Cl **00** *SC* **0** *P* *L* # 276

Chaplin, Clint F

Comment Type **TR** *Comment Status* **A** *Crypto-agility*

I also wonder if enough consideration has been given to "crypto-agility"--that is, to the possibility that it may at some point become necessary to replace one or more of the specific cryptographic algorithms used in the protocol. I assume that there are enough version numbers buried in the protocol that a new version could easily be made backward compatible. But even where the spec mandates specific algorithms for interoperability reasons, such as the PRF and MIC calculations, it might be worthwhile to consider adding algorithm (or algorithm suite) identifiers in those places, to allow for easier revision if necessary in the future.
(From the security review of Dan Simon)

SuggestedRemedy

See comment

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
P802.11r has defined a mechanism to provide "crypto-agility" through the AKM suite selector in the RSN information element. This was added in D6.0, and was not present in the version submitted for external security review.

Cl **00** *SC* **0** *P* *L* # 137

Chaplin, Clint F

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

People who submitted security reviews need to be acknowledged as contributors. (submitted by Bill Marshall)

SuggestedRemedy

Include another three-column list on page v, at line 52, "The following security experts reviewed this document:" Include in the list Bill Burr, Charles Clancy, Katrin Hoeper, and Scott Kelly.

Response *Response Status* **U**

ACCEPT.

Cl **00** *SC* **0** *P* *L* # 288

Chaplin, Clint F

Comment Type **TR** *Comment Status* **A** *Compromised AP*

In the event that an Access Point is completely compromised or a "rogue" Access Point is able to enter a Mobility Domain, it appears that this would be a major compromise of the whole Mobility Domain. In particular, any AP can get access to any PMKR1 from the AS and thus spoof communication with any Mobile Station. Thus one bad AP can disrupt the whole network. For efficiency and deployment reasons, this architecture might be favored over more secure ones. However, potential users of 802.11r should be aware of the consequences of a compromise of any access point.
From the revised security review of John Mitchell

SuggestedRemedy

See Comment

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
The text in 11A.2.2 specifies requirements for the authentication of potential R1KHs before that R1KH may receive any keys. Even if one R1KH is compromised, it cannot obtain the keys for other R1KHs. Any statements beyond this are outside the scope of 802.11.

Cl **00** *SC* **0** *P* *L* # 287

Chaplin, Clint F

Comment Type **TR** *Comment Status* **R** *Security Review*

Also, due to the same reason, the first message seems to provide an "oracle" for eavesdroppers, that identifies the next location of a Mobile Station - since the first message is not MAC'd, an attacker could spoof this message in response to which the AP will reveal the R1KH-ID. If the first message is MAC'd then this scenario is prevented.
From the revised security review of John Mitchell

SuggestedRemedy

See Comment

Response *Response Status* **U**

REJECT
While it is technically feasible to protect the first message of the Fast BSS Transition exchange, we have chosen not to do so. Even if the first message were to contain a MIC, the content is still visible and still an "oracle". If an attacker were to spoof the first message, the target AP will reveal the R1KH-ID, which is also avaiable for the probing by any unauthenticated STA.

Cl **00** *SC* **0** *P* *L* # 286

Chaplin, Clint F

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

Since the first two messages are unsecured, they could be spoofed. Further, a denial-of-service attack could be mounted by flooding AP2 with bogus authentication requests. AP2 would have to cache the nonces, and possibly have to talk to the AS to get key information. Note that injecting custom 802.11r messages is likely to be more than just a theoretical attack, as suggested by a recent presentation on 802.11 security testing [1].
From the revised security review of John Mitchell

SuggestedRemedy

See Comment

Response *Response Status* **U**

REJECT
While it is technically feasible to protect the first message of the Fast BSS Transition exchange, we have chosen not to do so. Even if the first message were to contain a MIC, the content is still visible and still an "oracle". If an attacker were to spoof the first message, the target AP will reveal the R1KH-ID, which is also avaiable for the probing by any unauthenticated STA.

Cl **00** *SC* **0** *P* *L* # 281

Chaplin, Clint F

Comment Type **TR** *Comment Status* **R** *Security Review*

The first message seems to provide an "oracle" for eavesdroppers, that identifies the location of a Mobile Station.
(From the security review of John Mitchell)

SuggestedRemedy

See comment

Response *Response Status* **U**

REJECT
While it is technically feasible to protect the first message of the Fast BSS Transition exchange, we have chosen not to do so. Even if the first message were to contain a MIC, the content is still visible and still an "oracle". If an attacker were to spoof the first message, the target AP will reveal the R1KH-ID, which is also avaiable for the probing by any unauthenticated STA.

Cl **00** *SC* **0** *P* *L* # 280

Chaplin, Clint F

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

In the event that an Access Point is completely compromised or a "rogue" Access Point is able to enter a Mobility Domain, what capabilities would an attacker have? It would appear that this would be a major compromise of the whole Mobility Domain.
(From the security review of John Mitchell)

SuggestedRemedy

See comment

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
The text in 11A.2.2 specifies requirements for the authentication of potential R1KHs before that R1KH may receive any keys. Even if one R1KH is compromised, it cannot obtain the keys for other R1KHs. Any statements beyond this are outside the scope of 802.11.

Cl **00** *SC* **0** *P* *L* # 279

Chaplin, Clint F

Comment Type **TR** *Comment Status* **A** *Security Review*

Since the first two messages are unsecured, they could be spoofed. Further, a denial-of-service attack could be mounted by flooding AP2 with bogus authentication requests. AP2 would have to cache the nonces, and possibly have to talk to the AS to get key information. Note that injecting custom 802.11r messages is likely to be more than just a theoretical attack, as suggested by a recent presentation on 802.11 security testing.
L. Butti. Wi-Fi Advanced Fuzzing. Black Hat Europe, 2007.
https://www.blackhat.com/presentations/bh-europe-07/ Butti/Presentation/bh-eu-07-Butti.pdf.
(From the security review of John Mitchell)

SuggestedRemedy

See comment

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
We acknowledge that this is a potential attack, and implementations need to be resistant to flooding and similar attacks. The existing 802.11-2007 security mechanism is already susceptible to similar denial-of-service attacks. To our knowledge, this amendment introduces no new types of vulnerabilities beyond the existing 802.11-2007. In addition, unlicensed spectrum is always susceptible to denial-of-service attacks through radio interference.

Cl **00** *SC* **0** *P* *L* # 277

Chaplin, Clint F

Comment Type **TR** *Comment Status* **A** *Key distribution*

When handling a Mobile Station transition, AP2 must be able to get access to the PMKR1 associated with the station. How is this handled? Pulled by AP2 from the AS, and then cached?
(From the security review of John Mitchell)

SuggestedRemedy

See comment

Response *Response Status* **U**

ACCEPT
This comment reflects a request by the external security reviewer for explanatory information. This information was provided by the TGr chair. No text changes.

Cl **00** *SC* **0** *P* *L* # 275

Chaplin, Clint F

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

My only recommendation would be to expand the labels in the key derivations to include the string, "802.11r", or some equivalent. That way, if somebody decides to reuse the same keys for some other purpose, there's no danger of a collision.
(From the security review of Dan Simon)

SuggestedRemedy

See comment

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Include "FT" in all of the labels.

Cl **00** *SC* **0** *P* *L* # 274

Chaplin, Clint F

Comment Type **TR** *Comment Status* **R** *MIC message 2*

One other area of concern is the lack of a MIC on the Authentication Response message, or the second message in the FT protocol exchange. The Target AP has the necessary fields to obtain or compute the PMK-R1. I assume the reason there is no MIC is due to latency concerns. However, this phase of the FT protocol is less susceptible to latency, as only the third and fourth messages of the FT protocol are in the critical path. By not including a MIC, a malicious AP can provide a false ANonce and R1KH-ID. A STA uses these values to essentially pre-authorize a Target AP before initiating a transition, and make a final decision about whether or not to transition to that AP. The transition would eventually fail, but the STA has wasted time in the critical path by transitioning to an invalid Target AP. Adding a MIC to the Authentication Response message would prevent this.
(From the security review of Charles Clancy)

SuggestedRemedy

See comment

Response *Response Status* **U**

REJECT
When a "pull" model is used for key distribution, the protocol is designed to allow the AP to respond to the Authentication Request without waiting for the key to arrive from the R0KH. In such cases, the AP will not have the necessary information to generate a MIC. All of the critical contents of the Authentication Request are repeated in the third message of the exchange, when they are covered by the MIC.

Cl **00** *SC* **0** *P* *L* # 273

Chaplin, Clint F

Comment Type **TR** *Comment Status* **R** *Key distribution*

IEEE 802.11r offers a sound cryptographic foundation for a fast transition protocol, but in and of itself has a few gaps. These gaps need to be filled in by higher-layer protocols. Another gap is the lack of a transport protocol for moving PMK-R1s from the R0-KH to the R1-KH. The decision that this should be an L3 protocol makes it outside the scope of the IEEE 802.11r specification, but will have serious impact on future interoperability in a multi-vendor AP environment. IEEE 802.11r-D5 specifies a set of security requirements for the protocol, and this is an obvious first start. Other options could include:
" Specification of a protocol without a transport: The 802.11r protocol could specify more of the protocol, at a variety of levels of detail. For example, it could define key transport payloads and require a secure transport (such as TLS or DTLS). Alternatively, it could define a secure key transport protocol based on key wraps, and assume a pre-existing security association. Finally, it could define an entire cryptographic protocol, along with the necessary portions for establishing an initial security association. With all this defined, it would be relatively easy to then publish an RFC to perform the actual L3 transport.
" Another option would be to have the STA perform the key distribution. The authorization phase could be between the STA and PMK-R0 (possibly brokered by a local AP), and the authorization response could contain the PMK-R1 wrapped with a key known only to the target AP. This wrapped key could then be included in the re-association message from the STA to the target AP. Again, there is the difficulty of establishing the pairwise security associations between the R0-KHs and R1-KHs that could either be in-scope or out of scope for this document.
I suspect all these options were considered by TGr during the document's development, and the minimalistic approach was deemed the best. There are a variety of IETF protocols that would be well suited to tackle the key distribution problem at L3, by implementing the necessary set of security associations, including Kerberos and AAA. Kerberos could be used to provision service tickets between PMK key holders, and then keys could be wrapped and transported between APs. Alternatively, it is likely there will be a pre-existing AAA infrastructure due to the EAP involvement, and that could also be leveraged to move keys between authenticators by implementing some sort of KDC/caching AAA service.
(From the security review of Charles Clancy)

SuggestedRemedy

See comment

Response *Response Status* **U**

REJECT
We wish to thank the commenter for their comment. TGr has considered each of these alternatives. In the end we decided the key distribution protocol would not be defined since the market need is for STA-to-AP interoperability rather than AP-AP interoperability.

Cl **00** *SC* **0** *P* *L* # 272

Chaplin, Clint F

Comment Type **TR** *Comment Status* **A** *Channel Bindings*

IEEE 802.11r offers a sound cryptographic foundation for a fast transition protocol, but in and of itself has a few gaps. These gaps need to be filled in by higher-layer protocols. The first is a lack of complete channel bindings. By advertising both IEEE 802.11 and AAA identities to the peer, and binding them into the cryptographic key derivation, the functionality is there, but it is up to EAP to fill in the gaps. At a minimum, EAP methods need to securely convey the NAS ID of the authenticator to the STA during the EAP authentication. This would in effect delegate authorization to the authenticator to use the EAP MSK for whatever purpose it wanted. Even better would be for key scope and context information for the MSK to be transported to the STA, so the STA would know how the MSK should be used by the authenticator. This could, for example, even dictate SSIDs, BSSIDs, ciphersuites, etc, that the peer is authorized to use the MSK for, depending on the policy of the network.
(From the security review of Charles Clancy)

SuggestedRemedy

See comment

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
To the extent that this is a problem with the existing EAP methods, it is out of scope of 802.11 and is a problem to be addressed by IETF. P802.11r has required the R0KH-ID as the NAS-Identifier to be used if the EAP method supports Channel Binding.

Cl **00** *SC* **0** *P* *L* # 270

Chaplin, Clint F

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

PTK and Pairwise transient Keys (KCK, KEK, TK) Discussion
" Output length PTKLen depends on negotiated CS. From Table 60 in Section 8.5.2 in core document: CCMP (128 bits), TKIP (256), WEP-40 (40), WEP-104 (104)
Hence PTK is 128, 256, 40, or 104 bits long. This is not long enough to derive the pairwise transient keys (KCK, KEK,TK) with
KCK = L(PTK, 0, 128), KEK = L(PTK, 128, 128), TK = L(PTK, 256, 128)
The described derivation of KCK, KEK, TK (Section 8.5.1.5.5) requires
PTK>= 3* 128 bits. However PTK<= 256 bits and thus never sufficiently long!
This is clearly a mistake in the description!
(From the security review of Bill Burr)

SuggestedRemedy

See comment

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
PTKLen depends on the negotiated cipher suite (as stated in the document). More specifically, it is 256+length(TK). However, use of PTKLen is confusing with only a single defined cipher from 8.5.2.
At page 24 line 25 changed cross reference from "Table 60" to "Table 8-2".
At page 24 line 54 inserted "For vendor specific cipher suites, the length of TK (and the value of PTKLen) depend on the vendor specific algorithm."

Cl **00** *SC* **0** *P* *L* # 269

Chaplin, Clint F

Comment Type **TR** *Comment Status* **R** *Security Review*

PMK-R1 Discussion
" Asymmetry in name derivation compared to PMK-R0
(From the security review of Bill Burr)

SuggestedRemedy

See comment

Response *Response Status* **U**

REJECT
At this point the group does not see any new vulnerability being introduced into the protocol by virtue of this asymmetry.

Cl **00** *SC* **0** *P* *L* # 268

Chaplin, Clint F

Comment Type **TR** *Comment Status* **R** *Security Review*

PMK-R0 Discussion
" Here KDF-384 is used, as opposed to KDF-256 as for the other keys. This is done to generate 128 bits as salt for the key identifier. Does this asymmetry introduce any security problems?
(From the security review of Bill Burr)

SuggestedRemedy

See comment

Response *Response Status* **U**

REJECT
At this point the group does not see any new vulnerability being introduced into the protocol by virtue of this asymmetry.

Cl **00** *SC* **0** *P* *L* # 265

Chaplin, Clint F

Comment Type **TR** *Comment Status* **A** *Security Review*

Broadcasted beacons of APs that support FT within the mobility domain contain some additional information about the mobility domain and the FT capabilities of the AP. This additional information is contained in a Mobility Domain Information Element (MDIE).
Beacon signals (by nature) cannot be protected and are thus vulnerable to Denial of Service (DoS) attacks. The new MDIE element enables the following DoS attacks:
1. Adversary changes bit indicating the FT ability of an AP to zero.
In that case, STAs won't request FT even though it is supported by the AP. Instead the STA will execute a full re-association and authentication. Hence, an adversary modifying the beacon can disable the FT feature.
This may not be detectable. (?)
2. Adversary changes bit indicating the FT ability of an AP to one.
In that case, a STA may request FT from an AP that does not offer this service.
This will be detected by the AP which results into an error code 54 ("invalid MDIE").
3. Adversary changes advertised FT capabilities of AP.
Detected if STA requests services that are not provided with error code 54, not detected if STA does not request FT due to wrong information in beacon.
Conclusions: no severe security risk. However, we should note that an adversary may be able to disable the FT service.
(From the security review of Bill Burr)

SuggestedRemedy

See comment

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
We acknowledge that this is a potential attack, and implementations need to be resistant to similar attacks. The contents of the MDIE from the Beacon are repeated in the FT authentication exchange, where they are covered by a MIC. The existing 802.11-2007 security mechanism is already susceptible to similar denial-of-service attacks. To our knowledge, this amendment introduces no new types of vulnerabilities beyond the existing 802.11-2007. In addition, unlicensed spectrum is always susceptible to denial-of-service attacks through radio interference.

Cl **00** *SC* **0** *P* *L* # 278

Chaplin, Clint F

Comment Type **TR** *Comment Status* **A** *Security Review*

The first two messages are NOT MAC'd or encrypted. They are sent within 802.11 "management frames", which are known to be unsecured. This is being addressed by the 802.11w group, which is supposed to finalize a spec by the middle of next year. If this is not already being done, making use of 802.11w encrypted management frames would add to the security of 802.11r.
(From the security review of John Mitchell)

SuggestedRemedy

See comment

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
The first two messages cannot be protected as they are exchanged prior to key establishment. P802.11w will protect the Action frames for over-the-DS Fast BSS Transitions.

Cl **00** *SC* **0** *P* *L* # 264

Chaplin, Clint F

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

People who submitted security reviews need to be acknowledged as contributors.

SuggestedRemedy

Include another three-column list on page v, at line 52, "The following security experts reviewed this document:" Include in the list Bill Burr, Charles Clancy, Anupam Datta, Katrin Hoeper, Srinivas Inguva, Scott Kelly, John C. Mitchell, Arnab Roy, Dan Simon.

Response *Response Status* **U**

ACCEPT.

