Cl **00** *SC* **0** *P* **0** *L* **8** # 49

Chaplin, Clint F

Comment Type **ER** *Comment Status* **X** *Editor*

WM: On page v of frontmatter, only Tim Godfrey is listed as WG Secretary.

SuggestedRemedy

Add Stephen McCann as another WG Secretary

Proposed Response *Response Status* **U**

ACCEPT

Cl **00** *SC* **0** *P* **1** *L* **41** # 59

Stanley, Dorothy V

Comment Type **TR** *Comment Status* **X** *Editor*

Definition of transition time can be made made more specific

SuggestedRemedy

Change from "after the receipt of the last acknowledged data frame sent within an originating BSS by the STA and ends after the receipt of the first acknowledged frame sent within the destination BSS" to
"after the receipt of the last acknowledged data frame sent within an originating BSS and ends after receipt of the first acknowledged data frame sent within the destination BSS"
Assuming it is true that the "last acknowledged data frame" can be sent by either the AP or the non-AP STA.

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changed to "after the receipt of the last acknowledged data frame sent within an originating BSS and ends after receipt of the first acknowledged data frame sent within the destination BSS, while the non-AP STA transitions."

All comments on the frontmatter are editorial.

This comment would normally be considered out of scope of this recirculation ballot, since it does not refer to changed text in D8.0. However, the entire frontmatter is deleted in generating the next revision of the standard. Resubmission of this comment during the next revision of the standard is not possible.

Cl **00** *SC* **0** *P* **67** *L* **1** # 46

Myles, Andrew F

Comment Type **TR** *Comment Status* **X** *reservation protocol*

11A.6) 6-way exchange is not useful in FT. It could lower the capacity of the network by reserving resources at various Aps. Please remove the 6-way exchange.

SuggestedRemedy

Remove Section 11A.6

Proposed Response *Response Status* **U**

REJECT.
This issue was dealt with in a previous ballot, where a response was provided. The commentor has not provided any new information to sway the decision of the resolution group.

Cl **00** *SC* **0** *P* **93** *L* **9** # 47

Myles, Andrew F

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

11A.10) Defining messages between APs is out of scope of 802.11. Besides, some architectures such as centralized switch architecture does not need any such message exchange since this communication can be performed in-memory. Therefore, we should not be defining a particular method of communication the way we do in the draft; it may be enough to just mention requirements for such communication.

SuggestedRemedy

Remove Section 11A.10

Response *Response Status* **W**

REJECT.

This comment was WITHDRAWN by the commenter.

Comment was withdrawn by the submitter

Cl **03** *SC* **3.125b** *P* **3** *L* **30** # 14

Webb, Stephen C

Comment Type **E** *Comment Status* **X** *Editor*

Sub-clause 3.125a does not exist

SuggestedRemedy

Insert 3.125a or undo change and revert to original number

Proposed Response *Response Status* **C**

REJECT
3.125a is being added by P802.11k, Amendment #1 to P802.11-2007.

Cl **03** *SC* **3.54b** *P* **2** *L* **23** # 15

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *other*

The definition of FT 4-way handshake seems to apply to even the FT protocol, whereas, it should be specific to the 4-way handshake in the Initial MD assoc only.

SuggestedRemedy

Change: "A pairwise key management protocol used during Fast BSS Initial Mobility Domain Association, when Fast BSS Transition is enabled."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changed to "A pairwise key management protocol used during Fast BSS Transition Initial Mobility Domain Association."

Cl **05** *SC* **5.2.3.2** *P* **4** *L* **48** # 51

Chaplin, Clint F

Comment Type **ER** *Comment Status* **X** *Editor*

WM: Typo

SuggestedRemedy

change "THese" to "These"

Proposed Response *Response Status* **U**

ACCEPT

Cl **05** *SC* **5.2.3.2** *P* **4** *L* **48** # 16

Sood, Kapil

Comment Type **ER** *Comment Status* **X** *Editor*

Typo on "THese"

SuggestedRemedy

Change: "THese" to "These"

Proposed Response *Response Status* **U**

ACCEPT

Cl **05** *SC* **5.2.3.2** *P* **4** *L* **64** # 18

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *other*

R0KH/R1KH is not clear

SuggestedRemedy

Change: "&between R0KH and R1KH Authenitcator components."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changed to "between the R0KH and R1KH Authenticator components"

Cl **05** *SC* **5.4.3.1** *P* **5** *L* **29** # 52

Chaplin, Clint F

Comment Type **TR** *Comment Status* **X** *Editor*

WM: With the addition in D8.0, there are now three authentication methods.

