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

Results of LMSC Ballot on Draft Standard 802.11 D5.0 -

Comment Resolutions on Comments in Clause 5

1	**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	**Editor to do**
2	**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.	OK, clause 5 changed - there are those who consider different PHY bands to be logically different ethers - and those who don't. We made the change in clause 5 to resolve the No portion of this comment.
3	**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.	**Request is respectfully declined. We believe the commenter misunderstood the architecture. As data flows from higher layers into the top of the MAC, this data must be delivered as a Stations moves. Hence, mobility is inherently a primary aspect of the functionality provided by 802.11. Note that it is the mobile STA that decides when to reassociate. While layers higher than layer 2 may well be involved in the implementation of mobility as provided by the MAC (via**

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
							invocation of a DS service), mobility is not a service which can be removed from the 802.11 MAC layer. primary purpose of 802.11 is to provide the mobility services requested - this is what the functions of association, reassociation etc accomplish.
4	**5.2, 1.2, 5.1.1.4, 5.4.2.1, 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.	**Respectfully declined. Please refer to resolution of comment 5 in this clause.**
5	**5.2.3 fig 4**	**SD**	**t**		**The Figure should beaccompaigned 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.**	The figure is ment to be qualitatively typical and not quantiative. The primary purpose is to illustrate that the actual environment is not uniform as many assume. Because the information provided is not quantitative, we declined to specify the power and frequency used in the example.

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
6	**5.2.3 fig5**	**SD**	**e**		**Labels ofSTAs are out of their frames.**	**Recenter them.**	The Sta albels are ok in the printed version of the document we have - we suspect that this is an artifact of how the document is printed - we willendevor to make sure this does not occur in the final printed versions of 802.11.
7	**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"**	Clairified. The previous sentence refers to a "non-802" LAN - the group believes this to be inclusive of "Wide Area Network". We did change a sentence toclairfy that the figure is an example and not the only case possible.

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
8	**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 to gridge 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.	The draft does address how to interconnect between the 802.11 architectue and other 802.X LANs - the method is the Portal. As a portal connects to the DSM, it may or may not include 802.X bridge functions. This is dependent upon the implementation choosen for a specific DS since a DS is not constrained to be an 802.X layer 2 mechanism - it may be an IP based layer 3 or higher system, in which case the subject of bridgeing is not relevant. DS implementation is considered outside the scope of 802 as it required to be a layer 2 issue. Pleas note that 802.11 specifies a MAC and PHY for the WM -ir is not intended to be a complete reference for eveything that might be required to implement a WLAN installation that includes 802.11 links.
9	**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.	**Changed.**
10	**5.3**	**RS**	**E**	**Y**	The statement, "The generality allows 802.11 to satisfy the diverse interests ..." is a clear statement	Eliminate the statement.	**The statement was deleted. (though not for the reasons**

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					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, and (2) looks like dirty laundry hanging out to dry.		**asserted by the reviewer). In fact the group does feel that multiple interests are well served by the generality, not that we did not know how to accomplish our task.**
11	**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.	**Declined. 802.11 has gone to a lot of effort to handle the problems unique to mobile stations using a WM. In order to do this is had to explain the architectural context within which the 802.11 MAC and PHYs operate. This information is crucial to understanding 802.11. Also, refer to resolution of comment 3 in this clause. The 802.11 draft does what is required and appropriate for a MAC layer. I.e. media access to the Wireless Media. DS internals are outside the scope of 802 (not just 802.11). The reviewer is asked to consider that the draft is a MAC/PHY std and not a complete reference fo everything required to create any type of netowork which includes 802.11 links.**
12	**5.3.3**	**GC**			see 7.1.3.3.1 G		
13	**5.4**	**DLP**	**e**		**Clause xx.xx needs to be specified.**	**Replace xx.xx with appropriate**	**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
						clause number.	
14	5.4	**JMZ**	**e**		Typos	Fill in reference marked "xx.xx" and change "DATA SERVICE" to "Data Service"	corrected
15	**5.4**	**KC**	**e**		**"clausexx.xx"**	**specify whatxx.xx is**	**corrected**
16	**5.4**	**MT**	**e**		**find and fill in clausexx.xx reference**		**corrected**
17	**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.	**corrected**
18	**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.	**Respectfully declined. Please refer to resolution of comment 5 in this clause.**
19	5.4.2.2	**JMZ**	**e**		Typo	"System" should not be in Courier font	corrected
20	**5.4.2.2**	**MT**	**t**		**ref: MT_1**	**Specify a minimum number of**	**respectfully declined.**

