TGi Draft 1Clause 8.2-8.2.2 Comments

IEEE P802.11E Security/D1.0
Letter Ballot# 25

Summary of Comments

- Editorial 30
- Technical
  - Minor 5
  - Serious 4
- Clarification Required 2
- Repeated 38

Editorial (by Comment ID)

- 374 – Insert word “the”
- 375 – Replace “this” with “these”
- 1290 – Replace “new” with “additional”
- 1484 – Change “data encapsulation” with “cipher suites”
- 376 – Replace “it” with “if”
- 377 – Replace "equipement" with "equipment"
- 1292 – Remove opinions
- 65 – Spell out abbreviation of init to initialization

Editorial (by Comment ID) (cont'd)

- 379 – Replace use of word "obtains"
- 380 – Clarify support for WEP and WEP2
- 381 – Delete duplicate word "with"
- 382 – Insert word "be"
- 383 – Correct figure reference
- 608 – Fix graphics arrows
- 757 – Remove unnecessary sentence
- 1296 – Clarify use of word "unique"

Editorial (by Comment ID) (cont'd)

- 1365 – Insert ref re ICV in WEP2 to WEP Basic
- 1366 – Repair graphics lines and arrows
- 1344 – Correct figure numbering
- 1433 – Clarify portion of frame that is encrypted
- 67 – Make byte count in figure consistent w/ text
- 385 – Insert word "in"
- 386 – Insert clause reference (clause xxx)

Editorial (by Comment ID) (cont'd)

- 1370 – Add example of key ID fields
- 1488 – Correct number of fields identified
- 1489 – Clarify IV field name reference
- 1561 – Minimize repetition in WEP/WEP2 description
- 1603 – Insert phrase "better privacy" re WEP2
- 1753 – Add reference for "Vernam" cipher
- 1754 – Remove word "catastrophically"

Technical - Minor (by Comment ID)

- 64 – WEP Basic use
- 93 – WEP2 ICV use
- 1295 – Key extension
- 1445 – PDU minimum length consistency
- 1609 - Define a MIC for use with WEP2

Technical - Major (by Comment ID)

- 66 – Key ID / pad use
- 590 – IV selection
- 1368 – Encryption algorithm indicator
- 1756 – AP knowledge of Cipher Suite

Clarification Required (by Comment ID)

- 759 – MIB Undecryptable Counter (unclear)
- 1232 - Add examples for Basic WEP, WEP2, AES, and PMAC (unclear)

Detailed Comments, Responses & Status

Comment ID	Sub clause	Pg	Line	Comment	Suggested Remedy	Editorial	Tech Minor	Tech Serious	Same as	Response	Refer to Group	Request for Clarification
1232	8.2			Samples of Basic WEP, WEP2, AES encryption and PMAC key derivation shall be added.	Add examples for Basic WEP, WEP2, AES, and PMAC.							1
1484	8.2	36	10	'data encapsulation" is not exactly what's going on.	Change to "Cipher Suites".	1					1	
374	8.2	36	14	Grammatical error.	Insert the word "the" between the words "enhancement to" and "original".	1				Agreed		
1290	8.2	36	14	"two new cipher suites" to "two additional cipher suites because "new" is a relative term.	"two new cipher suites" to "two additional cipher suites	1				Agreed		
1291	8.2	36	15	Delete the word "new" since one day this will no longer be new	Delete the word "new"				1290			
375	8.2	36	18	Grammatical error.	Replace the phrase "Sub-clause 8.2.4 closes this clauses..." with "Sub-clause 8.2.4 closes these clauses..."	1				Replace "this clauses" with "this clause"		
1603	8.2	37	27	Reword " ... there is any alternative" to	Reword to " ...there is a better privacy alternative"	1				Agree		
376	8.2.1.2	37	20	Typographical error.	Replace word "If" with "It" toward the end of the line.	1				Agreed		
1602	8.2	37	20	Typo .. "If offers no ..."	Change to .."It offers no .."				376			
1292	8.2.1.2	37	21-22	The end of the sentence "to offer any practical protection in this case" should be deleted since it is not clear that it is true and it adds no value to the sentence.	Delete the end of the sentence "to offer any practical protection in this case"	1				Agreed - May want to remove more of the opinions in this paragraph	1	
377	8.2.1.2	37	26	Typographical error.	Replace word "equipement" with "equipment".	1				Agreed		