Cl **00** *SC* **0** *P* *L* # 266

Chaplin, Clint F

Comment Type **TR** *Comment Status* **A** *KDF specification*

(KDF defined in Section 8.5.1.5.2)
" Format of used KDF same as in SP800-108, KDF in counter mode with prf=HMAC-SHA-256 and HMAC-256 considered being secure
" Is there KDF standard or guideline that can be cited?
" Encoding essential for KDF computations: i and length encoded according to Section 7.1.1 in core document. Hence, 802.11r must specify encoding for K, label, and content. In document encoding for "label" is explicitly described, however explicit encoding for key K and context missing.
(From the security review of Bill Burr)

SuggestedRemedy

See comment

Response *Response Status* **U**

ACCEPT
Inserted text at end of final paragraph in 8.5.1.5.2 "K, label, and Context are bit strings, and are represented using the ordering conventions of 7.1.1."

If SP800-108 is published during the Sponsor Ballot period of this amendment, we will include a reference to it.

Cl **00** *SC* **0** *P* *L* # 271

Chaplin, Clint F

Comment Type **TR** *Comment Status* **A** *Key distribution*

Based on my limited review, I also think the overall design is quite solid from a security perspective. I have
only one security-related concern, and that relates to the attempt to completely punt on R0KH-R1KH
communications security. Here is the current text from section 11A.2.2:
"The R0KH and the R1KH are assumed to have a secure channel between them that can be used to
exchange cryptographic keys without exposure to any intermediate parties. This standard assumes that the
key transfer includes the PMK-R1, the PMK-R1 context, and the associated key authorizations. The protocol
for distribution of keying material from the R0KH to the R1KH is outside the scope of this standard."
I understand that the 11r group does not want to design a capwap-like protocol, and I agree that such a
protocol should remain outside the scope of this work. Also, I don't know how thoroughly this sort of thing is
typically covered in other IEEE documents. However, were this an IETF document, I think most in the
security directorate would agree that the current text comes up short.
I won't attempt to rewrite the text myself, but I think it would be good if the text addressed the following:
- - cryptographic "impedence": the cryptographic properties of the key exchange channel must be greater
than or equal to the cryptographic properties of the channels for which the keys will be used. That is, if the
802.11i keys are for AES-CCM, then the crypto-integrity mechanism employed for the distribution channel
should be of similar (or better) strength.
- - if digital certificates are used for 802.1X (i.e. as part of the 802.11i key derivation, for example EAP-TLS),
then I think the ROKH-R1KH authentication should arguably be similarly strong. A simple way to sum this
and the previous bullet up is to say that the key distribution channel must not be the weak link in the security
chain. Otherwise, that is where attackers will aim.
Of course, it is not always possible to say whether one algorithm is stricly equivalent to (or stronger than)
another in every way, and it's easy to get into rathole discussions on this point. However, it is possible to
communicate the spirit of the concern without getting into this (e.g. see RFC 3776).
I think it would be a good thing if the text contained stronger language regarding the security requirements of

this key distribution channel and the associated risks.
(From the security review of Scott Kelly)

SuggestedRemedy

See comment

Response *Response Status* **U**

ACCEPT
Inserted text at page 50 line 16, after first sentence, "The cryptographic strength of the secure channel between the R0KH and R1KH is assumed to be greater than or equal to the cryptographic strength of the channels for which the keys will be used". Inserted text at page 50 line 27, "The cryptographic strength of the authentication is assumed to be greater than or equal to the cryptographic strength of the authentication between the STA and AS."

Cl **00** *SC* **0** *P* *L* # 267

Chaplin, Clint F

Comment Type **TR** *Comment Status* **A** *Security Review*

PMK-R0 Discussion
" What is R0KH-ID = identifier of PMK-R0 holder in authenticator? Specification needed for proper encoding and computation.
The identifier is probably the NAS address of the authenticator; however this is not mentioned here!
(From the security review of Bill Burr)

SuggestedRemedy

See comment

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
The definition of R0KH-ID is given in 11A.2.2. Text has been added in the definition of the kdf function that defines this as a bit string.

Cl **00** *SC* **0** *P* **0** *L* **0** # 317

Coordination, Editorial

Comment Type **GR** *Comment Status* **A**

Please submit seperate file for figures, if they weren't created in Framemaker.

SuggestedRemedy

Response *Response Status* **U**

ACCEPT.

Cl **00** *SC* **0** *P* **0** *L* **27** # 1

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

pre-auth & key-caching are not necessarily coupled
(Originally LB98/21 submitted by Ciotti, Frank, during LB98 with ID Ciotti/09)

SuggestedRemedy

Change text from:
"pre-authentication and key caching"
to:
"pre-authentication or key caching"

Response *Response Status* **C**

ACCEPT.

Cl **00** *SC* **0** *P* **0** *L* **30** # 2

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Typo
(Originally LB98/22 submitted by Ciotti, Frank, during LB98 with ID Ciotti/10)

SuggestedRemedy

"Install the key" --> "Install the keys"

Response *Response Status* **C**

ACCEPT.

Cl **00** *SC* **0** *P* **0** *L* **41** # 3

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

Basing the definition of FT time on acknowledged data frames could be a problem if the Q-STA is also (or only) sending data frames with the ack policy set to "no ack".
(Originally LB98/23 submitted by Ciotti, Frank, during LB98 with ID Ciotti/11)

SuggestedRemedy

Consider changing:
"transmission of the last/first acknowledged data frame"
to:
"receipt of the last/first data frame"

Response *Response Status* **C**

ACCEPT.

Cl **00** *SC* **0** *P* **1** *L* **18** # 135

Chaplin, Clint F

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

title incorrect, should be "specifications" (plural) (submitted by Bill Marshall)

SuggestedRemedy

change "specification" to "specifications"

Response *Response Status* **U**

ACCEPT.

Cl **00** *SC* **0** *P* **49** *L* **25** # 294

Edney, Jonathan

Comment Type **TR** *Comment Status* **A** *Security assumptions*

Clause 11A.2.2: This clause is very poorly written and should be revised or deleted. Here is a list of problems:
Line 26: "R1KH in the AP" This is the only place where it says the R1KH is in the AP and implies a constraint of implementation. I do not think this is intended
Line 30: "R0KH interacts with 802.1X": 802.1X is a standard and not capable of interaction with equipment
Line 30: 1st sentence: what does this mean? How can the R0KH receive the EAP authentication result via 802.1X. I just don't understand this sentence
Line 40: What is the intent of this statement? How could they derive the PTK non-mutually? Does it mean that have to do it at the same moment in time? I don't think that is intended - so what is?
Line 45: "Each key holder name is mapped to a physical entity in the DS where it resides" Earier it said that the keyholders were part of the SME on the STA which is not part of the DS. So what is meant here?
Line 52: "R0KH shall be co-resident..." What does "co-resident" mean. This is not a defined term and yet this is a normative statement. Does it mean in the same mechanical box? Running of the same processor? In the same building? I have no idea
Page 50: Line 5: "..shall provide the IEEE802.11 Authenticator function.." What is this? I understand 802.1X authenticator function but I am not familiar with this. It is not a defined term that I know.
Page 50:line 13: Typo "dot11FTR0eyHolderID"
Page 50: paragraph at line 17 seems to be pretty redundant with paragraph at line 23

SuggestedRemedy

Most of this clause is unhelpful, unecessary or redundant with other clauses. I feel that the whole clause should be reviewed to extract only the pertenent information for the standard and then this should be re-presented

Response *Response Status* **U**

ACCEPT
Page 49 line 26, deleted "in the AP"
Page 49 line 30, change "802.1X" to "the IEEE 802.1X Authenticator"
Page 49 line 31, change "with 802.1X" to "with the IEEE 802.1X Authenticator" (twice on this line)
Page 49 line 40, change "The R1KH shall derive the PTK mutually with the S1KH" to "The R1KH and S1KH each derive the PTK."
Page 49 line 46, delete "Each key holder name is mapped to a physical entity in the DS where it resides.
Page 49 line 52, change "co-resident" to "co-located"
Page 50 line 5, delete "provide the IEEE 802.11 Authenticator function to" (leaving "shall derive and distribute the GTK...")
typo fixed.
Page 50 line 17 is stating different requirements than the paragraph at line 23.

Cl **00** *SC* **0** *P* **50** *L* **63** # 295

Edney, Jonathan

Comment Type **E** *Comment Status* **A**

Clause 11A.3: talks about "setting...Fast BSS Transition over DS"

SuggestedRemedy

insert the word "field" or similar to clairfy meaning

Response *Response Status* **C**

ACCEPT.

Cl **00** *SC* **0** *P* **51** *L* **35** # 319

Hansen, C J

Comment Type **TR** *Comment Status* **R** *Initial MD Association*

Initial association should not require 4-way handshake.

SuggestedRemedy

Modified over-the-air fast BSS transition protocol can be employed. The 802.1X/EAP exchange can occur between the FT 802.11 Authentication exchange and the FT 802.11 Reassociation exchange, using data frames with ToDS = 0, FromDS = 0 for EAPOL-Key messages.

Response *Response Status* **U**

REJECT
Multiple alternatives were considered for the initial authentication, including this mechanism. The chosen result was selected because it reused many of the existing RSN mechanisms. Further, the focus of TGr is on the transitions, and the initial association is not a transition within the Mobility Domain.

Cl **00** *SC* **0** *P* **51** *L* **35** # 316

Ptasinski, Henry S

Comment Type **TR** *Comment Status* **R** *Initial MD Association*

Remove dependency on 802.11i 4-way handshake for initial association.

SuggestedRemedy

Use modified over-the-air fast BSS transition protocol instead. 802.1X/EAP exchange can occur between FT 802.11 Authentication exchange and FT 802.11 Reassociation exchange, using data frames with ToDS = 0, FromDS = 0 for EAPOL-Key messages.

Response *Response Status* **U**

REJECT
Multiple alternatives were considered for the initial authentication, including this mechanism. The chosen result was selected because it reused many of the existing RSN mechanisms. Further, the focus of TGr is on the transitions, and the initial association is not a transition within the Mobility Domain.

Cl **00** *SC* **0** *P* **61** *L* **23** # 318

Hansen, C J

Comment Type **TR** *Comment Status* **R** *reservation protocol*

The resource request protocol is adds extra time to the fast transition setup, and is unable to provide any service guarantees. It's benefits are dubious.

SuggestedRemedy

Remove.

Response *Response Status* **U**

REJECT
The 6-message exchange is critical in some deployments of Fast BSS Transition, specifically carrier grade deployments that use HCCA and high bandwidth/low jitter tolerance data streams, to accomodate TSPEC processing.

Cl **00** *SC* **0** *P* **61** *L* **23** # 315

Ptasinski, Henry S

Comment Type **TR** *Comment Status* **R** *reservation protocol*

Resource Request protocol is overly complex, adds extra processing time to the "fast transition" setup, and is unable to provide any service guarantees.

SuggestedRemedy

Delete the protocol.

Response *Response Status* **U**

REJECT
The 6-message exchange is critical in some deployments of Fast BSS Transition, specifically carrier grade deployments that use HCCA and high bandwidth/low jitter tolerance data streams, to accomodate TSPEC processing.

Cl **00** *SC* **0** *P* **97** *L* **37** # 136

Chaplin, Clint F

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

MIB variable wrong (submitted by Bill Marshall)

SuggestedRemedy

change "SpectrummanagementTable" to "SpectrumManagementTable"

Response *Response Status* **U**

ACCEPT.

Cl **01** *SC* **1** *P* **1** *L* **29** # 132

Kays, Ruediger

Comment Type **E** *Comment Status* **A**

Reference should be made to 802.11k-D8.0

SuggestedRemedy

change reference to
"(based on P802.11k-D8.0)"

Response *Response Status* **C**

ACCEPT.

Cl **02** *SC* **2** *P* **1** *L* **49** # 143

Mccann, Stephen

Comment Type **E** *Comment Status* **R**

The initial reference "FIPS PUB 180-2-2002" appears to be rather weak. Could a full title and date be also added

SuggestedRemedy

Add the full title of this reference and publication date

Response *Response Status* **C**

REJECT.
This reference follows the style used in 802.11-2007, specifically "FIPS PUB 180-1-1995, Secure Hash Standard." 802.11-2007 includes a footnote providing information for acquiring copies of FIPS publications.

Cl **03** *SC* **3** *P* **2** *L* **27** # 6

CHAPLIN, CLINT F

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

Add a definition of the "FT 4-Way Handshake" as this term has been used frequently in this specification. The definition of "4-Way Handshake" in 802.11-REVma9.0 can be used as a guide.
(Originally LB98/26 submitted by Sood, Kapil, during LB98 with ID Sood/046)

SuggestedRemedy

Insert "3.XX FT 4-Way Handshake: A pairwise key management protocol used when Fast BSS Transition is enabled. This handshake confirms mutual possession of a pairwise master key (PMK-R1) by two parties and distributes a group temporal key (GTK)"
Editor: Please number XX appropriately.

Response *Response Status* **U**

ACCEPT.

Cl **03** *SC* **3** *P* **2** *L* **37** # 134

Kays, Ruediger

Comment Type **T** *Comment Status* **A**

Numbers 3.95a already used in 802.11k D8.0

SuggestedRemedy

Change "3.95a" to "3.95b".
Change "3.95b" to "3.95c"

Response *Response Status* **C**

ACCEPT.
All other changes made in P802.11k in D8.0 (and 802.11-2007) also tracked in P802.11r.

Cl **03** *SC* **3.54b** *P* **2** *L* **23** # 5

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

"The first association or reassociation procedure&" is confusing. It implies that we either do a first association, or a (first/second/any) reassociation. This is not the intent of the definition. It is an association procedure or a reassociation procedure, in which the result is that the STA is associated with the AP.
(Originally LB98/25 submitted by Sood, Kapil, during LB98 with ID Sood/010)

SuggestedRemedy

Change "first association or reassociation procedure" to "first association procedure"
OR,
Change "first association or reassociation procedure" to "first association or first reassociation procedure"

Response *Response Status* **C**

ACCEPT.
Changed to "first association or first reassociation:

Cl **03** *SC* **3.89a** *P* **2** *L* **34** # 133

Kays, Ruediger

Comment Type **E** *Comment Status* **A**

Number 3.89a is already used in 802.11k-D8.0

SuggestedRemedy

Not possible in this draft, if alphabetic order has to be kept

Response *Response Status* **C**

ACCEPT.
Changed 3.89a to "3.89-5" and added an Editorial Note below explaining the required action

Cl **03** *SC* **3.99** *P* **2** *L* **7** # 4

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

"PMK-R1 value" is redundant.
(Originally LB98/24 submitted by Sood, Kapil, during LB98 with ID Sood/009)

SuggestedRemedy

Change "PMK-R1 value" to "PMK-R1".

Response *Response Status* **C**

ACCEPT.

Cl **04** *SC* **4** *P* **3** *L* **56** # 7

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Missing PMKR0Name and PMKR1Name abbreviations in this list
(Originally LB98/46 submitted by Sood, Kapil, during LB98 with ID Sood/013)

SuggestedRemedy

Add abbreviations for "PMKR0Name First level Pairwise Master Key name" and "PMKR1Name Second level Pairwise Master Key Name" to this list

Response *Response Status* **C**

ACCEPT IN PRINCIPLE.
PMKR0Name is not an acroynm. PMKR1Name is also not an acronym. Neither is PTKName. For consistency, PTKName deleted from clause 4.

Cl **05** *SC* **5** *P* *L* # 321

Malinen, Jouni

Comment Type **GR** *Comment Status* **A** *Clause5*

IEEE 802.11r adds number of security features into RSNA, but Clause 5 has not been updated to show a generic description of these additions. This leaves the standard in somewhat conflicting state or at last may leave the reader not get a good highlevel view on RSNA based on reading through the general description clause. IEEE 802.11r should update Clause 5 to describe the new features added to RSNA.

SuggestedRemedy

Insert following item into the end of the feature list in the beginning of 5.2.3.2:
- Fast BSS transition mechanism
Insert following paragraph to the end of 5.2.3.2:
"An RSNA using fast BSS transition relies on an external protocol to distribute keys between R0KH/R1KH Authenticator components. The requirements for this protocol are described in 11A.2.2."
In the third paragraph of 5.4.3.1, replace "IEEE 802.11 defines two authentication methods: Open System authentication and Shared Key authentication." with "IEEE 802.11 defines three authentication methods: Open System authentication, Shared Key authentication, and Fast BSS Transition authentication." Insert following sentence into the same paragraph before the last sentence ("The IEEE 802.11 authentication..."): "Fast BSS Transaction authentication relies on keys derived during the initial mobility domain association to authenticate the stations as defined in Clause 11A."
In 5.4.3.4, replace "provide fresh keys by means of protocols called the 4-Way Handshake and Group Key Handshake" with "provide fresh keys by means of protocols called the 4-Way Handshake, Group Key Handshake, FT 4-Way Handshake, FT protocol, and FT resource request protocol".
Add a new clause, 5.4.3.7 Fast BSS Transaction with following text:
"The fast BSS transaction mechanism defines means for setting up security and QoS parameters prior to re-association to a new AP. This allows time-consuming operations to be removed from the time-critical reassociation process."
In 5.8.1, replace "IEEE 802.11 depends upon IEEE 802.1X and the 4-Way Handshake and Group Key Handshake, described in Clause 8" with "IEEE 802.11 depends upon IEEE 802.1X and the 4-Way Handshake, Group Key Handshake, FT 4-Way Handshake, FT protocol, and FT resource request protocol, described in Clause 8 and Clause 11A".

