IEEE P802.11
Wireless LANs

802.11w May Sponsor Ballot Report

Date: 2008-05-16

Author(s):

Name	Affiliation	Address	Phone	email
Jesse Walker	Intel Corporation	2111 NE 25th Avenue JF3-206, Hillsboro, OR, USA 97124	+1-503-712-1849	jesse.walker@intel.com

Abstract

This document reports the results of the WG letter ballots on IEEE P802.11w. This report is to be submitted to the IEEE 802 Executive Committee to support the request to forward IEEE P802.11w to Sponsor Ballot.

1. Introduction and Summary

This report documents to the IEEE 802 Executive Committee all the WG letter ballots for IEEE P802.11w, including voting results, comment statistics, and unsatisfied negative comments.

The size of the IEEE P802.11w voter pool is 427. The final results for the Working Group balloting for IEEE P802.11w are 328 voted, 266 yes, 8 no, 54 abstained, for a 97.08% approval rate, a return percentage of 76.81%, and an abstain percentage of 16.46%.

There are 25 unsatisfied required negative comments from eight remaining negative voters, none from the latest latter ballot; all 25 unsatisfied negative comments are previously recirculated but whose resolution the commentors have not accepted. None of the voters with unsatisfied negative comments from prior have responded to our efforts to learn whether the resolutions adopted by IEEE 802.11 Task Group w satisfy their objections.

Based on results of the letter ballots on IEEE P802.11w as documented in this report, we are asking for approval from the IEEE 802 Executive Committee to forward IEEE P802.11w to sponsor ballot.

Agenda Items and motions requesting approval to forward when the prior ballot has closed shall be accompanied by:

- Date the ballot closed

- Vote tally including Approve, Disapprove and Abstain votes

- Comments that support the remaining disapprove votes and Working Group responses.

- Schedule for recirculation ballot and resolution meeting.

Letter Ballot 88 was a vote on Draft 1.0, and ran for 40 days starting 10 October 2006, and ending on 19 November 2008. 295 voted, 202 yes, 34 no (452 comments received), 59 abstained, 85.59% approval rate.

Letter Ballot 102 was a vote on Draft 2.0, and ran for 15 days starting 17 April 2007, and ending on 5 May 2007. 317 voted, 227 yes, 29 no, 61 (751 comments received), abstained, 88.67% approval rate.

Letter Ballot 114 was a vote on Draft 3.0, and ran for 15 days starting 4 October 2007, and ending on 19 October 2007. 325 voted, 245 yes, 21 no (146 comments received), 59 abstained, 92.10% approval rate.

Letter Ballot 117 was a vote on Draft 4.0, and ran for 15 days starting 10 October 2007, and ending on 19 November 2008. 326 voted, 245 yes, 21 no (87 comments received), 60 abstained, 92.10% approval rate.

Letter Ballot 121 was a vote on Draft 5.0, and ran for 15 days starting 5 February 2008, and ending on 20 February 2008. 328 voted, 259 yes, 14 no (52 comments received), 55 abstained, 94.87% approval rate.

Letter Ballot 128 was a vote on Draft 6.0, and ran for 15 days starting 3 April 2008, and ending on 18 April 2008. 328 voted, 266 yes, 8 no (29 comments received), 54 abstained, 97.08% approval rate.

The following table summarizes the no voters with unsatisfied negative comments:

Voter	**LB 88**	**LB 102**	**LB 114**	**LB 117**	**LB 121**	**LB 128**	**Total**
Keith Amann		3					**3**
John Bahr	1						**1**
Kaberi Banerjee	4						**4**
Pat Calhoun	1						**1**
Roger Durand	4						**4**
Jon Edney	1						**1**
Stephen Palm	5			4			**9**
Ning Zhang				2			**2**
Total	**16**	**3**		**6**			**25**

The following details each of the remaining unsatisfied comments:

Cl **03** *SC* **3** *P* **1** *L* **41-4** # 1097

Banerjee, Kaberi Individual

Comment Type **TR** *Comment Status* **R**

Define robust management frame exchange as a part of clause 3, as disassociation, deauthentication and management action frames; current definition seems

SuggestedRemedy

Response *Response Status* **U**

REJECT. The full definition is already defined in 5.4.3.7. This conforms to the customary usage in the base standard

Cl **05** *SC* **5.4.3.2** *P* **3** *L* **25** # 1092

Banerjee, Kaberi Individual

Comment Type **TR** *Comment Status* **A**

Define Disconnect Hash Value, before using the term.