Comment ID	Sub clause	Pg	Line	Comment	Suggested Remedy	Editorial	Tech Minor	Tech Serious	Same as	Response	Refer to Group	Request for Clarification
1441	8.2.1.2.	37	26	equipement is not a word	change to "equipment"				377			
64	8.2.1.2	37	5	Because of the deficiencies of the Basic WEP algorithm, we should warn against its use when this supplement is published.	Add the following statement to 8.2.1 (which is currently empty): "The use of the Basic WEP encapsulation methid is deprecated. Basic WEP is not strong enough, as of the development of this addendum, to prevent any but casual attempts to undermine its se		1				1	
378	8.2.1.2	37	27	The statement is made "Because of its weak protection guarantees, it should never be used when there is any alternative". This appears to be more of an opinion than a requirement, and seems to be something which applies to deployment of equipment rather					64			
756	8.2.1.2	37	27	Basic WEP remains in the standard for backward compatibility with already-deployed equipment only. Because of its weak protection guarantees, it should never be used when there is any alternative. Overstates the point somewhat. OK WEP is cryptographicall	Basic WEP remains in the standard for backward compatibility with already-deployed equipment only. Because of its cryptographic limitations, basic WEP is not recommended if Enhanced security services are present.				64			

Comment ID	Sub clause	Pg	Line	Comment	Suggested Remedy	Editorial	Tech Minor	Tech Serious	Same as	Response	Refer to Group	Request for Clarification
1293	8.2.1.2	37	27	Change: "Because of its weak protection guarantees," to "Because it is cryptographically weaker that the other methods," since "weak" is an undefined relative term.	Change: "Because of its weak protection guarantees," to "Because it is cryptographically weaker that the other methods,"				64			
1485	8.2.1.2	37	27	Wording	"... it should not be used when there is a stronger alternative."				64			
1752	8.2.1.2.	37		I do not agree with the premise that existing WEP is "weak". There is a wide gap between "casual montioring" and "cryptographically sophisticated adversaries". How is the statement that WEP offers "no protection" justified in this standard. Is this no	Find a less inflamatory way of editing this existing section to the standard. This is a standard and thus should minimize judgmental opinions in it's text.				64			
1753	8.2.1.3.	38	4	The term "Vernam" cipher is not defined anywhere.	Add definition in definition section or include a reference here.	1				Delete use of Vernam refernce	1	
93	8.2.2	38	9	WEP2 doesn't have a message integrity check. This severly limits the usefulness of WEP2.	Optionally include message integrity check.		1			Disagree		
1609	8.2.2.	39		WEP2 is next to useless without the inclusion of a cryptographic MIC.	Define a MIC for use with WEP2.		1				1	
608	8.2.2.1			Figure 7: An arrow connecting the ICV block to the Message block is missing	Add arrow	1				Disagree - technically incorrect		
65	8.2.2.1	38		Spell out all occurrences of "init" as "initialization".		1				Agreed (2 occurances)		

Comment ID	Sub clause	Pg	Line	Comment	Suggested Remedy	Editorial	Tech Minor	Tech Serious	Same as	Response	Refer to Group	Request for Clarification
1365	8.2.2.1	38		Here is no mentioning how the ICV is created.	Either refer to Basic WEP (clause 8.2.1.3) or add a decription how the ICV is created.	1				Add reference in 8.2.2.1 lines 11-16 to new 8.2.1.3		
757	8.2.2.1	38	11	and WEP2 is defined only so a standardized method exists to provide a degree of privacy using legacy hardware. A degree of privacy is provided by basic WEP. Surely WEP2 is defined so that an improved level of privacy may be provided using legacy hardware	and WEP2 is defined only so a standardized method exists to provide an improved degree of privacy using legacy hardware.	1				Replace "a degree" with "an improved degree" on line 16		
1294	8.2.2.1	38	11	The first sentence is superfluous. Remaining text is confusing.	Reorganize sentences to get the following text: "The WEP2 design provides additional data privacy by employing a larger MAC layer encryption key and a larger IV space. WEP2 is similar to Basic WEP and inherits many of its properties as described in clause				757			
379	8.2.2.1	38	17	Typographical/Grammatical Error.	The sentence starts "This recommendation obtains because...". Some word/phrase needs to replace "obtains", but I couldn't begin to tell you what.	1				Replace "obtains" with "is necessary"		