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
	5.4.3.1				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).	authentications which must be 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 (e.g., 1000 and 100 respectively)	Author ok - Any limits on the number of associations supported is a limitation of a specific AP implementation and/or the DS the AP is an interface to. Since DS implementations are outside the scope of 802.11, this can not be specified by 802.11.
21	5.4.2.2	MT	T		ref: MT_2 An AUTHENTICATION staleout time should be specified such that if no data is transferred between stations for the corresponding staleout 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 opposed to association staleout).	The ASSOCIATION staleout time should be a setable 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 a particular station finds that it is spending too much time maintaining an association because the network is	Respectfully declined. Author ok - The group feel that there is not need for additional functionality along the lines suggested. Should any specific STA desire not to maintina authentication after some time, then it may simply cause a deauthentication. Ther is no need to specify a time at which this would be required to be done - in fact there are cases where this would be undesireable. Hence we belive that the current draft is the most

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
						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.	general mechanism.
22	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.	Respectfully declined. Author ok - There is not such thing as a repeater in the 802.11 architecture. The data flow is from a STA into an AP, into the DS. The DS then determines at what AP the traffic should be delivered by using association information, then the destination AP is given the traffic. Note that a DS which retransmits all incoming traffic to all Aps would be a poor DS implementation. In the case of a WDS, an AP is an interface between two different logical media, even though the two media are the same phyically. In the case of DS traffic being transferred between two Wireless Aps, they are logically in an IBSS that links them together, this is not the same BSS as the one which contains the mobile STA and it's associated AP.
23	5.4.2.2	MT	t		ref: MT_4 In the case of a single cell which has no backbone		No change made as none requested. Author ok -

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					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.		We ask the reviewer to note that the case stipulated does not seem to be possible - how could a wireless AP exist as the only AP in an ESS - to be using the WM as the DSM there would have to be at least two WirelessAPs. It is possible to have a one AP ESS - in this case the DS is logically present (can't have an ESS without a DS) - but then the traffci flow is still as described in the resolution to comment 22 - the only difference is that all ingoing traffic has only one option for the DS exit point - note that not all trafficingoing will also be outgoing from that AP - only those frames with a DA for a STA associated with that AP - hence this is different from a blind repeater function.
24	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.		Authorok/withdrawn - declined. Multicast operation is independent of # stations associated.
25	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	Add text which explicitly disallows membership to multiple concurrent ESS's andIBSS's (a STA can only be a member of an ESS or IBSS at any	Corect - A sta mayon.y be a member of a single BSS at any instant, it does not matter if the BSS is part of

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					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.**	**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.**	**an Ess or an IBSS.** **We can not do > 1 BSs as there is no whay to specify the BSs the traffic is for at the 802.2 inerface.**
26	**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 10 µsec from the current local value.**		
27	**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	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.	**Declined.** **Please refer to resolution of comment 11 this clause.**

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					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.		
28	**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 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.** **-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**	**changes declinedtihe consent of author.**
29	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	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.	Accepted Daft changed as suggested.

