Results of LMSC Ballot on Draft Standard 802.11 D5.0

Resolutions for Comments on Clause 8

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
1	8.1	**JMZ**	**t**		It is conceivable that a STA may wish to require Shared Key Authentication from certain stations, but be willing to accept Open System Authentication from others. Or that (for some compatibility reason) it might wish to allow either. I think the standard should not restrict whether both can be in operation at the same time.	Clarify this point in 8.1, 8.1.1, 8.1.2, and 11.4.4.1.11 (change aAuthenticationType to aAuthenticationTypes).	
2	8.1.1	**JMZ**	**e**		Typo	Need a period after "Authentication"	corrected
3	**8.1.1**	JD	**e**		**typo**	Open system authentication is the simplest of the available authentication algorithms. Essentially it is a null authentication algorithm. Any station that requests authentication with this algorithm becomes authenticated if aAuthenticationAlgo~~r~~rithm at the recipient station is set to allow Open System Authentication Open system authentication is the default authentication algorithm.	**Corrected**
4	**8.1.1.2, 8.1.2.2, 8.1.2.3, 8.1.2.41 1.3.1,**	MAF	t	**(na)**	**There is nothing specified, either procedurally or in the MAC MIB to define an upper bound on the response time for Management frames other than Probes. There is a risk that conformant implementations might not be interoperable in the**	**Clause 11.3.1:** A station shall associate with an Access Point via the following	

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
	11.3.2, 11.3.3, 11.3.4, and 11.1.3.2.1, also				**absence of of such a bound on the time before the responding station attempts to send Association Response frames, Reassociation Response frames, and Authentication frames (for the 2nd through last frames of any defined authentication sequence).** **The problem could occur in a case where an AP (or other responder STA in the case of Authentication sequences) is implemented in such a manner that it will never respond to one or more of these request types within the time that some STA implementation considers a reasonable maximum waiting time for such a response. For power-managed stations, waiting "forever" is a poor alternative. I strongly recommend that we apply the time limits already in the MIB for aMinProbeResponseTime and aMaxProbeResponseTime to the request/response exchanges for Association, Reassociation, and Authentication (for each step in the authentication sequence), as well as for Probe (already specified in 11.1.3.2.2). There also needs to be a constraint that the AP (or responder in the case of Probes and Authentication sequences in an IBSS) shall make its first attempt to transmit the response within aMinProbeResponse of receipt of a valid request. The requirement for conformance & interoperability is to have an upper bound on the response time between successful receipt of the request and the first attempt to obtain control of the medium to transmit the response. With this time interval known, there is a basis for interoperability that allows local decisions at the stations as to how much longer (if any) to wait due to medium access delays, and whether to retry, look elsewhere, etc.** **A similar comment on D4.0 was declined (with commenter's agreement) at the July, 1996 meeting**	procedure: a) The station shall transmit an Association Request to an Access Point with which that station is authenticated b) If an Association Response frame is received with status value of "successful", the station is now associated with the Access Point. If the Association Request fails for any reason, the station may scan for a different Access Point with which to attempt association. The station may treat a period of at least aMaxProbeResponseTime duration following the transmission of an Association Request frame without receipt of any Association Response frames as a failure of the Association Request. **Clause 11.3.2:** An Access Point shall operate as follows in order to support the association of stations. a) Whenever an Association Request frame is received from a station and the station is	

