# IEEE P802.11

## Wireless Access Method and Physical Layer Specification

## Section 2 Response to Draft D1 Letter Ballot processed at March 1995 meeting

Davc Bagby
Advanced Micro Devices
PO Box 3453 M/S 17
One AMD Place
Sunnyvale CA 94088-3453 USA
Phone: +1 408 749 5425
Fax: +1 408 774 8446
E-Mail: david.bagby@amd.com

**Abstract:** This paper presents the Section 2 Response to the Draft D1 Letter Ballot proccesed at March 1995 meeting.

**Action:** Adopt the changes in this paper to replace the relevent portions of Section 2 of P802.11/D1, as shown in the companion document P802.11-95/56.

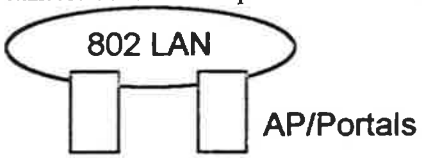
| DISPOSITION | C# | SECTION | AUTH. | T/E | ***PROPOSED CHANGE*** | RATIONALE |
|---|---|---|---|---|---|---|
| 1,2: recommended | 1 | 2 | David Bagby | T | ~~***[The text following reflects the closure of issues in sections 5 and 6 of the issues log]***~~<br>***[DB1]*** | See imbeded comments and annotations |
| recommended see 1 | 2 | 2 | Rick White | T | Remove Editor's comments | |
| 3: recommended: remove a, change b to Uses a medium shared with adjacent LANs and non-LAN devices. | 3 | | Bob O'Hara | T | delete a) and b) from the list | These characteristics are NOT different than a wired medium. |
| recommended | 4 | 2.1.1.2 | C. Thomas Baumgartner | t | add f) The assumption normally made that every STA can hear every other STA is not valid | This is one of the major differences between wireless and wired which has major implications |
| recommended | 5 | 2.1.1.2 | Fischer, Mike. | T | section headingÑNeither ÒThe Medium Impacts . . .Ó or ÒThe Media Impact . . .Ó<br>item (a)Ñchange ÒlimitedÓ to ÒshorterÓ and change ÒrangesÓ to Òranges than wired LANsÓ<br>item (b)Ñchange ÒmediumÓ to Òmedium that has neither absolute nor readily observable boundaries outside of which stations with conformant PHY receivers are known to be unable to receive the network frames.<br>item (d)Ñreplace with ÒExhibit significantly higher bit error rates than wired PHYsÓ | clarity, correct attribution of the Òless reliableÓ to data reliability reduction, not MTBF reduction |
| recommended | 6 | 2.1.1.2 | Rick White | T | 802.11 PHYs lack full connectivity even within a BSS. | This is a fundamental problem with RF LANs. |
| Recommendation: covered by rec 7 | 66 | 2.1.1.3 | CHRIS ZEGELIN | | NEED A STATEMENT AS TO HOW THE PROTOCOL EFFECTS POWER CONSUMPTION IN A MOBILE BATTERY POWERED UNIT. | THERE IS NO INDICATION AS TO THE IMPORTANCE OF POWER MANAGEMENT BUILT INTO THE PROTOCOL. |
| recommended | 7 | 2.1.1.3 | Greg Ennis | T | Add a third paragraph: "Another important aspect of mobile stations is that they will often be battery-powered and hence power management is an important consideration. For example, it cannot be presumed that a station's receiver will always be powered on. " | This is an important impact of handling mobile stations. |
| recommended | 8 | 2.1.1.4 | Fischer, Mike. | T | change Òreliability assumptionsÓ to Òreliability and security assumptionsÓ | The same logic aplies to the untraditional approach of including some security features in the MAC as for reliabilityÐrelated differences with tradition. |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | ***PROPOSED CHANGE*** | RATIONALE |
|---|---|---|---|---|---|---|
| Recommendation: accept | 67 | 2.2 | CHRIS ZEGELIN |  | 'BSS' DEFINITION USES THE UNDEFINED CONCEPT OF 'CF'. 'CF' IS DEFINED MUCH LATER. COPY 'CF' DEFINITION INTO THIS SECTION. |  |
| 10: recommendation:<br>ask author - does not seem to improve the doc. the text as described in he comment is correct, the picture is limited by drawing ability (can't draw fractal easily), so would recommend leaving text as is. | 10 | 2.2 | C Heide | T | last paragraph of section: "It is useful to think ... can remain in communication with all other member stations. The concept ... no longer communicate with all other members of the BSS." | This is required to remain consistent with the drawing. In the drawing the BSS's cover only where the two member stations can communicate with each other, not where the coverage of each individual station extends. This implies that the BSS only covers where all members can communicate with al other members, not just where any two can communicate with each other, which is what the existing text implies. |
| 11: recommended for a informative annex if someone volunteers to write and provide one. but is not part of the normative part of the text. | 11 | 2.2 | Rick White | T | Include some descriptions of possible physical implementations. | Section 2.2 is that it are very confusing. It may require some descriptions of possible physical implementations. The architecture components area have been very confusing to voting members of the committee. This is evident from the discussion on wireless distribution systems preceding the Nov. 94 meeting. |
| 12: recommended sentence improved to reflect comment - words "coverage area" recommended for removal from last sentence 2nd para after figure 2-1. | 12 | 2.2 | Rick White | T | Need to define what is meant by the coverage of a BSS | Last sentence of 2nd paragraph after Figure 2-1 - What defines the coverage of a BSS? In an ad hoc network is it area in which all STAs can communication with one another or does a station have to communicate with only one other member of the BSS? In an infrastructure network is it the coverage of the AP? |
| 13: recommended | 13 | 2.2.1 | Bob O'Hara | T | replace "close enough to form a direct connection" with " able to communicate directly" | Proximity does not imply ability to connect. |
| 14: recommended: already done in defs (and previous recs) - moot comment - ask author. | 14 | 2.2.1 | Rick White | T | Define that an Independent BSS has no connection to any other 802.11 LAN or a distribution system. | Clarifies what is meant by Independent BSS. |

| DISPOSITION | C# | SECTION | AUTH. | T/<br>E | ***PROPOSED CHANGE*** | RATIONALE |
|---|---|---|---|---|---|---|
| 15: recommendation: decline. answer to question is no. This is why draft is currently silent on this - i.e. must be able to talk to stas you want to talk to, but not all stas in an IBSS - this is why it is an "T". The DCF is not the same set of STAs as the IBSS... which is why it is not necess to define total connectivity as a requirement of an IBSS. | 15 | 2.2.1 | Rick White | T | Need to define if all STAs in an independent BSS must communicate with one another | Do all STAs of an Independent BSS have to be able to communicate with all other members of the BSS? If so, how does a station know what other STAs make up the IBSS. |
| 16: recommendation: decline: IBSS has no AP that is why it is an "T". | 16 | 2.2.1 | Rick White | T | Need to clarify the definition of a IBBS | Does a IBBS contain an AP or are there two different types of IBSSs, one containing a AP and another not containing an AP? |
| 17: recommendation: no change Misunderstanding we believe. An AP is the interface to an Infrastr net - thus the **logical** DS is present. even if only a physical AP is present. Comment confuses logical arch with physical boxes. | 17 | 2.2.1.1 | Rick White | T | An AP does not have to be part of an infrastructure network. | A standalone AP could be used for range extension. |
| recommendation: decline is described in the next section, strict define before use policy is satisfied by defs in sec 1 which precedes sec 2. | 68 | 2.2.2 | CHRIS ZEGELIN | | ESS IS USED BUT NOT DEFINED IN THIS SECTION. COPY THE ESS DEFINITION INTO THIS SECTION. | |
| recommendation: no change requested. also improved by sec 2 update to sec 1 c changs. | 69 | 2.2.2 | CHRIS ZEGELIN | | AP HAS A SUPERSET OF STA FUNCTIONALITY. THE WAY THE WORDING IS, IMPLIES THAT AN AP CAN BE MADE FROM A STA, WITH THE DS SERVICES BOLTED ON THE BACK. | |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| recommended | 18 | 2.2.2 | David Bagby | T | PHY limitations determine the direct station to station distance which can be supported. For some networks this *distance*~~limitation~~ is sufficient, other networks require increased coverage.<br>Instead of existing independently, a BSS may also form a component of an extended form of ~~an 802.11~~ network which is built with multiple BSSs. The architectural component used to interconnect BSSs is the Distribution System.<br>**Distribution System** (DS): A system used to interconnect a set of BSSs to create an ESS.<br>**Distribution System Medium** (DSM): The medium used by a DS (for *AP*~~BSS~~ interconnections).<br>*[DB2]* | See imbeded comments and annotations |
| 19: recommendation: not a tech comment - color of pic not important only difference in shading. re ? re color, unknown at this time - printing costs TDB. | 19 | 2.2.2 | Geiger | T | In figure 2-4 the red | Will the standard be in color? |
| 20: recommendation: text change declined. this is true as A form of DS, we don't know it is the "simplest" form. A submission to an informative example implementation annex is welcome but not change Id needed for the draft. | 20 | 2.2.2 | Rick White | T | It must be pointed out in that the simplest form of a distribution system in an 802.11 LAN is an AP that receives traffic from one station and relays it to another STA in the same BSS. | In my mind this is a form of an Independent BSS. Need to add figure showing three STAs in a BSS, one being an AP, that is not connected to an external DS (which is connected to another BSS). |
| recommended | 21 | 2.2.2, 7th paragraph | Fischer, Mike. | T | change Ò. . . seamless integration of multiple BSSs.Ó to Ò. . . seamless interconnection of multiple BSSes into a single logical network.Ó | ÒintegrationÓ is what is done with other, wired LANs, not between BSSes. |

