Section 5 comments from Ballot on Draft Standard D2 (Vic Hayes, Chair, AT&T WCND)

Seq. #	Section number	your ini-tials	Cmnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
	1.X, 2.X, 3.X 4.X, 5.X, 6.X 7.X 8.X	BD	E	N	My editorial comments are contained in the files D2lb_edx.doc (where x is the relevant major section number) which were submitted along with this ballot response. All comments in these files are purely 100% editorial in nature (incorrect fonts, extra blank lines, misformatting etc). Any change for which there was any question in my mind that anyone might think it other than editorial, I have included as separate comment in this table.	Doc D2 is of Insufficient quality. 1) There are numerous editorial errors in the D2 draft which need to be corrected before the draft can be forwarded for sponsor ballot. The editorial errors range from incorrect fonts in the middle of sentences & page formatting to a dire need to have a spelling check run on the document. 2) While no single item is enough to prevent forwarding of the draft, in aggregate they impact the draft quality to such an extent that it would be embarrassing to forward it in this state. I have forwarded to the editors a marked up copy of the draft showing the editorial errors I noticed during review (this was at the editors request, for various obscure reasons a hard copy was requested over an electronic copy as being easier to deal with in this instance). 3) Additionally all the section X.X, Y.Y etc place holder in the text need to be found and changed to correct section references.	
	5	FMi	T	N	Leave the current wording in clause 5, whereby WEP is applied to MSDUs not MPDUs. This actually involves NOT correcting the editing error which failed to incorporate changes to MPDU adopted at the July, 1995 meeting. This "non–change" is further described in	The reasons why applying WEP on a per–MPDU basis are less efficient and add unnecessary overhead are discussed in detail in document 95–187.	

Seq. #	Section number	your ini-tials	Cmnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
					document 95–196		
	5	FMi	T	N	Leave the current wording in clause 5, whereby WEP is applied to MSDUs not MPDUs. This actually involves NOT correcting the editing error which failed to incorporate changes to MPDU adopted at the July, 1995 meeting. This “non–change” is further described in document 95–196	The reasons why applying WEP on a per–MPDU basis are less efficient and add unnecessary overhead are discussed in detail in document 95–187.	
	5	**vj**	**T**	**N**	**refer to doc 95/187 and 95/196**	**revert wep applic to msdu per recomendations in paper(s)**	
	5.	**MB**	**e**		**numerous typographical errors in this section.** **It would be helpful to show an example of the Open Frame bit map as was used in section 4.2**		
	5.1	BTh	e		**correct spelling...** indicated iden~~f~~ti~~t~~fying with re~~r~~spect	typo, typo, typo	
	5.1	TM	e		correct spelling of idenfitfying to identifying correct witherspect to with respect add ‘the’ to ... to *the* authentication algorithm		
	5.1	**ws**	**e**		**“are self idenfitfying witherspect to authentication” should read “ are self-identifying with respect to authentication”**		
	5.1.1	BTh	e		**correct spelling and capitalization...** authenticated sysetem ~~I~~identity	typos identity assertion seems like an action instead of a proper noun in this sentence	
	5.1.1	TM	e		correct authentcated to authenticated correct syetem to system		
	5.1.1	**ws**	**e**		**the capitalization of the sub headings is inconsistent throughout 5.1.1**		
	5.1.1.1	TM	e		correct algortithm to algorithm correct infromation to information		
	5.1.1.2	TM	e		correct authenticatiing to authenticating		
	5.1.1.2	**ws**	**e**		**under Information Items - “infromation” should be**		