Seq. #	Clause number	your voter’s ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					because the solution proposed therein was found to be incomplete; not because there was a finding that the cited problem did not exist. While the risk of non-interoperability among “sane” STA and AP implementations is small, sooner or later this type of incompatibility will occur if a time bound is not defined in the standard. **There are two approaches to fixing this problem. One is to add new MIB attributes with minimum response time limits for each various management frame exchanges. The other is to re-use an existing response time MIB attribute, such as aMaxProbeResponseTime. The proposed text changes to the right use the later approach, since to this commenter there does not seem to be any compelling reason to need different response time bounds for different of the exchanges. Note that all of the referenced responses pertain to the establishment of communication (Association, Reassociation, Authentication), so the time bound selected does not impact the performance for MSDU delivery after communication is established.**	authenticated, the Access Point shall transmit an Association Response with a status value as defined in clause 7.3.1.9~~7.3.1.8~~. The Access Point shall make its initial attempt to transmit the Association Response frame soon enough after receipt of the Association Request frame that a successful transmission attempt will be complete within aMaxProbeResponeTime of the receipt of the request. If the status value is “successful”, the assigned Station ID to the station is included in the response. If the station is not authenticated, the Access Point shall transmit a Deauthentication frame to the station. b) When the Association Response with a status value of “successful” frame is acknowledged by the station, the station is considered to be associated with this Access Point.	

Seq. #	Clause number	your voter’s ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
						c) The AP shall inform the Distribution System of the association. **Clause 11.3.3:** A station shall reassociate with an Access Point via the following procedure: a) The station shall transmit a Reassociation Request frame to an Access Point. b) If a Reassociation Response frame is received with status value of “successful”, the station is now associated with the Access Point. If the Reassociation Request fails for any reason, the station may scan for a different Access Point with which to attempt reassociation.The station may treat a period of at least aMaxProbeResponseTime duration following the transmission of a Reassociation Request frame without receipt of any Reassociation Response frames as a failure of the Reassociation Request. **Clause 11.3.4:**	

Seq. #	Clause number	your voter’s ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
						An Access Point shall operate as follows in order to support the reassociation of stations. a) Whenever a Reassociation Request frame is received from a station and the station is authenticated, the Access Point shall transmit a Reassociation Response with a status value as defined in clause 7.3.1.97.3.-1.8. The Access Point shall make its initial attempt to transmit the Ressociation Response frame soon enough after receipt of the Ressociation Request frame that a successful transmission attempt will be complete within aMaxProbeResponeTime of the receipt of the request. -If the status value is “successful”, the assigned Station ID to the station is included in the response. If the station is not authenticated, the Access Point shall transmit a Deauthentication frame to the station.	

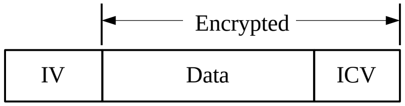
Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
						b) When the Reassociation Response with a status value of “successful” frame is acknowledged by the station, the station is considered to be associated with this Access Point. c) The AP shall inform the Distribution System of the reassociation. **Clause 11.1.3.2.1:** Stations, subject to criteria below, receiving ProbeRequest frames shall respond with a Probe Response only if: (1) the SSID is the broadcast SSID or matches the specific SSID of the station, and (2) the Capability Information field of the Probe indicates a match on the current BSS type. Probe Responses shall be sent as directed frames to the address of the station that generated the Probe. The Probe Response shall be sent using normal frame transmission rules.The responding station shall make its initial attempt to transmit the Probe Response frame within aMinProbeResponeTime of the receipt of the Probe Request frame An Access Point shall respond to all Probes meeting the criteria above. In an IBSS, the station that generated the	

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
						last Beacon shall respond to a Probe. In each BSS there shall be at least one node that is awake at any given time to respond to Probes. The station that sent the most recent Beacon shall remain in the Awake state and shall be the only station to respond to Probes until a Beacon frame is received. If the station is an Access Point, it shall always remain in the Awake state and always respond to Probes. **In each of Clauses 8.1.1.2, 8.1.2.2, 8.1.2.3, and 8.1.2.4 add the following two paragraphs after the current text:** The station sending this frameshall make its initial transmission attempt soon enough after receipt of the preceding Authenticationframe of this authentication sequencethat a successful transmission attempt will be complete within aMaxProbeResponeTime of the receipt of the preceding frame. The station waiting to receive this frame may treat a period of at least aMaxProbeResponseTime duration following its transmission of the Authentication frame to which this is a response, without receipt of any Authentication frames as an unsuccessful authentication attempt.	