| DISPOSITION | C# | SECTION | AUTH. | T/E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| 22: recommended: all defs in sec 2 need to be resolved to revised sec 1 text after all LB comments processed - this comment t falls into that category. | 22 | 2.2.2, 9th paragraph | Fischer, Mike. | T | add at end of sentence Ò for stations in the same BSS that do not have such access without using the WM.Ó | The key issue for ÒAPÓ is the provision of access via the WM to stations that lack any other communication path that gets their transmissions to the DSM. |
| 23: recommended. | 23 | 2.2.2, last paragraph | Fischer, Mike. | T | add at end of sentence Ò and the addresses used by an AP for communication on the WM and on the DSM are not necessarily the same.Ó | clarity |
| recommendation: insufficient data to know what to change. def improved in sec 1, assume that this will be enough. | 70 | 2.2.2.1 | CHRIS ZEGELIN | | ESS DEFINITION DOESN'T SEEM RIGHT | |
| recommendation: change - see rec 25 | 71 | 2.2.3 | CHRIS ZEGELIN | | INTENSITY MAP - COLOR VS. SIGNAL STRENGTH IS NOT DEFINED | |
| 24: recommended: harmonize with sec 1 after LB COMMENTS | 24 | 2.2.3 | David Bagby | T | **Basic Service Area** (BSA): The *conceptual* area within which members of a BSS can communicate.<br>**Extended Service Area** (ESA): The *conceptual* area within which members of an ESS can communicate. An ESA is larger than or equal to a BSA.<br>***[DB3]*** | See imbeded comments and annotations |
| 25: recommended, clarification paragraph would improve. exact quantification is not needed.<br>Suggestion for para:<br>The figure indicates relative differences in signal strength, colors are diff field strengths.<br>(will look for legend from orig picture and add in to doc). | 25 | 2.2.3 | Rick White | T | Figure 2-4 requires a legend to indication what the different colors represent. | |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | ***PROPOSED CHANGE*** | RATIONALE |
|---|---|---|---|---|---|---|
| 26: recommended: harmonize with sec 1, comment is editorial in nature and not needed as part of the actual def. | 26 | 2.2.3, last paragraph | Fischer, Mike. | T | add at end of sentence Òand may involve multiple, disjoint, physical BSAs and/or sites.Ó | The ESA is not only larger than or equal to the BSA, the ESA can have nonÐcontiguous coverage (by design, not just due to shadowing and signal interference) due to geographic separation of the BSAs. |
| recommendation: decline 802.11 does not spec DS implementations, this is a DS implementation attribute.<br>A contribution for an informative annex example is welcome. | 72 | 2.2.4 | CHRIS ZEGELIN | | NEED SOME TEXT TO DESCRIBE PROBLEMS WITH ROUTERS IN THE DS | PEOPLE WHO READ THE SPEC NEED TO KNOW THAT WE ARE AWARE OF THE PROBLEM |
| 27: 1/2 recommended, strike "traditional" but not add "802" as a qualifier as the portal concept is not limited to 802 connectivity. | 27 | 2.2.4 | Bob O'Hara | T | replace "a traditional wired" with "another 802" in the second paragraph | consistent with revised definition of integration (see comment on section 1.2, definition of "Integration"). |
| 28: recommended: if intent is to point out that AP and portal func could be in same physical box, this is already possible. Suggestion is to add a sentence that says: It is possible for one device to offer both the functions of and AP and a Portal, this could be the case when a DS is built from 802 LAN components. | 28 | 2.2.4 | Greg Ennis | T | Add the following at the end of the section: "Such an AP which is acting simultaneously as a portal to a distribution system which consists of a standard 802 LAN is depicted in the following figure:  | Clarifies the Portal concept in the context of 802-standard distribution systems. |
| 29: recommended: similar to 28, covered by that rec. comment 29 is an example, not the only possible case. | 29 | 2.2.4 | Rick White | T | Is it not true that the DS is probably an 802.x LAN? If so, than does that mean that an AP would contain a portal since a DS is defined as "a system used to interconnect a set of BSSs to create an ESS. Does it also follow that if the DS is an 802.x LAN then other non-802.1 devices could be connected to it. If this is not true then it must be stated that only APs can connect to a DS and if the DS is shared with other non-802.11 devices, the AP must contain a portal | |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| 30: recommended. | 30 | 2.2.4.1 | David Bagby | T | Physically, a Portal may, or may not, include bridging *or routing* functionality depending upon the physical implementation of the DS *and the wired LAN. [DB4]* | See imbeded comments and annotations |
| 31: recommended: add following to list:<br>MSDU delivery.<br>discussion: are the others a flavor of MSDU delivery or a separate service? ask group. | 31 | 2.3 | Greg Ennis | T | Add "Asynchronous Data Transfer", "Power Management", "Contention Free Connection Management", and "Time Bounded Data Transfer" to the list of the "complete" set of 802.11 services. | List is not complete |
| 32: decline - this done as contents of next section (2.4) - is it really necess as a tech comment that the text be part of sec 2.3? - ask author for opinion. | 32 | 2.3 | Rick White | T | Each architectural service must be defined in this section | |
| 33: recommended: change sentence to: "... with network layer mobility approaches (e.g. Layer 3 mobility standards such as IETF mobile IP)". | 33 | 2.3, last paragraph | Fischer, Mike. | T | Either define (or add an example of) Ònetwork layer mobility approachesÓ or change the sentence to use a term already defined in this document. | understandability by the target audience |
| recommendation: covered by rec 31. | 73 | 2.3.1 | CHRIS ZEGELIN | | STATION SERVICES ARE MORE THAN THE SUBSET LISTED. THAT OR THE DEFINITION OF SS IS WRONG. | |
| 34: recommended: really an editorial comment. | 34 | 2.3.1 | David Bagby | T | The Station Services are present in every 802.11 station (including APs; as APs include station functionality). Station Services are specified for use by MAC layer entities. All conformant stations provide Station Services. ~~In the figures, dots will represent Station Services.~~<br>deleted because the figures don't use dots.*[DB5]* | See imbeded comments and annotations |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| 35: recommended: dependent on figure 2-8 change comments - make consistent with those decisions. | 35 | 2.3.1 | David Bagby | T | The Station Services subset is:<br>a) Authentication<br>*b) Deauthentication*<br>c~~b~~) Privacy<br>***[DB6]*** | See imbeded comments and annotations |
| recommendation: insufficient info to know what the commenter wants. | 74 | 2.3.2 | CHRIS ZEGELIN |  | THE DEFINITION OF DSS IS WRONG. |  |
| 36: recommended: reference base doc instead of duplicating. also could refer to sec 4 where this info is in the frame format section? | 36 | 2.3.3 | Rick White | T | Include a diagram of the 802.11 802 48-bit address. | Help with understanding of the addressing. Does not require reader to get another standard. |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| 37: recommendation: needs big group disc. | 37 | 2.3; also 1.2 definition of ÒinfrastructureÓ2.4.1.1, 6th paragraph; 2.4.2.2, 3rd paragraph; 2.4.2.3, 3rd paragraph; 2.7 | Fischer, Mike. | T MAJOR ISSUE | The standard needs to specify the message formats used to communicate (intraÐESS) for the provision of (at least) association, reassociation, integration, and distribution. This requires enough words (and pictures), and impacts enough places in the document, that I have not attempted to put specific text in this box of the table. A set of changes adequate to overcome my ÒnoÓ vote on this subject appear in document 95/17.<br><br>The bulk of the message format information will end up in section 2.7. | The fundamental purpose of this standard is to provide a basis for mixedÐvendor interoperability across each of the exposed interfaces in the subject specification. The WM is one such exposed interface, and is covered in considerable detail in the D1 draft. The DSM is another such exposed interface, but the degree of abstraction of distributionÐrelated definitions makes interoperable distribution (even in simple cases such as multiple vendorsÕ APs attached to the same 802.3 wire) impossible without additional definitions. Even the current draft states that there is an exposed interface between access points and the distribution system (even if not stated very well, see above). The concept that 802.11 should Ònot specify specific DS implementationsÓ remains valid. What is needed is the definition of specific frame payloads, that can be delivered over 802Ðstyle LANs, which shall be used for interÐAP communication (called an IAPP in some submissions to this working group) to establish the necessary information about associations/reassociations to support mobility transitions; and for APÐto/fromÐportal communication to support integration of other 802 wired LANs.<br><br>In 2.4.1.1, 6th paragraph is states that Òall 802.11 is required to do is to provide the DS with enough information . . .Ó This is generally correct, but the support of reassociation for BSSÐtransition mobility, and the preservation of ÒauthentificationÓ across such transitions (even when using a wireless distribution system), require the directed exchange of information between the DSS at one AP and the DSS at another AP in the same ESS (among other intraÐESS exchanges between MAC LMEs over the DSM). How the DS gets the messages containing this information between APs may be external to this standard, but the formats of those messages must be defined or users will have to outfit an entire ESS with APs from a single vendor (or deÐfacto interoperabiity group of vendors operating outside of the 802 standards process), even if they can procure nonÐAP stations from multiple sources.<br><br>The other alternative is to remove mobility support and the ESS concept from the standard. This not only leaves aspects of the PAR unaddressed, but would yield a standard that fails to meet most usersÕ needs ÐÐ at the ranges discussed for several of the PHYs almost any potential customer for more than about 10 or 15 stations would probably need to deploy a multiÐAP ESS. |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| recommendation: none. insufficient info to know what commenter has in mind. | 75 | 2.4.1.1 | CHRIS ZEGELIN | | DISTRIBUTION DOES NOT NEED ASSOCIATION INFORMATION TO DELIVER AN MSDU FROM A STA TO THE DS. IT DOES NEED ASSOCIATION INFORMATION TO DELIVER FROM THE DS TO A STA. THE STATEMENTS ARE SLIGHTLY WRONG. | |
| 38; recommended | 38 | 2.4.1.1 | David Bagby | T | In either example, the Distribution service was logically invoked. Whether the message actually had to traverse the physical DSM or not is a DS implementation matter and not specified by 802.11.<br>*While 802.11* does *not specify DS implementations, it does recognize and support the use of the WM as the DSM. This is specifically supported by the 802.11 frame formats. (Refer to section 4 for details).*<br>***[DB7]*** | See imbeded comments and annotations |
| 39,40: recommendation: see comment on 37, group disc. | 39 | 2.4.1.1 | N. Silberman | T | needs definition of interconnectivity within the Distribution System in order to allow interoperabilty between access points | Without this definition of connectivity between APs the Distribution system is useless as an interoperable system and left to proprietary or incompatible implementations. |
| 39,40: recommendation: see comment on 37, group disc. | 40 | 2.4.1.1. | P. Brenner | T | The IAPP (Inter AP Protocol) is defined in section xxx | An Inter-AP_Protocol MUST be defined, otherwise the users will not be able to use different vendors APs in one single ESS. |
| 41: declined. removing this concept would eliminate the ability to connect with wired LANs. | 41 | 2.4.1.2 | N. Silberman | T | Remove the definition of Portal | If the statement starting with "The details of an integration service... is true then the definition of a portal just confuses the issues. |
| 42: recommendation: covered by comment 38 rec. frag part of comment incorrect - this will be gone by the time the logical portal function is invoked. | 42 | 2.4.1.2, 3rd paragraph | Fischer, Mike. | T | Add statement to the effect that: ÒIntegration service may use the 802.11 MAC for message delivery in cases that the DSM and WM are the same.Ó Also, add ÒrefragmentationÓ to the parenthesized list in the next-to-last sentence. | completeness |

