IEEE P802.15
Wireless Personal Area Networks

Project	IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)	
Title	**TG3 LB19 comment resolution**	
Date Submitted	[24 October, 2002]	
Source	[James P. K. Gilb] [Appairent Technologies] [9921 Carmel Mountain Rd. #247, San Diego, CA 92129]	Voice: [858-538-3903] Fax: [858-538-3903] E-mail: [gilb@ieee.org]
Re:	[]	
Abstract	[This document is a record of comment resolutions for LB19.]	
Purpose	[To provide a record of the comment resolution for LB19.]	
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, San Diego to Kauai

1.1 Merging SPS, PSPS and HIBERNATE to all use PS sets.

(the following is based on text from 02276r13P802-15_TG3-commentsD11_KO.doc and the resolution of the power save comments.)

6.3.21.1

MLME-PS-SET-INFORMATION.request (
RequestTimeOut
)

<rename SPS to PS, better name>

6.3.21.2 MLME-PS-SET-INFORMATION.confirm

<change in conformance with 6.3.21.1, SPS changed to PS>

6.3.21.3

MLME-PS-SET-CONFIGURE.request (
PSSetIndex,
PSSetOperation,
WakeBeaconInterval,
PSRequestTimeout
)

<next beacon decided by PNC.>

6.3.21.4

MLME-PS-SET-CONFIGURE.confirm (
PSSetIndex,
PSSetOperation,
NextWakeBeacon,
PSReasonCode,
ResultCode
)

6.3.21.5

MLME-PS-MODE-CHANGE.request (
PSSwitchOperation,
PSRequestTimeout
)

<Add PSSwithcOperation>

Name	Type	Valid Range	Description
PSSwitchOperation	Enumeration	ACTIVE, HIBER-NATE, PS	The PS mode requested by the DEV DME, 7.5.7.1

7.3.1 Beacon frame

(piconet synchronization field remains the same, “MCTA required” is added to the piconet mode field based on other comments.)

7.4.12 Capability information

(no power save related changes to the capabilities info field since all PS modes are mandatory for the PNC to support)

(Ed. note: PS status replaces both SPS status and PSPS status.)

7.4.13 PS Status

The PS status information element shall be formatted as illustrated in Figure 1.

octets: 1-32	1	1	2	1	1
DEVID bitmap	Start DEVID	PS set index	Next wake beacon	Length (=5-37)	Element ID

Figure 1—PS status information element format

The next system wake beacon field is the beacon number of the next system wake beacon, 8.13.1.

The PS set index field is set to the index of the power save set as follows:

0 -> Hibernate
1 -> PSPS

2-253 -> SPS

The start DEVID indicates the DEVID that corresponds to the first bit in the DEVID bitmap.

The DEVID bitmap field is 1 to n octets in length. Each bit of the DEVID bitmap corresponds to a DEVID that is equal to the start DEVID plus the bit position in the bit map. The bit position zero, i.e. the first bit or lsb of the bitmap, corresponds to the start DEVID. The bit correspoding to a DEVID shall be set to one when a DEV that is a member of this PS set is in a power save mode. It shall be set to zero otherwise.

The bits corresponding to the PNCID, UnassocID, BcstID, McstID, NbrIDs and the reserved IDs, 7.2.3, shall be set to zero upon transmission by the PNC and shall be ignored upon reception.

(end new PS status IE text)

7.4.14 PSPS Status

<delete>

7.5.7.1 PS Mode Change command

(New command format and description)

octets: 1	**2**	**2**
PS mode	Length (= 1)	Command type

Figure 2—PS mode change command format

The power save mode field shall be set as follows:

0 -> ACTIVE mode
1 -> Hibernate mode
2 ->PS mode
3-255 -> reserved

7.5.7.2 PS Configuration request command

(begin new text, this replaces the old command)

This command is used to set up and manage PS set memberships for PS DEVs currently participating or requesting to participate in one or more power save modes. The PS configuration request command shall be formatted as illustrated in Figure 3.

octets: 2	**1**	**1**	**2**	**2**
Wake beacon interval	PS set index	Operation type	Length (= 4)	Command type

Figure 3—PS configuration request command format

The operation type field indicates whether a DEV is requesting either to join or leave an existing PS set. The valid operation types are:

0 -> join

1 -> leave
2-255 reserved

The PS set index is used to identify the PS set the requesting DEV wants to create/join, join, configure, or leave. A PS Set index of zero (hibernation) shall not be used with this command. Table 1 illustrates how the fields are to be interpreted for various values of the fields.

Table 1—PS configuration request command parameter entries

Operation type	PS set index value	Wake beacon interval	Comments
0 (create/join)	Unallocated PS set (0xFE)	Any valid SPS wake beacon interval value. This value is decoded by the PNC upon reception	The unallocated PS set index (0xFE) shall be used to request the PNC to establish a new SPS set.
0 (join)	0x01	Any valid PSPS system wake beacon interval value. This value is decoded by the PNC upon reception	The PSPS mode is permanently associated with PS set index 0x01.
0 (join)	0x02-0xFD, 0xFF	Shall be set to zero and ignored by the PNC upon reception.	The DEV is requesting to join an existing SPS set.
1 (leave)	0x02-0xFD, 0xFF	Shall be set to zero and ignored by the PNC upon reception	The DEV is requesting to leave the indicated SPS set.

The wake beacon interval is the number of superframes between wake beacons. The wake beacon interval shall have a value between 4 and 255 for PSPS and between 4 and 65535 for SPS. Valid values for the wake beacon interval for either the PSPS or SPS ranges are in powers of 2 (e.g. 2, 4, 8, ...).

7.5.7.3 PS Configuration response command

This command is sent by the PNC as a response to a PS configuration request command from a DEV. The PS configuration response command shall be formatted as illustrated in Figure 4.

octets: 2	1	1	2	2
Next wake beacon	PS set index	Reason code	Length (= 4)	Command type

Figure 4—PS configuration response command format

The reason code field contains the result of the configuration request command. The valid reason codes are:

0 -> Success
1 -> Already member
2 -> Invalid PS set (i.e. attempting either to configure PS set 0 or to join a non existing set.)
3 -> Set creation failed
4-255 Reserved

The reason code is set to zero (Success), if the create or join operation is successful. If the PS set index shall be set to zero or any value not representing a PS set, the reason code shall be set to 'Invalid PS Set'. If a DEV requests to join an SPS set where it is already a member, the reason code shall be set to 'Already member'. However, a DEV is allowed to make multiple requests to join a PSPS set. This has the effect of updating the DEV's desired system wake beacon interval value. If an SPS set creation fails for any other reason than listed above, the reason code shall be set to 'Set creation failed'.

The PS set index is defined in 7.5.7.2.

The next wake beacon is either the next system wake beacon for the PSPS mode when the PS set index is set to one, or the next SPS wake beacon when the PS set index is greater than or equal to two and less than or equal to 253.

7.5.7.4 PS Set information request

<rename>

7.5.7.5 PS Set information response

<rename all SPS to PS, use standard DEVID table>

The PS set information response command shall be formatted as illustrated in Figure 5.

octets: 37	**...**	**37**	**1**	**2**	**2**
PS set structure n	...	PS set structure 1	Number of supported PS sets	Length (= (1+(n*37)))	Command type

Figure 5—PS set information response command format

The number of supported PS sets indicates the number of PS sets supported by the PNC of this piconet. The number of currently defined PS sets is determined from the number PS set structures in this command.

The PS set structure shall be formatted as illustrated in Figure 6.

octets: 1-32	**1**	**1**	**2**	**2**	**1**
DEVID bitmap	Start DEVID	Bitmap length	Next wake beacon	Wake beacon interval	PS set index

Figure 6—PS set structure field format

When the PS set index is zero, the DEVID bitmap lists the DEVs currently in HIBERNATION mode, if any. When the PS set index is one, the DEVID bitmap indicates the DEVs currently in PSPS mode, if any. When the PS set index is any other non zero value, the DEVID bitmap indicates the DEVs currently in this particular SPS set.

The wake beacon interval is set to the system wake beacon interval for PS sets 0 and 1. For all other PS sets it is set to the wake beacon interval of that SPS set.

The next wake beacon is set to the next system wake beacon for PS sets 0 and 1. For all other PS sets it is set to the next wake beacon of that SPS set.

The bitmap length field contains the number of octets in the DEVID bitmap. This field shall take on values from 1 to 32, inclusive.

The start DEVID indicates the DEVID corresponding to the lsb in the DEVID bitmap.

The DEVID bitmap field is a bitmap of the DEVIDs in a specific PS set. A value of 0 in a bitmap position indicates that a DEVID is not part of the PS set. A value of 1 in a bitmap position indicates that a DEVID is in the PS set.

8.2.3 Handover

Page 156, line 16, change ‘Once the PNC ... SPS inquiry response command, 7.5.7.5, to the new PNC.’ to be ‘

‘Once the PNC has successfully sent the PNC handover information command, it shall send the PS information response command, 7.5.7.5, to the new PNC. The PNC handover information command shall not be sent if the PNC has indicated in the PNC handover request command that it does not have any CTRBs to transfer. The PS information response command shall not be sent if the PNC has indicated in the PNC handover request command that it doesn’t have any PS sets to transfer.’

(ed note: keep the last sentence in the paragraph, changing SPS to PS. The previous copy of this on lines 8 and 9 of the same page were deleted with an editorial comment).

Table 58 – Comparison order of fields for PNC handover

(since all PS modes are mandatory, there is no need to list them here).

8.13 Power Management

(new text)

There are two states defined for this standard, the AWAKE state and the SLEEP state. There are four modes related to power management defined for this standard, ACTIVE, HIBERNATE, PSPS, and SPS modes. A DEV that is in either HIBERNATE mode or one or both of SPS and PSPS modes is defined to be in a power save mode DEV. 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. Regardless of power save mode, a DEV is allowed to go to the SLEEP state during a CTA where it is neither the source nor the destination. A DEV is also allowed to switch to the AWAKE state during any time when it is in a power save mode.

The wake beacon for a DEV is defined as the PNC defined system wake beacon for DEVs in PSPS mode, 8.13.1, and the wake beacon of the SPS set for a DEV in SPS mode, 8.13.2. A DEV that is in SPS mode may have multiple wake beacons. The wake beacon for a DEV in HIBERNATE mode occurs at times determined by the DEV and is unknown to the PNC and other DEVs in the piconet. Unlike the SPS and PSPS wake beacons, the wake beacon of the DEV in HIBERNATE mode is not periodic and is only guaranteed to happen once per ATP period for that DEV.

A DEV shall always associate and authenticate with the piconet starting in the ACTIVE mode.

Figure 2 lists the rules for the four modes of operation defined in this standard. Each cell indicates the state permitted, either WAKE or SLEEP, for the DEV.

Table 2—PS rules for superframe elements

Superframe portion	ACTIVE	HIBERNATE in wake superframe	PSPS or SPS DEV in wake superframe
Beacon	AWAKE	AWAKE	AWAKE
CAP	AWAKE	May SLEEP	AWAKE
CTA with BcstID as DestID (including MCTAs)	AWAKE	May SLEEP	AWAKE
CTA with McstID as DestID (including MCTAs)	May SLEEP	May SLEEP	May SLEEP
CTA with DEV as SrcID or DestID (including MCTAs)	AWAKE	May SLEEP	AWAKE
All other CTAs	May SLEEP	May SLEEP	May SLEEP

8.13.1 Piconet synchronized power save (PSPS) mode.

In the PSPS mode, the DEV is only required to be in AWAKE state during system wake superframes as indicated in Table 2. The wake beacon for PSPS DEVs is determined by the PNC. PSPS mode is identified by a PS set index equal to one.

The PNC shall announce the system wake beacon in the next wake beacon field in the PS status IE with PS set index one in the beacon. If none of the DEVs are in PSPS mode, the PNC may omit the PS status IE for PS set index equal to one from the beacon. In that case every beacon is a system wake beacons for the purpose of beacon information announcements, {xref 8.1.1}. The system wake beacon interval shall not be greater than 255.

It is the responsibility of the DEV using PSPS mode to synchronize with the system wake beacon before entering the sleep state.

Any DEV that wishes to use the PSPS mode shall send the PS configuration request command, {xref 7.5.7.2}, to the PNC with the Operation field set to ‘join’, PS set index set to one and the wake beacon interval set to its desired system wake beacon interval. The PNC shall upon reception of this command ACK the command and respond with a PS configuration response command with the next wake beacon.

A DEV may send the PS configuration request command more than once if its system wake beacon interval requirement changes. The DEV shall send the PS configuration request command with the operation type field set to ‘leave’ and the PS set index set to one to leave the PSPS set and no longer wishes to use PSPS mode.

A DEV shall send a PS mode change command to the PNC with the PS mode field set to PS and receive the ACK from the PNC before entering PSPS mode. When the PNC receives this command, it shall terminate all super-rate streams for which the DEV is the destination, {xref 8.5.1.3,} and set the DEVID bitmap field in the PS status IE for PS set index one appropriately, {xref 7.4.15}.

The PS status IE in the beacon for PS set index one with the bit for the DEV’s DEVID set shall serve as indication to other DEVs in the piconet that its peer has switched into PSPS mode.

When the DEV wants to switch to ACTIVE mode, it shall send a PS mode change command to the PNC with the PS mode field set to ACTIVE. Once this command is sent the DEV shall regard itself as in the ACTIVE mode regardless if the command was acknowledged by the PNC or not. If the PNC does not set the PS status bitmap appropriately, the DEV should resend the PS mode change command to the PNC. The PNC is not required to align subrate allocations for a PSPS DEV with the system wake beacon.

8.13.2 Synchronous power save (SPS) mode

Move “The PNC shall support at least one SPS set when the PNC is battery powered and support at least four SPS sets when the PNC is powered by the alternating current mains, Table 61.” to 8.13 and rewrite it as: “The PNC shall support one PS set for HIBERNATE and one PS set for PSPS. In addtion the PNC shall support at least one SPS set, i.e. a PS set with PS set index between 2 and 255, when the PNC is battery powered and support at least four SPS sets when the PNC is powered by the alternating current mains, {xref Table 61.}”

8.13.2.1 Creation, use and management of SPS sets

In order to use the SPS mode, the DEV is required to join an SPS set. Each SPS set has two associated parameters: the wake beacon interval and the next wake beacon. The SPS set is identified by an index value called the PS set index that is between 2 and 255. The wake beacon interval is the number of superframes between two successive wake beacons of that SPS set. This value is set by the DEV by creating the SPS set. The next wake beacon parameter is the beacon number corresponding to the immediate next wake beacon of that SPS set. This parameter is set by PNC when it creates the PS set. Both of these parameters shall be maintained by the PNC.

Any DEV that is a member of the piconet may request the information about the existing SPS sets by sending a PS set information request command, 7.5.7.4, to the PNC. The PNC shall respond by sending a PS set information response command, 7.5.7.5, that provides the parameters of all of the PS sets currently in use within the piconet.

The DEV may select an SPS set to join. If there are not any SPS sets currently in existence that match the DEVs requirements, the DEV may request the formation of a new SPS set by setting the PS set index field in the PS configuration request command, 7.5.7.2 to the ‘unallocated set’ value and the operation type field set to ‘join’. The DEV shall set the wake beacon interval field to its requested value. This value shall not be less than 4 and not greater than 65535. This value shall not be changed while the SPS set has any members. The PNC shall respond to the request by sending the PS configuration response command, 7.5.7.3, to the DEV indicating success or the reason the request failed. If the SPS set is created, the PNC assigns a PS set index to it. The PNC shall assign a unique number between 2 and 253 for the PS set index. The PNC includes in the PS configuration response command a value for the next wake beacon field set to the beacon number of the first wake beacon for the new SPS set. Once an SPS set is created, the PNC shall keep the next wake beacon for that set updated at all times. The maximum number of SPS sets supported by the PNC is implementation dependent up to a maximum of 252.

A DEV may join an existing SPS set by sending the PS configuration request command to the PNC with the PS set index field set to the index of an existing SPS set and the operation type field set to ‘join’. All other parameters shall be ignored. The PNC shall confirm or reject the request by sending the PS configuration response command to the DEV. Since a DEV may support multiple applications with different requirements, a DEV may register in more than one SPS set at a given time.

A DEV that no longer needs to be in an SPS set shall send the PS configuration request command to the PNC with operation type field set to ‘leave’. The PNC shall not send the PS configuration response command to the requesting DEV if the operation field was set to ‘leave’.

When the last member of an SPS set has left, the SPS set shall be terminated by the PNC.

8.13.2.2 Changing power save mode and operation

SPS DEVs alternate between SPS mode and ACTIVE mode depending on the amount and type of data traffic without leaving any of the SPS sets that the DEV has joined. The PS mode change command, 7.5.7.1, is used by a DEV to inform the PNC that it is changing its power save mode. A DEV shall have joined one or more SPS sets before it will be allowed to switch into SPS mode.

If the DEV wants to change its mode from ACTIVE to SPS, the DEV shall send the PS mode change command, 7.5.7.1, to the PNC with the PS mode field set to PS. The PNC shall then set the bit for the DEV in each PS status IE that corresponds to a PS set of which the DEV is a member. If the DEV is the source or destination of any streams, not including broadcast or multicast, which are not using an SPS wake beacon interval, the PNC shall terminate those streams, 8.5.1.3, when the DEV changes to SPS mode. The PNC does not automatically terminate any streams when the DEV changes from SPS to ACTIVE mode.

If the DEV has joined PS set one (PSPS) in addition to other SPS sets before issuing the PS mode change command, the DEV shall transition into a combined PSPS and SPS mode. In either case, the DEV shall not consider itself in either SPS or PSPS mode until at has received an Imm-ACK as response to the PS mode change command.

If the DEV wants to change its power save mode from SPS to ACTIVE, the DEV shall send the PS mode change command, 7.5.7.1, to the PNC with the PS mode field set to ACTIVE. Once this command is sent the DEV shall regard itself as in the ACTIVE mode regardless if the command was acknowledged by the PNC or not. If the PNC does not set the PS status bitmap appropriately, the DEV should resend the PS mode change command to the PNC. The PNC shall no longer set the bits for the DEV in the PS status IEs.

(Keep “If the state… is requested.”)

The PNC shall create one PS status IE in the beacon for each SPS set that has at least one member currently in SPS mode. When an SPS set is not in use, the PNC shall discontinue inserting its PS status IE in the beacon. The PNC needs to ensure that the number and size of the PS status IEs do not cause the beacon or extended beacon to exceed its maximum allowed size, 7.3.1.

Other DEVs may use the information in the PS status IE to learn when to transmit to an SPS DEV. In addition, the PS status IE informs SPS capable DEVs which SPS set is required in order to synchronize data transfers to the DEVs in SPS mode.

(Keep “Note that … beacon after the SPS DEV’s next wake beacon.”, 3 paragraphs)

Delete “If the CTR interval type set to super-rate then the SPS DEV shall have changed its power save mode from SPS to ACTIVE when it ACKs the CTA status command.” since we don’t use this command anymore.

Change “The PNC ... from ACTIVE to SPS” to be “The PNC shall no longer set the bits for the DEV in the PS status IEs. If the DEV did not wish to be switched to ACTIVE mode, it shall terminate the stream, 8.5.1.3, and use the PS mode change command to continue in SPS mode.”

If the CTR interval type of the new allocation is set to sub-rate the DEV may either:

— Stay in SPS mode while listening to the additional beacons required for the new allocation
— Switch to ACTIVE mode using the PS mode change command.
— Terminate the stream as described in 8.5.1.3.

8.13.3 Hibernation

HIBERNATE mode allows a DEV to conserve power for extended periods until the DEV chooses to listen for a beacon. The only responsibility of a DEV in HIBERNATE mode is to communicate with the PNC before the end of its ATP in order to preserve its membership in the piconet

In the HIBERNATE mode the DEV is not required to listen to any beacons or other traffic until it changes to either ACTIVE or a different power save mode using the PS mode change command, {xref }. HIBERNATE mode shall not be used in combination with any other power save mode.

All DEVs in HIBERNATE mode need to send at least one acknowledged frame to the PNC during their ATP in order to avoid being disassociated from the piconet, {xref disassoc}.

A DEV shall send a PS mode change command to the PNC with the PS mode field set to HIBERNATE and receive the ACK before entering HIBERNATE mode. When the PNC receives this command, it shall set the PS status bitmap appropriately, 7.4.14.

The PS status IE in the beacon with the bit for the DEV's DEVID set shall serve as indication to other DEVs in the piconet that its peer has switched to HIBERNATE mode. The PS set index of 0 shall only be used for HIBERNATE DEVs. Although a PS set index is assigned to the DEVs in HIBERNATE mode, the DEVs in this mode all act independently, unlike the DEVs that are members of other PS sets.

The DEV may leave HIBERNATE mode by sending a PS mode change command to the PNC with the PSMode field set to ACTIVE. Once this command is sent the DEV shall regard itself as in the ACTIVE mode regardless if the command was acknowledged by the PNC or not. If the PNC does not set the DEVID bitmap in the PS status IE appropriately, the DEV should resend the PS mode command to the PNC.

The HIBERNATE mode shall not be combined with any other power save modes and a DEV shall not use the PS configuration request command to set parameters for the HIBERNATE PS set.

8.13.4 Message sequence charts for power save modes

Figure 7 illustrates the message flow for a DEV requesting the creation of a new SPS set.

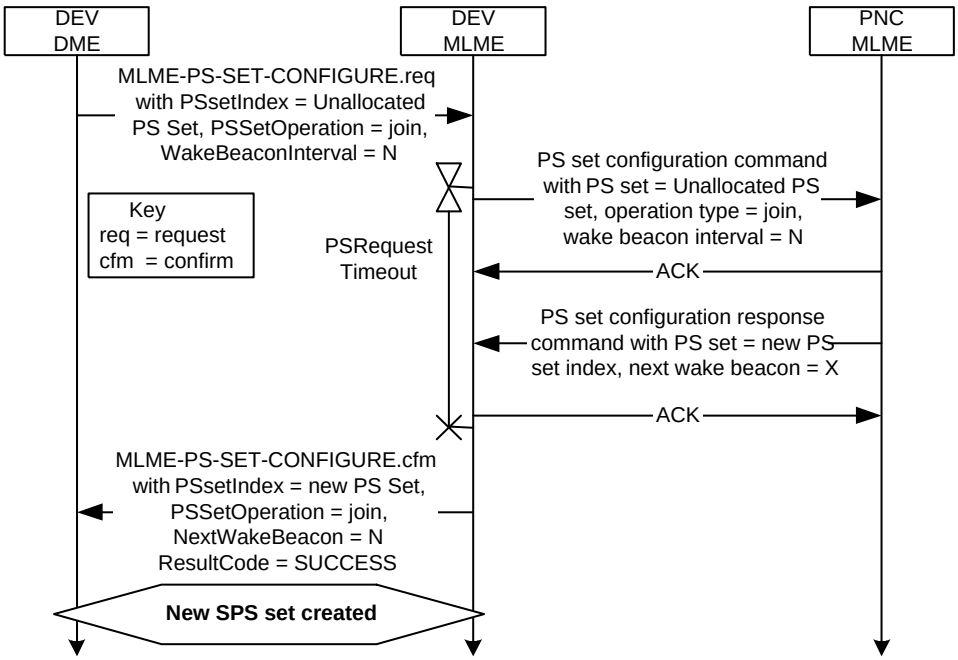


Figure 7—MSC for SPS set creation command

Figure 8 illustrates the message flow for a DEV requesting to add itself to an existing PS set.

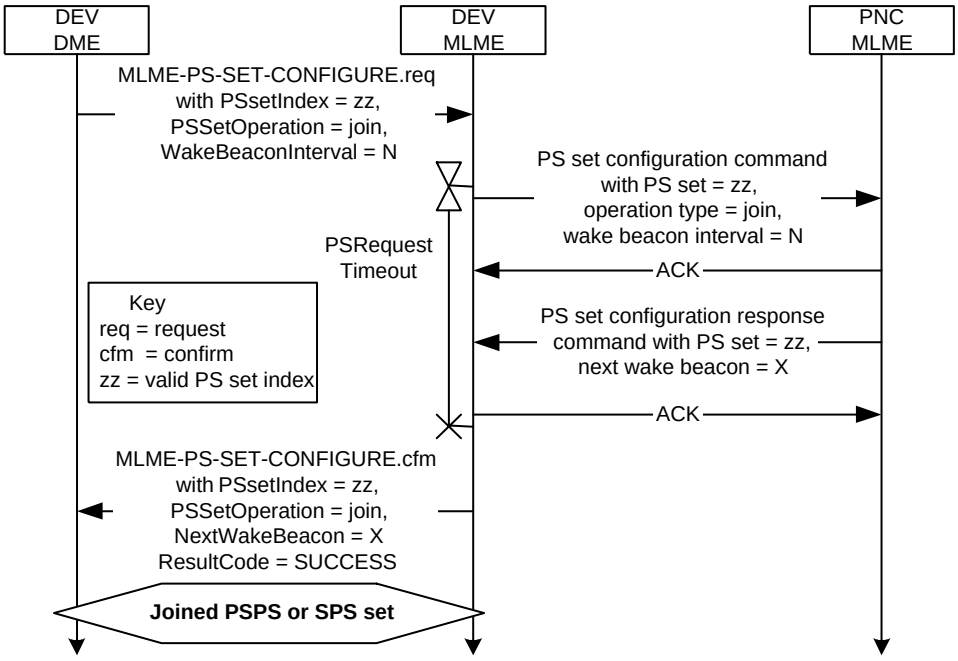


Figure 8—MSC showing a DEV requesting to join an existing PS set.

Figure 9 illustrates the message flow for a DEV requesting to leave a PS set.

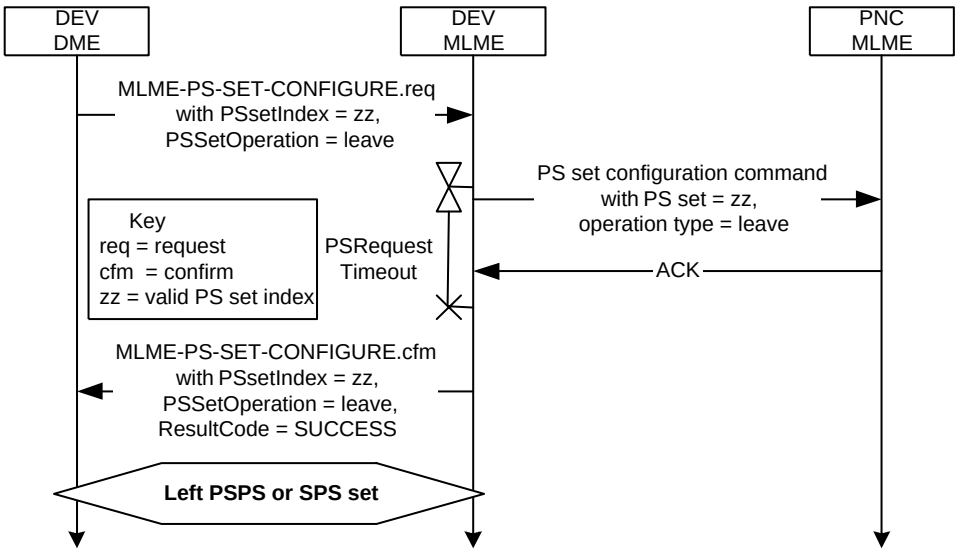


Figure 9—MSC showing a DEV requesting to leave a PS set.

Figure 10 illustrates the message flow for a DEV inquiring about the SPS sets that are currently defined within the PNC.

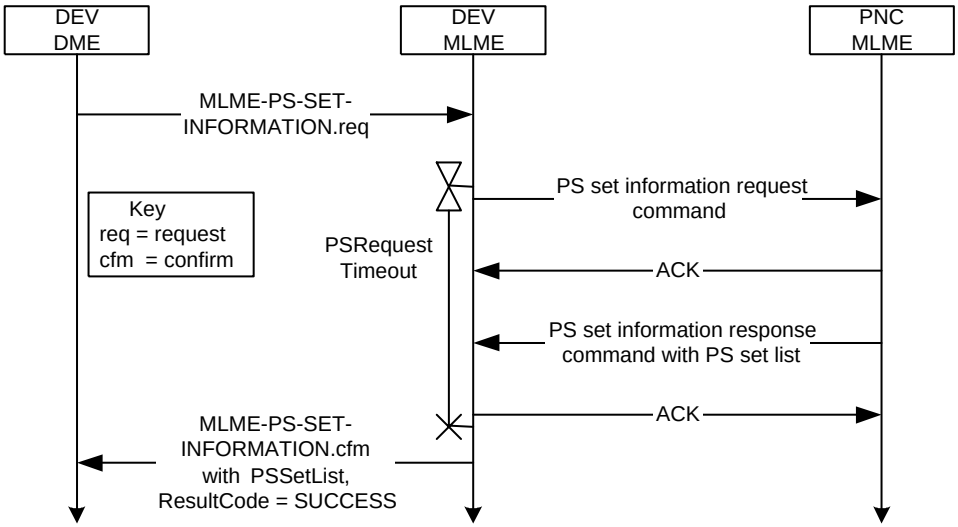


Figure 10—MSC for PS set inquiry command

Figure 11 illustrates the message flow for a DEV DME requesting to change the current PS mode of operation from ACTIVE to either PSPS or SPS when that DEV is a member of one or more PS sets.

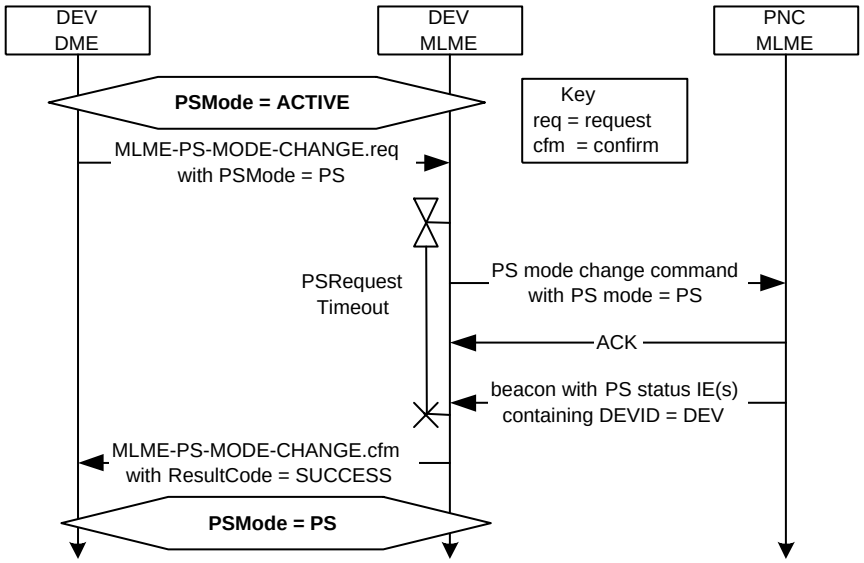


Figure 11—DME initiating PS mode change from ACTIVE to SPS, PSPS or both.

Figure 12 illustrates the message flow for a DEV DME requesting to change the current PS mode of operation from ACTIVE to HIBERNATE mode.

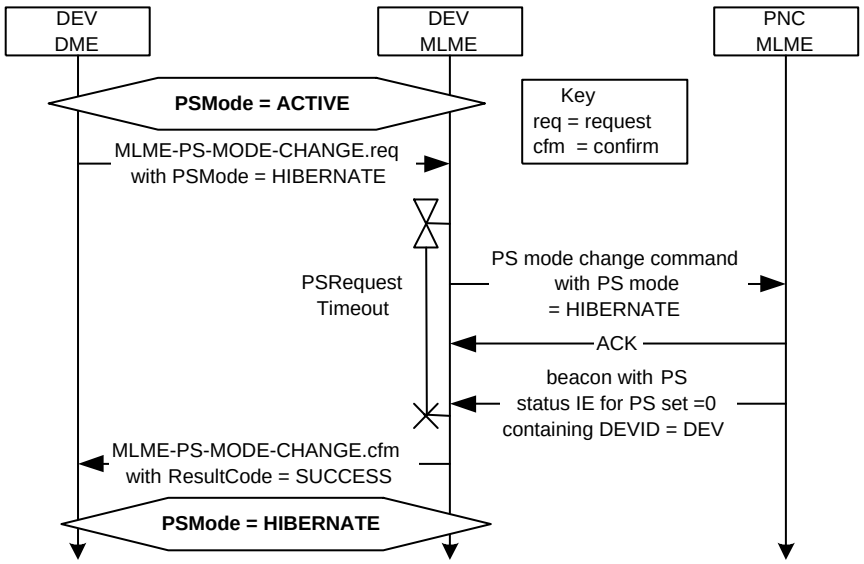


Figure 12—DME initiating PS mode change from ACTIVE to HIBERNATE

Figure 13 illustrates the message flow for a DEV DME requesting to change the current PS mode of operation from one of the power save modes to ACTIVE mode.

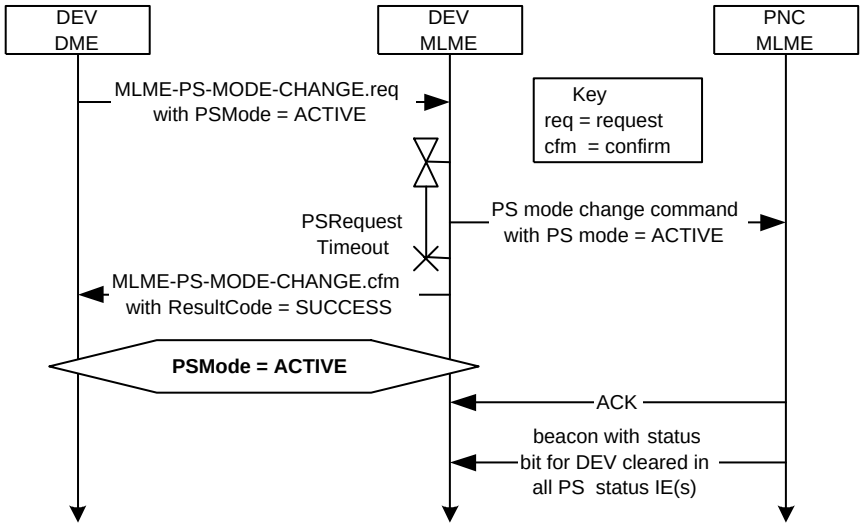


Figure 13—DME initiating PS mode change from any PS mode to ACTIVE

Keep the stream creation for SPS sets MSC (needs to be modified).

1.2 Email resolution of CID 93:

> "In 10.3.2.4.2, remove the final paragraph as this is considered out of scope (and isn't mentioned in the implicit certificate section) and is covered in the 'Verification of public key' part in 10.3.2.5.2.
>
> In 10.3.2.5.2, change the text in the 'verification of public key' part to: The DME extracts the public key from the received certificate as defined in 10.3.1.4 for use in the authentication protocol, verifies the binding of the received DEV address with the public key and uses its ACL to verify that the DEV is authorized to authenticate with that public key. The methods employed by the DME to accomplish these operations are outside the scope of this standard, but some suggested methods are described in C.4.
>
> Change the text in the 'verification of public key' part in the RSA and NTRU suites similarly.
>
> Replace sub-clause C.4 with the following text.

(begin new text for C.4)

C.4 Public-key to identity binding and device authorization

Each time a DEV participates in an authentication protocol, the DME bears the responsibility for verifying the binding between the other DEV's public key and identity and for authorizing that DEV to authenticate with it. Once this binding and authorization is completed, the device may proceed with the authentication protocol. If this protocol succeeds, it knows that the entity with which it authenticated is authorized to use the newly established management key for its intended purpose. If the binding cannot be verified or if authorization is denied, the DEV ends the authentication protocol.

The DME is able to use any set of methods to decide if the public key and address pair is correctly bound and authorized. These methods are outside of the scope of this standard, but options include:

- A digital certificate.
- An analog certificate. A manufacturer prints the DEV address and a hash of the public key on the bottom of the product for the user to verify.
- Low-power transmission. Two DEVs are brought into close physical proximity so they are able to "whisper" public keys over their radios.
- Range. The user confirms the distance between the two DEVs.
- Open enrollment. While located in a secure environment like a free-standing house, the DEVs simply trust public keys they receive over the air.
- Pre-loading. A manufacturer selling matched products, like the components of a home-entertainment system, would pre-load the ACLs with the addresses and public keys the system needs.
- User action. The user could push a button on both DEVs simultaneously.

