Results of LMSC Ballot on Draft Standard 802.11 D5.0 - Comments on clauses 0-5 and general comments

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
	2	VZ	E		Do you want the most current version of the references to be referenced? If so use the following introductory sentences in clause 2	This standard shall be used in conjunction with the following standards. When the following standards are superseded by an approved revision, the revision shall apply.	
	3	VZ	E		Each definition should be numbered	Number the defintins 3.1, 3.2, 3.3, etc.	
	3	MT	e		**Mobile Station definition requires a hard return to separate from the Minimally Conformant Network definition**	**add a hard return**	
	3	JD	e		**new par missed**	**Minimally Conformant Network.** An IEEE 802.11 network in which two stations in a single BSA are conformant with IEEE Std-802.11. **Mobile Station.** A mobile station uses network communications while in motion.	
	3.	JMZ	e		Typos	Change "ESS Basic Rate Set" to "BSS Basic Rate Set"; insert paragraph-break before Mobile Station definition; change ".11LAN" to ".11 LAN" in Portal definition	
	4	MT	e		**WEP = <…>**	**remove period from end**	
	4, 15.1.3	MT	e		**add the abbreviations from clause 15 (DSSS PHY) this maintains consistency among clauses**	**add abbreviations from clause 15 and delete from clause 15**	

Seq. #	Clause number	your voter’s ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal

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	VZ	E		Figure quality (in clause 5) is not acceptable for publication purposes.	Some figures will need to be redrawn (e.g., figures 1, 2, 3, 5, etc.) Each figure should the be saved in EPS in a file separate from the text	
	5.1.1.2 (c) 5.2.4.1 5.4 9.2.1 12.all 14.all 15.some 16.all	TLP	e	Yes	The wireless medium is definitely singular (unless there is an alternate universe with multiple “ethers”), or unless P802.11 is extending its charter to acoustic modes of transmission.	change “edia” to “edium” everywhere except when referring to wired media.	
	5.1.1.4, 5.2, 5.4.2.1, etc. 1.2,	RS	T	Y	The fact that high-layer applications may desire the ability to move within or among wireless LANs does NOT imply the requirement, as stated in 5.1.1.4, that this mobility must be provided within the MAC sublayer. In fact, 802.11 does not currently provide this mobility service (see discussion of DS and ESS below). Mobility is best relegated to higher-layer protocols (such as Network). 802.11 should provide the appropriate service interfaces (e.g., allowing a MAC client or management entity to determine the current associations of an AP) that allow higher-layer protocols to implement mobility, but not to attempt to implement it within the MAC. There is no need to “reinvent” the entire ISO protocol stack within the MAC, just because it’s wireless.	Eliminate mobility as a requirement of, and function provided by 802.11. Include a paragraph in the Scope section identifying mobility as a higher-layer function that can be provided among 802.11 LANs.	
	5.2, 1.2, 5.1.1.4,	RS	T	Y	The fact that high-layer applications may desire the ability to move within or among wireless LANs does NOT imply the requirement, as stated in	Eliminate mobility as a requirement of, and function provided by 802.11. Include a	

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
	5.4.2.1, etc.				5.1.1.4, that this mobility must be provided within the MAC sublayer. In fact, 802.11 does not currently provide this mobility service (see discussion of DS and ESS below). Mobility is best relegated to higher-layer protocols (such as Network). 802.11 should provide the appropriate service interfaces (e.g., allowing a MAC client or management entity to determine the current associations of an AP) that allow higher-layer protocols to implement mobility, but not to attempt to implement it within the MAC. There is no need to “reinvent” the entire ISO protocol stack within the MAC, just because it's wireless.	paragraph in the Scope section identifying mobility as a higher-layer function that can be provided among 802.11 LANs.	
	5.2.3 fig 4	**SD**	**t**		**The Figure should be accompaigned with some technical data as: the location of the source, its power, the frequency and so on ...**	**Add at least the location, the power and the frequency.**	
	5.2.3 fig5	**SD**	**e**		**Labels of STAs are out of their frames.**	**Recenter them.**	
	5.2.4	**DSM**	**t**		**I would assume that a portal could provide entrance to an 802.11 LAN from a WAN such as the Internet**	**Add a clause “or a Wide Area Network”**	