| DISPOSITION | C# | SECTION | AUTH. | T/E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| 43: recommendation: disc required by group | 43 | 2.4.1.2, last paragraph | Fischer, Mike. | T MAJOR ISSUE | The statement that details of an integration service are dependent on a DS implementation are correct. However, this does not mean that the subject should be ignored. Just as with DSSÐtoÐDSS messages across the exposed distribution system interface discussed in relation to 2.3, the ISÐtoÐDSS messages need to be specified to permit portals from one vendor to work on the same distribution system as APs from another vendor Ñ the alternative is to eliminate the portal as a separate functional element and make Integration a service that must take place on an AP (which I would expect to be a common implementation approach, but should not be required as the only practical approach). What should be done is the addition of specification of the functional characteristics of a portal, and the message contents that must be exchanged with DSS. These characteristics primarily concern address resolution (to/from the 802.11 address space, independent of the other sideÕs address space, frame size limitations on the DSM relative to the integrated LAN (the LANÕs limitations are outside our part of the problem and the DSM relative to the WM is covered in the existing draft), access to the DSS mechanism to resolve mobility transitions, and the point at which WEP ends (especially relevant when the ESS uses WEP and the integrated LAN uses a different 802.10 mechanism). Acceptable words to describe these functions appear in document 95/17. | see discussion in column to left |
| 44: recommended | 44 | 2.4.2 | C. Heide | T | Throughout the section the word "mobile" should not describe the word STA:<br>page 23, lines 12, 15, 19, and 29; page 24, line 1. | All STAs are required to adhere to the association services not just mobile ones. |
| 45: recommendation: see section 1 - really a sec 5 comment on services | 45 | 2.4.2,<br>1.1,<br>3.2,<br>5.8 | Jim Panian | **T** | Provide MAC service primitives to facilitate the three distribution system services:<br>• Association<br>• Reassociation<br>• Disassociation - including the detection of link outage<br>The above mentioned MAC service primitives will feed into the Association, Reassociation, and Disassocation services in the state machine descriptions as well. | Enough detail must be provided by the 802.11 standard to facilitate hand-off mechanisms on the distribution system. |
| 46: recommended. | 46 | 2.4.2.1 | C. Heide | T | Item (a), item (2), replace "e.g." with "i.e." | movement within PHY range of the communicating stations is within a BSA be definition - within a BSA is not an example f such movement. |
| recommendation; no change requested, treat as editorial | 76 | 2.4.2.2 | CHRIS ZEGELIN |  | ASSOCIATION IS REALLY THE ACT OF INFORMING THE DS HOW TO ROUTE A MESSAGE FROM THE DS TO THE MOBILE UNIT. THE TEXT IMPLIES THE OPPOSITE. |  |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | ***PROPOSED CHANGE*** | RATIONALE |
|---|---|---|---|---|---|---|
| recommendation: see rec 48 | 77 | 2.4.2.2 | CHRIS ZEGELIN | | THE CONCEPT OF A STA BEING CONNECTED TO TWO AP'S, EACH IN A DIFFERENT ESS IS PRECLUDED. REMOVE THE SENTENCE THAT SAYS THAT A STA CAN ONLY BE ATTACHED TO A SINGLE ESS. | MAKING IT CLEARER HOW THE MESSAGE ROUTING ACTUALLY WORKS IMPLIES THAT ITS OK TO BE CONNECTED TO TWO OR MORE SEPARATE ESS'S. PART OF THIS CONCEPT COMES FROM BEING SIMULTANEOUSLY PART OF AN AD HOC NETWORK AND AN INFRASTRUCTURE NETWORK WITH DIFFERENT ESS'S |
| 47: recommendation: decline<br>see 48, 77 also<br>Hum, the enforcement is at the STA not the DS? things break if multiple AP association is allowed. broadcast ack, response to msg etc? think this thru before making al alteration. group discussion needed. | 47 | 2.4.2.2 | C. Heide | T | To the end of the first sentence of the fourth paragraph which begins "At any given instance ...", add the clause "within an ESS". | Nothing can prevent a STA from becoming associated with two APs in different ESSs, as the APs cannot communicate with each other. The STA may think it is only associated in one places, but the APs don't know that (until perhaps some association timer expires on one of them). |
| 48: recommendation: decline this would break distribution as it would no longer be possible to determine the output point of the DS for distribution. | 48 | 2.4.2.2 | Lewis | T | Delete "at any given instant a mobile STA may be associated with no more than one AP." | This is not necessarliy true. and is dependent upon the handoff mechanisms utilized by the DS. During a roaming handoff, a STA reassociates with a new AP, and an infinitely instantanous handoff may not be possible. This results in brief instances where one of two possible conditions can exists: the mobile station may be associated with no APs, or with 2 APs until the handoff within the DS is completed. Since the mechanism of disasociation with the old AP is not defined in the standatd, and is implied to be a function of the DS, this statement places undo restirctions on the functionality of the DS. |
| 49,50: recommendation: not a section 2 problem other than editorial para reference. This is a sec 7 comment. | 49 | 2.4.2.2 | Rick White | T | Paragraph 8: Define how an STA determines what APs are present and determine which to use. | Paragraph 8: There is no information in Section 7 that defines how an STA determines what APs are present and determine which to use. This must be defined. |

| DISPOSITION | C# | SECTION | AUTH. | T/E | ***PROPOSED CHANGE*** | RATIONALE |
|---|---|---|---|---|---|---|
| 49,50: recommendation: not a section 2 problem other than editorial para reference. This is a sec 7 comment. | 50 | 2.4.2.2. | Mahany | T | Second to last sentence replace 7.xx with appropriate reference (scanning) | Omission |
| 51: recommendation: leave as is. choice is F1(a) => reassociate vs. F1 = assoc, F2 = reassoc. Explicit is preferred to context sensitive purpose determination. Grp discussion needed? | 51 | 2.4.2.3 | A. Bolea | T | | Reassociation Service is redundant and should be removed. Association Service is sufficient to handle mobile stations. An Association message with a "Current AP" element when joining a new AP can be used and will be much easier to implement. The "Current AP" is already defined as an element. The presence of this element indicates that the station is already associated with another AP. This simplifies the standard by removing one frame type. |
| 52: recommended | 52 | 2.4.2.3 | Fischer, Mike. | T | add ÒReassociation service also enables changing associationÐtime attributes of an established association to be changed while the STA remains associated with the same AP.Ó | consistency with other sections of the draft |
| 53: recommendation: decline<br>- not needed to spec. group discussion required? Who will spec and do required work in time available? | 53 | 2.4.2.3 | Lewis | T | need to specify algortihm that triggers a STA to initiate reassociation | This relates to the issue of roaming and handoffs. 802.11 need to specify boundary rules regarding roaming and reassociation. |