This range of options is allowed to enable applications that have an appropriate mixture of security, cost-effectiveness and user-friendliness. In each case, some initial trust establishment is required.

For applications where trust is established through the use of digital certificates, each DEV obtains an authentic copy of the certificate authority's public key. The certificate authority generates the certificate for each DEV by performing a cryptographic operation on the DEV's identity and public key using its private key. A DEV verifies the binding between the ID and public key and authorizes the other DEV by verifying the certificate using the certificate authority's public key and performing checks that the certificate is trusted. These checks may include, but are not limited to, CRL checking, validity period verification, key use checking and comparing the DEV address in the certificate with the DEV address stored in its ACL.

For applications that do not establish trust through the use of digital certificates, user intervention or preloaded keys are typically required to provide the needed binding and authorization."

(end new text)

1.3 Thursday, 24 October, 2002

Attendee: James Gilb, Rene Struik, John Sarallo, Mark Schrader, Jay Bain, Allen Heberling, Knut Odman, Bill Shvodian, Jim Allen

Meeting called to order at 8:07 am PDT.

Agenda

- Drafting status

- PM command reduction

- PM compromise/discussion

1.3.1 Drafting status

JCS finished with CIDs for others, has 2 open CIDs

JB: No progress

ADH: 3 open (1 PM), 262 - 8.13.2.2 text (JB says is closed), 102 (passed),

JG: Needs to do 407 (references to the PICS), 424 (OUI)

AS: CID 102 has 9 and 10 text, 93, 119, 92 (waiting for feedback)

1.3.2 PM command reduction

PS Status IE should be OK

KO: Suggest make 2 mandatory any sets for all PNC capable DEVs.

Text is OK, makes edits. KO and MKS to write alternate text for mandatory power save modes.

JPKG will send out letter ballot.

Meeting adjourned at 8:50 am PDT.

2. San Diego meeting.

Agenda

Monday, 7 October 2002

1:00 pm - Called to order
3:00-3:15 pm - Break
6:00 pm - Recess

Tuesday, 8 October 2002

8:00 am - Called to order
10:15-10:30 am - Break
12:00-1:30 pm - Lunch
3:00-3:15 pm - Break
6:00 pm - Recess

Wednesday, 9 October 2002

8:00 am - Called to order
10:15-10:30 am - Break
12:00 - Adjourn
3:00-3:15 pm - Break
6:00 pm - Recess

Our tasks are:

Resolve remaining comments
Address any potential re-opens
Identify text that needs to be created
Review any new text.

2.1 Monday, 7 October, 2002

Called to order at 1:30 pm PDT.

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

2.1.1 Misc

183, 170, 290, 294, 543, 359

183 (Heberling, TR) - [FrmFrmt/Payload] replace aMaxFrameSize-4 with aMaxPayloadSize which is equal to aMaxFrameSize-4. A CID 255 from LB17, although withdrawn, indicated the confusing nature of the text. Also change this sentence frag <from> "...the number of actual information octets by 12." <to> "...the aMaxPayloadSize by 12 octets." Please make the indicated changes. **Suggest accept in principle:** “CIDs 97(TR), 188(E), and 190(E) also address the current short comings in the text and placement of the Payload and FCS field descriptions. Consequently, it is recommended that 1) clause 7.2.7 be deleted 2) the current clauses 7.2.7.1 and 7.2.7.2 be promoted to 7.2.8 and 7.2.9 respectively after being moved to just after the the Secure MAC frame body subclauses which currently occupy clauses 7.2.8, 7.2.8.1, 7.2.8.2, 7.2.8.3. Please

note the Secure MAC frame body subclauses will be promoted to the 7.2.7, 7.2.7.1, 7.2.7.2, and 7.2.7.3 positions in the current text. 3) Modify the text in clause 7.2.7.1, which will become 7.2.8, to read as follows:

‘7.2.8 Payload field

The payload is a variable length field and contains information specific to individual frame types. When the SEC bit is set to 0, the minimum payload is zero octets and the maximum payload length is aMaxPayloadSize, which is equal to aMaxFrameSize-4 octets.

When the SEC bit is set to 1, the minimum payload is 12 octets (|IntegrityCode(8)|EncryptedData(0)|SFC(2)|SECID(2)|) and the maximum payload length is aMaxPaylo
dSize in which aMaxEncryptedData is equal to aMaxPayloadSize-12 octets.’

4) Modify Figure 6, page 105 to look like this:

|FCS|IntegrityCode|EncryptedData|SFC|SECID|

| |_____Payload_____|

|_____Secure MAC FrameBody _____|”

Suggest accept in principle, “Resolve as indicated in CID 97, Add a new figure between figure 5 and figure 6 that is the Non-secure MAC Frame body:
|FCS| Payload |
|_Non-secure MAC FrameBody _|”
Change ‘Payload field’ to be ‘Data field’ in the title and in the text.”

Accept suggested resolution.

170 (Heberling, T) - [MultiCast] MLME-MULTICAST-RX-SETUP.request is not referenced anywhere in clause 8.Should it affect reception filtering?/KO. Decide what it shall do and add it to clause 8. **Suggest accept in principle:** “This primitive is only used at the higher levels of the MAC and does not affect (other than in implementation dependnet ways) the operation of the MAC. Since it does not change the on-air behavior of a DEV, there is no need to mention it in clause 8. For example, MLME-RESET and MLME-SYNCH are not mentioned anywhere but in clause 6 since they only affects that interface.”

Table until Wednesday, 8 October, 2002, WMS to supply text for 8.5.3.

290 (Heberling, TR) - [ChnlChng] The second paragraph of subclause 8.11.1 is technically a mess. It inserts a description of the PNC's self channel scanning procedure into the middle of a description regarding the channel change procedure. It would be much better to seperate these two procedures into seperate subclauses: a) 8.9.5 PNC channel scanning b) 8.11.1 Dynamic Channel Selection.Consequently, perform these three operations:1)Move all of paragraph 2 (Lines 37-42) to a new subclause 8.9.5 PNC Channel Scanning.2) delete the first two sentences of paragraph three (lines 44-45) they will become unnecessary.3) Add this sentence at the beginning of paragraph 3, subclause 8.11.1. ‘If the PNC determines after performing its own scan of other channels, or requesting member DEVs to perform remote scans on its behalf that there are one or more other channels with better characteristics than exist in its current operating channel, then the PNC may decide to initiate the dynamic channel change procedure. In the case where the PNC decides to initiate a dynamic channel change, the PNC shall broadcast the piconet parameter change information element, 7.4.6, in its current channel via its beacon for up to a NmbrOfChangeBeacons. ...’ Please make the indicated change. **Suggest reject:** “The PNC is required to check for itself that the new channel is clear before it moves the piconet to it. Since the PNC is the center of the piconet, it is best able to determine if the channel is clear before it changes channels. The change proposed removes the requirement that the PNC check the new channel before changing to it. The PNC self channel scanning procedure is required only for

this process and so its description belongs in this location. The PNC may use other techniques for scanning channels at other times, but it is required to check for itself the quality of the channel, just as it does when it starts a piconet."

Tabled until October, 8 2002, ADH to provide text.

"Add new sub-clause (see 02/392r13 for formatting):

'8.9.5 PNC channel scanning

PNC channel scanning is a procedure by which the PNC is able determine the channel characteristics of not only its current operating channel but also the channel characteristics of one or more alternate channels. The PNC may use the results of its channel scans to determine whether the current channel in which it is operating has acceptable characteristics or that there is one or more other channels with better channel characteristics than its current channel.

The PNC may allocate CTAs such that there is unallocated channel time in the CFP. This provides quiet time for the PNC to scan channels for other 802.15.3 piconets, non 802.15.3 wireless networks, or interference.

If the PNC initiates a scan of one or more alternate channels, the PNC shall not transmit a beacon for one or more beacon intervals. The PNC shall not suspend beacon transmissions for more than twice aMinChannelScan. The PNC, upon returning to its current channel and resuming the transmission of its beacons, shall increment the beacon number field by the number of beacons not sent during the time the PNC was scanning one or more alternate channels.

After scanning the channels, if the PNC determines that the channel characteristics are acceptable, the PNC shall continue operating its piconet in the current channel.

After scanning both its current channel and one or more alternate channels, the PNC may initiate one of these options:

1) Do nothing since the PNC has determined that none of the alternate channels were better than its current channel.
2) Initiate the dynamic channel change procedure described in {xref: 8.11.1}.
3) Increase or decrease the max tx power level of the piconet {xref: 7.3.1, 8.11.2.1}.
4) Initiate some other unspecified action.

The algorithm for determining when to initiate any of these actions is outside the scope of this standard.'"

294 (Heberling, TR) [Scan/PNC] Subclause 8.11.1 Paragraph 2 Line 37-45 makes reference to a PNC scanning procedure which is incompletely defined in clause 8.11.1. Consequently, use this text describing the PNC's procedure for determining the piconet's channel quality: <New text>:8.9.5 PNC channel scanning-PNC channel scanning is a procedure by which the PNC may determine the channel characteristics of not only its current operating channel but also the channel characteristics of one or more alternate channels. The PNC may use the results of its channel scans to determine whether the current channel in which it is operating has acceptable characteristics or there is one or more other channels with better channel characteristics than its current channel. If the characteristics of the current channel are acceptable, the PNC shall continue operating its piconet in the current channel. If, however, the channel characteristics are unacceptable, and there exists one or more alternate channels with better characteristics than the current channel, the PNC may initiate a dynamic channel change {ref: 8.11.1} to a channel with better channel characteristics. The algorithm for determining when to change channels is outside the scope of this standard.The PNC may optionally allocate CTAs to itself such that there is quiet time during the superframe for it to scan its current channel for other 802.15.3 piconets, non 802.15.3 wireless networks, or interference. If the PNC, after scanning its current channel, determines that the channel characteristics are unacceptable, the PNC may initiate

channel scans of one or more other channels to determine whether there is an alternate channel with better characteristics than its current channel. While performing a scan of an alternate channel, the PNC shall not transmit a beacon for one or more beacon intervals. The PNC shall not suspend beacon transmissions for more than twice aMinChannelScan. The PNC, upon returning to its current channel and resuming the transmission of its beacons, shall increment the beacon number field by the number of beacons not sent during the time the PNC was scanning one or more alternate channels. The algorithm used to determine whether the characteristics of an alternate channel are better or worse than the current channel characteristics is outside the scope of this standard. The PNC after scanning its current channel and other channels may decide upon one of these actions:1) do nothing since the PNC determined that none of the alternate channels were better than its current channel2) initiate the dynamic channel change procedure described in {xref: 8.11.1}3) increase/decrease the Max Tx power level of the piconet {xref: 7.3.1, 8.11.2.1}4) initiate some other unspecified vendor specific action. **Suggest reject:** “The scanning procedure in 8.11.1 is only required when the PNC is looking to change channels and so it makes sense editorially to keep this description with the channel change description. Any other time that the PNC wished to scan for interference in the current channel or to assess the characteristics of other channels is already allowed since the standard does not prohibit it. The method that the PNC uses to make these additional scans is implementation dependent and therefore is outside of the scope of this standard. In the case of where the PNC is changing channels, it is important to require the PNC to first check the new channel to ensure that, from its point of view, the channel is quiet. The suggested text repeats information that is already in 8.11.1 and 8.11 and does not add any new information or technical requirements. See also the resolution of CID 290.”

> “Change 8.11.1 to read as follows:
>
> ‘8.11.1 Dynamic Channel selection
>
> The PNC initiates dynamic channel selection if it determines that the current conditions of its channel are poor. The PNC may use one or more of these methods to make this determination.
> 1) the PNC may perform a PNC channel scanning procedure, defined in {xref 8.9.5}.
> 2) the PNC may use the remote scan procedure, defined in {xref 8.9.4}.
> 3) the PNC may collect the channel status from its member DEVs by sending the channel status request command, defined in {xref 7.5.6.1}, to request that the DEVs provide their channel status via the channel status response command, {xref 7.5.6.2}.
>
> The algorithm required to use the channel status information when deciding whether to change of channel is outside of the scope of this standard.
>
> The PNC shall initiate a dynamic channel change procedure only after it has performed a PNC channel scan, {xref 8.9.5}, and has determined that there is one or more channels with better characteristics than exist in its current operating channel. If the PNC decides to initiate a dynamic channel change, the PNC shall broadcast the piconet parameter change information element, {xref 7.4.6}, in its current channel via its beacon for up to aNmbrOfChangeBeacons. ...’ continue with text from page 202, clause {xref 8.11.1}, Line 45 and on.”

359 (Schrader, TR) - A countdown counter for PSPS requires more PNC overhead than is necessary. The improved implementation shouuld be used for both SPS and PSPS. The Next Awake Beacon value must be update only once per awake beacon interval. The countdown must be updated every beacon. The Next Awake Beacon can have the same number of bits as the countdown timer. If the awake beacon is to be "pushed" to the next super frame, the Next Awake Beacon can be set to the beacon number of the next superframe. BOTH SPS and PSPS should have this.

> Suggest accept in principle, “Add 2 octets to the PSPS status IE (or piconet synchronization parameters) that has the “next system awake beacon” which indicates the beacon number of the next system awake beacon. Table until 8 October, 2002. Question for everyone, Where do the changes need to be made (MKS)? and Did we miss anything?

Accept in principle “The new PNC needs to get the requested intervals from the old PNC. In 7.5.4.2 - add 1 octet to the DEV info field ‘Requested system wake beacon’ with definition, ‘The requested system wake beacon interval is the value that the DEV sent to the old PNC in the PS mode change command, {xref 7.5.7.1}’. Add 2 octets to the PSPS status IE that are ‘Next system wake beacon’ with definition, ‘The next system wake beacon field is the beacon number of the next system wake beacon, {xref 8.system.wake.beacon}.’ Also, check 8.13.1 to match the new usage. 8.13.1, page 206, lines 38-39, change to

‘The PNC shall announce the system wake beacon in the next system wake beacon field in the PSPS status IE in the beacon. If no DEV is in PSPS mode, the PNC may omit the PSPS status IE from the beacon. In that case every beacon is a system wake beacons for the purpose of beacon information announcements, {xref 8.1?}. The system wake beacon interval shall not be greater than 255.’

This affects CIDs that talk about adding the system wake beacon to the synchronization field. Instead it is put into the IE. {Ed. note: we need more text for this to identify the changes.”

2.1.2 Security

101, 63, 111, 112, 124, 93

101 (Gilb, TR) [SEC] The disassociation request command may be sent before the device is authenticated. In addition, the table does not specify when the commands shall be sent with security turned on. The X should be removed from the “authenticated (if required)” column for the disassociation request command and a column should be added indicating which frames shall be sent with security when authenticated. Recommend allowing the probe command and piconet services command and all of the association, authentication and challenge commands not to require security and all the rest of the commands to require security when authenticated. Alternately, this information could be added to clause 9 if that is a more appropriate location. **Suggest accept in principle.** Remove the “X” from the disassociation request command. Add a column to Table 48 with the heading “Security required if authenticated” and insert an “X” in every entry except for association request, association response, authentication request, authentication response, challenge request, challenge response, probe and piconet services. Re-write the first paragraph of 7.5 to coordinate this resolution with the resolution to 63. Change first paragraph to:

“The MAC command types are listed in Table 48 and are described in the following subclauses. If the column labeled “Associated” in Table 48 is marked with an “X” then that command shall only be sent by a DEV that is associated in the piconet. If the column labeled “Authenticated (if required)” in Table 48 is marked with an “X” and authentication is required for the piconet, then that command shall only be sent by a DEV that is authenticated with the PNC in the piconet. For peer-to-peer communications, if the DEV requires security with the selected peer DEV, and the “Authenticated (if required)” column is marked with an “X”, that command shall be sent to the peer DEV only if the DEVs are authenticated to each other. If the column labeled “Security required if authenticated” in Table 48 is marked with an “X” and authentication is required for the piconet, then that command shall be sent securely using the key specified in {xref - Table 57} for that command. For peer-to-peer communications, if the DEV requires security with the selected peer DEV, and the column labeled “Security required if authenticated” in Table 48 is marked with an “X”, then that command shall be sent securely to the peer DEV using the key specified in {xref - Table 57}.”

Table, Singer to rewrite the text as list or table perhaps? Note that the sentence ‘For peer-to-peer communications, ... authenticated to each other.’

Table until 8 October, 2002.

Accept in principle “Remove the ‘X’ under ‘Authenticated (if required)’ for the disassociation request command.

In 9.2.7, replace the sentence

‘Table 57 provides a listing of which keys are to be used for protecting secure frames.’

with the following text:

‘Table 57 provides a listing of which keys shall be used to protect secure frames and which frames shall be sent without security. A DEV shall not send a secure frame if the only key selection in Table 57 is ‘none’. A DEV shall not send an unprotected frame or a frame with an incorrect SECID when security is required for that frame.’

In 9.2.8, add the following text to the beginning of the sub-clause:

‘Table 57 provides a listing of which keys shall be used to protect secure frames and which frames shall be sent without security. A DEV may ignore any secure frame if the only key selection in Table 57 is ‘none’. A DEV may ignore any non-secure frame or a secure frame with an incorrect SECID when security is required.’

In 9.2.11, change the sentence
‘If two DEVs in a secure piconet do not have a peer-to-peer security relationship, they may use the piconet group data key for secure commands and secure data frames transmitted between them.’

to:

‘If two DEVs in a secure piconet do not have a peer-to-peer security relationship, they shall use the piconet group data key for commands that are required to be sent securely and they may use the piconet group data key for data frames transmitted between them.’

Add an ‘X’ to the None column for data frames and add the following text before the existing text in that row under ‘Comment’:

‘Data frames may be sent at any time with or without security.’

Add an ‘X’ to the None column for disassociation request and add the following text in that row under ‘Comment’:

‘Disassociation request commands shall not be secured with any key before the DEV is authenticated with the PNC and shall be protected by the PNC-DEV management key otherwise.’

Add an ‘X’ to the None column for probe and add the following sentence before the existing text in that row under ‘Comment’:

‘If the probe command is sent to or from the PNC before authentication, the command shall not be secured by any key.’

For the piconet services command entry, put an ‘X’ in the ‘None’ column and remove the ‘X’ from all other columns. Delete the text in the ‘Comment’.”

111(Gilb, TR) [SEC] Table 57: It needs to be indicated either here or in clause 7 that the probe command, piconet services command and disassociate command may be sent insecurely before authentication has taken place. Add text that indicates that the probe command, piconet services command and disassociate command may be sent insecurely before authentication has taken place. **Suggest accept in principle.** See proposed resolution to 101.

Table pending resolution of CID 101.

124 (Gilb, TR) [SEC] It seems that the types of security support that are listed here are limited only to the methods that are explicitly defined in the standard. There may be additional methods that should be allowed and there should be a means for vendors to indicate that there are vendor specific methods implemented. For instance, certificates that are not in the format specified here, such as X.509 certificates used in browsers, may be useful to use to provide evidence of the validity of a public key while in mode 1 or mode 2. Change the ECC and RSA X.509 certificates to be simply an X.509 certificate. The certificate indicates the method used for authentication. **Suggest accept in principle.** Add PICS entries for supporting various kinds of ACL information in the ACL information command.

Send suggestion of added PICS to email.

Table 0.1—ACL information verification

Item Number	Item Description	Reference	Status	Support		
				N/A	Yes	No
S5	ACL info command {Ed. note, this may be in MAC frames instead of here, in which case this will be a heading.}	{xref ACL info}	O			
S5.1	NTRU SHA-1 hash	{Ed. note: Delete all rows that do not have corresponding text in clause 10}	S5: O.9?			
S5.2	RSA SHA-1 hash		S5: O.9?			
S5.3	NTRU X.509 CA certificate		S5: O.9?			
S5.4	ECC SHA-256 hash		S5: O.9?			
S5.5	ECMQV Koblitz-283 CA key		S5: O.9?			
S5.6	ECC X.509 CA certificate		S5: O.9?			
S5.7	RSA X.509 CA certificate		S5: O.9?			

Table 0.1—ACL information verification

Item Number	Item Description	Reference	Status	Support		
				N/A	Yes	No
S5.8	ECMQV Koblitz-283 key		S5: O.9?			
S5.9	NTRUEncrypt 251-1 key		S5: O.9?			
S5.10	RSA-OAEP raw 1024 key		S5: O.9?			
S5.11	ECC X.509 certificate		S5: O.9?			
S5.12	RSA X.509 certificate		S5: O.9?			
S5.10	NTRU X.509 certificate		S5: O.9?			
S5.11	ECC certificate chain URL		S5: O.9?			
S5.12	RSA certificate chain URL		S5: O.9?			
S5.12	NTRU certificate chain URL		S5: O.9?			
S5.13	ECMQV Koblitz-283 implicit certificates		S5: O.9?			

Accept in principle, “Add new entries to the PICS as indicated in 02/392r13.”

63 (Gilb, TR) [SEC] We still don't have a good description of what to do with commands sent or received with security on. Also need to generalize for the case of peer-to-peer security. Add description including peer-to-peer security. **Suggest accept in principle. (Note that this introduces functionality to maintain separate modes for different DEVs)** Add the following text to the beginning of 9.2.11:

“DEVs shall maintain a security state denoting whether security is required for each security relationship. If security is required for a particular security relationship, all frames transmitted to and received from another DEV in that relationship shall be protected by the keys indicated in {xref - Table 57}. A DEV may send or receive certain command frames without protection as indicated in {xref - Table 48}. If a DEV receives a frame that is not protected as required, the DEV shall discard the frame. If security is not required for a security relationship, all frames transmitted to and received from another DEV in that relationship shall be sent without security. If a DEV receives a protected frame when security is not required, the DEV shall discard the frame.

If the DEV is participating in a secure piconet, the security state for the relationship with the PNC, and consequently the broadcast key, shall be set to security required. For peer-to-peer communications, the DEV may choose to require security or not for that relationship, regardless of the security state shared with the PNC. If security is required in a peer-to-peer relationship, but the DEVs have not authenticated with each other, the group data key shall be used to protect frames between the DEVs.”

Suggest accept in principle, “Require that commands in a secure relationship are sent according to table 48 for both PNC-DEV as well as DEV-DEV relationships. (AS needs to write new text for 7.5 that says this, see also CID 101). Allow data to be sent any way you want, add a new parameter to

the table, “PayloadProtected”; “Enumeration”; “NONE, GROUP, PEER”; “The type of protection that is applied to the payload, {xref 9.8.8, payload protection}. Add the parameter ‘PayloadProtected’ to the MAC-{ASYNC,ISOCH}-DATA.request and MAC-{ASYNC,ISOCH}-DATA.indication”.

Accept in principle. “Line 7, change ‘The PNC shall not respond to any command ...’ to be ‘The PNC or a DEV shall not respond to any command ...’ on line 8, change ‘The PNC may transmit an ACK ...’ to be ‘The PNC or a DEV may transmit an ACK ...’”

93 (Gilb, TR) [SEC/PIB] The security suite and public-key verification information have been removed from the MAC PIB. This implies that there is no accessible information that the MLME can use to perform verification on the public key. In particular, the CA certificate or hash of the public key are not available. In clause 10, each security sub-suite specifies that the ACL indicates which public-keys shall be accepted and which shall be rejected. Add public-key verification information back into the ACL and specify in each security suite how that ACL information is to be used. If there are operations to be performed by the DME to verify the public key, those should be mentioned in the security suites as well. This applies to 6.5.6 as well. **Suggest accept in principle.** The public key verification operations are performed by the DME and are hence outside the scope of the standard. Rather than adding this information to the PIB, the description of the security suites in clause 10 should be modified to reflect that this is out of scope. Make the following changes to clause 10:

In clause 10.3.1.4.3, change the paragraph in lines 18-19 to: “The certificate shall be generated using the digital signature algorithm ECDSA as specified in 10.3.1.4.4. The validation of the certificate is outside the scope of this standard.”

In 10.3.2.2.2, remove step 2) and the final sentence and add the following text:

“Processing shall be aborted if the public key is not successfully extracted.

The DEV should perform additional checks such as comparing the DEV address in the ManCert to the DEV address in the authentication request or comparing the received key and ID to values stored in its ACL to verify the authenticity of the public key.”

In 10.3.2.3.2, remove step 2) and the final sentence and add the following text:

“Processing shall be aborted if the public key is not successfully extracted.

The DEV should perform additional checks such as comparing the DEV address authenticated in the ImplCert with the DEV address stored in its ACL to verify that the device is authorized.”

In 10.3.2.4.2, remove step 2) and the following paragraphs and add the following text:

“Processing shall be aborted if the public key is not successfully extracted.

The DEV should perform additional checks such as signature verification as specified in 10.3.1.4.3, CRL checking, validity period verification, key use checking and comparing the DEV address in the X.509 certificate with the DEV address stored in its ACL to verify that the device is authorized.”

In 10.4.2.2, change the table entry for Verification of Public-Key to the following text:

“The ID and public-key received during the authentication protocol should be verified by the DME using checks such as generating the SHA-1 hash of the device address concatenated with the public-key and comparing that to the hash of the ID and public key stored in the ACL.”

In 10.5.2.2, change the table entry for Verification of Public-Key to the following text:

"The ID and public-key received during the authentication protocol should be verified by the DME using checks such as generating the SHA-1 hash of the device address concatenated with the public-key and comparing that to the hash of the ID and public key stored in the ACL."

In 10.5.3.2, change the table entry for Verification of Public-Key to the following text:

"The X.509 certificate received in the authentication protocol should be verified by performing checks such as signature verification as specified in 10.5.1.7, CRL checking, validity period verification, key use checking and comparing the DEV address in the X.509 certificate with the DEV address stored in its ACL to verify that the device is authorized."

Table until it can be reviewed with Rene.

112 (Gilb, TR) [SEC] There needs to be a clear delineation between the aspects of the certificate usage that are within scope and those that are out of scope. If we are specifying the exact format of the entity certificate, it seems that the format of the CA key and the other information should be specified as well. It should be made clear what checks, if any, are performed by the MLME and what checks should be pushed up to the higher layer. **Suggest accept in principle.** Resolve as proposed in 93. As in the proposed resolution to 93, the manner in which the public key is accepted for the authentication protocol is out of scope. It is appropriate to clearly define the manner in which the certificate itself can be verified, so the definition of how to create and verify the certificate should not be removed. Instead, make changes indicated in 93 to state that devices should (instead of shall) verify the authenticity of the public key by performing the certificate checking operations. The resolution to 102 provides the ability for each security suite to define ACL entries, which may include CA certificates, which include CA keys.

Table pending resolution of CID 93.

2.2 Tuesday, 8 October, 2002

101 (Gilb, TR) [SEC] The disassociation request command may be sent before the device is authenticated. In addition, the table does not specify when the commands shall be sent with security turned on. The X should be removed from the "authenticated (if required)" column for the disassociation request command and a column should be added indicating which frames shall be sent with security when authenticated. Recommend allowing the probe command and piconet services command and all of the association, authentication and challenge commands not to require security and all the rest of the commands to require security when authenticated. Alternately, this information could be added to clause 9 if that is a more appropriate location. **Suggest accept in principle.** Remove the "X" from the disassociation request command. Add a column to Table 48 with the heading "Security required if authenticated" and insert an "X" in every entry except for association request, association response, authentication request, authentication response, challenge request, challenge response, probe and piconet services. Re-write the first paragraph of 7.5 to coordinate this resolution with the resolution to 63. Change first paragraph to:

"The MAC command types are listed in Table 48 and are described in the following subclauses. If the column labeled "Associated" in Table 48 is marked with an "X" then that command shall only be sent by a DEV that is associated in the piconet. If the column labeled "Authenticated (if required)" in Table 48 is marked with an "X" and authentication is required for the piconet, then that command shall only be sent by a DEV that is authenticated with the PNC in the piconet. For peer-to-peer communications, if the DEV requires security with the selected peer DEV, and the "Authenticated (if required)" column is marked with an "X", that command shall be sent to the peer DEV only if the DEVs are authenticated to each other. If the column labeled "Security required if authenticated" in Table 48 is marked with an "X" and authentication is required for the piconet, then that command shall be sent securely using the key specified in {xref - Table

57} for that command. For peer-to-peer communications, if the DEV requires security with the selected peer DEV, and the column labeled “Security required if authenticated” in Table 48 is marked with an “X”, then that command shall be sent securely to the peer DEV using the key specified in {xref - Table 57}.”

Accept in principle “Remove the ‘X’ under ‘Authenticated (if required)’ for the disassociation request command.
In 9.2.7, replace the sentence

‘Table 57 provides a listing of which keys are to be used for protecting secure frames.’

with the following text:

‘Table 57 provides a listing of which keys shall be used to protect secure frames and which frames shall be sent without security. A DEV shall not send a secure frame if the only key selection in Table 57 is ‘none’. A DEV shall not send an unprotected frame or a frame with an incorrect SECID when security is required for that frame.’

In 9.2.8, add the following text to the beginning of the sub-clause:

‘Table 57 provides a listing of which keys shall be used to protect secure frames and which frames shall be sent without security. A DEV may ignore any secure frame if the only key selection in Table 57 is ‘none’. A DEV may ignore any non-secure frame or a secure frame with an incorrect SECID when security is required.’

In 9.2.11, change the sentence
‘If two DEVs in a secure piconet do not have a peer-to-peer security relationship, they may use the piconet group data key for secure commands and secure data frames transmitted between them.’

to:

‘If two DEVs in a secure piconet do not have a peer-to-peer security relationship, they shall use the piconet group data key for commands that are required to be sent securely and they may use the piconet group data key for data frames transmitted between them.’

Add an ‘X’ to the None column for data frames and add the following text before the existing text in that row under ‘Comment’:

‘Data frames may be sent at any time with or without security.’

Add an ‘X’ to the None column for disassociation request and add the following text in that row under ‘Comment’:

‘Disassociation request commands shall not be secured with any key before the DEV is authenticated with the PNC and shall be protected by the PNC-DEV management key otherwise.’

Add an ‘X’ to the None column for probe and add the following sentence before the existing text in that row under ‘Comment’:

‘If the probe command is sent to or from the PNC before authentication, the command shall not be secured by any key.’

For the piconet services command entry, put an ‘X’ in the ‘None’ column and remove the ‘X’ from all other columns. Delete the text in the ‘Comment’.”

111(Gilb, TR) - [SEC] Table 57: It needs to be indicated either here or in clause 7 that the probe command, piconet services command and disassociate command may be sent insecurely before authentication has taken place. Add text that indicates that the probe command, piconet services command and disassociate command may be sent insecurely before authentication has taken place. **Suggest accept in principle.** See proposed resolution to 101.

Accept in principle, “Resolve as indicated in CID 101.”.

102 (Gilb, TR) - In 02/399r4 section 1.2.2.2, replace the text for the verification info type with the following text and remove section 1.2.4 (this will be replaced by text in the security suites - see below):

“The verification info type indicates the type of verification information that is included in the transmitted ACL entry. The verification info types are security suite specific. The definition and format of the valid verification information elements for each security suite are defined in the security suites, see {xref - 10}. The encoding of this octet shall be formatted as illustrated in Figure 14.

b7-b5	b4-b0
Security suite	Verification information format

Figure 14—Verification info type field

The verification information format indicates the type of information that is being transmitted in the verification info type field. The valid verification info types are encoded as illustrated in Table 3.

Table 3—Verification information format field encodings

Type value b4 b3 b2 b1 b0	Verification information format
00000	NULL
00001	ECMQV Koblitz-283 key
00010	NTRUEncrypt 251-1 key
00011	RSA-OAEP raw 1024-1 key
00100	ECMQV Koblitz-283 implicit certificate
00101	X.509 certificate
00110	X.509 CA certificate
00111	ECMQV Koblitz-283 CA key
01000	SHA-1 hash
01001	SHA-256 hash
01010	Certificate chain URL
01011-11111	Reserved

The security suite format indicates the security suite with which the verification info shall be used. The valid security suite types are encoded as illustrated in Table 4."

Table 4—Security suite field encodings

Type value b7 b6 b5	Security suite format
001	ECMQV Koblitz-283
010	NTRUEncrypt 251-1
011	RSA-OAEP 1024-1
100-111	Reserved

Author's note: Add a new section 10.4.2 as follows:

2.2.1 NTRUEncrypt verification information types

The following verification information types are defined for inclusion in the ACL information command in the NTRUEncrypt 251-1 security suite. Each of the following verification information types use the encoding for NTRUEncrypt 251-1, see Table 4.

2.2.1.1 NTRUEncrypt 251-1 key

If an ACL information command is transmitted with the verification information format field set to 'NTRUEncrypt 251-1 key' and the security suite field set to 'NTRUEncrypt 251-1', see {xref - clause with ACL information command in it}, the verification info field shall be the NTRUEncrypt public key associated with the corresponding DEV. This key shall be transmitted in the form indicated in {xref - 10.4.1.2}.

2.2.1.2 X.509 Certificate

If an ACL information command is transmitted with the verification information format field set to 'X.509 certificate' and the security suite field set to 'NTRUEncrypt 251-1', see {xref - clause with ACL information command in it}, the verification info field shall be an X.509 certificate as specified in RFC 3280 including an NTRUEncrypt public key associated with the corresponding DEV.

2.2.1.3 X.509 CA Certificate

If an ACL information command is transmitted with the verification information format field set to 'X.509 CA certificate' and the security suite field set to 'NTRUEncrypt 251-1', see {xref - clause with ACL information command in it}, the verification info field shall be an X.509 certificate as specified in RFC 3280 including the public key of a certificate authority that has signed the NTRUEncrypt public key associated with the corresponding DEV.

2.2.1.4 SHA-1 hash

If an ACL information command is transmitted with the verification information format field set to 'SHA-1 hash' and the security suite field set to 'NTRUEncrypt 251-1', see {xref - clause with ACL information command in it}, the verification info field shall be the result of a SHA-1 hash as specified in {xref 10.4.1.4}

of the concatenation of the 6-byte DEV address and the public key of the corresponding DEV formatted as specified in {xref 10.4.1.2}.

2.2.1.5 Certificate chain URL

If an ACL information command is transmitted with the verification information format field set to 'Certificate chain URL' and the security suite field set to 'NTRUEncrypt 251-1', see {xref - clause with ACL information command in it}, the verification info field shall be the URL of a certificate chain that leads to a certificate including the public key of the corresponding DEV formatted and encoded as specified in RFC 1738.

Author's note: Add the following reference to RFC 1738

IETF RFC 1738: Uniform Resource Locators (URL) Profile, December 1994.

Author's note: Add a new section 10.5.2 as follows:

2.2.2 RSA-OAEP verification information types

The following verification information types are defined for inclusion in the ACL information command in the RSA-OAEP 1024-1security suite. Each of the following verification information types use the encoding for RSA-OAEP 1024-1, see Table 4.

2.2.2.1 RSA-OAEP raw 1024-1 key

If an ACL information command is transmitted with the verification information format field set to 'RSA-OAEP raw 1024-1 key' and the security suite field set to 'RSA-OAEP 1024-1', see {xref - clause with ACL information command in it}, the verification info field shall be the RSA-OAEP public key associated with the corresponding DEV. This key shall be transmitted in the form indicated in {xref - 10.5.1.3}.

2.2.2.2 X.509 Certificate

If an ACL information command is transmitted with the verification information format field set to 'X.509 certificate' and the security suite field set to 'RSA-OAEP 1024-1', see {xref - clause with ACL information command in it}, the verification info field shall be an X.509 certificate as specified in RFC 3280 including an RSA public key associated with the corresponding DEV.

2.2.2.3 X.509 CA Certificate

If an ACL information command is transmitted with the verification information format field set to 'X.509 CA certificate' and the security suite field set to 'RSA-OAEP 1024-1', see {xref - clause with ACL information command in it}, the verification info field shall be an X.509 certificate as specified in RFC 3280 including the public key of a certificate authority that has signed the RSA public key associated with the corresponding DEV.

2.2.2.4 SHA-1 hash

If an ACL information command is transmitted with the verification information format field set to 'SHA-1 hash' and the security suite field set to 'RSA-OAEP 1024-1', see {xref - clause with ACL information command in it}, the verification info field shall be the result of a SHA-1 hash as specified in {xref 10.5.1.5} of the concatenation of the 6-byte DEV address and the public key of the corresponding DEV formatted as specified in {xref 10.5.1.3}.