Seq. #	Clause number	your voter’s ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal

Seq. #	Clause number	your voter’s ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
	5.2.4	**apu**		**y**	Although the PAR does not specifically state this, I believe that 803.11 must address the issues of interoperability with existing (wired) 802.3 LANs. In particular, this draft standard (5.0) is ambiguous regarding the issue of bridging. Section 5.2.4 incompletely describes a Portal, and, in fact, poses a question without giving any guidance to the implementor as to how to resolve the issue. I refer to the sentence: "Bridgin to the 802.11 architecture raises the question of which logical medium togridge to; the DSM or the WM?"	At a minimum, the standard must define a set of requirements for a bridge or a portal between an 802.11 wireless LAN and an 802 wired LAN. It would be preferable to go further that this by unambiguously describing such a bridge, including resolving the issues resulting from multiple bridges attached to a large ESS at different points, such as spanning tree convergence and stability.	
	5.2.4.1 **5.1.1.2 (c)** **5.4** **9.2.1** **12.all** **14.all** **15.some** **16.all**	**TLP**	e	Yes	The wireless medium is definitely singular (unless there is an alternate universe with multiple “ethers”), or unless P802.11 is extending its charter to acoustic modes of transmission.	change “edia” to “edium” everywhere except when referring to wired media.	
	5.3	**RS**	**E**	**Y**	The statement, “The generality allows 802.11 to satisfy the diverse interests ...” is a clear statement that “We couldn’t agree on how to standardize this, so we left it up in the air.” While this may be true, it: (1) indicates the importance of the previous comment on a lack of DS and ESS requirements,	Eliminate the statement.	

Seq. #	Clause number	your voter’s ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal

Seq. #	Clause number	your voter’s ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					and (2) looks like dirty laundry hanging out to dry.		
	5.3, 5.4.2.2, etc.	**RS**	**T**	**Y**	There is no specification provided for the DS; neither a specific implementation nor a set of service interfaces and invariants that ensure proper MAC operation across the ESS. Since 802.11 depends on the DS to provide mobility and ESS coverage, it is clear that this standard currently does not provide sufficient information to build an interoperable, conformant ESS. Without conformance requirements, DS’s and ESS’s become proprietary entities. In addition, the inclusion of an “unspecified” DS makes the delay as seen at the LLC service interface unbounded and uncontrolled. LAN MAC clients expect a low delay; the inclusion of an arbitrary internetwork (including possible WAN links) invalidates any assumptions about delay that are typically made by LAN clients. IEEE 802.1G allows WAN links for Remote Bridges, but it puts an upper bound on their number and delay, and makes this information available to a management entity.	Eliminate the concept of DS and ESS from the standard at this time, and note that this is “under study” or “work-in-progress”. When specifications are available that allow interoperable, conformant implementations to be built, revise the standard to include these new specifications. Eliminate all discussion of mobility as an 802.11-provided service.	
	5.3.3	**GC**			see 7.1.3.3.1 G		
	5.4	**DLP**	**e**		**Clause xx.xx needs to be specified.**	**Replace xx.xx with appropriate clause number.**	
	5.4	**JMZ**	**e**		Typos	Fill in reference marked “xx.xx” and change “DATA SERVICE” to “Data Service”	
	5.4	**KC**	**e**		**"clause xx.xx"**	**specify whatxx.xx 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

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
	5.4	**MT**	**e**		**find and fill in clausexx.xx reference**		
	5.4	**JD**	**e**		**reference not done**	Each of the services is supported by one or more MAC frame types. Some of the services are supported by MAC Management messages and some by MAC Data messages. All of the messages gain access to the WM via the 802.11 MAC layer media access methods specified in clause?~~xx~~.?~~xx~~ of the standard.	
	5.4.2.1, 1.2, 5.1.1.4, 5.2, etc.	**RS**	**T**	**Y**	The fact that high-layer applications may desire the ability to move within or among wireless LANs does NOT imply the requirement, as stated in 5.1.1.4, that this mobility must be provided within the MAC sublayer. In fact, 802.11 does not currently provide this mobility service (see discussion of DS and ESS below). Mobility is best relegated to higher-layer protocols (such as Network). 802.11 should provide the appropriate service interfaces (e.g., allowing a MAC client or management entity to determine the current associations of an AP) that allow higher-layer protocols to implement mobility, but not to attempt to implement it within the MAC. There is no need to "reinvent" the entire ISO protocol stack within the MAC, just because it's wireless.	Eliminate mobility as a requirement of, and function provided by 802.11. Include a paragraph in the Scope section identifying mobility as a higher-layer function that can be provided among 802.11 LANs.	
	5.4.2.2	**JMZ**	**e**		Typo	"System" should not be in Courier font	
	5.4.2.2 5.4.3.1	**MT**	**t**		**ref: MT_1**	**Specify a minimum number of authentications which must be**	