SuggestedRemedy

change "two" to "three"

Proposed Response *Response Status* **U**

ACCEPT

Cl **05** *SC* **5.4.3.1** *P* **5** *L* **29** # 19

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *Editor*

defines 3, not two

SuggestedRemedy

Change: "&defines three authentication&"

Proposed Response *Response Status* **U**

ACCEPT

Cl **05** *SC* **5.4.3.1** *P* **5** *L* **34** # 20

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *non-AP STA*

Not just any "station" - these should be non-AP STA

SuggestedRemedy

change: "the non-AP STAs as defined in Clause 11A."

Proposed Response *Response Status* **U**

ACCEPT

Cl **05** *SC* **5.4.3.4** *P* **5** *L* **45** # 21

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *other*

Missing the FT 4-way handshake in the list

SuggestedRemedy

Change: "the 4-Way Handshake, Fast BSS Transition 4-Way Handshake, the Fast BSS Transition protocol&"

Proposed Response *Response Status* **U**

ACCEPT

Cl **05** *SC* **5.4.3.7** *P* **5** *L* **54** # 22

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *non-AP STA*

Sentence is incomplete without the mention of "who" is the other party besides the AP that is involved in the FT.

SuggestedRemedy

Change: "defines means for a non-AP STA for setting up security&"

Proposed Response *Response Status* **U**

ACCEPT

Cl **05** *SC* **5.8.1** *P* **6** *L* **1** # 23

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *other*

Missing the FT 4-way handshake in the list

SuggestedRemedy

Change: "the 4-Way Handshake, Fast BSS Transition 4-Way Handshake, the Fast BSS Transition protocol&"

Proposed Response *Response Status* **U**

ACCEPT

Cl **05** *SC* **5.8.2.1** *P* **6** *L* **15** # 24

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *other*

Missing the FT 4-way handshake in the sentence

SuggestedRemedy

Change: "A 4-Way Handshake or FT 4-Way Handshake utilizing&"

Proposed Response *Response Status* **U**

ACCEPT

Cl **06** *SC* **6.1.2** *P* *L* # 7

Malinen, Jouni

Comment Type **TR** *Comment Status* **X** *TKIP*

This is in reference to my comment (CID 31, CommentID 308) in the initial sponsor ballot. The proposed text "The use of TKIP as a pairwise cipher when using Fast BSS Transition is deprecated. TKIP was designed as a temporary solution with a limited lifetime and it is unsuitable for new deployments." is clearly mentioning that TKIP is not suitable for _new_ deployments. As such, I cannot agree with the reason given to reject this comment ("There are existing deployments that cannot support AES but would benefit from Fast BSS Transition."). My proposed change was avoiding limiting _existing_ deployments. Furthermore, this kind of deprecation of TKIP does not prevent it from being used in existing deployments, it is just making it clear that the task group acknowledges potential security issues with TKIP and makes them known to the users of the standard. I believe it is the duty of the group to make sure that this kind of warning is provided in the standard taken into account the current knowledge of attacks against TKIP construction.

SuggestedRemedy

Add following paragraph to the end of 6.1.2 (just after the paragraph that deprecates WEP): "The use of TKIP as a pairwise cipher when using Fast BSS Transition is deprecated. TKIP was designed as a temporary solution with a limited lifetime and it is unsuitable for new deployments."

Proposed Response *Response Status* **U**

REJECT.
This comment is a resubmission of a previous comment by this commenter. The previous resolution is unchanged, as the commenter has not provided any additional information to sway the decision of the resolution group.

Cl **07** *SC* **7.3.2.46** *P* **16** *L* **16** # 61

Stanley, Dorothy V

Comment Type **TR** *Comment Status* **X** *Scope*

"Current mesage number" is a duplicate definition of "RSC value", and is not needed

SuggestedRemedy

Change from "The RSC field gives the current message number for the GTK, to allow a STA" to "Delivery of the RSC field value allows a STA"

Proposed Response *Response Status* **U**

REJECT
The text referenced in the comment is not a proper subject of this recirculation ballot. This comment should be forwarded to TGmb during the next revision of the standard

Cl **07** *SC* **7.3.2.49** *P* **17** *L* **54** # 2

Malinen, Jouni

Comment Type **E** *Comment Status* **X** *Editor*

Typo

SuggestedRemedy

Replace "element.." with "element." (remove extra period).

Proposed Response *Response Status* **C**

ACCEPT

Cl **07** *SC* **7.3.2.49** *P* **17** *L* **56** # 25

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *other*

The definition of "Variable parameters" is missing from this clause.

SuggestedRemedy

Add a definition on page 18, line 20: "Variable parameters contains any additonal data based on the resource type"

Proposed Response *Response Status* **U**

ACCEPT

Cl **07** *SC* **7.3.2.49** *P* **18** *L* **10** # 27

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *other*

Are the "optional parameters" defined in Table 7-43f related to the "variable parameters" field in the 7-95y?