2.2.2.5 Certificate chain URL

If an ACL information command is transmitted with the verification information format field set to 'Certificate chain URL' and the security suite field set to 'RSA-OAEP 1024-1', see {xref - clause with ACL information command in it}, the verification info field shall be the URL of a certificate chain that leads to a certificate including the public key of the corresponding DEV formatted and encoded as specified in RFC 1738.

Author's note: Add a similar sub-clause to the ECMQV security suite.

Ed. note: Ari will propose similar text for approval by Rene for the ECMQV suite.

Author's note: End text for comment 102.

196 - Accept in principle, "Resolve as indicated in CID 359."

320 - Update comment

> Accept in principle, "Change 8.13.1, page 206, line 44-45 to be: 'The PSPS bitmap in the beacon shall serve as indication to a DEV that its peer has gone into PSPS mode.', Add on page 206, line 54: 'The PNC is not required to align subrate allocations for a PSPS DEV with the system wake beacon.' In the MSC on page 207, Figure 130, change PSAVE to be PSPS in the MLME_PS_MODE_CHANGE.req. See also CID 359 for other changes."

170 MLME-MULTICAST-RX-SETUP.request is not referenced anywhere in clause 8. Should it affect reception filtering?/KO. Decide what it shall do and add it to clause 8. **Suggest accept in principle:** "This primitive is only used at the higher levels of the MAC and does not affect (other than in implementation dependnet ways) the operation of the MAC. Since it does not change the on-air behavior of a DEV, there is no need to mention it in clause 8. For example, MLME-RESET and MLME-SYNCH are not mentioned anywhere but in clause 6 since they only affects that interface."

> Accept in principle, "Add to 8.5.1.1 'DEVs perform multicast negotiations at a higher layer. IP multicast is one example. A DEV sets up a multicast stream at the request of the upper layer by sending a request to the PNC for a stream with the multicast ID as the destination. A DEV enables reception of a multicast stream by using the MLME-MULTICAST-RX-SETUP.request. This tells the MAC to receive frames from a particular DEV with the DestD set to McstID and with the stream index specified in the MLME.' Add to 8.4.4.2, page 171, line 47: 'If the DestID of the CTA is the McstID or BcstID, the source DEV may still send directed frames to any associated DEV.'"

22 - Editorial note: Change 'Flush bit' to be 'Destination ID list bit'

92 - ACCEPT IN PRINCIPLE. Suggest a table that has security levels (i.e. claimed bits) and if the OID offers cryptographic authenticiation of public keys for each of the OIDs. Merge Mode 1 and Mode 2 services offered, pointing out that some OIDs use certificates, some don't. Throughout the draft, use only mode 0 or mode 1 or security off or security on. Change the SEC mode field in the beacon to be only one bit.

138 -

Accept in principle, add the following entries to Table 9.

142 - Add as above

156 - Add a definition for priority as given in Table 6.

Table 5—MLME-ASSOCIATE primitive parameters

Name	Type	Valid Range	Description
New entries below			
MaxAssociations	Integer	0-255	The maximum number of DEVs that the PNC is able to handle as a PNC.
MaxCTRBs	Integer	0-255	The maximum number of isochronous CTRBs that the DEV is able to handle as a PNC.
TxPowerLevel	Integer	PHY dependent	The maximum transmitter power for the DEV, contained in PHYPIB_TxMaxPower. This is PHY dependent and is defined in {xref 11.7.1} for the 2.4 GHz PHY
PiconetServicesInquiry	Enumeration	REQUEST, NO_REQUEST	Indicates if the DEV is requesting that the PNC send the piconet services, information command, {xref 7.5.x}.

Table 6—MLME-CREATE-STREAM, ... primitive parameters

Name	Type	Valid Range	Description
New entries below			
Priority	Integer	0-7	As defined in A.1.2.1

119 (Gilb, TR) - The symmetric cryptography operations specified in Table 89 do not describe fully what data is to be authenticated. The input to the HMAC operation is not fully specified, so interoperability cannot be achieved. Completely specify the data (and the order of the data) that is to be authenticated in the HMAC operation. This should include information from previous frames of the authentication protocol, such as the OID and the identities of each participant. Diagrams should be added to this sub-clause and the NTRU and RSA subclauses showing the data input to the symmetric key operations for the challenge response and authentication response.

> Accept in principle: “Add to the end of each of the descriptions in Table 89, ‘, as defined in 10.3.1.3.’ Proposed diagrams for authentication in the NTRU and RSA suites will be provided by Ari Singer.”

92 - Additional text:

(begin new additional text for CID 92)

The frame requirements field indicates additional security policies imposed by the security manager. This field shall be formatted as specified in Table 7.

Table 7—Security requirements field

b7-b2	b1	b0
Reserved	128-bit security required	Certificates required

If the certificates required bit is set to 1, the security manager shall only authenticate DEVs with a security suite that uses certificates, {xref 10.2.1}, while it operates as the security manager.

If the 128-bit security required bit is set to 1, the security manager shall only authenticate DEVs with a security suite that is stated to provide 128-bit security in {xref Annex B.x} while it operates as the security manager.

(end additional text for CID 92)

Accept additional resolution.

CID 5 - New resolution, “Change ‘An associated device that has not yet authenticated to the ... to the value in the beacon and send a key request command to the PNC to obtain the new key.’ to be

‘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, {xref 9.8.5}, and verfied the integrity code on a beacon, it shall set the LastValidTimeToken to be the time token in that beacon.

Once a DEV has received the piconet group data key, it shall use the beacon to help maintain the current time token and the current piconet group data key. When the DEV receives a secure beacon (a beacon with the SEC field in the frame control field set to 1), it shall verify that the time token in the beacon is greater than the LastValidTimeToken, that the SECID matches the stored broadcast SECID and the integrity code passes. If all of these checks succeed, accept the time token in the beacon as the LastValidTimeToken. If the time token in the beacon is greater than the LastValidTimeToken, but the SECID does not match the stored broadcast SECID, the device 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.’

{Sec. Ed. note: Change beacon number to time token for security related uses}

Delete ‘stored in the MACPIB_CurrentBeaconNumber in the MAC PIB’ from line 16 on page 221.

On page 220, line 41, Change ‘greater than the CurrentBeaconNumber and less than the CurrentBeaconNumber + aMaxBeaconChange.’ to "greater than the LastValidTimeToken and less than the LastValidTimeToken + aMaxTimeTokenChange.’, Change ‘aMaxBeaconChange’ to be ‘aMaxTimeTokenChange’ in clause 8.”

CID 481 (Gubbi, TR) Text to finish the changes. Change ‘There are two IFSs that are defined; the short inter-frame space (SIFS) and the retransmission inter-frame space (RIFS). The relation between the IFSs is that RIFS = 2*SIFS+ACKTime. The ACKtime is the time duration of the ACK frame, either Dly-ACK or Imm-ACK, at the appropriate data rate. The actual values of the SIFS is PHY dependent. For the 2.4 GHz PHY it is listed in 11.2.7.1.’ to ‘There are four IFSs that are defined; the minimum inter-frame space

(MIFS), the short inter-frame space (SIFS), the backoff inter-frame space (BIFS) and the retransmission inter-frame space (RIFS). The actual values of the MIFS, SIFS, BIFS and RIFS are PHY dependent. For the 2.4 GHz PHY it is listed in 11.2.7.1.'

Change 'Similarly a SIFS duration shall be allowed between a frame that does not expect an immediate response and the next successive frame transmitted over the medium.' to be 'A MIFS duration shall be allowed in the CTA between between a frame with no-ACK policy or Dly-ACK policy and Dly-ACK request bit not set and the next successive frame transmitted over the medium.'

In 11.2.7.1, define these as follows,

Table 8—Interframe spacing parameters

802.15.3 MAC parameter	Corresponding PHY parameter	Definition
MIFS	aPHYMIFSTime	11.2.7.2
SIFS	aPHYSIFSTime	11.2.7.2
aBackoffSlot	aCCADetectTime	11.6.5
BIFS	aPHYSIFSTime + aCCADetectTime	11.2.7.2 + 11.6.5
RIFS	2*aPHYSIFSTime + aCCADetectTime	11.2.7.2 + 11.6.5

Add new subclause, 11.2.7.4 between the current 11.2.7.3 and 11.2.7.4

(begin new 11.2.7.x subclause text)

2.2.2.6 Time between successive transmissions

The time, aPHYMIFSTime, shall be 2 μs, including the power-up ramp specified in 11.5.7.

The aPHYMIFSTime shall be measured at the air interface from the trailing edge of the last symbol transmitted until the first symbol of the PHY preamble is present at the air interface.

(end new 11.2.7.x subclause text)

2.3 Wednesday, 9 October, 2002

2.3.1 MTS

CIDs 56, 349, 350, 351, 352, 353, 354, 355, 407, 513

Suggested resolution: Make MTS PHY dependent.

"Add new subclause 11.2.10, 'Channel access methods' with text 'A PNC-capable DEV compliant to this standard shall allow the use of the CAP for contention based access for association, data and commands, {xref 7.3.1} when using the 2.4 GHz PHY. A DEV compliant to this standard shall support the use of the CAP when using the 2.4 GHz PHY.'

Use 1 bit from the reserved bits to the 'Piconet mode field', 'MCTAs used' with definitions 'The MCTAs used bit shall be set to 1 if the PNC will be using open or association MCTAs.' Delete the sentence on page

111, lines 1-2, ‘If the CAP end time indicates no available time and no message types are permitted during the CAP, then MTSs are implied.’ (note this deletion is in response to CID 407).

Expand MLF13 in the PICs (note this will become MLF13.1 and MLF13.2 due to another comment.)

MLF13.1; Open and association MCTA operations; 8.4.4.4, 8.4.4.5; O.1

MLF13.2; Regular MCTA operations; 8.4.4.4; M

{ed. note: the CAP stuff is like MLF13.3 now}”

Accept in principle for Gilb - 56, Schrader - 349, 350, 351, 352, 353, 354, 355, Gubbi (not present) - 387, 407, 513

2.3.2 Power management

CIDs Heberling - 321, 324, 339, Roberts - 343, Schrader - 358, 360, 361, Shvodian - 363, 364

Key issue: Is one SPS set for battery powered PNC capable DEVs and 4 SPS sets for other PNC capable DEVs mandatory or optional? (321, 324, 339, 343, 364)

3 suggest merging SPS and PSPS to the extent possible 358, 360, 361.

Points of discussion:

Ability of DEV to count on power savings from PNC
Complexity of implementation.
Sub-rate allocations?

Potential compromise positions?

O.1 for both (or all three?)
PHY dependent
O for all.
Leave it as is.

Merge for frame functionality?

Merge SPS/PSPS status IE into by using set 1 as PSPS, merge SPS configuration request into PS mode request.

3. Conference calls

3.1 Thursday, 3 October 2002

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

3.1.1 Power management

(begin HIBERNATE text, ref CID 508)

MkS note: I suggest that the text describing HIBERNATE mode be inserted between the section describing SPS mode, 8.13.2, and the section describing the creation and use of SPS sets, 8.13.2.1. This is located on page 208, line 8. The text follows:

HIBERNATE mode allows a DEV to conserve power for extended periods until it chooses to listen for a beacon. The only responsibility of a DEV in Hibernation mode is to communicate with the PNC before the end of its ATP interval in order to preserve its membership in the piconet (see {xref} section 8.3.4).

MkS note: This text should be inserted at the end of 8.13, on page 214, line 33. The text follows:

If the DEV wants to change its mode from ACTIVE to HIBERNATE, the DEV shall send the PS change command, {xref} 7.5.7.1, to the PNC with the power save mode field set to HIBERNATE. The PNC shall then set the bit for the DEV in the SPS IE that corresponds to a virtual SPS set 0 (0 means HIBERNATE mode).

The DEV may be the source or destination of one or more streams. The PNC shall terminate all streams for which the DEV is either the source or the destination, {xref} 8.5.1.3, when the DEV changes to HIBERNATE mode.

If the DEV wants to change its power save mode from HIBERNATE to ACTIVE, the DEV shall send the PS change command, {xref} 7.5.7.1, to the PNC with the power save mode field set to ACTIVE. The PNC shall then no longer set the bit for that DEV in the SPS IE 0.

MkS note: In addition we need to add the HIBERNATE parameter anywhere where SPS and PSPS are now listed in section 6:

Page 78, Table 23, line 6, column 3: Change ‘ACTIVE, SPS, PSPS’ to ‘ACTIVE, SPS, PSPS, HIBERNATE’

Page 81, line 24, and line 38, Change the following in two places: Change ‘...from SPS or PSPS to ACTIVE.’ to ‘...from SPS, PSPS, or HIBERNATE to ACTIVE.’

Page 85, Table 29, line 19, column 3: Add the text: 0x03=HIBERNATE

Page 85, Table 29, line 24, column 3: Add the text: 0x03=HIBERNATE

MkS note: In addition we need to add the HIBERNATE parameter anywhere where SPS and PSPS are now listed in section 7.

Page 147, Line 48: Increase the width of the power save mode field to three bits, and decrease the width of the reserved field to 5 bits.

7.5.7.1 PS Change Command, Page 148, Line 7: Add the following text: -- 4 for HIBERNATE mode

MkS note: Make changes to the PS change MSC's, Page 211, Figure 134 and Figure 135:

Change "SPS" to "SPS, PSPS and HIBERNATE" for all instances.

(end HIBERNATE text)

356 (Schrader, TR) 8.13.2.2, pg 209,210 - In removing implicit stream resumption when changing from SPS to ACTIVE mode, too much inefficiency was introduced for DEVs that need to restart ACTIVE mode streams quickly. - Still in the spirit of our compromise: Allow the mode change command along with one or more CTRs to occur anywhere that multiple CTRs are currently allowed. Require that the mode change command be the first command in the sequence. The result: switching to ACTIVE mode and starting an ACTIVE stream becomes efficient. **Suggest accept in principle:** "Change subclause 8.13.2.2, page 210, Lines 25-28 as indicated in 02/393r11."

(begin text for CID 356 ~~deleted text in strikethroug~~h, added text underline)

The PNC may grant~~s~~ an ACTIVE mode DEV's channel time request~~, i.e. one~~ with CTR type set to ACTIVE, and with an SPS mode DEV as the DestID. ~~The PNC shall send a CTA status command, 7.5.5.3, to that DEV in one of its wake beacons to inform it that an allocation has been granted that is not aligned with its wake beacons.~~ In the SPS DEV's next awake superframe, the PNC shall put the SPS DEV's PCTM bit in the beacon IE, and provide a GTS slot with SPS DEV as source and the PNC as destination. The SPS DEV shall use this slot to send a PS change command.

If the SPS DEV sends the PS change command with the Power save mode set to ACTIVE, then it may append up to two channel time request commands for the creation of ACTIVE isochronous or asynchronous GTS slots along with the PS change command. On receipt of the PS change command, the PNC shall begin inserting the CTAs for the granted channel time into the first beacon after the SPS DEV's awake beacon.

If the SPS DEV sends a PS change command with the Power save mode set to SPS (or PSPS) then the PNC shall terminate the granted stream without generating any CTAs.

(end text for CID 356)

> Accept in principle, apply edits as above with new added text instead of "In the SPS DEV's next ..." as "In the SPS DEV's next wake superframe, the PNC shall provide an MCTA that is long enough to handle a PS change command and a channel time request command with 4 isochronous CTRBs. The SPS DEV shall use this CTA to send a PS change command.
>
> The SPS DEV may send a channel time request command following the PS change command. On receipt of the PS change command, the PNC shall begin inserting the CTAs for the granted channel time into the first beacon after the SPS DEV's next wake beacon."

535 (Bain, T) 7.5.7.2, pg 148, ln 25 - there is a mismatch on text and references in this grouping of commands with regard to next awake beacon. line 24 mentions that figure 49 has something to do with next awake beacon and it doesn't. Other sections in 7.5.7 xref back to 7.5.7.2 to get the definition of next awake beacon. There is none there. - Update text to correct. **Suggest accept**.

> Accept in principle, "Resolve as indicated in CID 16."

543 (Bain, TR) – 8.13.2, pg 209, ln 47 - With d11 is the change to establishing a CTR as SPS DEVs toggle between SPS mode and ACTIVE mode rather than predefining CTRs. Missing is text to provide for an "asynchronous" CTR to provide the functionality of the intermittent (persistence bit) operation. – Please add

text as requested. **Suggest accept in principle:** “Insert at end of 8.13.2.3 ‘An SPS mode DEV may have an SPS asynchronous channel time request assigned to it by a sending DEV. An SPS asynchronous CTR command has the CTR type set to SPS.’ {Ed. note: In addition, a scrub of clauses 6, and 7 is required to fix any prohibition of SPS mode.}”

> Accept in principle, “This functionality is provided by the channel time request command, the PNC allocates channel time only when the sleeping DEVs are scheduled to be listening to the beacon. This is document in D11, page 187, lines 13-19.”

427 (Gubbi, TR) 7.4.8, pg 124, ln 50 - Inclusion of BcstID and McstID in this sentence - When a CTA for BC/MC dest address is being allocated, these bits shall be set - revert back to the sentences in D10 (pp124, ln 41:45) **Suggest Reject:** There is no need for multicast or broadcast. This IE is dealing with individual devices that need to monitor an additional superframe for traffic.

or

Suggest accept in principle: “The use of the PCTM IE has changed from D10 to D11 although the name remained the same. It is now used to indicate to SPS DEVs that they will have a CTA in the following beacon (or that they will be given another PCTM IE that tells them it will be in the next one, up to 3 times). However it could be useful to SPS DEVs to indicate that there will be BC or MC allocations in the next superframe. Then it is up to the SPS DEVs if they want to remain awake for the next beacon (or beacons). Delete ‘BcstID and McstID from line 50. Add a new sentence prior to that paragraph that says ‘If the BcstID or McstID bit is set, then the PNC is indicating that there will be a CTA with the BcstID or McstID as the destination in the next superframe.’ {Ed. note: is this too much effort for the PNC? Should it be a should?}”

> Reject, “The use of the PCTM IE has changed from D10 to D11 although the name remained the same. It is now used to indicate to SPS DEVs that they will have a CTA in the following beacon (or that they will be given another PCTM IE that tells them it will be in the next one, up to 3 times). For DEVs that want to listen to BC/MC traffic, they need to listen to the system wake beacon where that traffic will be sent.”

511 (Gubbi, TR) 8.13.2.2, pg 210, ln 27-28 – Command in beacon? - Change it to mean superframe instead of beacon. **Suggest accept in principle:** This paragraph may change with another comment. The resulting new paragraph requires use of “superframe” when talking about a GTS within the superframe rather than the beacon.

> Accept in principle, “The sentence that said this was deleted in the resolution of CID 356.”

3.1.2 Others

27 (Gilb, TR) - There is no discussion of what is meant by static or dynamic. Either add a defintion, i.e. "Static means that the parameter is an unchangeable characteristic of the DEV while dynamic means that it is possible for the parameter to change while the DEV is operating." or simply delete the column. **Suggest accept in principle:** “Add text to 6.5 that says ‘In the type column of the tables, static indicates that the parameter is normally an unchangeable characteristic of the DEV while dynamic indicates that it is possible for the parameter to change while the DEV is operating.’”

> Accept

147 (Heberling, T) 6.3.3.2.2 pg 34 line 9 - Change these sentence fragments 1) <from> "If another piconet is already established,..." <to> "If the piconet is already established,..."2) <from> If all of the channels for the PHY are either occupied by other 802.15.3 piconets or have unacceptable interference, ..." <to> "If all the channels for the PHY are occupied by other 802.15.3 piconets, ..." <and to> " If all the channels have unacceptable interference, then the ResultCode shall be set to "CHANNEL-NOISY". **suggest accept in princi-**

ple - “Delete all but the result code for the start.cfm, and that there is too much text here for clause 6, Change the effect of reciept as indicated below (see 02/392r12 for formatting).”

‘The DME is notified of the results of the piconet creation procedure. A ResultCode of SUCCESS indicates that the DEV is the PNC. ~~If another piconet is already established, the ResultCode shall be ALREADY_STARTED.~~ If the requested channel for starting the piconet is occupied by another 802.15.3 piconet, ~~If all of the channels for the PHY are either occupied by other 802.15.3 piconets or have unacceptable interference,~~ then the ResultCode shall be set to PICONET_DETECTED. ~~The PNC DME then has the option of either ending another MLME-START.request to its MLME with a different ChannelIndex to start a piconet in a different channel or to send an MLME-ASSOCIATE.request to its MLME to initiate an association as either a regular DEV, child or neighbor piconet of the PNC.~~ If the piconet is already started the ResultCode shall be set to ALREADY_STARTED. If the requested channel for starting the piconet has unacceptable interference, then the ResultCode shall be set to "CHANNEL-INTERFERENCE. If any of the parameters are in error the ResultCode shall be INVALID_PARAMETERS.’

Change table 6, pg 32, to add the CHANNEL-INTERFERENCE and ALREADY_STARTED enumerations to the ResultCode parameter.

In clause 8.2.2 pg. 155, line 15, add the following text - ‘The DME then has options that include sending another MLME-START.request with a different ChannelIndex to start a piconet in a different channel, associate as a regular DEV, or a dependent piconet.’”

Accept in principle.

536 (Bain, TR) - Since the text on line 8 says that DEVs can ignore any elements in the beacon payload that are not in table 39, it seems that the table needs to be corrected.A better choice may be to move the content to table 47 (information elements) with an additional column to indicate use (beacon, command, both). change table 47 as suggested. Delete table 39change text between lines 5 and 9 to remove table 39, add table 47 content and remove the text that says that IEs may be ignored. **Suggest accept in principle:** “Add a column ‘Present in beacon’ to table 47 for all of the IEs. For IEs that are not supposed to be in the beacon, put ‘Non-beacon IE’ in the column. For IEs that may be in the beacon, put ‘Beacon IE’ and for ‘CTA request IE’ put in ‘Shall not be in beacon’, Add text prior to table 47 that says ‘If the ‘present in beacon’ column has the entry ‘Non-beacon IE’, the PNC may put the IE in the beacon and DEVs in the piconet may ignore the contents of this IE when it is sent in the beacon. {Ed. note: Consider moving text from page 110, line 8-9 to this location if it seems to flow better.} Delete table 39 and change the cross reference to indicate the new table. Also move the probe tables to the probe command in clause 7.”

Accept suggested resolution.

481 (Gubbi, TR) - Relationship between RIFS and SIFS:Strongly NO to changes in D11. RIFS is deviced such that in a GTS if theGTS owner does not waste a lot of time in waiting for the response thatdoes not arrive. If the Sender of a data frame (say) did not see PHYenergy in one slot after SIFS, it should be allowed to assume that theresponse is not going to come and hence start retransmissions.An entire ACK time is way too much waste of time. Remove the changes from D10 to D11. **Suggest reject:** “The commenter incorrectly states that RIFS is only used in a GTS. Clause 8.4.3 states that RIFS is used for backoff.”

Accept in principle, “Make RIFS PHY dependent and define it in clause 11.2.7.1 table 108 using the D10 definition of a RIFS = BIFS = SIFS + aBackoffSlot.”

3.1.3 PM stream termination

Note: In the discussion Tuesday, we agreed that the PNC should terminate super-rate streams with the PM DEV as the destination when it switched from ACTIVE to a PM mode.

262 (Heberling, TR) - [CTM/CTR] PSPS mode DEVs don't get their streams terminated when they go topowersave, since they still follow their GTSs. If they want a stream terminated they have to ask for it./KO Change reason code from: '6->Stream terminated, DEV entered power save mode"to:"6->Stream terminated, DEV entered SPS mode' **Suggest accept in principle:** "Insert the following text in section 8.13.2.2 Changing power save mode and operation, page 210, line 4: 'The DEV may be the source or destination of one or more streams. The PNC shall terminate all super-rate streams for which the DEV is the destination, {xref 8.5.1.3}, when the DEV changes to SPS mode. The PNC shall terminate all streams for which the DEV is the source or destination when the DEV changes to HIBERNATE mode. Modify the following text in section 8.13.1 PSPS Mode, page 206, line 42-43: Current D11 Text: 'When the PNC receives this command, it sets the PSPS status bitmap appropriately, 7.4.14.' Modified Text: When the PNC receives this command, it shall terminate all super-rate streams for which the DEV is the destination, {xref 8.5.1.3,} and set the PSPS status bitmap appropriately, {xref 7.4.14}.'"

Accept suggested resolution.

450 (Gubbi, TR) 7.5.5.2, pg 144, ln 2 - Reason code 6 has become unreasonable. Why should a stream be terminated just because DEV is in PS mode? - Remove the inserted text "Stream terminated," **Suggest accept in principle:** "Certain streams are terminatedwhen a DEV switches from ACTIVE to a power management mode. This is described in the resolution of CID 262. Resolve as indicated in CID 262."

Accept suggested resolution.

65 (Gilb, TR) - Shouldn't the PNC terminate all streams with the CTR interval type set to 1?What about switching a DEV to ACTIVE mode? Are there any restrictions on the stream allocations? Need to mention here that the PNC will not necessarily align subrate allocations to the system wake beacon. Add to PSPS that the PNC terminates all streams with CTR interval type set to 1 when the DEV enters PSPS mode.Add text similar to SPS that says if the DEV gets an ACTIVE mode allocation, it shall be considered to be in ACTIVE mode. Also add the note that the PNC will not necessarily align a subrate allocation to the system wake beacon. **Suggest accept in principle:** "Resolve as indicated in CID 262."

Accept suggested resolution.

3.1.4 Security

105 (Gilb, TR) [SEC] The probe command will not function as specified in this sub-clause, as the recipient device will assume that the public-key information being sent belongs to the old PNC, not the new PNC. Change this paragraph to reference a new command that may be sent to pass ACL information to other DEVs. **Suggest accept in principle.** "Reference the new command included in the resolution to 102. Change the last paragraph of 9.2.4 to the following:

> 'The old PNC may send ACL information about the new PNC to the other DEVs in the piconet and send ACL information about all of the authenticated DEVs in the piconet to the new PNC when it hands over the role of the PNC. This is accomplished by sending a directed ACL information command, {xref new command} to the new PNC with the ACL information of all of the authenticated DEVs in it and by sending a broadcast ACL information command or a directed ACL information command to each authenticated DEV with the ACL information of the new PNC. If the DME of each DEV chooses to accept this ACL information, the authentication process between the new PNC and each authenticated DEV may proceed without any interruption of service.'"

Accept suggested resolution.

111(Gilb, TR) [SEC] Table 57: It needs to be indicated either here or in clause 7 that the probe command, piconet services command and disassociate command may be sent insecurely before authentication has taken place. Add text that indicates that the probe command, piconet services command and disassociate

command may be sent insecurely before authentication has taken place. **Suggest accept in principle.** See proposed resolution to 101.

Table pending resolution of CID 101.

112 (Gilb, TR) [SEC] There needs to be a clear delineation between the aspects of the certificate usage that are within scope and those that are out of scope. If we are specifying the exact format of the entity certificate, it seems that the format of the CA key and the other information should be specified as well. It should be made clear what checks, if any, are performed by the MLME and what checks should be pushed up to the higher layer. **Suggest accept in principle.** Resolve as proposed in 93. As in the proposed resolution to 93, the manner in which the public key is accepted for the authentication protocol is out of scope. It is appropriate to clearly define the manner in which the certificate itself can be verified, so the definition of how to create and verify the certificate should not be removed. Instead, make changes indicated in 93 to state that devices should (instead of shall) verify the authenticity of the public key by performing the certificate checking operations. The resolution to 102 provides the ability for each security suite to define ACL entries, which may include CA certificates, which include CA keys.

Table pending resolution of CID 93.

116 (Gilb, TR) [SEC] Figure 168: This figure does not reflect the current version of secure beacons. This figure should be updated to match the secure beacon frame format specified in 7.3.1.2. Better still, replace this with a cross reference to the correct figure. **Suggest accept in principle.** Replace figure 168 with the figure in 02/392r12. {Ed. note: verify length of piconet synchronization parameters}. Also change Enc Data Length and Auth Data Length fields in the other figures to match this format."

Octets: 2	**2**
Enc Data Length *l(m)* = 0	Auth Data Length *l(a)* = $27+L_1+...+L_{n-1}$

L_{n-1}	...	L_1	**13**	**2**	**2**	**10**
Information element-(n-1)	...	Information element-1	Piconet synch. parameters	Secure frame counter	SECID	Frame header

Figure 15—CCM input for secure beacons

Accept suggested resolution.

124 (Gilb, TR) [SEC] It seems that the types of security support that are listed here are limited only to the methods that are explicitly defined in the standard. There may be additional methods that should be allowed and there should be a means for vendors to indicate that there are vendor specific methods implemented. For instance, certificates that are not in the format specified here, such as X.509 certificates used in browsers, may be useful to use to provide evidence of the validity of a public key while in mode 1 or mode 2. Change the ECC and RSA X.509 certificates to be simply an X.509 certificate. The certificate indicates the method used for authentication. **Suggest accept in principle.** Add PICS entries for supporting various kinds of ACL information in the ACL information command.

Send suggestion of added PICS to email.

362 (Schrader, T) [SEC] The way that states are numbered and and state transitions can lead to confusion and difficulty understanding the transitions. Label states 1.0, 2.0, 3.0, ... N.0 and label state transitions as n.m to indicate a transition from state n.0 to state m.0. This impacts a lot of diagrams and text, but it would be a major improvement. Use "x" as the "any" state indicator. **Suggest accept.**

Accept.

370 (Shvodian, TR) [SEC] Why can't a mode 0 PNC use the ACL? I thought this is how we got rid of mode 1. Maybe this is just an oversight. Change to "A device operating in mode 0 shall not perform any security related operations on MAC frames." **Suggest accept in principle. "**Change text in 9.3.1 to the following:

'A device operating in security mode 0 shall not perform any cryptographic operations on MAC frames. While in this mode, if the MAC receives a frame with the SEC field set to 1, the MAC shall discard the frame and the MLME shall return an MLME-SECURITY-ERROR.indication to the higher layer with the ReasonCode set to UNAVAILABLE-KEY.'"

Accept suggested resolution.

431 (Gubbi, TR) [SEC] Text in ln 19:22 and Figure-41 are utterly confusing. Is this trying to tell that Public-key objects larger than 254 octets can be fragmented and can be sent in multiple IEs that have appropriate indices? In any case, state clearly. Change the text in ln 19:22 and figure 41 to following:Text:If the public-key object is larger than 254 octets, it can be fragementedwith fragment size of 254 and sent in atmost 4 IEs. The fragmentation isonly due to the reason that IEs do not accommodate more than 254 octets.For this purpose there are four public-key object IE indices defined for this in Table-47. They are - Public-key object carrying first fragment or the entire public key object if it is less than 255 octets long - Public-key object-1 carrying second fragment, if present - Public-key object-2 carrying third fragment, if present - Public-key object-3 carrying fourth fragment, if presentWhen fragmentation is performed, the corresponding IEs shall be placedtogether in the frame carrying them and they shall appear in the order ofthe fragment they are carrying with fragment-0 appearing first.Figure: four different boxes, one for each IE, with their payload joining to form overall Public-key-object **Suggest accept in principle.** See resolution proposed in 02/399r2. It seems that perhaps it would be more flexible to simply have one public-key object IE and simply have two indication bytes at the beginning. The first indication byte would say the number in the sequence. So the first public key object IE of the extended group would have a value of 1 for that byte and the 3rd would have a value of 3. The second indication byte would be a TRUE or FALSE byte where 1 indicates that it is the last IE for this public-key object and 0 indicates that it is not the last. This simplifies the IEs and also allows for longer public-key objects if they are ever needed.

Accept in principle "Change the public key object-n IEs to a single IE, add two octets at the beginning of the IE, the first octet is the 'number of fragments,; the second octet is the 'sequence number' with definitions: 'The number of fragments indicates the number of IEs into which the public key object is split.', 'The sequence number indicates the fragment of the public key that is contained in this IE."

Meeting adjourned at 10:38 am PDT.

63 (Gilb, TR) [SEC] We still don't have a good description of what to do with commands sent or received with security on. Also need to generalize for the case of peer-to-peer security. Add description including peer-to-peer security. **Suggest accept in principle. (Note that this introduces functionality to maintain separate modes for different DEVs)** Add the following text to the beginning of 9.2.11:

"DEVs shall maintain a security state denoting whether security is required for each security relationship. If security is required for a particular security relationship, all frames transmitted to and received from another DEV in that relationship shall be protected by the keys indicated in {xref - Table 57}. A DEV may send or receive certain command frames without protection as indicated in {xref - Table 48}. If a DEV receives a frame that is not protected as required, the DEV shall discard the frame. If security is not required for a security relationship, all frames transmitted to and received from another DEV in that relationship shall be sent without security. If a DEV receives a protected frame when security is not required, the DEV shall discard the frame.

If the DEV is participating in a secure piconet, the security state for the relationship with the PNC, and consequently the broadcast key, shall be set to security required. For peer-to-peer communications, the DEV may choose to require security or not for that relationship, regardless of the security state shared with the PNC. If security is required in a peer-to-peer relationship, but the DEVs have not authenticated with each other, the group data key shall be used to protect frames between the DEVs."

> Table, How do the peer DEVs know what security state they are supposed to be in if they have not mutually authenticated. Data protection as a separate capability? Take the discussion to the email list.

93 (Gilb, TR) [SEC/PIB] The security suite and public-key verification information have been removed from the MAC PIB. This implies that there is no accessible information that the MLME can use to perform verification on the public key. In particular, the CA certificate or hash of the public key are not available. In clause 10, each security sub-suite specifies that the ACL indicates which public-keys shall be accepted and which shall be rejected. Add public-key verification information back into the ACL and specify in each security suite how that ACL information is to be used. If there are operations to be performed by the DME to verify the public key, those should be mentioned in the security suites as well. This applies to 6.5.6 as well. **Suggest accept in principle.** The public key verification operations are performed by the DME and are hence outside the scope of the standard. Rather than adding this information to the PIB, the description of the security suites in clause 10 should be modified to reflect that this is out of scope. Make the following changes to clause 10:

In clause 10.3.1.4.3, change the paragraph in lines 18-19 to: "The certificate shall be generated using the digital signature algorithm ECDSA as specified in 10.3.1.4.4. The validation of the certificate is outside the scope of this standard."

In 10.3.2.2.2, remove step 2) and the final sentence and add the following text:

"Processing shall be aborted if the public key is not successfully extracted.

The DEV should perform additional checks such as comparing the DEV address in the ManCert to the DEV address in the authentication request or comparing the received key and ID to values stored in its ACL to verify the authenticity of the public key."

In 10.3.2.3.2, remove step 2) and the final sentence and add the following text:

"Processing shall be aborted if the public key is not successfully extracted.

The DEV should perform additional checks such as comparing the DEV address authenticated in the ImplCert with the DEV address stored in its ACL to verify that the device is authorized."

In 10.3.2.4.2, remove step 2) and the following paragraphs and add the following text:

"Processing shall be aborted if the public key is not successfully extracted.

The DEV should perform additional checks such as signature verification as specified in 10.3.1.4.3, CRL checking, validity period verification, key use checking and comparing the DEV address in the X.509 certificate with the DEV address stored in its ACL to verify that the device is authorized."

In 10.4.2.2, change the table entry for Verification of Public-Key to the following text:

"The ID and public-key received during the authentication protocol should be verified by the DME using checks such as generating the SHA-1 hash of the device address concatenated with the public-key and comparing that to the hash of the ID and public key stored in the ACL."

In 10.5.2.2, change the table entry for Verification of Public-Key to the following text:

"The ID and public-key received during the authentication protocol should be verified by the DME using checks such as generating the SHA-1 hash of the device address concatenated with the public-key and comparing that to the hash of the ID and public key stored in the ACL."

In 10.5.3.2, change the table entry for Verification of Public-Key to the following text:

"The X.509 certificate received in the authentication protocol should be verified by performing checks such as signature verification as specified in 10.5.1.7, CRL checking, validity period verification, key use checking and comparing the DEV address in the X.509 certificate with the DEV address stored in its ACL to verify that the device is authorized."

Table until it can be reviewed with Rene.