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
5	**8.1.2** **7.2.3.10** **7.3.1.1**	**GMG**	**T**	**Y**	**Given that Authentication is considered useless in an environment which does not provide confidentiality, because without confidentiality, a station can always pretend to be an other station by using its address as a false identity source address.** **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.** **Frames that do not have the proper WEP key (ICV is wrong) are not forwarded to the DS.** **The fact that the stations have the proper WEP key that has been distributed (supposedly in a secure way, which is outside the scope of this standard) is an implicit form of authentication.** **Shared Key Authentication depends on both sides having the same WEP key. This is exactly equivalent to 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 having the same correct key.** **Therefore there is no justification for the additional complexity, and or the considerable additional delay during reassociation, or the complexity of the pre-authentication.**	**Delete the Shared Key Authentication method from the standard, or make it optional also for stations supporting WEP . Change 8.1 as follows:** 802.11 currently defines only one~~defines two~~ subtype~~s~~ of authentication service; "Open System" ~~and "Shared Key"~~. The subtype invoked is indicated in the body of authentication management frames. Thus authentication frames are self identifying with respect to authentication algorithm. **Therefore delete section 8.1.2 entirely, or make it explicitly optional in section 8.1.2.** **Change Table 14 by deleting all Shared Key entries.** **Change section 7.3.1.1 as follows:** Authentication Algorithm Number = 0: Open System ~~Authentication Algorithm Number = 1: Shared Key~~ All other values of Authentication Number shall	**Please see comment #31 in clause 5 for resolution of this comment.**

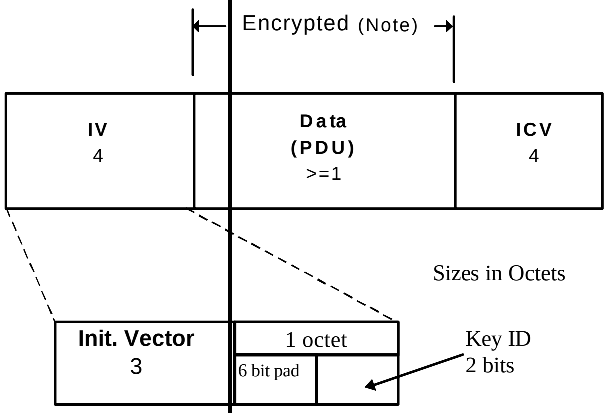
Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
						be reserved.	
6	8.1.2.2	PMK	e		PRNG used in the clauses but not definied.	Insert in sheet 4: PRGN=Pseudo Random Number Generator	**added to clause 3 definitions**
7	8.1.2.3	TLP	E		What is encrypted? Which fields? DA? CRC/FCS? As currently stated any implementation decision is supportable, but implementations will not be interoperable unless all implementors accidentally make the same choices. <not likely>	Specify the extent of encryption — the first through last fields encrypted.	
8	8.2.1	TLP	e		Disambiguate the references to 802.11.	Change to read " The 802.11 standards committee specifically recommends against running an 802.11 LAN with privacy but without authentication."	**Corrected**
9	8.2.2	TLP	e		Get the name of the U.S. gevernment agency correct and the English language clear.	Change to read "the chances of approval, by the U.S. Department of Commerce, of export from the U.S. of products containing a WEP implementation".	**Corrected**
10	8.2.3	DSM	E		**You should describe this algorithn using the term given in a text such as Schneier's Applied Cryptography**	**Add a sentence indicating this is a "Stream" cipher.**	
11	8.2.3 fig 33	SD	e		**The label «(MAX_MSG_SZ)» is useless.**	**Remove it from figure.**	
12	8.2.3	SD	t		**The IV has to be transmitted in the clear to allow self-synchronization in case some MPDUs are lost.**	**Modify the sentence: «The IV may be transmitted in the clear since it does not provide an attacker with any information about the secret key.» in : «The IV is transmitted in the clear since it does not provide an attacker with any information about the secret key and allows self-synchronization.»**	**"may" changed to "is".**
13	8.2.3 fig 34	SD	e		**Figure has to be improved.**	**Move the arrow head to the end of the lines, recenter the label « Integrity Algorithm», add the**	