Response *Response Status* **U**

ACCEPT.

Cl **05** *SC* **5** *P* **4** *L* **25** # 138

Chaplin, Clint F

Comment Type **TR** *Comment Status* **A** *Clause5*

Some introductory text is needed in clause 5 (submitted by Bill Marshall)

SuggestedRemedy

In 5.4.2.1, change list item (b) to read "BSS-transition: This type is defined as a station movement from one BSS in one ESS to another BSS within the same ESS. A Fast BSS transition is a BSS transition that establishes the state necessary for data connectivity before the reassociation rather than after the reassociation"

Response *Response Status* **U**

ACCEPT.

Cl **05** *SC* **5.4.2.1** *P* **4** *L* **25** # 296

Montemurro, Michael

Comment Type **T** *Comment Status* **A** *Clause5*

There should be a short description of Fast BSS-Transition in this clause.

SuggestedRemedy

Add the following text to this subclause as a new paragraph following the first paragraph: The Fast BSS-Transition protocol provides a mechanism for a non-AP STA to perform a BSS-Transition between access points in an RSN, or when QoS Admission Control is enabled in the ESS.

Response *Response Status* **C**

ACCEPT.

Cl **05** *SC* **5.4.3.4** *P* **4** *L* **25** # 297

Montemurro, Michael

Comment Type **T** *Comment Status* **A** *Clause5*

The Fast-BSS Transition protocol adds an additional mechanism to establish a new security association.

SuggestedRemedy

Modify the second sentence of the first paragraph of 5.4.3.4 as follows: The procedures defined in this standard provide fresh keys by means of protocols called
the 4-Way Handshake, the Fast BSS-Transition protocol, and Group Key Handshake.

Response *Response Status* **C**

ACCEPT.

Cl **05** *SC* **5.8** *P* **4** *L* **25** # 298

Montemurro, Michael

Comment Type **T** *Comment Status* **A** *Clause5*

The Fast-BSS Transition protocol adds an additional mechanism to establish a new security association.

SuggestedRemedy

Modify the first sentence of the second paragraph of clause 5.8.1 as follows: IEEE Std 802.11 depends upon IEEE Std 802.1X-2004 and the 4-Way Handshake, the Fast BSS-Transition protocol, and Group Key
Handshake, described in Clauses 8 and 11A, to establish and change cryptographic keys.

Response *Response Status* **C**

ACCEPT.

Cl **05** *SC* **5.8.2.1** *P* **4** *L* **25** # 299

Montemurro, Michael

Comment Type **T** *Comment Status* **A** *Clause5*

The Fast-BSS Transition protocol adds an additional mechanism to establish a new security association.

SuggestedRemedy

Add the following text after the second bullet of the second paragraph: "- In the case of Fast BSS-Transition, derive PMK-R0 and PMK-R1 keys.

Response *Response Status* **C**

ACCEPT.

Cl **05** *SC* **5.8.2.1** *P* **5** *L* **25** # 300

Montemurro, Michael

Comment Type **T** *Comment Status* **A** *Clause5*

The Fast-BSS Transition protocol adds an additional mechanism to establish a new security association.

SuggestedRemedy

Modify the third bullet of the second paragraph as follows: -- Derive a fresh pairwise transient key (PTK) from the PMK, or the PMK-R1 in the case of Fast BSS-Transition.

Response *Response Status* **C**

ACCEPT.

Cl **06** *SC* **6.1.2** *P* *L* # 320

Malinen, Jouni

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

802.11r introduces a new authentication exchange (FT protocol) which is described in Clause 11A. However, 6.1.2 was not updated to point to this clause.

SuggestedRemedy

Modify the third paragraph of 6.1.2 by adding a reference to Clause 11A: replace "During the authentication exchange, both parties exchange authentication information as described in Clause 8" with "During the authentication exchange, both parties exchange authentication information as described in Clause 8 and Clause 11A."

Response *Response Status* **U**

ACCEPT.

Cl **06** *SC* **6.1.2** *P* *L* # 308

Malinen, Jouni

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

IEEE 802.11r/D7.0 seems to allow TKIP to be negotiated as a pairwise cipher with FT. However, TKIP was designed as a temporary solution with limited lifetime and we have already reached the estimated end of that lifetime. While use of TKIP as a group cipher may be needed to allow smooth transition to more secure solutions, use of TKIP as the pairwise cipher for new deployments should be deprecated.

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." More general deprecation of TKIP for IEEE 802.11 or strict requirement of not allowing it to be negotiated for FT would also be an acceptable way of addressing this comment.

Response *Response Status* **U**

REJECT
There are existing deployments that cannot support AES but would benefit from Fast BSS Transition.

Cl **07** *SC* **7** *P* **14** *L* **26** # 142

Chaplin, Clint F

Comment Type **TR** *Comment Status* **A** *RIC format*

RIC as defined can only describe resources that are defined by information elements, such as QoS resources. It can't define non-IE resources, such as Block Ack settings. The definition of RDIE needs to be extended so that this additional functionality can be negotiated between a STA and the target AP prior to Reassociation. (submitted by Bill Marshall)

SuggestedRemedy

In Figure 7-95x, add two fields after "Status Code", named "Resource Type" and "Optional Parameters". Change paragraph below Figure 7-95x to "The length field for this element indicates the length of the information field, as defined below.". At end of 7.3.2.48, insert "The Resource Type is one of the values from Table 43f. Optional parameters are present as indicated in Table 43f." Table 43f - Resource type codes in RIC Data information element. Columns "Resource type value", "Meaning", and "Optional parameters". Row 1: "0 - Reserved - None". Row 2: "1 - 802.11 QoS - None; RDIE is followed by TSPEC, TCLAS, and TCLAS Processing information elements, as described in 11A.11.2". Row 3: "2 - Block Ack - Sequences of Block Ack Parameter Set, Block Ack Timeout Value, and Block Ack Starting Sequence Control, as described in 11A.11.2". In 11A.11.2, page 89 line 20, change "Each Resource Descriptor consists of one or more information elements" to "Each Resource Descriptor is either included in the RDIE or in one or more information elements following the RDIE." Change entry in Table 11A-3 for QoS Resource Descriptor Definition to prepend "Resource Descriptor is contained in separate information elements following the RDIE." Insert second row with Resource Type "Block Ack Parameters", Resource Descriptor definition "Resource Descriptor(s) are contained in the RDIE. In a request: Block Ack Parameter Set field (see 7.3.1.14) followed by Block Ack Timeout Value (see 7.3.1.15), followed by Block Ack Starting Sequence Control (see 7.2.1.7). In a response: Block Ack Parameter Set field (see 7.3.1.14) followed by Block Ack Timeout Value (see 7.3.1.15)." Notes "Resource request procedures shall be as given in 11.5."

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Add new subclause 7.3.2.49, "Resource Information Container Descriptor", text "The Resource Information Container Descriptor information element is used with an RDIE to negotiate resources during a Fast BSS Transition that are not otherwise described by information elements. See 11A.11 for procedures for including this information element into a RIC. Figure 7-95x shows this information element." Figure 7-95x, "Resource Information Container Descriptor information element", with fields "Element ID" (1 octet), "Length" (1 octet), "Resource Type" (1 octet), "Variable parameters" (variable). Text below figure "The length field is set to the number of octets in this information element (variable).<p>The Resource type field contains one of the values given in Table 7-43f:". Table 7-43f - Resource type codes in RIC Descriptor information element. Columns "Resource type value", "Meaning", and "Optional parameters". Row 1: "1 - Block Ack - Block Ack Parameter Set as defined in 7.3.1.14, Block Ack Timeout Value as defined in 7.3.1.15, and Block Ack Starting Sequence Control as described in 7.2.1.7"; Row 2: "0, 2-255 - Reserved - Reserved". Insert new row in Table 7-26, Information element "Resource Information Container Descriptor", Element ID "<ANA>", and Length "3-257". Insert row after "QoS" in Table 11A-3 with Resource Type "Block Ack Parameters", Resource Descriptor definition "In a request: Resource Information Container Descriptor (see 7.3.2.49), containing a Resource Type field identifying Block Ack. In a response: Resource Information Container Descriptor (see 7.3.2.49), containing a Resource Type field identifying Block Ack." Notes "Resource request procedures shall be as given in 11.5."

Cl **07** *SC* **7.3.2.45** *P* **10** *L* **63** # 8

CHAPLIN, CLINT F

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

The text refers to the "Fast BSS Transition Capability and Policy field" in Figure 112q. However, the label on Figure 112q is Fast BSS transition capability and policy value". The capitalisation is inconsistent and the use of "value" instead of "field" is inconsistent (Originally LB98/147 submitted by Myles, Andrew, during LB98 with ID Mtles/10)

SuggestedRemedy

Change "value" to "field" and make capitalisation consistent

Response *Response Status* **U**

ACCEPT.
Figure 112q title changed to "Fast BSS Transition Capability and Policy field"

Cl **07** *SC* **7.3.2.45** *P* **11** *L* **4** # 151

Sood, Kapil

Comment Type **TR** *Comment Status* **A** *DIE indication of FT capability*

"Over the Air" is always the natural mechanism by which an AP and a STA can interact. Having worked closely with WLAN roaming implementation design of 2 very large IT organizations, I have not found any usage where "over the air" will ever be disabled in their deployments. I do not see any other usage that will benefit by disabling this over-the-air mechanism. I do not see this capability adding any value, and find it extraneous.

SuggestedRemedy

Remove Bit B0 from the Fast BSS transition capability and policy value in Fig 7-95. Clause 11A.3, pg 50-51, change "The Fast BSS Transition capability is advertised in the Beacon and Probe Response frames by including the MDIE. Fast BSS Transition over DS may be set to one in the MDIE. The MDIE is advertised in the Beacons and Probe Response frames to indicate the MDID, Fast BSS Transition capability, and the Fast BSS Transition Policy." Clause 11A.3, pg 51, lines 5-10, change "The Mobility Domain Identifier shall be the value of dot11FTMobilityDomainID. The Fast BSS Transition policy bits in the MDIE, Fast BSS Transition over DS, and Resource request
protocol capability, shall be set according to the values of the MIB variables dot11FTOverDSEnabled, and dot11FTResourceRequestSupported, respectively." Annex D, pg 101 line 26-37, delete lines 26-37 MIB entry for dot11FTOverAirEnabled. Annex D, pg 100 line 41, delete line "dot11FTOverAirEnabled Truthvalue,". Clause 11A.5.2 pg 55 line 61 delete lines 61-62.

Response *Response Status* **U**

ACCEPT

Cl **07** *SC* **7.3.2.45** *P* **11** *L* **4** # 326

Sood, Kapil

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

"Over the Air" is always the natural mechanism by which an AP and a STA can interact. Having worked closely with WLAN roaming implementation design of 2 very large IT organizations, I have not found any usage where "over the air" will ever be disabled in their deployments. I do not see any other usage that will benefit by disabling this over-the-air mechanism. I do not see this capability adding any value, and find it extraneous. (This is a revision of similar comment)

SuggestedRemedy

Remove Bit B0 from the Fast BSS transition capability and policy value in Fig 7-95. Clause 11A.3, pg 50-51, change "The Fast BSS Transition capability is advertised in the Beacon and Probe Response frames by including the MDIE. Fast BSS Transition over DS may be set to one in the MDIE. The MDIE is advertised in the Beacons and Probe Response frames to indicate the MDID, Fast BSS Transition capability, and the Fast BSS Transition Policy." Clause 11A.3, pg 51, lines 5-10, change "The Mobility Domain Identifier shall be the value of dot11FTMobilityDomainID. The Fast BSS Transition policy bits in the MDIE, Fast BSS Transition over DS, and Resource request
protocol capability, shall be set according to the values of the MIB variables dot11FTOverDSEnabled, and dot11FTResourceRequestSupported, respectively." Annex D, pg 101 line 26-37, delete lines 26-37 MIB entry for dot11FTOverAirEnabled. Annex D, pg 100 line 41, delete line "dot11FTOverAirEnabled Truthvalue,". Clause 11A.5.2 pg 55 line 61 delete lines 61-62.

Response *Response Status* **U**

ACCEPT

Cl **07** *SC* **7.3.2.46** *P* **11** *L* **64** # 154

Sood, Kapil

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

It is not clear where the number of optional parameters is accounted for, in the FTIE. The Information element count should also include the count of all optional parameters that are included in the FTIE.

SuggestedRemedy

Change Clause 7.3.2.46, pg 11 line 64 "The Information Element Count of the MIC Control field contains the total number of information elements and optional parameters that are included in the MIC calculation."

Response *Response Status* **U**

REJECT.
Optional parameters are included in the length of the FTIE. The Information element count in the MIC Control field is a count of information elements (which counts the FTIE with all of its optional parameters as a single IE).

Cl **07** *SC* **7.3.2.46** *P* **11** *L* **64** # 328

Sood, Kapil

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

It is not clear where the number of optional parameters is accounted for, in the FTIE. The Information element count should also include the count of all optional parameters that are included in the FTIE. (This is a revision of similar comment)

SuggestedRemedy

Change Clause 7.3.2.46, pg 11 line 64 "The Information Element Count of the MIC Control field contains the total number of information elements and optional parameters that are included in the MIC calculation."

Response *Response Status* **U**

REJECT.
Optional parameters are included in the length of the FTIE. The Information element count in the MIC Control field is a count of information elements (which counts the FTIE with all of its optional parameters as a single IE).

Cl **07** *SC* **7.3.2.46** *P* **12** *L* **14** # 290

Edney, Jonathan

Comment Type **T** *Comment Status* **A**

Figure 7-95t suggest that only one optional parameter is allowed. Inserting the field show here to Figure 7-95r does not allow for mulotiple optional parameters

SuggestedRemedy

The field show be shown as optionally repeating or this should be clear from the text

Response *Response Status* **C**

ACCEPT.
Change "Optional parameters" in Figure 7-95r to "Optional parameter(s)". Changed page 12 line 9 to "The format of an optional parameter is shown in Figure 7-95t."

Cl **07** *SC* **7.3.2.46** *P* **12** *L* **50** # 153

Sood, Kapil

Comment Type **T** *Comment Status* **A**

TGw D2.1 is using an IGTK with a keyid of 2 octets. This seems to imply that the fields in the GTK sub-element format are inadequate to handle TGw defined IGTK. This needs to be updated to account for 2 octets for Fig 7-95u and 7-95v.

SuggestedRemedy

Change Clause 7.3.2.46, pg 12-13, Figs 7-95u with Key Info length to be 2 and in Fig 7-95v to be 2 octets, as well.

Response *Response Status* **C**

ACCEPT.

Cl **07** *SC* **7.3.2.46** *P* **13** *L* **16** # 291

Edney, Jonathan

Comment Type **T** *Comment Status* **A**

There is inconsistent naming. Fig 7-95u shows a "RSC" and "Key" field but the text here refers to a "Key RSC" field. What field is this?

SuggestedRemedy

Clarify naming in this paragraph

Response *Response Status* **C**

ACCEPT.
Changed "The Key RSC field" to "The RSC field"

Cl **07** *SC* **7.3.2.46** *P* **13** *L* **22** # 127

HEUBAUM, KARL F

Comment Type **E** *Comment Status* **A**

The word "it" is missing in "...for CCMP is the Packet Number (PN)..."

SuggestedRemedy

Change to "...for CCMP it is the Packet Number (PN)..."

Response *Response Status* **C**

ACCEPT.

Cl **07** *SC* **7.3.2.47** *P* **13** *L* **36** # 9

CHAPLIN, CLINT F

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

The description of TI IE is not clear:'specifies various types of time intervals and timeouts" (Originally LB98/175 submitted by Zaks, Artur, during LB98 with ID Zaks/10)

SuggestedRemedy

Define the purpose of this IE in a concise manner.

Response *Response Status* **U**

ACCEPT.
Changed to "specifies time intervals and timeouts."

Cl **07** *SC* **7.3.2.48** *P* **14** *L* **38** # 283

Malinen, Jouni

Comment Type **E** *Comment Status* **A**

Typo

SuggestedRemedy

Replace "to uniquely identifies" with "to uniquely identify".

Response *Response Status* **C**

ACCEPT.

Cl **07** *SC* **7.3.2.48** *P* **14** *L* **38** # 292

Edney, Jonathan

Comment Type **E** *Comment Status* **A**

Typo: "identities" should be "identify"

SuggestedRemedy

Correct typo

Response *Response Status* **C**

ACCEPT.