Seq. #	Section number	your initials	Cmnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
					“information”		
	5.1.1.2	**ws**	**e**		**under Direction of Message - “authenticatiing”**	**spelling**	
	5.1.2	BTh	e		**correct spelling...** which	typo	
	5.1.2	BTh	E		**change 2nd sentence in 2nd paragraph...** This shared key is stored via the MAC management path in a MIB variable that is read-only for the MAC.	As written in std. we are writing to a read-only variable, one of the classic oxymorons.	
	5.1.2	TM	e		correct wich to which correct independnt to independent		
	5.1.2	**ws**	**e**		**2nd paragraph - “wich”**	**spelling**	
	5.1.2.1	TM	e		correct algortithm to algorithm correct infromation to information		
	5.1.2.2	BTh	e		**correct spelling...** fileld	typo	
	5.1.2.2	TM	e		correct Challlenge to challenge correct filed to field		
	5.1.2.2	**ws**	**e**		**under Information Items - “filed” and “Challlenge”**	**spelling**	
	5.1.2.2 **4.1.2.2**	**DW**	**T**		**It should be better specified how the 128 octets challenge text is generated, and what it contains. It should either include a IV field, or use a default to be specified IV. An ICV would not be needed, but the standard should specify the format such that it is clear whether it is includeuded or not.**	**Sinse this is encryption within a subfield, we do not need to specify the IV/ICV format to be equal to the normal payload format.** **Specifying an IV as the first 4 octets of the 128 octet field is I think most desirable.**	
	5.1.2.2	**DW**	**T**	**Y**	**The “Shared Key Authentication” method should be deleted from the standard, because it does not provide any additional authentication level above the “Open System Authentication” with WEP enabled for data transfers.**	**Shared Key Authentication depends on both sides having the same WEP key. This is exactly equivalent to the the implicit authentication that is achieved with the “Open Authentication”, combined with WEP on for all data traffic.** **This does also rely on both sides havingthe same correct key.**	
	5.1.2.3	TM	e		correct recieved to received correct algortithm to algorithm correct infromation to information		
	5.1.2.3	ZJ	t	N	Add the following: “Notice that both the challenge text	Attackers can decrypt the first 128	

Seq. #	Section number	your ini-tials	Cmnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
					and the encrypted challenge text are transmitted. This allows an eavesdropper to determine the PRN sequence associated with the given key/IV pair. Implementations should therefore not use the same IV for any future frame exchanges."	octets of any subsequent transaction with the same key/IV.	
	5.1.2.4	TM	e		correct recieves to receives correct suffcient to sufficient correct algortithm to algorithm correct infromation to information		
	5.14. 2.3.9	FMi	t	N	Add material and make changes from Clause 3 of document 95–222 on combined Authentication and (Re)Association frames. • 4.2.3.9: Define the combined frame format. • 5.1: Add new subsection 5.1.3 on usage rules for the combined frames.	Allowing a (Re)Association request to be combined with the first frame in the Authentication sequence, and the corresponding (Re)Association response to be conbined with the final frame in the Authentication sequence improves efficiency, especially for faster BSS–transition reassociations, without requiring these mechanisms be combined in mandatory usage, nor preventing the addition of future authentication algorithms which require a different number of authentication frames to be exchanged.	
	5.2	TM	e		remove two instances of P802.11 to 802.11 for consistency with this section and whole document		
	5.2	**Smr**	**t**			In my copy of the standard, the WEP functions on a MSDU. This should be on MPDU as voted by the body.	
	5.2	**SA**	**T**	**N**	**Replace MSDU based encryption with MPDU based encryption as agreed at the July meeting.**	**Hardware based encryption/decrytion is much simpler at the MPDU level than at the MSDU level, while software based encryption would be modestly more expensive.** **A hardware mechanism that only needs to initialize the PRNG based on an IV and the key is much simpler**	