SuggestedRemedy

If so, then change the names of one of the entities to match the other - make them consistent.

Proposed Response *Response Status* **U**

ACCEPT
Change to "Variable parameters" in table heading

Cl **07** *SC* **7.3.2.49** *P* **18** *L* **13** # 3

Malinen, Jouni

Comment Type **E** *Comment Status* **X** *Editor*

Typo

SuggestedRemedy

Replace "TImeout" with "Timeout" in the Optional parameters column of Table 7-43f.

Proposed Response *Response Status* **C**

ACCEPT

Cl **08** *SC* **8.4.1.1.2** *P* *L* # 11

Stephens, Adrian P

Comment Type **E** *Comment Status* **X** *Editor*

"thee shall be only one PTKSA"

SuggestedRemedy

thee -> there

Proposed Response *Response Status* **C**

ACCEPT

Cl **08** *SC* **8.4.1.1.2** *P* **23** *L* **34** # 4

Malinen, Jouni

Comment Type **E** *Comment Status* **X** *Editor*

Typo

SuggestedRemedy

Replace "thee shall be" with "there shall be".

Proposed Response *Response Status* **C**

ACCEPT

Cl **08** *SC* **8.4.1.1.2** *P* **23** *L* **34** # 62

Stanley, Dorothy V

Comment Type **ER** *Comment Status* **X** *Editor*

Typo: change "thee" to "there"

SuggestedRemedy

As in comment

Proposed Response *Response Status* **U**

ACCEPT

Cl **08** *SC* **8.4.1.1.2** *P* **23** *L* **34** # 28

Sood, Kapil

Comment Type **ER** *Comment Status* **X** *Editor*

Typo on thee

SuggestedRemedy

Change: "thee" to "there"

Proposed Response *Response Status* **U**

ACCEPT

Cl **08** *SC* **8.4.10** *P* **24** *L* **24** # 29

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *Scope*

"The IEEE 802.1X Controlled Port returns to being blocked. As a result, all data frames are unauthorized before invocation of an MLME-DELETEKEYS.request primitive." - this change seems out-of-scope for this group, as this is not pertinent to 11r. Moreover, the second sentence is ambiguous and even, technically incorrect. The data frames may be valid before invocation of the DELETEKEYS.requst primitive.

SuggestedRemedy

Delete both the sentences. If these are considered within scope of 11r PAR, then either delete the second sentence. OR, change:"As a result of the 802.1X Controlled port being blocked, all data frames are unauthorized before invocation of an MLME-DELETEKEYS.request primitive."

Proposed Response *Response Status* **U**

REJECT
The text referenced in the comment is unchanged text from P802.11-2007, and is not a proper subject of this recirculation ballot. This comment should be forwarded to TGmb during the next revision of the standard.

Cl **08** *SC* **8.4.10** *P* **24** *L* **25** # 63

Stanley, Dorothy V

Comment Type **TR** *Comment Status* **X** *Scope*

The last sentence in the paragraph: "As a result, all data frames are unauthorized before invocation of an MLME-DELETEKEYS.request primitive"
seems to be missing a statement of the beginning of the interval.

SuggestedRemedy

Change to "...are unauthorized after receipt of the MLME Association or Reassociation confirm primitive that is not part of a Fast BSS Transition, MLME Disassociation or Deauthentication primitive and before invocation of an MLME-DELETEKEYS.request primitive."

Proposed Response *Response Status* **U**

REJECT
The text referenced in the comment is unchanged text from P802.11-2007, and is not a proper subject of this recirculation ballot. This comment should be forwarded to TGmb during the next revision of the standard.

Cl **08** *SC* **8.5.1.5.1** *P* **25** *L* **55** # 30

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *other*

The change "Upon a successful authentication, the R0KH shall delete (the) any prior PMK-R0 SA for this Mobility Domain for the supplicant that was just authenticated, and all PMK-R1 SAs (in its possession which were previously created between the S0KH and S1KH and any other R0KH and R1KH in the same Mobility domain) derived from that prior PMK-R0 SA." - this wording is (I believe, unintentionally) removing the distinction of the S0KH and S1KH and makes this statement ambiguous and hence, unimplementable.

SuggestedRemedy

Change on line 54 page 25: "Upon a successful authentication, the R0KH shall delete any prior PMK-R0 SA for this Mobility Domain pertaining to this S0KH. R0KH shall also delete all PMK-R1 SAs derived from that prior PMK-R0 SA."

Proposed Response *Response Status* **U**

ACCEPT

Cl **08** *SC* **8.5.1.5.1** *P* **25** *L* **61** # 31

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *other*

The change introduced in line 56 "for the suplicant that was just authenticated&" is conflicting with the sentence "&PMK-R1 key for a STA, an R1KH&". This conflict makes the draft ambiguous and hence, unimplementable.