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					Clause 7.3.1.9 references status codes for reporting 'too many stations'. The standard should specify a minimum number of stations to be supported by an access point. The standard should also specify a minimum number of stations so be supported by an IBSS node. Refer to MT_2 for related partial solution/problem. By adding this number (along with the number of currently associated stations) within the ASSOCIATION, PROBE and BEACON frames, a mobile station can use this information in determining which BSS is best to join – this provides the starting means for automatic load balancing (the main ingredient, current load, is missing but a more intelligent decision can be made).	supported by an access point and a member of an IBSS (not necessarily the same value). Specify a method which allows a new station an opportunity to join the network. One method would be to deauthenticate the station which has not transferred data for the longest interval. Another would be to deauthenticate the station which has transferred the least amount of data during the last sample interval. The 'best' solution is to avoid the problem by adding to the standard the requirement that access points and IBSS stations must support a sufficiently large number of authenticated stations (eg., 1000 and 100 respectively)	
	5.4.2.2	MT	T		ref: MT_2 An AUTHENTICATIONstaleout time should be specified such that if no data is transferred between stations for the correspondingstaleout period, the authentication (and if appropriate, association) is dropped. This feature is needed in order to guarantee network security as well as to prevent the "too many stations" situation detailed in MT_1. Authentication is common among infrastructure and IBSS networks and should therefore be used (as	The ASSOCIATIONstaleout time should be asetable MIB variable to allow for changes in system performance due to fluctuations in the number of associated stations for example. In order to simplify implementation, this parameter can be added to the ASSOCIATION, BEACON and PROBE frames. The longest time specified should be used by all stations in the BSS cell (or IBSS). If	

Seq. #	Clause number	your voter’s ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal

Seq. #	Clause number	your voter’s ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					opposed to association staleout).	**a particular station finds that it is spending too much time maintaining an association because the network is busy enough that it is not getting air time, it can reassociate with a longer staleout time. This information can be interpreted and conveyed to all other stations in the BSS or IBSS in the ASSOCIATION.response or from following BEACON and PROBE frames.**	
	5.4.2.2	**MT**	**E/t**		**ref: MT_3** **text should be adjusted / added to show that in the wireless distribution system, a wireless AP (acting as a repeater and connection to a distribution system) must itself be associated *before* both accepting authentications/associations requests and before allowing or forwarding any traffic to and from the distribution system.**	**Adjust the text as suggested to reflect the ASSOCIATION procedure of wireless AP repeater operation.**	
	5.4.2.2	**MT**	**t**		**ref: MT_4** **In the case of a single cell which has no backbone distribution system and where a wireless AP is used to transfer information among mobile stations (is the sole piece of the distribution system), the wireless AP will begin by sending BEACONS until other stations join the BSS. Only traffic with the TO_DS bit set and with a corresponding final destination address of another currently associated station will be forwarded (with the FROM_DS bit set). ie., no directed data will be transferred until at least two stations are associated to the wireless AP.**		

Seq. #	Clause number	your voter’s ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal

Seq. #	Clause number	your voter’s ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
	5.4.2.2	MT	t/E		ref: MT_5 access point operation should be clarified to state that multicast frames are allowed to be forwarded in all cases (to and from the distribution system) in the case of an access point connected to the backbone, a wireless access point operating as the sole piece of the distribution system, and after a wireless repeater has itself established an association. Multicast retransmission should be allowed as long as at least one station is associated with the access point.		
	5.4.2.2	MT	t/e		ref: MT_7 This section states that a STA may be associated with only one AP at a time. The implication here is that one AP at a time per ESS. There are no restrictions on being a member of two ESS’s at the same time. Further, there is no restriction placed on being a member of an IBSS and an ESS at the same time. These situations can have an impact on performance, (see comment below) when considering how multicasts are handled.	Add text which explicitly disallows membership to multiple concurrent ESS’s and IBSS’s (a STA can only be a member of an ESS or IBSS at any one time). Recognizing that it is not practical for a single station to be members of multiple xSS’s because packet filtering cannot be properly accomplished and NAV will be difficult to maintain.	
	5.4.2.2	MT	t		The ESSID is not part of many management frames (RTS/CTS) - which will/could cause great difficulty in the case of collocated ESS’s as well as BSS’s. Text should be added to clarify operation in these collocated situations. Such as the NAV or TSF will only be updated when a value is received which is greater than the local value but within a specified tolerance. ie., don’t update the TSF if it greater than		

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					10 µsec from the current local value.		
	5.4.2.2, 5.3, etc.	**RS**	**T**	**Y**	There is no specification provided for the DS; neither a specific implementation nor a set of service interfaces and invariants that ensure proper MAC operation across the ESS. Since 802.11 depends on the DS to provide mobility and ESS coverage, it is clear that this standard currently does not provide sufficient information to build an interoperable, conformant ESS. Without conformance requirements, DS's and ESS's become proprietary entities. In addition, the inclusion of an "unspecified" DS makes the delay as seen at the LLC service interface unbounded and uncontrolled. LAN MAC clients expect a low delay; the inclusion of an arbitrary internetwork (including possible WAN links) invalidates any assumptions about delay that are typically made by LAN clients. IEEE 802.1G allows WAN links for Remote Bridges, but it puts an upper bound on their number and delay, and makes this information available to a management entity.	Eliminate the concept of DS and ESS from the standard at this time, and note that this is "under study" or "work-in-progress". When specifications are available that allow interoperable, conformant implementations to be built, revise the standard to include these new specifications. Eliminate all discussion of mobility as an 802.11-provided service.	
	5.4.3 8.x.x.x	**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**	**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**	

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 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)**	**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.** **-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**	
	5.4.3.1	**JMZ**	**t**		The standard does not explicitly define procedures for implementing Access-Control Lists. Since an IBSS does not have an Association function, the only way for a unit to refuse to communicate with another unit that is not on its ACL is through the Authentication mechanism. The most sensible way would seem to be to allow Open System Authentication to fail for unspecified reasons. This would allow arbitrary STA-address based discrimination.	Reword 5.4.3.1 and 8.1.1 to make it clear that Open SystemAuthentiction does not ***have*** to succeed just because Shared Key is not supported. Adding a clarification to this effect would be good, too.	
	5.4.3.1 **5.4.2.2**	**MT**	**t**		**ref: MT_1** **Clause 7.3.1.9 references status codes for reporting ‘too many stations’.** **The standard should specify a minimum number of**	**Specify a minimum number of authentications which must be supported by an access point and a member of an IBSS (not necessarily the same value).**	

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					stations to be supported by an access point. **The standard should also specify a minimum number of stations so be supported by an IBSS node.** **Refer to MT_2 for related partial solution/problem.** **By adding this number (along with the number of currently associated stations) within the ASSOCIATION, PROBE and BEACON frames, a mobile station can use this information in determining which BSS is best to join – this provides the starting means for automatic load balancing (the main ingredient, current load, is missing but a more intelligent decision can be made).**	**Specify a method which allows a new station an opportunity to join the network. One method would be to deauthenticate the station which has not transferred data for the longest interval. Another would be to deauthenticate the station which has transferred the least amount of data during the last sample interval.** **The 'best' solution is to avoid the problem by adding to the standard the requirement that access points and IBSS stations must support a sufficiently large number of authenticated stations (eg., 1000 and 100 respectively)**	
	5.4.3.1 **5.5**	**GMG**	**T**	**Y**	**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.** **Authentication should only be needed to use the DS Services, because this is the point where a wired network is entered that otherwise assumes the closed physical nature of a wire, which is no longer true when extended with a wireless network.** **In an IBSS explicit authentication should not be needed. Instead implicit authentication can be assumed when the stations do use the confidentiality provisions, by the fact that all stations in the IBSS use the same WEP key.**	**Following text need to change in section 5.4.3.1 to explain the implicit authentication as follows:** An equivalent ability to control LAN access is provided via the Authentication service. This service is used by all stations to establish their identity to stations with which they wish to communicate. This is true for all stations in an ~~both~~ ESS ~~and IBSS~~ network~~s~~. If a mutually acceptable level of authentication has not been established between two stations, an Association shall not be established.	

