Miscellaneous Comments on Draft 6.0

Simon Black, Intalk

Below some comments submitted following a review of D5.2/D6. All comments are provided in the best interests of improving the draft before recirculation ballot.

1. MA-UNITDATA.indication has a status in it, documented as "The reception status parameter indicates the success or failure of the received frame for those frames which 802.11 reports via a MA-UNITDATA.indication". This seems of limited use - what status conditions can be reported other than success? The possible failure conditions appear to be CRC failure, partially received fragmented frames that timeout, WEP failures, and invalid MAC headers which all result in the incoming frame being "discarded without indication to LLC".

2. In MLME-SCAN.request, no units are quoted for ProbeDelay - microseconds would seem to be appropriate.

3. MLME-SCAN.confirm has no status parameter; it should have one for protocol errors - an example would be for example swapping min and max channel times in the primitive. In this case one does not have the information to do a sensible SCAN. These things should be handled as parameter errors and there should indeed be a status returned in the MLME-SCAN.confirm with valid values SUCCESS and INVALID PARAMETERS. If one submits a primitive with invalid parameters then an immediate MLME-SCAN.confirm should be issued with a status of invalid parameters.

4. aAuthenticationAlgorithms is listed under oSMT (11.4.2.1.1), but not under Station Management Attributes (11.4.1.1.1); it is also neither listed in an attribute group, nor listed explicitly as ungrouped. It should I believe be in the agStationConfiggrp (for consistency since it is defined in 14.4.4.1.2).

5. The "Generic Management Primitives" section, 10.2, says that an MLME reset primitive "may include a list of attributes for items to be initialized to non-default values"; however, the parameter set, both here and at 10.3.9.1, is "-none-". My opinion is that primitives are exactly what there name suggests - primitive. So following this logic leads me to suggest that MLME reset should not have any parameters.

6. A MLME reset is said to be mandatory prior to a MLME-SCAN. I'm not sure why you would want to mandate this since MLME SCAN carries all of the parameters that sensibly need to be set (and others that are non-default may have to be set via MLME-SET regardless of the MLME-RESET or not). I suggest that this is removed.

7. aMulticastReceivedFrameCount is named inconsistently: "Frame" is sometimes absent (in attribute group definitions).

8. The PICS for FH says that aSlotTime, aRxTxTurnaroundTime, and aSIFSTime are mandatory attributes (for some reason!). The DS part of the PICS doesn't seem to care about the MIB at all. Please be consistent between PHYs as to whether the MIB, or parts of it, are mandatory

9. aPrefMaxMPDUFragmentLength (agPhyRateGroup, 13.1.1.2) is defined in section 13, would be handy to know from the MAC's point of view, and isn't instantiated in any of the PHY definitions.

10. The definitions of antenna-related PHY MIB groups are inconsistent. In 13.1.1.3, agPhyAntennaGroup contains only aCurrentTxAntenna and aDiversitySupport, while in 13.1.3.3 it adds aSupported[TR]xAntennas and aDiversitySelectionRx, which in 13.1.1 are under 13.1.1.9, agAntennasList. The latter is also defined at 13.1.3.9, as agAntennaListGroup...

11. ListenInterval should not be in be in a PowerMgmt.req primitive, given that it's communicated to the AP in an association request frame. It's not used in an IBSS, so it could be in the Associate.req/Reassociate.req primitives instead. An explicit reassociation is required to change this value - there is no way to communicate information to the AP for the MLME-PowerMgmt.req. primitive.

12. I believe that certain PHY MIB attributes should have no external interface: for example, aCurrentDwellTime. The MLME START primitive passes an FH parameter set, which includes dwell time; aCurrentDwellTime is defined as Integer, GET-REPLACE, but with a description of "The current time in Kus that the transmitter shall operate on a single channel, as set by the MAC". This seems to apply that it's accessible at the MLME-PLME interface, but not at the external PLME-SAP. I'm not sure whether this is worth fixing … silly implementations will break things … opinions ?

13. The textual definition of aMaxTransmitMSDULifetime (D6.0 s9.4) and the MIB definition (11.4.4.2.19) conflict. The former says that the timer starts on receipt of the MAUNITDATA.request primitive from LLC; the latter starts at initial transmission of the MSDU. The former also appears to state that you should terminate an active fragment burst, discarding remaining fragments at timer expiry, while the latter is more forgiving. I prefer the MIB definition … it's consistent with the receive side.