Seq. #	Section number	your ini-tials	Cmnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
						than one that needs to be able to do that plus save and restore intermediate states for up to six MSDUs. **The software mechanism would require that the PRNG be initialized for each MPDU, whereas it 'may' be faster to save and restore intermediate states. However , this expense is easier to absorb in a software implementation than in a hardware one.** **Finally, encryption at the MPDU level would discourage the reuse of IVs which is probably a good idea since that compromises the strength of the encryption algorithm.**	
	5.2.1	**PP**	**e**		**Suggest changing references to "P802.11" to "802.11"**		
	5.2.1	BTh	E	N	**add...** This service is intended to provide functionality for the Wireless LAN subjectively equivalent to that provided by the physical security...	The original definition of WEP in 1.1 uses this language which is important to maintain.	
	5.2.1	BTh	E	N	**correct sentence...** Data confidentiality depends on an external key management service to ~~authenticate users and~~ distribute data enciphering/deciphering keys.	Of course external key management service does not authenticate users. If the author meant that the external key management is charged with delivering the keys only to those who are supposed to have it, then please write a sentence to say that.	
	5.2.1	BTh	E	N	**rewrite...** ~~P802.11 specifically recommends against r~~Running an 802.11 LAN with privacy but without authentication is possible, but it leaves the system open to ~~significant~~ security threats.	I object to the editorial comments. The statement of the facts will suffice.	
	5.2.1	**DW**	**T**	**y**	**The second paragraph declares that privacy without authentication does not make much sense. This**	**Privacy without authentication does make much more sense, because if**	

Seq. #	Section number	your ini-tials	Cmnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
					sentence should be dropped, because in my view it is the other way around. Authentication without Privacy does not make any sense.	**WEP is in use, then the fact that the other station does indeed have the correct key provides sufficient implicit authentication.**	
	5.2.2	BTh	E		add... Export from the United States of America:	Since this is an international standard we should be specific in the title as well as the body of the text.	
	5.2.2	GE	T	X	Change optional to mandatory	This WLAN should provide the same or close to the same security of a wired network. We have got a license to export the RC4 algorithm as well as others. This should not be a reason to make this an option. This also fails to make units interoperatable for security purposes when some stations don't implementation the WEP algorithm.	
	5.2.3	BTh	e		add... initialization vector<period>	typo	
	5.2.3	TM	e		add period --- initialization vector. The WEP ...		
	5.2.3	TM	e		correct realtive to relative correct last sentence --- passed to LLC and and error ...		
	5.2.3	**ws**	e		**in Figure 5-2 the I in Integrity is off**		
	5.2.3	**BD**	**T**	**N**	**Correct text per doc 95/212.**	**Motions passed not reflected in D2, see 95/212 for D2 corrections.**	
	5.2.3	**BSi**	**T**	**N**	**Change WEP encryption back to being on an MSDU basis, not MPDU (change was not properly made in text anyway)**	**Aim was efficient implementation in software or hardware. Compute overhead too high for efficient implementation in software when on an MPDU basis. See Mike Fischer's paper 95/187.**	
	5.2.3	**BSi**	**T**	**N**	**Chane ICV to CRC-16**	**Aim was efficient implementation in software or hardware. CRC-32 quite inefficient in software. See Mike Fischer's paper 95/187. (Also note Kerry's comments on CRC-16/CRC-32 which may over-ride my comment).**	

Seq. #	Section number	your ini-tials	Cmnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
	5.2.3	**BSi**	**t**	**N**	**Paragraph starting 'For WEP protected frames ...' define whether msbyte or lsbyte is padded for 16 bit WEP IV in 24 bit field**	**Position of 16 bit WEP IV in 24 bit field not specified.**	
	5.2.3	BTh	T	N	**change 3rd paragraph preceding Figure 5-3...** the first four octets of the ~~F~~frame Body contain the IV field...	The first 4 octets of the frame are in the MAC header and are not the IV field.	
	5.2.3	BTh	T	N	**Missing some important information in 3rd paragraph preceding Figure 5-3. In 2 places is says the WEP IV is 16 bits to be placed in a 24 bit field. The standard must specify which 2 of 3 octets contain the IV and what the value for the unused octets must be.**	I don't know the correct answer. We are careful to specify reserved bit values in the header but have totally ignored the same problem here. It would be impossible to construct a compliant MAC without the missing information.	
	5.2.3	BTh	T	N	**in 6th paragraph preceding Figure 5-3 replace two times...** ~~MSDU~~MPDU **in 5th paragraph preceding Figure 5-3 replace...** ~~MSDU~~MPDU **delete entire 4th paragraph preceding Figure 5-3 (beginning "Because IV and"** **in 3rd paragraph preceding Figure 5-3 replace two times...** ~~MSDU~~MPDU **change 2nd paragraph preceding Figure 5-3...** The ~~entire~~ WEP encryption is performed after fragmentation of the MSDU ~~{IV, MSDU, ICV} package may be split into several fragments~~ (depending on the realative values of the MSDU and the active MPDU size), creating {IV, MPDU, ICV} packets. **in 1st paragraph following Figure 5-3 replace...** ~~MSDU~~MPDU	I may have a bad memory but I'm sure we voted to do encryption on individual fragments. If I'm wrong I apologize for wasting the committee's time with this comment. 4th paragraph is entirely incorrect; correcting it would yield a paragraph with the same information as the corrected 2nd paragraph	
	5.2.3 5.2.5 5.3 5.3.1	FMi	t	N	Incorporate changes from relevant sections of document 95–212 to properly describe and depict the IV length and presence of the one–octet pad field, plus a few other editorial fixes. Warning: If these changes, as well as the changes from document 95–211 are adopted, it is important to make these updates BEFORE the updates to 5.2.5 from	Correct error in D2.0 updates (changes were approved at July meeting), see summary section of document 95–212.	