SuggestedRemedy

Change on line 61 page 25: "...PMK-R1 key for a S0KH, an R1KH..."

Proposed Response *Response Status* **U**

ACCEPT

Cl **08** *SC* **8.5.1.5.1** *P* **26** *L* **12** # 57

Chaplin, Clint F

Comment Type **ER** *Comment Status* **X** *Editor*

"During a Fast BSS Transition a non-AP STA shall negotiate the same pairwise cipher suite with Target APs, as was negotiated in the FT Initial Mobility Domain association"

SuggestedRemedy

Delete the comma

Proposed Response *Response Status* **U**

ACCEPT

Cl **08** *SC* **8.5.1.5.1** *P* **26** *L* **12** # 65

Stanley, Dorothy V

Comment Type **TR** *Comment Status* **X** *other*

"...a non-AP STA shall negotiate the same pairwise ciphersuite with Target APs as was negotiated in the FT Initial Mobility Domain Association" . How does the target APs validate this? pairwise cipher suite selector is included in the PMKR1 SA.

SuggestedRemedy

Add a sentence along the lines of "The target AP shall verify that the same pairwise cipher suite selector is used, using the pairwise ciphersuite selector value in the PMKR1 SA received form the PMKR0KH."

Proposed Response *Response Status* **U**

ACCEPT

Cl **08** *SC* **8.5.1.5.3** *P* **27** *L* **27** # 8

Malinen, Jouni

Comment Type **TR** *Comment Status* **X** *labels*

PTKR0Name derivation was changed to use the same label ("FT-R0") in the derivation that is used with R0-Key-Data derivation. While I agree that the shorter labels are fine here, I do not like the idea of using the same label in two different derivations. The purpose of this label in the first place is to make sure that the derivations are unique. Even though this particular case uses different constructions (SHA-256 vs. HMAC-SHA256), it would be better to use unique labels.

SuggestedRemedy

Replace "FT-R0" with "FT-R0N" in PMKR0Name construction (page 27 line 27). Replace "0x46542D5230" with "0x46542D52304E" (page 27 line 32).

Proposed Response *Response Status* **U**

ACCEPT

Cl **08** *SC* **8.5.1.5.3** *P* **27** *L* **32** # 53

Chaplin, Clint F

Comment Type **TR** *Comment Status* **X** *labels*

WM: As a result of changing "R0 Key Name" to "FT-R0" in the derivation of R0-Key-Data and PMKR0Name, the string "FT-R0" is defined in both R0-Key-Data and PMKR0Name; none of the other items that are defined in R0-Key-Data are listed after the definition of PMKR0Name

SuggestedRemedy

Delete the "where FT-R0 is&" on line 32, or change the string so that it is distinct from the one defined earlier.

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changed "FT-R0" to "FT-R0N"

Cl **08** *SC* **8.5.1.5.3** *P* **27** *L* **32** # 43

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *labels*

The change to make the keyname labels as the same as the labels used in deriving the key, defeats the purpose of giving individual names to each key/keyname derivation. Key labels are used to unambiguiously determine the use of the derived keys/keynames. Also, I do not see any significant savings (maybe, one round of SHA-256), in reducing the original key name labels "R0 Key Name" with "FT-R0". More so, non-AP STAs do NOT need to compute keynames during FT operation. Overall, I do not see any benefit in reducing label size for key names - It merely blurs the distinct labeling that this draft had, and defeats crypto clarity.

SuggestedRemedy

Revert the changes in 8.5.1.5.3 page 27 lines 28 and 32 to what they were in D7.0. OR, Change "FT-R0" to "R0Name" on page 27 line 28, and on line 32, Change "R0Name is 0x52304e616d65"

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changed "FT-R0" to "FT-R0N"

Cl **08** *SC* **8.5.1.5.3** *P* **27** *L* **9** # 48

Edney, Jonathan

Comment Type **TR** *Comment Status* **X** *labels*

The use of this long integer is confusing or, worse, wrong if encoded using little endianism as is normal for 802.11. This long number format appears here and in the following two clauses.The issue is the text:
"FT-R1" is 0x46542D5231.
(and other similar cases)
By convention a symbol of the form 0xdd..dd where d is a hexadecimal digit is interpreted as a hexadecimal number not a string of octets. A string of octets should be represented by text in quotes or as a list:
0x46 0x54 0x2d 0x52 0x31
If you choose to show the string as a large hexadecimal number (as you have done) then you must either specify the endianism or follow the prevailing convention in the standard (which is little endian.) The text does not specify the endianism and therefore the number shown is incorrect since using little endian interpretation the first octet of the string would be encoded as 0x31.

SuggestedRemedy

Clarify endianism or (better) show this as a string of octets

Proposed Response *Response Status* **U**

ACCEPT
Changed to "0x46 0x54 0x2d 0x52 0x31.
Similar change to other uses of these hexidecimal string definitions.