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
						label « Seed » as in figure 33.	
14	**8.2.3**	**TLP**	t		The statement would be true only for symmetric-key systems. But the concept and need for symmetric keys has not yet been specified as necessary or even relevant. The easiest way to fix this problem is the change the text as shown.	Change to read “note that if the same key can be used for encryption and decryption then $D_k(E_k(P)) = P$”	**Corrected**
15	**8.2.4**	**rdh**	**T**	**y**	This section requires the use of RC4. RC4 requires a license from RSA Data Security, Inc. I believe that stream ciphers without licesne requirements are available. Also, the RC4 algorithm specification is not public.	I suggest that the IEEE 802.11 working group select a public, license free algorithm. Some alternatives inlcude A5 and ORYX, but there are other alternatives. • A5. The A5 algorithm is the stream cipher used for encryption in Group Special Mobile (GSM) telephones. IEEE must enter into an agreement with the GSM standards developers to use the algorithm, but once this agreement is reached. The A5 algorithm is fully described in Bruce Schneier’s book, *Applied Cryptography* (second edition). ORYX. AT&T has developed the ORYX algorithm, and a representative from AT&T told me that they are willing to make this algorithm avaliable.	802.11 declines to change the algorithm from Rc4 to something else. Rc4 was picked after very careful evaluation. There are attributes of Rc4 that are very important which are not strictly of a technical nature. The group decided that it was a requirement that the privacy features implemented be exportable from the U.S. To accomplish this Wep was designed to conform to some very strict guidlelines which maximize the ability to acquire a CJ export license. These design constraints mandated that we use a system which meets the SPA rules for CJ export. RC4 was the only algorithm which meets that particular criteria. Additionally, we went to great effort to make RC4 available to anyone who wants to use it for 802.11 on fair and equitable terms - in fact, RSA has offered Rc4 for 802.11 implementation on identical terms to anyone. Even if the terms of the other algorithms suggested happened to be better, the other algorithms would not hold the

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
							special status that RC4 enjoys wrt to export restrictions. Finally, we have a successful test case for the WEP export license in that at least one WEP implementation has been granted a CJ export license.
16	**8.2.4**	**TLP**	E		A means of locating the company called "RSA Data Security, Inc", which presumably is located somewhere on the planet, needs to be specified.	Add "If necessary, contact the IEEE Standards Office for details on how to communicate with RSA." at the end of the last paragraph.	**Corrected**
17	**8.2.5**	**MT**	**e**		**remove page break just before figure 35**		**Corrected**
18	**8.2.5**	**rdh**	**t**	**y**	Encryption must cover the Integrity Check Value (ICV) as well as the data	. The top of Figure 35 should be redrawn as follows:  	Declined. Even though the reviewer is correct in that having the ICV encrypted would strengthen the privacy feature, we can not do this. Part of the export restrictions in the WEP design are that the ICV NOT be encrypted. NSA requires this in order to get a CJ export license.
19	**8.2.5**	**RM**	**T**	**Y**	**Section 8.25 and Figure 35 are contradictory:** **From Section 8.2.5** The key ID occupies the two least significant bits of the last octet of the IV field, while the pad occupies the six most significant bits of this octet. **From Section 7.1.1 Conventions** .... The least significant bit of each octet is defined as bit 0 for that octet and is the **leftmost** bit of the octet (except the FCS field). Figure 35 shows the key ID as the rightmost 2 bits.	**Revise Section 8.2.5** The key ID occupies the two most ~~least~~ significant bits of the last octet of the IV field, while the pad occupies the six least ~~most~~ significant bits of this octet [alternatively, correction of the figure is acceptable]	**accepted - text corrected.**
20	8.2.5	SB	E	N	The type of CRC for the ICV and the transmission order are undefined	Amend 8.2.5 as follows, or to capture this intent:	Accepted.