Seq. #	Section number	your ini-tials	Cmnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
					document 95–211.		
	5.2.3	FMi	T	N	If the use of a 16–bit ICV is permitted under the guidelines for expedited CJ approval of cryptosystems, the ICV field should be shortened to 2 octets, and the ICV algorithm should be changed to SLRC–1 (LRC with a 1–bit left circular shift after each octet). If the ICV must remain as 4 octets, the ICV algorithm should still be changed to SLRC–1, but with a 32–bit accumulator. The commenter will provide the text updates for this change once the question of whether a 16–bit ICV is usable has been established.	The major benefit of error detection using CRC is that an n–bit CRC can detect all possible burst errors up to length n–1. Since ICV checking only occurs on data received in a frame with a valid CRC–32 on the MPDU itself, the integrity check function of the ICV does not have to contend with burst errors, so a CRC is unnecessary. CRCs in general, and CRC–32 in particular, are very inefficient to implement in software or firmware on conventional instruction sets. Because one of the stated objectives of WEP is that it may be implemented in either hardware or software, the ICV algorithm should provide comparable information scattering to a CRC, but using calculations which are practical to implement efficiently in either hardware or software. (Furthermore, the details about WEP mechanism, as discussed in document 95–187 imply that even if the ICV was calculated using CRC–32 a hardware implementation would need a separate CRC generator, rather than being able to share the one used for the MAC CRC generation/checking.) A 16–bit ICV achieves a false positive rate of 1.5e–5, which seems more than adequate when applied to CRC–validated ciphertext. Unless required for export approval, the practical advantage of the 2.3e–10 false positive	

Seq. #	Section number	your ini-tials	Cmnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
						rate of the 32–bit ICV is unclear.	
	5.2.3	KJ	T	N	see document 95-212		
	5.2.3	ZJ	t	N	Adopt text for this section from submission 95/212.	It makes sense to transmit the stuff in the order we voted to accept in July.	
	5.2.3	ZJ	T	N	Change ICV length to 16 bits and algorithm to CRC-16	Software implementations of WEP will be encumbered by having to do a CRC-32. The currently specified mechanism is too computationally expensive.	
	5.2.3	TM	E/T	X	The frame formats of section 4 should be updated to show that if WEP is used, the IV must also be transmitted and is an additional part of the frame. The maximum MPDU length should be adjusted accordingly. Some reference is given in 5.2.5		
	5.2.3	TM	E/T	X	Why are three bytes used to send two bytes (16 bit IV). This is in conflict with section 5.2.5 which says the IV is 4 bytes. Either an error has occurred or more information is needed to convey where the 16 bits reside in a 24 bit or a 32 bit field.		
	5.2.3 5.2.5 5.3 5.3.1	**DW**	**T**	**Y**	**Implement the changes as documented in 95/212, such that it reflects the changes as adopted in the July 1995 meeting.**	**Approved changes are not properly included in the draft.**	
	5.2.4	**BA**	**E**		Need to insert RSA document reference.		
	5.2.4	**RJa**	**E**		Need to insert RSA document reference.		
	5.2.4	TM	e		remove extra period correct paragraph justification correct liscense to license		
	5.2.4	BTh	E	N	**need reference document name or number**	How can we be voting to approve a standard when we don't have the references?	
	5.2.4	**BD**	**T**	**N**	Details of the RC4 algorithm are ~~specified in <insert document reference here>~~ available from RSA.	**This was a change adopted in July '95 which apparently did not get included in D2. There is no specific document to reference.**	
	5.2.4	ZJ	t	N	Insert appropriate RSA document reference.	It is needed.	
	5.2.5	**BD**	**T**	**N**	**Correct text per doc 95/212.**	**Motions passed not reflected in D2, see 95/212 for D2 corrections.**	

