IEEE 802.11
Wireless Access Method and Physical Layer Specifications

Title: D1 Draft Comments on the WEP

Author: Dave Bagby
AMD
Email:david.bagby@amd.com

This is the comment table from the D1 letterballot responses on the Wired Equivalency Privacy (WEP). The entries in this table are only those that were **not** addressed in march 95 and incorporated into draft D1.1.
The remaining comments below were addressed by proposals in document 95/95 and 95/96 and will be incorporated into draft D1.2 (when the papers are formally adopted).

37: recommendation: needs big group disc. **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	37	2.3; also 1.2 definition of Òinfrastructure Ó2.4.1.1, 6th paragraph; 2.4.2.2, 3rd paragraph; 2.4.2.3, 3rd paragraph; 2.7	Fischer, Mike.	T M AJ OR ISS UE	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. 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. 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. 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.

43: recommendation: disc required by group **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	43	2.4.1.2, last paragraph	Fischer, Mike.	T M AJ OR ISS UE	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
recommendation: group discussion commetors wants a better auth default than "open". **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	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. 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 ? 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 - group discussion, see rec 65 **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	83	2.4.3.1 also relates to 2.5	Wim Diepstrate n	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. It is unclear why authentication support functions need to be included in the MAC. It is unclear what the minimum authentication frame exchange is when the network wants to run without explicit authentication. Figure 2-8 in section 2.5 should be changed to reflect this. 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. If a station is able to send a frame with the proper encription key, then that is sufficient prove of a stations identity. 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 **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	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: disc required, maybe possible to simplify internal structure of auth msg - tbd. **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	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.

rec: group disc required. MAY 95: addressed in 95/95 and/or 95/96 proposals.	**93**	**2.4.3.2**	**Siep**	**T**	EnciphermentPrivacy 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. 802.10 SDE settings • clear header length =0 • protected header length =0 • pad =none • ICV =32 bits. *[algorithm MUST be specified]* The encipherment model assumes a default, ESS–wide key to permit implict authentification. • 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) • 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. 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.**
rec: group disc re security **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	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 **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	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: security interest discussion **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	132	2.7.2	Tim Phipps	T	*Incomplete.* *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.

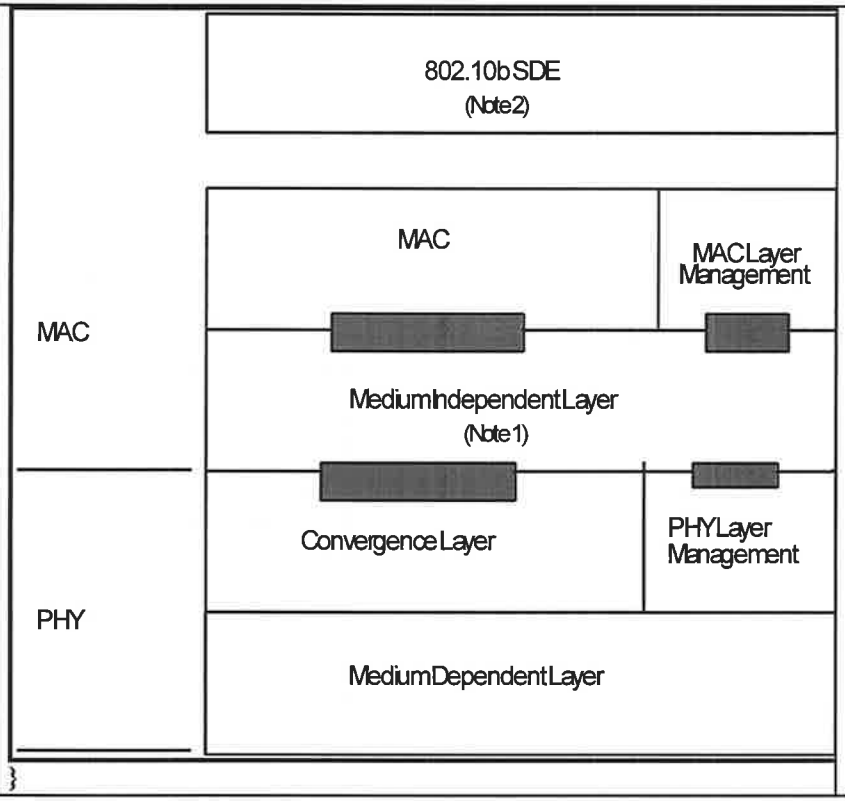
rec: remain open until alg number known. also group disc of security stuff required. **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	136	2.7.5	David Bagby	T	**No Privacy Algorithm in use:** Value = ?? **Wired Equivalent Privacy (WEP) algorithm:** Value = ?? draft can not go to sponsor ballot until these values are received from 802.10 since the standard can not be implemented without these values. 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. This satisfies the minimal operational needs of 802.11. 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. appendix missing - create and put in it the two initial values referenced above. **1. Authentication**	See imbeded comments and annotations
rec:; group disc needed. **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	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.
ec 136 **95: addressed in 95/95 or 95/96 proposals.**	138	2.7.5	Geiger	T	**No Privacy Algorithm in use: Value ??** **(WEP) algorithm: Value = ??** appendix XX	Resolve

rec: see 136 **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	140	2.7.5	Jon Rosdahl	T	No Privacy Algorithm in use: Value = ?? Wired Equivalent Privacy (WEP) algorithm: Value = ??	The values need to be determined and added. I am unable determine or assign these values.
rec: see 136 **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	141	2.7.5	Mahany	T	Privacy Response Add 802.10 Algorithm Numbers for No Privacy Algorithm, and WEP, Add Correct Appendix reference for Appendix X	Completeness
rec: see 136 **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	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 MAY 95: addressed in 95/95 and/or 95/96 proposals.	**145**	**2.7.5**	**Siep**	**T**	Pirvacy*[SUBSTITUE TEXT]* The MAC header specifies a bit in the FC field which indicates if the MDSU in the data frame is encripted. --OR-- *[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.** **The second option (deletion) conflicts with section 2.8**
rec: see 136 **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	143	2.7.5	Tim Phipps	T	*Incomplete.* *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 **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	144	2.7.5.	Fischerma :Privacy	T	must come from 802.10	802.10 algorithm numbers for privacy not specified.

rec: security group discussion needed - must remain open until auth alg specified and number provided or default auth details worked out an accepted. **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	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: **No Authentication algorithm in use:** Value = ?? need value from 802.10 - can not go to sponsor ballot until value received since can not implement the standard without this value. 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 complment 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. This satisfies the minimal operational needs of 802.11. 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. referenced appendix is missing - create and put in initial minimum value referenced in this section.	See imbeded comments and annotations

see 146 **Y 95: addressed in 95/95 nd/or 95/96 proposals.**	147	2.7.6	Geiger	T	**No Authentication algorithm in use: Value = ??** appendix XX	Resolve
rec: see 146 **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	148	2.7.6	Jon Rosdahl	T	No Authentication Algorighm in use: Value = ??	The values need to be determined and added. I am unable determine or assign these values.
rec: see 146 **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	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. **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	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 **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	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: see 146 **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	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 **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	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.

MAY 95: addressed in 95/95 and/or 95/96 proposals.	158	2.8 and 3.1.1.3	Fischer, Mike.	T	Add the following regarding 802.10 subset: 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). 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. 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. 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. 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. 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.)

rec: Joint group discussion required of full 802.11. **MAY 95: addressed in 95/95 and/or 95/96 proposals.**	159	2.9	Dean Kawaguchi	E		MAC layer management entity sends PLME service primitives to the PHY layer management entity.