Cl **07** *SC* **7.3.2.48** *P* **14** *L* **38** # 156

Sood, Kapil

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

Typo "to uniquely identifies"

SuggestedRemedy

Change "to uniquely identify"

Response *Response Status* **U**

ACCEPT.

Cl **07** *SC* **7.3.2.48** *P* **14** *L* **38** # 157

Sood, Kapil

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

The scope of the unique RDIE Identifier should be larger than the current RIC. The reason being that the same number (say, RDIE Id =2) may be used in different resource requests to same AP.

SuggestedRemedy

Change "to uniquely identify the RDIE within the RIC" to "to uniquely identify the RDIE for all resource requests issued by the STA to a specific AP".

Response *Response Status* **U**

REJECT.
Procedures in 11A.11 state that a non-AP STA can only have a single RIC-Request outstanding at an AP, so there is no confusion.

Cl **07** *SC* **7.3.2.48** *P* **14** *L* **38** # 330

Sood, Kapil

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

The scope of the unique RDIE Identifier should be larger than the current RIC. The reason being that the same number (say, RDIE Id =2) may be used in different resource requests to same AP.(This is revision of similar comment)

SuggestedRemedy

Change "to uniquely identify the RDIE within the RIC" to "to uniquely identify the RDIE for all resource requests issued by the STA to a specific AP".

Response *Response Status* **U**

REJECT.
Procedures in 11A.11 state that a non-AP STA can only have a single RIC-Request outstanding at an AP, so there is no confusion.

Cl **07** *SC* **7.3.2.48** *P* **14** *L* **43** # 158

Sood, Kapil

Comment Type **E** *Comment Status* **R**

"Resource Descriptor" sounds too ominous for someone reading this for the first time (or, even 10th!), and gives an impression of yet another complex protocol structure.

SuggestedRemedy

Rename "Resource Descriptor" to "Resource"throughout the draft

Response *Response Status* **C**

REJECT.
"Resource descriptor" is a much more accurate term for the field than "Resource"

Cl **07** *SC* **7.3.2.48** *P* **14** *L* **43** # 331

Sood, Kapil

Comment Type **E** *Comment Status* **R**

"Resource Descriptor" sounds too ominous for someone reading this for the first time (or, even 10th!), and gives an impression of yet another complex protocol structure. (This is revision of similar comment)

SuggestedRemedy

Rename "Resource Descriptor" to "Resource"throughout the draft

Response *Response Status* **C**

REJECT.
"Resource descriptor" is a much more accurate term for the field than "Resource"

Cl **07** *SC* **7.4.7** *P* **14** *L* **64** # 332

Sood, Kapil

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

It is not certain that the action frames will not impact the operation of the link between the STA and AP in any way. In fact, they certainly will impact channel conditions. I do not see what value this subjective statement is adding to the protocol definition.

SuggestedRemedy

Change: "The FT action frames are sent over the air between the STA and the current AP."

Response *Response Status* **U**

ACCEPT.

Cl **07** *SC* **7.4.7** *P* **14** *L* **64** # 159

Sood, Kapil

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

It is not certain that the action frames will not impact the operation of the link between the STA and AP in any way. I do not see what value this subjective statement is adding to the protocol definition.

SuggestedRemedy

Change: "The FT action frames are sent over the air between the STA and the current AP."

Response *Response Status* **U**

ACCEPT.

Cl **07** *SC* **7.4.7** *P* **14** *L* **65** # 10

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

"&do not affect the operation of the link between the STA and the current AP in any way." (the last "in any way" is not needed).
(Originally LB98/196 submitted by Cam-Winget, Nancy, during LB98 with ID Cam-Winget/11)

SuggestedRemedy

Removed "in any way" from this sentence.

Response *Response Status* **C**

ACCEPT.

Cl **07** *SC* **7.4.7** *P* **14** *L* **65** # 11

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

Strictly speaking, FT action frames can affect the operation of the link between the STA and the current AP, so it is not correct to claim them not to affect this "in any way". For example, PwrMgt flag in the frame control field in the action frames could be used to move the STA between power save and awake states. These frames do not change the FT-related parameters at the current AP, but "operation of the link" sounds more general than that.
(Originally LB98/197 submitted by Malinen, Jouni, during LB98 with ID Malinen/12)

SuggestedRemedy

Replace "do not affect the operation of the link between the STA and the current AP in any way" with "do not affect the FT association state between the current AP and the STA".

Response *Response Status* **C**

ACCEPT IN PRINCIPLE.
Changed to "do not affect the state of the link between the STA and the current AP."

Cl **07** *SC* **7.4.7.1** *P* **15** *L* **42** # 128

HEUBAUM, KARL F

Comment Type **E** *Comment Status* **A**

"Frames" in "...for Fast BSS Transition Action Frames." should be lower case

SuggestedRemedy

Change to "...for Fast BSS Transition Action frames."

Response *Response Status* **C**

ACCEPT.

Cl **08** *SC* **8.4.1.1** *P* **18** *L* **52** # 114

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Calling one thing an "FT protocol" and calling another an "FT resource request protocol" implies, at least in my mind, that the second one is a specialization of the first.
However, this is clearly not the case as the text includes "FT protocol or a successful FT resource request protocol".
I believe this will confuse the reader, and any possible confusion in normative text gets my "no" vote.
(Originally LB105/6 submitted by Stephens, Adrian, during LB105 with ID Stephens/09)

SuggestedRemedy

Rename "FT protocol" to "FT <something> protocol" that indicates its special purpose. Consider defining FT protocol as "one of the FT procols, comprising the FT <something> protocol and the FT resource request protocol". And use that term in this subclause and elsewhere where the quoted phrase crops up.

Response *Response Status* **C**

ACCEPT IN PRINCIPLE.
It is intended that the FT resource request protocol be a specialization of the FT protocol, and that is consistently maintained throughout the remainder of the document. Changed "a successful FT protocol or a successful FT resource request protocol" in 8.4.1.1 to "a successful FT authentication sequence" (three places).

Cl **08** *SC* **8.4.1.1** *P* **18** *L* **58** # 12

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

There is a "." after Handshake"
(Originally LB98/212 submitted by Sood, Kapil, during LB98 with ID Sood/020)

SuggestedRemedy

Change "." to ","

Response *Response Status* **C**

ACCEPT.

Cl **08** *SC* **8.4.1.1.1a** *P* **19** *L* **17** # 334

Sood, Kapil

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

"This can include parameters such as the STA's authorized SSID" - The example of STA's authorized SSID is not correct, as SSID shall always be part of the PMK-R0 SA. BTW, what is a "STA's Authorized SSID"? Indicate some other example, if needed. (This is revision of similar comment)

SuggestedRemedy

Delete "This can include parameters such as STA's authorized SSID" and add "- SSID" as first component of the PMK-R0 SA.

Response *Response Status* **U**

ACCEPT.

Cl **08** *SC* **8.4.1.1.1a** *P* **19** *L* **17** # 161

Sood, Kapil

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

"This can include parameters such as the STA's authorized SSID" - The example of STA's authorized SSID is not correct, as SSID shall always be part of the PMK-R0 SA. BTW, what is a "STA's Authorized SSID"? Indicate some other example, if needed.

SuggestedRemedy

Delete "This can include parameters such as STA's authorized SSID" and add "- SSID" as first component of the PMK-R0 SA.

Response *Response Status* **U**

ACCEPT.

Cl **08** *SC* **8.4.1.1.1a** *P* **19** *L* **43** # 335

Sood, Kapil

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

This can include parameters such as the STA's authorized SSID - The example of STA's authorized SSID is not correct, as SSID shall always be part of the PMK-R1 SA. BTW, what is a "STA's Authorized SSID"? Indicate some other example, if needed. (This is revision of similar comment)

SuggestedRemedy

Delete "This can include parameters such as STA's authorized SSID" and add "- SSID" as first component of the PMK-R1 SA.

Response *Response Status* **U**

ACCEPT.

Cl **08** *SC* **8.4.1.1.1a** *P* **19** *L* **43** # 162

Sood, Kapil

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

This can include parameters such as the STA's authorized SSID - The example of STA's authorized SSID is not correct, as SSID shall always be part of the PMK-R1 SA. BTW, what is a "STA's Authorized SSID"? Indicate some other example, if needed.

SuggestedRemedy

Delete "This can include parameters such as STA's authorized SSID" and add "- SSID" as first component of the PMK-R1 SA.

Response *Response Status* **U**

ACCEPT.

Cl **08** *SC* **8.4.1.1.1a** *P* **19** *L* **7** # 160

Sood, Kapil

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

SSID is missing from PMK-R0 SA, but is (correctly) included in the PMK-R0 key derivation

SuggestedRemedy

Add "- SSID" as the first component of the PMK-R0 SA list

Response *Response Status* **U**

ACCEPT.

Cl **08** *SC* **8.4.1.1.1a** *P* **19** *L* **7** # 333

Sood, Kapil

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

SSID is missing from PMK-R0 SA, but is (correctly) included in the PMK-R0 key derivation (This is revision of similar comment)

SuggestedRemedy

Add "- SSID" as the first component of the PMK-R0 SA list

Response *Response Status* **U**

ACCEPT.

Cl **08** *SC* **8.4.1.1.2** *P* **19** *L* **56** # 13

CHAPLIN, CLINT F

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

"There shall be only one PTKSA with the same
Supplicant and Authenticator MAC addresses." is not true for FT. This is because we have defined additional components to be part of the Auth and Suppl, and this statement become ambiguous for FT key hierarchy design.
(Originally LB98/219 submitted by Sood, Kapil, during LB98 with ID Sood/022)

SuggestedRemedy

Change sentence to "For the PTKSA derived as a result of the 4-Way Handshake, there shall be only one PTKSA with the same Supplicant and Authenticator MAC addresses."

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
After requested sentence, also inserted "For the PTKSA derived as a result of an Initial Mobility Domain Association or Fast BSS Transition, there shall be only one PTKSA with the same non-AP STA MAC address and BSSID."

Cl **08** *SC* **8.4.1.1.2** *P* **20** *L* **3** # 14

CHAPLIN, CLINT F

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

The PTKName is missing from the PTKSA.
(Originally LB98/221 submitted by Cam-Winget, Nancy, during LB98 with ID Cam-Winget/16)

SuggestedRemedy

Include PTKName in the PTKSA list.

Response *Response Status* **U**

ACCEPT.
Inserted bullet item "If Fast BSS Transition key hierarchy is used, PTKName"

Cl **08** *SC* **8.4.1.1.2** *P* **20** *L* **3** # 15

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

PTKSA does not include PTKName even though both PMK-R0 and PMK-R1 SAs do include a name for the key. Shouldn't PTKName be added into PTKSA? Then again, PTKName is not really used for anything in the current draft, so it could be removed completely.
(Originally LB98/222 submitted by Malinen, Jouni, during LB98 with ID Malinen/14)

SuggestedRemedy

Either remove PTKName completely (per my comment on 8.5.1.5.5) or add PTKName to the PTKSA by inserting a new item after PTK: "PTKName".

Response *Response Status* **C**

ACCEPT.
Inserted bullet item "If Fast BSS Transition key hierarchy is used, PTKName"

Cl **08** *SC* **8.4.3** *P* **20** *L* **12** # 115

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **R** *TKIP*

Removal of 8.4.3 and related changed in D6.0 brought back TKIP as a fully supported pairwise cipher for FT use. While the other changes were necessary to allow vendor specific ciphers to be used, the part of allowing TKIP as a fully supported cipher does not fit well with the current state of TKIP. TKIP was designed as a temporary solution with a limited lifetime and we are at the end of its designed lifetime. As such, its use in any new amendment is questionable. While it may still be desirable for some deployments to be able to use TKIP, this could be done even if the 802.11 standard were to deprecate TKIPs use. Having some language in 802.11 to discourage the use of TKIP would be a good thing to do now.
(Originally LB105/7 submitted by Malinen, Jouni, during LB105 with ID Malinen/11)

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."

Response *Response Status* **C**

REJECT
There are existing deployments that cannot support AES but would benefit from Fast BSS Transition.

Cl **08** *SC* **8.4.3** *P* **20** *L* **12** # 116

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **R** *TKIP*

In D5.0, 8.4.3 included text that required use of CCMP with FT, specifically prohibiting use of FT with TKIP. As TKIP has passed its design goal, moving past TKIP seems to be the right approach. Change the text to specifically prokibit use of TKIP as the pairwise cipher.
(Originally LB105/8 submitted by Stanley, Dorothy, during LB105 with ID Stanley/09)

SuggestedRemedy

Re-insert the text from 8.4.3 D5.0, and apply the changes suggested by Comment 233: Replace "STA shall use CCMP as the pairwise cipher suite" with "STA shall not use TKIP as the pairwise cipher suite" and replace (on line 50) 'also selects CCMP as the pairwise cipher suite, and reject the association with status code 42 ("Invalid pairwise cipher") if any other cipher suite is selected' with 'does not select TKIP as the pairwise cipher suite, and reject the association with status code 42 ("Invalid pairwise cipher") if TKIP is selected'.

Response *Response Status* **C**

REJECT
There are existing deployments that cannot support AES but would benefit from Fast BSS Transition.

Cl **08** *SC* **8.5.1.1** *P* **20** *L* **50** # 16

CHAPLIN, CLINT F

Comment Type **TR** *Comment Status* **R** *SHA-1 vs SHA-256*

Comment: Changes to remove use of SHA-1 are incomplete
(Originally LB98/243 submitted by Stanley, Dorothy, during LB98 with ID Stanley/09)

SuggestedRemedy

(a) In 8.5.1.1, insert the following text prior to the sentence beginning "In the following"
"When the RSNA Capabilities field B6 is set to 1 in the RSNA information element of both the AP and the non-AP STA, or between peer STAs (for PeerKey derivations) PRF functions are as defined below, where KDF is as defined in 8.5.1.5.2:
PRF-128(K, A, B) = KDF-128(K, A, B, 128)
PRF-192(K, A, B) = KDF-192(K, A, B, 192)
PRF-256(K, A, B) = KDF-256(K, A, B, 256)
PRF-384(K, A, B) = KDF-384(K, A, B, 384)
PRF-512(K, A, B) = KDF-512(K, A, B, 512)
Otherwise, PRF functions are as defined below." In the following&.
(b) In 8.5.1.2, insert the following text prior to the sentence beginning "A PMK identifier is&"
"When the RSNA Capabilities field B6 is set to 1 in the RSNA information element of both the AP and the non-AP STA, a PMK identifier is defined as
PMKID = HMAC-SHA256-128(PMK, "PMK Name" || AA || SPA)
Here, HMAC-SHA256-128 is the first 128 bits of the HMAC-SHA256 of its argument list.
Otherwise, a" PMK identifier is&
(c) In 8.5.1.4, insert the following text prior to the sentence beginning "A PMK identifier is&"
"When the RSNA Capabilities field B6 is set to 1 in the RSNA information element of both peer STAs a SMK identifier is defined as
SMKID = HMAC-SHA256-128(SMK, "SMK Name" || PNonce || MAC_P || INonce || MAC_I)
Here, HMAC-SHA256-128 is the first 128 bits of the HMAC-SHA256 of its argument list.
Otherwise, a" SMK identifier is&

Response *Response Status* **U**

REJECT
The technical opinion obtained from NIST is that SHA-1 is adequate for our uses in a key derivation function.

Cl **08** *SC* **8.5.1.5.1** *P* **21** *L* **58** # 285

Housley, Russell D

Comment Type **E** *Comment Status* **A** *Editor*

The document says:
Upon a successful authentication, the R0KH shall delete the prior PMK-R0 SA 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.
This is very confusing to me. I think the goal is to delete the prior PMK-R0 SA and any SAs that were derived from it that are related to the supplicant that was just authenticated for this Mobility Domain.
These words do not provide this meaning to me.
Part of the confusion comes from STA, Supplicant, S0KH, and S1KH all refering to the same entity in this section.

SuggestedRemedy

Rewite the few sentences.

Response *Response Status* **C**

ACCEPT
Text changed to "Upon a successful authentication, the R0KH shall delete any prior PMK-R0 SA for this Mobility Domain for the supplicant that was just authenticated, and all PMK-R1 SAs derived from that prior PMK-R0 SA."

Cl **08** *SC* **8.5.1.5.1** *P* **22** *L* **13** # 166

Sood, Kapil

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

There is a security flaw in the current key hierarchy. The current design makes it possible for a STA to derive a key hierarchy and then negotiate and use different ciphers as it FTs between different APs in the same MD, using the same key hierarchy. The attack is that the same PMK-R1 is now being used to derive PTKs for different ciphers with different APs. In addition, making a STA behave nicely and consistently is a desirable security practice - it is not the intent of this standard that STAs derive a FT key hierarchy, and then use this same key hierarchy to derive PTK keys for CCMP, then TKIP, then vendor-specific ciphers.