3.2 Tuesday, 1 October 2002 - Security issues

Roll call: John Barr, Gregg Rasor, Ari Singer, Dan Bailey, James Gilb, Bill Shvodian

Meeting called to order at 12:05 pm PDT.

Agenda

- Roll call
- Unresolved CIDs, 100, 431, 101, 362, 54, 63, 105, 111, 370, 112, 116, 124, 93, 384.
- Suggestions to re-open resolutions of 92 and 98.
- Adjourn

384 (Barr, TR) [SEC/PIB] MAC PIB ACL group defined as an array whose contents are defined in Table 33. All of the entries are dynamic, but no clear mechanism to update these entries has been included in the draft. There are no limits on the minimum and maximum number of entries allowed in the ACL. The only use for this array in the MAC is for generation of the CCM nonce and obtaining the keys associated with a particular SECID for encoding or decoding payloads. Either remove the MAC PIB ACL or add appropriate method for updating the information in the array. If the ACL is kept, add limit for the minimum number of ACLs that must be supported for a DEV, SM, and PNC. Provide a mechanism for updating and accessing the contents of an ACL entry. Suggest defining MLME commands for doing this using an index to the array. Add MAC PIB entries to indicate last index used in the array. Finally, clarify relationship between DEVHost and MAC regarding use and management of informaiton in the ACL. **Suggest accept in principle.** "Add new MLME as indicated in 02392r11. Remove sub-clause 6.5.6 on page 87, lines 8-31. Add MLME-SECID-UPDATE.req on DEV and PNC sides to end of figure 147 on page 241."

(begin new text for CID 384)

3.2.1 Initializing and Updating SECID Information

This primitive is used to initialize or update the security information associated with a new SECID as the result of an authentication or key change process. The parameters used for the MLME-SECID-UPDATE primitive are defined in Table 9.

Table 9—MLME-SECID-UPDATE primitive parameters

Name	Type	Valid range	Description
SECID	Integer	Any valid SECID as defined in {xref 7.2.8.1}	Specifies the security session ID for the key.
KeyType	Enumeration	MANAGMENT, DATA	Specifies the type of key that is being updated, {xref 10}.
TrgtID	Integer	Any valid DEVID as defined in {xref 7.2.3}.	The DEVID of the target DEV for this relationship.
SecurityManager	Boolean	True/False	This DEV is the security manager for this relationship.
KeyInfoLength	Integer	0-255	Length of KeyInfo
KeyInfo	Dynamic	Any valid symmetric key as defined by the security suite, {xref 10}.	The key agreed upon during authentication or key update process that are used for protecting frames between this DEV and the TrgtID DEV.

3.2.1.1 SECID-UPDATE.request

This primitive requests that the SECID and keying information associated with the DEV be included or updated. The semantics of the primitive are as follows:

```
MLME-SECID-UPDATE.request    (
                             SECID,
                             KeyType,
                             TrgtID,
                             SecurityManager,
                             KeyInfoLength
                             KeyInfo
                             )
```

The primitive parameters are defined in Table 1.

3.2.1.1.1 When generated

The DME sends this request to the MLME after completing authentication or key update process with the PNC or a DEV.

3.2.1.1.2 Effect of receipt

The MLME adds this SECID to the list of authenticated SECIDs that can be used to protect frames with the target DEV in this authentication relationship.

(end new text for CID 384)

Accept suggested resolution.

3.2.2 Following provided by Ari Singer, Ntru.

54 (Gilb, TR) [SEC] We should specify that commands that fail IC check should be ignored. Sometimes they aren't (e.g. beacons). Add text as indicated. **Suggest accept in principle.** "Add the following text to the end of 9.1.7: 'All secure data frames that fail integrity checks are discarded.' Add the following text to the end of 9.1.8: 'Under normal operations, the integrity check on the beacon provides evidence that the piconet is operating properly and that no security changes have occurred. If the integrity check on the beacon fails, the DEV is alerted to the fact that the DEV does not have its security state synchronized with the PNC.' Add the following text to the end of 9.1.10: 'All secure commands that fail integrity checks are discarded.'"

Accept suggested resolution.

63 (Gilb, TR) [SEC] We still don't have a good description of what to do with commands sent or received with security on. Also need to generalize for the case of peer-to-peer security. Add description including peer-to-peer security. **Suggest accept in principle. (Note that this introduces functionality to maintain separate modes for different DEVs)** Add the following text to the beginning of 9.2.11:

"DEVs shall maintain a security state denoting whether security is required for each security relationship. If security is required for a particular security relationship, all frames transmitted to and received from another DEV in that relationship shall be protected by the keys indicated in {xref - Table 57}. A DEV may send or receive certain command frames without protection as indicated in {xref - Table 48}. If a DEV receives a frame that is not protected as required, the DEV shall discard the frame. If security is not required for a security relationship, all frames transmitted to and received from another DEV in that relationship shall be sent without security. If a DEV receives a protected frame when security is not required, the DEV shall discard the frame.

If the DEV is participating in a secure piconet, the security state for the relationship with the PNC, and consequently the broadcast key, shall be set to security required. For peer-to-peer communications, the DEV may choose to require security or not for that relationship, regardless of the security state shared with the PNC. If security is required in a peer-to-peer relationship, but the DEVs have not authenticated with each other, the group data key shall be used to protect frames between the DEVs."

Table, How do the peer DEVs know what security state they are supposed to be in if they have not mutually authenticated. Data protection as a separate capability? Take the discussion to the email list.

93 (Gilb, TR) [SEC/PIB] The security suite and public-key verification information have been removed from the MAC PIB. This implies that there is no accessible information that the MLME can use to perform verification on the public key. In particular, the CA certificate or hash of the public key are not available. In clause 10, each security sub-suite specifies that the ACL indicates which public-keys shall be accepted and which shall be rejected. Add public-key verification information back into the ACL and specify in each security suite how that ACL information is to be used. If there are operations to be performed by the DME to verify the public key, those should be mentioned in the security suites as well. This applies to 6.5.6 as well. **Suggest accept in principle.** The public key verification operations are performed by the DME and are hence outside the scope of the standard. Rather than adding this information to the PIB, the description of the security suites in clause 10 should be modified to reflect that this is out of scope. Make the following changes to clause 10:

In clause 10.3.1.4.3, change the paragraph in lines 18-19 to: "The certificate shall be generated using the digital signature algorithm ECDSA as specified in 10.3.1.4.4. The validation of the certificate is outside the scope of this standard."

In 10.3.2.2.2, remove step 2) and the final sentence and add the following text:

"Processing shall be aborted if the public key is not successfully extracted.

The DEV should perform additional checks such as comparing the DEV address in the ManCert to the DEV address in the authentication request or comparing the received key and ID to values stored in its ACL to verify the authenticity of the public key."

In 10.3.2.3.2, remove step 2) and the final sentence and add the following text:

"Processing shall be aborted if the public key is not successfully extracted.

The DEV should perform additional checks such as comparing the DEV address authenticated in the ImplCert with the DEV address stored in its ACL to verify that the device is authorized."

In 10.3.2.4.2, remove step 2) and the following paragraphs and add the following text:

"Processing shall be aborted if the public key is not successfully extracted.

The DEV should perform additional checks such as signature verification as specified in 10.3.1.4.3, CRL checking, validity period verification, key use checking and comparing the DEV address in the X.509 certificate with the DEV address stored in its ACL to verify that the device is authorized."

In 10.4.2.2, change the table entry for Verification of Public-Key to the following text:

"The ID and public-key received during the authentication protocol should be verified by the DME using checks such as generating the SHA-1 hash of the device address concatenated with the public-key and comparing that to the hash of the ID and public key stored in the ACL."

In 10.5.2.2, change the table entry for Verification of Public-Key to the following text:

"The ID and public-key received during the authentication protocol should be verified by the DME using checks such as generating the SHA-1 hash of the device address concatenated with the public-key and comparing that to the hash of the ID and public key stored in the ACL."

In 10.5.3.2, change the table entry for Verification of Public-Key to the following text:

"The X.509 certificate received in the authentication protocol should be verified by performing checks such as signature verification as specified in 10.5.1.7, CRL checking, validity period verification, key use checking and comparing the DEV address in the X.509 certificate with the DEV address stored in its ACL to verify that the device is authorized."

Table until it can be reviewed with Rene.

100 (Gilb, TR) [SEC] The public-key object types listed in 7.5.2.1 are not necessarily sufficient for information to verify a public-key object that is received. A new information element called ACL entry value should be added. The ACL entry value should have a type, length, DEV address and verification value. This verification value may be a SHA-1 hash, a SHA-256 hash, an X.509 CA certificate, an implicit certificate CA certificate or some other as yet undefined field. This should be flexible since in future iterations, the verification information may change form. **Suggest accept in principle.** "A new command is being added to pass ACL information as specified in the resolution to 102. There are reserved types, so this will be extensible if needed. This also includes an updated table for ACL entries that include the listed values. Resolve as indicated in 102."

Accept suggested resolution.

101 (Gilb, TR) [SEC] The disassociation request command may be sent before the device is authenticated. In addition, the table does not specify when the commands shall be sent with security turned on. The X should be removed from the “authenticated (if required)” column for the disassociation request command and a column should be added indicating which frames shall be sent with security when authenticated. Recommend allowing the probe command and piconet services command and all of the association, authentication and challenge commands not to require security and all the rest of the commands to require security when authenticated. Alternately, this information could be added to clause 9 if that is a more appropriate location. **Suggest accept in principle.** Remove the “X” from the disassociation request command. Add a column to Table 48 with the heading “Security required if authenticated” and insert an “X” in every entry except for association request, association response, authentication request, authentication response, challenge request, challenge response, probe and piconet services. Re-write the first paragraph of 7.5 to coordinate this resolution with the resolution to 63. Change first paragraph to:

“The MAC command types are listed in Table 48 and are described in the following subclauses. If the column labeled “Associated” in Table 48 is marked with an “X” then that command shall only be sent by a DEV that is associated in the piconet. If the column labeled “Authenticated (if required)” in Table 48 is marked with an “X” and authentication is required for the piconet, then that command shall only be sent by a DEV that is authenticated with the PNC in the piconet. For peer-to-peer communications, if the DEV requires security with the selected peer DEV, and the “Authenticated (if required)” column is marked with an “X”, that command shall be sent to the peer DEV only if the DEVs are authenticated to each other. If the column labeled “Security required if authenticated” in Table 48 is marked with an “X” and authentication is required for the piconet, then that command shall be sent securely using the key specified in {xref - Table 57} for that command. For peer-to-peer communications, if the DEV requires security with the selected peer DEV, and the column labeled “Security required if authenticated” in Table 48 is marked with an “X”, then that command shall be sent securely to the peer DEV using the key specified in {xref - Table 57}.”

> Table, Singer to rewrite the text as list or table perhaps? Note that the sentence ‘For peer-to-peer communications, ... authenticated to each other.’

Adjourned ata 1:41 pm PDT.

3.3 Tuesday, 1 October, 2002

Roll call: Ari Singer, Dan Bailey, John Sarallo, Jeyhan Karaoguz, Allen Heberling, Knut Odman, Jay Bain, Mark Schrader.

Meeting called to order at 9:08 am PDT

Agenda

- Roll call
- Email comments
- Comment resolution, 02/392r10
- Adjourn

3.3.1 Email resolutions

Did not receive comments via email: 131, 132, 147.

> Accept suggested resolutions for 131, 132, 147.

459 (Gubbi, TR) - [Start] Although I think it is against the intention, the text seems to overburden the task of starting piconet. DME needs some channel statistics to decide on channel, which I presume obtained at the

time of scanning procedure. Then DME decides the channel. The text further imposes that DEV check for channel being clear and then start a piconet. If DME has already taken the channel stats into account and has decided the channel (a) this causes the DEV to second check the channel which is waste of time and overhead for implementations and (b) Especially the last sentence in the para that mandates (use of shall) return of failure without starting a piconet contradicts the next (new) para where a capable DEV can start a neighbor (or child) piconet in a channel where a piconet already in existence. Change all "shall" to "may" in the para and let implementors decide which of the three solutions they want in their products **Suggest accept in principle:** "There has been considerable debate whether a PNC capable DEV should initiate a second scan of the channel prior to the DEV transmitting its first beacon as a PNC. The consensus arrived at was that during the time that the PNC-DME was evaluating the results of its first scan that a second DEV could have initiated a piconet in a channel that the first DEV originally scanned as being clear. Consequently, it was decided that a second scan just prior to transmitting the first DEV's beacon was a good interference mitigating practice.

Item (b): I agree that returning an error code indicating a failure is not descriptive enough. However clause 6.3.3.2.2 does describe in more detail which ResultCode is to be returned and I believe addresses the commenters concern regarding the lack of detail in the sentence in line 13-15 on page 155. In addtion, I agree that there is need for a sentence at the end of the sentence in line 15, page 155, that states that 'The DEV-DME upon receiving the failure code may decide to change to a diferenct channel {xref 8.11.1} or become a dependent piconet of the other piconet.' Now in regards to the paragraph starting on line 17 page 155, this paragraph is describing the behaviour of the PNC after it is already established not after performing its second scan."

Accept suggested resolution.

170 (Heberling, T) - [MultiCast] MLME-MULTICAST-RX-SETUP.request is not referenced anywhere in clause 8.Should it affect reception filtering?/KO. Decide what it shall do and add it to clause 8. **Suggest accept in principle:** "This primitive is only used at the higher levels of the MAC and does not affect (other than in implementation dependnet ways) the operation of the MAC. Since it does not change the on-air behavior of a DEV, there is no need to mention it in clause 8. For example, MLME-RESET and MLME-SYNCH are not mentioned anywhere but in clause 6 since they only affects that interface."

Table until Thursday, WMS to supply text for 8.5.3.

3.3.2 MaxProcessed and MaxAssignedCTAs

219 (Heberling TR) - [MaxCTA] MaxProcessedCTAs and MaxAssigned CTAs are only needed for handover. It is much better to put them in the DEV info set./KO. Delete MaxProcessedCTAs and MaxAssigned CTAs from Figure 28. Move corresponding text to 7.5.1.1, since they are first used in the association request. **Suggest accept.**

Accept in principle, "Delete MaxProcessedCTAs and MaxAssigned CTAs from Figure 28 and the associated text."

416 (Gubbi, TR) - What is the use of information on (a) MaxProcessedCTAs and (b) MaxAssignedCTAs at the DEVs that receive this info in the beacon? Whatare they supposed to do with it? Remove (a) MaxProcessedCTAs and (b) MaxAssignedCTAs from DEV-association IE. **Suggest accept.** "Resolve as indicated in CID 219. See also CID 193 and 201."

Accept.

193 (Heberling, TR) - [MaxCTA] Are the MaxProcessedCTAs and MaxAssignedCTAs fields really necessary? If not delete them from the figure as well as any supporting text in clause 7.4.4. Please make the requested deletions. **Suggest accept.** "Resolve as indicated in CID 219. See also CID 416 and 201."

Accept.

229 (Heberling, TR) - [MaxCTA] MaxProcessedCTAs and MaxAssigned CTAs are only needed for handover. It is much better to put them in the DEV info set. Elements included separately in association request, 7.5.1.1 and PNC information , 7.5.4.2/KO. Delete MaxProcessedCTAs and MaxAssigned CTAs from Figure 35 delete corresponding text on page 126, line 32-34. **Suggest accept.** "See also CID 197 and 201."

Accept.

197 (Heberling, TR) - [MaxCTA] Remove the MaxProcessedCTAs and MaxAssignedCTAs from the Capability IE. These two fields are unnecessary. They are of no interest to any other DEV other than the PNC. Please make the requested changes. **Suggest accept.** "See also CID 229 and 201."

Accept.

201 (Heberling, TR) - [MaxCTA] Remove the MaxProcessedCTAs and MaxAssignedCTAs from the Association request command. These two fields are unnecessary. It is unclear to me why these parameters are needed at all. Please make the requested change.

Accept in principle: "Delete MaxProcessedCTAs and MaxAssignedCTAs from everywhere in the draft. This affects clauses 6, 7 and 8. Change the error code for page 143, line 54 to be 'Stream terminated by PNC' and add a new error code following it that is 'Stream terminated by target DEV' and add this error code to clause 8.5.1.3 for when the target DEV terminates the stream. Add the error code to the MSC in Figure 114 as well."

206 (Heberling, TR) - [MaxCTA] Remove the MaxProcessedCTAs and MaxAssignedCTAs from the PNC Information command. These two fields are unnecessary. Please make the requested change. **Suggest accept in principle:** "Resolve as indicated in CID 201."

Accept suggested resolution.

3.3.3 Fragmentation

59 (Gilb, TR) - The aMaxTransferUnitSize is so large that it will prevent implementers from creating very low cost compliant DEVs. Note that upper layer protocols are already able to determine the MTU and adjust their fragmentation accordingly.The biggest MSDU you have to reassemble is 64 kB, period. Thus for 8 QoSstreams plus asynchronous, you might have to reassemble 9*64 kB, which is pretty damn big. 2 k to 8 k should be fine and would significantly reduce the buffering requirements for re-assembling the frames. **Suggest accept in principle:** "Change aMaxTransferUnitSize to be PHY dependent, for the 2.4 GHz PHY define it to be 2044 octets in 11.7. Add a note to 11.7 that if security is enabled, the upper layers should fragement to 2044 minus the security overhead as defined in {xref 7.2.x secure data frame}."

Accept suggested resolution.

68 (Gilb, TR) - Reassembly of fragmented data is not supportable, practically speaking, if aMaxTransferUnitSize is set to 65535 octets and the MAC must reassemble at least 8 isochronous streams and 1 asynchronous "stream". The amount of memory required by an implemention for reassembly alone would be 9*(655535) - 9*(2044) or roughly 571,000 octets. aMaxTransferUnitSize should be limited to match the MTU for the 802.15.3 since this is larger than any probable implementation of the standard will use. For the 2.4GHz PHY, change aMaxTransferUnitSize to 2044 in Table 56 on page 215. Given this size, the amount of memory required to reassemble 9 streams is approximately a minimum of 18,400 octets. Also see another comment regarding fragmentation thresholds. **Suggest accept in principle:** "Resolve as indicated in CID 59."

Accept suggested resolution.

69 (Gilb, TR) - Presently the standard doesn't provide a minimum fragment size. One effect is that some implemention might cause severe channel usage inefficiency with multiple small fragments. An undefined fragment size also complicates the design of memory management data structures in an implementation. In addition, although a "fragmentation threshold" is mentioned in this subclause, it doesn't appear to be a PIB object or a MAC sublayer parameter. Each DEV should publish its desired fragmentation threshold during association since different implementations will have varying needs, and the PNC should circulate these values to each DEV in the piconet using beacon MMPDUs. Add a MAC sublayer parameter "aMinFragmentSize" in Table 56 on page 215, and set this to 128 (octets). If fragmentation is in use, DEVs may not transmit frames (except the last) with payloads smaller than this value. Also change the definition of the "Capability" field in association and beacon MMPDUs, as defined on page 126 in Figure 36, by using bits b8-b5 and naming this field "FragmentationThreshold". DEVs must store and use this information on a per-destination DEV basis, fragmenting any frames sent to the DEV when a frame's payload exceeds FragmentationThreshold octets. This relationship holds: aMinFragmentSize <= FragmentationThreshold <= aMaxFrameSize. All fragments except the last shall be sent using the same fragment size. **Suggest accept in principe:** "Add a MAC sublayer parameter "aMinFragmentSize" in Table 56 on page 215, and set this to be a PHY dependent parameter. In 11.7 define this to be 128 (octets). Modify figure 36 - Capability field format as follows: Define bits b7-b5 to be "Preferred fragment size". Add the following text to section 7.4.1 after the paragraph describing the supported data rates field: 'The preferred fragment size field is a PHY dependent mapping that indicates the MAC frame size preferred to be received by the DEV when fragmentation is used. For the 2.4 GHz PHY, the mapping of a field value to a preferred fragment size is defined in Table 126.' Replace the following text in section 11.7: 'The PHY dependent PIB values for the 2.4 GHz PHY are given in Table 126 and Table 127.' with: 'The encoding of the preferred fragment size used in the capabilities information element, 7.4.11, is given in Table 10.'

Table 10—2.4 GHz PHY preferred fragment size encoding

Field value	Preferred fragment size (octets)
0	{xref aMaxFrameSize}
1	1792
2	1536
3	1280
4	1024
5	512
6	256
7	{xref aMinFragmentSize}

The PHY dependent PIB values for the 2.4 GHz PHY are given in {xref Table 127} and {xref Table 128.}'

Accept suggested resolution except use 64 bytes as MinFragmentationtSize.

3.3.4 PM/SPS

338 – text completed – awaiting commenter approval

344 – text completed – awaiting commenter approval

365 – text completed – awaiting commenter approval

In a) change ‘via the IE for that’ to be ‘via the SPS status IE for that’
b) OK, this is really answered with the last sentence.
c) OK
d) OK
e) OK
f) OK
Accept suggested resolution (WMS and ADH)

16 (Gilb, TR) 7.5.7.3 pg 149, ln 17 - Next awake beacon is no longer defined in 7.5.7.2. - Change the field definition to be the following "The next awake beacon field is a beacon number, 7.4.2, when the DEV is scheduled to be awake." **Suggest accept in principle:** “Add the 2 octet version {place correct term} of next awake beacon into the SPS IE and that should fix the underlying problem.”

Accept in principle, “Add the 2 octet version {place correct term, currently beacon number} of next awake beacon into the SPS status IE and that should fix the underlying problem.”

534 (Bain, T) 7.5.7.5, pg 150, ln 33 - next awake beacon is a 4 octet field while beacon count is now a 6 octet field. Either note that the next awake beacon is the last 4 octets of beacon counter or change next awake beacon to be 6 octets. - Make one of the suggested changes. **Suggest accept in principle:** “Resolve as indicated in CID 16.”

Accept suggested resolution.

335 (Heberling, TR) 7 fig 82 pg 148, ln 17 - Why does the SPS configuration request command format have to vary between 2 and 4 octets? Why not just keep it 4 octets? Seems it would make it less complicated to to decode. - Please fix the SPS configuration request command length to 4 octets. Also make appropriate changes to Table 49 to reflect the fact that the frame format is fixed. **Suggest reject:** “The BRC discussed this for LB17 and decided on the variable length.”

Accept original resolution, fix to 4 octets.

336 (Heberling, TR) 7 fig 83 pg 149, ln 9 - Why does the SPS configuration response command format have to vary between 2 and 8 octets? Why not just keep it 8 octets? Seems it would make it less complicated to to decode. - Please fix the SPS configuration request command length to 8 octets. Also make appropriate changes to Table 50 to reflect the fact that the frame format is fixed. **Suggest reject:** “The BRC discussed this for LB17 and decided on the variable length.”

Accept in principle, “Fix the SPS configuration request command length to 6 octets since the next awake beacon is now 2 octets, see CID 16. Also make appropriate changes to Table 50 to reflect the fact that the frame format is fixed. {Ed. note unused fields shall be set to zero and may be ignored on reception.}”

356 (Schrader, TR) 8.13.2.2, pg 209,210 - In removing implicit stream resumption when changing from SPS to ACTIVE mode, too much inefficiency was introduced for DEVs that need to restart ACTIVE mode streams quickly. - Still in the spirit of our compromise: Allow the mode change command along with one or more CTRs to occur anywhere that multiple CTRs are currently allowed. Require that the mode change command be the first command in the sequence. The result: switching to ACTIVE mode and starting an ACTIVE stream becomes efficient. **Suggest accept in principle:** “SPS DEV shall be given a directed frame to the PNC in its awake beacon. The SPS DEV shall be allowed to send a PS change command with the ACTIVE parameter and up 2 CTR commands in the same directed frame.”

Discussion is to allow the two commands to be sent in the uplink MTS. Do we need to add help in the CAP? Feeling is that the PNC allocates the CTA to the SPS DEV always since it is expecting a response. MKS to provide text for Thursday, 3 October 2002.

450 (Gubbi, TR) 7.5.5.2, pg 144, ln 2 - Reason code 6 has become unreasonable. Why should a stream be terminated just because DEV is in PS mode? - Remove the inserted text "Stream terminated, " **Suggest reject:** "The actual termination is based on changing from mode to mode. The DEV is no longer in ACTIVE mode and doesn't need the same stream."

Mark will write text, the idea is that the PNC shall terminate all super-rate streams where the power save DEV is the destination when the DEV sends a PS mode change command to the PNC requesting a change to a power save mode. Send text via email for comments. Also applies to 262. What if someone allocates a super-rate stream to a DEV in power save mode? It is up to the DEV to the terminate the stream.

Meeting adjourned at 10:33 pm PDT.

3.4 Thursday, 26 September, 2002

Attendees: James Gilb, Allen Heberling, Knut Odman, Ari Singer, Jay Bain.

Meeting called to order at 9:11 am PDT.

The agenda is:

- Roll call
- Schedule additional security call for next week?
- Schedule for next week
    - Max assigned/processed CTAs on Tuesday
    - Security either Tuesday or Wednesday
    - BRC email ballots
- Comment resolution, 02/392r9
- Resolution writing update, 02/406r3
- Adjourn

Security call for 1.5 hours on Wednesday, 2 October, 2002 at 10 am, James Gilb will sponsor the call.

BRC email ballots: PM, MTS, PMWake. These will be due on Friday 4 October, 2002, 5 pm PDT.

3.4.1 CTA status IE/command

208 (Heberling, TR) [CTM/CTAStat] The CTA status command lacks any description of what it is used for or any reference to another clause where its functional use is described. Either delete this command from the draft or provide text describing the purpose of this command as well as references to where it is used. If the above changes are made, then also make these changes: 1) change the Start beacon number field length from 4 octets to 6. 2) change the command length from 5 to 10. Please make the requested change. **Suggest accept in priciple:** "The CTA status command is replaced by CTA status IE. The start beacon number will be the 2 octets with LSb of the 6 octet beacon number. See the resolution of CID 301."

Accept suggested resolution.

301 (Heberling, TR) - [CTM/CTAStat] The idea to send a directed CTA status command to DEVs in sleep modeand for all pseudostatic streams is not good for the following reasons.1) multicast/broadcast. We have

already said that PSDEVs are not required to listen to non directed streams,but unless we announce them, they don’t even have thechance to do so.This is true regardless of the stream is psudo-stat ordynamic, subrate or regular.2) The PNC has to allocate a down MTS for this directed frame.If the frame is not ack’ed it's supposed to allocate another down MTS and resend it. This will be hard to implementand the risk is that all implementors will make a long defaultdown MTS to broadcast to allow for all events. That would suck power. Conclusion: since it's already taking the pain to allocate MTS in the beacon, why not put the announcement there as proposed in 02/276r6.This would solve all the above cases./KO Delete this clause and replace with CTA status IE, see02276r7P802-15_TG3-commentsD11_KO.doc, Resolution [14]. **Suggest accept in principle**, “Delete 7.5.5.3 and add a new IE, the CTR status IE with the text in 02/392r8.”

(begin new text for CTR status IE)

7.4.x CTR status IE

The CTA status IE is used by the PNC to inform DEVs about certain characteristics of allocated CTAs. The CTA status IE shall be formatted a Figure 16.

octets: 2	**2**	**1**	**1**	**1**	**1**
Start beacon cycle	CTR interval	CTR control	Stream index	Length (=6)	Element ID

Figure 16—CTA status information element format

The stream index field is defined in {xref 7.5.5.1}.

The CTR control field is defined in {xref 7.5.5.1}.

The CTR interval is set to the number of beacons between every GTS as described in {xref 7.5.5.1}. If either a single or multiple CTAs per superframe are allocated, this value shall be set to zero.

The start beacon cycle is set to the 16 lsbs of the beacon number, {xref 7.3.1}, of the first beacon where the first GTS of the new or modified stream will be allocated.

(end new text for CTR status IE).

Accept suggested resolution

303 (Heberling, TR) - [CTM/CTAStat] The idea to send a directed CTA status command to DEVs in sleep modeand for all pseudostatic streams is not good for the following reasons.1) multicast/broadcast. We have already said that PSDEVs are not required to listen to non directed streams,but unless we announce them, they don't even have thechance to do so.This is true regardless of the stream is psudo-stat ordynamic, subrate or regular.2) The PNC has to allocate a down MTS for this directed frame.If the frame is not ack:ed it's supposed to allocate another down MTS and resend it. This will be hard to implementand the risk is that all implementors will make a long defaultdown MTS to broadcast to allow for all events. That wouldsuck power.Conclusion:since it's already taking the pain to allocate MTS in thebeacon, why not put the announcement there as proposed in 02/276r6.This would solve all the above cases./KO Replace text on line 14-17 with new text in:02276r7P802-15_TG3-commentsD11_KO.doc, Resolution [14]. **Suggest accept in principle:** “Change 8.5.1.1, page 179, line 14-17 to be: ‘The PNC shall announce the creation of all pseudo-static streams. It shall also announce creation of a stream where the target DEV is in a power save mode and streams with the TrgtId set to BcstId or McstId if any DEV is in a power save mode. The PNC shall make the

announcement with the CTR status IE, {xref 7.4.x} using the beacon information announcement mechanism {xref 8.1.1}. The PNC shall issue the first GTS for the stream in the superframe indicated in the IE.'"

Accept in principle, "Change 8.5.1.1, page 179, line 14-17 to be: 'The PNC shall announce the creation of all pseudo-static streams. It shall also announce creation of a stream where the target DEV is in a power save mode and streams with the TrgtId set to BcstId or McstId if any DEV is in a power save mode. The PNC shall make the announcement with the CTR status IE, {xref 7.4.x} using the beacon information announcement mechanism {xref 8.1.1}.' Add to 8.4.4.4 'It the PNC allocates a new isochronous CTA or modifies the CTR interval of an existing CTA with an SPS DEV as the target, the PNC shall also allocate an uplink MTS, in the same superframe as when the CTA is allocated. The PNC is not required to allocate the MTS if the commands are allowed in the CAP, {xref 7.3.1}.'"

305 (Heberling, TR) - [CTM/CTAStat] The idea to send a directed CTA status command to DEVs in sleep modeand for all pseudostatic streams is not good for the following reasons.1) multicast/broadcast. We have already said that PSDEVs are not required to listen to non directed streams,but unless we announce them, they don't even have thechance to do so.This is true regardless of the stream is psudo-stat ordynamic, subrate or regular.2) The PNC has to allocate a down MTS for this directed frame.If the frame is not ack:ed it's supposed to allocate another down MTS and resend it. This will be hard to implementand the risk is that all implementors will make a long defaultdown MTS to broadcast to allow for all events. That wouldsuck power.Conclusion:since it's already taking the pain to allocate MTS in thebeacon, why not put the announcement there as proposed in 02/276r6.This would solve all the above cases./KO Replace text on line 40-45 with new text in:02276r7P802-15_TG3-commentsD11_KO.doc, Resolution [14]. **Suggest accept in principle:** "Change 8.5.1.2, page 182, line 40-45 to be: 'The PNC shall announce the modification of all streams where the target DEV is in a power save mode and for streams with the TrgtId set to BcstId or McstId if any DEV is in a power save mode, if the CTR type or CTR interval is modified. The PNC shall make the announcement with the CTR Status IE, {xref 7.4.x} using the beacon information announcement mechanism {xref 8.1.1}. The PNC shall issue the first modified GTS for the stream in the superframe indicated in the IE. If the target DEV is in SPS mode, the PNC shall also allocate an uplink MTS in the same superframe as when the CTA is allocated.'"

Accept suggested resolution.

299 (Heberling, TR) - [CTM/CTAStat] The idea to send a directed CTA status command to DEVs in sleep modeand for all pseudostatic streams is not good for the following reasons.1) multicast/broadcast. We have already said that PSDEVs are not required to listen to non directed streams,but unless we announce them, they don't even have thechance to do so.This is true regardless of the stream is psudo-stat ordynamic, subrate or regular.2) The PNC has to allocate a down MTS for this directed frame.If the frame is not ack:ed it's supposed to allocate another down MTS and resend it. This will be hard to implementand the risk is that all implementors will make a long defaultdown MTS to broadcast to allow for all events. That wouldsuck power.Conclusion:since it's already taking the pain to allocate MTS in thebeacon, why not put the announcement there as proposed in 02/276r6.This would solve all the above cases./KO. Introduce a CTA status IE, see 02276r7P802-15_TG3-commentsD11_KO.doc, Resolution [14]. **Suggest accept in principle:** "Resolve as indicated in CID 301."

Accept suggested resolution.

493 (Gubbi, TR) - Command in a beacon? There are three options: 1. Remove this sentence completely OR 2.Change "DEV in its wake beacon" to "DEV in the superframe corresponding toits wake beacon" OR 3. Define channel status as an IE and include it in Beacon. **Suggest accept in principle:** "The text should have said the command was sent in the wake superframe rather than the wake beacon. However, as a result of the resolution of CID 303 and 305, this information is now sent as an IE in the wake beacon for the power save mode DEV, as suggested in option 3."

Accept suggested resolution.

3.4.2 Others

454 (Gubbi, TR) - The term "wake beacon" deserves a clear description. What is it intended for as far as DEV is concerned? Clearly state if DEV is allowed to sleep ONLY between two wake beacons and not allowed to sleep at TBTT of wake beacons. But if this is true, note that this is not acceptable for DEVs intending to save power in a large magnitude.Retain APS scheme from D10. **Suggest accept in principle**: "DEVs are allowed to refuse listening to system wake beacons. A DEV in an SPS set sets its own sleep period and may choose to participate or not participate in the PSPS. SPS DEVs not listening to system wake beacons (i.e. not participating in PSPS) would miss PNC parameter change and broadcast announcements. If the piconet has changed in some manner during their sleep time, they have to scan and recover in a fashion out of scope of the standard. Add clarifying text in 8.13 'The wake beacon for a DEV is defined as the PNC defined system wake beacon for DEVs in PSPS mode {xref 8.13.1} and the wake beacon of the SPS set for a DEV in SPS mode {xref 8.13.2}'. Also, a new Hibernate mode will be added as indicated in CID 508 that provides essentially all of the functionality of APS using SPS set 0."

Accept suggested resolution.

323 (Heberling, T) - [MTS] I think the idea is that the PNC shall support at least one CAP or MTS. If so, a better notation would be to collect the two as subclausesunder MLF 12 and list support as O.1. As it stands now it's not obviouswhat the O.1 is an anlternative of.Second: only the PNC has this option, however the DEV needs to supportboth to be able to associate. In practicality it's likely that different PHY will use different options, but at a MAC level we need to specifyit in the way listed in the Suggested Remedy./KO Change to: 12 - Management channel time support12.1 - CAP channel access during piconet operations - 8.4.2 - FD1:M, FD2:O.112.2 - MTS operations - 8.4.4.4 - FD1:M, FD2: O.1 **Suggest accept in principle:** "Change to: MLF12 and MLF13 to the text in 02/392r9. Re-number the rest of the PICS table as appropriate."

(new rows for PIICs table)

MLF12	**Contention access methods**					
MLF12.1	CAP channel access during piconet operations	8.4.2	O.1			
MLF12.2	MTS operations	8.4.4.4	O.1			

(end new rows for PICs table)

Accept suggested resolution.

422 (Gubbi, TR) - This IE unncessarily tries to carry too many unrelated things in one baggage. Splitting this into multiple IEs eases both the understandingof the IE and its implementation. Additonal question is, if ChangeTypeis to be extended in the future for to convey some other "change" how are the new fields required introduced into this closed bag? There is no needto require two levels of parsing to know what the intent of IE is. Split this IE into the following:1. PNID/BSID change IE with both PNID and BSID being present and being current all the time2. TBTT change IE (define the term TBTT - it is a very useful term)3. Superframe-Size change IE4. Channel change IE. **Suggest reject:** "The TG felt that it was better to define fewer IEs and use the change type to indicate what item in the piconet is changing. There is a trade-off in defining more IEs and using a single field in this IE to indicate what parameter of the piconet is changing. TBTT is not appropriate for this standard because the beacon occurs at a precise interval, meaning there is

no offset from the target time. The term superframe duration is used in this standard to indicate this interval. In the case of the superframe size change, a extra parameter would be required to indicate if it is the superframe duration or the superframe time location that is changing."

Resolution is to reject.