14. The standard is very confused on frames allowed in DCF. 9.2 says "Data frames sent during under the DCF shall use the Frame Type Data and Subtype Data."; but 9.3 says "Data frames sent during under the DCF shall use the Data Subtypes: Data, or Null Function". I think the 9.3 definition is correct. Null frames cause no indication to LLC and should not be relayed to other stations in the BSS.

15. It occurs to me that there is a problem with aExcludeUnencrypted behaviour:

    Section 7 is fine. It says: "The Frame Body consists of the MSDU or a fragment thereof, and a WEP IV and ICV (if and only if the WEP subfield in the frame control field is set to 1). The frame body is null (zero octets in length) in Data frames of Subtype Null Function (no data), CF-Ack (no data), CF-Poll (no data) and CF-Ack+CF-Poll (no data)." So no WEP in CF control frames. Now …

    CF-Ack has a null data field, and thus no WEP IV or ICV; by "if and only if" I infer that it thus must have the WEP subfield set to 0. Close, but no banana – since a STA with aExcludeUnencrypted set then bins CF-Acks.

    The problem is probably in s8.3.2 which says: "When the boolean attribute aExcludeUnencypted is set to True, MPDUs of type Data received by the station with the WEP subfield of the Frame Control Field equal to zero shall be discarded". This should say something like "… MPDUs of Type Data with a frame body that is not null (no data) that are received …"

16. There is a change to the third paragraph of s8.3.2, which changes behaviour when a null key is used from (5.0) an error, to (6.0) no encryption, but with IV and ICV still inserted and checked. This is not a good change since it effectively gives a way to get data frames to STAs that have aExcludeUnencrypted set. It also seems to be a departure from true RC4 - since you are defining a special condition where the algorithm is different. I strongly recommend that we revert to the D5.0 state.

17. The PLME reset primitive is not defined in Section 10.4.

18. Section 10.3.9.2 refers to a MLME reset procedure … where is the behaviour of this defined then ?

19. In section 10.3.2.1 (MLME-SCAN) aProbeDelay should have the 'a' removed - also note upper case on MinChannelTime in definition of MaxChannelTime.

20. Preauthentication (5.4.3.1.1) is not possible without two radio's. Since the MAC cannot support multiple simultaneous PHYs then Preauthentication is not possible except via the DS. I suggest removing this entirely since anything else would seem the require too much controversy !

21. aStationID … I think this takes a locally administered MAC address … but we don't use this anywhere in the Standard ! Please clarify.

22. There are some station management MIB attributes defined … but in figure 65 (clause 10) there is no SME MIB and GET/SET primitives. How exactly does one GET/SET SME attributes then - using MLME-SET/GET ?!

23. In section 11.2.2.4 (d) you probably want to allow ACK frames in an ATIM window … else nothing is going to get very far !

24. In section 11.2.2.1 paragraph 4 first line typo 'that' should be 'than'

25. In section 11.1.2.1 it uses the text 'medium sensed to be unavailable' … this is a poor definition … does it included NAV. Should say for instance 'determined to be busy' according to clause xx.xx. It would then be clear whether this included NAV.

26. Section 9.2.5.2 fourth paragraph is unclear - particularly the DIFS/EIFS as appropriate. I believe that this refers to the success, or failure of the frame that caused medium busy. I also assume that a DIFS is used even if a PHY.RX.START indication does not result from the medium activity … though this is not stated explicitly. The timing reference point of such a DIFS is not clear … since clause 9.2.10 suggests it should be the last symbol on the medium … in this case is this the last correctly received symbol … what if there was CCA and no data recovery? This has an impact on interoperability.

27. Some time points for MIB attribute applicability have been included in the major redraft of 8.3.2. I accept the need to have something but these points are not consistent with the WEP application - which is per MPDU and imply that historical WEP attribute values must be kept with each MPDU since those MPDUs can be delayed within the MAC (fragmentation, power management, …). I would suggest using WEP attributes at the time of transmission if a point in time is required. It is up to SME to coordinate things.

    There is a similar problem for authentication where the attribute values at the time of a previous frame reception are used.

    I see the intent … but one can still screw things up even with the synchronisation points proposed. I would prefer to avoid keeping all this state with each MPDU.