Cl **00** *SC* **00** *P* **00** *L* **00** # **154**

Gubbi, Rajugopal Independent

Comment Type **TR** *Comment Status* **R** *ASIE*

Remove app-specific IE ref: CID 446, 477, 478 and 479 - LB19, CID 71 - LB22. Use of Vendor specific command is the answer to the issue that is intended to be solved through this app-specific IE. This is expecially since neither the standard nor an implementation of PNC can force the interpretation of bits in the currently undefined payload of this IE at each DEV which may be implemented by variety of vendors with their own "application" specific interpretations of those bits.

SuggestedRemedy

Make the change as requested.

Proposed Response *Response Status* **U**

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

Cl **00** *SC* **00** *P* **00** *L* **00** # **152**

Gubbi, Rajugopal Independent

Comment Type **TR** *Comment Status* **R** *IFS*

Replace MIFS with SIFS ref: CID 68 - LB22
- MIFS is less than SIFS
- it does not result in any significant time eficiency given the low probability of its use
- But introduces yet another IFS at the lowest level of MAC
- Mandates that the receive frames be processed within MIFS instead of SIFS since the worst case IFS is MIFS and hence drastically increases the complexity at the MAC and PHY
Remove MIFS and use SIFS in its place.

SuggestedRemedy

Make the change as requested.

Proposed Response *Response Status* **U**

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

Cl **00** *SC* **00** *P* **00** *L* **00** # **151**

Gubbi, Rajugopal Independent

Comment Type **TR** *Comment Status* **R** *CTA/M*

Remove MCTA scheme from the standard ref: CID 536 - LB12, CID 513 - LB19, and CID 63 - LB22. Why can't the open and association be performed in CAP instead of devicing a new mechanism altogether for such a relatively low probability events? what is the point in having another collision based access mechanism inside a declared "collision free period (CFP)". If the concern is about a new PHY that may be added in the future, this mechanism can be added at the time of including the new PHY as allocations to a currently reserved stream ID (or DEVID) so that the legacy DEVs keep off of those slots and the new DEVs use them as per the new rules.

SuggestedRemedy

Make the change as requested.

Proposed Response *Response Status* **U**

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

Cl **00** *SC* **00** *P* **00** *L* **00** # **150**

Gubbi, Rajugopal — Independent

Comment Type **TR** *Comment Status* **R** *CTA/M*

Remove Slotted aloha scheme from the draft ref: CID 537 - LB12, CID 387 - LB19, and CID 56 - LB22. What is the point in having slotted aloha access in addition to the backoff in CAP, TDMA in CFP? I don't see any justification in having yet another access scheme with WPAN. Why is this unncessary additional complexity being forced on to the implementors of this "low cost", "low complexity" and "low power" standard? If some future PHYs need it, let this be added as and when such a PHY is added to the 802.15.3 standard.

SuggestedRemedy

Make the change as requested.

Proposed Response *Response Status* **U**

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

Cl **07** *SC* **7.2.7.5** *P* **113114** *L* # **356**

Struik, Rene — Certicom Corporation

Comment Type **TR** *Comment Status* **R** *FrmFrmt/FCS*

the description of the FCS field is completely unclear. It is unclear whether the provision of a CRC check and the verification hereof are inverses of one another: conversion between bit strings and polynomials and encoding/decoding procedures lack clarity and precision. Moreover, statements as 'in the absence of transmission errors …' (Page 114, line 2) lack meaning.

SuggestedRemedy

replace the text by an unambiguous and clear description of the encoding/decoding procedures.

Proposed Response *Response Status* **U**

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

Cl **07** *SC* **7.3.1.1, Figure 13** *P* **115116** *L* # **360**

Struik, Rene — Certicom Corporation

Comment Type **TR** *Comment Status* **R** *FrmFrmt/Bcn*

The piconet controller should indicate in its piconet mode field (see Figure 13) the security policy the piconet adheres to. Currently, it only indicates whether security is ON or OFF, but this does not sufficiently indicate other security characteristics, such as the minimum bit-security level at which access control in the piconet is arranged. This information, in the current D15 draft contained in the Security Requirements Field (see Table 54), logically belongs in the piconet mode field and should be moved there.

SuggestedRemedy

Change the Draft D15 text to accommodate for this sound security policy principle and adopt impacted text, both in Clause 7.3.1.1 and in Clause 7.5.2.2. See also the discussion in document 02/364r2.

Proposed Response *Response Status* **U**

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

Cl **09** *SC* *P* *L* # **373**

Struik, Rene — Certicom Corporation

Comment Type **TR** *Comment Status* **R** *SEC/Key*

In the current draft, if devices do not yet share a key, these use the broadcast key. This creates a false sense of security.

SuggestedRemedy

Suggested remedy: correct this violation of proper security policy.

Proposed Response *Response Status* **U**

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