Cl **08** *SC* **8.5.1.5.4** *P* **27** *L* **59** # 9

Malinen, Jouni

Comment Type **TR** *Comment Status* **X** *labels*

PTKR1Name derivation was changed to use the same label ("FT-R1") in the derivation that is used with PMK-R1 derivation. While I agree that the shorter labels are fine here, I do not like the idea of using the same label in two different derivations. The purpose of this label in the first place is to make sure that the derivations are unique. Even though this particular case uses different constructions (SHA-256 vs. HMAC-SHA256), it would be better to use unique labels.

SuggestedRemedy

Replace "FT-R1" with "FT-R1N" in PMKR1Name construction (page 27 line 59). Replace "0x46542D5231" with "0x46542D52314E" (page 27 line 65).

Proposed Response *Response Status* **U**

ACCEPT

Cl **08** *SC* **8.5.1.5.4** *P* **27** *L* **59** # 44

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *labels*

The change to make the keyname labels as the same as the labels used in deriving the key, defeats the purpose of giving individual names to each key/keyname derivation. Key labels are used to unambiguiously determine the use of the derived keys/keynames. Also, I do not see any significant savings (maybe, one round of SHA-256), in reducing the original key name labels "R1 Key Name" with "FT-R1". More so, non-AP STAs do NOT need to compute keynames during FT operation. Overall, I do not see any benefit in reducing label size for key names - It merely blurs the distinct key/keyname labeling that this draft had, and defeats crypto clarity.

SuggestedRemedy

Revert the changes in 8.5.1.5.4 page 27 lines 59 and 65 to what they were in D7.0. OR, Change "FT-R1" to "R1Name" on page 27, line 59, and on line 32, Change "R1Name is 0x52314e616d65"

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changed "FT-R1" to "FT-R1N"

Cl **08** *SC* **8.5.1.5.4** *P* **27** *L* **65** # 54

Chaplin, Clint F

Comment Type **TR** *Comment Status* **X** *labels*

WM: As a result of changing "R1 Key Name" to "FT-R1" in the derivation of PMK-R1 and PMKR1Name, the string "FT-R1" is defined in both PMK-R1 and PMKR1Name; none of the other items that are defined in PMK-R1 are listed after the definition of PMKR1Name

SuggestedRemedy

Delete the "where FT-R1 is&" on line 65, or change the string so that it is distinct from the one defined earlier.

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changed "FT-R1" to "FT-R1N"

Cl **08** *SC* **8.5.1.5.5** *P* **29** *L* **3** # 10

Malinen, Jouni

Comment Type **TR** *Comment Status* **X** *labels*

PTKName derivation was changed to use the same label ("FT-PTK") in the derivation that is used with PTK derivation. While I agree that the shorter labels are fine here, I do not like the idea of using the same label in two different derivations. The purpose of this label in the first place is to make sure that the derivations are unique. Even though this particular case uses different constructions (SHA-256 vs. HMAC-SHA256), it would be better to use unique labels.

SuggestedRemedy

Replace "FT-PTK" with "FT-PTKN" in PTKName construction (page 29 line 3). Replace "0x46542D50544B" with "0x46542D50544B4E" (page 29 line 10).

Proposed Response *Response Status* **U**

ACCEPT

Cl **08** *SC* **8.5.1.5.5** *P* **29** *L* **4** # 45

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *labels*

The change to make the keyname labels as the same as the labels used in deriving the key, defeats the purpose of giving individual names to each key/keyname derivation. Key labels are used to unambiguiously determine the use of the derived keys/keynames. Also, I do not see any significant savings (maybe, one round of SHA-256), in reducing the original key name labels "PTK Name" with "FT-PTK". More so, non-AP STAs do NOT need to compute PTK keynames during FT operation. Overall, I do not see any benefit in reducing label size for key names - It merely blurs the distinct key/keyname labeling that this draft had, and defeats crypto clarity.

SuggestedRemedy

Revert the changes in 8.5.1.5.5 page 29 lines 4 and 10 to what they were in D7.0. OR, Change "FT-PTK" to "PTKName" on page 29, line 4, and on line 10, Change "PTKName is 0x50544b4e616d65"

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changed "FT-PTK" to "FT-PTKN"

Cl **08** *SC* **8.5.1.5.5** *P* **29** *L* **9** # 55

Chaplin, Clint F

Comment Type **TR** *Comment Status* **X** *labels*

WM: As a result of changing "PTK Name" to "FT-PTK" in the derivation of PTK and PTKName, the string "FT-PTK" is defined in the derivation of both PTK and PTKName; none of the other items that are defined in PTK are listed after the definition of PTKName

SuggestedRemedy

Delete the "where FT-PTK is&" on line 9, or change the string so that it is distinct from the one defined earlier.