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
						The WEP ICV ~~= 32 bits~~ shall be a 32-bit field containing the 32-bit Cyclic Redundancy Check (CRC) defined in clause 7.1.3.6 calculated over the Data (PDU) field as depicted in figure 35. The expanded MPDU shall include a 32 bit IV field immediately preceding the MPDU. This field shall contain three sub-fields: A three octet field that contains the initialization vector, a 2 bit key ID field and a 6 bit pad field. The ordering conventions defined in clause 7.1.1 apply to the IV field~~s~~ and its sub-fields and to the ICV field~~.~~	
21	8.2.5	SB	E	N	There would seem to be an error in figure 35 since the figure does not match the statement: *The key ID occupies the two least significant bits of the last octet of the IV field, while the pad occupies the six most significant bits of this octet.*	Edit figure 35 to show the KeyID and pad as follows Key ID 6-bit pad	test and figure are now consistent.
22	**8.2.5**	**TLP**	e		Equal signs should not occur in text.	Change to read "The WEP ICV is 32 bits in length."	**corrected**
23	**8.2.5**	**TLP**	e		Within figures, field names should be within their drawn boundaries where possible. Single-digit numbers should be written out when they occur in text, unless there are multi-digit numbers in the same text.	Redraw figure 35 and change the immediately-following text as follows. Put the "Key ID 2 bits" text inside the lower octet subfield drawing. Use spelled-out numerals when all numerals in the sentence are single digit.	
24	**8.2.5** (also see related issue with 7.1.1)	**MAF**	**E**	**(na)**	**Text was added to the 2nd paragraph of Clause 8.2.5 at the July 1996 meeting to clarify IV field bit ordering by referring explicitly to the ordering conventions in Clause 7.1.1. However, the added text did not address the ICV field ordering. This is a potentially major oversight, because the sole specification of the ICV field contents is the sentence**	The WEP ICV = 32 bits. The ICV field shall contain a CRC-32 value, calculated and transferred in an identical manner as is described for the MAC CRC field in Clause 7.1.3.6, except that the ICV field value shall be calculated using only the contents of	**Corrected with alternate wording.**

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					"The WEP Integrity Check algorithm is CRC-32." (in clause 8.2.3, just above Figure 34). **While the polynomial for "CRC-32" is well-known, there is a risk that different implementers will transfer the resulting check value in opposite order; as some think that the global bit ordering convention (LSb first) applies to the ICV field, while others think that the CRC bit ordering exception (coefficient of the highest order term first) applies to the ICV field. The stated rationale for using CRC-32 as the ICV algorithm, at the time of its adoption (at the August, 1995 meeting in Schamberg, Illinois) was that CRC-32 was a check code of adequate (if not excessive) quality that already had to be implemented at all stations for the MAC frame check CRC. If the specifics of ICV calculation (other than the range of octets of the MPDU which are included in the calculation) or transfer bit order are not identical to that used for the CRC field, this advantage of reusing CRC-32 is lost, for no apparent benefit. The corrected text makes this consistency explicit, referring to the relevant portions of Clause 7.**	the Data field, as shown in Figure 35. The expanded MPDU shall include a 32 bit IV field immediately preceding the MPDU. This field shall contain three sub-fields: A three octet field that contains the initialization vector, a 2 bit key ID field and a 6 bit pad field. The ordering conventions defined in clause 7.1.1 apply to the IV fields and its sub-fields. The key ID field contents select one of four possible secret key values for use decrypting this MPDU. Interpretation of these bits is discussed further in section 8.3.2. The contents of the pad field shall be zero. The key ID occupies the two least significant bits of the last octet of the IV field, while the pad occupies the six most significant bits of this octet.	
25	**8.2.5 (figure 35)**	**MAF**	**E**	**(na)**	**Text was added to the 2nd paragraph of Clause 8.2.5 at the July 1996 meeting to clarify IV field bit ordering by referring explicitly to the ordering conventions in Clause 7.1.1. However, Figure 35 was not updated to show the key ID bits at the left side of their octet, which is needed for consistency with the order stated in the text: "The key ID occupies the two least significant bits of the last octet of the IV field, while the pad occupies the six most significant bits of this octet."** **(I had to convert the drawing from its original format to "Word 6.0 Picture Object" before Word 6 for the Macintosh would let me edit the drawing. It may be**	Replacement for Figure 35 drawing:	