SuggestedRemedy

Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Resolved by submission 11-06-1932r0

Cl **05** *SC* **5.4.3.7** *P* **4** *L* **25-2** # 1093

Banerjee, Kaberi Individual

Comment Type **TR** *Comment Status* **R**

EAPOL frame exchanges to perform the IGTK transfer and installation are done via RSNA protected frames ?Please clarify

SuggestedRemedy

Response *Response Status* **U**

REJECT. This question is more relevant to the base 802.11 standard, whereby EAPoL frames are protected by the 4-Way Handshake or the Group Key Handshake to distribute group keys. TGw protection does not change this definition.

Cl **05** *SC* **5.8.2.1** *P* **10** *L* **8** # 1194

Palm, Stephen Individual

Comment Type **TR** *Comment Status* **R**

Is "Robust management Frame" a state? If so, where is the bitfield?

SuggestedRemedy

Clarify how to "enable"

Response *Response Status* **U**

REJECT. We cannot correlate the comment with the cited page and line

Cl **07** *SC* **7.3.2.27** *P* **10** *L* **24** # 1084

Bahr, John Individual

Comment Type **TR** *Comment Status* **A**

Draft is not complete: "{edNOTE : TBD}"

SuggestedRemedy

Determine the Element ID field value.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE. An editorial note has been added to note that a value must be assigned by ANA, until such time, TBD remains.

Cl **07** *SC* **Table 9** *P* **8** *L* # 1099

Banerjee, Kaberi Individual

Comment Type **TR** *Comment Status* **R**

TBD in Table 9

SuggestedRemedy

Response *Response Status* **U**

REJECT. ANA, not TGw, must assign this code (Note: comment refers to Table 19, not Table 9)

Cl **08** *SC* **8.3.3.3.2** *P* **18** *L* **20** # 47

Zhang, Ning Individual

Comment Type **TR** *Comment Status* **A**

Since the text now states that the Order bit will be "set to 1 otherwise", this will not allow interoperation with non-HT STAs. Such STAs which are currently compliant to the 2007 std will NOT set the Order bit in the frame control field and will NOT set it to 1 in the AAD.

SuggestedRemedy

Change "set to 1 otherwise" to "unmasked otherwise".

Response *Response Status* **U**

ACCEPT IN PRINCIPLE. The text has been introduced by TGn which is no longer tracked by TGw and thus, the offending text no longer exists in TGw.

Cl **08** *SC* **8.3.3.3.2** *P* **23** *L* **52** # 53

Palm, Stephen Individual

Comment Type **TR** *Comment Status* **A**

Presence or absence of a fielf is not a sufficient criteria for setting the mask

SuggestedRemedy

Make dependent on the value of a field

Response *Response Status* **U**

ACCEPT IN PRINCIPLE. The comment is insufficient to decipher wha "fielf" is the offending one as the page and line number do not correspond to clause 8.3.3.3.2 and several fields are masked in that clause. If it is in reference to the Order bit, see CID 44.

Cl **08** *SC* **8.3.4.2** *P* **20** *L* **5** # 73

Amann, Keith Individual

Comment Type **ER** *Comment Status* **R**

Frame formats are defined in clause 7. The inclusion of this frame format here is confusing.

SuggestedRemedy

Move the frame format definition to clause 7 with the other frame formats.

Response *Response Status* **U**

REJECT. The BIP encapsulation is not defining a new frame format much like TKIP (8.3.2.2) and CCMP (8.3.3.2) as they also do not define a new frame format but rather describe how security is added to the existing data or management frame format.

Cl **08** *SC* **8.3.4.3** *P* **20** *L* **1** # 1200

Palm, Stephen Individual

Comment Type **TR** *Comment Status* **A**

Why mention 802.11 here?

SuggestedRemedy

Delete "802.11", add a better modifier

Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Remove "IEEE 802.11"

Cl **08** *SC* **8.3.4.3** *P* **20** *L* **3** # 1201

Palm, Stephen Individual

Comment Type **TR** *Comment Status* **R**

Why mention 802.11 here?