SuggestedRemedy

Insert on pg 22, line 13: "During FT, a non-AP STA shall use the derived FT key hierarchy with the same pairwise cipher suite with Target APs, as was negotiated in the FT Initial Mobility Domain Association." OR "During FT, a non-AP STA shall negotiate the same pairwise cipher suite with the Target AP as was negotiated in the FT Initial Mobility Domain Association." In addition to above, Insert in Clause 11A.5.2 page 57 at end of line 5: "If the non-AP STA selects a pairwise cipher suite in RSNIE that is different from the one it used in FT 4-way handshake, then AP shall reject the Authentication Request with status code 19 ("Invalid Pairwise Cipher")". Insert in Clause 11A.5.3 page 58 at end of line 65: "If the non-AP STA selects a pairwise cipher suite in RSNIE that is different from the one it used in FT 4-way handshake, then AP shall reject the Authentication Request with status code 19 ("Invalid Pairwise Cipher")". Clause 8.4.1.1.1b page 19 line 41 add " - pairwise cipher suite to be used with PMK-R1 key".

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Suggested remedy, with text in 8.4.1.1b "Pairwise cipher suite selector" . Same insertion to 8.4.1.1.1a for PMK-R0 SA.

Cl **08** *SC* **8.5.1.5.1** *P* **22** *L* **13** # 338

Sood, Kapil

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

There is a security flaw in the current key hierarchy. The current design makes it possible for a STA to derive a key hierarchy and then negotiate and use different ciphers as it FTs between different APs in the same MD, using the same key hierarchy. The attack is that the same PMK-R1 is now being used to derive PTKs for different ciphers with different APs. In addition, making a STA behave nicely and consistently is a desirable security practice - it is not the intent of this standard that STAs derive a FT key hierarchy, and then use this same key hierarchy to derive PTK keys for CCMP, then TKIP, then vendor-specific ciphers. (This is revision of similar comment)

SuggestedRemedy

Insert on pg 22, line 13: "During FT, a non-AP STA shall use the derived FT key hierarchy with the same pairwise cipher suite with Target APs, as was negotiated in the FT Initial Mobility Domain Association." OR "During FT, a non-AP STA shall negotiate the same pairwise cipher suite with the Target AP as was negotiated in the FT Initial Mobility Domain Association." In addition to above, Insert in Clause 11A.5.2 page 57 at end of line 5: "If the non-AP STA selects a pairwise cipher suite in RSNIE that is different from the one it used in FT 4-way handshake, then AP shall reject the Authentication Request with status code 19 ("Invalid Pairwise Cipher")". Insert in Clause 11A.5.3 page 58 at end of line 65: "If the non-AP STA selects a pairwise cipher suite in RSNIE that is different from the one it used in FT 4-way handshake, then AP shall reject the Authentication Request with status code 19 ("Invalid Pairwise Cipher")". Clause 8.4.1.1.1b page 19 line 41 add " - pairwise cipher suite to be used with PMK-R1 key".

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Suggested remedy, with text in 8.4.1.1b "Pairwise cipher suite selector" . Same insertion to 8.4.1.1.1a for PMK-R0 SA.

Cl **08** *SC* **8.5.1.5.1** *P* **22** *L* **14** # 117

CHAPLIN, CLINT F

Comment Type **TR** *Comment Status* **R** *Key distribution*

The claim is that key distribution is outside the scope of this draft. Further claims are made in the "resolution" of comment 491 that the IETF has "ongoing" work to define a key distribution protocol. Not only is there no "ongoing" work on this subject there is no plans to address this. If the resolver of comment 491 is referring to the HOKEY working group in the IETF then let it be known that both chairmen of the HOKEY working group as well as both its Area Directors have stated that HOKEY is not doing this, and will not do this.
(Originally LB105/9 submitted by Harkins, Dan, during LB105 with ID Harkins/10)

SuggestedRemedy

This draft is not implementable in a standard fashion by which interoperability between two independent implementations can be assured if there is no definition on how critical data are conveyed to the components that need it-- namely, how a keys get from the R0KH to all R1KHs. Furthermore, by not specifying how the keys are distributed it leaves a gaping security hole which lessens the security of 802.11 and therefore violates the PAR of TGr--see CID 6.

Response *Response Status* **U**

REJECT
From a system point of view, key distribution should be done by a layer three protocol. Any layer three protocol would be out of scope for IEEE 802.11r; the PAR only authorizes MAC changes. Assumed requirements for the key distribution are given in 11A.2.2.

Cl **08** *SC* **8.5.1.5.2** *P* **22** *L* **31** # 17

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Suggested wording
(Originally LB98/277 submitted by Malinen, Jouni, during LB98 with ID Malinen/19)

SuggestedRemedy

Replace "256 bit key" with "256-bit key".

Response *Response Status* **C**

ACCEPT.

Cl **08** *SC* **8.5.1.5.2** *P* **22** *L* **42** # 302

Malinen, Jouni

Comment Type **TR** *Comment Status* **R** *SHA-1 vs SHA-256*

During the TGr adhoc meeting at NIST, use of SHA-1 vs SHA-256 was discussed and the conclusion from that discussion was the SHA-256 is not actually needed for the KDF since SHA-1 is still fine for deriving keys. Taken into account how much more expensive SHA-256 is from CPU usage view point when compared to SHA-1, it would be possible to optimize the 802.11r KDF by changing the KDF to use SHA-1 instead of SHA256. The current SHA-256-based construction can add couple of milliseconds to the transition process when using current low-end WLAN devices (e.g., WLAN VoIP phones). This can increase the time the data connection is down especially when using over-the-air FT protocol.

SuggestedRemedy

Replace use of HMAC-SHA256 with HMAC-SHA1 in the KDF function defined in 8.5.1.5.2: replace "(Length+255)/256" with "(Length+159)/160" on line 40 and "HMAC-SHA256" with "HMAC-SHA1" on line 42).
Furthermore, the use of SHA256 for key name derivation does not look necessary; especially so, since the result is truncated to 128-bits anyway. In order to simplify requirements for new crypto algortihms, use of SHA-256 should be removed from PMKR0Name, PMKR1Name, and PTKName derivations to remove need for SHA-256 altogether in 802.11r. The key name derivations can be changed by replacing "Truncate-128(SHA-256" with "Truncate-128(SHA-1" in 8.5.1.5.3 (page 23, line 25), 8.5.1.5.4 (page 23, line 57), and 8.5.1.5.5 (page 24, line 61). Alternatively, AES-128-CMAC could be used to derive the key names.

Response *Response Status* **U**

REJECT
We are concerned about the political problem of SHA-1 vs SHA-256; that the US Government may overreact to the problems identified in SHA-1 (for its use in certificates) and ban all uses of SHA-1.

Cl **08** *SC* **8.5.1.5.2** *P* **22** *L* **42** # 18

CHAPLIN, CLINT F

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

Adding extra 0x00 after 'label' into KDF() data for HMAC-SHA256() does not seem to add any real value. It is not needed here since 'i' and 'label' are of fixed length. As such, it is just adding extra complexity and making KDF slower.
(Originally LB98/278 submitted by Malinen, Jouni, during LB98 with ID Malinen/20)

SuggestedRemedy

Remove "0x00 ||" from HMAC-SHA256() parameters.

Response *Response Status* **U**

ACCEPT.

Cl **08** *SC* **8.5.1.5.2** *P* **22** *L* **42** # 301

Malinen, Jouni

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

0x00 after label in the HMAC-SHA256 data serves no purpose in KDF. It just makes this more complex to implement and uses more CPU to run derive the keys without any added benefit.

SuggestedRemedy

Delete "0x00 || " from HMAC-SHA256 data in the KDF.

Response *Response Status* **U**

ACCEPT

Cl **08** *SC* **8.5.1.5.2** *P* **22** *L* **42** # 130

Stanley, Dorothy V

Comment Type **TR** *Comment Status* **R** *SHA-1 vs SHA-256*

Use of SHA256 introduces a computational burden on the STA which is not warranted

SuggestedRemedy

Change to use HMAC-SHA-1, as in IEEE 802.11-2007.

Response *Response Status* **U**

REJECT
We are concerned about the political problem of SHA-1 vs SHA-256; that the US Government may overreact to the problems identified in SHA-1 (for its use in certificates) and ban all uses of SHA-1.

Cl **08** *SC* **8.5.1.5.2** *P* **22** *L* **47** # 19

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Suggested wording
(Originally LB98/279 submitted by Malinen, Jouni, during LB98 with ID Malinen/21)

SuggestedRemedy

Replace "16 bit unsigned integers" with "16-bit unsigned integers".

Response *Response Status* **C**

ACCEPT.

Cl **08** *SC* **8.5.1.5.3** *P* **22** *L* **58** # 20

CHAPLIN, CLINT F

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

Use of a long label "R0 Key Derivation" is not needed to keep key derivations unique; shorter label would meet that requirement. Long string here is just adding extra cost to KDF operation which is already quite CPU expensive.
(Originally LB98/283 submitted by Malinen, Jouni, during LB98 with ID Malinen/22)

SuggestedRemedy

Replace "R0 Key Derivation" with "R0" in R0-Key-Data derivation. On page 24 line 7, replace '"R0 Key Derivation" is 0x5230204B6579204465726976617469 6F6E' with '"R0" is 0x5230'. On page 24 line 25, replace "R0 Key Name" with "R0N". On page 24 line 30, replace '"R0 Key Name" is 0x5230204b6579204e616d65' with '"R0N" is 0x52304E'.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Changed to "FT-R0" (0x46542d5230) in calculation of PMK-R0 and PMKR0Name.

Cl **08** *SC* **8.5.1.5.3** *P* **22** *L* **58** # 21

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

During the evaluation of s-PRF versus v-PRF and AES versus SHA256 KDFs in last meeting, it was clear that we can reduce a SHA operation if we shorten the label. I do not see any loss of cryptographic security in doing so.
(Originally LB98/284 submitted by Sood, Kapil, during LB98 with ID Sood/025)

SuggestedRemedy

Change "R0 Key Derivation" to "R0 Key" in formulae for deriving R0-Key-Data.

Response *Response Status* **C**

ACCEPT IN PRINCIPLE.
Changed to "FT-R0" (0x46542d5230) in calculation of PMK-R0 and PMKR0Name.

Cl **08** *SC* **8.5.1.5.3** *P* **22** *L* **7** # 293

Edney, Jonathan

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

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

SuggestedRemedy

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

Response *Response Status* **U**

REJECT.
This is not a long integer. It is shown as a string of octets, twice, in two different formats to minimize confusion about string termination.

Cl **08** *SC* **8.5.1.5.3** *P* **23** *L* **7** # 22

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

Reduce label length of "R0 Key Derivation"
(Originally LB98/289 submitted by Sood, Kapil, during LB98 with ID Sood/026)

SuggestedRemedy

Change as follows: "- "R0 Key" is 0x5230204B6579"

Response *Response Status* **C**

ACCEPT IN PRINCIPLE.
Changed to "FT-R0" (0x46542d5230) in calculation of PMK-R0 and PMKR0Name.

Cl **08** *SC* **8.5.1.5.3** *P* **23** *L* **9** # 23

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Suggested wording
(Originally LB98/290 submitted by Malinen, Jouni, during LB98 with ID Malinen/23)

SuggestedRemedy

Replace "Beacons and Probe Responses" with "Beacon and Probe Response frames".

Response *Response Status* **C**

ACCEPT.

Cl **08** *SC* **8.5.1.5.4** *P* **23** *L* **39** # 24

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Suggested wording
(Originally LB98/296 submitted by Malinen, Jouni, during LB98 with ID Malinen/24)

SuggestedRemedy

Replace "256 bit key" with "256-bit key".

Response *Response Status* **C**

ACCEPT.

Cl **08** *SC* **8.5.1.5.4** *P* **23** *L* **42** # 25

CHAPLIN, CLINT F

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

Use of a long label "R1 Key Derivation" is not needed to keep key derivations unique; shorter label would meet that requirement. Long string here is just adding extra cost to KDF operation which is already quite CPU expensive.
(Originally LB98/298 submitted by Malinen, Jouni, during LB98 with ID Malinen/25)

SuggestedRemedy

Replace "R1 Key Derivation" with "R1" in PMK-R1 derivation. On line 49, replace "'R1 Key Derivation" is 0x5231204B6579204465726976617469 6F6E' with "'R1" is 0x5231'. On line 56, replace "R1 Key Name" with "R1N". On line 61, replace "'R1 Key Name" is 0x5231204b6579204e616d65' with "'R1N" is 0x52314E'.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Changed to "FT-R1" (0x46542d5231) in calculation of PMK-R1 and PMKR1Name.

Cl **08** *SC* **8.5.1.5.4** *P* **23** *L* **42** # 26

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

During the evaluation of s-PRF versus v-PRF and AES versus SHA256 KDFs in last meeting, it was clear that we can reduce a SHA operation if we shorten the label. I do not see any loss of cryptographic security in doing so.
(Originally LB98/299 submitted by Sood, Kapil, during LB98 with ID Sood/027)

SuggestedRemedy

Change "R1 Key Derivation" to "R1 Key" in formulae for deriving PMK-R1.

Response *Response Status* **C**

ACCEPT IN PRINCIPLE.
Changed to "FT-R1" (0x46542d5231) in calculation of PMK-R1 and PMKR1Name.

Cl **08** *SC* **8.5.1.5.4** *P* **23** *L* **50** # 27

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

Reduce label length of "R1 Key Derivation"
(Originally LB98/300 submitted by Sood, Kapil, during LB98 with ID Sood/028)

SuggestedRemedy

Change as follows: "- "R1 Key" is 0x5231204B6579"

Response *Response Status* **C**

ACCEPT IN PRINCIPLE.
Changed to "FT-R1" (0x46542d5231) in calculation of PMK-R1 and PMKR1Name.

Cl **08** *SC* **8.5.1.5.4** *P* **23** *L* **52** # 163

Sood, Kapil

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

All APs have an R1KH, including the first AP with which the STA performed Initial Auth. So, "R1KH-ID is a MAC address of the holder of the PMK-R1 in the Authenticator of the target AP" is not accurate.

SuggestedRemedy

Change: "R1KH-ID is a MAC address of the holder of the PMK-R1 in the Authenticator of the AP" OR "R1KH-ID is a MAC address of the holder of the PMK-R1 in the Authenticator of the Initial or target AP"

Response *Response Status* **U**

ACCEPT.
First alternative taken.

Cl **08** *SC* **8.5.1.5.4** *P* **23** *L* **52** # 336

Sood, Kapil

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

All APs have an R1KH, including the first AP with which the STA performed Initial Auth. So, "R1KH-ID is a MAC address of the holder of the PMK-R1 in the Authenticator of the target AP" is not accurate. (This is revision of similar comment)

SuggestedRemedy

Change: "R1KH-ID is a MAC address of the holder of the PMK-R1 in the Authenticator of the AP" OR "R1KH-ID is a MAC address of the holder of the PMK-R1 in the Authenticator of the Initial or target AP"

Response *Response Status* **U**

ACCEPT.
First alternative taken.

Cl **08** *SC* **8.5.1.5.5** *P* **24** *L* **10** # 28

CHAPLIN, CLINT F

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

Use of a long label "PTK Key derivation" is not needed to keep key derivations unique; shorter label would meet that requirement. Long string here is just adding extra cost to KDF operation which is already quite CPU expensive.
(Originally LB98/310 submitted by Malinen, Jouni, during LB98 with ID Malinen/26)

SuggestedRemedy

Replace "PTK Key derivation" with "PTK" in PTK derivation. On line 18, replace "'PTK Key derivation" is 0x50544B204B6579206465726976617469 6F6E' with "'PTK" is 0x50544B'.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Changed to "FT-PTK" (0x46542d50544b) in calculation of PTK and PTKName.

Cl **08** *SC* **8.5.1.5.5** *P* **24** *L* **10** # 284

Housley, Russell D

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

The document says:
... the PTK derivation is as follows:
PTK = KDF-PTKLen(PMK-R1, "PTK Key derivation", ...
The document also says:
KCK = L(PTK, 0, 128)
KEK = L(PTK, 128, 128)
TK = L(PTK, 256, 128)
If the PTK will always be composed of three 128-bit keys, then the flexibility of PTKLen can be removed from the specification. I suspect that this flexibility is needed and that the derivation of the KCK, KEK, and TK need to reflect it.

SuggestedRemedy

Change the text derivation of the KCK, KEK, and TK need to reflect the possibility of more than one PTK key size.

Response *Response Status* **U**

ACCEPT.
At page 24 line 54 inserted "For vendor specific cipher suites, the length of TK (and the value of PTKLen) depend on the vendor specific algorithm."

Cl **08** *SC* **8.5.1.5.5** *P* **24** *L* **10** # 29

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

During the evaluation of s-PRF versus v-PRF and AES versus SHA256 KDFs in last meeting, it was clear that we can reduce a SHA operation if we shorten the label. I do not see any loss of cryptographic security in doing so.
(Originally LB98/311 submitted by Sood, Kapil, during LB98 with ID Sood/029)

SuggestedRemedy

Change "PTK Key derivation" to "PTK Key" in formula for deriving PTK

Response *Response Status* **C**

ACCEPT IN PRINCIPLE.
Changed to "FT-PTK" (0x46542d50544b) in calculation of PTK and PTKName.