428 (Gubbi, TR) - There is limited use of "PNC handover" IE as it is defined and that is conveys that the current PNC is not going to continue as PNC. Instead if the DEV-ID and DEV address of the new PNC are also announced, then it provides all the required info at the associated DEVs. Include DEV-ID and DEV address of the new PNC in Figure-33 and add theirdescriptions in 7.4.9 AND change the caption appropriately. it is definitely not "DEV address information" **Suggest accept in princple:** "Add two fields to the handover element, 'New PNC DEVID" and "New PNC DEV address" with the new caption and the descriptions as indicated 02/392r8."

(begin new PNC handover IE description).

octets: 6	**1**	**1**	**1**	**1**
New PNC DEV address	New PNC DEVID	Handover countdown	Length (=1)	Element ID

Figure 17—PNC handover information element format

The handover countdown field shall be decremented by the old PNC from its initial value of NbrOfHandoverBeacons -1 to 0 before ceasing the transmission of its beacons during the handover process.

The new PNC DEVID field contains the current DEVID of the DEV that will be taking over as PNC.

The new PNC DEV address field contains the DEV address of the DEV that will be taking over as PNC.

(end new PNC handover IE description)

Accept suggested resolution.

457 (Gubbi, TR) - use "channel statistics": In order to make the implementations uniform and interoperating in this respect, it is a good idea to define channel statistics in a concrete manner, like PER. Otherwise each implementor chhoses his/her own "channel statistics" and hence resulting in potentially conflicting conclusions on channel condition. Mandate DEVs to measure PER and use that as a measure for rating thechannels. **Suggest reject:** "The scanning and channel rating process is a passive one and therefore PER is not necessarily a good measure. The only way to use PER in a passive manner would be for the DEV to promiscuously receiver 802.15.3 frames and calculate how many fail FCS or HCS check. Then the question is: which is the best channel? If there are only one 802.15.3 piconet, then the best channel is the one with the highest PER since this might imply that the level of interference from the other piconet in this channel would be the least. However, if there is a non 802.15.3 interferer, e.g. 802.11, near the DEV peforming the scan, then the PER would be high, but the channel would be bad due to the interferer. Furthermore, PER does not report the presence of other types of networks in the channel. For example, if there were 802.15.3 piconets with weak signal strength in channels 1 and 3 and an strong 802.11 WLAN in channel 5, the PER measure would rate channel 5 as best when in reality either channel 1 or channel 3 might be better. Additionally, it is not just the PER, but the frequency of the traffic or interference in the channel that is important. Simply reporting PER does not indicate how heavily the channel is used. Finally, the channel assesment is performed by the prospective PNC internally, it makes the measurement and it makes the decision. Therefore, there are no interoperability problems in letting the implementer determine how to best choose the channel."

Resolution is to reject.

482 (Gubbi, TR) - Updates are incomplete and not quite specific: Beacons in a superframe are sent at the start of superframe. Since all CAP transmissions are mandated to end before the end of CAP, there should not be any hesitation in saying that the beacon must start at TBTT, defining TBTTs to be the start of superframe which occur at strictly regular intervals conditioned upon the clock accuracies as spcified by the standardand/or MOVE of superframes as decided by PNC. right? If there are other special cases, please do list them, instead of leaving unspecified/vague the very basic concept in the standard. Specifying it now will avoid lot of headaches later, especially in the presence of psuedo static and private GTSs. Define TBTTs to to be the start of superframe which occur at strictly regular intervals conditioned upon the clock accuracies as spcified bythe standard and/or MOVE of superframes as decided by PNC. **Suggest accept in principle:** "The standard already defines a fixed superframe duration, 8.6 and it clearly states that the beacon shall be sent a 'superframe duration' after the start of the last beacon, 8.6.2. TBTT is not a good acronym since it is the "target beacon transmission time" rather than the fixed time specified in this standard. Using TBTT would confuse the reader since this acronym is also used in 802.11 where it means only the "target" and not the actual time when the beacon will be sent. The standard clearly states in 8.10.1 and 8.10.2 that the PNC may change the duration or position of the beacon but that it shall use a specific process to accomplish this change. There are no other exceptions allowed for the PNC in sending the beacon and this is clearly stated in the draft. The clock accuracy for the timing is specified in 8.6.1. Add a sentence to 8.6.2, which says 'The PNC shall transmit the beacon such that the time between beacons is the superframe duration with an error or no more than aPHYClockAccuracy times the superframe duration. The PNC changes the superframe position or duration using the procedures indicated in {xref 8.10.1} and {8.10.2}, respectively.'"

Accept suggested resolution.

490 (Gubbi, T) - The update does not cover whether the indicated responsiveness in the beacon can change over time due to reasons like network load. I get the impressionthat is the intention, but it is not clearly stated. State that the PNC can change the value of CTRRespTime from time to time.It may be a good idea to restrict PNC from changing it an association process is ongoing to avoid any confusion. **Suggest accept in principle:** "The value of the CTRRespTime is described in 7.3.1, which is cross-referenced in 8.4.4.3. The text in 7.3.1 states "The CTRRespTime field is an estimate by the PNC of the number of superframes it will currently take to respond to a channel time request by a DEV, 8.4.4.3. A value of zero indicates that the PNC estimates that it will take longer than 15 superframes to respond to a channel time requests.' Thus this value is the current estimate and therefore may change. A clarification will be added as indicated in the resolution of CID 491.'"

Accept suggested resolution.

550 (Bain, TR) - Elsewhere is a reserved 0xFD for MTS traffic. Should there be some mention of that here?I have not figured the method for a DEV to request additional MTS slots. Is it in this text? Add reference if appropriate. **Suggest accept in principle:** "The description for requesting MTS slots was added to 8.4.4.4 with CID 293. Add a sentence to the end of line 20, page 142, 'If the stream index field is set to the MTS stream index, {xref 7.2.5}, then the command is a request to modify the rate of uplink MTSs as described in {xref 8.4.4.4}.'"

Accept suggested resolution.

344 (Roberts, TR) 8.13.2, pg 208, ln 1 - CID 365 from LB17 is still not fully resolved. This item raises numerous questions regarding protocol issues that the SPS power management scheme has yet to address. Consequently, the issues it raised during LB17 are still valid for LB19. Also this CID provides additional reasons for why SPS should be optional at best._CID 365 "KO> _a) A DEV can join several SPS but how does it know when to be awake? _b) How do you send to broadcast of DEVs are in different SPS? _c) What are you supposed to do with "suspended CTA?"? _d) How do transmitters know when an intended receiver is awake? _e) How does it fit with ATP? With pseudostat? with subrate? _f) How is PNC supposed to calcu-

late available CTA when DEvs of different SPS may end up with all their CTA needs in the same superframe at some intervals? " 1) Ideally remove all the SPS Power managment scheme Clauses(8.13.2, 7.5.7.2,3,4,and 5, 6.3.12.1,2,3,4) ; 2) Have the authors of the SPS Pwr Mgt scheme address the questions raised in CID 365; 3) just make the SPS Pwr Mgt scheme optional for all DEVs. **Suggest accept in principle** "Adopt commenter option 2. The answers to the questions are as follows:

(begin answers for CIDs 338, 344 and 365)

a) *A DEV can join several SPS but how does it know when to be awake?* Each SPS set has an SPS interval and a next awake beacon. When a device is in SPS mode, it will wake up in awake superframes that are completely specified in each every beacon via the IE for that SPS set (documented in D10, 8.12.3, page 204, lines 43-45 and the same text in D11, 8.13.3, page 213, lines 52-54). The next awake beacon is no different than the countdown timer for PSPS except that it PNC only updates it once per awake interval rather than every superframe. The DEV will wake up for each awake beacon of each SPS Set that it has joined. If it can keep track of multiple subrate slots, then it can keep track of multiple sets of awake beacons. The process is no different. Currently the next awake beacon may be obtained with the SPS inquiry request command (documented in D10, 8.12.2.1, page 200 lines 49-52 and in D11, 8.13.2.1, page 208, lines 17-20). However, to make this easier for DEVs, add a 2 octet field to the SPS status command named 'Next awake beacon' defined as 'The 2 least significant octets of the beacon number when the members of the SPS set will be awake to listen for the beacon and any assigned CTAs.'

b) *How do you send to broadcast of DEVs are in different SPS?* You do it one of the following ways: 1. You allocate a slot every superframe and only transmit to the SPS DEV in the awake superframe, whose beacon number is listed in the beacon IE for the SPS set with SPS DEV's bit set in the bit map. 2. You join the same SPS set as the SPS DEV, allocate channel time with that set, and transmit when you see your CTA in the beacon. The SPS DEV always and only listens during its awake beacon and superframe. You can transmit during that time or you will not be heard. It is exactly the same as PSPS, except the DEV determines the awake interval instead of the PNC. This behavior is documented in D10, 8.12.2.2, page 202, lines 49-52 and in D11, 8.13.2.2, page 210, lines 21-24 (same text as in D10).

c) *What are you supposed to do with "suspended CTA?"?* D11 requires that channel time requests be made at the time of need. No longer does a DEV pre-request an ACTIVE and an SPS channel time. As a result, suspend and resume were removed with d11. There are no longer any suspended CTAs of any type. (In D10, the use of suspend and resume for CTAs was described in 8.12.2.2, page 202, lines 41-44).

d) *How do transmitters know when an intended receiver is awake?* Each SPS set has an SPS interval and a next awake beacon. You find out about an SPS set using an SPS inquiry command, 7.5.7.4 (documented in D10, 8.12.2.1, page 200 lines 49-52 and in D11, 8.13.2.1, page 208, lines 17-20). In addition, by adding the 2 least significant octets of the next awake beacon number to the SPS status IE (as described in answer a), this information will be available in every beacon as well. If both DEVs are in SPS mode, then they will both have awake beacons in the same superframe based on the timing of the SPS set that they're both using.

e) *How does it fit with*:

   1) *ATP?* ATP rules must be obeyed. The SPS DEV must transmit to the PNC in one of its awake superfames or wake up one additional time per ATP period in order to satisfy this requirement. The text of 8.3.4 (pg 166, ln 51) covers all DEVs.

   2) *With pseudostatic ?* Use of pseudo-static GTSs is not permitted for SPS DEVs. Text for this in D11 is in 8.4.4.1, page 171 line 1, which prohibits the use of sub-rate pseudo-static CTAs. In D10, sub-rate pseudo-static CTAs were allowed and an SPS DEV could have requested a sub-rate pseudo-static CTA aligned to its set, just as any other DEV could request one. The fact that an allocation is pseudo-static had no impact on DEVs in power save mode.

   3) *with subrate?* SPS is subrate with a shared time base. See 8.13.3 in D11, page 212, lines 32-41 (in D10, in subclause 8.12.3, page 204, lines 36-41).

f) *How is PNC supposed to calculate available CTA when DEvs of different SPS may end up with all their CTA needs in the same superframe at some intervals?* The PNC knows how much bandwidth is left and it knows what the maximum overloading of its worst superframe will be. If allowing another DEV to use channel time will produce too much superframe overloading, then the PNC will refuse the channel time based on that criteria (7.5.5.2 reason code 5). In addition, if the PNC is unable to allocate the slot at this particular time, then in both D10 and D11, the PNC simply does not allocate the CTA (D10, 8.12.2.2, page 202, lines 46-47 and in D11, 8.13.3, page 213, lines 41-50). In D11, the PNC has another option (along with the one it always had, i.e. to terminate the stream). The PNC is also able to allocate the CTA in one of the following superframes (up to 3), informing the SPS DEVs via the PCTM IE in the beacon. SPS is "synchronized" by design. The time slots are supposed to be the same superframe. At some point the awake superframes will not tolerate an additional slot allocation. This will not happen until too many DEVs are using the same SPS set. One way to minimize this possibility is to allow a larger minimum for the number of SPS sets. This will lessen the probability of overloading. The issues of allocating SPS CTAs is exactly the same as allocating any other sub-rate CTA. The PNC needs to determine if it can allocate the time. If it finds it is unable to allocate the time, it either refuses to create the allocation or terminates an existing allocation.

For additional flexibility, change the text in 8.13.2 (move 8.13.3 to be 8.13.2.3) so that the PNC is able to change the next awake beacon for SPS DEVs by changing the value in the beacon. This way, the PNC is able to spread out the SPS wake intervals to reduce superframe loading. However, the PNC will be constrained to not change it more than every aMinSPSWakeBeaconChange (=255 superframes).

(end response for CIDs 338, 344 and 365)"

Table until Tuesday, 1 October, 2002

338 (Heberling, TR) - 8.13.2, pg 208, ln 1 - CID 365 from LB17 is still not fully resolved. This item raises numerous questions regarding protocol issues that the SPS power management scheme has yet to address. Consequently, the issues it raised during LB17 are still valid for LB19. Also this CID provides additional reasons for why SPS should be optional at best._CID 365 "KO> _a) A DEV can join several SPS but how does it know when to be awake? _b) How do you send to broadcast of DEVs are in different SPS? _c) What are you supposed to do with "suspended CTA?"? _d) How do transmitters know when an intended receiver is awake? _e) How does it fit with ATP? With pseudostat? with subrate? _f) How is PNC supposed to calculate available CTA when DEvs of different SPS may end up with all their CTA needs in the same superframe at some intervals? " 1) Ideally remove all the SPS Power managment scheme Clauses(8.13.2, 7.5.7.2,3,4,and 5, 6.3.12.1,2,3,4) ; 2) Have the authors of the SPS Pwr Mgt scheme address the questions raised in CID 365; 3) just make the SPS Pwr Mgt scheme optional for all DEVs. **Suggest accept in principle "**Resolve as indicated in CID 344."

Table until Tuesday, 1 October, 2002

365 (Shvodian, TR) - 8.13.2, pg 208, ln 1 - CID 365 from LB17 is still not fully resolved. This item raises numerous questions regarding protocol issues that the SPS power management scheme has yet to address. Consequently, the issues it raised during LB17 are still valid for LB19. Also this CID provides additional reasons for why SPS should be optional at best._CID 365 "KO> _a) A DEV can join several SPS but how does it know when to be awake? _b) How do you send to broadcast of DEVs are in different SPS? _c) What are you supposed to do with "suspended CTA?"? _d) How do transmitters know when an intended receiver is awake? _e) How does it fit with ATP? With pseudostat? with subrate? _f) How is PNC supposed to calculate available CTA when DEvs of different SPS may end up with all their CTA needs in the same superframe at some intervals? " 1) Ideally remove all the SPS Power managment scheme Clauses(8.13.2, 7.5.7.2,3,4,and 5, 6.3.12.1,2,3,4) ; 2) Have the authors of the SPS Pwr Mgt scheme address the questions raised in CID 365; 3) just make the SPS Pwr Mgt scheme optional for all DEVs. **Suggest accept in principle "**Resolve as indicated in CID 344."

Table until Tuesday, 1 October, 2002

526 (Bain, TR) - The delayed ack text has a few problems -1) no mention of the setting for the Dly-ACK policy initially2) no mention of what to do with ACK policy bits on decline.3) no mention of what kind of data frame (The first fragment of the stream?) is used for at least the initial negotiation.4) The third paragraph mentions max burst value when talking about the Imm-ACK sent to decline the Dly-ACK negotiation. Doesn't seem to belong there.5) last sentence on pg 192, spelling of "source"6) there doesn't seem to be tie in to the DME providing the policy. There doesn't seem to be feedback to the DME that the requested policy has been denied by the recipiant. There is a result code in two tables in clause 6 MLME and MAC SAPs that talks about INVALID_ACK_POLICY but this seems to address the local capability to support Dly-ACK rather than a rejection by the destination.7) no mention of the rest of the content of the negotiation Dly-ACK frame body fields8) what does it mean that as an alternative to repeating the last data frame, an empty data frame which was not in the original burst. Suggest a rewrite of this subclause. **Suggest accept in principle:** "1) This is fixed by referencing both "Dly-ACK policy and Dly-ACK request bit" being set. 2) The FCSL is now notified in the MAC-ISOCH-DATA.confirm as indicated in CID 310. 3) Same resolution as 1). 4) Move the sentence "The destination DEV may change the max burst value in each Dly-ACK frame." to the end of the previous paragraph that ends "... max num (sp) frames, as provided in the Dly-ACK frame 7.3.2.2." (note spelling error). 5) Change "souce" to "source" 6) Add a sentence that says "The FCSL would then notify the DME that the Dly-ACK negotiation failed. The DME then knows that a modification of the channel time allocation might be required." 7) Add to page 192, line 42, "The MPDUs ACKed field shall be set to one and the MPDU ID field shall contain the information for the frame that was sent to negotiate the Dly-ACK.' 8) Resolved as indicated in CID 189. Also add to 7.3.2.2, page 114, line 3 a new paragraph, 'The MPDUs ACKed field shall contain the number of MPDUs that is being ACKed with this frame. This field shall be greater than or equal to 1.'"

Accept suggested resolution.

In the MSC on page 193, figure 120, Change data to be data frame, have ACK policy = Dly-ACK, Dly-ACK request bit = 1. In the response, change name to Dly-ACK frame with parameters, max num frame (or max frames), burst size, MPDUs ACKed and MPDU IDs.

Meeting adjourned at 10:36 am PDT.

3.5 Tuesday, 24 September, 2002

Attendees: Jim Allen, Allen Heberling, Ari Singer, James Gilb, Knut Odman, Jay Bain, Mark Schrader

Meeting called to order at 9:08 am.

Agenda

- Roll call
- Comment resolution, reference 02/392r8.
- Adjourn

394 (Gubbi, TR) - The requirement in "All DEVs in PSPS mode are required to listen to wake _beacons" is not clear. What does this mean? All PSPS DEVs have to receive _it or just be awake to receive it if channel permits? I am sure the intent _if NOT the former. If it is latter, then the maximum sleep time is made _same for all PSPS DEVs. This is not acceptable. Depending on the power requirements some devices might want to go for longer, but permitted by _PNC, sleep and wake up. Making those DEVs to wakeup to the time of TBTT _is fine as in 802.11. This sounds similar to DTIMs in 802.11, but with _worst performance outcome. Remove PSPS and revert back to APS mode as in D10 of the draft. **Suggest accept in principle:** "The requirement is that PSPS DEVs attempt to receive the system wake beacon. This sentence was clarified in

the resolution of CID 499. SPS serves the function of allowing the DEVs to specify their own power management requirements. As long as SPS remains in the standard, this concern will be satisfied. A new HIBERNATE mode will also be added that allows DEVs to sleep for long periods of times as in APS mode."

Accept suggested resolution.

395 (Gubbi, TR) - The sentence "All asynchronous traffic to DEVs in PSPS mode will be allocated in the wake beacon". What does this mean? if a DEV is in PSPS mode and there are 100 other DEVs requesting to send async data to it, all the 100 requests are allocated in the wake beacon? Why is this sentence needed. Remove PSPS and revert back to APS mode as in D10 of the draft. **Suggest accept in principle** "Change text to: "For asychronous time allocations to a destination DEV that is in either PSPS mode or SPS mode, the PNC shall not allocate any CTAs in superframes other than the awake superframes for that DEV." Part 2: This sentence is needed in order for the implementor to know what behavior to implement and to expect from PNCs. In this case the implementer needs to know that allocations will be made with an awarness of the correct superframes in which to insert them rather than in any superframe that is convenient. The PNC is allowed to chain multiple system wake beacons to avoid superframe congestion if it has more CTAs to allocate than will fit in the current superframe. The PNC is free to schedule asynchronous allocations whenever there is time."

Accept suggested resolution.

508 (Gubbi, TR) - (1) I am not sure how this new scheme (PSPS) can assume that all DEVs in the piconet have the same power save requirements and hence can use the same wake-beacon-interval. 802.15.3 caters for variety of devices and applications and hence there is a need for different such intervals depending on the kind of application served by the DEV. (2) At least in_802.11 the DEVs are not mandated to be awake at all DTIMs and hence they can be sure that there will not be any directed frame that they are going to miss when they are asleep (doze mode). In APS mode this was enhnaced for better efficiency by allowing the DEV to request the sleep duration it wishes and the PNC permitting up to that duration. In PSPS mode that advantage has disappeared and hence this forces an upper limit on power saving for all DEVs in a given 802.15.3 piconet. Worst is it is same across the board for all DEVs in the piconet. To get around this issue, PSPS mode needs to allow DEVs to request intervals in multiples of wake-beacon-intervals. However given the quantization of the time durations involved and other drawbacks of the scheme, it is not recommended to retain this scheme. Remove PSPS mode update from the draft and retain the APS mode as in D10However the PS status bit map is useful and hence retain that as applicableto APS instead of PSPS mode. This includes retaining APS related commandsin clause 7 in D10. **Suggest accept in principle:** "The first part (1) of this comment is accepted in principle based on the retention of SPS to allow custom power saving intervals. The APS part of the comment (2) should be satisfied by adding in "HIBERNATE mode". I suggest that the text describing HIBERNATE mode be inserted between the section describing SPS mode, 8.13.2, and the section describing the creation and use of SPS sets, 8.13.2.1. This is located on page 208, line 8. The text follows:

HIBERNATE mode allows a DEV to conserve power for extended periods until it chooses to listen for a beacon. The only responsibility of a DEV in HIBERNATE mode is to communicate with the PNC before the end of its ATP interval in order to preserve its membership in the piconet (see {xref} section 8.3.4).

MkS note: This text should be inserted at the end of 8.13, on page 214, line 33. The text follows:

If the DEV wants to change its mode from ACTIVE to HIBERNATE, the DEV shall send the PS change command, {xref} 7.5.7.1, to the PNC with the power save mode field set to HIBERNATE. The PNC shall then set the bit for the DEV in the SPS IE that corresponds to a virtual SPS set 0 (0 means HIBERNATE mode). If the DEV is the source or destination of any streams, the PNC shall terminate those streams, {xref} 8.5.1.3, when the DEV changes to HIBERNATE mode. If the DEV wants to change its power save mode from HIBERNATE to ACTIVE, the DEV shall send the PS change command, {xref} 7.5.7.1, to the PNC with the power save mode field set to ACTIVE. The PNC shall then no longer set the bit for that DEV in the SPS IE 0.

MkS note: In addition we need to add the HIBERNATE parameter anywhere where SPS and PSPS are now listed in sections 6 and 7.

Accept suggested resolution (new text due by Tuesday 30 September, 2002, Schrader/Bain).

320 (Heberling, TR) - Change 8.5.1.2, [PM/PSPS] Some parts of 02/276r6 resolution [14] missed regarding PSPS. MSC in Figure 207 has old PSAVE name./KO See resolution for 8.13.1 in 02276r7P802-15_TG3-commentsD11_KO.doc, Resolution [14] **Suggest accept in principle:** "Change 8.13.1, page 206, line 44-45 to be: 'The PSPS bitmap in the beacon shall serve as indication to a DEV that its peer has gone into PSAVE mode. The PNC may (shall ?) omit the PSPS status bitmap from the beacon if none of its DEV are in PSPS mode.', Add on page 206, line 54: 'The PNC is not required to align subrate allocations for a PSAVE DEV with the system wake beacon.' In the MSC on page 207, Figure 130, change PSAVE to be PSPS in the MLME_PS_MODE_CHANGE.req."

Accept in principle, "Change 8.13.1, page 206, line 44-45 to be: 'The PSPS bitmap in the beacon shall serve as indication to a DEV that its peer has gone into PSPS mode. The PNC shall omit the PSPS status bitmap from the beacon if none of its DEV are in PSPS mode.', Add on page 206, line 54: 'The PNC is not required to align subrate allocations for a PSPS DEV with the system wake beacon.' In the MSC on page 207, Figure 130, change PSAVE to be PSPS in the MLME_PS_MODE_CHANGE.req."

509 (Gubbi, TR) - PS status bit map has an issue and that is, let's say DEV-A and DEV-B are members of the same piconet managed by a PNC. If DEV-A sees the PS-status-bit corresponding to DEV-B as set in the beacon from PNC (meaning DEV-B is in power save mode), but in the same superframe receives a frame (directed or not) from DEV-B, can DEV-A assume that the DEV-B is in AWAKE state for that superframe? I think that should be allowed. it helps certain BC/MC traffic transactions. 1. If a DEV in in PSPS (APS) mode in a superframe, but transmits a frame the DEV shall consider itself in AWAKE state and hence may enter SLEEP state only after another succesful transaction of power-save-commands(s) with PNC. AND 2. The DEV shall enter SLEEP state only at the start of superframe following the succesful transaction of power-save-commands(s) with PNC. **Suggest accept in principle:** "1. A DEV in PSPS keeps it's GTS and may transmit in them. This does not imply that the DEV wishes to change power save mode. 2. It is specified in 13.1 that a DEV may enter the SLEEP state only after having received an ACK from PNC on a PS mode change command with the PS Mode set to PSPS."

Accept suggested resolution.

3.5.1 Others

130 (Heberling, TR) - [IE/Capabilities] Add parameters for capabilities etc./KO. Add parameters to MLME-START.request: MaxAssociations, MaxCTRB, SupportedDataRates. **Suggest accept in principle:** "Add MaxAssociations and MaxCTRB to the MACPIB in the PNC PIB group as 'MACPIB_MaxAssociations; 2; As defined in {xref association request}; static', add 'MACPIB_MAXCTRBs; 2; As defined in {xref association request, static'. The supported data rates are PHY dependent are are defined in 11.7 as PHYPIB_DataRateVector. The MLME can retrieve this using the MLME-GET.xxx commands."

Accept suggested resolution.

225 (Heberling, TR) - [ChnlChng] The change of channels takes effect just before the first beacon after the countdown. The superframe after countdown=0 is still on the old channel.This is necessary to allow uninterrupted data exchange./KO Change text to:If the change type is CHANNEL, the new channel field is set to the channel where the first beacon after the beacon with the countdown field equal to 0/zero will be sent. Otherwise this field shall be ignored upon reception. **Suggest accept in principle:** "Change the first sentence to read 'If change type is set to CHANNEL, the new channel index field is set to the new channel that will be used after the countdown has completed as described in {xref 8.11.1}'"

Accept in principle, “If the change type is CHANNEL, the new channel field is set to the channel where the first beacon after the beacon with the countdown field equal to zero will be sent. Otherwise this field shall be ignored upon reception.”

288 (Heberling, TR) - [ChnlChng] Replace the first paragraph of 8.11.1 starting at line 30 and ending at line 35 with this text: "The PNC may intiate dynamic channel selection, if it determines the conditions of the current channel in which it is operating are unsatisfactory and that there exist one or more other channels with better characteristics. The PNC has three mechanisms, at its disposal, to determine its current channel condition. These mechanisms are:1) Requesting one or more member DEVs to report their channel status information as described in {xref: 8.9.3} via the channel status response command {xref: 7.5.6.2}.2) Requesting one or more member DEVs to perform a remote scan {xref: 8.9.4} of the current channel and reporting their results via remote scan response commands {xref: 7.5.6.4}. 3) Performing self scans of the current channel as described in {xref: 8.9.5). In addition, the PNC may use the remote channel scanning and PNC channel scanning procedures to determine whether the conditions in other channels are better than the conditions in its current channel.The algorithm for deciding whether to change channels, is outside the scope of this standard. Please make the requested changes for these reasons:1) The text is better organized, 2) easier to understand, and 3) much more succinct. **Suggest accept in principle:** “Change the paragraph to read:

‘The PNC may intiate dynamic channel selection, if it determines the conditions of the current channel in which it is operating are unsatisfactory and that there exist one or more other channels with better characteristics. Three of the mechanisms that the PNC has at its disposal to determine the current channel condition are:

1) Requesting one or more member DEVs to report their channel status information as described in {xref: 8.9.3} via the channel status response command {xref: 7.5.6.2}.
2) Requesting one or more member DEVs to perform a remote scan {xref: 8.9.4} of the current channel and reporting their results via remote scan response commands {xref: 7.5.6.4}.
3) Performing self scans of the current channel as described in {xref: 8.9.5}.

In addition, the PNC may use the remote channel scanning and PNC channel scanning procedures to determine whether the conditions in other channels are better than the conditions in its current channel. The algorithm for deciding whether to change channels, is outside the scope of this standard.’”

Accept suggested resolution.

290 (Heberling, TR) - [ChnlChng] The second paragraph of subclause 8.11.1 is technically a mess. It inserts a description of the PNC's self channel scanning procedure into the middle of a description regarding the channel change procedure. It would be much better to seperate these two procedures into seperate subclauses: a) 8.9.5 PNC channel scanning b) 8.11.1 Dynamic Channel Selection.Consequently, perform these three operations:1)Move all of paragraph 2 (Lines 37-42) to a new subclause 8.9.5 PNC Channel Scanning.2) delete the first two sentences of paragraph three (lines 44-45) they will become unnecessary.3) Add this sentence at the beginning of paragraph 3, subclause 8.11.1. : "If the PNC determines after performing its own scan of other channels, or requesting member DEVs to perform remote scans on its behalf that there are one or more other channels with better characteristics than exist in its current operating channel, then the PNC may decide to initiate the dynamic channel change procedure. In the case where the PNC decides to initiate a dynamic channel change, the PNC shall broadcast the piconet parameter change information element, 7.4.6, in its current channel via its beacon for up to a NmbrOfChangeBeacons. ..." Please make the indicated change. **Suggest reject:** “The PNC is required to check for itself that the new channel is clear before it moves the piconet to it. Since the PNC is the center of the piconet, it is best able to determine if the channel is clear before it changes channels. The change proposed removes the requirement that the PNC check the new channel before changing to it. The PNC self channel scanning procedure is required only for this process and so its description belongs in this location. The PNC may use other techniques for scanning channels at other times, but it is required to check for itself the quality of the channel, just as it does when it starts a piconet.”

Tabled for email resolution.

294 (Heberling, TR) [Scan/PNC] Subclause 8.11.1 Paragraph 2 Line 37-45 makes reference to a PNC scanning procedure which is incompletely defined in clause 8.11.1. Consequently, use this text describing the PNC's procedure for determining the piconet's channel quality: <New text>:8.9.5 PNC channel scanning-PNC channel scanning is a procedure by which the PNC may determine the channel characteristics of not only its current operating channel but also the channel characteristics of one or more alternate channels. The PNC may use the results of its channel scans to determine whether the current channel in which it is operating has acceptable characteristics or there is one or more other channels with better channel characteristics than its current channel. If the characteristics of the current channel are acceptable, the PNC shall continue operating its piconet in the current channel. If, however, the channel characteristics are unacceptable, and there exists one or more alternate channels with better characteristics than the current channel, the PNC may initiate a dynamic channel change {ref: 8.11.1} to a channel with better channel characteristics. The algorithm for determining when to change channels is outside the scope of this standard.The PNC may optionally allocate CTAs to itself such that there is quiet time during the superframe for it to scan its current channel for other 802.15.3 piconets, non 802.15.3 wireless networks, or interference. If the PNC, after scanning its current channel, determines that the channel characteristics are unacceptable, the PNC may initiate channel scans of one or more other channels to determine whether there is an alternate channel with better characteristics than its current channel. While performing a scan of an alternate channel, the PNC shall not transmit a beacon for one or more beacon intervals. The PNC shall not suspend beacon transmissions for more than twice aMinChannelScan. The PNC, upon returning to its current channel and resuming the transmission of its beacons, shall increment the beacon number field by the number of beacons not sent during the time the PNC was scanning one or more alternate channels. The algorithm used to determine whether the characteristics of an alternate channel are better or worse than the current channel characteristics is outside the scope of this standard. The PNC after scanning its current channel and other channels may decide upon one of these actions:1) do nothing since the PNC determined that none of the alternate channels were better than its current channel2) initiate the dynamic channel change procedure described in {xref: 8.11.1}3) increase/decrease the Max Tx power level of the piconet {xref: 7.3.1, 8.11.2.1}4) initiate some other unspecified vendor specific action. **Suggest reject:** "The scanning procedure in 8.11.1 is only required when the PNC is looking to change channels and so it makes sense editorially to keep this description with the channel change description. Any other time that the PNC wished to scan for interference in the current channel or to assess the characteristics of other channels is already allowed since the standard does not prohibit it. The method that the PNC uses to make these additional scans is implementation dependent and therefore is outside of the scope of this standard. In the case of where the PNC is changing channels, it is important to require the PNC to first check the new channel to ensure that, from its point of view, the channel is quiet. The suggested text repeats information that is already in 8.11.1 and 8.11 and does not add any new information or technical requirements. See also the resolution of CID 290."

Table for email resolution.

291 (Heberling, TR) - [MTS] The MTS stream ID is sufficient to identify an MTS in the CTA since that ID shall not be used for anything else. Change first sentence to:"Management Time Slots (MTSs) are identical to GTSs except that the streamindex is set to the MTS stream index, 7.2.5" **Suggest reject:** "While it is true that the MTS stream ID is used in a CTA, it is also a requirement that the PNCID is either the source or the destination ID of the CTA. Thus the current sentence is correct in stating that both are requirements for identifying an MTS."

Resolution is to reject.

293 (Heberling, TR) - [MTS] MTS interval may be requested, as agreed in Schaumburg (ref 02/276r6 Resolution [19]/KO Add text: A DEV May request MTS allocation more or less often my sending a Channel Time Request command to the PNC with the Stream Index set to the MTS stream index, 7.2.5, and the CTR-Interval, 7.5.5.1, set to the DEV's desired interval for dedicated MTS. All other parameters of the CTRB shall be set to 0 and may be ignored by the PNC upon reception. **Suggest accept in principle:** "Add the fol-

lowing to page 173, line 31, ‘A DEV may request the frequency of MTS allocations by sending a channel time request command, {xref 7.5.5.1}, to the PNC with the stream index set to the MTS stream index, 7.2.5, and the CTR interval, 7.5.5.1, set to the DEV's desired interval for uplink MTSs. All other parameters of the CTRB shall be set to 0 and may be ignored by the PNC upon reception.’”

> Accept in principle “Add the following to page 173, line 31, ‘A DEV may request the frequency of MTS allocations by sending a channel time request command, {xref 7.5.5.1}, to the PNC with the stream index set to the MTS stream index, {xref 7.2.5}, and the CTR interval, {xref 7.5.5.1}, set to the DEV's desired interval for uplink MTSs. All other parameters of the CTRB shall be set to 0 and may be ignored by the PNC upon reception.’ Delete the two sentences on page 172, lines 47-48, ‘A DEV may also request that the PNC adjust the repetition rate of open MTSs for the piconet using the channel time request command, 7.5.5.1. The PNC may either grant or reject the request.’”

55 (Gilb, TR) - When requesting a change to MTS allocations, only the CTRB fields CTR-interval and CTR-interval type = 1 has a meaning. All other fields/values should be ignored/rejected. PNC decides duration, dest-ID (implied) and all other params. The DEV can ask for MTS every N superframe, nothing else. Add appropriate text as indicated. **Suggest accept in principle:** “Resolve as indicated in CID 293.”

> Accept suggested resolution.

412 (Gubbi, TR) - In D10 the start of Information element was adjusted to be from even pos (2 octets) to help implementations having to deal with octet level searching for the start of required IE. Complexity involved in octet level searching is too much for low-cost implementations. This will also halve the computations needed in implementations that use higher size ords (like 4-octet). Put back the paragraph that mandated the start of an IE at even position of octets and hence the padding of a zero if an IE whenever the total size of that IE is odd number. **Suggest accept in principle:** “The frame formats specified only shows the bits sent over the air. Implementations of the receiver functions of a DEV are free to pad and rearrange to any word length, endian or bitorder they may choose to optimize the interface to their host.”

> Reject “The frame formats specified only shows the bits sent over the air. Implementations of the receiver functions of a DEV are free to pad and rearrange to any word length, endian or bit order they may choose to optimize the interface to their host. This issue was discussed multiple times before the TG agreed to make the change.”

314 (Heberling, TR) - [ParmChng] Two errors in text, dependent PNC shall copy parent IE and the trigger for changing channels is ChangeType=CHANNEL/KO. See resolution for 8.10 in 02276r7P802-15_TG3-commentsD11_KO.doc, Resolution [11]. **Suggest accept in principle:** “Resolve as indicated in CID 317.”

> Accept suggested resolution.