SuggestedRemedy

Delete "802.11", add a better modifier

Response *Response Status* **U**

REJECT. The same language is already used for CCMP in the base standard

Cl **08** *SC* **8.3.4.3** *P* **21** *L* **32** # 58

Zhang, Ning Individual

Comment Type **ER** *Comment Status* **A**

To be consistent with figure 8-17, I recommend removing the muted bits from Figure 8-19b,Remove the muted bits.

SuggestedRemedy

ACCEPT

Response *Response Status* **U**

ACCEPT.

Cl **08** *SC* **8.3.4.4** *P* **27** *L* **25** # 61

Palm, Stephen Individual

Comment Type **TR** *Comment Status* **A**

By monotonically increasing do you mean increment by one?

SuggestedRemedy

Clarify

Response *Response Status* **U**

ACCEPT IN PRINCIPLE. This usage is consistent with existing 802.11-2007. As mentioned in the same clause, the receiver will check for the new SeqNo to be higher than the one received in an earlier frame.

Cl **08** *SC* **8.3.4.4** *P* **27** *L* **25** # 62

Palm, Stephen Individual

Comment Type **TR** *Comment Status* **A**

How is wrap around handled?

SuggestedRemedy

Clarify

Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Insert the text on page 21 line 54: "The transmitter may refresh the IGTK with a new sequence number at any time."

Cl **08** *SC* **8.3.4.4** *P* **27** *L* **25** # 63

Palm, Stephen Individual

Comment Type **TR** *Comment Status* **A**

Should the "replay" in line 26 and subsequent also be replaced with Sequence as in the previous line? The field operations seem to be a jumble in this paragraph

SuggestedRemedy

Clarify

Response *Response Status* **U**

ACCEPT IN PRINCIPLE. See CID 60

Cl **08** *SC* **8.4.1.2.1** *P* **22** *L* **38** # 1202

Palm, Stephen Individual

Comment Type **TR** *Comment Status* **R**

Why mention 802.11 here?

SuggestedRemedy

Delete "802.11", add a better modifier

Response *Response Status* **U**

REJECT. This modifier is already in the base standard, and TGw is not changing the nomenclature used in the based standard

Cl **08** *SC* **8.5.1.3A** *P* **29** *L* **27** # 74

Amann, Keith Individual

Comment Type **TR** *Comment Status* **A**

If I interpret the text correctly here the IGTK is nothing more that a random value. Should there be some rules around this to prevent having the same random value used as a seed every time?

SuggestedRemedy

Add normative text to more clearly define the key initialization/derivation rules for the IGTK. I understand that this clause was not updated, and that the task group may elect to reject this comment, but I think that it is important to clarify the intent here to ensure that this key is acceptable.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Replace the first sentence in 8.5.1.3A with "The Authenticator shall select the IGTK as a random value each time it is generated." Annex H.5 already provides guidance on generating and selecting random values.

Cl **08** *SC* **8.5.4** *P* **22** *L* # 331

Edney, Jon Individual

Comment Type **TR** *Comment Status* **R**

There is no mechnism specified to enable a station to reconnect to the network in the event that it unexpectedly loses key state, such as due to a reboot while out of range of the AP.

SuggestedRemedy

Consider mechanisms to avoid deadlock

Response *Response Status* **U**

REJECT. 802.11i requires the AP to flush its PTK for the STA when receiving an associate request (yes; this is a DoS problem, but it is what 802.11i says)

Cl **08** *SC* **8.5.6.3** *P* **29** *L* **14** # 1203

Palm, Stephen Individual

Comment Type **TR** *Comment Status* **A**

Is the psudo-code normative?

SuggestedRemedy

clarify

Response *Response Status* **U**

ACCEPT. Pseudo-code is normative, as it intends to describe behavior that is externally visible. How the function defined by the pseudo-code is implemented is outside the scope of the standard

Cl **08** *SC* **8.7.2.3a** *P* **43** *L* **1** # 71

Amann, Keith Individual

Comment Type **TR** *Comment Status* **A**

There is a problem with the pseudo-code through here where the if/else/else if statements don't align. For example, line 1 on page 43 is an "else" statement that appears to align with the "if" statement on line 38 of page 41, but the comment immediately following this if doesn't match with the "if" condition."