Cl **08** *SC* **8.5.1.5.5** *P* **24** *L* **11** # 149

Chen, Lidong

Comment Type **T** *Comment Status* **A** *PTKLen*

According to the main document, 802.11m, PTKLen depends on the cipher suite. In 802.11r, KCK and KEK are both 128 bits. TK depends on cipher suite. If only CCMP is allowed, then TK is 128 bits and the PTKLen must be 384 bits. It must be consistent with 802.11m.
Otherwise, PTKLen should be modified in 11r.

SuggestedRemedy

Response *Response Status* **C**

ACCEPT.
At page 24 line 54 inserted "For vendor specific cipher suites, the length of TK (and the value of PTKLen) depend on the vendor specific algorithm."

Cl **08** *SC* **8.5.1.5.5** *P* **24** *L* **17** # 164

Sood, Kapil

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

Typo "S1KHand"

SuggestedRemedy

Change: "S1KH and"

Response *Response Status* **U**

ACCEPT.

Cl **08** *SC* **8.5.1.5.5** *P* **24** *L* **18** # 30

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

Reduce length of "PTK Key derivation"
(Originally LB98/313 submitted by Sood, Kapil, during LB98 with ID Sood/030)

SuggestedRemedy

Change "-- "PTK Key" is x50544B204B6579."

Response *Response Status* **C**

ACCEPT IN PRINCIPLE.
Changed to "FT-PTK" (0x46542d50544b) in calculation of PTK and PTKName.

Cl **08** *SC* **8.5.1.5.5** *P* **24** *L* **24** # 337

Sood, Kapil

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

"The KEK is used to provide data confidentiality in EAPOL-Key messages, as defined in 8.5.2" falsely implies that the EAPOL-Key messages have data confidentiality. In fact, certain fields within the EAPOL-Key are confidentiality protected. (This is revision of similar comment)

SuggestedRemedy

Change: "The KEK is used to provide data confidentiality for Key Data field in EAPOL-Key messages, as defined in 8.5.2"

Response *Response Status* **U**

ACCEPT.

Cl **08** *SC* **8.5.1.5.5** *P* **24** *L* **24** # 165

Sood, Kapil

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

"The KEK is used to provide data confidentiality in EAPOL-Key messages, as defined in 8.5.2" falsely implies that the EAPOL-Key messages have data confidentiality. In fact, certain fields within the EAPOL-Key are confidentiality protected.

SuggestedRemedy

Change: "The KEK is used to provide data confidentiality for certain fields (Key Data) in EAPOL-Key messages, as defined in 8.5.2"

Response *Response Status* **U**

ACCEPT.

Cl **08** *SC* **8.5.1.5.5** *P* **24** *L* **59** # 31

CHAPLIN, CLINT F

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

PTKName is not really used anywhere in 802.11r draft. However, its derivation adds extra cost--and potentially latency--to FT. As an example, I ran some performance tests on a SIP phone and it took about 2.7 ms to derive PMK-R1 and PTK with names for each. This is needed for each FT and is already quite large amount of time if done while data connection is down (e.g., over-the-air). PTK and PTKName derivation took about 1.7 ms and taking out PTKName dropped this to close to 1.0 ms. In other words, deriving the mostly useless PTKName on this particular device could add 0.7 ms or so to each transition.
(Originally LB98/316 submitted by Malinen, Jouni, during LB98 with ID Malinen/28)

SuggestedRemedy

Remove PTKName description by removing text from page 25 line 59 ("The PTK is referenced and named ...") to page 26 line 4 ("... identify the PTK key."). In addition, remove 3.97k on page 3 line 16, remove "PTKName" from Clause 4 on page 3 line 55, remove "and PTKName" from 11A.5.2 on page 57 lines 46, remove "and PTKName" from 11A.5.3 on page 59 line 13.

Response *Response Status* **U**

REJECT.
The current text does not require the calculation of PTKName.

Cl **08** *SC* **8.5.1.5.5** *P* **24** *L* **61** # 32

CHAPLIN, CLINT F

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

Use of a long label "PTK Name" is not needed to keep key derivations unique; shorter label would meet that requirement. Long string here is just adding extra cost to KDF operation which is already quite CPU expensive.
(Originally LB98/317 submitted by Malinen, Jouni, during LB98 with ID Malinen/27)

SuggestedRemedy

Either remove PTKName completely (per my another comment on 8.5.1.5.5) or replace "PTK Name" with "PTKN" in PTKName derivation and on page 26 line 1, replace '"PTK Name" is 0x50544b204e616d65' with '"PTKN" is 0x50544B4E'.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Changed to "FT-PTK" (0x46542d50544b) in calculation of PTK and PTKName.

Cl **10** *SC* **10.3.34.2.3** *P* **38** *L* **30** # 213

Sood, Kapil

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

It is the MAC who generates the primitive.

SuggestedRemedy

Change: "This primitive is generated by the MAC at an AP to indicate"

Response *Response Status* **U**

REJECT.
The primitive is generated by the MLME when the MAC receives the third frame of the authentication sequence. See, for example, 10.3.6.3.3 in 802.11-2007.

Cl **10** *SC* **10.3.34.2.3** *P* **38** *L* **30** # 362

Sood, Kapil

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

It is the MAC who generates the primitive. (This is revision of similar comment)

SuggestedRemedy

Change: "This primitive is generated by the MAC at an AP to indicate"

Response *Response Status* **U**

REJECT.
The primitive is generated by the MLME when the MAC receives the third frame of the authentication sequence. See, for example, 10.3.6.3.3 in 802.11-2007.

Cl **10** *SC* **10.3.34.4.4** *P* **40** *L* **12** # 33

CHAPLIN, CLINT F

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

This paragraph seems to indicate that there could be a "next message in the resource request sequence" after the fourth frame. What would that message be? Isn't the resource request sequence completed with the fourth message and this is followed by reassociation?
(Originally LB98/346 submitted by Malinen, Jouni, during LB98 with ID Malinen/29)

SuggestedRemedy

Replace "examines the content of the message and either responds to the PeerMACAddress with the next message in the resource request sequence or completes its processing of the resource request" with "examines the content of the message and completes its processing of the resource request".

Response *Response Status* **U**

ACCEPT.

Cl **10** *SC* **10.3.35** *P* **41** *L* **56** # 340

Sood, Kapil

Comment Type **TR** *Comment Status* **A** *MLME diagram*

The MLME's defined in this clause are confusing, and need further clarification. This standard amendment has not seen a single proof of inter-operable behavior between 2 independent entities - so, all steps much be taken to ensure very lucid description of complex functions. (This is revision of similar comment)

SuggestedRemedy

Add a MLME interface diagram indicating which MLME functions are invoked at which entities for Fast BSS Transition protocol (4-message flow) using over-the-DS. A similar diagram has been drawn in multiple TGr adhoc meetings, and adding one such diagram is essential to make this spec more comprehensible and hence, easier to inter-operate. Accept my contribution (11-07-2352-00-000r-FT-MLME-Figure) to address this comment.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changes to 11A.5.3 as given in 11-07-2352-02-000r-ft-mlme-figure.doc; not the changes shown to 11A.10.

Cl **10** *SC* **10.3.35** *P* **41** *L* **56** # 170

Sood, Kapil

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

The MLME's defined in this clause are confusing, and need further clarification. This standard amendment has not seen a single proof of inter-operable behavior between 2 independent entities - so, all steps much be taken to ensure very lucid description of complex functions.

SuggestedRemedy

Add a MLME interface diagram indicating which MLME functions are invoked at which entities. A similar diagram has been drawn in multiple TGr adhoc meetings, and adding one such diagram to this clause (or, at a different location in this document) will go a long way in making this spec more comprehensible and hence, easier to inter-operate.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changes to 11A.5.3 as given in 11-07-2352-02-000r-ft-mlme-figure.doc; not the changes shown to 11A.10.

Cl **10** *SC* **10.3.35.1.2** *P* **42** *L* **17** # 167

Sood, Kapil

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

Why is the row for "PeerMACAddress" listed as a component separate from the "Contents of Action Frame" - the contents of Action frame contain the STA and Target APs addresses

SuggestedRemedy

Delete first row (line 17) "PeerMACAddress" and delete "PeerMACAddress" on line 7

Response *Response Status* **U**

REJECT.
The MAC can and should report the MAC address of the originator of the frame to the SME; it is the SME that understands the contents of the Action frame and is able to verify that the contents match the MAC address of the originator.

Cl **10** *SC* **10.3.35.1.2** *P* **42** *L* **36** # 168

Sood, Kapil

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

"and at the non-AP STA the response is delivered to the SME for processing." - what does this mean. I suspect this means that the MAC of non-AP STA sends a "response" to the SME of non-AP STA, correct? Is this response "MLME-REMOTE-REQUEST.confirm"?

SuggestedRemedy

Change "&Action Frame. At the non-AP STA, the MAC delivers the MLME-REMOTE-REQUEST.confirm to the SME for processing." OR, delete this sentence, as this is covered in 10.3.35.3.

Response *Response Status* **U**

ACCEPT.
Phrase starting "and at the non-AP STA" deleted

Cl **10** *SC* **10.3.35.1.2** *P* **42** *L* **36** # 339

Sood, Kapil

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

"and at the non-AP STA the response is delivered to the SME for processing." - what does this mean. I suspect this means that the MAC of non-AP STA sends a "response" to the SME of non-AP STA, correct? Is this response "MLME-REMOTE-REQUEST.confirm"? (This is revision of similar comment)

SuggestedRemedy

Change "&Action Frame. At the non-AP STA, the MAC delivers the MLME-REMOTE-REQUEST.confirm to the SME for processing." OR, delete this sentence, as this is covered in 10.3.35.3.

Response *Response Status* **U**

ACCEPT.
Phrase starting "and at the non-AP STA" deleted

Cl **10** *SC* **10.3.35.2.1** *P* **42** *L* **44** # 341

Sood, Kapil

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

"This primitive is used by the SME to request the MAC to send a Management Frame of Subtype&" - only non-AP STA can send this message. This must be indicated clearly. The entire MLME clause for MLME-Remote_Request is used on non-AP STA and on AP for different messages. The text, as written, is very confusing and should be clarified. (This is revision of similar comment)

SuggestedRemedy

Change: "This primitive is used by the SME of non-AP STA (to send over-the-DS Request) and SME of AP (to send over-the-DS response) to request the MAC to send a Management Frame of Subtype&"

Response *Response Status* **U**

ACCEPT.

Cl **10** *SC* **10.3.35.2.1** *P* **42** *L* **44** # 171

Sood, Kapil

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

"This primitive is used by the SME to request the MAC to send a Management Frame of Subtype&" - only non-AP STA can send this message. This must be indicated clearly. The entire MLME clause for MLME-Remote_Request is used on non-AP STA and on AP for different messages. The text, as written, is very confusing and should be clarified.

SuggestedRemedy

Change: "This primitive is used by the SME of non-AP STA (to send over-the-DS Request) and SME of AP (to send over-the-DS response) to request the MAC to send a Management Frame of Subtype&"

Response *Response Status* **U**

ACCEPT.

Cl **10** *SC* **10.3.35.2.2** *P* **42** *L* **39** # 169

Sood, Kapil

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

The definition of ".request" should appear before the definition of ".indication"

SuggestedRemedy

Change 10.3.35.2 to 10.3.35.1, and change 10.3.35.1 to 10.3.35.2

Response *Response Status* **U**

ACCEPT.

Cl **10** *SC* **10.3.35.3.1** *P* **43** *L* **28** # 342

Sood, Kapil

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

"This primitive is used by the MAC to indicate that it has completed sending a Management Frame&" is issued by the MAC of non-AP STA to its SME. Make this explicit. (This is revision of similar comment)

SuggestedRemedy

Change: "This primitive is used by the MAC of non-AP STA to indicate that it has completed sending a Management Frame"

Response *Response Status* **U**

REJECT.
This primitive is also used by the MAC of the AP to indicate that it has completed sending the response.

Cl **10** *SC* **10.3.35.3.1** *P* **43** *L* **28** # 172

Sood, Kapil

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

"This primitive is used by the MAC to indicate that it has completed sending a Management Frame&" is issued by the MAC of non-AP STA to its SME. Make this explicit.

SuggestedRemedy

Change: "This primitive is used by the MAC of non-AP STA to indicate that it has completed sending a Management Frame"

Response *Response Status* **U**

REJECT.
This primitive is also used by the MAC of the AP to indicate that it has completed sending the response.

Cl **11** *SC* **11.3.1.1** *P* **44** *L* **24** # 34

CHAPLIN, CLINT F

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

It is mentioned that Fast BSS Transition is possible in IBSS - which is not true
(Originally LB98/352 submitted by Zaks, Artur, during LB98 with ID Zaks/11)

SuggestedRemedy

Remove IBSS from the definition. State clearly that FT is not applicable to IBSS

Response *Response Status* **U**

ACCEPT.
Change second dash list item to "If in an ESS, and the Authentication Algorithm."

Cl **11** *SC* **11.3.1.2** *P* **44** *L* **64** # 35

CHAPLIN, CLINT F

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

The PTKSA should be deleted even on an FT.
(Originally LB98/353 submitted by Cam-Winget, Nancy, during LB98 with ID Cam-Winget/18)

SuggestedRemedy

Remove the added "If" clause of this sentence.

Response *Response Status* **U**

REJECT.
Text changes to 11.3.1.2 are to insure that the pre-11r behavior does not delete security associations created by 11r. Current text in 11A.4.2 (at 53.24) and 11A.5.4 (at 60.22) describe the 11r conditions for deleting security associations.

Cl **11** *SC* **11.3.2.1** *P* **45** *L* **13** # 37

CHAPLIN, CLINT F

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

As far as FT is concerned, Association is only used during the initial MD association; it is not used for FT protocol. Taken into account how initial MD association works, it is more or less identical process to the 802.11i association and as such, there is no need to modify the description of how PTKSA is to be deleted. This deletion can, and should, happen also in case of FT. The change to PTKSA deletion is only needed for reassociation procedure.
(Originally LB98/355 submitted by Malinen, Jouni, during LB98 with ID Malinen/30)

SuggestedRemedy

Remove changes to 11.3.2.1.

Response *Response Status* **U**

ACCEPT.

Cl **11** *SC* **11.3.2.1** *P* **45** *L* **13** # 36

CHAPLIN, CLINT F

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

The PTKSA should be deleted even on an FT.
(Originally LB98/354 submitted by Cam-Winget, Nancy, during LB98 with ID Cam-Winget/19)

SuggestedRemedy

Remove the added "Except when..." clause of this sentence.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Association is only used during the Initial Mobility Domain Association, and not for the FT protocols. Changes to 11.3.2.1 deleted.

Cl **11** *SC* **11.3.2.2** *P* **45** *L* **23** # 38

CHAPLIN, CLINT F

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

The PTKSA should be deleted even on an FT.
(Originally LB98/356 submitted by Cam-Winget, Nancy, during LB98 with ID Cam-Winget/20)

SuggestedRemedy

Remove the added "Except when..." clause of this sentence.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Association is only used during the Initial Mobility Domain Association, and not for the FT protocols. Changes to 11.3.2.2 deleted.

Cl **11** *SC* **11.3.2.2** *P* **45** *L* **23** # 39

CHAPLIN, CLINT F

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

As far as FT is concerned, Association is only used during the initial MD association; it is not used for FT protocol. Taken into account how initial MD association works, it is more or less identical process to the 802.11i association and as such, there is no need to modify the description of how PTKSA is to be deleted. This deletion can, and should, happen also in case of FT. The change to PTKSA deletion is only needed for reassociation procedure.
(Originally LB98/357 submitted by Malinen, Jouni, during LB98 with ID Malinen/31)

SuggestedRemedy

Remove changes to 11.3.2.2.

Response *Response Status* **U**

ACCEPT.

Cl **11** *SC* **11.3.2.3** *P* **45** *L* **36** # 40

CHAPLIN, CLINT F

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

Per 11A.5 State 2 is entered after successful completion of authentication phase in both over-the-air and over-the-DS FT. In other words, when reassociation request is sent, the STAs will already be in State 2 and as such, the change for MLME-REASSOCIATE.request behavior to ignore State 1 verification is not needed for FT.
(Originally LB98/358 submitted by Malinen, Jouni, during LB98 with ID Malinen/32)

SuggestedRemedy

Remove changes to point (a) of the lettered list in the first paragraph of 11.3.2.3.

Response *Response Status* **U**

ACCEPT.

Cl **11** *SC* **11.3.2.3** *P* **45** *L* **44** # 41

CHAPLIN, CLINT F

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

The PTKSA should be deleted even on an FT.
(Originally LB98/359 submitted by Cam-Winget, Nancy, during LB98 with ID Cam-Winget/21)

SuggestedRemedy

Remove the added "Except when..." clause of this sentence.

Response *Response Status* **U**

REJECT.
Text changes to 11.3.2.3 are to insure that the pre-11r behavior does not delete security associations created by 11r. Current text in 11A.4.2 (at 53.24) and 11A.5.4 (at 60.22) describe the 11r conditions for deleting security associations.