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					Only when all stations use the same WEP key, they are able to communicate at all. The fact that such a secret key (which has a separate distribution mechanism outside this standard) is available to the participants is makes authentication implicit, and a useless extra complexity. **Please note that this complexity is much larger then in the ESS case, where a station in general only needs to maintain knowledge of the authentication state with the AP.** **In an IBSS, stations need to maintain the authentication state for each of the participating stations it may send data to in the IBSS.** **The Authentication requirement implies for an ad-hoc network that it has to maintain a Service State variable for each station it is communicating with. Again this is an unnecessary extra complexity, since authentication is only relevant in combination with privacy. If privacy is used, then the plain fact that the other station has the same key is sufficient to authenticate that station for ad-hoc communication.**	Authentication is a Station Service. **For direct communication between stations in an IBSS (so without invocation of DS Services), implicit authentication is assumed when the station is using the same key for the WEP.** **Section 5.5 changes.** **Data frames with the FC control bits "To DS and From DS" both false should be Class 1 frames (instead of Class 2 as currently specified).** **In addition an ATIM should be Class 1. Both are currently defined as Type-2 frames, and must be moved to the Type-1 frame definitions.**	
5.4.3.3	**JMZ**	**t**			It isn't clear to me why Privacy is a service, rather than just a parameter to the MSDU delivery service. The relationship between the two services (since one modifies the activity of the other) should be clearer.	Clarify how they interact.	
5.4.3.3 **6.1.2** **8.x.x.x**	**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**	**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**	

Seq. #	Clause number	your voter’s ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					clear and again encrypted with WEP?	also receive and not reject these broadcasts based on WEP bit.	
	5.4.3.3 6.1.2 8.x.x.x	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 translation providing a potential breach. The same situation exists when they are associated to different APs.	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.	
	5.45.1.1.2 (c) 5.2.4.1 9.2.1 12.all 14.all 15.some 16.all	TLP	e	Yes	The wireless medium is definitely singular (unless there is an alternate universe with multiple “ethers”), or unless P802.11 is extending its charter to acoustic modes of transmission.	change “edia” to “edium” everywhere except when referring to wired media.	

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
	5.5	**DBA**	**T**	**Y**	The following sentence is incorrect: “An AP shall always be in State 3. ” With this sentence the MAC as specified can not work. Consider that the effect of this sentence is to place an AP permanently in state 3. The impact is tantamount to not having a state distinction forAPs. As a result the system can not operate and will end up in deadlock. Consider: Since an AP would always be in state 3 from it’s point of view, it will send any frame it wants to any other station. Now consider the “other” station - if it is not an AP it may be in state 1 or 2, if it receives a class x frame where X > it’s believed state, it is required by the draft to respond with either a de-authentication or disassociation frame - both of which are intended to resolve a state mismatch between communicating stations. However since the AP is locked into state 3, the mismatch can not be resolved as the AP CAN NOT change out of state 3. Clearly the protocol is broken by the added sentence. .	Delete the following sentence from clause 5.5: “An AP shall always be in State 3.” Change: “It provides the logical connection to the DS and as a Point Coordinator (PC), it may provide a Contention Free Period (CFP).” To: “An AP provides the logical connection to the DS and as a Point Coordinator (PC), it may provide a Contention Free Period (CFP).” .	
	5.5	**JMZ**	**t**		The new sentence “An AP shall always be in State 3” that Dave objected to ought to make it clear that this is with respect to the broadcast address (which is, conceptually, a STA that is always associated). Otherwise an AP could only have CFPs and/or transmit beacons if someone is associated.	Change “An AP shall always be in State 3” to “With respect to the broadcast destination, an AP shall always be in State 3. In particular, an AP may transmit broadcast frames at any time.”	