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					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.	Adding a clarification to this effect would be good, too.	
30	**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 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 minimum number of authentications which must be 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 (e.g., 1000 and 100 respectively)**	**sams as comment # 20 Please see resolution of that comment.**
31	**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**	**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	Respectfully declined. The group does not share the opinion that authentication is useless w/o encryption. IT is true that authentication is more useful when encryption is also used. While 802.11 authentication does not provide full protection against impostor attacks, it is also true

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					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.** **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.**	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. 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.**	that does provide some protection. To significantly increase the protection against impostor attacks, it would be necessary to encrypt MAC headers - this we can not do because it would require all implementations to do encryption which the group was unwilling to mandate due to the product impact ofU.S. export regulations for encryption. The review comment makes the assumption that an encryption key is always shared by a set of stations. In that senario, one could do what was called implicit authentication, however, limiting system operation to only implicit authentication has not been acceptable to the group. There is a need to be able to handle situations where potentially every pair of communicating stations may have a different encryption key. This requires that we have support for the general authentication mechanism - this same mechanism is also required as some members anticipate extending the standard eventually to support public key authentication and dynamic session encryption keys - the authentication mechanism is necessary to provide that upgrade path. OF

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
							In the IBSS case, if authentication were removed entirely, then it would only be possible to run either an unsecured LAN or a shared key LAN where every member used the same shared key. The group feels that there are clearly many situations where not all Stations in an IBSS want all other stations to hear every frame and so finds that restriction undesirable.
32	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.	
33	**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 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.**	**Author ok.** **This operation has been calirified as the result of other comments. It is required that all STAs implement Open sys auth, but not all instances of open stat auth must be successful.**
34	**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**	**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**	**Comment withdrawn by author after discussion.**

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					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 differenAPs.	**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.**	
35	**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.	**Corrected in clause 5**

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
36	**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)." .	**both the Original problemsshich lead to the statement objected to and the statement have been corrected.**
37	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 haveCFPs 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."	See comment #37 resolution.
38	5.5	**JMZ**	**t**		The three requirements to send aDeauthentication or Disassociation frame to STA B should not apply to an AP. Otherwise, anunassociated STA would have to complain whenever it received a broadcast, which would	Add ", except if STA B in an AP" to the end of the three appropriate sentences that now end with "STA B".	text clairified to explain that this requiement does not apply to reception of broadcast messages.

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					clearly be harmful.		
39	5.5	MT	t		ref: MT_10 Clarify operation of AP which is 'always in state 3'. If no stations are associated, are multicast packets to be forwarded via the RF anyway? If the AP supports WEP, how should multicasts be transmitted? By disallowing multicast retransmission without any association will conserve bandwidth only in the case of overlapping coverage areas. However, By allowing multicast 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 that multicast 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.	Problem Correct in draft text.
40	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 all multicasts 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)	Author OK In the case sitpulated the frame is "received" at the phy, but it is not "received" at the top of the mac as if will not pass the filtering criteria specified in other clauses of the draft - the frame is dropped - this is the surrently specified operation of the MAC in 5.0.
41	5.5	MT	T		ATIMs must be allowed in state 1 (at least for the 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		

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					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.		
42	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.		commnet withdranw. Question of multicast vs wep is still being handled as part of other comments.
43	5.5	MT	t		ref: MT_12 are multicast authentication packets allowed? Allowing such, could improve IBSS setup performance.		No, this is not allowed as all authentication is pair wise. Text added to clairify this.
44	5.5	MT	t		ref: MT_13 the standard identifies that a frame received from a non-authenticated station requires that a 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		This has been corrected in the draft text for the next revision.

Seq. #	Clause number	your voter's ID code	Cmnt type E, e, T, t	Part of NO vote	Comment/Rationale	Recommended change	Disposition/Rebuttal
					responded to with a deauthentication frame.		
45	**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?**		**Author withdraws comment as it is covered by previous comment resolutions to other comments from the Author.66**
46	**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.**	**Reference is unnecessary as the terms are previously defined in cluase 3 definitions.**
47	**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 wait until the DTIM time to deliver the dissociation request to the broadcast address.*{this is normal operation, but should be clarified here}***		
48	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.	
49	**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	