Comment ID	Sub clause	Pg	Line	Comment	Suggested Remedy	Editorial	Tech Minor	Tech Serious	Same as	Response	Refer to Group	Request for Clarification
1486	8.2.2.1	38	17	Grammer. "This recommendation obtains because in general...". Something is missing after obtains.	Completely reword to obtain intended meaning or insert "backward-compatibility, " after "obtains".				379			
1404	8.2.2.1.	38	17	Grammar	Change "obtains" to ???				379			
1442	8.2.2.1.	38	17	"This recommendation obtains because in general it will be infeasible to upgrade all Basic WEP hardware to WEP2 at once, so Basic WEP will be required for multicast communication." The sentence doens't make sense. Is this a recommendation or a requireme	Change to "This requirement exists because in general it will be infeasible to upgrade all Basic WEP hardware to WEP2 at once, so Basic WEP will be required for multicast communication."				379			
380	8.2.2.1	38	17	The statement is made that "WEP2 should also support Basic WEP", then the paragraph goes on to indicate this is necessary in order to provide an upgrade path, and that "...Basic WEP will be required for multicast communication". These two statements woul	Change the text to make the intent regarding the implementation of Basic WEP clear.	1				DISCUSS		
758	8.2.2.1	38	17	Note that implementations supporting WEP2 should also support Basic WEP. This recommendation obtains because in general it will be infeasible to upgrade all Basic WEP hardware to WEP2 at once, so Basic WEP will be required for multicast communication. sh	Clarify intent				380			

Comment ID	Sub clause	Pg	Line	Comment	Suggested Remedy	Editorial	Tech Minor	Tech Serious	Same as	Response	Refer to Group	Request for Clarification
66	8.2.2.1	38	262 7	Using the keyid and pad field as part of the IV will result in these 8 bits always being zero for any individual session key. The result is that the XOR of the key and IV will always result in the 8 bits of the key that align with the keyid/pad portion o	Eliminate the use of the keyid/pad as part of the IV. Use a true 128-bit IV or reduce the size of the key and IV to only 120 bits.			1			1	
68	8.2.2.2	40	4	The description of the IV field here does not match that of 8.2.2.1, where there is also a pad field described.	Fix 8.2.2.1 or 8.2.2.2 to be correct.				66			
1166	8.2.2.2	40	1	Figure 8 note is inconsistent with the size of IV shown above it. The text at line 8 mentions a non-existant "pad" field.	Use 16 bytes for size of IV. Remove mention of pad field.				68			
69	8.2.2.2	40	8	The use of the keyid field should not be described (again) here. Simply reference the description of this field in the Basic WEP subclause. Also, there is a description of a pad field that is not shown in the figure.	Delete the last 4 sentences of this paragraph and replace with a reference to the keyid field in Basic WEP.				68			
387	8.2.2.2	40	8	The statement is made, "The contents of the pad subfield shall be zero". There does not appear to be a pad subfield in the figure.	Either remove this reference to the pad subfield, or modify figure 8 to correctly represent the expanded packet, including all subfields.				68			
1406	8.2.2.2.	40	1	Figure 8 mislabels the pad field as IV	Change Figure 5 by replacing IV with pad in the appropriate place				68			

Comment ID	Sub clause	Pg	Line	Comment	Suggested Remedy	Editorial	Tech Minor	Tech Serious	Same as	Response	Refer to Group	Request for Clarification
610	8.2.2.2			The text mentions a 'pad' subfield but the figure has no such field.	Modify the firuge to include a pad subfield				68			
381	8.2.2.1	38	28	Typographical error.	Replace the phrase "...with the with initialization..." with "...with the initialization..."	1				Agreed		
1295	8.2.2.1	38	303 1	In the case of both key extension and truncation it is not specified which end of the key should be padded to (or truncated) to adjust the size. This needs to be added.	Need to define way to truncate and extend keys		1				1	
382	8.2.2.1	38	31	Grammatical error.	Insert the word "be" between the phrases "...128-bits shall" and "truncated to..."	1				Agreed		
1487	8.2.2.1	38	26	Clarity and grammer.	"WEP2 bitwise XORs the secret key with the initialization vector. The last byte of the IV includes the key ID, and it is included in the XOR." Insert "be" after "larger than 128-bits shall".				382			
1405	8.2.2.1.	38	31	Grammar	Change "shall truncated" to "shall be truncated"				382			
1657	8.2.2.1.	38	31	Missing verb - shall truncated	shall be truncated				382			

Comment ID	Sub clause	Pg	Line	Comment	Suggested Remedy	Editorial	Tech Minor	Tech Serious	Same as	Response	Refer to Group	Request for Clarification
590	8.2.2.1	38	32	WEP2 currently does not offer (modified) replay protection. Rudimentary replay protection can be added however by defining an IV selection algorithm that allows the receiver to catch old frames with very limited implementation overhead. It is suggested th	Replace paragraph by "A conformant WEP2 implementation shall construct the IV by taking the IV Selection Element in the Association Request/Response received from the peer STA as the most significant 64 bits, and taking the TSF timer at the time of WEP en			1			1	
1296	8.2.2.1	38	32	Meaning of the word "unique" is unclear.	Suggest new text "A conformant WEP2 implementation shall with high probability select an <IV, key> pair which is unique within the operating lifetime of the STA.	1				Disagree - Draft statement is sufficient		
1561	8.2.2.1	38-39		Reduce the description to highlights of the REAL differences between WEP and WEP2 and eliminate all the information that is repeated in this sectrion including the figure on page 39. Repetition can lead to inconsistency and hence causing interoperability		1					1	