Seq. #	Clause number	your voter’s ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					perferable to make equivalnet changes in the original drawing rather than inserting the picture object to the right in place of the existing Figure 35.)	 Encrypted (Note) IV 4 Data (PDU) >=1 ICV 4 Sizes in Octets Init. Vector 3 1 octet 6 bit pad Key ID 2 bits Note: The encipherment process has expanded the original MPDU by 8 Octets, 4 for the Init field and 4 for the Integrity Check Value (ICV). The ICV is calculated on the Data field onl	
26	**8.3.2**	**TLP**	E		The second sentence needs to constrain STA construction, not ultimate users. The indicated change accomplishes this shift in focus.	Change sentence to end “shall not be readable via MAC management SAPs.”	**corrected**
27	**8.3.2**	**TLP**	E		The last two sentences of the third paragraph are redundant (the material presented is covered better in the following paragraph), premature (it presumes knowledge of concepts not yet explicated) and unneeded.	Delete the last two sentences of the third paragraph.	**Corrected**

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
28	**8.3.2**	**TLP**	T	Yes	If the array aWEPKeyMapping is "indexed by MAC address", then the array is 2^{47} entries long. Clearly, and from the following text, this is not the case. The array is really an array of three-element records, where one element is a MAC address, which is searched using a content-addressable search.	Please reformulate this description so that it is conceptually correct and matches the MIB attributes which specify the maximum and currently-used number of elements in the array.	**Accepted - Text corrected.**
29	**8.3.2**	**TLP**	e		There are a number of English language restructurings needed which are indicated in the submitted edited file.	Correct as indicated in the submitted revision-marked files.	**Corrected**
30	**8.3.2**	**TLP**	E		The statement "The values in this attribute shall take precedence over the aWEPDefault and aDefaultWEPKey variables." is sloppy description. The value False in WEPOn can take precedence over the aWEPDefault and aDefaultWEPKey variables only if the text states that the default value of WEPOn does not apply when the RA or TA address does not have an entry in the aWEPKeyMapping array.	Please clean up this description, either to indicate that the WEPOn default does not apply when no corresponding array entry exists, or to indicate that it is only WEPOn True that takes precedence, and not WEPOn False.	**Corrected**
31	**8.x.x.x** **5.4.3**	**MT**	**E/t**		**ref: MT_6** **In the case of an access point with two associated stations. The access point is aware of (at least) two authentication methods. STA A associates using method A and STA B associates using method B. STA A and STA B cannot associate directly and can therefore, not transfer data. The AP is not aware (unless internal rules are established) that it may not be allowable for it transfer data between these two stations.** **According to the PICS, open authentication must be supported, and WEP is optional. Therefore, clarity ought to be provided such in the case that WEP is enabled. Should a station authenticating using the open method be allowed to join a BSS which has WEP enabled? According to the current wording, it seems that the answer is yes or the system is in danger of non-compliance. However, this opens a can of security worms. (MT_8,9,10,11)**	**Distribution system services can only be invoked in the case that similar authentication methods (or by established management rules in the AP).** **In the case that the final destination is not within the current BSS, the frame should be forwarded with appended information identifying the authentication method used by the initiating station. The responsibility of checking is placed on the AP providing service to the final destination STA.** **-or-** **Recommend a*mandatory* authentication method within 802.11 so that this breach of security and accompanying overhead as described above can be averted.**	

