

Seq. #	Section number	your initials	Comment type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
--------	----------------	---------------	-------------------------	-----------------	------------------------	-----------	----------------------

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

1	1.X, 2.X, 3.X 4.X, 5.X, 6.X 7.X 8.X	BD	E	N	<p>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.</p> <p>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.</p>	<p>Doc D2 is of Insufficient quality.</p> <p>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.</p> <p>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).</p> <p>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.</p>	accepted.
2	5	FMi	T	N	<p>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</p>	<p>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.</p>	<p>declined 95/196 rejected by MAC group.</p>
3	5	FMi	T	N	<p>Leave the current wording in clause 5, whereby WEP is</p>	<p>The reasons why applying WEP on a</p>	declined

Seq. #	Section number	your initials	Cmnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
					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	per-MPDU basis are less efficient and add unnecessary overhead are discussed in detail in document 95-187.	95/196 rejected by MAC group
4	5	vj	T	N	refer to doc 95/187 and 95/196	revert wep applic to msdu per recomendations in paper(s)	Declined 95/196 rejected by MAC group
5	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		corrected
6	5.1	BTh	e		correct spelling... indicated idenfitying with_rerspect	typo, typo, typo	corrected
7	5.1	TM	e		correct spelling of idenfitying to identifying correct witherspect to with respect add 'the' to ... to the authentication algorithm		corrected
8 9	5.1	ws	e		"are self idenfitying witherspect to authentication" should read " are self-identifying with respect to authentication"		corrected
10	5.1.1	BTh	e		correct spelling and capitalization... authenticaded sysetem Iidentity	typos identity assertion seems like an action instead of a proper noun in this sentence	corrected
11	5.1.1	TM	e		correct authenticaded to authenticated correct syetem to system		corrected
12	5.1.1	ws	e		the capitalization of the sub headings is inconsistent throughout 5.1.1		corrected
13	5.1.1.1	TM	e		correct algortithm to algorithm correct infromation to information		corrected
14	5.1.1.2	TM	e		correct authenticatiing to authenticating		corrected
15	5.1.1.2	ws	e		under Information Items - "infromation" should be "information"		corrected

Seq. #	Section number	your initials	Comnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
16	5.1.1.2	ws	e		under Direction of Message - "authenticatiing"	spelling	corrected
17	5.1.2	BTh	e		correct spelling... which	typo	corrected
18	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.	corrected
19	5.1.2	TM	e		correct wich to which correct independnt to independent		corrected
20	5.1.2	ws	e		2nd paragraph - "wich"	spelling	corrected
21	5.1.2.1	TM	e		correct algortithm to algorithm correct infromation to information		corrected
22	5.1.2.2	BTh	e		correct spelling... fileld	typo	corrected
23	5.1.2.2	TM	e		correct Challenge to challenge correct filed to field		corrected
24	5.1.2.2	ws	e		under Information Items - "filed" and "Challenge"	spelling	corrected
25	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.	Since 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.	Text corrected. The 128 bit is generated by the Wep PRNG not the total Wep mechanism. The actual value of the challenge is not important, it can be derived from any key (but not a static value or the challenge is rendered worthless).
26	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.	Declined. The commnet indicates that the commentor does not understand the difference between authentication and privacy. There is a significant difference. Authentication identifies entities, privacy protects information flow between entities. Open systems run with null authentication. Shared key

Seq. #	Section number	your initials	Comment type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
							systems require that both sides have a shared secret key (delivered by a mechanism with a secure side channel). Authentication and Privacy are into the same security service. Supportin docs for the comment indicate that the author misunderstands "open authentication" - open does no checks at all. Shared key is the only auth scheme currently in the standard - to remove it is not acceptable.
27	5.1.2.3	TM	e		correct recieved to received correct algortithm to algorithm correct infromation to information		corrected
28	5.1.2.3	ZJ	t	N	Add the following: "Notice that both the challenge text 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."	Attackers can decrypt the first 128 octets of any subsequent transaction with the same key/IV.	Accpeted similar wording inserted.
29	5.1.2.4	TM	e		correct recieves to receives correct suffcient to sufficient correct algortithm to algorithm correct infromation to information		corrected
30	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. <ul style="list-style-type: none"> 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 combined with the final frame in the Authentication sequence improves efficiency, especially for faster BSS-transition reassociations, without requiring these mechanisms be	Declined insufficient reason for new functionality. Possibility looked at in July and not adopted then. Required change in frame formats is not appropriate at this point in the standard process.