Cl **11** *SC* **11.3.2.4** *P* **45** *L* **54** # 42

CHAPLIN, CLINT F

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

The PTKSA should be deleted even on an FT.
(Originally LB98/360 submitted by Cam-Winget, Nancy, during LB98 with ID Cam-Winget/22)

SuggestedRemedy

Remove the added "Except when..." clause of this sentence.

Response *Response Status* **U**

REJECT.
Text changes to 11.3.2.4 are to insure that the pre-11r behavior does not delete security associations created by 11r. Current text in 11A.4.2 (at 53.24) and 11A.5.4 (at 60.22) describe the 11r conditions for deleting security associations.

Cl **11** *SC* **11.4.1** *P* **46** *L* **4** # 43

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

Missing function that Traffic Stream can be created when the TSPEC is sent in the reassociation message.
(Originally LB98/363 submitted by Sood, Kapil, during LB98 with ID Sood/033)

SuggestedRemedy

Change "&initiating a transition to that AP, or in the reassociation request to that AP"

Response *Response Status* **C**

ACCEPT.

Cl **11** *SC* **11.4.4a** *P* **47** *L* **18** # 44

CHAPLIN, CLINT F

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

Unfortunately, we have inconsistent use of terms. "Inactive", "Accepted", and "Active" refer to the three states of a TS. "Admit" is a looser word. Furthermore, accepting the resource, rather than placing it in an intermediate state, would allow for STAs to request for resources at more than one AP simultaneously, and that has been shown to lead to instability when performed as written.
(Originally LB98/368 submitted by Epstein, Joseph, during LB98 with ID Epstein/15)

SuggestedRemedy

Change "admit" to "accept" in both places.

Response *Response Status* **U**

ACCEPT.

Cl **11** *SC* **11.4.4a** *P* **47** *L* **22** # 45

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Grammar
(Originally LB98/370 submitted by Malinen, Jouni, during LB98 with ID Malinen/33)

SuggestedRemedy

Replace "Each TS established by this resource request are" with "Each TS established by this resource request is".

Response *Response Status* **C**

ACCEPT.

Cl **11** *SC* **11.4.4a** *P* **47** *L* **27** # 46

CHAPLIN, CLINT F

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

This text clearly leads to unstable systems, by allowing non-active resources to count against available resources. Text was accepted elsewhere into the draft to forbid this behavior; this must have been a straggler.
(Originally LB98/371 submitted by Epstein, Joseph, during LB98 with ID Epstein/14)

SuggestedRemedy

Reverse the logic by changing to "The SME in the HC shall not take the resource/timing requirements of the TS in the Accepted state into consideration before assigning any further resources to any other admitted or accepted TS, nor in calculating the Available Admission Capacity for the BSS Load information element." (By the way, "shall take into account" is meaningless, as electronic systems cannot "take things into account", and cannot be accused of abusing discretion: ignoring is a valid way of taking things into account. "Shall take into account" is, thus, equivalent to "may take into account". "Shall not take into account", however, is valid.)

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changes given in submission 11-07-2516-01.

Cl **11A** *SC* **11A** *P* **47** *L* **44** # 329

Sood, Kapil

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

No inter-operability of the protocol mechanisms defined in draft D7.0 have been demonstrated in testbeds/ interops prior to going for the Sponsor Ballot circulation. For all the best efforts that this group has put in, we possible cannot determine if we have covered all corner cases and that our specification (as produced) will be completely interoperable without requiring any modifications. I would have much preferred to see even preliminary results proving interoperability of this protocol - not FT latency - just basic execution of this protocol. (This is revision of similar comment)

SuggestedRemedy

Remove Clause 11A until the time atleast 2 independent implementations have shown to interoperate and any updates/modifications made to this clause.

Response *Response Status* **U**

REJECT
The IEEE procedure for publishing standards is not the subject of this ballot.

Cl **11A** *SC* **11A** *P* **47** *L* **44** # 219

Sood, Kapil

Comment Type **TR** *Comment Status* **R** *out-of-order IEs*

The FT protocols do not define the scenario if IEs are sent in different order between a non-AP STA and AP. In other words, none of the FT message will get rejected if ordering of the IE is not as per the orders listed in this specification.

SuggestedRemedy

Discuss, and insert a new status code ("IE out of order") if the group feels that the ordering of IEs should be maintained.

Response *Response Status* **U**

REJECT.
Subclause 11A.8 specifies the order for IEs for the MIC calculation, which is independent of the order of the IEs in the frame. The order of the IEs within the RIC is specified in 11A.11. General ordering of IEs in the frames is covered in base specification in 7.2.3. No changes needed to 802.11r.

Cl **11A** *SC* **11A** *P* **47** *L* **44** # 155

Sood, Kapil

Comment Type **TR** *Comment Status* **R** *Wait for Interoperability*

No inter-operability of the protocol mechanisms defined in draft D7.0 have been demonstrated in testbeds/ interops prior to going for the Sponsor Ballot circulation. For all the best efforts that this group has put in, we possible cannot determine if we have covered all corner cases and that our specification (as produced) will be completely interoperable without requiring any modifications. I would have much preferred to see even preliminary results proving interoperability of this protocol - not FT latency - just basic execution of this protocol.

SuggestedRemedy

Remove Clause 11A until the time atleast 2 independent implementations have shown to interoperate and any updates/modifications made to this clause.

Response *Response Status* **U**

REJECT
The IEEE procedure for publishing standards is not the subject of this ballot.

Cl **11A** *SC* **11A.1** *P* **47** *L* **50** # 144

Mccann, Stephen

Comment Type **E** *Comment Status* **A**

Typo "connectivity is lost"

SuggestedRemedy

"connectivity that is lost"

Response *Response Status* **C**

ACCEPT IN PRINCIPLE.
Changed to "time that connectivity is lost."

Cl **11A** *SC* **11A.1** *P* **47** *L* **51** # 145

Mccann, Stephen

Comment Type **E** *Comment Status* **A**

Specifically what "protocols" are referred to

SuggestedRemedy

Add "Fast Transition Procotols"

Response *Response Status* **C**

ACCEPT IN PRINCIPLE.
Change "These protocols" to "The Fast BSS Transition protocols"

Cl **11A** *SC* **11A.1** *P* **47** *L* **55** # 173

Sood, Kapil

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

"First" is inconsistent with the use of "Initial" elsewhere in the document.

SuggestedRemedy

Change: first to Initial

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.1** *P* **48** *L* **1** # 47

CHAPLIN, CLINT F

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

The following sentence "Fast BSS Transition Resource Request: this protocol is executed when a STA needs increased likelihood that the required resources be available prior to a transition, or to mitigate AP latencies involved in QoS scheduling." hinges on subjective and unsubstantiated claims and adds no value or guidance to developers. The statement here should be aligned with that in bullet (1) for "Fast BSS Transition". Why a specific procedure is executed is outside the scope of this standard.
(Originally LB98/376 submitted by Sood, Kapil, during LB98 with ID Sood/034)

SuggestedRemedy

Change as follows: "Fast BSS Transition Resource Request: this protocol is executed when a STA requires resource requests prior to its transition."
If the intent is to describe the conditions under which the Fast BSS Transition Resource Request protocol will be executed, then a more specific document is needed and does not belong into this standard.

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.1** *P* **48** *L* **47** # 146

Mccann, Stephen

Comment Type **E** *Comment Status* **A**

The abbreviation "FT" seems to refer to both "Fast BSS Transition" and also "Fast BSS Transition Authentication Algorithm", as used within the whole of clause 11A.1. I.e. "FT protocols" are referred to, of which Fast BSS Transition Authentication Algorithm then appears to be a parameter.

SuggestedRemedy

Clarify the definition of the abbreviation "FT"

Response *Response Status* **C**

ACCEPT.
Added acronym "FTAA" for FT Authentication Algorithm. Changes at 48.27, Figure 11A-4 (56.12 and 56.15), 56.43, 56.46, Figure 11A-6 (59.43, 59.45), 59.63, 59.65, Figure 11A-8 (62.11, 62.13, 62.16, 62.18), Figure 11A-9 (63.11, 63.13, 63.15, 63.17), 63.39, 63.42

Cl **11A** *SC* **11A.10** *P* **84** *L* **1** # 314

Myles, Andrew F

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

The function of RRB is unverifiable function and therefore should be taken out of the draft. The RRB is insisting that messages in specific format be tranmitted across the DS. This is beyond the scope of 802.11. Various implementations may choose to communicate between APs across the DS in different formats or methods. In some cases, such as a wirless centralized switch architecture such a communication may not even be needed inform of network messages (rather it may just need pointer manipulation). 802.11 should not dictate how the entities between the DS communicate.
Therefore it is suggested that we get rid of the notion of RRB from the draft. We should just mention that the that an AP communicates to the target AP and passes the necessary information. Formats and message flows should be removed. The DS just needs to gaurantee that the two APs are reachable by each other which would be the case if they belong to the same MDIE.

SuggestedRemedy

Remove Section 11A.10

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Insert at beginning of 11A.10.3 "This subclause defines a mechanism to transport the RemoteRequest and RemoteResponse between the current AP and the target AP. Any other mechanism may be used."
Annex A page 96 line 40 insert "PC35.14.1", "Remote Request/Response frame definition", "11A.10.3", "PC35.14:O", "yes/no/N/A". Insert "*" in PC35.14.

Cl **11A** *SC* **11A.10** *P* **86** *L* **1** # 324

Malinen, Jouni

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

11A.10 describes a new component, remote request broker, that is used to convert between Action frames and data frames with a specific Ethertype. This functionality is unnecessary and the AP design could be simplified by removing RRB frame conversion completely since the non-AP STAs could send and receive data frames as easily, if not even more easily, than new Action frames. In addition, this allows the non-AP STA <-> current AP communication to be protected since data frames are encrypted in the RSNA without having to wait for 802.11w to add management frame protection.

SuggestedRemedy

Remove RRB frame conversion (Action <-> data) from 802.11r and instead, use the frames defined in 11A.10.3 by sending and receiving them directly from/to the non-AP STA to/from the destination AP. The frames will still go through the current AP, but since they are normal data frames, there is no need to have specific RRB processing in the current AP.

Response *Response Status* **U**

REJECT
Use of Action frames is consistent with the over-the-air FT methods

Cl **11A** *SC* **11A.10** *P* **86** *L* **1** # 141

Chaplin, Clint F

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

The Remote Request Broker, and the AP-AP protool defined in 11A.10, are outside the MAC/PHY scope of 802.11. While some mechanism is needed to perform the over-the-DS fast BSS transition, it needs to be defined with the scope of the project. One such design is to define a special format data frame sent over-the-air to the current AP that is directed to the target AP to accomplish this. (submitted by Bill Marshall)

SuggestedRemedy

Incorporate latest revision of 11-06-1622-xx-000r-CID-1835-General-Encapsulation.doc into the amendment

Response *Response Status* **U**

REJECT
AP to AP communication is in scope to facilitate Fast BSS Transitions over-the-DS
The design decision is to use Action frames to enable over-the-DS transitions to remain consistent with use of Authentication frames in over-the-air transitions. One sample AP-to-AP protocol is defined here, but any such protocol can be used.

Cl **11A** *SC* **11A.10.1** *P* **86** *L* **11** # 88

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Expand ACK
(Originally LB98/621 submitted by Sood, Kapil, during LB98 with ID Sood/081)

SuggestedRemedy

Change "ACK" to "Acknowledgement"

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.10.1** *P* **86** *L* **15** # 89

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

Make STA more specific
(Originally LB98/622 submitted by Sood, Kapil, during LB98 with ID Sood/082)

SuggestedRemedy

Change "STA" to "non-AP STA"

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.10.1** *P* **86** *L* **31** # 255

Sood, Kapil

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

"it passes it" - who passes what? Clarify

SuggestedRemedy

Change "Fast BSS Transition, the MAC passes the Action Frame to the SME"

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.10.1** *P* **86** *L* **54** # 256

Sood, Kapil

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

Which AP will forward it - clarify.

SuggestedRemedy

Change "the current AP will forward the Request to that target AP"

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.10.1** *P* **86** *L* **6** # 87

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

The "STA" in the introduction of RRB should be more specific.
(Originally LB98/620 submitted by Sood, Kapil, during LB98 with ID Sood/080)

SuggestedRemedy

Change "STA" to "non-AP STA"

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.10.1** *P* **86** *L* **6** # 254

Sood, Kapil

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

"its" - who does its refer to? Clarify.

SuggestedRemedy

Change "AP through non-AP STA's existing"

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.10.1** *P* **86** *L* **6** # 253

Sood, Kapil

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

STA is not just any STA - It is non-AP STA

SuggestedRemedy

Change line 6, 7, 11, 15, 49, 51, 62, : "STA" to "non-AP STA"

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.10.1** *P* **86** *L* **6** # 252

Sood, Kapil

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

"This" is not the correct way to start a new section.

SuggestedRemedy

Change "Remote Request Broker (RRB) mechanism allows&"

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Changed to "The Remote Request Broker (RRB) mechanism allows."

Cl **11A** *SC* **11A.10.2** *P* **86** *L* **38** # 90

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

There are Responses, Confirm, Acks, besides Requests.
(Originally LB98/634 submitted by Sood, Kapil, during LB98 with ID Sood/094)

SuggestedRemedy

Change "Requests" to "protocol messages"

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.10.2** *P* **86** *L* **48** # 91

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

Make STA more specific
(Originally LB98/640 submitted by Sood, Kapil, during LB98 with ID Sood/095)

SuggestedRemedy

Change "STA" to "non-AP STA"

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.10.2** *P* **86** *L* **51** # 92

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

Make STA more specific
(Originally LB98/641 submitted by Sood, Kapil, during LB98 with ID Sood/096)

SuggestedRemedy

Change "STA" to "non-AP STA"

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.10.2** *P* **86** *L* **52** # 93

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

This sentence is confusing
(Originally LB98/642 submitted by Sood, Kapil, during LB98 with ID Sood/097)

SuggestedRemedy

Change "...directed to a Target AP in the same Mobility Domain (and therefore supporting "over-the-DS" communications) the Current AP will forward the messages to that target AP"

Response *Response Status* **C**

ACCEPT.
Change indicated in the proposed resolution changes "AP will forward" to "Current AP will forward". Also deleted the parenthesized phrase, as it is repeated from two paragraphs above.

Cl **11A** *SC* **11A.10.2** *P* **86** *L* **55** # 94

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

This section don't do a good job in connecting Action Frames and Remote Request/Response messages
(Originally LB98/643 submitted by Sood, Kapil, during LB98 with ID Sood/098)

SuggestedRemedy

Add a sentence at end of line 54, pg 86: "The RRB on Current AP converts Action Frames into Remote Requests, and converts Remote Response into Action Frames"

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.10.2** *P* **87** *L* **3** # 257

Sood, Kapil

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

STA is not just any STA - It is non-AP STA

SuggestedRemedy

Change line 3, : "STA" to "non-AP STA"

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.10.3** *P* **87** *L* **40** # 323

Malinen, Jouni

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

IEEE 802.11r is introducing a new Ethertype for AP-to-AP communication for the Remote request/response frames. This kind of functionality is similar to the format used with RSNA pre-authentication. In order to avoid adding new Ethertypes for every new functionality that requires AP-to-AP communication, it would be easier to share a single Ethertype and use subtyping for the different uses. This would allow the subtyping to be administered inside IEEE 802.11.

SuggestedRemedy

Replace "Protocol Version" field in Table 11A-2 with "Remote Frame Type". Replace "The Protocol Version field shall be set to 1. Received messages with Protocol Version other than 1 shall be discarded." with "The Remote Frame Type for FT Remote request/response messages shall be set to 1. Received messages with Remote Frame Type other than 1 shall be discarded."
It would be even better to move the description of the generic encapsulation (just the Remote Frame Type field) and the Ethertype in general to be outside Clause 11A so that it is clearer that this Ethertype can be used for other than FT purposes, too.

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.10.3** *P* **87** *L* **45** # 306

Malinen, Jouni

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

The Ethertype for Remote Request/Response frame has not yet been assigned. The editorial note here is pointing out that this would be done "one this amendment is approved for Sponsor Ballot". Taken into account that the amendment is already in Sponsor Ballot, the time to get this Ethertype assigned has arrived.

SuggestedRemedy

Request an Ethertype for Remote Request/Response frame and replace "??-??" with the allocated Ethertype.

Response *Response Status* **U**

ACCEPT
Application will be initiated, and the value will be inserted in the draft when it is provided by IEEE.

Cl **11A** *SC* **11A.11.1** *P* **88** *L* **34** # 258

Sood, Kapil

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

STA is not just any STA - It is non-AP STA

SuggestedRemedy

Change lines 34, 35, 50, 44, :"STA" to "non-AP STA"

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.11.1** *P* **88** *L* **34** # 95

CHAPLIN, CLINT F

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

The text emphasing that resource requests don't take place until reassociation has become muddled. Allowing stations to request resources to more than one AP at a time, in a binding manner before association, leads to instability because of overrequesting of resources. This was previously accepted by the group, but somehow, the text became unclear.
(Originally LB98/648 submitted by Epstein, Joseph, during LB98 with ID Epstein/10)

SuggestedRemedy

Change to "When using the resource request procedure, the STA has the option to, before or during (re)association, request a (re)association-time resource allocation at the target AP. To request resources for (re)association, the STA creates a Resource Information Container (RIC) and inserts it in an appropriate request message to the target AP."