Seq. #	Section number	your ini-tials	Cmnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
	5.2.5	**BSi**	**t**	**N**	**Figure 5.4 is broken. Initialisation Vector field is three octets, algothithm ID is not shown.**		
	5.2.5	BTh	T	N	**change title of section and delete colon in title...** WEP M~~S~~PDU Expansion~~:~~ **in 2nd paragraph change...** M~~S~~PDU	I may have a bad memory but I'm sure we voted to do encryption on individual fragments. If I'm wrong I apologize for wasting the committee's time with this comment.	
	5.2.5	BTh	T	N	**in 1st paragraph change...** Figure 5-4 shows the expanded M~~S~~PDU Frame Body as constructed... **in 2nd paragraph change...** The expanded M~~S~~PDU Frame Body shall include...	Figure 5-4 doesn't show the entire MPDU frame, just the Frame Body.	
	5.2.5 5.3.2 8.4	FMi	T	N	Incorporate changes from document 95–211 to add a Key ID field to the IV field of the WEP frames to allow many common key management techniques to be used with WEP. Warning: If these changes, as well as the changes from document 95–212 are adopted, it is important to make these updates AFTER the updates to 5.2.5 from document 95–212.	Provide a useful enabling mechanism (already present in HIPERLAN) that is available at no "cost" because there is already space (the pad octet in the IV field) to hold the necessary infomation. For a detailed reasons for and usage of the Key ID, see document 95–187.	
	5.2.5	ZJ	T	N	Change ICV length to 16 bits and algorithm to CRC-16	Software implementations of WEP will be encumbered by having to do a CRC-32. The currently specified mechanism is too computationally expensive.	
	5.2.5	ZJ	T	N	Adopt text from submission 95/211	A mechanism that can be used by higher layers to manage keys is needed.	
	5.2.5	TM	E/T	X	Why are four bytes used to send two bytes (16 bit IV as stated in 5.2.3). This is in conflict with section 5.2.3 which says the IV is 2 bytes (3 bytes on transmit). Either an error has occurred or more information is needed to convey where the 16 bits reside in a 24 bit or a 32 bit field.		
	5.2.5 **5.3.2** **8.4**	**DW**	**T**	**Y**	**Adopt changes as documented in doc 95/211. An exception is the Figure 5-4 which does reference an SDE_SDU of size >=1, with a DSAP, SSAP Control**	**A 2-bit key ID field should be added to allow Key rollover in a dynamic way.**	