Seq. #	Clause number	your voter’s ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal

Seq. #	Clause number	your voter’s ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
	5.5	JMZ	t		The three requirements to send aDeauthentication or Disassociation frame to STA B should not apply to an AP. Otherwise, an unassociated STA would have to complain whenever it received a broadcast, which would clearly be harmful.	Add “, except if STA B in an AP” to the end of the three appropriate sentences that now end with “STA B”.	
	5.5	**MT**	**t**		**ref: MT_10** **Clarify operation of AP which is ‘always in state 3’. If no stations are associated, aremulticast packets to be forwarded via the RF anyway? If the AP supports WEP, how shouldmulticasts be transmitted?** **By disallowingmulticast retransmission without any association will conserve bandwidth only in the case of overlapping coverage areas.** **However,** **By allowingmulticast retransmission, the scanning process of a mobile station could be reduced by having the added traffic available.**	**Since the station is always in state 3, the text should state thatmulticast packets are to be retransmitted even in the case that no stations are associated.** **Reference MT_1 and MT_2, without staleout, an AP may be in this situation frequently.**	
	5.5	**MT**	**t**		**ref: MT_11** **text should be added to clarify station operation in situation where a STA A is associated with STA B and multicasts are received from STA C (also associated with STA B but not STA A) and all are members of the same ESS**	**Text should be added which clarifies system operation. One method is to drop the frames and another is to assume allmulticasts are processed.** **Another mode which the standard could specify is that all traffic within an infracture network must go through an access point. Therefore, a station would only accept traffic from its current access point (exception is during the scanning process)**	
	5.5	**MT**	**T**		**ATIMs must be allowed in state 1 (at least for 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

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					IBSS mode) rationale: 1) cannot authenticate to a PSP node 2) only ATIMs and beacons are allowed during the ATIM window (no authentication packets are allowed) which means that the PSP node will likely be asleep and not available to receive the authentication request. problem: if you are in state 1 (unauthenticated) one cannot send an ATIM to keep the other STA awake allowing ATIMs from non-authenticated stations will allow the station to authenticate and/or send other management frames.		
	5.5	MT	t		ref: MT_11 In an IBSS, clarify the authentication method and define how frames are handled in the event that multiple authentication methods are simultaneously supported. Are all multicast frames encrypted if WEP is enabled? etc.		
	5.5	MT	t		ref: MT_12 are multicast authentication packets allowed? Allowing such, could improve IBSS setup performance.		
	5.5	MT	t		ref: MT_13 the standard identifies that a frame received from a non-authenticated station requires that a		

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					deauthentication frame be returned. Clarify if this refers to only a directed frame, or if the receipt of a multicast from a non-authenticated station will require that a deauthentication packet be sent. Example, ARPs will continuously fail for a particular node that is not authenticated. If a protocol (transmission sequence) consists only of multicast frames, two stations will not be aware of each other in order to establish communication - therefore, multicasts from non-authenticated stations must be responded to with a deauthentication frame.		
	5.5	MT	E		general information should be added to the standard which clarifies how a station becomes authenticated with other members of an IBSS. Can multicast authentication packets be sent? (MT_12) Can a multicast data frame be sent and the returned deauthentication frames be processed by authenticating to each node. (MT_13) In general, How does a station become aware of other members of the IBSS?		
	5.7	SD	t		Nothing is said or even no référence is given to how the fields BSSID and ESSID are to be defined.	Give the référence to the related section.	
	5.7.4	MT	t		Clarify this section to state that an AP wishing to disassociate a station in power save mode will use the power save data delivery method by setting the SID bit of the station and delivering the DISASSOCIATION.request via this method. In the case of an AP wishing to disassociate from all stations (some of which are in power save mode) will		