Seq. #	Section number	your initials	Comnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
						combined in mandatory usage, nor preventing the addition of future authentication algorithms which require a different number of authentication frames to be exchanged.	
31	5.2	TM	e		remove two instances of P802.11 to 802.11 for consistency with this section and whole document		corrected
32	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.	95/196 rejected - now on MPDU.
33	5.2	SA	T	N	Replace MSDU based encryption with MPDU based encryption as agreed at the July meeting.	<p>Hardware based encryption/decryption is much simpler at the MPDU level than at the MSDU level, while software based encryption would be modestly more expensive.</p> <p>A hardware mechanism that only needs to initialize the PRNG based on an IV and the key is much simpler than one that needs to be able to do that plus save and restore intermediate states for up to six MSDUs.</p> <p>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.</p> <p>Finally, encryption at the MPDU level would discourage the reuse of</p>	95/196 rejected - now on MPDU

Seq. #	Section number	your initials	Cmnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
						IVs which is probably a good idea since that compromises the strength of the encryption algorithm.	
34	5.2.1	PP	e		Suggest changing references to "P802.11" to "802.11"		corrected
35	5.2.1	BTh	E	N	add... This service is intended to provide functionality for the Wireless LAN <u>subjectively</u> equivalent to that provided by the physical security...	The original definition of WEP in 1.1 uses this language which is important to maintain.	declined
36	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.	Accepted
37	5.2.1	BTh	E	N	rewrite... P802.11 specifically recommends against Running an 802.11 LAN with privacy but without authentication is possible, <u>but</u> it leaves the system open to significant security threats.	I object to the editorial comments. The statement of the facts will suffice.	The comment is not editorial in nature - is cautionary. As such, it is proper to caution implementors about subtle, dangerous situations.
38	5.2.1	DW	T	y	The second paragraph declares that privacy without authentication does not make much sense. This sentence should be dropped, because in my view it is the other way around. Authentication without Privacy does not make any sense.	Privacy without authentication does make much more sense, because if WEP is in use, then the fact that the other station does indeed have the correct key provides sufficient implicit authentication.	Declined - please see response to comment 26.
39	5.2.2	BTh	E		add... Export <u>from the United States of America</u> :	Since this is an international standard we should be specific in the title as well as the body of the text.	corrected.
40	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	declined. One export license does not guarantee exportability for all who follow. Also, some situations don't

Seq. #	Section number	your initials	Comnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
						some stations don't implement the WEP algorithm.	require privacy and don't want to pay for the mechanism.
41	5.2.3	BTh	e		add... initialization vector<period>	typo	corrected
42	5.2.3	TM	e		add period --- initialization vector. The WEP ...		corrected
43	5.2.3	TM	e		correct relative to relative correct last sentence --- passed to LLC and and error ...		corrected
44	5.2.3	ws	e		in Figure 5-2 the I in Integrity is off		corrected
45	5.2.3	BD	T	N	Correct text per doc 95/212.	Motions passed not reflected in D2, see 95/212 for D2 corrections.	accepted
46	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.	declined 95/196 rejected by MAC group
47	5.2.3	BSi	T	N	Change 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 override my comment).	declined. It has been specifically pointed out that this change would invalidate the exportability of WEP.
48	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.	corrected in picture 5-4 from 95/212 adoption.
49	5.2.3	BTh	T	N	change 3rd paragraph preceding Figure 5-3... the first four octets of the Eframe Body contain the IV field...	The first 4 octets of the frame are in the MAC header and are not the IV field.	corrected
50	5.2.3	BTh	T	N	Missing some important information in 3rd paragraph preceding Figure 5-3. In 2 places it 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	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	fixed

Seq. #	Section number	your initials	Comnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
					be.		
51	5.2.3	BTh	T	N	<p>in 6th paragraph preceding Figure 5-3 replace two times... MSDUMPDU</p> <p>in 5th paragraph preceding Figure 5-3 replace... MSDUMPDU</p> <p>delete entire 4th paragraph preceding Figure 5-3 (beginning "Because IV and"</p> <p>in 3rd paragraph preceding Figure 5-3 replace two times... MSDUMPDU</p> <p>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 relative values of the MSDU and the active MPDU size), creating {IV, MPDU, ICV} packets.</p> <p>in 1st paragraph following Figure 5-3 replace... MSDUMPDU</p>	<p>MAC without the missing information.</p> <p>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.</p> <p>4th paragraph is entirely incorrect; correcting it would yield a paragraph with the same information as the corrected 2nd paragraph</p>	95/196 decision makes it on MPDUs.
52	5.2.3 5.2.5 5.3 5.3.1	FMi	t	N	<p>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.</p> <p>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 document 95-211.</p>	Correct error in D2.0 updates (changes were approved at July meeting), see summary section of document 95-212.	95/212 adopted.
53	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	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	<p>declined.</p> <p>It has been specifically pointed out that this change would invalidate the exportability of WEP</p>

Seq. #	Section number	your initials	Cmnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
					<p>changed to SLRC-1, but with a 32-bit accumulator.</p> <p>The commenter will provide the text updates for this change once the question of whether a 16-bit ICV is usable has been established.</p>	<p>does not have to contend with burst errors, so a CRC is unnecessary.</p> <p>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.)</p> <p>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 rate of the 32-bit ICV is unclear.</p>	
54	5.2.3	KJ	T	N	see document 95-212		95/212 adopted
55	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.	95/212 adopted
56	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-	<p>declined.</p> <p>It has been specifically pointed</p>