| DISPOSITION | C# | SECTION | AUTH. | T/<br>E | ***PROPOSED CHANGE*** | RATIONALE |
|---|---|---|---|---|---|---|
| 54: recommendation: decline<br>- see comment 51. comment is to delete as a separate msg, this implies must scan msg body to know is reassoc, this is harder than header scanning which is more likely to be in hdw than body scanning. | 54 | 2.4.2.3 | Renfro | T | Delete Reassociation | Reassociation is redundant with the Association function. First, I believe it is dangerous to assume just because an AP receives an Association message from a STA that that STA is not currently associated with another AP. It is not unreasonable to assume that in an office environment someone might turn off their laptop (and NIC) and move to another location and try to acquire the network. This could result in a resetting of the NIC such that it would perform association (not Reassociation) even though it never disassociated with the previous AP. For this reason, all APs tied to the DS should be informed when a new association occurs. Second, if it is still desirable to include information about the previous AP, it can be done by adding the Current AP element to the association message. |
| 55: recommendation: no change needed - decline: no need, sta is initiator in both cases. If Sta doesn't know then it is broken.<br>if sta thinks is associated, then use reassoc, otherwise do assoc. | 55 | 2.4.2.3 | Rick White | T | Must define how a STA determines if should use Association or Reassociation. | For example, a STA may only use Association the very first time it is used or it may use Association after power-up or after it hasn't "heard" the current AP for some period of time, etc. |
| 56: recommendation: no change.<br>sec 7 (MIB) has timers to protect against these situations. If something is missing from Mib then work in mib is needed but sec 2 sentence is ok. | 56 | 2.4.2.4 | C. Heide | t | remove last paragraph | the MAC management does nothing to "protect itself against STAs which simply dies or go away". The addition and removal of STAs from the polling list, or even what to do with the fact a STA has associated, is described as beyond the scope of this standard. |
| 57: recommended | 57 | 2.4.2.4, 4th paragraph | Fischer, Mike. | T | delete ÒmobileÓ in Òmobile STAÓ also change Òis not a requestÓ to Òis a notification, not a requestÓ | first change removes overÐspecification, as mobility is irrelevant in this case, the second change is for clarity |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| 58: recommendation: decline<br>- harmonize w/ sec 1 - already improved in those recs. | 58 | 2.4.3 | C. Thomas Baumgartner | t | change first sentence "...to provide functionality which is subjectively equivalent to that which..." | The definition of wired equivalent privacy in 1.2 uses the word subjectively. The more difinitive statement now made has not been proven to be correct technically. |
| 59: recommendation: decline: encryption is the mechanism, the service is privacy/confidentiality. so the suggested change would be incorrect. | 59 | **2.4.3** | **Siep** | **T** | **Access and Confidentiallity Control Services** Two services are provided to bring the 802.11 functionality in line with wired LAN assumptions; Authentication and *Encipherment*~~Privacy~~. Authentication is used instead of the wired media physical connection. *Encipherment* ~~Privacy~~ is used to provide the confidential aspects of closed wired media. | Encipherment more accurately reflects what is being done. Since addresses are in the clear (see 2.4.3.2, below) traffic analysis is still possible. Without hiding the addresses, true privacy is not achieved. |
| recommendation: no change requested. comment is incorrect in that assoc is not req, but auth is by design. | 78 | 2.4.3.1 | CHRIS ZEGELIN | | THERE IS AN INCONSISTENT USE OF 802.10, A HIGHER LAYER , THAT IS IMPOSSIBLE TO GET TO WITHOUT FIRST ASSOCIATING. | NEED TO THINK OF AUTHENTICATION AS A SERVICE THAT HAPPENS AFTER ASSOCIATION. THIS WILL REMOVE LIMITATIONS ON INNOVATIVE PRODUCTS. |
| 60: recommendation: no change requested or needed.<br>in commentary the answer to 1 is that auth is always required, but can be null C/R. Ques 2 is an editorial comment that the author would like something different from what the draft currently says. math arg is based on assumption of auth scheme in use which is not necess either true or false.<br>Auth is already speced for both infra and ad-hoc, see other place in sec 2 (sta state diagram). | 60 | 2.4.3.1 | A. Bolea | T | | The following sentence found in this section is confusing:<br>**"If desired, an 802.11 network can be run without authentication..."**<br>Question 1: Is authentication required? If the above sentence refers to authentication with a Null challenge/response, it should be worded as such.<br>Question 2: Is authentication required for an Ad-Hoc Network? I think that it should not be required. For a 10 station Ad-Hoc network in which all stations chose to talk to each other, 10!/(2*8!)=45 different authentications will be required. Each authentication requires 6 messages. This seems excessive.<br>If we decide to require authentication in Ad-Hoc Networks it should be clearly spelled out in this section. |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| 61: recommendation: decline . sentence is correct as stated." may" means is possible (which is true). Sentence does not preclude "open" / unsecured operation. The sentence is truthful. | 61 | 2.4.3.1 | C. Heide | T | remove the second sentence of the sixth paragraph "802.11 cautions against ... network layers.". | This does not reflect the feelings of the group. Operation in the clear is something the group agreed must be an option. |
| 62: recommendation: decline similar misunderstanding as comment 61. No just given for 2nd change requested (C/r sufficient etc...) - declined. | 62 | 2.4.3.1 | C. Thomas Baumgartner | t | Delete paragraph "If desired, an 802.11 network can be run without authentication. 802.11 cautions against this as it may violate implicit assumptions made by higher network layers."<br>Delete sentence in 4th from last paragraph "C/R exchanges are sufficient to support authentication from password based..." | Every time there has been a vote on this subject my recollection is that the majority voted that authentication by what is called "open system example" is a valid choice. These sentences contain editorial comment of the minority in these votes which is trying to scare the public. The paragraph contradicts the penultimate paragraph in this same section which says 802.11 requires authentication. The security of wire is a matter of degree and perception. NIC's can be doctored to be any MAC address; a Sniffer can hear everything that goes over the cable, there is enough stray energy from 10BASE-T that a good receiver can pick it up outside the physical confines. Anyone truly worried about this subject has taken steps at higher layers of the network, even on a wired network. The ability to confine IR to an area, giving the same physical access control as wire, makes this paragraph inappropriate for at least one of the 802.11 PHY's. I dare say there are more people with the ability to tap wired LANs than there are who will be able to intercept DSSS. |
| 63: recommended. | 63 | 2.4.3.1 | David Bagby | T | deleted redundant para - already said a couple of paras above.<br>~~C/R exchanges are sufficient to support authentication from password based systems up through cryptographic authentication schemes.~~ *[DB8]*Details of the usage of cryptographic authentication schemes are outside the scope of this standard. | See imbeded comments and annotations |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | ***PROPOSED CHANGE*** | RATIONALE |
|---|---|---|---|---|---|---|
| 64: recommendation: no change - commenter is fine with this. | 64 | 2.4.3.1 | Fischer, Mike. | T | delete next-to-last paragraph, which conflicts with 6th paragraph | remove internal contradiction in manner compatible with following recommendations from MAC group at January, 1995 interim meeting (reported in 95/06) |
| recommendation: group discussion<br>commetors wants a better auth default than "open". | 65 | 2.4.3.1 | Jim Panian | **T** | A standardized authentication scheme, or set of schemes, must be specified. This does not preclude the use of non standardized authentication schemes, but allows any pair of 802.11 compliant stations to find a common scheme that can ensure interoperability.<br>For conformance, support for the standardized authentication scheme must be static (must be implemented). The actual use of the common authentication scheme may be dynamic (may not be used on every association). | How can interoperability be ensured if no common authentication scheme is defined ?<br>Let assume that the 802.11 standard standardizes an authentication scheme "A". Assume now that a first station X supports the schemes A, B and C and that a second station Y supports the schemes A and D. These stations will be able to use the common scheme A although they support other (proprietary) schemes. Another aspect that should be addressed by the standard is the protocol used by the stations to determine the set of commonly supported authentication schemes. |
| recommendation: decline as incorrect. arg given is only valid for specific auth algs - is not always true for all cases. | 79 | 2.4.3.1 | Renfro | T | Specify that Authentication is an Infrastructure service only. | If authentication is required for Ad Hoc networks, it becomes increasingly difficult as the size of the network grows. If a station must authenticate with every other station in the network it can take a considerable amount of bandwidth to accomplish this. If not, would a station accept either a broadcast message or beacon message from a station it has not authenticated? |
| recommendation - see 65 | 80 | 2.4.3.1 | Rick White | T | A default challenge / response exchange must be defined. | There is no authentication procedure defined in 802.11, only a service. The implementer can use any challege / response exchange. This leads to non-interoperability. |
| recommendation: decline the example altered is just that en example - the proposal is an improved PW scheme but the example in the section was intended to give a classic PW case (with all the attendant PW flaws of PWs) | 81 | 2.4.3.1 | Scaldeferri | T | A password based example:<br>c) Response: Here is my password ( suitably timestamped and hashed). | under "examples of C/R exchange": In a password passed system you would not respond to the challenge with your password in the clear, but would use your password plus some data in the challenge, e.g. timestamp, hashed using a suitably secure hash algorithm. Otherwise any promiscuous listener can obtain the users password and use it to become authenticated. |

| DISPOSITION | C# | SECTION | AUTH. | T/E | ***PROPOSED CHANGE*** | RATIONALE |
|---|---|---|---|---|---|---|
| recommendation: remove sentence (though for diff reasons that commetor gave - auth work incomplete at this time in 802.10) | 82 | 2.4.3.1 | Tim Phipps | T | *Remove*: "802.11 uses 802.10 services to perform the actual challenge and response calculations". | 802.10 Does not support authentication algorithms. |
| recommendation - group discussion, see rec 65 | 83 | 2.4.3.1 also relates to 2.5 | Wim Diepstraten | T | The standard should at least support an "Implicit authentication" mechanism, that does not require any Authentication frame exchange to be exchanged to establish a (re)-association. This should be the default mode of operation.<br>It is unclear why authentication support functions need to be included in the MAC.<br>It is unclear what the minimum authentication frame exchange is when the network wants to run without explicit authentication.<br>Figure 2-8 in section 2.5 should be changed to reflect this.<br>It is also unclear from section 2.4.3.2 which of the frames are in the clear, and which are encripted. It should be specified that only data frames will be encripted by the specified privacy algorithm, and all management and control frames should be transmitted in the clear. | Authentication is only relevant when also the privacy services are used. If Privacy services are used, then a specific Key needs to be distributed outside the MAC, and is assumed present within the MIB before a privacy protected mode can be entered.<br>If a station is able to send a frame with the proper encription key, then that is sufficient prove of a stations identity.<br>Beacons, Probes and Probe Responses should not be encripted without loss of functionality. There are no privacy holes created when Management frames are not encripted. |
| recommendation - group discussion, see rec 65 | 84 | 2.4.3.1.1 | Fischer, Mike. | T | add text to describe implicit authentification for use with WEP and allow this to serve as another form of pre-authentification (which will probably work better by adding a new section 2.4.3.1.2 Implicit Authentification) Ñ acceptable text appears in 95/15 | When operating with WEP, if we assume the existence of an acceptable key distribution scheme (which could be manual) and is certainly external to the 802.11 MAC, the posession of the correct ESS key is sufficient evidence of identity. Users who wish greater security can use a more complete 802.10 SDE implementation above the MAC, in which case the 802.10 Òsecurity associationÓ is where the more comprehensive authentication takes place. This is consistent with the recommendations from the MAC meeting in January, 1995 (reported in 95/06) |
| recommendation: decline. there are no pre-auth frames. the section describes a time when Auth can be done which would achieve pre-auth, but no explicit different frame type is required. | 85 | 2.4.3.1.1 | P. Brenner | T | Add Definitions of the Pre-Authentication frames (or delete this section) | Pre-authentication is not being supported by the current set of management frames. |

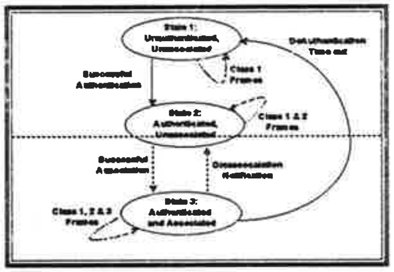
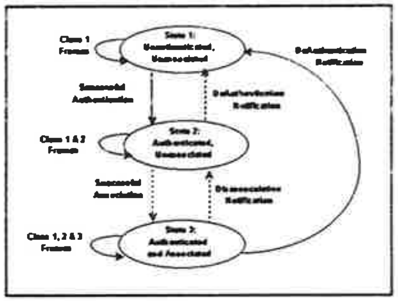
| DISPOSITION | C# | SECTION | AUTH. | T/ E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| recommendation: disc required, maybe possible to simplify internal structure of auth msg - tbd. | 86 | 2.4.3.1; also 2.7.6 | Fischer, Mike. | T | Remove most of the multiÐway (>2) challenge/response stuff. Unless we build specific algorithms more complex than appropriate for WEP into the authentication service, the cryptographic challange style of authentification, if a user wants this, will be done by an 802.10 implementation sitting above the MAC (or a nonÐ802.10 security service sitting above the MAC). There is no reason to provide a service path for an SDE above the MAC to use MAC mechanisms to exchange the authentication messages, as 802.10 is designed to work on top of any MAC, so letÕs save the complexity and just deal with WEPÐappropriate mechanisms in the MAC. The basic concepts of the simpler approach is that message 1 is implicit due to the limited algorithm list within any given version of the 802.11 MAC and message 2 is implicit because authentication is always initiated (as is association) by the nonÐAP station, so the identity of the AP (e.g. the network) is not in question. Therefore, by the time of an associate request, the STA believes the network identity to be valid and the station can include its assertion of identity in the associate or reassociate request (piggybacking message 3) and the AP can do the same with message 4 in the associate/reassociate response. At most we need a pair of messages (which could be the authenticate request/response, which still only needs one frame type because the request is always ToDS=1 and the response is always FromDS=1) to handle preÐauthentication in an ESS that used different of the algorithms for authentication and privacy. Detailed wording changes appear in 95/15. | see column to the left. |
| recommendation: no change requested - none recommended. comment appears to be incorrect. | 87 | 2.4.3.2 | CHRIS ZEGELIN | | INCONSISTENT: TALKS ABOUT ALL STATIONS STARTING "IN THE CLEAR". THIS IS NOT THE WAY THE CURRENT STATEMENTS ABOUT AUTHENTICATION ALLOW ACCESS TO THE DS TO OCCUR. | |
| recommendation: change “would” to “may” | 88 | 2.4.3.2 | C. Heide | T | second paragraph, last sentence replace the word "would" with the word "could". | it is subjective as to whether or not a wireless segment degrades security if the WM is limited range. |