SuggestedRemedy

Unfortunately I'm not familiar enough with the draft to be able to provide a suitable resolution, but it does appear that the pseudo-code is either incorrect, or incomplete, and I would recommend that the task group review the pseudo-code, and correct any discrepencies discovered.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE. The pseudocode has been updated per submission 07/243r7 to endeavor clarification and completeness.

Cl **General** *SC* *P* *L* # 87

Zhang, Ning Individual

Comment Type **ER** *Comment Status* **A**

Various phrases such as "Robust Management Frames" and "Management Frame Protection" are used to describe this new feature. As an example, see 8.4.3, line 45. "Robust Management Frame Protection Capable" should be "Management Frame Protection Capable".

SuggestedRemedy

Please use only a single phrase to describe the feature.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE. The service is now consistantly referred to as "Management Frame Protection" however the frames are still referred to as Robust Management frames.

Cl **General** *SC* *P* *L* # 466

Durand, Roger Individual

Comment Type **TR** *Comment Status* **R**

The disassociate or dis auth is often legitimently used to re-sync or start over a client that has gotten it's present state "lost" thru any of several scenarios that could happen on either end to include a cold or partial re-boot of either the client or the AP. It is unclear how to communicate to a client to "start everything over" if the frame becomes protected.

SuggestedRemedy

Either we allow a finite number of non-protected de-auth/dis-assoc and we somehow limit it's use (say once every x minutes) or we need to create a new frame that communicates the need to reset state or that one end has recently reset (and this command may need to be time limited to usage of once every x minutes).

Response *Response Status* **U**

REJECT. This feature is not supported by the base standard when security is used. 8.4.10 requires that the security association is deleted upon receiving a disassociate or deauthenticate. TGw is not authorized to change the behavior for data frames.

Cl **General** *SC* *P* *L* # 465

Durand, Roger Individual

Comment Type **TR** *Comment Status* **R**

The document is incomplete or unclear relative to providing management frame protection for each access control scenario, how does this happen when no radius server is present or specifically when a pre-shared key method is the network scenario.

SuggestedRemedy

Separately call out the key creation and exchange mechanism for each access control scenario so as to create an 11w protected network, in particular when using a pre-shared key.

Response *Response Status* **U**

REJECT. No changes are made to the PMK by 802.11w; 802.11w uses the same PMK for management as for unicast data. 802.11i uses PSK as a PMK. The only new key added is the IGTK, which is used to protect broadcast management frames. It is assigned by the AP, just as the GTK is, not derived from the PMK.

Cl **General** *SC* *P* *L* # 454

Durand, Roger Individual

Comment Type **TR** *Comment Status* **R**

The disassociate or dis auth is often legitimently used to re-sync or start over a client that has gotten it's present state "lost" thru any of several scenarios that could happen on either end to include a cold or partial re-boot of either the client or the AP. It is unclear how to communicate to a client to "start everything over" if the frame becomes protected.

SuggestedRemedy

Either we allow a finite number of non-protected de-auth/dis-assoc and we somehow limit it's use (say once every x minutes) or we need to create a new frame that communicates the need to reset state or that one end has recently reset (and this command may need to be time limited to usage of once every x minutes).

Response *Response Status* **U**

REJECT. This feature is not supported by the base standard when security is used. 8.4.10 requires that the security association is deleted upon receiving a disassociate or deauthenticate. TGw is not authorized to change the behavior for data frames.

Cl **General** *SC* *P* *L* # 453

Durand, Roger Individual

Comment Type **TR** *Comment Status* **R**

The document is incomplete or unclear relative to providing management frame protection for each access control scenario, how does this happen when no radius server is present or specifically when a pre-shared key method is the network scenario.

SuggestedRemedy

Separately call out the key creation and exchange mechanism for each access control scenario so as to create an 11w protected network, in particular when using a pre-shared key.

Response *Response Status* **U**

REJECT. No changes are made to the PMK by 802.11w; 802.11w uses the same PMK for management as for unicast data. 802.11i uses PSK as a PMK. The only new key added is the IGTK, which is used to protect broadcast management frames. It is assigned by the AP, just as the GTK is, not derived from the PMK.