Comment ID	Sub clause	Pg	Line	Comment	Suggested Remedy	Editorial	Tech Minor	Tech Serious	Same as	Response	Refer to Group	Request for Clarification
1678	8.2.2.1	38-39		The description can be significantly reduced by highlighting the real differences between WEP and WEP2 and by eliminating all the information that is repeated in this sectrion including the figure on page 39. Repetition can lead to inconsistency and hence					1561			
1700	8.2.2.1	38-39		The description can be significantly reduced by highlighting the real differences between WEP and WEP2 and by eliminating all the information that is repeated in this sectrion including the figure on page 39. Repetition can lead to inconsistency and hence					1561			
1366	8.2.2.1	39	1	The lines and arrows in Figure 7 are shifted in respect to the boxes.		1				Agreed		
759	8.2.2.1	39	12	MSDUs with erroneous MPDUs (due to inability to decrypt) shall not be passed to LLC. Should some MIB counter be incremented (aUndecryptable)? (In general there seem to be no MIB additions).	Review MIB requirements.							1
383	8.2.2.1	39	6	Sentence states "Referring to Figure 7 and following from left to right, decipherment begins with...". Figure 7 refers to "encipherment".	Change text to refer to the correct figure number.	1				Agreed		

Comment ID	Sub clause	Pg	Line	Comment	Suggested Remedy	Editorial	Tech Minor	Tech Serious	Same as	Response	Refer to Group	Request for Clarification
1367	8.2.2.1	39	6	The reference to figure 7 (the encipherment diagram) is wrong.	It must refer to figure XXX, being the decipherment diagram				383			
1345	8.2.2.1.diagram	39		Un labeled diagram has WEP decipher block generating ICV? Is this correct?	Clarify reason for ICV? or remove ?				383			
1443	8.2.2.1.	38	24	"The WEP2 algorithm is applied to the Frame Body of an MPDU." which implies the entire Frame Body is encrypted	Please change to: "The WEP2 algorithm encrypts the PDU and ICV fields of the Frame Body of an MPDU."	1				Agreed		
1754	8.2.2.1.	38	35	Please refrain from the use of unquantifiable adverbs such as fail "catastrophically".		1				Replace "fail catastrophically" with "fail"		
1344	8.2.2.1.	39	68	THERE IS A FIGURE BETWEEN 7 & 8 WITH NO FIGURE NUMBER	aDJUST FIGURE NUMBERS AND TIE CORRECTLY TO EXPLANTORY TEXT.	1				Agreed		
67	8.2.2.2	40	1	The note in the figure claims that the MPDU is expanded by 21 octets. The text in 8.2.2.1 and the figure itself describe only 20 octets.	Fix either the note or the figure to be correct.	1				Agreed - fix the Note		
609	8.2.2.2			Figure 8: The Note says that WEP2 has expanded the MPDU by 21 octets, 17 for the IV.	Change to show that the MPDU is expanded by 20 octets including 16 octets for the IV.				67			
384	8.2.2.2	40		The note on the figure states that the MPDU has been expanded by 21 bytes, with 17 for the initialization vector. The figure itself only indicates an expansion of 20 bytes, 16 for the IV.	Correct note to indicate the correct number of bytes.				67			

Comment ID	Sub clause	Pg	Line	Comment	Suggested Remedy	Editorial	Tech Minor	Tech Serious	Same as	Response	Refer to Group	Request for Clarification
1189	8.2.2.2	40		There is an inconsistency with regards to the length of the IV as shown in the picture (16 octets) and was is described under the picture, there the IV is said to be 17 octets in length.	The text should be modified to set the IV length to 16 octets (not 17 octets), the MPDU is expanded by 20 octets and not 21.				67			
1446	8.2.2.2.	40	1	Figure 8 caption reads: "Note: The encipherment process has expanded the original MPDU by 21 Octets, 17 for the Initialization Vector (IV) field and 4 for the Integrity Check Value (ICV). The ICV is calculated on the Data field only." 21 should be 20,	Please change to read: "Note: The encipherment process has expanded the original MPDU by 20 Octets, 16 for the Initialization Vector (IV) field and 4 for the Integrity Check Value (ICV). The ICV is calculated on the Data field only."				67			
1369	8.2.2.2	40	1	The numbers given in the note of Figure 8 are incorrect.	...has expanded the original MPDU by 20 octets, 16 for the				67			
1605	8.2.2.2	40	1	Inconsistency between the figure and figure_text. In figure IV looks like 16 octets and in text says "...,17 for the Initialization Vector".	Remedy inconsistency				67			
598	8.2.2.2	40	1	Encipherment process only expands the original MPDU by 20 octets (16 for the IV).	Replace 21 by 20 and 17 by 16				67			