| DISPOSITION | C# | SECTION | AUTH. | T/<br>E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| recommendation: decline 1st suggestion is covered by rec 88.<br>2nd suggested change declined - the intent is not to provide "perception of security". | 89 | 2.4.3.2 | C. Thomas Baumgartner | t | Change the 2nd paragraph to "In a wired LAN one normally assumes that only those stations physically connected to the wire can hear LAN traffic. This assumption give the perception of privacy. With a wireless shared medium one knows that any compliant adapter can hear all 802.11 traffic in its range. Thus the connection of a single wireless link (without privacy) to an existing wired LAN could degrade the security of the wired LAN."<br>Change sentence in last paragraph to "The algorithm is not designed for ultimate security, but rather to give the perception of security "at least as secure as wire."" | These sentences as written contain editorial comment which is trying to scare the public. They are not technically correct in assuming that wired LAN's are private. NIC's can be doctored to be any MAC address; a Sniffer can hear everything that goes over the cable, there is enough stray energy from 10BASE-T that a good receiver can pick it up outside the physical confines. Anyone truly worried about this subject has taken steps at higher layers of the network, even on a wired network. The ability to confine IR to an area, giving the same physical access control as wire, makes this paragraph inappropriate for at least one of the 802.11 PHY's. I dare say there are more people with the ability to tap wired LANs than there are who will be able to intercept DSSS. |
| rec: part of rec 90 adoption. | 91 | 2.4.3.2 | David Bagby | T | **1. *Deauthentication***<br>***Deauthentication**: The service which voids an existing Authentication.*<br>*The Deauthentication Service is invoked whenever an existing Authentication must be terminated. Deauthentication is a Station Service.*<br>*in an ESS, since Authentication is a prerequisite for Association, the act of Deauthentication can cause and explicit* Disassociation.<br>*The Deauthentication Service can be invoked by either authenticated party (mobile STA or AP). Deauthentication is not a request, it is a notification. Deauthentication can not be refused by either party.*<br>*[DB9]* | See imbeded comments and annotations |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| rec: discussion required by group. | 92 | 2.4.3.2 | Geiger | T | Privacy. 802.11 specifies an ~~optional~~ privacy algorithm | Options in standards are useless. Either everyone will implement it or no one will. Privacy is a feature that should be required not optionally implemented. If you want to set up a WLAN without privacy, fine, but the user, not the station implementor should make that decision. One of the bigger issues of security that this standard doesn't completely address is how do parties using a LAN know if one or more segments in the LAN are wireless and secure. I believe that the standards process put some liability on the people involved to do the responsible thing in terms of providing the same protection to the wireless user as the wired user. Car manufacturers are required to equip vehicles with seat belts, regardless of whether the users of the vehicle wear them or not. I feel security is the same type of issue. |
| **rec: group disc required.** | **93** | **2.4.3.2** | **Siep** | **T** | *Encipherment*~~**Privacy**~~ 802.11 uses IEEE 802.10 SDE clause 2 to perform the actual encryption of messages.~~A MIB function is provided to inquire the encryption algorithms supported by a station.~~ *The MAC header specifies a bit in the FC field which indicates if the MDSU in the data frame is encripted. Only data frames are optionally encrypted. Management and control frames are not encrypted.*<br>*802.10 SDE settings*<br>• *clear header length =0*<br>• *protected header length =0*<br>• *pad =none*<br>• *ICV =32 bits, [algorithm MUST be specified]*<br>*The encipherment model assumes a default, ESS–wide key to permit implict authentification.*<br>• *Any station in possession of the default key is considered pre–authentificated (e.g. in State 2 of figure 2–8 of the D1 draft)*<br>• *This is fully compatible with the 802.10 concept of receivers having tables that associate keys with station addresses. The default key is used in cases where there is no table entry for the sender's address.*<br>*More comprehensive security, or different algorithms, can be directly applied by users that want to provide a full 802.10 implementation above the 802.11 MAC.* | **This reflects the discussions on Encipherment held in the January MAC meeting in San Jose. This is a reasonable default set of security features. If a given installation desires more security, it can implement additional 802.10 layers transparently above the MAC.** |

| DISPOSITION | C# | SECTION | AUTH. | T/E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| rec: see rec 92 - same subject | 94 | 2.4.3.2, 5.4 | Jim Panian | T | For conformance, support for the WEP privacy algorithm (or other standardized privacy algorithm) must be static (must be implemented). The actual use of the WEP privacy scheme may be dynamic (may not be used on every association). | Why isn't a standard privacy algorithm specified? The lack of a standard specified privacy algorithm will hinder interoperability. |
| rec: decline - ok with commetor. | 95 | 2.4.3.2, 2nd paragraph | Fischer, Mike. | T | change 3rd & 4th sentences to ÒAny 802.11 conformant station adapter can receive any 802.11 frames transmitted (on the same channel) within the wireless reception range of its PHY receiver, whether or not the sender is in the same BSS or ESS. Thus the integration of a single wireless link (without privacy) to an existing, wired LAN will seriously compromise the security level of the wired LAN. | grammar, terminology, greater technical correctness |
| rec: see 92 | 96 | 2.4.3.2, 3rd from last paragraph | Fischer, Mike. | T | change Òin the clearÓ to ÒWEP as defined in section 5.4.Ó | The default should be WEP because the whole concept of ÒwiredÐequivalentÓ is to provide as close an approximation to what users of wired LANs expect as we can with practical methods. This is done not just for security but also for the link itself (MACÐlayer acknowledgements to partially compensate for the lower link reliability). The default for a wire is ÒprivateÓ unless somebody physically gains access to the cable. The equivalent for 802.11 is to default to WEP. (Of course, if somebody chose to make their network key a simple constant such as all zeros, and never change the IV, they might as well be sending in the clear.) |
| rec: group disc re security | 97 | 2.4.3.3 | Rick White | T | Must identify if the "default privacy algorithm" is executed by the MAC or 802.10. | Section 5.4 does not specify if WEP is part of the MAC |
| rec: group disc re security | 98 | 2.4.3.3 | Rick White | T | 802.11 must provide a privacy algorithm that does not require 802.10 for implementation. It could well be the WEP algorithm. | Customers will require privacy on their WLANs. They will not what to be required to used another standard to implement it. |
| rec: decline - this is major change of the draft insufficiently justified by the brief comment supplied. can not determine detailed action desired from this comment. | 99 | 2.5 | CHRIS ZEGELIN |  | THE WHOLE RELATIONSHIP BETWEEN ASSOCIATION AND AUTHENTICATION IS WRONG OR AT THE VERY LEAST CONFUSING. THIS IS COMPOUNDED WHEN THE CLASS OF LEGAL FRAMES FOR VARIOUS STATES IS REVIEWED. | THERE IS AN IMPLICATION THAT AUTHENTICATION AND OR ASSOCIATION STATUS MUST BE CHECKED ON A DATA FRAME FROM A STA BEFORE THE FRAME IS ACK'ED. |
| rec: partial change - move Poll (really power save poll) to class 3, other msgs are correct as stated | 100 | 2.5 | A. Bolea | T |  | Why allow an Unauthenticated, Unassociated station to transmit/receive RTS,CTS or Poll Messages? RTS/CTS should only be allowed for class 2, 3 stations. Poll messages should only be allowed for class 3 stations. |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| rec: covered by 90 | 101 | 2.5 | Bob O'Hara | T | The state diagram and related text do not provide for explicit "de-authentication" by a station sending a message. This must be provided. | The protocol does not allow for dynamic changes in authentication requirements. |
| rec: covered by 90 | 102 | 2.5 | C. Heide | T | on figure 2-8 change "DeAuthentication Time out" to "DeAuthentication" only. | there is no description of any kind of time out on authentication anywhere |
| rec: covered by 90 | 103 | 2.5 | C. Heide | T | on figure 2-8 remove direct path from State 3 to State 1; or define de-authentication and the method of accomplishing it. | There is no definition of, or reference to, deauthentication anywhere else but this figure. |
| rec: covered by 90 | 104 | 2.5 | C. Heide | T | Class 2, (a) should be:<br>"a) Asynchronous Data frames:<br>1) subtype Data, with FC control bits "To DS" and "From DS" both false.<br>Class 3, a) should be<br>a) Asynchronous Data frames:<br>All subtypes, FC control bits "To DS" and "From DS" may be set to utilize DS Services.<br>Class 3, b) should have added to it<br>3) Connection subtypes: Connection Request, Grant Connection, and End Connection<br>Class 3, c) should be removed. | the frames in this section do not jive with the types/subtypes listed in table 4-1. |
| rec: part of 90 | 105 | 2.5 | David Bagby | T | State 1:<br>Initial start state, Unauthenticated, Unassociated.<br>State 2:<br>Authenticated, not Associated<br>State 3:<br>*[DB10]*Authenticated and Associated. | See imbeded comments and annotations |