388 (Gubbi, TR) Same as comment #548 in LB12. ORIGINAL COMMENT (LB12) Without SDL there is an higher risk of non-interoperable implementations CommentEnd: ORIGINAL SUGGESTED REMEDY (LB12) Provide formal description of the MAC and PHY. SDL can be one option. ORIGINAL Response: PROPOSED REJECT. The committee does not want to add normative content that may conflict with the other clauses. Informative content will not be available until at least 3 months after the final draft has been approved. SDL clause will be removed from the draft and left for a follow on project. REBUTTAL: While it is agreed that ideally all clauses in a standard must be coherent and non-conflicting with each other, it is well known that textual descriptions can be vague at many places even after many reviews. On the other hand, formal descriptions do not have that problem since the checks and reviews are done by tools in addition to human reviews. Also note that it is virtually impossible to avoid repeatition of information in textual description due to the very nature of such description. This repetition leads to inconsistencies and hence resulting in multiple intepretations of the same operation. Formal descriptions can be written to have NO repititions of the same operation anywhere and hence provide unique interpretation. **Suggest reject:** “This comment reviewer agrees with the commenter that SDL is an excellent formal language which is capable of

providing an unambiguous description of the 15.3 specification. In addition, it is agreed that the validation capability of the SDL would enable a rigourous method for validating the 15.3 protocol. Given the benefits that an SDL model would provide, the real reason for SDL not being part of the 15.3 standard has more to do with the fact that the SDL modeling capable individuals currently working with the 15.3 standards committee are constrained by corporate concerns regarding the release of a corporately developed model to the wider community. This is a topic of discussion we have had with the IEEE editors over the past couple of years. One of the recommendations resulting from one such discussion is for the IEEE standards body to institute a policy, similar to ETSI's, whereby the IEEE publishing organization provides an SDL editor to each task group to assist each task group in the development of its standard. This is the most promising approach to resolving this issue. In the mean time, the 15.3 standards team has expended much effort to include detailed message sequence charts to augment the text describing the functional behaviour of the 15.3 MAC protocol with the hopes of mitigating some of the concerns the commenter has raised in his comment. In short, the BRC recommends that this comment be rejected for the reason that the IEEE publishing organization has not provided an SDL editor to assist the 15.3 standards committee in developing an SDL model."

Resolution is to reject.

183 (Heberling, TR) - [FrmFrmt/Payload] replace aMaxFrameSize-4 with aMaxPayloadSize which is equal to aMaxFrameSize-4. A CID 255 from LB17, although withdrawn, indicated the confusing nature of the text. Also change this sentence frag <from> "...the number of actual information octets by 12." <to> "...the aMaxPayloadSize by 12 octets." Please make the indicated changes. Suggest accept in principle: "CIDs 97(TR), 188(E), and 190(E) also address the current short comings in the text and placement of the Payload and FCS field descriptions. Consequently, it is recommended that 1) clause 7.2.7 be deleted 2) the current clauses 7.2.7.1 and 7.2.7.2 be promoted to 7.2.8 and 7.2.9 respectively after being moved to just after the the Secure MAC frame body subclauses which currently occupy clauses 7.2.8, 7.2.8.1, 7.2.8.2, 7.2.8.3. Please note the Secure MAC frame body subclauses will be promoted to the 7.2.7, 7.2.7.1, 7.2.7.2, and 7.2.7.3 positions in the current text. 3) Modify the text in clause 7.2.7.1, which will become 7.2.8, to read as follows:

'7.2.8 Payload field

The payload is a variable length field and contains information specific to individual frame types. When the SEC bit is set to 0, the minimum payload is zero octets and the maximum payload length is aMaxPayloadSize, which is equal to aMaxFrameSize-4 octets.

When the SEC bit is set to 1, the minimum payload is 12 octets (|IntegrityCode(8)|EncryptedData(0)|SFC(2)|SECID(2)|) and the maximum payload length is aMaxPayloadSize in which aMaxEncryptedData is equal to aMaxPayloadSize-12 octets.'

4) Modify Figure 6, page 105 to look like this:

|FCS|IntegrityCode|EncryptedData|SFC|SECID|

| |_____Payload_____|

|_____Secure MAC FrameBody _____|"

Suggest accept in principle, "Resolve as indicated in CID 97, modify Figure 6, page 105 to look like this:
|FCS|IntegrityCode|EncryptedData|SFC|SECID|
| |_____Payload_____|
|_____Secure MAC FrameBody _____|"
Add a new figure between figure 5 and figure 6 that is the Non-secure MAC Frame body:
|FCS| Data ||
| |_Payload_|

|_Non-secure MAC FrameBody _|”
Change ‘Payload field’ to be ‘Data field’ in the title and in the text”

Table until we get all the text in one place, ADH to provide suggestion, possibly use MPDU?

3.5.2 CTA status IE/command

CIDs - 299, 301, 303, 305, 208, 71, 493.

71 (Gilb, TR) - The is currently no way for a DEV to request the channel time response information if it missed it. Change CTA response command to send IEs or simply declare the IEs to be sent with the probe command. Either way, this lets the DEV request the information if it thinks that it lost it. This would also give us an easy way to send multiple confirms in one CTA response command. **Suggest accept in principle:** “Add a new IE to request the CTA status, formatted text in 02392r8. Add text to 8.9.2 Probe: ‘A DEV may request information about an isochronous stream by sending a probe command with the CTA status request IE with the stream index set to the stream index of the stream for which CTA information is requested. The DEV shall not set the bits for either the CTA status IE or the CTA request status IE in the information request field. If the stream index is set to 0, the DEV is requesting information about all isochronous streams directed to the OrigID and to BcstId and McstId. The PNC shall respond to a probe command with the CTA information request IE by sending a probe command with the appropriate CTA status IE(s), {xref 7.4.x }.’ Add to the probe tables that the new IE may be sent by a DEV to the PNC, not by a PNC to a DEV and not by a DEV to a DEV. Also add to the appropriate probe table this new IE may not be requested by anyone.”

(begin new IE text)

7.4.x CTA status request

The CTA status request IE is used by a DEV to request the CTA status IE for an isochronous stream. The CTA status request IE shall be formatted as in Figure 18.

octets: 1	**1**	**1**
Stream index	Length (=1)	Element ID

Figure 18—CTA status request information element format

The stream index indicates the stream allocation for which the DEV is requesting information.

(end new IE text)

Accept suggested resolution.

Meeting adjourned at 10:30 am PDT.

3.6 Email resolution, due 30 September, 2002

131 (Heberling, TR) - [Start] Remove all the parameters listed under the MLME-START.confirm primitive except the ResultCode. The start functionality described in clause 8.2.2 no longer includes a scan process except to verify that the chosen channel is still clear. Please make the requested technical change. **Suggest accept**.

132 (Heberling, TR) - [Start] Pass back only parameters that can be changed by MLME or PNC/KO. Delete all parameters from MLME-START.confirm except (ResultCode) **Suggest accept**

147 (Heberling, TR) - [Start] Change this sentence fragment: 1) <from> "If another piconet is already established,..." <to> "If the piconet is already established,..." 2) Split this sentence fragment <from> "If all of the channels for the PHY are either occupied by other 802.15.3 piconets or have unacceptable interference, ..." <to> "If all the channels for the PHY are occupied by other 802.15.3 piconets, ..." <and> " If all the channels have unacceptable interference, then the ResultCode shall be set to "CHANNEL-NOISY(or CHANNEL-IMPAIRED)". Please make the requested change. **Suggest accept**

459 (Gubbi, TR) - [Start] Although I think it is against the intention, the text seems to overburden the task of starting piconet. DME needs some channel statistics to decide on channel, which I presume obtained at the time of scanning procedure. Then DME decides the channel. The text further imposes that DEV check for channel being clear and then start a piconet. If DME has already taken the channel stats into account and has decided the channel (a) this causes the DEV to second check the channel which is waste of time and overhead for implementations and (b) Especially the last sentence in the para that mandates (use of shall) return of failure without starting a piconet contradicts the next (new) para where a capable DEV can start a neighbor (or child) piconet in a channel where a piconet already in existence. Change all "shall" to "may" in the para and let implementors decide which of the three solutions they want in their products **Suggest accept in principle:** “There has been considerable debate whether a PNC capable DEV should initiate a second scan of the channel prior to the DEV transmitting its first beacon as a PNC. The consensus arrived at was that during the time that the PNC-DME was evaluating the results of its first scan that a second DEV could have initiated a piconet in a channel that the first DEV originally scanned as being clear. Consequently, it was decided that a second scan just prior to transmitting the first DEV's beacon was a good interference mitigating practice.

Item (b): I agree that returning an error code indicating a failure is not descriptive enough. However clause 6.3.3.2.2 does describe in more detail which ResultCode is to be returned and I believe addresses the commenters concern regarding the lack of detail in the sentence in line 13-15 on page 155. In addtion, I agree that there is need for a sentence at the end of the sentence in line 15, page 155, that states that the DEV-DME upon receiving the failure code may decide to change to a diferenct channel 8.11.1 or become a child or neighbor piconet of the other piconet. Now in regards to the paragraph starting on line 17 page 155, this paragraph is describing the behaviour of the PNC after it is already established not after performing its second scan.”

170 (Heberling, T) - [MultiCast] MLME-MULTICAST-RX-SETUP.request is not referenced anywhere in clause 8.Should it affect reception filtering?/KO. Decide what it shall do and add it to clause 8. **Suggest accept in principle:** “This primitive is only used at the higher levels of the MAC and does not affect (other than in implementation dependnet ways) the operation of the MAC. Since it does not change the on-air behavior of a DEV, there is no need to mention it in clause 8. For example, MLME-RESET and MLME-SYNCH are not mentioned anywhere but in clause 6 since they only affects that interface.”

3.7 Friday, 20 September, 2002

Meeting called to order at 1:07 pm PDT.

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

64 (Gilb, TR) - IN B.3 it references a to-be-published reference, which is a big no-no and quite silly. Delete the references to RFC 3280 and RFC 3278. **Suggest accept in principle**: “Change the typo on Page 347, line 19: RFC 3278 should be RFC 3279. On page 347, lines 17 and 19, delete ‘(soon to be published)’. Add

the following references to the bibliography and put in the appropriate cross-references on page 347 (see 02/392r7 for formatted text).

[B1] RFC 3279, L. Bassham, R. Housley, W. Polk, “Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) profile”, Internet Request for Comments 3279, April 2002. See also http://www.faqs.org/rfcs/rfc3279.html.

[B2] RFC 3280, W. Ford, R. Housley, W. Polk, D. Solo, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, Internet Request for Comments 3280, April 2002. See also http://www.ietf.org/rfc/rfc3280.txt.”

Accept suggested resolution.

3.7.1 Security issues

104 (Gilb, TR) - After the authentication process has been completed, all security suites behave in an interoperable manner. Text should be added to clause 9 indicating that a PNC may support multiple security suites in the same piconet. **Suggest accept in principle**: “On page 226, lines 9-11, change this paragraph in sub-clause 9.4 to the following: ‘A security suite defines mechanisms that may be used to perform the authentication process. A security subsuite, identified by a unique OID, specifies the operations within a security suite for performing authentication. After two DEVs perform the authentication process using any security suite, the two DEVs share keying material for use in the symmetric operations defined in {xref - 10.2.4}. The PNC may perform the authentication process using different security suites with different devices in the same piconet, since the resulting keying material will be of the same form in all cases. The list of accepted security suites and subsuites are specified in clause {xref - 10}.’”

> Accept in principle “On page 226, lines 9-11, change this paragraph in sub-clause 9.4 to the following: ‘A security suite defines mechanisms that may be used to perform the authentication process. A security subsuite, identified by a unique OID, specifies the operations within a security suite for performing authentication. After two DEVs perform the authentication process using any security suite, the two DEVs share keying material for use in the symmetric operations defined in {xref - 10.2.4}. The PNC may perform the authentication process using different security suites with different devices in the same piconet, since the resulting keying material will be of the same form in all cases. The list of accepted security suites and subsuites are specified in clause {xref - 10}. While the security suites are interoperable, it is possible that there are differences in the levels of security provided as described in {xref C.x}’ {ed note this is where the bit strengths is discussed}.”

113 (Gilb, TR) - There is no longer a mandatory sub-suite. Change last sentence in this paragraph to: “The list of accepted security suites and sub-suites are specified in clause 10.” **Suggest accept in principle**, “Resolve as indicated in CID 104.”

Accept suggested resolution.

115 (Gilb, TR) - Since the symmetric cryptography building blocks are shared by each security suite, there is no reason to reference them in the security suites themselves. Make sub-clause 10.2.4 a stand alone section that does not relate to the security suites. Each security suite should deal only with the authentication operations and the reference to 10.2.4 from the security suites should be removed. **Suggest accept in principle:** “Page 275, lines 36-37: Replace the text at the beginning of 10.2.4 with the following: ‘An authenticated DEV operating in a secure piconet or a DEV that is authenticated with a peer DEV shall protect frames using the symmetric cryptography building blocks specified in {xref new sub-clauses}.’ Page 276, lines 53-54: Replace the text at the beginning of 10.2.5 with the following: ‘An authenticated DEV operating in a secure piconet or a DEV that is authenticated with a peer DEV shall protect frames using the symmetric cryptography operations specified in the following sub-clauses.’ Page 282, lines 40-41: Change the text in 10.3.2.1 to the following: ‘All sub-suites of the ECMQV Koblitz-283 security suite shall perform the symmetric operations within the authentication protocol as specified in the following sub-clauses.’ Remove the sentence

'The symmetric operations performed in this security suite are those specified in 10.2.5.' from 10.4 on page 289 linhe 16. Remove the sentence 'The symmetric operations performed in this security suite are those specified in subclause 10.2.5." from 10.5 on page 291 lines 29-30.'

> Accept in principle, "Page 282, lines 40-41: Change the text in 10.3.2.1 to the following: 'All ECMQV Koblitz-283 security sub-suites shall perform the symmetric operations after authentication as specified in {xref 10.2.5}. All ECMQV Koblitz-283 security sub-suites shall perform the symmetric operations within the authentication protocol as specified in {xref 10.3.2.1.1 and 10.3.2.1.2}.'"

384 (Barr, TR) - MAC PIB ACL group defined as an array whose contents are defined in Table 33. All of the entries are dynamic, but no clear mechanism to update these entries has been included in the draft. There are no limits on the minimum and maximum number of entries allowed in the ACL. The only use for this array in the MAC is for generation of the CCM nonce and obtaining the keys associated with a particular SECID for encoding or decoding payloads. Either remove the MAC PIB ACL or add appropriate method for updating the information in the array. If the ACL is kept, add limit for the minimum number of ACLs that must be supported for a DEV, SM, and PNC. Provide a mechanism for updating and accessing the contents of an ACL entry. Suggest defining MLME commands for doing this using an index to the array. Add MAC PIB entries to indicate last index used in the array. Finally, clarify relationship between DEVHost and MAC regarding use and management of informaiton in the ACL. **Suggest accept in principle:** "Delete the subclause 6.5.6. Insert a new subclause in 6.3 with the text given in 02/392r7.

(begin new text for CID 384)

3.7.2 Initializing and Updating SECID Information

This primitive is used to initialize or update the management security information associated with a new SECID as the result of an authorization process. The parameters used for the MLME-SECID-UPDATE primitive are defined in Table 11..

Table 11—MLME-SECID-UPDATE primitive parameters

Name	Type	Valid Range	Description
ManagementSECID	Integer	Any valid SECID as defined in {xref }	Specifies the security session ID for the management key.
TrgtID	Integer	Any valid DEVID as defined in {xref 7.2.3.}	The DEVID of the target DEV for this relationship.
SecurityManager	Boolean	TRUE, FALSE	This DEV is the security manager for this relationship.
KeyInfoLength	Integer	0-255	Length of ManagementKeyInfo
ManagementKeyInfo	Octet string	Any valid key	The key agreed upon during authentication that are used for protecting commands.

3.7.2.1 SECID-UPDATE.request

This primitive requests that the SECID and management keying information associated with the DEV be included or updated. The semantics of the primitive are as follows:

```
MLME-SECID-UPDATE.request   (
                            ManagementSECID,
                            TrgtID,
                            SecurityManager,
                            KeyInfoLength
                            ManagementKeyInfo
                            )
```

The primitive parameters are defined in Table 11.

3.7.2.1.1 When generated

The DME sends this request to the MLME after completing authentication with the PNC or a peer DEV.

3.7.2.1.2 Effect of receipt

The MLME adds this SECID to the list of authenticated SECIDs that can be used to protect command data with the target DEV in this authentication relationship.

(end new text for CID 384)

Table until Tuesday 24 September, 2002. Look for consensus on email.

3.7.3 Others

430 (Gubbi, TR) - The changes in command frames (Assoc and disassoc) have rendered this IE useless. Where is this IE used? Remove this IE and move the defintion of "capability field" to 7.4.4 whereit is used first. **Suggest accept in principle**: “The only command which includes the Capability Information IE is the probe command. DEVs in the piconet receive the capability information for a DEV when it associates and the PNC broadcasts a PNC Information Command for all DEVs in the piconet. This information is also periodically broadcast by the PNC. A DEV can also request the capability info for a DEV from the PNC using the PNC Information Request command. Therefore, there is no need for the Capability Information IE to exist. Delete clause 7.4.11. Move Figure 36 - Capability field format and associated field description text to clause 7.5.1.1 replacing the text "The capability field is defined in 7.4.11". Note that clause 7.5.1.1 is the first location to use the two byte capability field as this field has been removed from the DEV Association IE. Replace all further occurrences of "The capability field is defined in 7.4.11" with "The capability field is defined in 7.5.1.1". Replace all references to "7.4.11" regarding the capability field with a reference to "7.5.1.1". Remove all references to "7.4.11" regarding the Capability Information IE. In clause 8.12, remove method "b" and rename method "c" method "b". In clause 11.7, replace the text "The encoding of the supported PHY data rates used in the capabilities information element, 7.4.11," with "The encoding of the supported PHY data rates used in the capabilities field defined in 7.5.1.1,’”

Reject, “The IE is used to request information from a DEV about its supported data rates as decribed in 8.12, page 205, line 36.”

227 (Heberling, TR) - [IE/DEVAddr] DEV Adress is no longer needed as an element since the beacon contains the BSID and not the MAC address of parent and dependents. It is not used anywhere in the standard./ KO. Delete this element/clause. **Suggest accept**.

Accept.

429 (Gubbi, TR) - Where is this "DEV address" IE used? I can't see any use for it since atall places there seems to be direct 6-octet field for the same purpose. Remove this IE. **Suggest accept**.

Accept.

460 (Gubbi, TR) - Removal handover timeout: What if the DEV to which the handover is happening dies or its power is plugged out? What does the PNC do in that case? Do NOT remove the timeout from the handover request command and hence in this paragraph. **Suggest reject**: "The new PNC cannot abort in the midst of the information transfer based on a remote timeout. The timeout only has a value for the DEV DME setting it. There is a local timeout in the old PNC, so that it can recover from a failed information transfer. The information transfer is considered completed when the handover response command has been received by the old PNC. At that time the old PNC starts the beacon countdown. This is the point of no return. After the countdown, the old PNC must stop sending beacons. Exception analysis:

1) Old PNC gets no handover response command before timeout:
   => hand over to other DEV, shut down or remain PNC (example in CID 460)
2) New PNC gets no ACK on handover response command
   => repeat command until retry limit. Wait for countdown beacons.
3) New PNC doesn't receives any countdown beacons.
   => remain as DEV. If no beacons received, considers itself disassociated after the ATP expires.
4) New PNC misses some countdown beacons, but get some
   => assume PNC role at the time for the first beacon after the countdown.

No other exceptions have been identified."

Resolution is to reject.

491 (Gubbi, T) - Sentence "There is no guarantee of the length ...": Isn't CTRRespTime designed to provide this? - Remove this sentence - **Suggest accept in principle:** "The CTRRespTime is provided to DEVs to give them an approximation of the number of superframes for processing of commands. Change the sentence to 'There is no absolute guarantee of .... time allocation.' Then add 'The CTRRespTime {xref .. } is available to provide an average of the time the PNC is currently taking to process channel time requests.'"

Accept in principle: "The CTRRespTime is provided to DEVs to give them an approximation of the number of superframes for processing of commands. Change the sentence to 'There is no absolute guarantee of .... time allocation.' Then add 'The CTRRespTime {xref .. } is available to provide the average number of superframes the PNC is currently taking to process channel time requests.'"

455 (Gubbi, T) - There is a grave mistake here. This is not supposed to be "number of supported SPS sets" it is supposed to be "Number of existing SPS sets".What if a PNC supports 100 sets but only 3 are existing currently. How does the implementor is supposed to interpret this line in that case? PS: This this text has been there since D10, the comment is marked "Tech"only as opposed to "Tech-Req". The voter is aware that this comment maybe rejected since it is not a change from D10 to D11. **Suggest reject:** "This field is intended to communicate the number of SPS sets that are supported by the PNC. The number of sets currently defined may be determined counting the number of sets returned by this command (it returns all of them)."

Accept in principle: "This field is intended to communicate the number of SPS sets that are supported by the PNC. The number of sets currently defined may be determined counting the number of sets returned by this command (it returns all of them). To clarify this, following the sentence page 150, line 27, add 'The number of currently defined SPS sets is given by the number SPS set structures in this command.'"

395 (Gubbi, TR) - The sentence "All asynchronous traffic to DEVs in PSPS mode will be allocated in the wake beacon". What does this mean? if a DEV is in PSPS mode and there are 100 other DEVs requesting to send async data to it, all the 100 requests are allocated in the wake beacon? Why is this sentence needed. Remove PSPS and revert back to APS mode as in D10 of the draft. **Suggest accept in principle** "Change text to: "For asychronous time allocations to a destination DEV that is in either PSPS mode or SPS mode, the PNC shall not allocate any CTAs in superframes other than the awake superframes for that DEV." Part 2: This sentence is needed in order for the implementor to know what behavior to implement and to expect from PNCs. In this case the implementer needs to know that allocations will be made with an awarness of the correct superframes in which to insert them rather than in any superframe that is convenient."

Table until Tuesday,24 September 2002, JPKG to suggest new text via email.

3.7.4 PN Services

434 (Gubbi, TR) 1. The very concept of indicating "application layer" capabilities does not belong in MAC. This is a potential issue in sponsor ballot. If this is absolutely needed, there is application specific IE that can be used for this purpose. The payload of the "piconet services" IE is not defined in this draft anyway (that is, it is already vendor specific). 2. Inclusion of DEVID is redundant. Given that this IE is sent by a DEV in piconet to indicate its "application layer" capabilities, what is the need for adding DEVID here since the MAC header of the frame already contains the DEVID? - If possible remove this IE or at least remove DEVID. **Suggest reject**: "The DEVID is provided so that the associating DEV known which DEV in the piconet is providing a certain service. It is useful in reducing the thrashing after association to locate the DEV offering the service absent the DEVID.

PNServices provide a useful capability for DEVs considering membership in a piconet.

There is precious little information provided during scan procedures as to what services may be available to an associating DEV. The PNServices provides early information to associating DEVs of a broader range of DEV (application) information.

Application level information tagged to individual DEVIDs in a piconet and available early in the "connection" process is a valuable addition to this standard. PNServices are provided during association to reduce the time expended between scanning and payload delivery, a key performance parameter of this standard.

Devices that are sleeping need may not be able to respond to a new DEV trying to obtain information about it in a timely manner so having this information available via the PNServices IE is additional value.

This standard does not define the content of the information field. It only defines a method of carriage of information provided by DEVs to the PNC and at the appropriate time. The use of the registered vendor ID assures that devices sharing the same vendor ID will interoperate. Further, it is expected that the vendor ID will represent industry organizations as well as individual companies and thus a single vendor ID will cover a wide range of interpretation of the field information represented in the PNServices."

Resolution is to reject.

446 (Gubbi, TR) - The very concept of indicating "application layer" capabilities does not belong in MAC. This is a potential issue in sponsor ballot. If this is absolutely needed, there is application specific IE that can be used for this purpose with vendor specific command. The payload of the "piconet services" IE is not defined in this draft anyway (that is, it is already vendor specific). Let the vendor use the combination of "Vendor specific command" and "Vendor specific IE" and the freedom of command payload format to achieve whatever is desired in their products without causing any interoperability issues - Remove this command from the draft. **Suggest reject:** "See also the response to cid 434. The potential interoperability issues are handled by using a unique ID, the vendor ID, so that DEVs know which elements to interpret and how to do it."

Resolution is to reject.

438 (Gubbi, TR) - DEV utility field is unnecessary. Since piconet services are vendor specific this should be part of vendor-specific command that can be sent by any PNC or DEV at any time after the assoc/auth process is complete as per the needs of the implementation. - Remove DEV-utility field from Figure 45 and clause 7.5.1.1. **Suggest reject:** “The intent of PNServices is to provide the information early in the connection process. The DEV utility field indicates the desire of the associating DEV to receive information available from other DEVs in the piconet as “part of” the association process.”

Resolution is to reject.

479 (Gubbi, TR) - Another hoops to go through at PNC for this information that standard does not have any control on. LEt the vendors decide how to communicate that info. This is not the only vendor specific info that is communicated in implementations. - Remove any updates to this clause (and preferably the entire clause). **Suggest reject:** “The vendors do in fact determine how to communicate the information. The standard provides the vehicle for carriage of the information at the appropriate time in the DEV connection process.”

Resolution is to reject.

477 (Gubbi, TR) - First complete paragraph of cluse 8.3.2: It's disappointing to see how much time and energy has been wated on this piconet services IE given that there is very little use for it and the same can be better achieved by Vendor-specific commands and/or IE. If the pcionet services field definition is outside the scope of the standard how can that standard decide how this info is exchanged between DEVs? -Remove this exchange mechanism (and preferably the piconet services IE) from the draft. **Suggest reject:** “On the first part of the comment, there is a spelling error (associating) in line 54. The remaining portions of the comment are addressed in cid 438 and 434.”

Resolution is to reject.

478 (Gubbi, TR) - Third and fourth complete paragraph of cluse 8.3.2: It's disappointing to see how much time and energy has been wated on this piconet services IE given that there is very little use for it and the same can be better achieved by Vendor-specific commands and/or IE. If the pcionet services field definition is outside the scope of the standard how can that standard decide how this info is exchanged between DEVs? a probe from any interested DEV to another interesting DEV can obtain this IE. Why should PNC go through this hoops for this otherwise easily achivable task? Bottom line is, once a DEV comes to know of existence of another DEV in the piconet, through PNC, the second DEVs properties must be obtained by the first DEV by sending a SIMPLE, DIRECTED probe (req) and getting a probe (Response) in return. - Remove this exchange mechanism (and preferably the piconet services IE) completely from the draft. **Suggest reject:** “See CIDs 438 and 434. This IE and the exchange provides this information very early on in the association process. It also allows the DEV to find all of the capabilites in the piconet with being required to individually probe every single DEV in the piconet.”

Resolution is to reject.

13 (Gilb, TR) - References for "Association Status", "MaxAssignedCTAs", "MaxProcessedCTAs", and "ATP" are missing. More importantly, the reference for the octet "SPS Info" says "shall be formatted as illustrated in Figure 38 and is defined in 7.4.13." Figure 38 is a multi-octet element named "SPS Status", with no clear correlation to "SPS Info". Delete SPS info, add cross references that define "Association Status", "MaxAssignedCTAs", "MaxProcessedCTAs", and "ATP". The SPS information is passed in the SPS information command. **Suggest accept in principle:** “Delete SPS info, change the name of ‘Association Status’ in this command to be ‘Membership status’ and add the following definitions: “The membership status field shall be set to 0 if the DEV is associated but not authenticated and shall be set to 1 if the DEV is associated and authenticated.’, ‘The MaxAssignedCTAs field is defined in {xref 7.4.4.}’, ‘The MaxProcessedCTAs

field is defined in {xref 7.4.4.}' Ed. note: the Max{Assigned,Processed}CTAs fields may be modified or deleted as a result of CIDs 201, 206, 219."

Accept suggested resolution.

97 (Gilb, TR) - There is no description for the payload field and FCS field for the secure frame body. The text for Payload field and FCS field in sub-clause 7.2.7 should be duplicated or referenced in 7.2.8. **Suggest accept in principle:** "On page 108, line 30, delete the sentences 'The minimum payload is zero octets ... will reduce the number of actual information octets by 12.' since they are covered in 7.2. On page 104, line 42 add this sentence 'The maximum length includes the length of the security fields, if present.' Change 7.2.7.x and 7.2.8.x to 3rd level headings, and delete the old headings for 7.2.7 and 7.2.8. {Ed. note sychronize this with CID 147}."

Accept suggested resolution.

231 (Heberling, TR) - [IE/Capabilities] For handover, it is necessary to know if a DEV supports any power save modes./KO. Add to Figure 36 - capability field:b10: SPS Capableb11: PSPS CapableAdd text:The SPS Capable bit shall be set to 1 if the DEV is capable of administraring at least one SPS set as a PNC. Othwerwise this bit shall be set to 0.The PSPS Capable bit shall be set to 1 if the DEV as PNC is capable of generating system wake beacons and administrating PSPS requests. Otherwise this bit shall be set to 0. **Suggest accept in principle:** "Resolve as indicated in CID 273."

Accept suggested resolution.

Adjourned at 2:31 pm PDT

3.8 Thursday, 19 September, 2002

Meeting called to order at 8:06 am

Attendees: Allen Heberling, Knut Odman, Rene Struik, Dan Bailey, Ari Singer, John Barr, Jay Bain, James Gilb

533 (Bain, T) - The idea of sleep is perhaps greater than not receiving. It is at least not transmitting or receiving and perhaps reducing power in other portions of the DEV. Awake is also more than just receive. Make suggested change. **Suggest accept in principle**, "Resolve as indicated in CID 506."

Accept suggested resolution.

304 (Heberling, T) - [ChnlChng/MSC] The MSC for changing piconet parameters is flawed. Please make these changes:Place a hexagon spanning the PNC DME and MLME columns just below the last beacon w/ Piconet parameter change IE and just above the first beacon(on new channel). The text in the hexagon shall be: "PNC moves to new channel"Extend the current "DEV moves to new channel hexagon so that it spans both the DEV-1 MLME and DME columns. Please make the indicated changes. **Suggest accept**.

Accept.

58 (Gilb, TR) - Based on the clause 6 text, there should be an MLME-PNC-HANDOVER.ind after the DEV (now PNC) sends its first beacon. Add primitive to MSC. **Suggest accept**.

Accept.

232 (Heberling, TR) - [PNCHndOvr] Make these corrections to the MSC: 1) There are two DEV-2 MLMEs. Replace the one furthest to the right with a DEV-2 DME. 2) The MLME-PNC-INFO.cfm is incorrect. Replace it with an MLME-PNC-INFO.ind. Confirms are only used when a service layer receives a request from the layer above it. An indication is used when an unexpected signal is received. 3) Remove the MLME-NEW-PNC.ind primitive directed from the PNC MLME to the PNC DME. The PNC does not need to tell itself that there is going to be a new PNC. It already knows that. Please make the indicated changes. **Suggest accept in principle** "Accept in principle. "1) change as requested, 2) no change, it was decided to use the confirm signal in Monterey, 3) change as requested."

> Accept in principle, "1) change as requested, 2) no change, it was decided to use the confirm signal in Monterey, 3) change as requested. Add block in 02/275r9 that indicates the optional ACL handover."

269 (Heberling, TR) - [PNCHndOvr] Some errors in text remain or were introduced after LB17.MSC in Figure 91 is also wrong./KO Text changes for 8.2.3 and ne MSC for Figure 91 are all collected in:02276r7P802-15_TG3-commentsD11_KO.doc, Resolution [03]. **Suggest accept in princple**, "The MSC will be modified as indicated in the resolutions of CID 58 and 232. Make the following text changes: In 6.3.13.4, page 59, line 45, change 'This primitive informs the originating DME its request for information from the PNC is complete.' to be 'This primitive informs the DME that the MLME has received a PNC information command, {xref 7.5.4.2}.' In 7.5.3.1, page 138, line 20 'the number of information records to be transferred using the PNC information command frame(s).' to be 'the number of DEV information records, {xref PNC handover info command}, that will be transfered from the old PNC to the new PNC.' In 8.2.3 PNC Handover, delete page 156, line 8-9, redundant, same text in paragraph below. Add to page 156, line 19, 'The PNC handover information command shall not be sent if the PNC has indicated in the PNC handover request command that it does not have any CTRBs to transfer.

The SPS inquiry response command shall not be sent if the PNC has indicated in the PNC handover request command that it doesn't have any SPS sets to transfer.'

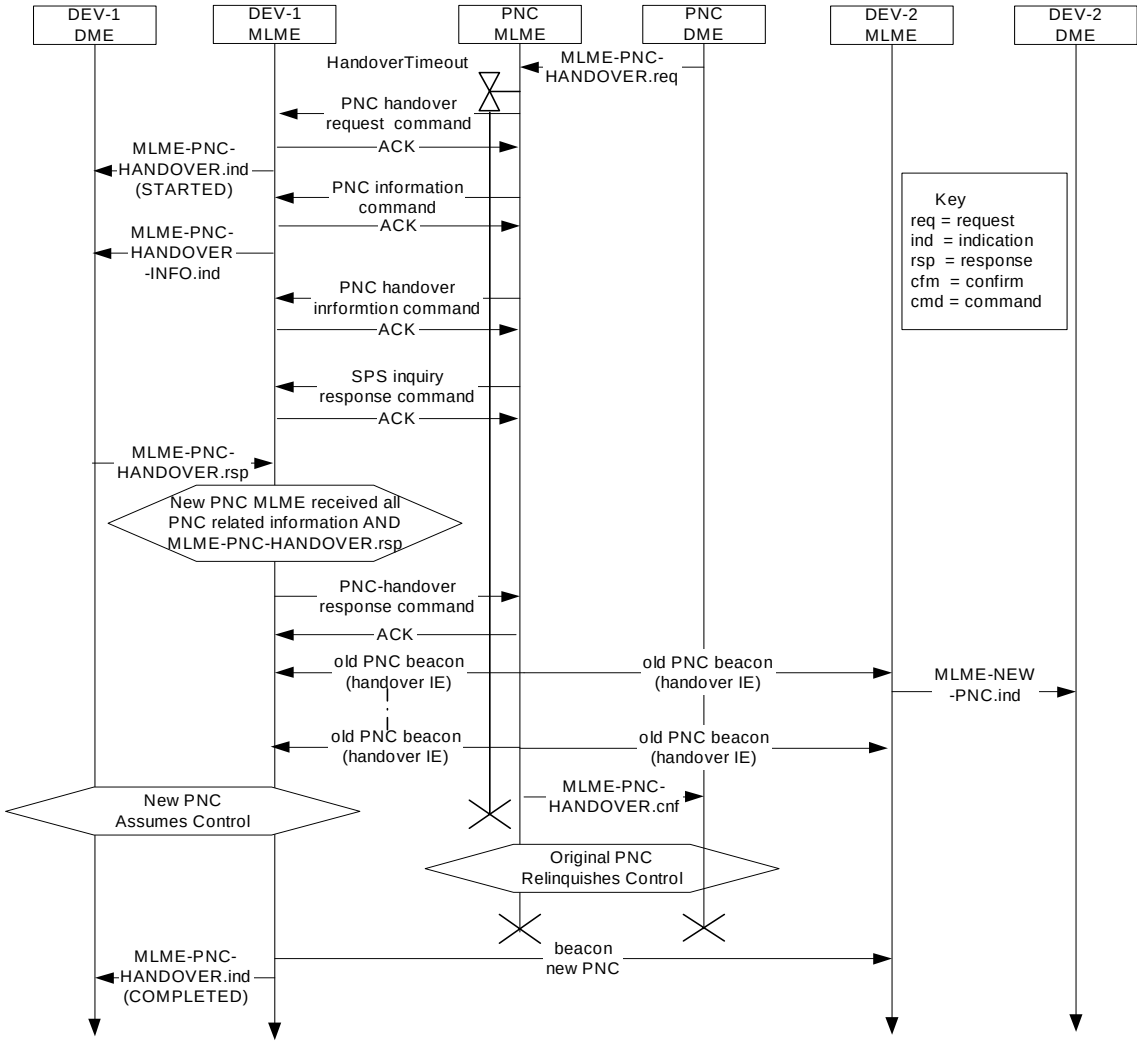
Add to page 156, line 35, 'The new PNC shall broadcast its first beacon at the time the beacon would have been sent by the old PNC. This time may vary from the actual time due to clock inaccuracies of old and new PNCs. The new PNC shall start sending beacons with the beacon number counter set to one more than the beacon number of the last beacon that will be sent by the old PNC.'