Comment ID	Sub clause	Pg	Line	Comment	Suggested Remedy	Editorial	Tech Minor	Tech Serious	Same as	Response	Refer to Group	Request for Clarification
1368	8.2.2.2	40	1	The definition of the IV/key block in the Expanded WEP Mpdu, although pleasing for the human eye, has the disadvantage that a receiving entity in a MAC controller must have access to the station database to figure out how long the IV/keyId block is. It ca	Have the KeyId field in its original (basic WEP) place and have the Encryption algorithm indicator in the KeyId byte. Thus 3 bytes IV, 1 byte with KeyId, EncAlg and pads, 13 bytes IV. The EncAlg can be a single bit that differentiates between short IV blo			1			1	
1488	8.2.2.2	40	4	Disagreement on quantity.	change "three sub-fields" to "two sub-fields".	1				Agreed		
1447	8.2.2.2.	40	39	There is an inconsistency in meaning between the sentence in lines 3 and 4 and Figure 8: "IV 6 bits" "This field shall contain three sub-fields: a 126 bit field that contains the initialization vector proper and a 2 bit key ID field." and the sentence	If the 6 bit field of the 16th octet of the IV is intended to be a nonzero subfield of the Init. Vector, then the sentence in lines 8 and 9 should be struck out, and the word "three" in lines 3 and 4 changed to "two". Otherwise, the label in Figure 8 sho				1488			
1489	8.2.2.2	40	5	The keyid IS part of the IV, as figure 8 shows both the field and two subfields are all called IVs. Confusing field naming going on here.	Find better names for fields, if possible. Indicate that, while the keyID contains specific information, it is used as part of the XOR with the rest of the bits.	1				Disagree		
385	8.2.2.2	40	7	Grammatical error.	Insert the word "in" between the phases "...key values for use" and "decrypting this MPDU".	1				Agreed		

Comment ID	Sub clause	Pg	Line	Comment	Suggested Remedy	Editorial	Tech Minor	Tech Serious	Same as	Response	Refer to Group	Request for Clarification
386	8.2.2.2	40	8	The statement is made, "Interpretation of these bits is discussed further in clause XXX". XXX appears to be a missing reference.	Correct the text to include the referenced clause number.	1				Agreed - reference clause 8.3.2 in 802.11 1999		
599	8.2.2.2	40	8	There is a reference to a non-existing clause XXX and the pad subfield doesn't exist.	Fix reference to clause and remove reference to pad field				386			
1370	8.2.2.2	40	9	It is handy to write out the keyIDs to avoid ambiguous situations	Add the following text: The KeyIds are defined as follows: bit7 bit6 0 0 KeyId 0 0 1 KeyId 1 1 0 KeyId 2 1 1 KeyId 3 The same applies to clause 8.2.1.5 of the Basic WEP frame body expansion	1				Disagree - reference response to Comment # 386		
1407	8.2.2.2.	40	8	Where is the interpretation of the Key ID subfield discussed further?	Clarify				386			
1444	8.2.2.2.	40	8	The clause reference XXX needs to be resolved					386			
1756	8.2.2.2.	40		I may have missed something along the way, but I don't see how the enhanced MAC in an AP knows whether the frame is being encrypted with WEP, WEP2, or AES. Is it based on the MAC address in the RA field of the packet?	Should clarify how the MAC in the AP knows how to decrypt the frame, since there is only a single WEP bit in the frame control field.			1			1	
1445	8.2.2.2.	40	1	The figure for clause 8.2.2.2 says the minimum length of the PDU is 1, while clause 7.1.3.5 of the standard says the minimum length of a PDU is 0.	The text in the figure should be changed from ">=1" to ">=0", or an explanation should be provided to explain the inconsistency with clause 7.1.3.5.		1				1	

Comment ID	Sub clause	Pg	Line	Comment	Suggested Remedy	Editorial	Tech Minor	Tech Serious	Same as	Response	Refer to Group	Request for Clarification
1413	8.2.2.3.3.	45	10	Typo	Change "Ci" to "Cn"					Believe refers to 8.3.2.3		
Total						30	5	4			12	2