Seq. #	Section number	your initials	Comment type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
						32. The currently specified mechanism is too computationally expensive.	out that this change would invalidate the exportability of WEP
57	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		declined - no change needed. The text in clause 4 was checked, it is correct as is. The text in section 6 re fragmentation was also checked and corrected to reflect Wep on MPDU (this may result in MPDU expansion above frag_threshold due to IV and ICV).
58	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.		95/212 corrects this
59	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.	95/212 adopted
60	5.2.4	BA	E		Need to insert RSA document reference.		corrected
61	5.2.4	RJa	E		Need to insert RSA document reference.		corrected
62	5.2.4	TM	e		remove extra period correct paragraph justification correct license to license		corrected
63	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?	corrected
64	5.2.4	BD	T	N	Details of the RC4 algorithm are specified in 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.	corrected
65	5.2.4	ZJ	t	N	Insert appropriate RSA document reference.	It is needed.	corrected
66	5.2.5	BD	T	N	Correct text per doc 95/212.	Motions passed not reflected in D2,	95/212 adopted

Seq. #	Section number	your initials	Cmnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
						see 95/212 for D2 corrections.	
67	5.2.5	BSi	t	N	Figure 5.4 is broken. Initialisation Vector field is three octets, algorithm ID is not shown.		95/212 adoption corrects the figure
68	5.2.5	BTh	T	N	change title of section and delete colon in title... WEP MSPDU Expansion: in 2nd paragraph change... MSPDU	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.	95/196 rejection makes wep apply to MPDUs.
69	5.2.5	BTh	T	N	in 1st paragraph change... Figure 5-4 shows the expanded MSPDU <u>Frame Body</u> as constructed... in 2nd paragraph change... The expanded MSPDU <u>Frame Body</u> shall include...	Figure 5-4 doesn't show the entire MPDU frame, just the Frame Body.	corrected
70	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 information. For a detailed reasons for and usage of the Key ID, see document 95-187.	95/211 adopted
71	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.	declined. It has been specifically pointed out that this change would invalidate the exportability of WEP
72	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.	95/211 adopted
73	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.		corrected by 95/212

Seq. #	Section number	your initials	Comment type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
74	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 and Datafield. This should be replaced by an MSDU with length between 0 and 2304.	A 2-bit key ID field should be added to allow Key rollover in a dynamic way. The figure is too specific, and still relates to a 802.10 representation.	95/211 adopted
75	5.3	ws	e		"section 7.x" should be "7.x"	consistency	corrected
76	5.3	ZJ	e		Replace "7.X" with "8.4"		corrected
77	5.3	BTh	E	N	replace... section 7.X8.4	Based on the previous 71 pages the word "section" is not used in references. 8.4 is the best reference I found.	corrected
78	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	corrected
79	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. <u>The numeric encoding of these values is given in section 4.3.1.7 (Authentication Algorithm Number).</u>	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.	accepted.
80	5.3.2	BTh	e		in 3rd paragraph change... not allow WEP_Default 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	typos	corrected

Seq. #	Section number	your initials	Comnt type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
					these variables" change 4 places... Trure		
81	5.3.2	TM	e		correct deafault to default correct True to TRUE correct encrypted to encrypted correct DEfault to Default correct Dfault to Default correct false to FALSE		corrected
82	5.3.2	TM	e		correct supprts to supports correct station which which-a station correct ...WEP_ON fields is FALSE		corrected
83	5.3.2	TM	e		correct implmentation to implementation correct dependant to dependent		corrected
84	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		corrected
85	5.3.2	ws	e		"deafault"	spelling	corrected
86	5.3.2	ws	e		under receive case - "Ture"	spelling	corrected
87	5.3.2	BD	T	N	Add the following as the first paragraph of the section: <u>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.</u>	Tie description of WEP MIB variables to clause 8 where they are (or will be, see separate LB comment in sec 8) defined.	accepted
88	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.	95/198 adopted
89	5.3.2	KJ	T	N	see document 95-198		95/198 adopted

Seq. #	Section number	your initials	Comment type E, e, T, t	Part of NO vote	Corrected Text/Comment	Rationale	Disposition/Rebuttal
90	5.3.2	vj	T	N	refer to 95/198	allow exclusion of unencrypted msdus	95/198 adopted
91	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 much for security.	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 specific packet structure could be defined to accomplish this.	Text in 5.3.2. clarified to make explicit the externally read-only nature of the MIB variables which hold WEP keys (they of course can be read internal to MAC mgt).
92	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 too late in the document. The section was accidentally placed incorrectly into D2 by the editors.	referred to editors for section movement
93	Figure 5-4	BTh	T	N	change title... MSPDU add to blank box in the expanded IV a legend of... ID 1 correct legend in other expanded IV box... 43 change in note... MSPDU	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.	corrected by 95/212