Seq. #	Section number	your ini-tials	Cmnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
					and Datafield. This should be replaced by an MSDU with length between 0 and 2304.	**The figure is too specific, and still relates to a 802.10 representation.**	
	5.3	**ws**	**e**		**"section 7.x" should be "7.x"**	**consistency**	
	5.3	ZJ	e		Replace "7.X" with "8.4"		
	5.3	BTh	E	N	**replace...** ~~section 7.X~~8.4	Based on the previous 71 pages the word "section" is not used in references. 8.4 is the best reference I found.	
	5.3	**HDa**	**e**	**N**	This section gives an overview of the security related MIB variables and how they are used. For details of the MIB variable definitions, refer to section 7.X.	**Identify 7.X**	
	5.3.1	**BD**	**T**	**N**	The type of authentication invoked when authentication is attempted is controlled by the MIB variable Authentication_Type. This variable may have the following values: ~~1 =~~Open System ~~2 =~~Shared Key All other values are reserved. The numeric encoding of these values is given in section 4.3.1.7 (Authentication Algorithm Number).	**The values shown are inconsistent with sec 4. I have removed the specific values given in this section and replaced them with a reference to sec 4.**	
	5.3.2	BTh	e		**in 3rd paragraph change...** not allow WEP_D~~E~~efault to be set to TRUE if Default_WEP_Key **in 4th paragraph change...** The MIB supports the ability to have a separate WEP key for each station ~~which~~with which **in the outline beginning "The interactions between these variables" change 4 places...** Tru~~r~~e	typos	
	5.3.2	TM	e		correct deafault to default correct True to TRUE		

Seq. #	Section number	your ini-tials	Cmnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
					correct encypted to encrypted correct DEfault to Default correct Dfault to Default correct false to FALSE		
	5.3.2	TM	e		correct supprts to supports correct station which ~~which~~ a station correct ...WEP_ON fields is FALSE		
	5.3.2	TM	e		correct implmementation to implementation correct dependant to dependent		
	5.3.2	TM	e		under both Transmit Case: and Receive Case: correct WEP_On to WEP_ON correct Ture to TRUE correct Ture to TRUE correct do no encrypt to do not encrypt		
	5.3.2	**ws**	**e**		**"deafault"**	**spelling**	
	5.3.2	**ws**	**e**		**under receive case - "Ture"**	**spelling**	
	5.3.2	**BD**	**T**	**N**	**Add the following as the first paragraph of the section:** **WEP invocation is controlled by MIB variables. An overview of the variables and their usage is given in this section. See Section 8 for the formal MIB definitions of these variables.**	**Tie description of WEP MIB variables to clause 8 where they are (or will be, see separate LB comment in sec 8) defined.**	
	5.3.2 8.4 4.3.1.3	FMi	T	N	Incorporate changes from document 95–198 to provide a means to configure a station to exclude unencrypted MSDUs received from the WM. Also, for 4.3.1.3, incorporate changes from Clause 11 of document 95–222 to add the exclusion of unencrypted frames to the indicated capabilities of a station.	Plug an existing hole in the WEP security model. For details of the problem and a description of this solution, see document 95–187.	
	5.3.2	KJ	T	N	see document 95-198		
	5.3.2	**vj**	**T**	**N**	**refer to 95/198**	**allow exclusion of unencrypted msdus**	
	5.3.2	TM	T	X	What method is used to protect the MIB table from unauthorized access? The MIB holds a WEP_Key_Mapping table which is the key to unlocking all encrypted traffic. This is an exposed interface then so	One possible method is to define a 'super user' password which must be employed before access to sections of (or the entire) MIB are viewable. A	

Seq. #	Section number	your ini-tials	Cmnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
					much for security.	specific packet structure could be defined to accomplish this.	
	5.X	**BD**	**E**	**N**	**Move section 5 to immediately after D2 section 3. (I.e. D2 sec 5 becomes sec 4 and D2 sec 4 becomes sec 5).**	**The text in Section 5 was intended to come after sec 2 (where the information contents of msgs to support the various services are presented), after sec 3 (which introduces security) and before sec 4 (which contains the details of the encoding of frames) - thus the current sec 5 is one section to late in the document. The section was accidentally placed incorrectly into D2 by the editors.**	
	Figure 5-4	BTh	T	N	**change title...** M~~S~~PDU **add to blank box in the expanded IV a legend of...** ID 1 **correct legend in other expanded IV box...** 43 **change in note...** M~~S~~PDU	I may have a bad memory but I'm sure we voted to do encryption on individual fragments. If I'm wrong I apologize for wasting the committee's time with this comment.	