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
						-or- Remove all references to authentication from the standard and allow a user to chose a vendor which supplies appropriate security vs. overhead/protection tradeoff	
32	8.x.x.x 5.4.3.3 6.1.2	MT	t		ref: MT_8 Clarification should be added to state what happens in the case of an access point which supports both 'clear mode' and WEP mode. Specifically: Can both modes be simultaneously supported? How are multicasts handled - sent twice once in the clear and again encrypted with WEP?	Both methods must be able to be simultaneously supported since WEP is optional and compliance criteria is in the clear. Therefore, in order to reduce overhead, the standard ought to state that all multicasts will be sent in the clear and that WEP stations must also receive and not reject these broadcasts based on WEP bit.	
33	8.x.x.x 5.4.3.3 6.1.2	MT	T		ref: MT_9 A potential security problem exists in the case where a station can support both/several authentication methods. Consider the 'obvious' case of a wireless access point operating as a repeater. In this situation, the repeater associates to an access point connected to the distribution system using the WEP authentication method. A mobile station associates to the repeater using the 'clear' method. If the repeater forwards the packets from the mobile station using the WEP encryption, then a possible network infringement exists. A similar scenario is two stations associated to the same ESS. One station uses 'clear' and the other uses WEP. If both associated to the same AP, the AP must perform the clear-WEP or WEP-clear	It seems there should be a strong line formed which allows only a single authentication method allowed by the standard. -or- At the very least (referring back to the previous comment) the user ought to be informed whether the standard allows for authentication method translation and the standard should provide the hooks for enabling or disabling this translation via a MIB variable. -or- remove authentication from the standard.	

Seq. #	Clause number	your voter’s ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					translation providing a potential breach. The same situation exists when they are associated to different APs.		
34	8.x.x.x 7.1.3.1.3 7.1.3.1.4	MT	T		ref: MT_17 The TO_DS and FROM_DS bits should be allowed to be used in control packets. In particular, these bits could identify a wireless access point which is operating in a repeater function. The repeater upon association to another access point could identify itself as part of the (wireless) distribution system. In this fashion, a Network administrator can establish a security level for the distribution system (such as requiring all data to be WEP encrypted) but stations can be allowed to associate to individual APs using the ‘clear mode’. In this case, the AP could filter those ‘clear mode’ packet requests from the distribution system. Therefore, two stations can communicate in the clear to each other (using the services of the access point and/or distribution system) without having access to any other data from the distribution system.	AUTHENTICATION.request, ASSOCIATION.request frames from a repeater (or Wireless AP) should set the FROM_DS bit to identify themselves as such. Appropriate authentication methods (those as established for the distribution system by a system administrator) can be used. TO FM meaning 0 0 normal STA operation 0 1 repeater associations Appropriate hooks should be provided to allow various levels of security or the standard could simply adopt a single authentication method.	
35	8.x.x.x 7.1.3.1.3 7.1.3.1.4	MT	t		ref: MT_18 The use of these bits during the association process (ref MT_17) would enable automatic distribution systems functions. By not defining these bits this way, the standard cannot support interoperability among vendors supplying repeaters. Each vendor will have to resort to proprietary packet exchanges to establish the station as part of the distribution system. I point out the situation of a repeater which has associated one or more power save stations associated to it. The packets must be sent to the repeater for	define the bits to be allowed in AUTHENTICATION and ASSOCIATION request frames. Further refinements could be the addition of a required authentication method (as establish via MIB variables of a system administrator, for instance) and automatic conveyance of station capability information.	

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					queuing and delivery. Without the standard specifying a way to identify a wireless distribution system component, all this becomes proprietary or left to another consortium such as the IAPP		