| DISPOSITION | C# | SECTION | AUTH. | T/<br>E | PROPOSED CHANGE | RATIONALE |
|---|---|---|---|---|---|---|
| recommendation: accept set of changes that support the missing transition. this includes supporting change in sec 4 also. | 90 | 2.5 | David Bagby | T | The state diagram needs to be corrected. It was noted at the Nov 94 mtg that there is an error in that there is not way to transition back from state 2 to state 1 (except via state 3 which is impossible in an IBSS network).<br>To solve this I have added the missing sate transition. Since the act of de-authentication is analogous to disassociation and is done for similar reasons, a message to notify the other station of the event also had to be added to section 4. The previous time out condition can still occur (so that authentication can be aged) and will now result in the de-authentication notification.<br>The set of changes which accomplish this correction are annotated as "deauthentication".<br><br> State 1: Unauthenticated, Unassociated<br>DeAuthentication Time out<br>Successful Authentication<br>Class 1 Frames<br>State 2: Authenticated, Unassociated<br>Class 1 & 2 Frames<br>Successful Association<br>Disassociation Notification<br>Class 1, 2 & 3 Frames<br>State 3: Authenticated and Associated<br><br> Class 1 Frames<br>State 1: Unauthenticated, Unassociated<br>DeAuthentication Notification<br>Successful Authentication<br>DeAuthentication Notification<br>Class 1 & 2 Frames<br>State 2: Authenticated, Unassociated<br>Successful Association<br>Disassociation Notification<br>Class 1, 2 & 3 Frames<br>State 3: Authenticated and Associated<br>*[DB11]***Figure 2-8: Relationship Between State Variables and Services** | See imbeded comments and annotations |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| rec: part of 90 | 106 | 2.5 | David Bagby | T | Class 1 frames (Legal from within States 1, 2 and 3):<br>a) Control Frames:<br>1) RTS<br>2) CTS<br>3) ACK<br>4) Poll<br>b) Management Frames:<br>1) Probe Request/Response<br>2) Beacon<br>3) Authentication<br>Successful Authentication enables a station to exchange Class 2 frames.<br>Unsuccessful Authentication leaves the Station in State 1.<br>Class 2 frames (IFF Authenticated; allowed from within States 2 and 3 only):<br>a) Data frames:<br>1) Asynchronous data<br>Direct data frames only (FC control bits "To DS and From DS" both false).<br>b) Management frames:<br>1) Privacy Request/Response<br>2) ATIM<br>3) Association R/R<br>Successful Association enables Class 3 frames.<br>Unsuccessful Association leaves STA in state 2.<br>*4) Deauthentication[DB12]*<br>Class 3 frames (IFF Associated; allowed only from within State 3):<br>a) Data frames:<br>1) Asynchronous Data<br>Indirect Data frames allowed. I.e. the "To Ds" and "From DS" FC control bits may be set to utilize DS Services.<br>b) Management frames:<br>1) Reassociation Request/Response<br>2) Disassociation<br>Disassociation notification changes a Stations state from 3 to 2. Thus a Station must become Associated again if it wishes to utilize the DS.<br>*3) Deauthentication[DB13]*<br>c) CF Data frames:<br>1) CF DATA<br>2) CF DATA + ACK<br>d) CF Control frames:<br>1) CF END<br>*[DB14]* | See imbeded comments and annotations |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | ***PROPOSED CHANGE*** | RATIONALE |
|---|---|---|---|---|---|---|
| rec: decline, perhaps text is better placed elsewhere (editor's job), but figure requires text for completion of specification. | 107 | 2.5 | Greg Ennis | T | Remove all references to frame "classes", and end the section after the figure. | If this is supposed to be an overview section, the discussion of individual frame types is confusing, as they have not been previously described. |
| rec: decline, because req/grant are not fame types. | 108 | 2.5 | Joe Kubler | T | add req and grant request frames to Class 3 frames allowed | completeness |
| rec: editorial - add IFF to abbreviation section - means if an only if | 109 | 2.5 | Lewis | T | clarify what IFF Authenticated means | |
| rec: fixed as part of 90 | 110 | 2.5 | Rick White | T | Class 3 CF Data Frames should be Asynchronous Data frames & CF Control frames should be Control Frames | We should be consistent with terms defined in Section 4. |
| rec: fixed as part of 90 | 111 | 2.5 | Rick White | T | Must define the Deauthentication time-out. | Not defined. |
| rec: fixed by 90 | 112 | 2.5, figure 2Ð8 | Fischer, Mike. | T | Add transition from state 2 to state 1, labelled Òassociation failure timeoutÓ | There needs to be a transition from state 2 to state 1, since association will not always be successful even after state 2 is entered. This transition occurs when an association request is rejected with a denial code, or when attempts to associate are ungranted and undenied for a defined period of time. |
| rec: adopt clarity change | 113 | 2.5, under Class 1, Class 2, and Class 3 | Fischer, Mike. | T | Add words to make it clear that the list is for frames legal to send when in these states. At the top of the page add a sentence to the effect that ÒStations in a given state are allowed to send the types of frames in equal or lower numbered classes. However, since a station cannot be relied upon to operate in the intended fashion (otherwise authentication would not be necessary), it is the responsibility of the receiving station to only accept class 2 and class 3 frames from stations known to be in an acceptable authentication state.Ó | clarify the intent of this classification of frames and explain that this is a policy that is imposed on the senders but can only be enforced at the receivers |
| rec: fixed sufficiently by 90 says commenter. | 114 | 2.5, under class 3 | Fischer, Mike. | T | Simplify this by stating that all frame types are permitted in Class 3. This avoids the need to update the list (which is badly out of date, expecially for CF frames). | simplicity while retaining current functional intent |
| rec: this is what sec 2.6 is, also defs in sec 1, no additional change required (we think) | 115 | 2.6 | Glen Sherwoo d | T | Add text to define IBSS's and ad-hoc networks. | Independent BSS (IBSS) or "Ad-hoc" networks are not well defined. |
| rec; no text change needed (further clarified in earlier recs). An IBSS has no AP - a BSS can. see rec 14 | 116 | 2.6 | Rick White | T | It is not clear whether an Independent BSS can contain an AP. Must be clarified. | It states that there is no physical DS but does not indicate whether there can be a logical DS which would be part of an AP. |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| see rec 15 | 117 | 2.6 | Rick White | T | Must clarify the communications within an IBSS. | Must all STAs in an Independent BSS be able to communicate with all other STAs in the Independent BSS? If so, how does it know what STAs are part of the IBSS. |
| rec: adopt - also see rec 16. | 118 | 2.6 | Rick White | T | Paragraph 4: There can be DS Services without a physical DS if there is an AP with a logic DS. | |
| rec: decline, the info in 2.7 is needed, perhaps it could be incorporated into other sections without info loss, but it can not be simply removed. sec 2.7 describes info to support service, but is not the specification of specific frame formats. | 119 | 2.7 | CHRIS ZEGELIN | | REMOVE ENTIRE SECTION 2.7 | FRAME FORMATS ARE DESCRIBED IN SECTION 4. |
| rec: adopt | 120 | 2.7 | David Bagby | T | ~~***[eds: this section may need minor tweaking in light of the Nov 94 mtg frame formats and element language adopted.***~~<br>*[DB15]*Information items are given by name, for corresponding values, see section 4.<br>~~***[eds: update section number]***~~<br>*[DB16]* | See imbeded comments and annotations |
| rec: no change requested, none made. comments indicate some misunderstanding, will talk to author to clarify. | 123 | 2.7 | Gegier | T | | In general, the Distributed System Services is build around a set of entities that must exists for the services to be available. These entities include APs, BSSs, ESSs and possibly Portals as well. At the lowest level, a station gets these services through an AP. Unfortunately, stations may enter a BSS with an AP but not have access to the AP because of medium constraints. Further more, that station may not need access to the AP but only an in-range STA. Privacy and Authentication should be allowed between STA1 and STA2 even if STA2 is not an AP but is associated with an AP. |
| rec: see rec 119 | 121 | 2.7 | Greg Ennis | T | Move this material into sections 5 and 7 | This is too detailed for an overview and must be covered in exact detail in the later sections. |

| DISPOSITION | C# | SECTION | AUTH. | T/E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| rec: see rec 119 | 122 | 2.7 | Marvin Sojka | T | Remove Section 2.7. It gives the impression of contents that is better expained in later sections | |
| rec: decline to add. insufficient justification for a new general mechanism given by the comment. group discussion required? | 124 | 2.7 | P. Brenner | T | Add a general Query-Request message, and a corresponding Query-Response. | A general mechanism for exchanging management information is required |
| rec: adopt - see 120 | 125 | 2.7 | Rick White | T | Resolve editor's comment relating to Management frame formats | |
| rec: refer to sec 4 for addition, prob in 4.2.1.3 as part of "to DS" bit discussion. | 126 | 2.7.1 | Fischer, Mike. | T | Add sentence after opening sentence of section ÒDirect stationÐtoÐstation transmission is allowed when the sending station knows that the intended (unicast) recipient is associated in the same BSS. However, for intraÐBSS communication that is transparent to BSSÐtransition mobility, as well as all interÐBSS (intraÐESS) communication, the sender invokes distribution service.Ó<br>also, delete the Òif the message ...Ó under Òinformation itemsÓ since all data frames now include the BSSID | consistency, correct recitation of when STAÐtoÐSTA transfers are usable and when they are not |
| rec: adopt - this is a correction. | 127 | 2.7.1 | Joe Kubler | T | BSS ID is always required, even in AD HOC. remove "iif" qualification. a comment about the fourth address in WDS data frames would be useful as well such as: In the case of WDS services, a fourth address field is included. The addresses then are receiver address, transmitter address, destination address and source address. | see table 4-4 |
| rec: see 127 | 128 | 2.7.1 | Lewis | T | BSSID should always be included | |
| rec: decline, change not needed.<br>the set is identified by the category, the individual frames are in sec 4. | 129 | 2.7.1 | Rick White | T | There are several different types of Asynchronous Data frames - All must be shown. | Standard incomplete |
| rec: see 127 | 130 | 2.7.1 | Rick White | T | Info items should include the fourth address for Wireless Distribution. | |
| rec: correct by removing parenthetical, STA to STA covers all cases | 131 | 2.7.1 | Rick White | T | Direction could also be AP to AP. | This is true for wireless distribution. |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | ***PROPOSED CHANGE*** | RATIONALE |
|---|---|---|---|---|---|---|
| rec: security interest discussion | 132 | 2.7.2 | Tim Phipps | T | *Incomplete.*<br>*The privacy algorithm number is just one of the 802.10 SMIB variables required to achieve a security association.* | Just providing a privacy algorithm number makes the assumption that the other 802.10 SMIB variables (e.g. the block size, the presence of a clear header) can be inferred from the algorithm number. This is a more restricted form of behaviour than 802.10 describes. It may limit future support for algorithms which require more of the SMIB to be exchanged to achieve a security association. |
| rec: add ESSID as it is required for assoc support (which is what this section is about), the others are referred to sec 4 discussion as there is insufficient justification for each item supplied in the comment. | 133 | 2.7.2<br>2.7.3 | Wim Diepstraten | T | More information is needed in the Association Request and Response frames. The following elements should be added to the Association Request:<br>- ESSID<br>- Rate Capability<br>- CF_Aware indication<br>- PM_mode<br>- Aging_Time (for PSP stations)<br>The Association response should contain additionally to the list in section 2.7.2:<br>- Rate capability<br>- Possibly the ESSID<br>In addition the Reassociation frame should contain the Privacy Number, because it also part of the Association Request.<br>The following elements do also need to be part of the Beacon:<br>- SF_Length<br>- CF_Boundary<br>A number of the listed elements need to be defined in section 4.4, because they are currently undefined. | There are a lot of inconsistencies between section 2.7.2 and 2.7.3 and other sections of the standard. The additional elements listed are considered to be required at association time so that a station can properly operate in the BSS it is associated with.<br>It is benificial for an AP to know which PM mode is being used by the station. In particular it is usefull to know which station will utilize the CAM mode (static non power conservation), and which stations are using one of the power saving modes (including the TAM).<br>The SID assignment would only be needed for power saving stations, and more in particularthe PSP mode. |
| rec: decline - see rec 54 | 134 | 2.7.3 | Renfro | T | Remove Reassociation | Reassociation is not necessary. The same thing can easily be accomplished using the existing association message. Though I think it is better to implement mobility without relying upon information about the current AP, it is still possible to include that information in the association message using the current AP element. |
| rec: change “enables” to “facilitates”. | 135 | 2.7.3, sentence just above ÒReassociation ResponseÓ | Fischer, Mike. | T | add appropriate text from 95/17 to the various 2.7.x sections, in this case making the reference sentence meaningful | This statement is true in a very narrow sense that is essentially useless in the absence of defined message formats for delivery Òindependent of DS implementation.Ó |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| rec: remain open until alg number known. also group disc of security stuff required. | 136 | 2.7.5 | David Bagby | T | **No Privacy Algorithm in use:** Value = ??<br>**Wired Equivalent Privacy (WEP) algorithm**: Value = ??<br>draft can not go to sponsor ballot until these values are received from 802.10 since the standard can not be implemented without these values.<br>*[DB17]**~~Eds: Fill in these values when received from 802.10 registration authority.~~**[DB18]*<br>A rework of the privacy sections to make the explicit use of 802.10 unnecessary by making the default behavior of 802.11 to be a compatible subset of 802.10 would be a nice improvement. The details need to be worked out but the approach discussed during the Jan MAC 95 mtg sounds like a very good approach. This reviewer would consider those changes in place of or in addition to the comments provided. Those changes could impact the applicability of the comments made above. [DB19]<br>This satisfies the minimal operational needs of 802.11.<br>Additional privacy algorithms, which have been registered with 802.10 for use within 802.11 implementations, and were known at the time of publication are contained in appendix XX.<br>appendix missing - create and put in it the two initial values referenced above.<br>*[DB20]***2.Authentication** | See imbeded comments and annotations |
| rec:; group disc needed. | 137 | 2.7.5 | Fischer, Mike. | T | The privacy request/response is unnecessary as a MAC management exchange. The MAC privacy (WEP) has a single or very small set of available algorithms, which can be handled as fields in the association request and response frames and/or obviated by inclusion of the BSSÕs algorithm in the beacon frames. Specific text in document 95/15. | simplicity and conservation of mechanism N leave negotiated, arbitraryÐalgorithm privacy to a full 802.10 implementation above the MAC for customers who want this degree of security. |
| see rec 136 | 138 | 2.7.5 | Geiger | T | **No Privacy Algorithm in use: Value ??**<br>**(WEP) algorithm: Value = ??**<br>appendix XX | Resolve |