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changed "FT-PTK" to "FT-PTKN"

Cl **10** *SC* **10.3.34** *P* **41** *L* **1** # 50

Chaplin, Clint F

Comment Type **ER** *Comment Status* **X** *Editor*

WM: P802.11k D9.0 deleted their insertion of 10.3.33

SuggestedRemedy

change 10.3.34 to 10.3.33, and renumber all following

Proposed Response *Response Status* **U**

ACCEPT

Cl **10** *SC* **10.3.35.1.1** *P* **45** *L* **62** # 32

Sood, Kapil

Comment Type **ER** *Comment Status* **X** *Editor*

typo on SMA

SuggestedRemedy

Change "SMA" to "SME"

Proposed Response *Response Status* **U**

ACCEPT

Cl **10** *SC* **10.3.35.1.1** *P* **45** *L* **62** # 5

Malinen, Jouni

Comment Type **ER** *Comment Status* **X** *Editor*

Typo

SuggestedRemedy

Replace "SMA of an AP" with "SME of an AP".

Proposed Response *Response Status* **U**

ACCEPT

Cl **10** *SC* **10.3.35.1.1** *P* **45** *L* **63** # 64

Stanley, Dorothy V

Comment Type **ER** *Comment Status* **X** *Editor*

Typo, chang e"SMA" to "SME"

SuggestedRemedy

As in comment

Proposed Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.1** *P* **52** *L* **39** # 33

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *Scope*

Not just any "STA" - this should be a non-AP STA

SuggestedRemedy

Change page 52 lines 39, 41: "STA" to "non-AP STA"

Proposed Response *Response Status* **U**

REJECT
The text referenced in the comment is not a proper subject of this recirculation ballot. This comment should be forwarded to TGmb during the next revision of the standard

Cl **11A** *SC* **11A.10** *P* **93** *L* **14** # 12

Montemurro, Michael

Comment Type **T** *Comment Status* **R** *RRB*

This clause defines an L2 mechanism for passing remote request/response messages over-the-DS between AP's. L2 mechanisms are not sufficient to address possible AP infrastructures where the AP's may be reachable, but not have connectivity over L2.

SuggestedRemedy

Replace this clause and subclauses with text that describes generically how FT remote request/response messages can be passed over-the-DS as well as the requirements for a protocol to facilitate over-the-DS transitions.

Response *Response Status* **C**

REJECT.

This comment was WITHDRAWN by the commenter.

Comment was withdrawn by the submitter

Cl **11A** *SC* **11A.10.3** *P* **95** *L* **5** # 13

Montemurro, Michael

Comment Type **T** *Comment Status* **R** *Version number*

Does 11r need a version number for remote request/response?

SuggestedRemedy

If so, add one to the table and specify in the text that it has a value of 0.

Response *Response Status* **C**

REJECT.

This comment was WITHDRAWN by the commenter.

Comment was withdrawn by the submitter

Cl **11A** *SC* **11A.11.2** *P* **97** *L* **44** # 26

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *RIC example*

How is this RIC Descriptor IE used when one resource type (w/o IE) like BlockAck needs to be requested - there is no example.

SuggestedRemedy

Add an example: On page 97 line 44 insert: "An example of a RIC with a RIC Descriptor IE is given in Figure XX. This indicates that the target AP can acknowledge if the resource specified in the RIC Descriptor IE is available." Insert a Figure XX as a row with 2 columns. First column will contain the RDIE, and seconf column will contain a RIC Descriptor IE

Proposed Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.2.2** *P* **54** *L* **4** # 34

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *other*

"&within the SME of a STA" - is incorrect, as R0KH and R1Kh are within the SME of the AP, not any STA.

SuggestedRemedy

Change: "&occur within the SME."

Proposed Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.2.2** *P* **55** *L* **3** # 6

Malinen, Jouni

Comment Type **TR** *Comment Status* **X** *other*

"authentication between the STA and AS" is both confusing (STA could be AP or non-AP STA) and inconsistent (AS is an IEEE 802.1X element and it is authenticating with Supplicant).

SuggestedRemedy

Replace "authentication between the STA and AS" with "authentication between the Supplicant and AS".

Proposed Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.4.2** *P* **56** *L* **64** # 35

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *Scope*

Not just any "STA" - this should be a non-AP STA. Comment based on text affected by changed text.

SuggestedRemedy

Change "STA" to "non-AP STA"

Proposed Response *Response Status* **U**

REJECT
The text referenced in the comment is not a proper subject of this recirculation ballot. This comment should be forwarded to TGmb during the next revision of the standard

Cl **11A** *SC* **11A.4.2** *P* **57** *L* **6** # 36

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *Scope*

Not just any "STA" - this should be a non-AP STA. Comment based on text affected by changed text.

