When the Target DEV in HIBERNATE mode receives a beacon with its bit set in the PCTM IE, it shall send a PS mode change command to the PNC. If the DEV wants to remain in HIBERNATE mode it shall set the PS mode field in the PS mode change command to 'HIBERNATE'. The PNC shall then terminate the stream, 8.5.1.3.

If the power save DEV wishes to listen to the new allocation, it shall set the PS mode field in the PS mode change command to 'ACTIVE'. The PNC shall then begin allocating the channel time in the beacon for the stream. The PNC shall no longer set the bits for the DEV in the PS status IEs.

If the PNC does not receive the PS change command from the HIBERNATE DEV within a timeout determined by the PNC, the PNC shall terminate the channel time request, 8.5.1.3, and unset the DEV's bit in the PCTM IE.

4. Status summary

4.1 Status at opening of Ft. Lauderdale

.

Table 11—Ballot resolution at opening of Ft. Lauderdale meeting

Type	SB1
T (technical)	447
E (editorial)	379
Total	826

4.2 Running status at Ft. Lauderdale

.

Table 12—Ballot resolution at opening of Ft. Lauderdale meeting

Type	SB1	10 pm, 1/13/03	10 pm, 1/14/03	6 pm, 1/15/03	10 pm, 1/16/03
T (technical)	447	361	225		
E (editorial)	379	378	378		
Total remaining	826	739	603		
Total resolved/day	N/A	87	136		

4.3 Status at closing in Ft. Lauderdale

Table 13—Ballot resolution as of close of Ft. Lauderdale meeting

Type	SB1	SB1 (after resolution)	Unresolved as of 17 January, 2002
T (technical)	447		
E (editorial)	379		
Total	826		