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					wait until the DTIM time to deliver the dissociation request to the broadcast address.*{this is normal operation, but should be clarified here}*		
	5.7.7	**JMZ**	**t**		The broadcast address should be allowed for Deauthentication frames just as it is for Disassociation frames.	Harmonize with Information Items: section from 5.7.4.	
	5.8	**JD**	**e**		**it is distracting to have two PLME_SAP (even though they have the same function) I suggest using their full names**	See figure at the end	
	6.1.3 9.8 Annex A.4.4.1	**MAF**	**T**	**Y**	**The strictly ordered service class was included in this standard to provide an alternative method to handle those cases where the type of frame reordering possible when using Power Management buffering might cause a problem for a higher layer protocol.** **The intent of this provision was to provide a strictly ordered alternative for the applications which may require one, but not to make this facility mandatory for all implementations. Unfortunately, the cited sections and the PICS do not list this facility as optional.**	**Change PC8.2 from status "M" to status "O". Add a sentence to 6.1.3 and 9.8 to indicate the strictly ordered service is optional.** **Note that, in 6.2.1.3, the transmission status of "unavailable service class" is already specified to be returned if strictly ordered service is requested but is not available.**	
	Comments on Recirculation ballot	**PMK**			Comments on recirculation Ballot dated August 1996 1. ⎤Concur with recomandations 2. ⎦ 3.Do not understand the comments 4.⎤ 5.⎢Concur with recomandation 6.⎦ 7.⎤ 8.⎢Obstain lack of time to study 10 ⎦		

Seq. #	Clause number	your voter’s ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal

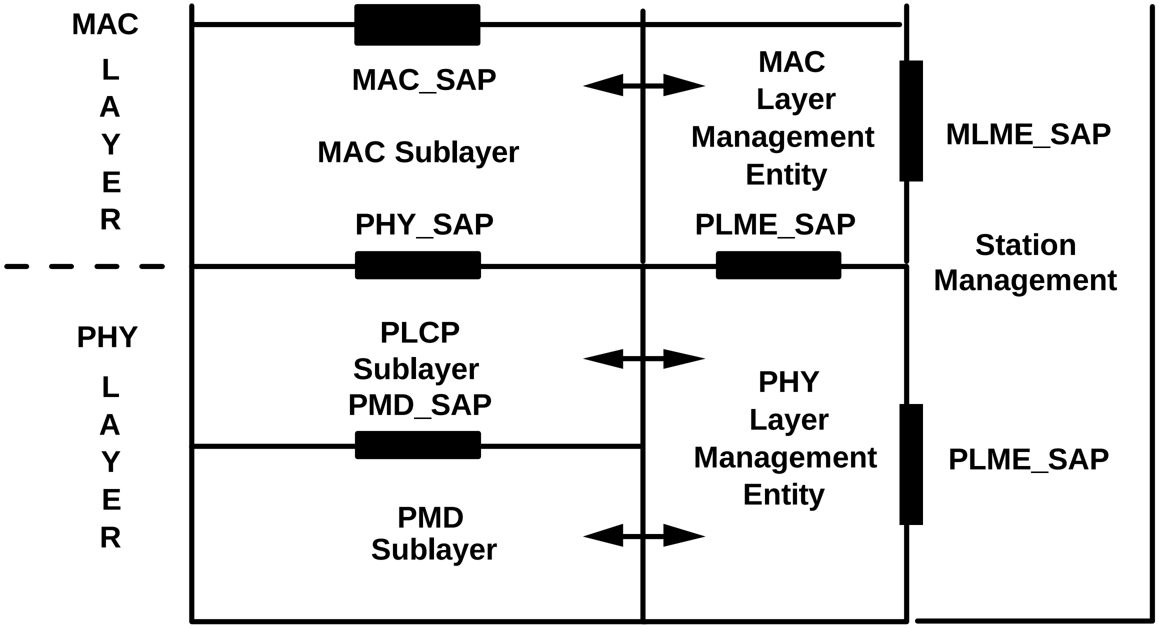
Seq. #	Clause number	your voter’s ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					9. 11. 12. Concur with recomendations 13. 14. 15. Obstain for lack of time to study		
	Foreword	**VZ**	**E**		The foreword should be called Introduction	Change Foreword into Introduction	
	general	**CAR**	**T**		**See end of this document**		
	general	**MT**	**T/e**		**This protocol is based on an assumption that all propagation delays are less than 1µsec. This implies a range of less than 978 feet. In order for this protocol to be used in longer range situations, such as building to building bridges, some adaptations will have to be made.** **Corrections must be made in order to maintain transmit slotting fairness and to adjust the time a station waits for an ACK**	**Add a disclaimer to an introductory section which highlights the range restrictions.** **Additional capability can be accomplished by adding a MIB variable which identifies the distance between to stations. (only useful in a point to point link and point to limited multipoint links) The protocol can be ‘tweaked’ to allow for the extra propagation time.** **A range determination method can be added to the ASSOCIATION protocol which will estimate the range between two stations and adjust the protocol timing accordingly. In the case of point to multipoint, the longest propagation time should be used by all stations in**	