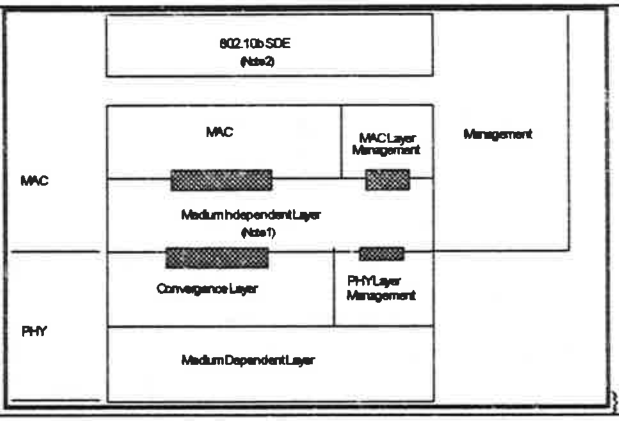
| DISPOSITION | C# | SECTION | AUTH. | T/ E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| rec: no change needed, add reference top sec 5.4 | 139 | 2.7.5 | Glen Sherwood | T | Define WEP algorithm. | Undefined WEP algorithm. |
| rec: see 136 | 140 | 2.7.5 | Jon Rosdahl | T | No Privacy Algorithm in use: Value = ??<br>Wired Equivalent Privacy (WEP) algorithm: Value = ?? | The values need to be determined and added. I am unable to determine or assign these values. |
| rec: see 136 | 141 | 2.7.5 | Mahany | T | Privacy Response<br>Add 802.10 Algorithm Numbers for No Privacy Algorithm, and WEP,<br>Add Correct Appendix reference for Appendix X | Completeness |
| rec: see 136 | 142 | 2.7.5 | Mark Demange | t | Value = ?? needs to be defined for both "No privacy Algorithm in use:" and "Wired Equivalent Privacy (WEP) algorithm:" | Undefined values for necessary variable is inappropriate for a standard. |
| **rec: security group discussion needed** | **145** | **2.7.5** | **Siep** | **T** | Pirvacy*[SUBSTITUE TEXT]*<br>*The MAC header specifies a bit in the FC field which indicates if the MDSU in the data frame is encripted.*<br>—OR—<br>*[Delete section]* | **The first option reflects the discussions on Encipherment held in the January MAC meeting in San Jose. This is a reasonable default set of security features. If a given installation desires more security, it can implement additional 802.10 layers transparently above the MAC.**<br>**The second option (deletion) conflicts with section 2.8** |
| rec: see 136 | 143 | 2.7.5 | Tim Phipps | T | *Incomplete.*<br>*802.10 requires privacy and integrity algorithm numbers. It may require the exchange of additional SMIB parameters to achieve a security association by which to provide privacy. These message types, and frame formats and element types described here and elsewhere provide only partial support for the exchange of 802.10 SMIB variables.* | 802.10 Supports privacy and integrity. Both require a number of managed objects within the security management information base (SMIB). |
| rec: see 136 | 144 | 2.7.5. | Fischerma:Privacy | T | must come from 802.10 | 802.10 algorithm numbers for privacy not specified. |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | ***PROPOSED CHANGE*** | RATIONALE |
|---|---|---|---|---|---|---|
| rec: security group discussion needed - must remain open until auth alg specified and number provided or default auth details worked out an accepted. | 146 | 2.7.6 | David Bagby | T | Note: 802.10 does not specify specific cryptographic algorithms for authentication or privacy. However the algorithm numbers must be known for proper operation of 802.11. P802.11 has registered the following algorithms with 802.10:<br>**No Authentication algorithm in use:** Value = ??<br>need value from 802.10 - can not go to sponsor ballot until value received since can not implement the standard without this value.<br>*[DB21]**~~Eds: Fill in this value when received from 802.10 registration authority.~~**[DB22]*<br>An authentication scheme must be specified to complement the use of the WEP privacy feature. It does not good to implement the optional privacy with out the ability to authenticate the end nodes of the secured link. A default of "no authentication" must also be specified to match the default situation of "no privacy". Further an explicit sentence must be added that it is not required that an implementation must accept unauthenticated and unencrypted frames. Even though a STA must be *capable* of understanding unsecured communication frames, it is not required that any particular STA be required to convers in the open. It must be possible for any station to decide that it will only communicate with other secure stations. The WEP compliment authentication shceme is open for discussion, but it sounded at the Jan 95 MAC mtg taht something along the lines of that suggestedby Kerry Lynn would be acceptable to the group.*[DB23]*<br>This satisfies the minimal operational needs of 802.11.<br>Additional authentication algorithms which have been registered with 802.10 for use within 802.11 implementations and were known at the time of publication are contained in appendix XX.<br>referenced appendix is missing - create and put in initial minimum value referenced in this section.<br>*[DB24]* | See imbeded comments and annotations |
| rec: see 146 | 147 | 2.7.6 | Geiger | T | **No Authenticaticn algorithm in use: Value = ??**<br>appendix XX | Resolve |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| rec: see 146 | 148 | 2.7.6 | Jon Rosdahl | T | No Authentication Algorighm in use: Value = ?? | The values need to be determined and added. I am unable to determine or assign these values. |
| rec: see 146 | 149 | 2.7.6 | Mark Demange | t | Value = ?? needs to be defined for "No authentication in use:" | Undefined values for necessary variable is inappropriate for a standard. |
| rec: see 146 re auth details, also portions of comment improved by rec 90. | 150 | 2.7.6 | Renfro | T | | Authentication in Ad Hoc network not well defined and should be deleted. Must each station authenticate with every other station? (Results in a lot of messages for even a small network) Will a station accept a broadcast/multicast message from another station it has not authenticated? If included, need to clearly define authentication procedures for both Ad Hoc and Infrastructure networks. If authentication is optional, as implied in 2.4.3.1, how is compatibility between stations implementing this option and those not ensured? |
| rec: see 146 | 151 | 2.7.6 | Rick White | T | Must define Authentication transaction sequence number. | Is the Authentication transaction sequence number the same as the Authentication message number? |
| **rec: author withdraws objection after discussion.** | **152** | **2.7.6** | **Siep** | **T** | Authentication*[Delete section]* | **Conflicts with section 2.8** |
| rec: see 146 | 153 | 2.7.6 | Simon Black | T | Authentication procedure and algorithm required for interworking. Currently missing from the standard. | Authentication is essentially undefined in this standard. IEEE 802.10 authentication is mentioned in several places, but .10 does not provide this fuinctionality. |
| rec: see 146 | 154 | 2.7.6 | Tim Phipps | T | *Delete:* "Additional authentication algorithms ... appendex XX". | Authentication algorithms cannot be registered with 802.10, only privacy and integrity algorithms. |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| rec: adopt - part of rec 90 | 155 | 2.7.7 | David Bagby | T | **3. *Deauthentication***<br>*When a STA wishes to cancel an active authentication, the following message is sent.*<br>***Deauthentication***<br>*Message type:*<br>*Management*<br>*Message sub-type:*<br>*Deauthentication*<br>*Information Items:*<br>*IEEE address of the station which is being deauthenticated.*<br>*IEEE address of the AP which the Station is currently authenticated with.*<br>*Direction of message:*<br>*From STA to STA (e.g. STA to AP or AP to STA).*<br>*[DB25]* | See imbeded comments and annotations |
| rec: ability already provided, no cange needed, if intent is for requirement, then this is already under discussion as result of other comments. | 157 | 2.8 | McDonald | t | Provide security or privacy to the text of the mpdu | An 802.11 link may be an extension of a wired system. As such, the user would expect the wireless extension to provide the same level of privacy as the wired link. Clear text RF won't come close to meeting this need. If an 802.11 unit with simple modifications, for instance could be mounted outside the boundary of an operational 802.11 BSS and be used to eavesdrop, then the 802.11 standard will fail. The text being transferred must be protected at the 802.11 level. Higher level privacy is not good enough. This would require a user to change his network/operating/applications program to use the wireless extension |