Add page 156, line 40ff, 'The PNC shall ensure that the beacon countdown includes at least one system wake beacon and at least aMaxLostBeacons beacons following that system wake beacon. The only exception to this requirement is if the PNC will be shutting down and does not have enought time to to wait for the next system wake beacon to complete the handover process. {Ed. note: This line may be moved to a new 8.1.1 that describes all beacon announcements.'}

The parent PNC shall not hand over to a DEV that is currently operating as a dependent PNC.'"

> Accept suggested resolution.

Handover MSC - various comments, suggestion from 02276r7P802-15_TG3-commentsD11_KO.doc below (with some editorial work):



Original MSC:.

Figure 19—PNC handover MSC

463 (Gubbi, TR) - Figure-91 is a well done job, but the text needs to supplement some infothat can not expressed in the figure, which is incomplete in the currentupdate to this para. It should be mentioned that these commands shall besent by PNC even if there is no information present that fits into thosecommands so that the rx-DEV knows the exact end of the transaction. For example , what if there are no DEVs in power save mode. Still the SPS-inquiry-response-command shall be sent by PNC. It should be mentioned that the three commands in Figure-91 (PNC-info-command, PNC-handover-info-command and SPS-inquirey-response-cmd) shall be sent by PNC even if there is no information present that fits nto those commands so that the rx-DEV knows the exact end of the transaction. For example , what if there are no DEVs in power savemode. Still the SPS-inquiry-response-command shall be sent by PNC. **Suggest accept in principle**, “Rather than send the empty commands, the PNC handover request will contain the number of CTRBs and SPS sets that will be transferred. If the number of items is zero, then the old PNC shall not send the command and the new PNC will not expect to receive it. It is not possible for the number of DEVs to be less than 2 (i.e. the old PNC and the new PNC), so the PNC information command will always be sent. This is documented in the resolution of CID 269.”

Accept suggested resolution.

273 (Heberling, TR) - [PNCHndOvr] When chosing a DEV for voluntary or forced handover, one of the most important parts is support for power save. A new PNC shall be selectedin order of how advanced powersave it supports/KO Add Table entries on 4th place, after PSRC: 4, SPS bit in Capability field, SPS=1 is preferred5, PSPS bit in Capability field, PSPS=1 is preferred. **Suggest accept in principle** "Add the entries for PSPS in the table and in the capability field, the definition is: 'The PSPS bit shall be set to 1 if the DEV is capable of supporting PSPS as a PNC, {xref 8.13.1}. Otherwise the PSPS bit shall be set to 0.' If SPS is made optional for PNC capable DEVs, then add the SPS entries as well (see resolution of CIDs 321, 324, 339, and 343), the definition for the capability field is: 'The SPS bit shall be set to 1 if the DEV is capable of supporting SPS as a PNC, {xref 8.13.1}. Otherwise the SPS bit shall be set to 0.'"

Accept suggested resolution.

271 (Heberling, TR) [PNCHndOvr] Again: It is not the number of GTS that is the limiting factor of a PNC,it's the number of CTRB it can support.In some superframes a CTRB doesn't lead to a GTS -> subrates Sometimes a CTRB leads to multiple GTS -> superrate Sometimes a CTRB only leads to one instance of a GTS -> asynchronous Sometimes a CTRB is split into GTS due to CT availability./KO Change table entry 5 from "Max number GTS" to "Max number of CTRB". **Suggest reject**, "Either measure, CTRB or GTS is somewhat inaccurate with respect to determining the capabilites of the PNC. GTS has been used for many versions of the draft (at least since D09) and is adequate for the purpose of PNC handover."

Accept in principle, "Change table entry 5 from 'Max number GTS' to 'Max number of CTRB' and other appropriate locations, e.g. association request command."

3.8.1 What to information to include in handover?

235 (Heberling, TR) - [PNCHndOvr] It is crucial for handover that the old PNC knows if the new PNC canhandle all associations and CTRB it manages. Therefore a DEV shall pass this info during association (ref 02/276r6 page 21, LB 17 CID 206,422) In addition, Power level needs to be passed. Last, MaxProcessedCTA and MaxAssignedCTA should be moved here from 7.4.4 and 7.4.11./KO Add to Figure 45: 1 octet: MaxAssociations 1 octet: MaxCTRB 1 octet: MaxTXPowerLevel Move text for MaxProcessedCTA and MaxAssignedCTA from 7.4.4 to this clause. Add text: The MaxAssociations field describes how many associated DEVs this DEV can manage if it is PNC Capable and becomes the PNC. Non PNC Capable DEVs shall set this value to 0.The MaxCTRB field describes how many CTRB this DEV can manage if it is PNC Capable and becomes the PNC. Non PNC Capable DEVs shall set this value to 0.The MaxTXPowerLevel describes the maximum transmit power of this DEV as defined in {xref TxPowerLevel}. **Suggest accept in principle**, "In the resolution of the last letter ballot, the TG considered the issue of handing over too many DEVs or streams to the new PNC. The feeling was that it is best for the new PNC to determine which DEVs or streams to retain and to disassociate any extra DEVs or terminate any streams that it was unable to support. The DEVs that are in range of the new PNC could be different than the DEVs that are in range of the old PNC. However, the max number of GTSs and max TX power level fields need to be added with the following definitions:

'The max number of GTS indicates how many GTSs the DEV is capable of allocating as a PNC. This shall be set to 0 in a non-PNC capable DEV.

The max TX power level indicates the maximum transmit power that is possible for the DEV. The power level is in dBm, encoded in 2s complement notation. For example, if a DEV was capable of 14 dBm TX power, the field would take on the value 0x0E while if the DEV was capable of -4 dBm TX power, the field would take on the value 0xFC.'"

Accept in prinple: "The max associated DEVS, max number of GTSs and max TX power level fields need to be added with the following definitions:

'The max associated DEVs field indicatess how many associated DEVs this DEV can manage if it is PNC capable and becomes the PNC. Non PNC capable DEVs shall set this value to 0.

The max number of GTS indicates how many GTSs the DEV is capable of allocating as a PNC. This shall be set to 0 in a non-PNC capable DEV.

The max TX power level indicates the maximum transmit power that is possible for the DEV. The power level is in dBm, encoded in 2s complement notation. For example, if a DEV was capable of 14 dBm TX power, the field would take on the value 0x0E while if the DEV was capable of -4 dBm TX power, the field would take on the value 0xFC.'"

243 (Heberling, TR) - [PNCHndOvr] Since we now also hand over SPS sets, we need to add a numberof SPS set field to the PNC handover request./KO See frame and text in 02276r7P802-15_TG3-commentsD11_KO.doc, Resolution [03]. **Suggest accept in principle**, "Add one octet to the PNC handover request command named 'number of SPS sets' with the definition 'The number of SPS sets indicates the total number of SPS sets that will be transferred from the old PNC to the new PNC.'"

Accept suggested resolution.

253 (Heberling, TR) - [PNCHndOvr] MaxAssociations, MaxCTRB and MaxTxPowerLevel need to be passed during handover.(ref 02/276r6 page 21, CID 206)/KO. Add to Figure 64:1 octet: MaxAssociations1 octet: MaxCTRB1 octet: MaxTXPowerLevelAdd text:The MaxAssociations field is described in 7.5.1.1The MaxCTRB field is described in 7.5.1.1The MaxTXPowerLevel describes the maximum transmit power of this DEV as defined in {xref TxPowerLevel}. **Suggest accept in principle**, "Add max number of GTSs and max TX power level as indicated in the resolution of CID 235. Add definitions to this subclause for the new fields that say: 'The max CTRB field is defined in {xref Association request}.' and 'The max TX power level field is defined in {xref Association request}.'

Accept in principle: "Add max associated DEVs, max number of GTSs and max TX power level as indicated in the resolution of CID 235. Add definitions to this subclause for the new fields that say: 'The max associated DEVs field is defined in {{xref Association request}.', 'The max CTRB field is defined in {xref Association request}.' and 'The max TX power level field is defined in {xref Association request}.'"

40 (Gilb, TR) - The Number of CTRBs is probably unnecessary now that we are fragmenting the handover information command. Delete the field from the PNC handover request command. **Suggest reject**, "The CTRB field is used to indicate if the PNC will be sending the handover information command and the number of CTRBs it will be sending."

Resolution is to reject.

443 (Gubbi, TR) - Why is "Next Beacon" required? Once the CTRB description is provided tothe new PNC, it is upto that PNC to allocate CTAs? Remove all occurrences of the field "Next Beacon" from Figure-61. **Suggest reject**, "The next beacon field is used to facilitate seemless handover. DEVs with subrate allocations are expecting their allocations at a certain time and it is helpful if the new PNC is aware of these and is able to keep the allocations at the same time intervals. The new PNC is allowed to change the occurances of these allocations at any time (just as the old PNC was able to)."

Resolution is to reject.

Meeting adjourned at 9:30 am PDT.

3.9 Tuesday, 17 September, 2002

Attendees: Rene Struik, Ari Singer, Jay Bain, Jim Allen, John Barr, Allen Heberling, Knut Odman, Mark Schrader, James Gilb.

Meeting called to order, 8:07 am.

Agenda:

- Roll call
- Call schedule, volunteers to sponsor calls
- Comment resolution assignments (02/406r1)
- Comment resolution (02/392r5)
- Discuss other possible resolutions
- Jokes
- Adjourn

Call schedule - Oct 1 - Bailey/NTRU, Oct. 3 - Stuik/Certicom, September 24 - Bain/TDSI, September 20 - Barr/Motorola, September 19- Heberling/XSI, September 26 - Gilb/Appairent.

James to send update that calls are 1.5 hours. James to send out hotels in the area, drive time, alternate airports.

Comment resolution assignment. John Barr wanted to be assigned all of Singer's comments. Request to reopen 92 - Change security to one mode.

357 (Schrader, TR) - The powering down between awake beacons is spoken of as mandatory. See text changes in Schrader-LB19-T1.doc. **Suggest accept in principle**, "Change 'Being in the SLEEP state is defined as having the receiver function disabled.' to 'Being in the SLEEP state is defined as not listening for traffic and possibly being in a reduced power state.' change 'listens to all beacons and will listen to all CTAs' to be '... listens to all beacons and listens to all CTAs ...' Change 'In the SPS mode, a DEV is required to listen to periodic wake beacons and to GTSs allocated in its wake beacons.' to be 'In the SPS mode, a DEV is required to listen to periodic wake beacons and to the GTSs allocated with its DEVID as the destination.'"

> Accept in principle, "Resolve SLEEP and AWAKE as indicated in CID 506. Also Change 'In the SPS mode, a DEV is required to listen to periodic wake beacons and to GTSs allocated in its wake beacons.' to be 'In the SPS mode, a DEV is required to listen to periodic wake beacons and to the GTSs allocated with its DEVID as the destination.'".

506 (Gubbi, TR) - The new definitions of AWAKE and SLEEP states are vague and leave lot ofroom of contradicting interpretations. Change two sentences starting from "Being in the AWAKE state...." to the following: "AWAKE state 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."

> Accept.

394 (Gubbi, TR) - The requirement in "All DEVs in PSPS mode are required to listen to wake beacons" is not clear. What does this mean? All PSPS DEVs have to receive it or just be awake to receive it if channel permits? I am sure the intent if NOT the former. If it is latter, then the maximum sleep time is made same for all PSPS DEVs. This is not acceptable. Depending on the power requirements some devices might want to go for longer, but permitted by PNC, sleep and wake up. Making those DEVs to wakeup to the time of TBTT is fine as in 802.11. This sounds similar to DTIMs in 802.11, but with worst performance outcome. Remove PSPS and revert back to APS mode as in D10 of the draft **Suggest reject**: "The text 'required to lis-

ten' means that the DEVs shall stay awake for certain beacons named system wake beacons and attempt to receive this beacon. They are not required to stay awake for and listen to any other beacons. PSPS allows DEVs, as well as APS did, to select the time they wish to stay in power save mode, up to the ATP of the DEV. PSPS adds a solution to a shortcoming of APS, that there was no way to inform sleeping DEVs about broadcasts or system parameter changes such as channel change and shutdown. Note that a DEV in SPS may decline listening to system wake beacons."

> Suggest add an SPS set 0 which allows DEVs to go to sleep up to the ATP. Text and MSCs to be generated by Schrader/Bain.

395 (Gubbi, TR) - The sentence "All asynchronous traffic to DEVs in PSPS mode will be allocated in the wake beacon". What does this mean? if a DEV is in PSPS mode and there are 100 other DEVs requesting to send async data to it, all the 100 requests are allocated in the wake beacon? Why is this sentence needed. Remove PSPS and revert back to APS mode as in D10 of the draft. **Suggest reject**: "The PNC is allowed to chain multiple system wake beacons if it has more GTS or announcements that would fit in a single beacon. This solves the rare events with clustered asynchronous traffic. In addition, the PNC is allowed to change the interval between system wake beacon to trade off between power save need and message transfer latency needs in the piconet."

> Suggest add an SPS set 0 which allows DEVs to go to sleep up to the ATP. Text and MSCs to be generated by Schrader/Bain.

454 (Gubbi, TR) - The term "wake beacon" deserves a clear description. What is it intended for as far as DEV is concerned? Clearly state if DEV is allowed to sleep ONLY between two wake beacons and not allowed to sleep at TBTT of wake beacons. But if this is true, note that this is not acceptable for DEVs intending to save power in a large magnitude.Retain APS scheme from D10. **Suggest accept in principle**: "DEVs are allowed to refuse listening to system wake beacons. A DEV in an SPS set sets its own sleep period and may choose to participate or not participate in the PSPS. SPS DEVs not listening to system wake beacons (i.e. not participating in PSPS) will miss all PNC parameter change and broadcast announcements. If the piconet has changed in some manner during their sleep time, they have to scan and recover in a fashion out of scope of the standard. Add clarifying text in 8.13 'Wake beacon for a DEV is defined as the PNC defined system wake beacon for DEVs in PSPS mode {xref 8.13.1} and the SPS set wake beacon for a DEV in SPS mode {xref 8.13.2}'"

> Suggest add an SPS set 0 which allows DEVs to go to sleep up to the ATP. Text and MSCs to be generated by Schrader/Bain.

499 (Gubbi, TR) - The DEVs must be required to "be awake to listen" than "required to listen" the latter gives the impression that they HAVE to somehow receive it as it is said in clause-5. Change "DEVs are required to listen to it" to "DEVs are required to be awake to listen to it" **Suggest accept in principle**: 'Change text on page 189, line 42 to: 'The system wake beacon is a normal beacon, with the additional requirement that all DEVs in PSPS mode shall be awake and listen for the system wake beacon.'"

> Accept in principle: "Change text on page 189, line 42 to: 'The system wake beacon is a normal beacon, with the additional requirement that all DEVs in PSPS mode shall be awake and listen for the system wake beacon.' Add to the end of that paragraph 'If the there are not DEVs in PSPS mode or the PNC does not wish to use system wake beacons, it shall set the {Ed. note check name in new comment} system wake beacon field to 0x80 which indicates that every beacon is a system wake beacon.'"

507 (Gubbi, TR) - PSPS mode is very similar to DTIMs in 802.11 but only worse. There is no way that the PNC can stop a DEV from entering PSPS mode and hence sleep state. Hence if there is BC/MC traffic that is pending transmission and a rogue DEV insists on going to SLEEP state, the BC/MC traffic gets held causing issues at other DEVs. If the thinking is that the ACK from PNC can be avoided, it causes other problems,

like (a) Forcing PNC to take that decision of allowing DEV to enter PSPS mode within SIFS duration (Actually only the MAC part of it) (b) avoids the implementations to implement ACK transmission part independent of higher MAC functionality and (c) unnecessary retransmissions of PS mode command at the DEV To avoid this PSPS mode needs a PS-mode-response frame from PNC before which the DEV is not allowed to enter PSPS mode. However since there are other drawbacks as highlighted in later comments, this is not an acceptable scheme Remove PSPS mode update from the draft and retain the APS mode as in D10 However the PS status bit map is useful and hence retain that as applicable to APS instead of PSPS mode. This includes retaining APS related commands in clause 7 in D10 **Suggest reject**: “There is no desire in a piconet with power save mode to stop a DEV from entering power save mode. In this standard, DEVs are not required to follow BC/MC traffic. In PSPS mode, all BC/MC traffic is announced in the system wake beacon, giving all PSPS DEVs the option to listen to it if the so desire. a)PNC takes no decision. The entering of PSPS is always allowed. The PNC just ACKs the PS mode command using the normal Imm-ACK procedure. The requirement is that the DEV shall not consider itself in PSPS mode until the PNC confirms reception of the PS mode change command by an Imm-ACK. b)See a). No separate ACK procedure is used c) Since PNC cannot deny the request, no response in necessary. Note that no isochronous streams are terminated when the DEV enters sleep mode. The DEV enetering PSPS mode may terminate undesirable streams.”

> Reject “There is no desire in a piconet with power save mode to stop a DEV from entering power save mode. In this standard, DEVs are not required to follow BC/MC traffic. In PSPS mode, all BC/MC traffic is announced in the system wake beacon, giving all PSPS DEVs the option to listen to it if the so desire. a)PNC takes no decision. The entering of PSPS is always allowed. The PNC just ACKs the PS mode command using the normal Imm-ACK procedure. The requirement is that the DEV shall not consider itself in PSPS mode until the PNC confirms reception of the PS mode change command by an Imm-ACK. b)See a). No separate ACK procedure is used c) Since PNC cannot deny the request, no response in necessary. Note that no isochronous streams are terminated when the DEV enters sleep mode. The DEV enetering PSPS mode may terminate undesirable streams. Asynchronous allocations are re-scheduled by the PNC to occur in the system wake beacon or in beacons that immediately follow the system wake beacon.”

508 (Gubbi, TR) - I am not sure how this new scheme (PSPS) can assume that all DEVs in the piconet have the same power save requirements and hence can use the same wake-beacon-interval. 802.15.3 caters for variety of devices and applications and hence there is a need for different such intervals depending on the kind of application served by the DEV. At least in 802.11 the DEVs are not mandated to be awake at all DTIMs and hence they can be sure that there will not be any directed frame that they are going to miss when they are asleep (doze mode). In APS mode this was enhnaced for better efficiency by allowing the DEV to request the sleep duration it wishes and the PNC permitting upto that duration. In PSPS mode that advantage has disappeared and hence this forces an upper limit on power saving for all DEVs in a given 802.15.3 piconet. Worst is it is same across the board for all DEVs in the piconet. To get around this issue, PSPS mode needs to allow DEVs to request intervals in multiples of wake-beacon-intervals. However given the quantization of the time durations involved and other drawbacks of the scheme, it is not recommended to retain this scheme. Remove PSPS mode update from the draft and retain the APS mode as in D10. However the PS status bit map is useful and hence retain that as applicable to APS instead of PSPS mode. This includes retaining APS related commands in clause 7 in D10: **Suggest reject**: “While it is true that the PNC makes the final decision of the system wake beacon interval, all DEVs indicate their preference in the PS mode change command and PNC makes a best effort compromize. Note that DEVs may refuse to participate in PSPS and its wake beacons by creating or joining an SPS set that fits their needs.”

> Suggest add an SPS set 0 which allows DEVs to go to sleep up to the ATP. Text and MSCs to be generated by Schrader/Bain.

315 (Heberling, TR) - [ParmChng] The whole paragraph on line 16-19 is residue from old text and totally wrong now/KO. Delete paragraph on line 16-19 "If the PNC decides to change PNID or BSID... ...value within the time-out duration and wait for beacons with the new PNID or BSID" **Suggest accept in princi-**

ple: Change text on page 201, line 16-19 to: 'If the PNC decides to change the PNID or BSID, the PNC shall send a beacon with the piconet parameter change element indicating the new PNID or BSID. The DEVs that received the beacon with the piconet parameter change element shall change the PNID or BSID to the new value at the time of the first beacon after the beacon with the change countdown field equal to zero has been sent.'"

Accept.

64 (Gilb, TR) - IN B.3 it references a to-be-published reference, which is a big no-no and quite silly. Delete the references to RFC 3280 and RFC 3278. **Suggest accept**.

Rene to provide new text.

CIDs 533 and 357 are similar to 506

Adjourned at 9:00 am.

3.9.1 Directed notification vs. announcement of CTAs

CIDs - 299, 301, 303, 305, 208, 71, 493.

3.9.2 Max CTAs

Is it useful to specify MAX assigned CTAs? MAX processed CTAs?

CIDs 201, 206, 219

3.10 Hard Issues

The hard issues are listed in the assignment spreadsheet by the terms in brackets.

3.10.1 MTS - do we need it? [MTS]

CIDs 56, 349, 350, 351, 352, 353, 354, 355, 513,

3.10.2 PM - SPS optional? Merge PSPS into SPS? [PM]

CIDs 321, 324, 339, 343,

3.10.3 PM - terminating streams when DEVs sleep. [PMwake]

CIDs - 65, 262, 450

3.11 Editorial work:

New description of piconet parameter change

3.11.1 Piconet parameter change

The piconet parameter change information element shall be formatted as illustrated in Figure 20.

octets: 6-32	2	2	1	1	1	1	1
BSID	PNID	Superframe timing	New channel index	Change countdown	Change type	Length (=13-39)	Element ID

Figure 20—Piconet parameter change information element format

The change type field indicates the parameter of the piconet is changing and therefore, the field that shall be interpreted by the DEV. The change type field value and its interpretation is given in Table 12.

Table 12—Description of field contents for change type values.

Change type field value	Interpretation	Field to decode	Description of field contents
0	PNID	PNID	The new PNID that will take effect beginning with the first beacon after the beacon with the change countdown field equal to zero has been sent.
1	BSID	BSID	The new BSID that will take effect beginning with the first beacon after the beacon with the change countdown field equal to zero has been sent.
2	MOVE	Superframe timing	The offset in milliseconds with which the first beacon after the beacon with change countdown set to zero has been sent will be sent relative the previous beacon position. ~~The superframe duration field in the piconet synchronization parameters field of the beacon shall remain unchanged~~.
3	SIZE	Superframe timing	The new superframe duration, with which the first beacon after the beacon with change countdown equal to zero has been sent. ~~The first beacon with the new superframe duration shall have its superframe duration field in the piconet synchronization parameters field set to the same value as the superframe timing field in this element~~.
4	CHANNEL	Channel index	The channel where the PNC will send its first beacon after NbrOfChangeBeacons beacons have been sent on the old channel.
5-255	Reserved	None	

The change countdown field shall count down from NbrOfChangeBeacons-1 to zero before the PNC stops transmitting on the old channel, with the old PNID or BSID or with the old superframe size or beacon position. For a piconet without pseudo-static GTSs, NbrOfChangeBeacons shall be at least two. For a piconet that has pseudo-static GTSs, NbrOfChangeBeacons shall be at least four. For a piconet that has child or neighbor piconets, NbrOfChangeBeacons shall be at least eight. However, a child or neighbor PNC may set the NbrOfChangeBeacons to a different number based on the change countdown field in the parent PNCs beacon as defined in 8.11.1.

4. Opening report

4.1 Status at opening in Monterey

.

Table 13—Ballot resolution as of opening of Monterey meeting

Type	LB19
T (technical)	72
TR (Technical required)	326
T and TR	398
E (editorial)	153
Total	551

4.2 Process for comment resolution

a) Add topic category to comments
b) Identify hot button topics
c) Schedule resolution of hot button topics
d) Begin resolution by topic of comments
    1) Write resolutions if possible
    2) Table issues that need more work
    3) Add to hot topics if necessary
e) Resolve hot button topics
f) Get all text written and posted
g) Hold BRC meeting if required

4.3 Editing process

a) Put editorial edits into draft (already started)
b) Send clauses to editors
c) Integrate results
d) Post interim version of the draft for review.
e) Final edits
f) Post for letter ballot

5. Comment resolution in Monterey

5.1 Hot topic issues

Bit order

Monday 7:00 pm - Resolved

Notifying DEVs of new CTA - Directed vs. in beacon (previously resolved by BRC as directed)

Tuesday Morning, 8:00 am. - Resolved, waiting text. Open issues: how to request the CTA status IE? What is done with SPS DEVs waking up? (use PCTM to wake up plus allow mode change + CTRB?) James to gather up, Jay and Mark to handle SPS wakeup.

Probe - possible error code?

Tuesday 8:00 am after notifying DEVs - Resolved, waiting text - James to locate CID and get text.

PNService IE - use probe instead of command? - Resolved

Tuesday 8:00 am after probe

CTRB - fixed vs. variable length format?

Tuesday 3:30 pm

Open/association MTS - Do we still need them?

Tuesday 1:00 pm

Security modes - Do we have 2 or 3 modes?

ACL/PIB

Wedneday 8:00 am

PM/SPS - SPS mandatory or optional?

Wednesday 1:00 pm

5.2 Monday resolution

ACK

272 - Accept

274 - ACCEPT IN PRINCIPLE. On line 36, change "Dly-ACK request bit" with "Dly-ACK policy and the DlyACK request bit" , same change on line 48.

289 - Accept

233 - REJECT. The ACK serves the purpose of telling the transmit state machine if it was successful in getting the frame. The response is used to close the process at the DME level.

310 - ACCEPT IN PRINCIPLE. Add text: 'The source upon reception of the Imm-ACK shall send a MAC_ISOCH_DATA.confirm with the ResultCode set to DLY_ACK_FAILED to the FCSL. This implies acknowledgment of the data frame and additionally indicates that the dly-ACK policy has been refused by the destination.'

312 - Accept

270 - Accept

215 - Accept

526 - Proposed resolution, pending more text: "1) This is fixed by referencing both "Dly-ACK policy and Dly-ACK request bit" being set. 2) The FCSL is now notified in the MAC-ISOCH-DATA.confirm as indicated in CID 310. 3) Same resolution as 1). 4) Move the sentence "The destination DEV may change the max burst value in each Dly-ACK frame." to the end of the previous paragraph that ends "... max num (sp) frames, as provided in the Dly-ACK frame 7.3.2.2." (note spelling error). 5) Change "souce" to "source" 6) Add a sentence that says "The FCSL would then notify the DME that the Dly-ACK negotiation failed. The DME then knows that a modification of the channel time allocation might be required." 7) Some more text? Jay to write suggested new text to clarify, due Tuesday by 1:00 pm. 8) Resolved as indicated in CID 189.

523 - Accept

195 - Accept in principle: ACCEPT IN PRINCIPLE. Add the text for clause 6 and clause 8 from Clause 2.2.7 of 02/273r17 to describe the use of the ASIE.

347 - Accept in principle: ACCEPT IN PRINCIPLE. Add the text for clause 6 and clause 8 from Clause 2.2.7 of 02/273r17 to describe the use of the ASIE.

331 - Accept in principle: ACCEPT IN PRINCIPLE. Add the text for clause 6 and clause 8 from Clause 2.2.7 of 02/273r17 to describe the use of the ASIE.

217 - Accept

318 - ACCEPT IN PRINCIPLE. Change to UnassocID and change the acronym list to be UnassocID - unassociated ID.

530 - ACCEPT. Change from "Before a DEV has completed the association process, all frames between the PNC and the DEV shall be exchanged either in the CAP of the superframe or in an association MTS." to be "Before a DEV has completed the association process, all frames sent to the PNC by the DEV shall be exchanged either in the CAP of the superframe or in an association MTS."

Add additional sentence at the end of the first paragraph "For association using MTS, the association response command is sent in an MTS with PNCID as source and UnassocID as destination."

34 - Accept

35 - Accept in principle: ACCEPT IN PRINCIPLE. Insert the PiconetServicesInquiry field (values: enumeration; REQUEST, NOREQUEST; Requests that the PNC sends the services information about the piconet as described in {xref AssociationRequest}) into the table. The capability field is still used.

133 - ACCEPT IN PRINCIPLE. Insert the PiconetServicesInquiry field (values: enumeration; REQUEST, NOREQUEST; Requests that the PNC sends the services information about the piconet as described in {xref AssociationRequest}) into the table. The capability field is still used.

149 - Accept.

411 - Accept

425 - Can we remove the application data ID? Ask M. Schrader. Table until response, AI for JPKG to contact him.

426 - Can we remove the DEVID? Ask M. Schrader. Table until response, AI for JPKG to contact him.

414 - ACCEPT IN PRINCIPLE. Delete the sentence "The PNC may use multiple beacons to broadcast successive DEV association IEs if too many DEVs are associating than will fit in a single beacon.." as it is confusing and does not add any new information. The PNC is able to choose when it sends any IE.

417 - ACCEPT IN PRINCIPLE. Delete the capability field, change the name of the Association status field to be "DEV characteristic". In the new DEV characteristic field, put in a 1 bit Association status field that is 0 for disassociated and 1 for associated, a 5 bit "Supported data rates" with an xref to where defined in 7.11 (or where this goes in the future) and 2 reserved bits. Check in other places where Association status field is defined to see if they need to be changed to match.

418 - ACCEPT IN PRINCIPLE. DEVs are not required to authenticate to other DEVs in a piconet. They are only required to authenticate with the PNC in a secure piconet. However, this status is not useful here, therefore it will be removed as valid value as indicated in the resolution of CID 417.

415 - ACCEPT IN PRINCIPLE. This is already required in 8.3.1, page 164, lines 50-51 where the PNC repeats it at least aMinBeaconInfo which has a value of 4.

419 - ACCEPT IN PRINCIPLE. Move DEV address to the first position in this IE and in the PNC info command's DEV record on page 139, figure 64.

33 - ACCEPT IN PRINCIPLE. Delete the three sentences. In 8.3.4 change the last sentence in the paragraph on page 167, line 1 to be 'Similarly, if the beacons from the PNC are not received by the DEV for longer than the ATP, the DEV shall consider itself disassociated from the piconet and may try to associate again. The DEV notifies the DME that the ATP expired using the MLME-ATP-EXPIRED.ind primitive.' Keep MLME-SYNCH.{request,confirm} as they are used for the association process. Delete figure119. Rename MLME-SYNCH-LOST as MLME-ATP-EXPIRED. Add text to 8.3.1 that indicates that the DEV needs to perform an MLME-SYNCH prior to starting the association process. {Ed. note: Generate the text}.

18 - Accept

37 - ACCEPT IN PRINCIPLE. Add a second MLME-ASSOCIATE.ind to the MSC after the second association request command. Add the OrigID to the MLME-ASSOCIATE.ind and put a definition in table 8 that says it is either the UnassocID or the DEVID that was just assigned by the PNC. Add DEVID=UnassocID to the first MLME-ASSOCIATE.ind and DEVID=0xzz to the second one.

439 - Accept.

53 - ACCEPT IN PRINCIPLE. Delete aDEVIDReuseTime. Change 'However, the reallocation of the same DEVID by PNC shall be at least aDEVIDReuseTime after the disassociation of the DEV that was allocated the same DEVID.' to be 'After the PNC sends a disassociation command to a DEV, the PNC shall not reuse the same DEVID of that DEV until at least two times the ATP duration for that DEV has passed.' Add to the

ATP discussion in disasociation ‘The PNC shall send a disassociation command to a DEV that sends a frame after its ATP has expired.’

437 - ACCEPT IN PRINCIPLE. Add that the units are in millisconds here and in 7.5.1.2.

43 - ACCEPT. Double check to make sure that all of the IEs that need to be there are in Table 39 (e.g. PSPS status and SPS status).

38 - REJECT. Although in some cases it may help to have the CTAs last so that a DEV can shutdown early if it has not decoded a CTA assigned to that DEV within MaxProcessedCTAs. However, with the CTAs first, the DEVs have more time to react to the channel time allocations and the CTAs start in a known location.

405 - REJECT. Although in some cases it may help to have the CTAs last so that a DEV can shutdown early if it has not decoded a CTA assigned to that DEV within MaxProcessedCTAs. However, with the CTAs first, the DEVs have more time to react to the channel time allocations and the CTAs start in a known location.

413 - ACCEPT. Double check to make sure that all of the IEs that need to be there are in Table 39.

406 - ACCEPT IN PRINCIPLE. Change the figure 9 title to be ‘Piconet synchronization parameters field format.’ Change the sentence ‘All beacons include the piconet synchronization parameter field.’ to be ‘All beacons include the piconet synchronization parameter field, as shown in the frame formats for the non-secure, {xref} and secure beacons, {xref}.’

94 - Accept.

192, 345 - Table, everyone to ask for help.

281 - Accept

467 - REJECT. The PNC DEV-Address is no longer used to distinguish the piconet, instead BSID identifies the piconet (with the PNID). However, many parts of the standard refer to the Parent PNC DEV-Address and these will be changed to refer to the Parent BSID.

433 - REJECT. The overlapping PNID element is only used to report PNIDs. The PNC is required to change its PNID if an overlapping piconet is found that uses the same one. However, the PNC is not required to change its BSID. The actual number of piconets using the PNID is not important, rather it is simply the existence of at least one piconet with that PNID that matters. Furthermore, this IE is sent even if only a frame and not the beacon is detected on another channel. In this case, the DEV doesn't know the BSID.

242 - ACCEPT IN PRINCIPLE. Change this sentence frag.: <from> "...remove the parent PNC DEV address element from ..." <to> "...remove the parent BSID IE from ..."

238 - ACCEPT IN PRINCIPLE. Change this sentence frag.: <from> "...remove the parent PNC DEV address element from ..." <to> "...remove the parent BSID IE from ..."

408 - ACCEPT IN PRINCIPLE. After the sentence ending "... the CAP of the current superframe." add "The CAP command bit applies to all commands except for the association request command, which is covered by the CAP association bit."

67 - Accept.

74 - ACCEPT IN PRINCIPLE. Add a new timing parameter called BIFS = SIFS + aCCADetectTime and use it instead of RIFS in the backoff procedure. Add BIFS - backoff interframe spacing to the acronyms clause. Modify clause 11 to match this new usage.

451 - ‘When the DestID of this command is 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.’

5.3 Tuesday

Directed vs. beacon announcement of new CTA.

299, 301, 303, 305 - Use IEs in the beacon, for BC/MC and pseudo-static slots to ACTIVE DEVs they are in the system wake beacon plus 3 following. For power save DEVs, they are in the DEVs wake beacon plus 3 following wake beacons. Also, a DEV that wants this info but missed it, may request it from the PNC with with probe command? How do you indicate the stream index? Or do you get all of them. How do we add text to probe to request multiple IEs? Do we add a CTA information request and CTA information response (or use PNC handover information command).

PNService IE - use probe instead of command?

Tuesday 8:00 am after probe

255 - REJECT. The information sent in the PN services command is likely much longer than an IE, thus it is easier to send it in a command. With a single command, the DEV knows when it has received all of the data, as opposed to an set of IEs.

283 - REJECT. The information sent in the PN services command is likely much longer than an IE, thus it is easier to send it in a command. With a single command, the DEV knows when it has received all of the data, as opposed to an set of IEs.

346 - REJECT. The information sent in the PN services command is likely much longer than an IE, thus it is easier to send it in a command. With a single command, the DEV knows when it has received all of the data, as opposed to an set of IEs.

Probe - possible error code?

Tuesday 8:00 am after notifying DEVs

CID ?? - Which one do we need to say no? Suggest overall probe procedure, if you get an IE you are not able to respond to (i.e. it is listed as may respond or shall not respond), the DEV sends back the appropriate IE with the identifier and a zero length. Also need to work on the clause 8 table for different wording, you always respond, but sometimes you give a null IE. {Ed. note: Need to work on the words}.

282 -Withdrawn

46 - Accept.

23 - ACCEPT IN PRINCIPLE. For the PNC received request from DEV, change the following to shall ignore: DEV association, PNC shutdown, Piconet parameter change, PNC handover, SPS status.

44 - ACCEPT IN PRINCIPLE. Add an MLME-PROBE.confirm to just before the first MLME-PROBE.ind sent to DEV-2. Change the probe primitve parameters to match the following (same definitions).

```
MLME_PROBE.request
(
TrgtId,
InfoElementMap,
InfoElementList,
ProbeTimeout
)
```

```
MLME_PROBE.indicate
                    (
                    OrigId
                    InfoElementMap
                    )
```

```
MLME-PROBE.response (
                    OrigId,
                    InfoElementMap,
                    InfoElementList,
                    ProbeTimeout
                    )
```

```
MLME-PROBE.confirm  (
                    TrgtId,
                    InfoElementList,
                    ResultCode
                    )
```

52 - Replace Table 53 with the following.