SuggestedRemedy

Change page 57 lines 6, 10, 13, 20, 40, 51, 54, 55: "STA" to "non-AP STA"

Proposed Response *Response Status* **U**

REJECT
The text referenced in the comment is not a proper subject of this recirculation ballot. This comment should be forwarded to TGmb during the next revision of the standard

Cl **11A** *SC* **11A.4.3** *P* **59** *L* **4** # 37

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *Scope*

Not just any "STA" - this should be a non-AP STA. Comment based on text affected by changed text.

SuggestedRemedy

Change page 59 lines 4, 35, 43, 48 : "STA" to "non-AP STA"

Proposed Response *Response Status* **U**

REJECT
The text referenced in the comment is not a proper subject of this recirculation ballot. This comment should be forwarded to TGmb during the next revision of the standard

Cl **11A** *SC* **11A.5.2** *P* **61** *L* **6** # 38

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *Scope*

Not just any "STA" - this should be a non-AP STA. Comment based on text affected by changed text.

SuggestedRemedy

Change page 61 lines 6, 22, 64: "STA" to "non-AP STA"

Proposed Response *Response Status* **U**

REJECT
The text referenced in the comment is not a proper subject of this recirculation ballot. This comment should be forwarded to TGmb during the next revision of the standard

Cl **11A** *SC* **11A.5.2** *P* **62** *L* **1** # 39

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *Scope*

Not just any "STA" - this should be a non-AP STA. Comment based on text affected by changed text.

SuggestedRemedy

Change page 62 lines 1, 4, 6, 8, 16, 58, :"STA" to "non-AP STA".

Proposed Response *Response Status* **U**

REJECT
The text referenced in the comment is not a proper subject of this recirculation ballot. This comment should be forwarded to TGmb during the next revision of the standard

Cl **11A** *SC* **11A.5.3** *P* **64** *L* **1** # 40

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *latency of pull*

The error status: "If the AP has not determined whether the PMKR0Name is valid (e.g., key distribution is done via a "pull" model, and the AP does not wait for the PMK-R1 key from the R0KH), the AP may respond to the FT Request with status code 0." - While a rare possibility of using this can be understood for 0ver-the-air, there is no rationale for using this over-the-DS. The non-AP STA has not switched channels for doing over-the-DS, so it can better tolerate the delays in an attempt to get a more concrete response.

SuggestedRemedy

Delete this sentence. OR, if the group decides that they prefer symmetry for over-the-air and over-the-DS, then delete this sentence and the same sentence in 11A.5.2, page 61, line 44.

Proposed Response *Response Status* **U**

ACCEPT
Both statements deleted

Cl **11A** *SC* **11A.5.4** *P* **65** *L* **35** # 41

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *Scope*

Not just any "STA" - this should be a non-AP STA. Comment based on text affected by changed text.

SuggestedRemedy

Change page 65 line 35, 55, 60, 63, 64:"STA" to "non-AP STA"

Proposed Response *Response Status* **U**

REJECT
The text referenced in the comment is not a proper subject of this recirculation ballot. This comment should be forwarded to TGmb during the next revision of the standard

Cl **11A** *SC* **11A.5.5** *P* **66** *L* **37** # 42

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *Scope*

Not just any "STA" - this should be a non-AP STA. Comment based on text affected by changed text.

SuggestedRemedy

Change page 66 line 37, 60, 63:"STA" to "non-AP STA". Change on line 54, page 66: "MAC address of non-AP STA".

Proposed Response *Response Status* **U**

REJECT
The text referenced in the comment is not a proper subject of this recirculation ballot. This comment should be forwarded to TGmb during the next revision of the standard

Cl **11A** *SC* **11A.6** *P* **67** *L* **1** # 58

Epstein, Joseph

Comment Type **TR** *Comment Status* **X** *reservation protocol*

The necessity, given the overhead, of the six-message resource reservation scheme is still in doubt.

SuggestedRemedy

Remove this section.

Proposed Response *Response Status* **U**

REJECT.
This issue was dealt with in a previous ballot, where a response was provided. The commentor has not provided any new information to sway the decision of the resolution group.