| DISPOSITION | C# | SECTION | AUTH. | T/<br>E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| rec: treat as input for security group discussion. text APPLIES TO 3.1.1.3 | 158 | 2.8 and 3.1.1.3 | Fischer, Mike. | T | Add the following regarding 802.10 subset:<br>The use of the 802.10 subset for privacy is optional. If privacy (WEP) is in use, that fact is indicated by a bit in the frame header. When this bit is set, the algorithm number, from the list of (initially 1) algorithm(s) supported by 802.11 for WEP, is indicated as part of the IV (see section 5.4).<br><br>Privacy only applies to the MSDU, not to the MAC header nor CRC. When MSDUs are fragmented, the privacy algorithm is applied to the MSDU before fragmentation, and validated on the MSDU after reassembly. When privacy is in use, data frames are always encrypted, control frames are never encrypted, and management frames are never encrypted other than as needed for authentication. If the ICV of an encrypted data frame does not check, the existence of the MSDU shall not be indicated to the LLC at the receiving station, and the contents of the MSDU shall not be passed to the LLC.<br><br>The 802.10 SDE settings for 802.11 WEP shall be: clear header length = 0, protected header length = 0, pad = none, and ICV = 32 bits. The data field shall include a 32Ðbit IV field immediately preceding the MSDU. This field shall contain an 8Ðbit privacy algorithm number followed by a 24Ðbit initialization vector value. The length of the IV field is never less than 32 bits. If the designated algorithm requires an IV longer than 24 bits, a longer IV field may be used, subject to the restriction that the IV must always contain an even number of octets.<br><br>There shall be an ESSÐwide, default key to permit implict authentification and lowÐoverhead mobility transitions. Any station in possession of the default key is considered to be preÐauthenticated. Stations may, optionally, maintain receive privacy tables that associate stationÐspecific, nonÐdefault keys with station addresses. The default key is used in cases where this table not used and where the table has no station specific key corresponding to the source address of the received MSDU.<br><br>The 802.10 SDE mechanism allows for more than one SDE entity to be operating in the same protocol stack. If a user chooses to deploy an SDE environment that requires SDE settings more comprehensive than those in the WEP subset, and/or based on an encryption algorithm not supported for the WEP function, that user may disable the WEP function, thereby avoiding the overhead of performing encryption and security processing twice on the same MSDU. This is consistent with the 802.10 model, in which lowerÐlayer SDE entities are generally disabled when higherÐlayer SDE entities are present.<br><br>Replace figure 3Ð1 with one that shows the 802.10 subset listed above rather than the full generality of the 802.10 SDE_PDU. Replace the text after the first paragraph of 3.1.1.3 with a reference to 802.10 and its use above the MAC in cases where security functions beyond WEP are desired by a user of 802.11. | This embodies the recommendations made at the MAC group meeting on WEP held during the January, 1995 Interim Meeting. (The minutes of that meeting are document 95/06.) |

| DISPOSITION | C# | SECTION | AUTH. | T/<br>E | ***PROPOSED CHANGE*** | RATIONALE |
|---|---|---|---|---|---|---|
| rec: Joint group discussion required of full 802.11. | 159 | 2.9 | Dean Kawaguchi | E |   802.10b SDE<br>(Note2)<br>MAC<br>MAC Layer Management<br>Management<br>MAC<br>Medium Independent Layer<br>(Note1)<br>Convergence Layer<br>PHY Layer Management<br>PHY<br>Medium Dependent Layer | MAC layer management entity sends PLME service primitives to the PHY layer management entity. |
| | | | | | | |
| rec: ask author to provide picture to match draft text. | 161 | 2.9 | Bob O'Hara | T | Figure 2-11 does not represent the content of the current draft and must be redrawn | Out of date/sync with rest of document |
| rec: adopt to make document internally consistent - if picture later changed then alter agin if necessary. | 162 | 2.9 | David Bagby | T | **Figure 2-11, Portion of the ISO Basic Reference Model Covered in this Standard**<br>~~Note 1 – Optional exposed DTE/DCE interface~~<br>802.11 has decided that there is no exposed interface between the mac and phy layers thus the picture is incorrect. Edit the picture to remove the interface block at that point. Then renumber notes accordingly for the picture.<br>Note 2 - 802.10 SDE: IEEE 802.10 - Secure Data Exchange [2]<br>*[DB26]*~~***(Insert general overview of the 802.11 MAC and PHY Layers)***~~*[DB27]* | See imbeded comments and annotations |
| rec: see 162 | 163 | 2.9 | Geiger | T | ~~Note 1 – Optional exposed DTE/DCE Interface~~ | This is not an option. There is reference to exposed interfaces anywhere, we voted in the PHY group not to do this, remove this reference. |
| rec: see 162 | 164 | 2.9 | Lewis | T | delete reference to optional DTE/DCE interface or add the specification of such to<br>the draft standard | |

| DISPOSITION | C# | SECTION | AUTH. | T/E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| REC: SEE 162 | 165 | 2.9 | N. Silberman | T | Re:”Note1-Optional exposed DTE/ DCE interface” | If there is an exposed DTE/DCE interface it should be defined and specified. The use of it should be optional. When implemented, it should meet specifications defined in the standard.<br>There is no good way to test certain PHY parameters specified in the standard without an exposed interface.(e.g BER, receiver sensitivity, etc.) |
| REC: GROUP discussion | 166 | 2.9 | Rick White | T | Resolve Editor's comment to provide general overview of MAC & PHY. | This would be a greathelp in the understanding of the standard. |
| REC: SEE 162 | 167 | 2.9 | Rick White | T | It has been decided that there is no optional exposed DTE/DCE interface between the MAC & PHY. | There is no exposed interface between the MAC and PHY. |
| rec: group discussion | 168 | 2.9 | Rick White | T | Need to identify what the Service Access Points are in the Reference Model. Also need to identify what types of information flows across the SAPs | |
| **rec: see 162** | **169** | **2.9** | **Siep** | **T** | **Reference Model Figure 2-11, Portion of the ISO Basic Reference Model Covered in this Standard**<br>Note 1 - Optional exposed DTE/DCE interface *[add reference]*<br>Note 2 - 802.10 SDE: IEEE 802.10 - Secure Data Exchange [2] | **The interface between the MAC and the PHY, if exposed, must be governed by a standard.** |
| | | | | | | |
| | 171 | 2.9, also 10.1, 10.5, 11.1, 11.4, and 12.2 | Fischer, Mike. | T | The reference model in figure 2Ð11 should be replaced with one that matches the remainder of the standard. A recommended replacement drawing appears in document 95/16. To the extent that it makes editorial sense to include reference model drawings in subsequent (e.g. PHY) chapters, those drawings should be copies of, or subsets of, the drawing in section 2.9. | There should be a consistent reference model for all sections of the specification, and for all PHYs; otherwise the concept of a reference model is of dubious value. The existing drawings in 4 chapters are all different, and none fully match the description of the MAC and PHY elsewhere in this document. |

| DISPOSITION | C# | SECTION | AUTH. | T/ E | *PROPOSED CHANGE* | RATIONALE |
|---|---|---|---|---|---|---|
| rec: see 162 - args for changing current doc and piucture at same time. | 172 | 2.9, also 8.1 | Fischer, Mike. | T<br>MAJOR ISSUE | The optional, exposed DTE/DCE interface at the MAC/PHY boundary is identified in section 2.9, but defined nowhere in the document. This should be corrected by including the definition of such an exposable interface. A plausible definition for this interface appears in document 95/16. {NOTE: I encourage members of 802.11 who doubt that an abstracted, exposable interface between MAC and PHY is achievable to read a recent draft of IEEE P1394ÑHigh Performance Serial Bus (I believe the latest released draft is D6.8, dated March 1994 and available from IEEE Standards Dept. as an unapproved draft.), P1394 has defined, in addition to a fullyÐspecified exposed interface at the bus cable connection point, an abstracted interface between their functional blocks equivalent to MAC and PHY which adds very few constraints not already inherent in their protocol and the available implementation technologies. If 802.11 can define the exposable DTE/DCE interface to a similar degree of Òprecise abstraction,Ó the need to define the realization of the optional exposed interface (connector, pin assignments, signal levels) is delayed until after publication of the first version of the standard, and perhaps delayed indefinitely. | This optional exposed interface is needed for several reasons<br>a) The existence of multiple PHYs using the same MAC creates situations where users will have reason to deploy infrastructures based upon different PHYs at different sites (for example due to regulatory differences at those sites or different nearby sources of interference in different frequency bands). For a class of communication devices which are specifically intended to support and facilitate mobility, there needs to be a means (allowed, not mandated, hence the optional nature of this exposed interface) for the user to easily change PHYs. While changing the MAC/PHY as a set is possible, much of the usage of wireless LAN communication is for equipment that needs to be small, lightweight, and reasonably resistant to environmental contamination. Providing the basis for a mixedÐvendor way to build the MAC functionality into these sorts of portable devices, while allowing the PHYs to be changed at the exposed interface, is highly desirable. The precedent for this already exists in 802.3, which has an exposed interface (AUI) that allows a MAC control function to be built into a piece of equipment while permitting the user to easily change mediaÐspecific adapters for use in different sites. The greater complexity and functionality embodied in the 802.11 PHYs is due to the use of wireless media, not due to an architectural difference in the MAC/PHY relationship.<br>b) The PAR requires that 802.11 use the same MAC over all of the different PHYs. If there are no exposed interfaces between the LLC and the WM, there is no way to interoperate between MAC implementations that are pared with different PHYs, hence neither a way to demonstrate compliance with the PAR nor a justifiable reason for this provision of the PAR. We need either to define this interface or to modify the PAR, then generate separate, PHYÐspecific MACs for each PHY (802.11a, b, c . . .)<br>c) If we are going to retain multiple, nonÐinteroperable PHYs in a single frequency band, users will demand some way to preserve at least part of their investment in network adapters (if they will be willing to make an investment in the first place). In my comments concerning section 8.1, I make some other comments regarding the use of different PHYs in the same frequency band, but as long as PHYs such as the current DSSS and FHSS for 2.4GHz band exist, there is yet another reason to provide this exposed interface. To do otherwise is likely to relegate the applicability of the results of our work to a niche no larger than that for wireline modems that only are able to provide their published performance when calling to another, identicalÐmodel modem. |
| Recommendation: decline | 173 | 2.10 | CHRIS ZEGELIN | | SERVICE PRIMITIVES ARE THE INTERCONNECTS BETWEEN THE MAC LAYER AND THE PHY LAYER. THIS HAS NOT BEEN CLEARLY STATED. | |
| recommended | 9 | 2.10 | David Bagby | T | ~~*(editor's note: extracted from X.210 – September 1993)*~~<br>*[DB28]* | See imbeded comments and annotations |