Table 14—Rules for sending to probe requests

Information element	Subclause	PNC allowed to request	DEV allowed to request	PNC sends	DEV sends
Channel time allocation	7.4.1	Shall not request	Shall not request (no)	Shall not send	Shall not send
Piconet	7.4.2	Shall not request	May request (yes)	Shall not send	Shall not send
Parent piconet	7.4.3	Shall not request	May request	Shall not send	Shall not send
DEV association	7.4.4	Shall not request	Shall not request	May send	Shall not send
PNC shutdown	7.4.5	Shall not request	Shall not request	May send	Shall not send
Piconet parameter change	7.4.6	Shall not request	Shall not request	May send	Shall not send
Application specific	7.4.7	May request	May request	May send	May send
Pending channel time map (PCTM)	7.4.8	Shall not request	May request	May send	Shall not send
PNC handover	7.4.9	Shall not request	Shall not request	May send	Shall not send
DEV address	7.4.10	May request	May request	May send	May send
Capability information	7.4.12	May request	May request	May send	May send
Transmit power parameters	7.4.13	May request	May request	May send	May send
SPS status	7.4.14	Shall not request	Shall not request	May send	Shall not send
PSPS status	7.4.15	Shall not request	May request	May send	Shall not send
Public-key object	7.4.16	May request	May request	May send	May send
Security suite OID	7.4.17	May request	May request	May send	May send
Overlapping PNID	7.4.18	May request	Shall not request	Shall not send	May send
Piconet services	7.4.19	May request	May request	May send	May send
Vendor specific or reserved	7.4	May request	May request	May send	May send

503 - ACCEPT IN PRINCIPLE. Change the sentence to ’A DEV shall not report overlapping piconets if it determines that the beacons were received from a child or 802.15.3 neighbor piconet that is associated with the DEVs current piconet.’

306 - ACCEPT IN PRINCIPLE. Change the field to be the Parent BSID IE, length 8-34, change the text to be: The parent BSID IE is the address from a parent BSID IE, 7.4.3, found by the DEV in a beacon. If the DEV found only a frame and did not find a beacon, it shall include a zero length parent BSID IE. Change the length of the Piconet BSID IE to be 8-34.

45 - Accept.

452 - ACCEPT. Change the BSID IEs to include the MAC address of the PNC (or parent PNC). Rename the IEs to be the Piconet IE and Parent piconet IE. Rename throughout (after change from Parent DEV address IE to Parent BSID IE.) Change the lengths of the fields in this command to be 14-40.

24 - ACCEPT IN PRINCIPLE. Add a table to 6.3.18 called remote piconet description, as shown in 02/392r2. In table 21, change PiconetDescription to be RemotePiconetDescription with cross references to the new table.

Table 15—Elements of RemotePiconetDescription

Name	Type	Valid Range	Description
BSID	As defined in Table 4	As defined in 7.4.2	The text string of a discovered piconet.
PNCDEVAddress	MAC address	Any valid individual MAC address	The MAC address of the PNC of the piconet that was found.
PNID	As defined in Table 4.	As defined in Table 4.	The PNID of a discovered piconet
PiconetType	Enumeration	PARENT, DEPENDENT	The type of a discovered piconet.
Parent BSID	As defined in 7.4.3.	As defined in 7.4.3.	The BSID of the parent piconet if a beacon of a dependent piconet was found.
ParentPNCDEVAddress	MAC address	Any valid individual MAC address.	The MAC address of the parent PNC of the piconet that was found.
ScannedFrameType	Enumeration	BEACON, NON-BEACON	Indicates what type of frame was found. {Ed. note: change table 5 as well}
ChannelIndex	Integer	0-255	A PHY dependent channel as defined in 7.5.6.4

216 - ACCEPT IN PRINCIPLE. Add a table to 6.3.18 called remote piconet description, as shown in 02/392r2. In table 21, change PiconetDescription to be RemotePiconetDescription with cross references to the new table.

500 - ACCEPT IN PRINCIPLE. Change "Any frame may beattempted at most aMaxRetransmissionLimit number of times before the transmitting DEV gives up on that frame and discards it. If a fragment of an MSDU fails retransmission up to the retry limit, the source DEV shall discard all MPDUs of that MSDU. However, a DEV might choose to attempt retransmission of an MPDU a fewer number of times as some data streams have a short life time." to be "A DEV determines the number of times a frame is retried before the DEV gives up on that frame and discards it. If the DEV gives up on a fragment of an MSDU, the DEV shall discard all MPDUs of that MSDU."

Open/association MTS - Do we still need them?

Tuesday 1:00 pm, CIDs 56, 349, 350, 351, 352, 353, 354, 355, 387, 513

Issues:

Con MTS: Do we need two multiple access methods? IP cost if any? Complexity from supporting both and in the specifying in the standard. Efficiency of contention? How much efficiency? For minimum CAP of say

160 us, average backoff is 16 (1/2 of 32) with 16 us slots or 320 us. That makes about a 1 out of 2 or 3 possibility of getting through. Lack of predictability of determinism of when an MTS is made available by the PNC. Any prior art? WMS says that there are plenty of examples of sloted aloha in the literature. KO: Hiperlan uses RACH (random access channel). Gubbi proposal used RACH anyway (Q slot for reQuest slot). For predictable responses, would sub-rate CAPs work as well?

Pro MTS: CAP needs to be long enough. If you want a minimum contention period, then slotted aloha takes up the least amount of time. Will new PHYs really be able to support a CAP?

Reschedule for Thursday 1:00 pm.

425 - Accept

426 - Accept

435 - ACCEPT IN PRINCIPLE. Change "PNC" to be "PNC or destination DEV"

488 - ACCEPT IN PRINCIPLE. Change the sentence 'If an Imm-ACK or del-ACK is expected for that frame, ... PHY rate as the transmitted frame.' to be 'If an Imm-ACK or Dly-ACK is expected for that frame, the DEV shall check whether there is enough time remaining in the time slot to accomodate the current frame, 2 SIFS periods and the Imm-ACK or Dly-ACK frame at the same PHY rate as the transmitted frame.'

22 - Options: New request replaces all old for both? Or add a single bit that says what to do?

483 - ACCEPT IN PRINCIPLE. 1. Add definitions for subrate and super-rate slots to Clause 3. 2. The TG is open for suggestions for new names for subrate and super-rate. To date, we have been unable to find better terminology. 3. Yes, the text indicates that psuedo-static CTAs are not allowed to happen once per many superframes, rather they are allocated every superframe.

484 - Accept.

400 - ACCEPT IN PRINCIPLE. Change 'of an isochronous stream that is currently employing the Dly-ACK mechanism.' to be 'of a stream that is currently employing the Dly-ACK mechanism. It is not valid for frames using the asynchronous stream index or the MTS index.'

166 - ACCEPT IN PRINCIPLE. Add to when generated in MLME-CREATE-STREAM.request: 'If a multicast or broadcast stream was opened with any other ACK-Policy than no-ACK, the MLME will not send a channel time request command to the PNC and shall be respond with MLME-CREATE-STREAM.confirm with ResultCode set to ILLEGAL_ACK_POLICY.'

182 - ACCEPT IN PRINCIPLE. Add text to When generated: 'If the dly-ACK policy was used, but the destination refused the use of dly-ACK, the ResultCode shall be set to DLY_ACK_FAILED. This indicates successful transmission of the corresponding data frame.'

498- REJECT. The use of null CTAs allows DEVs that were listening to a BC or MC stream to know that it is no longer allocated. This can't be done with a directed frame. In addition, the standard is using directed frames to communicate with the source and IEs in the beacon to communicate with destinations. The TG discussed this issue at length in Vancouver, on conference calls, the ad-hoc meeting in Schaumburg and in Monterey. Both methods, directed frames and null-CTAs were considered in the discussions and it was felt that null-CTAs would better serve the purposes of the standard.

168 - Accept.

449 - Accept.

48 - ACCEPT IN PRINCIPLE. Add the priority parameter with definition in the table as indicated in CID 160.

51 - ACCEPT IN PRINCIPLE. Change as indicated. Also, show the data frame as coming from the MAC/ MLME to the other MAC/MLME as well as the ACK.

265 - ACCEPT IN PRINCIPLE. Correct the figure as indicated in CID 51.

50 - Accept in principle “Delete figure 110. Add to MAC-ISOCH-DATA.request to the end of 6.6.4.2 ‘If the StreamIndex is not assigned to the DEV as a source, the MLME will not attempt to transmit the frame and will respond with the MAC-ISOCH-DATA.respond with error code ‘INVALID_STREAM.’ Add ‘INVALID_STREAM’ to table 34.”

156 - Accept.

160 - Accept.

307 - Accept.

485 - ACCEPT IN PRINCIPLE. Change "the PNC may overlap the allocations for the old and new psuedo-static GTSs" to "However note that the PNC may overlap the old and new locations of the same psuedo-static GTS within a superframe as it does not cause any issue of frame collisions. If PNC sees the usage of the new allocation by both the source of the destination of old allocation before the expiration of aMAxLost-Beacons number of supreframes, then the PNC may reuse the old allocation for another pair of DEVs" After the end of sentence "... and begin using the new GTS." The second point is already handled in the draft with the requirment on page 171, line 6, "When the source of a pseudo-static GTS receives a beacon with the new CTA, it shall cease using the old GTS and begin using the new GTS."

256 - Accept.

5.4 Wednesday, 11 September, 2002

Security modes - Do we have 2 or 3 modes?

ACL/PIB

PNC handover of ACL information

Wedneday 8:00 am

PM/SPS - SPS mandatory or optional?

Wednesday 1:00 pm

92 - ACCEPT IN PRINCIPLE. Suggest a table that has security levels (i.e. claimed bits) and if the OID offers cryptographic authenticiation of public keys for each of the OIDs. Merge Mode 1 and Mode 2 services offered, pointing out that some OIDs use certificates, some don’t. Throughout the draft, use only mode 0 or mode 1 or security off or security on. Change the SEC mode field in the beacon to be only one bit.

ACL

370 - Why can't a mode 0 PNC use the ACL? I thought this is how we got rid of mode 1. Maybe this is just an oversight.

384 - MAC PIB ACL group defined as an array whose contents are defined in Table 33. All of the entries are dynamic, but no clear mechanism to update these entries has been included in the draft. There are no limits on the minimum and maximum number of entries allowed in the ACL. The only use for this array in the MAC is for generation of the CCM nonce and obtaining the keys associated with a particular SECID for encoding or decoding payloads.

Table until Thursday at 1:00 pm, look for compromise text.

Handover - Dan Bailey from NTRU said that they have no patents or applications on this method. He does not personally know of any from other companies.

102, 91 - Suggest passing hashes of public keys. Add 160 bit (20 octets) with the associated DEV address and the OID (possibly length). Rene asked why not hand over the public keys instead of the hash? Dan said for length concerns (160 up to 1757 bits, 20-200 octets, currently. It could be up to 4 times 256 bytes for certificates). Table until Thursday at 1:00 pm, need specific text that describes how to do it.

520 - Accept.

49 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 166.

180 - Accept.

258 - Accept.

154 - Accept.

212 - Accept.

494 - ACCEPT IN PRINCIPLE. The sentence was to indicate that this was the initial allocation of the CTA, not to say that it would occur first in the superframe. Therefore, change 'The PNC shall issue the first GTS for the stream in the superframe indicated in the channel time allocation command.' to be 'The PNC shall issue the initial GTS for the stream in the superframe indicated in the CTA status IE.'

492 - REJECT. The goal here is that the PNC is allowed to update its CTAs without waiting for another process to complete, either partially or completely. This is the fastest way to get the channel time allocated. As soon as the DEV sees the CTA in the beacon, it is able to use the time.

160 - Accept.

162 - Accept.

169 - ACCEPT IN PRINCIPLE. The stream termination bit is implied by the MLME-TERMINATE-STREAM command and doesn't need to be passed. It is implied as well for the other MLME-XXX-STREAM commands. The priority parameter will be added as indicated in CID 160.

257 - ACCEPT IN PRINCIPLE. Modify the MSC in Figure 108 as follows: 1) Delete the Evaluate request symbol from the PNC MLME column. 2) Delete the Allocate resources symbol from the PNC MLME column. 3) Move the channel time response command to just below the Check resources symbol, since this is where the decision regarding the two error conditions is determined. Also move the ACK up in the diagram as well. 4) Move the MLME-CREATE-STREAM.cfm primitive to just below the starting point of the ACK to the channel time response command.

263 - ACCEPT IN PRINCIPLE. Add the MLME-TERMINATE-STREAM.request and the MLME-TERMINATE-STREAM.confirm to the MSC. Also, delete the first condition symbol 'de-allocate stream'.

259 - ACCEPT IN PRINCIPLE. Delete figure 110.

134 - ACCEPT IN PRINCIPLE. Also add a definition to the table, StreamIndex, As defined in {xref}; As defined in {xref}; The stream index that was assigned in the channel time allocation process for the dependent piconet.

277 - Withdrawn, 11 September, 2002

221 - ACCEPT IN PRINCIPLE. Add to the figure ‘1 octet, Remaining DEVID’, Also add the description 'The remaining DEVID indicates which dependent piconet is able to continue operation as described in {xref shutdown}. It shall be set to the PNCID if there are not dependent piconets in the current piconet.

541 - ACCEPT IN PRINCIPLE. Delete all parameters for the MLME-START-DEPENDENT.confirm except for the ResultCode.

141 - Accept, See also CID 541 and 136.

136 - ACCEPT. See also CID 541 and 141.

140 - Accept.

487 - ACCEPT IN PRINCIPLE. Delete the sentence 'However, the PNC shall not reduce the channel time allocation of a private GTS allocated for a child or neighbor network.'

317 - ACCEPT IN PRINCIPLE. (see 02/392r3 for formatting help) Page 199, lines 45 and 46 change ‘The exceptions to this are when the parent is changing its PNID or BSID and that a child or neighbor PNC decides not to change channels, 8.11.1, with the parent PNC.’ to ‘The exceptions to this are:

— When the parent is changing its PNID or BSID.
— A child or neighbor PNC decides not to change channels with the parent PNC and is shutting down, 8.11.1.’

page 202, line 44: Change ‘... piconet parameter change IE, 7.4.6 in ...’ to be’... piconet parameter change IE, 7.4.6, with ChangeType set to CHANNEL, in ...’

page 203, at appropriate location, ‘All DEVs shall not transmit on the new channel until a beacon has been correctly received on the new channel.’

page 202, line 51, Change ‘from their current channel to the new channel immediately after the beacon when the change countdown field becomes zero.’ to be ‘from their current channel to the new channel before the first expected beacon on the new channel.’

472 - ACCEPT IN PRINCIPLE. On page 163, line 12 Change 'shall cease operations by the time of the last beacon sent by the parent PNC.' to be 'shall either cease operations, change channels or join another piconet as a dependent piconet by the time of the last beacon sent by the parent PNC.'

469 - ACCEPT IN PRINCIPLE. On page 162, line 53, change 'shall cease operations by the time of the last beacon' to be 'shall either cease operations, change channels or join another piconet as a dependent piconet by the time of the last beacon'

465 - ACCEPT IN PRINCIPLE. Add text at the end of line 2 that says, 'There is no restriction in this standard on the number of levels that may be created. However, there is a practical limitation to the number of dependent piconets and the levels that are able to be supported.’

464 - ACCEPT IN PRINCIPLE. Change ‘a child of a child or child of a neighbor’ to be ‘It is also possible for another dependent piconet to be formed in a child or neighbor piconet’. Ed. Note: combine all stuff that is common to child and neighbor in an introductory subclause, if possible.

391 - REJECT. The standard allows the child PNC to allocate its channel time in any way that it wants. Therefore, a child PNC may allow the formation of both child and neighbor piconets. See also the resolution CID 464.

392 - ACCEPT IN PRINCIPLE. The standard already requires a DEV to be a member of a piconet in order to communicate with other DEVs in that piconet. Therefore, a member of a child piconet shall not communicate with members of the parent piconet, unless that DEV is a member of the parent piconet (which is allowed).

458 - ACCEPT IN PRINCIPLE. The primitive has had the StreamIndex added which indicates the CTA to be used as well as the DEVID. The DEVID indicates if the dependent piconet is a child or neighbor. At this point in the process, the only difference between the two piconets is the DEVID used in the CTA. Within its own piconet, there is no difference between a child or neighbor.

521 - ACCEPT IN PRINCIPLE. Change to "A piconet which allocates guaranteed time slots for another piconet (child or neighbor types) operating in the same channel".

Suggested text for CID 475:

‘8.2.6.4 Parent PNC termination of a dependent piconet

If the parent PNC wishes to stop the child piconet, it shall terminate the stream allocated to the child piconet using the isochronous stream termination procedure, 8.5.1.3. If the parent PNC wishes to stop the neighbor piconet, it shall send a disassociate request, 8.3.4, to the neighbor PNC. In either case, the dependent PNC shall then immediately initiate its shutdown procedure, 8.2.6. The parent PNC shall listen for the dependent PNC shutdown beacon sequence to determine when the dependent piconet CTA should be removed. The parent PNC may set a maximum time for the completion of the dependent shutdown sequence, after which the CTA will be removed regardless of the completion of the dependent shutdown procedure. In the case of a child piconet, this timeout is set in the MLME while for a neighbor piconet, this time is set via the MLME-DISASSOCIATE. request primitive, 6.3.6.1. If the dependent PNC is a neighbor that is not 802.15.3 compliant, the parent PNC shall provide the same time as it allows for its own shutdown sequence, for the neighbor PNC to stop its piconet before removing its private CTA.’

Suggested text for Beacon information announcement.

8.1.1 Beacon Information Announcement

The PNC sends several IEs in its beacons to inform the piconet about constant or temporary conditions. Some are sent in every beacon. In some cases these are only sent if certain features are in use, such as power save or a dependent piconet. Other IEs are only sent as an announcement of a changed condition in the piconet. These IEs could be for the benefit of all DEVs or for a particular DEV. IEs not sent in every beacon are called announcements and shall be sent for {xref aMinBeaconInfoRepeat} beacons.

If the intended recipient of the IE is all DEVs, the following rules apply:

— The IEs shall be sent in aMinBeaconInfoRepeat subsequent beacons.
— If any DEV is in PSPS or SPS mode, the first IE announcement shall be made in a system wake beacon.

If the intended recipient of the IE is one individual DEV, the following rules apply:

Table 16—Repeated beacon announcements

Element	Clause	Announced in	Intended for	Clause
DEV association	7.4.4	aMinBeaconInfoRepeat	All DEVs	8.3.1, 8.3.4
PNC shutdown	7.4.5	aMinBeaconInforRepeat	All DEVs	8.2.6
Piconet parameter change	3.11.1	a MinBeaconInfoRepeat	All DEVs	8.10, 8.11.1, 8.11.2
Application specific	7.4.7	As needed	As appropriate	
Pending channel time map (PCTM)	7.4.8	As needed	All DEVs	
PNC handover	7.4.9	aMinBeaconInfoRepeat	All DEVs	8.2.3
SPS status	7.4.13	As needed	All DEVs	8.13.2
PSPS status	7.4.14	As needed	All DEVs	8.13.1
CTA status IE	{xref 7.4.x}	aMinBeaconInfoRepeat	Depends on DestID	8.5.1.1, 8.5.1.2

— If the DEV is in Active mode, the IEs shall be sent in aMinBeaconInfoRepeat subsequent beacons.
— If the DEV is in PSPS mode, the first IE announcement shall be made in a system wake beacon.
— If the DEV is in SPS mode, the IEs shall be sent in aMinBeaconInfoRepeat subsequent SPS set wake beacons.

In the case of the CTA status IE, this is considered to be intended for all DEVs if the TrgtId of a CTRB for a stream is BcstId or McstId. Otherwise it is considered to be for an individual DEV.

5.5 Thursday, 12 September, 2002.

Bit ordering, CIDs 192, 345

Suggest adding ‘The payload in the data frame is sent with the lowest numbered octet first, least significant bit first, over the air.’ to the beginning of line 51. After ‘the highest numbered bits.’ add ‘For any text fields, the first character is in the first octet of the field with other characters following sequentially.’ Also add a new figure for the data payload from 02/239r4.

192 - ACCEPT IN PRINCIPLE. Add ‘The payload in the data frame is sent with the lowest numbered octet first, least significant bit first, over the air.’ to the beginning of line 51. After ‘the highest numbered bits.’ add ‘For any text fields, the first character is in the first octet of the field with other characters following sequentially.’ Also add a new figure for the data payload from 02/392r14.

345 - ACCEPT IN PRINCIPLE. Add ‘The payload in the data frame is sent with the lowest numbered octet first, least significant bit first, over the air.’ to the beginning of line 51. After ‘the highest numbered bits.’ add ‘For any text fields, the first character is in the first octet of the field with other characters following sequentially.’ Also add a new figure for the data payload from 02/392r4.

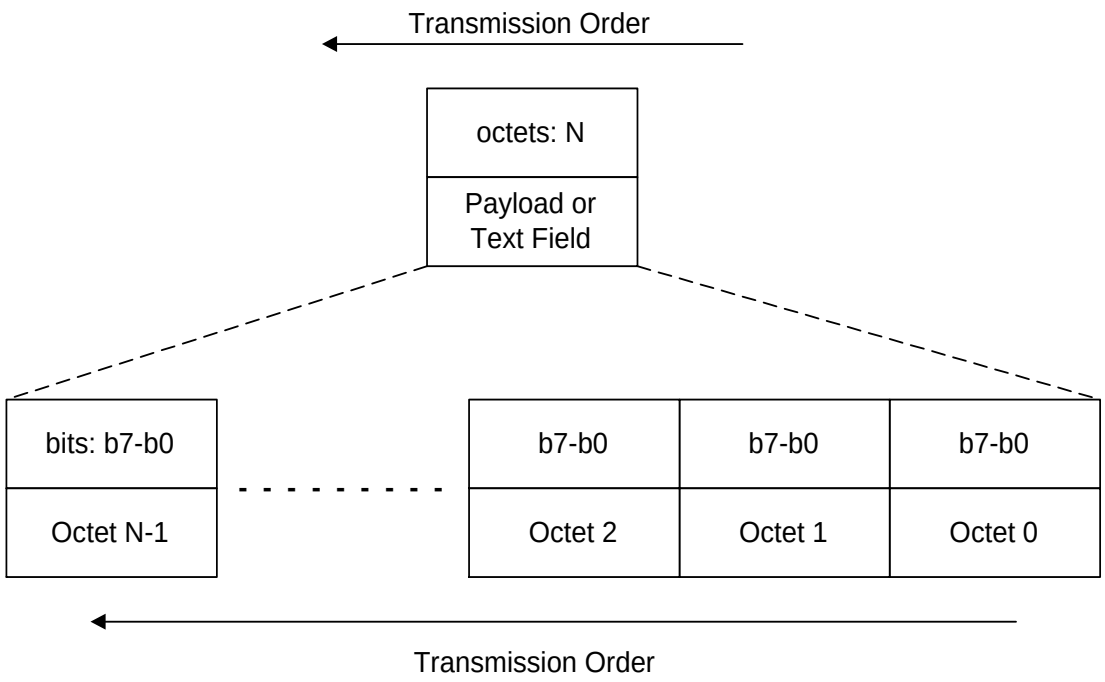


Figure 21—Illustration of bit ordering for data payload and text fields.

22 - ACCEPT IN PRINCIPLE. Define the reserved bit in the CTRB field to be the ‘flush’ bit, definition, ‘The flush bit field shall be set to 0 for isochronous requests (i.e. for requests that do not use the asynchronous stream index). It shall be set to 0 in an asynchronous request if the originating DEV wants this request to replace all of the previous asynchronous requests or if there is more than one TrgtID in the CTRB. It shall be set to 1 otherwise.’ Also update 8.5.2.1 to indicate that this bit is used with the two request methods.

436 - ACCEPT IN PRINCIPLE. Add the following at the end of sentences on ln 31:35 'The fragmentation and defragmentation of these commands use the same method as data frames, described in {xerf 8.7} and update 8.7 by replacing all occurences of MSDU with "MSDU/MCDU", define MCDU in the acronyms clause as "MAC command data unit"

59, 68 - (Push) Make MaxTransferUnitSize to PHY depedent in table 56, define it in clause 11.2.8 to be 8091 octets.

69 - (Push) Add a MAC sublayer parameter "aMinFragmentSize" in Table 56 on page 215, and set this to 128 (octets). If fragmentation is in use, DEVs may not transmit frames (except the last) with payloads smaller than this value. Also change the definition of the "Capability" field in association and beacon MMPDUs, as defined on page 126 in Figure 36, by using bits b8-b5 and naming this field "FragmentationThreshold". DEVs must store and use this information on a per-destination DEV basis, fragmenting any frames sent to the DEV when a frame's payload exceeds FragmentationThreshold octets. This relationship holds: aMinFragmentSize <= FragmentationThreshold <= aMaxFrameSize. All fragments except the last shall be sent using the same fragment size.

70 - ACCEPT IN PRINCIPLE. Add: 'A DEV shall support concurrent reception of fragments of at least three MSDUs.'

60 - ACCEPT IN PRINCIPLE. Add a sentence that says 'The smallest size of a fragment, excluding the last fragment shall be at least aMinFragmentSize.' and define aMinFragmentSize in table 56 to be PHY depdent, and define it in 11.2.8 to be 128 octets.

189 - ACCEPT IN PRINCIPLE. After 'aMaxFrameSize-4, inclusive.' add 'Note that null data frames, I.e. a zero length are allowed. For example, a null data frame may be used with Dly-ACK negotiation, {xref Dly-ACK}.'

95 - ACCEPT IN PRINCIPLE. After 'the frame control field.' add 'The payload field in the secure MAC frame body is protected as indicated {xref 10.2.4.2}.'

191 - ACCEPT IN PRINCIPLE. The FCS is always in a secure frame, therfore, change the octet indication for the FCS to be only 4.

183 - Pending new text.

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

322 - ACCEPT IN PRINCIPLE. Delete the table and the subclause.

249 - ACCEPT IN PRINCIPLE. Change the SPS info field in figure 64 to be the PS info field and add definition, 'The PS info field is defined in {xref 7.5.7.1}.'

42 - Accept in principle, “Add text to subclause 8.2.3 that says "In the MSC, the MLME-PNC-HANDOVER.rsp is sent when the DME is ready for the handover and is not tied to the arrival of the PNC handover information commands or SPS inquiry response commands." Move the MLME-PNC-HANDOVER.rsp arrow for it so that it happens in the middle of the messaging. Note this happens after the optional ACL handover which needs to be added to the MSC as well via CID 232.”

442 - REJECT. The standard has stated since before D09 and LB12 that a DEV shall accept the nomination to become the new PNC. Therefore, it is not possible to have a rejection code because this behavior is not allowed. If a DEV really doesn't want to do it, it could disassociate in the middle of handover and reassociate with PNC capable bit set off.

161 - Accept.

297 - ACCEPT IN PRINCIPLE. If the request is for a private pseudo-static GTS, and the PNC will not support the creation of a child piconet, it shall respond with the reason code set to ‘request denied’.

275 - ACCEPT IN PRINCIPLE. If the PNC rejects the formation of a child PNC for any other reason than insufficient channel time or unable to allocate as pseudo-static, it shall send the channel time response command with the reason code set to ‘request denied’ (check final text with Bob Huang).

547 - ACCEPT IN PRINCIPLE. Change the text 'Figure 92 illustrates the relationship between the parent piconet superframe and the child piconet superframe. Note that in the figure the superframe periodicity is the same for both the child and the parent piconets.'

148 - Accept.

57 - Accept.

72 - Mark Schrader to provide reference.

544 - ACCEPT IN PRINCIPLE. Change the minimum to be 2 (the current PNC and the new one) add {xref 7.2.x.x} as the maximum. Change the valid range for number of handover beacons to be ’As defined in {xref 8.2.3}’

66 - ACCEPT IN PRINCIPLE. Change line 43 to read "source and destination DEVID, by communicating in an unspecified manner with the DME, which maintains this information."

39 - ACCEPT IN PRINCIPLE. Change the description to read "A set of DEV record elements for all of the DEVs currently associated in the piconet." Ed. Note: Check globally for DEV information elements to change to DEV record elements.

475 - ACCEPT IN PRINCIPLE. 1. and 2. Merge the two subclauses, text is:

’8.2.6.4 Parent PNC termination of a dependent piconet

If the parent PNC wishes to stop the child piconet, it shall terminate the stream allocated to the child piconet using the isochronous stream termination procedure, 8.5.1.3. If the parent PNC wishes to stop the neighbor piconet, it shall send a disassociate request, 8.3.4, to the neighbor PNC. In either case, the dependent PNC shall either change channels, join another piconet as a dependent piconet or immediately initiate its shutdown procedure, 8.2.6. The parent PNC shall listen for the dependent PNC shutdown beacon sequence to determine when the dependent piconet CTA should be removed. The parent PNC may set a maximum time for the completion of the dependent shutdown sequence, after which the CTA will be removed regardless of the completion of the dependent shutdown procedure. In the case of a child piconet, this timeout is set in the MLME while for a neighbor piconet, this time is set via the MLME-DISASSOCIATE. request primitive, 6.3.6.1. If the dependent PNC is a neighbor that is not 802.15.3 compliant, the parent PNC shall provide the same time as it allows for its own shutdown sequence, for the neighbor PNC to cease operations as a dependent piconet of the parent piconet before removing its private CTA.’

3. Not all timeouts are communicated in the standard, for example the time that a DEV attempts a packet transmission. In addition, the dependent PNCs requirement for shutting down is unknown the parent PNC. Due to the added complexity to add a new command to handle this case, the TG decided not to send the timeout information.

4. The standard does not require a PNC to disassociate a child PNC when it terminates the child piconet's CTA. However, in the case of a neighbor, the process is to disassociate the neighbor, because its only purpose in being in the piconet is to act as a neighbor PNC.”

150 - Accept.

152 - ACCEPT IN PRINCIPLE. Add text to the end of line 10 on page 60, 'If the PNC info command was received as an unsolicited frame then the DME is informed of the current information for all of the DEVs currently a member of the piconet.'

41 - ‘Add a new field to PNC handover request, 1 octet, title "Handover status". Add the following description for the field 'The handover status field shall be set to 0 when the PNC is starting the PNC handover process with destination DEV. It shall be set to 1 if the PNC is cancelling the handover process with the destination DEV.'

Add a parameter to MLME-PNC-HANDOVER.{request, indication}, called HandoverStatus. Add HandoverStatus to the table with type enumeration, valid range STARTED, CANCELLED, description: Indicates if the PNC is beginning or cancelling a handover to the DEV.

Add to clause 8, PNC handover, ‘When the handover is initiated, the HandoverStatus is STARTED. If the handover timer expires, the PNC handover command shall be sent to the DEV with a HandoverStatus of CANCELLED.’

Also add text to clause 8 that indicates if the DEV sees a shutdown IE from the PNC during the handover process, it knows that the handover was cancelled.

218 - Accept.

548 - ACCEPT IN PRINCIPLE. Delete all of the parameters except ResultCode from the MLME-START.confirm primitive. In 6.3.3.2.2, change ‘If all of the channels for the PHY are either occupied by other 802.15.3 piconets or have unacceptable then the ResultCode shall be set to CHANNEL_BUSY.’ to be ‘If the channel for the PHY is either occupied by other 802.15.3 piconets or has unacceptable interference, then the ResultCode shall be set to PICONET_DETECTED.’. Change ‘as either a regular DEV, child or neighbor piconet’ to be ‘as either a regular DEV or a dependent piconet’

31 - Accept.

145 - Accept.

129 - Accept.

32 - Accept.

17 - Accept.

471 - ACCEPT IN PRINCIPLE. Add the DEVID field to the PNC handover IE as indicated in CID 221.

470 - ACCEPT IN PRINCIPLE. Add the DEVID field to the PNC handover IE as indicated in CID 221.

135 - Accept.

424 - ACCEPT IN PRINCIPLE. Change "Vendor ID" length to 3 octets, change the definition to be 'The vendor ID field is the OUI as assigned by the IEEE RAC." (Ed. Note, find out best reference) Add OUI to acronyms as "Organization unique identifier' (Ed. Note verify this).

313 - Accept.

209 - ACCEPT IN PRINCIPLE. Add a sentence to the end of line 5, page 107, 'The PNID shall be set to the current PNID for the piconet and is used to identify frames from DEVs in the piconet.' Change 0x00 in stream index to be 0x00 or 0xFD.

207 - ACCEPT IN PRINCIPLE. Add a sentence to the end of line 5, page 107, 'The PNID shall be set to the current PNID for the piconet and is used to identify frames from DEVs in the piconet.' Change 0x00 in stream index to be 0x00 or 0xFD.

205 - ACCEPT IN PRINCIPLE. Add a sentence to the end of line 5, page 107, 'The PNID shall be set to the current PNID for the piconet and is used to identify frames from DEVs in the piconet.' Change SEC Interpretation on reception to: May be decoded.

204 - ACCEPT IN PRINCIPLE. Add a sentence to the end of line 5, page 107, 'The PNID shall be set to the current PNID for the piconet and is used to identify frames from DEVs in the piconet.' Change SEC Interpretation on reception to: May be decoded.

202 - ACCEPT IN PRINCIPLE. Add a sentence to the end of line 5, page 107, ’The PNID shall be set to the current PNID for the piconet and is used to identify frames from DEVs in the piconet.’

200 - ACCEPT IN PRINCIPLE. Add a sentence to the end of line 5, page 107, ’The PNID shall be set to the current PNID for the piconet and is used to identify frames from DEVs in the piconet.’

153 - Accept.

144 - Accept.

151 - Accept.

137 - Accept.

19 - Accept.

36 - Accept.

278 - Accept.

540 - Accept.

337 - ACCEPT IN PRINCIPLE. Page 99, line 31 second sentence "Add this is called an extended beacon." Also add a definition to clause 3 "extended beacon - A beacon followed by one or more broadcasted probe commands from the piconet controller."

14 - Accept.

266 - Withdrawn, 12 September, 2002.

29 - Accept.

28 - Accept.

178 - Accept.

25 - Accept.

266 - Withdrawn, 12 September, 2002.

62 - Accept.

30 - Accept.

504 - ACCEPT IN PRINCIPLE. Change "aMinChannelScan" to "aMinChannelScan and less than the shortest ATP of any of the current member DEVs in the piconet"

47 - Accept.

545 - ACCEPT IN PRINCIPLE. Change BeaconDuration to SuperframeTiming.

501 - REJECT. While it is true that the stream index uniquely identifies the source of an isochronous stream, it is not true of commands or asynchronous data where many sources share a single stream index.

456 - Accept.

26 - Accept.

512 - REJECT. While we all appreciate the hard work that goes into reviewing a document for letter ballot, neither the ballot resolution committee nor the task group has the power to set the length of the letter ballot. The working group voted to set that duration.

142 - Accept.

138 - Accept.

247 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 249.

21 - ACCEPT IN PRINCIPLE. Add a sentence to page 138, line 53, "Note that asynchronous CTRBs are not passed in this command, thus the num targets field is always 1 and so the CTRBs are all of a fixed length."

245 - Withdrawn, 12 September, 2002.

441 - ACCEPT IN PRINCIPLE. Resolve as indicated in CID 41.

196 - ACCEPT IN PRINCIPLE. Add the text from 02/273r18, 2.1.7.2.2.

96 - Accept.

72 - ACCEPT IN PRINCIPLE. ANSI X3.66-1979: Advanced data communication control procedures (ADCCP). Change the reference clause 7.2.7.2 to be "ANSI X3.66-1979"

6. Status Thursday, 3:30 pm in Monterey

.

Table 17—Ballot resolution as of close of Monterey meeting

Type	LB19	Unresolved as of 13 September, 2002
T (technical)	72	31
TR (Technical required)	326	172
T and TR	398	203
E (editorial)	153	153
Total	551	356

7. Status at closing in Monterey

.

Table 18—Ballot resolution as of close of Monterey meeting

Type	LB19	Unresolved as of 13 September, 2002
T (technical)	72	17
TR (Technical required)	326	117
T and TR	398	134
E (editorial)	153	153
Total	551	287