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
						order to maintain fairness.	
	general, 2.3.1, 4	**VZ**	**E**		Incorrect references to sections and paragraphs	Refer to clauses andsubclauses, not “sections” or “paragraphs” like in clause 4 and 2.3.1	
	Introduction	**VZ**	**E**		The Working Group will need to provide an introduction (giving the history of the standard and a description of its purpose) for the front matter	Vic Hayes: I have asked a copy of 802.12 as input material.	
	Table of contents for Figures and Tables	**VZ**	**E**		Redundancy in Table of Contents	Figures and Tables are not normally included in the table of contents	
	various	**RS**	**T**	**Y**	Use of “shall” and PICS: The use of the word “shall” is critically important in IEEE standards. A “shall” mandates a conformance requirement. Therefore, the word should be used SPARINGLY, in precisely those clauses that absolutely require conformance for interoperability or correctness. In addition, EACH AND EVERY “shall” must have an associated entry in the PICS proforma. This has not been done in this standard. The PICS refers generally to sections that contain many shall statements. This in incorrect. There should be a 1:1 correspondence between the number of “ shalls” in the document and the number of conformance requirements in the PICS.. Rather than have a lot of “ shalls”, it is common practice to have a complete detailed description of some desired behavior, either in prose or a formal language/state-machine, then have *ONE*	Eliminate and restructure the use of the term “shall” as indicated, or correct the PICS such that there is a 1:1 correspondence between “shalls” and PICS requirements entries.	

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal

Seq. #	Clause numbe r	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					statement, such as: "The MAC shall implement the requirements of the Transmit State Machine as specified in clause x.x.". This allows one PICS entry for a complex entity.		
	WEP	GC			8 (Vic Hayes ?????)		



Comments fromChan Rypinski:

RC (?) T

Dear Colleagues:

My **Affirmative** vote on this matter is a response to the questions: "Should this document be published as a Standard?" It is not an opinion on whether it is technically adequate. In the past, I have repeatedly expressed to the 802.11 Committee my reservations about the power sensing deferral access method and distributed logic generally. The difficulties remain, and there is little to be gained by revisiting them now.

The difficulties that will be experienced will not occur for the case of one isolated system. There will be difficulty when there are numbers of units comprising numbers of contiguous coverage areas. Because use in contiguous coverages is not coordinated, the aggregate capacity will be much less than it might be and probably much less than is expected.

The ease with which this and any deferral system can be jammed is a major vulnerability. The frequency of occurrence of individuals with both malevolent motives and technical skill is underestimated. The actions of some otherwise normal individuals when frustrated will also find this opening for technical retribution. Also, some technicians will soon learn that strapping the RSSI input to a permanent no-signal condition will greatly improve a minority of users ability to access the channel.

There are additional technical difficulties which will be present if any attempt is made to provide a low bandwidth connection-type service as was announced in the first requirements document.

The high level of skill shown in the protocol work-arounds and technical descriptions cannot undo the weaknesses of the physical medium concepts. The amount of effort expended to create this Standard could have produced something much better. The present result is a distributed logic system with a series of "patches" to provide the unavoidable necessary functionalities of a centrally managed system. Many of these necessary functions, I called to the attention of the Committee in '92 and '93 with little effect. My present concern is with the eventual disappointment of the using public and the consequential loss of confidence in radio systems generally.

If, at the halfway point, a central channel manager function had been defined as the norm with ad hoc as a necessary and useful subset, then a satisfactory standard could have been evolved, which at a minimum would have far fewer pages and management functions.

Publication of this document could well result in a useful standard showing the upward interface for a radio system to the higher layers. Different and better physical mediums can be designed to use it or a subset. I do not doubt that such products will appear on the market.

Chandos A. Rypinski,
Life Fellow IEEE