Cl **11A** *SC* **11A.6.3** *P* **65** *L* **20** # 66

Amann, Keith

Comment Type **GR** *Comment Status* **X** *reassociation deadline*

This is a resubmittal of a previous comment. The original comment was "The state diagram indicates that the 'Reassociation Deadline Time' is not to be exceeded by the station in attempting to move from the authentication steps to the association step. This time is apparently defined by the target AP. By having this timeout value defined by the AP it forces all stations to conform to the same requirement, even though they each may have a different 'view' of how their individual traffic needs to be delivered, and when it might be feasible to perform the (re)association step. In fact, it is conceivable that an AP could configure this parameter such that some stations/applications simply can't work."
I suggested two remedies to the problem. The response I received was as follows:
ACCEPT IN PRINCIPLE.
The Reassociation Deadline is provided to the STA during the Initial Mobility Domain Association, and is consistent across the Mobility Domain. This is essentially equivalent to your second alternative. The value is protected by a MIC, which deals with the potential security issues.
The problem with this response is that it is stating what appears to be a fact with regard to the consistency of the Reassociation deadline across the mobility domain, yet in clause 11A.4.2, page 58, line 39 (I'm referencing the redline document, which appears to be the only one available at the moment), there is a note that states "NOTE 2-- It is assumed by this standard that the Reassociation Deadline is administered consistently across the Mobility
Domain.". An assumption is not a statement of fact, or a requirement.

SuggestedRemedy

If the intent is that the reassociation deadline shall be consistent across the mobility domain then state that as a matter of fact, and a requirement of this standard. I believe this means that the referenced "note" needs to be removed, and text stating that this is a requirement needs to be added. I don't know where the best location is to add that text, and will leave it to the sponsor to determine.

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changed "Note 1" to "Note" on page 58 line 37.
Changed "Note 2" and the remainder of that paragraph to normal textual paragraph that states "It is assumed by this standard that the Reassociation Deadline is administered to be consistend across the Mobility Domain. The mechanism for such consistent administration is outside the scope of this standard."

Cl **7,4,7,1** *SC* **7,4,7,1** *P* **18** *L* **60** # 60

Stanley, Dorothy V

Comment Type **ER** *Comment Status* **X** *Scope*

Delete "in order"

SuggestedRemedy

Proposed Response *Response Status* **U**

REJECT
The text referenced in the comment is not a proper subject of this recirculation ballot. This comment should be forwarded to TGmb during the next revision of the standard

Cl **A** *SC* **A** *P* **104** *L* **37** # 56

Chaplin, Clint F

Comment Type **TR** *Comment Status* **X** *RRB*

WM: Addition of the optional vendor-specific protocol for AP-AP communication in 11A.10 should be reflected in the PICS

SuggestedRemedy

Insert a new PICS entry PC35.14.1, Remote Request/Response frame support, 11A.10.3, PC35.14:O, Y-N-N/A. Insert another new PICS entry PC35.14.2, Vendor-specific Remote Request Broker mechanism, 11A.10.3, PC35.14:O, Y-N-N/A. Change PICS entry PC35.14 to *PC35.14.

Proposed Response *Response Status* **U**

ACCEPT.

Cl **Introdu** *SC* **Introduction (page iii)** *P* **3** *L* **41** # 17

Sood, Kapil

Comment Type **TR** *Comment Status* **X** *Editor*

Ambiguous use of "STA" and "station" - these should be non-AP STA

SuggestedRemedy

Change: "The Fast BSS transition time is the total transition time that starts after the receipt of the last acknowledged data frame sent within an originating BSS by the non-AP STA and ends after the receipt
of the first acknowledged data frame sent within the destination BSS, while the non-AP STA transitions from one
BSS to another using the Fast BSS Transition mechanisms."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE
The "last acknowledged data frame" and the "first acknowledged data frame" may be sent in either direction. But the STA making the transition is a non-AP STA.
Changed to "after the receipt of the last acknowledged data frame sent within an originating BSS and ends after receipt of the first acknowledged data frame sent within the destination BSS, while the non-AP STA transitions."

All comments on the frontmatter are editorial.

This comment would normally be considered out of scope of this recirculation ballot, since it does not refer to changed text in D8.0. However, the entire frontmatter is deleted in generating the next revision of the standard. Resubmission of this comment during the next revision of the standard is not possible.

Cl **Particip** *SC* **Participants** *P* *L* **54** # 1

Malinen, Jouni

Comment Type **GR** *Comment Status* **X** *Contributors*

(this applies to page "v", but myBallot does not allow this page number to be entered)
The security experts are claimed to have reviewed "this document" while most of them reviewed an earlier draft (D5.0) which has since then been modified in the area of security, e.g., by re-introducing TKIP.. It would be better not to claim that the persons listed here reviewed the final version of 802.11r amendment. Furthermore, I don't see much need for separating different classes of contributors to the TGr. There are now three (or actually four, if counting the asterisk marking). These lists could be collapsed into a single list of contributors.

SuggestedRemedy

At minimum, change "security experts reviewed this document" to "security experts reviewed an earlier draft of this document", but I would actually suggest to just get rid of this separate category completely and merge all three lists of contributors into a single list (and remove the asterisks from the first list) of contributors. The new list could be titled "The following individuals made contributions to this document:".

Proposed Response *Response Status* **U**

ACCEPT
All contributors merged into a single list