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changes given in submission 11-07-2516-01.

Cl **11A** *SC* **11A.11.1** *P* **88** *L* **34** # 96

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

Make STA more specific
(Originally LB98/649 submitted by Sood, Kapil, during LB98 with ID Sood/102)

SuggestedRemedy

Change "STA" to "non-AP STA"

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.11.1** *P* **88** *L* **43** # 97

CHAPLIN, CLINT F

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

The text emphasing that resource requests don't take place until reassociation has become muddled. Allowing stations to request resources to more than one AP at a time, in a binding manner before association, leads to instability because of overrequesting of resources. This was previously accepted by the group, but somehow, the text became unclear.
(Originally LB98/650 submitted by Epstein, Joseph, during LB98 with ID Epstein/11)

SuggestedRemedy

Change to "The RIC contains a complete list of resources requested by the STA, for reservation after the transition. An AP that receives a resource request from a STA shall discard any previous resource request from that STA. In an RSN, this
resource request shall first be authenticated by the AP through checking of the MIC before the AP discards any previous resource request."

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changes given in submission 11-07-2516-01.

Cl **11A** *SC* **11A.11.1** *P* **88** *L* **43** # 98

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

"after the transition" is confusing? Does text mean before the transition? During the transition?
(Originally LB98/651 submitted by Sood, Kapil, during LB98 with ID Sood/100)

SuggestedRemedy

Delete this phrase from the sentence

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.11.1** *P* **88** *L* **49** # 99

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

Make STA more specific
(Originally LB98/654 submitted by Sood, Kapil, during LB98 with ID Sood/104)

SuggestedRemedy

Change "STA" to "non-AP STA"

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.11.1** *P* **88** *L* **54** # 100

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

Make STA more specific
(Originally LB98/655 submitted by Sood, Kapil, during LB98 with ID Sood/105)

SuggestedRemedy

Change "STA" to "non-AP STA"

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.11.2** *P* **89** *L* **1** # 101

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

We have established an abbreviation for "Resource Information Contained"
(Originally LB98/661 submitted by Sood, Kapil, during LB98 with ID Sood/101)

SuggestedRemedy

Use "RIC" instead of "Resource Information Container"

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.11.2** *P* **89** *L* **24** # 131

Trainin, Solomon

Comment Type **TR** *Comment Status* **A** *RIC format*

It is not completely clear how to request resources identified by Vendor Specific information element. It may be important in case if an AP supports QoS in parallel of the IEEE QoS and WMM QoS specification as well. In this case the STA may request an alternative of both resources. More explanation may be very useful.

SuggestedRemedy

Provide explanation, change format of the Resource Information Container if needed

Response *Response Status* **U**

ACCEPT
Insert row in Table 11A-3 with Resource Type "Vendor Specific" and Resource Descriptor definition "RDIE is followed by any Vendor-specific information elements required to specify this resource."

Cl **11A** *SC* **11A.11.2** *P* **89** *L* **30** # 102

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

Make STA more specific in "Notes" column
(Originally LB98/665 submitted by Sood, Kapil, during LB98 with ID Sood/106)

SuggestedRemedy

Change "STA" to "non-AP STA"

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.11.2** *P* **89** *L* **30** # 375

Sood, Kapil

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

The resource types currently defined in the specification only mentions 802.11 QoS, and has no accomodation for WMM TSPECs as defined by WiFi Alliance. The marketplace has adopted and implemented the WMM resource formats and processing, and it is an absolute requirement that the 802.11r procedure for resources be flexible to accomodate not just 802.11e, but all WMM (WFA) and other formats in future. This specification should be made extensible to accomodate co-existence of multiple resource formats. (This is revision of similar comment)

SuggestedRemedy

Accept my submission which addresses this problem, by extending the resource identifiers and advertising correct resource support policies.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Insert row in Table 11A-3 with Resource Type "Vendor Specific" and Resource Descriptor definition "RDIE is followed by any Vendor-specific information elements required to specify this resource."

Cl **11A** *SC* **11A.11.2** *P* **89** *L* **30** # 247

Sood, Kapil

Comment Type **TR** *Comment Status* **A** *RIC format*

The resource types currently defined in the specification only mentions 802.11 QoS, and has no accomodation for WMM TSPECs as defined by WiFi Alliance. The marketplace has adopted and implemented the WMM resource formats and processing, and it is an absolute requirement that the 802.11r procedure for resources be flexible to accomodate not just 802.11e, but all WMM (WFA) and other formats in future. This specification should be made extensible to accomodate co-existence of multiple resource formats.

SuggestedRemedy

Accept my submission which addresses this problem, by extending the resource identifiers and advertising correct resource support policies.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Insert row in Table 11A-3 with Resource Type "Vendor Specific" and Resource Descriptor definition "RDIE is followed by any Vendor-specific information elements required to specify this resource."

Cl **11A** *SC* **11A.11.3.1** *P* **91** *L* **11** # 103

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

"These Resource Descriptors are included in a Resource Information Container (RIC)" - This sentence is confusing and technically correct. RDs are within a Resource Request, which are within a RIC request. A very good explaination exists in 11A.10.2, so why do we need this here.
(Originally LB98/672 submitted by Sood, Kapil, during LB98 with ID Sood/107)

SuggestedRemedy

Remove this sentence.

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.11.3.1** *P* **91** *L* **18** # 104

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

Which is the "next" AP? This draft has used "Target" throughout.
(Originally LB98/673 submitted by Sood, Kapil, during LB98 with ID Sood/108)

SuggestedRemedy

Replace "next" with "Target"

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.11.3.1** *P* **91** *L* **19** # 260

Sood, Kapil

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

This spec has used target AP, so why use next AP here

SuggestedRemedy

Change "Next AP" to "target AP"

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.11.3.1** *P* **91** *L* **44** # 261

Sood, Kapil

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

The use case of whether a reassoc request can be failed if resource request were failed, is not considered here.

SuggestedRemedy

Insert on line 44 page 91 :"The non-AP STA shall not have its reassociation request rejected by a target AP solely on the basis of target AP not being able to allocate any resources requests from that non-AP STA.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Subclause 11A.11.3.1 is the STA procedures, not the AP procedures, and the text currently tells the STA how to interpret a zero status in the frame and a non-zero status in the RIC. In 11A.11.3.2 page 93 line 17 changed "The Status Code shall be set" to "The Status Code in the RDIE shall be set". Inserted after line 27 "A non-zero Status Code in an RDIE shall not cause a non-zero Status Code in the frame containing the RIC Request."

Cl **11A** *SC* **11A.11.3.1** *P* **91** *L* **44** # 380

Sood, Kapil

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

The use case of whether a reassoc request can be failed if resource request were failed, is not considered here. (This is revision of similar comment)

SuggestedRemedy

Insert on line 44 page 91 :"The non-AP STA shall not have its reassociation request rejected by a target AP solely on the basis of target AP not being able to allocate any resources requests from that non-AP STA."

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Subclause 11A.11.3.1 is the STA procedures, not the AP procedures, and the text currently tells the STA how to interpret a zero status in the frame and a non-zero status in the RIC. In 11A.11.3.2 page 93 line 17 changed "The Status Code shall be set" to "The Status Code in the RDIE shall be set". Inserted after line 27 "A non-zero Status Code in an RDIE shall not cause a non-zero Status Code in the frame containing the RIC Request."

Cl **11A** *SC* **11A.11.3.1** *P* **91** *L* **5** # 259

Sood, Kapil

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

STA is not just any STA - It is non-AP STA

SuggestedRemedy

Change lines 6, 7, 9, 16, 21, 26, 30, 40, 43, :"STA" to "non-AP STA"

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.11.3.1** *P* **91** *L* **62** # 105

CHAPLIN, CLINT F

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

The text emphasing that resource requests don't take place until reassociation has become muddled. Allowing stations to request resources to more than one AP at a time, in a binding manner before association, leads to instability because of overrequesting of resources. This was previously accepted by the group, but somehow, the text became unclear.
(Originally LB98/683 submitted by Epstein, Joseph, during LB98 with ID Epstein/12)

SuggestedRemedy

Change to "Failure to do so will result in the abandonment of any resource requests held by the target AP on behalf of the STA."

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changes given in submission 11-07-2516-01.

Cl **11A** *SC* **11A.11.3.2** *P* **92** *L* **30** # 106

CHAPLIN, CLINT F

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

The flowchart's text does not match the text below it, or the actual algorithm all that well. The algorithm is for "accepting" resource requests, not "allocating" resources--where "accepting" is defined in 11.4.
(Originally LB98/685 submitted by Epstein, Joseph, during LB98 with ID Epstein/13)

SuggestedRemedy

Change "Able to allocate these resources?" to "Able to accept these resource requests?"

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.11.3.2** *P* **93** *L* **12** # 262

Sood, Kapil

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

The use case of whether a reassoc request can be failed if resource request were failed, is not considered here.

SuggestedRemedy

Insert on line 12 page 93 :"The target AP shall not reject a reassociation request from a non-AP STA solely on the basis of target AP not being able to allocate any resources requests from that non-AP STA.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Page 93 line 17 changed "The Status Code shall be set" to "The Status Code in the RDIE shall be set". Inserted after line 27 "A non-zero Status Code in an RDIE shall not cause a non-zero Status Code in the frame containing the RIC Request."

Cl **11A** *SC* **11A.11.3.2** *P* **93** *L* **12** # 381

Sood, Kapil

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

The use case of whether a reassoc request can be failed if resource request were failed, is not considered here. (This is revision of similar comment)

SuggestedRemedy

Insert on line 12 page 93 :"The target AP shall not reject a reassociation request from a non-AP STA solely on the basis of target AP not being able to allocate any resources requests from that non-AP STA.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Page 93 line 17 changed "The Status Code shall be set" to "The Status Code in the RDIE shall be set". Inserted after line 27 "A non-zero Status Code in an RDIE shall not cause a non-zero Status Code in the frame containing the RIC Request."

Cl **11A** *SC* **11A.11.3.2** *P* **93** *L* **13** # 108

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

Which response frame?
(Originally LB98/688 submitted by Sood, Kapil, during LB98 with ID Sood/111)

SuggestedRemedy

Change: "&in the fourth message (See 11A.7.5)."

Response *Response Status* **C**

ACCEPT IN PRINCIPLE.
Delete "and include it in the response frame."

Cl **11A** *SC* **11A.11.3.2** *P* **93** *L* **2** # 263

Sood, Kapil

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

STA is not just any STA - It is non-AP STA

SuggestedRemedy

Change lines 2, :"STA" to "non-AP STA"

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.11.3.2** *P* **93** *L* **32** # 109

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

What is a "response RIC"?
(Originally LB98/691 submitted by Sood, Kapil, during LB98 with ID Sood/113)

SuggestedRemedy

Change "RIC response"

Response *Response Status* **C**

ACCEPT.
(Comment reclassified as Editorial)

Cl **11A** *SC* **11A.11.3.2** *P* **93** *L* **5** # 107

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

Clarify which SME?
(Originally LB98/687 submitted by Sood, Kapil, during LB98 with ID Sood/110)

SuggestedRemedy

Change: "The Target AP's SME examines the&"

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.2.1** *P* **48** *L* **32** # 118

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

"General" is not an appropriate title, as this sub-clause is introducing a new architecture.
(Originally LB105/10 submitted by Sood, Kapil, during LB105 with ID Sood/09)

SuggestedRemedy

Change "General" to "Introduction"

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.2.1** *P* **48** *L* **34** # 345

Sood, Kapil

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

"The FT key holder architecture, shown in Figure 11A-1, describes the FT key management entities" - sounds like exists in a vaccum. How does one relate this to the IEEE 802.11 architecture? This relationship is missing, and is a cause of complexity. (This is revision of similar comment)

SuggestedRemedy

Change: "The FT key holder architecture, shown in Figure 11A-1, describes the FT key management entities and is defined in context of 802.11 basic reference model (Fig 5-10)."

Response *Response Status* **U**

ACCEPT.
In proposed change, "Fig 5-10" changed to "see Figure 5-10 in 5.9", and "802.11 basic reference model" changed to "the IEEE 802.11 basic reference model".

Cl **11A** *SC* **11A.2.1** *P* **48** *L* **34** # 176

Sood, Kapil

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

"The FT key holder architecture, shown in Figure 11A-1, describes the FT key management entities" - sounds like exists in a vaccum. How does one relate this to the IEEE 802.11 architecture? This relationship is missing, and is a cause of complexity.

SuggestedRemedy

Change: "The FT key holder architecture, shown in Figure 11A-1, describes the FT key management entities and is defined in context of 802.11 basic reference model (Fig 5-10)."

Response *Response Status* **U**

ACCEPT.
In proposed change, "Fig 5-10" changed to "see Figure 5-10 in 5.9", and "802.11 basic reference model" changed to "the IEEE 802.11 basic reference model".

Cl **11A** *SC* **11A.2.2** *P* **49** *L* **26** # 147

Mccann, Stephen

Comment Type **E** *Comment Status* **A**

Both "IEEE 802.1X" and "802.1X" are referred to.

SuggestedRemedy

Clarify this term, based on the traditional use within IEEE 802.11-2007. There are many ohter areas of the document where this ambiguity also appears.

Response *Response Status* **C**

ACCEPT.
According to IEEE Style Guide, "IEEE 802.1X" is the correct form.

Cl **11A** *SC* **11A.2.2** *P* **49** *L* **30** # 174

Sood, Kapil

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

Line 26 in the 11A.2.2 clause reads "the functions of the IEEE 802.1X Authenticator are distributed among the R0KH and R1KH". Then, line 30 in same clause reads "The R0KH interacts with 802.1X to receive the MSK resulting from an EAP authentication" - sounds contradictory? First says that 802.1X resides between R0KH and R1KH; Second says that R0KH and 802.1X are distinct. This needs to be fixed.

SuggestedRemedy

Change: Line 30: The R0KH receives the MSK resulting from an EAP authentication. Line 26: "the functions of the Authenticator (defined in IEEE 802.1X) are distributed among the R0KH and R1KH"

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Page 49 line 30 changed to "The R0KH interacts with the IEEE 802.1X Authenticator to receive the MSK."

Cl **11A** *SC* **11A.2.2** *P* **49** *L* **30** # 343

Sood, Kapil

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

Line 26 in the 11A.2.2 clause reads "the functions of the IEEE 802.1X Authenticator are distributed among the R0KH and R1KH". Then, line 30 in same clause reads "The R0KH interacts with 802.1X to receive the MSK resulting from an EAP authentication" - sounds contradictory? First says that 802.1X resides between R0KH and R1KH; Second says that R0KH and 802.1X are distinct. This needs to be fixed. (This is revision of similar comment)

SuggestedRemedy

Change: Line 30: The R0KH receives the MSK resulting from an EAP authentication. Line 26: "the functions of the Authenticator (defined in IEEE 802.1X) are distributed among the R0KH and R1KH"

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Page 49 line 30 changed to "The R0KH interacts with the IEEE 802.1X Authenticator to receive the MSK."

Cl **11A** *SC* **11A.2.2** *P* **49** *L* **31** # 175

Sood, Kapil

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

R1KH is said to be part of 802.1X and then re-iterated to be interacting with 802.1X - sounds contradictory

SuggestedRemedy

Change: "The R1KH interacts with 802.1X functional block (Fig 5-10) to open the controlled port. Both the R0KH and R1KH interactions with 802.1X functional block occur within the SME of a STA.

Response *Response Status* **U**

REJECT
R1KH is not stated to be part of 802.1X.

Cl **11A** *SC* **11A.2.2** *P* **49** *L* **31** # 344

Sood, Kapil

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

R1KH is said to be part of 802.1X and then re-iterated to be interacting with 802.1X - sounds contradictory. (This is revision of similar comment)

SuggestedRemedy

Change: "The R1KH interacts with 802.1X functional block (Fig 5-10) to open the controlled port. Both the R0KH and R1KH interactions with 802.1X functional block occur within the SME of a STA.

Response *Response Status* **U**

REJECT
R1KH is not stated to be part of 802.1X.

Cl **11A** *SC* **11A.2.2** *P* **49** *L* **35** # 48

CHAPLIN, CLINT F

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

"The PMK-R0 in the Authenticator shall be cached&." seems to imply that the PMK-R0 must be cached, when 8.5.1.5.1 states that it may be deleted (e.g. not cached).
(Originally LB98/381 submitted by Cam-Winget, Nancy, during LB98 with ID Cam-Winget/23)

SuggestedRemedy

Change to "The PMK-R0 in the Authenticator shall be derived and may be cached in a component called the R0KH."

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Sentence deleted

Cl **11A** *SC* **11A.2.2** *P* **49** *L* **43** # 49

CHAPLIN, CLINT F

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

R0KH-ID and R1KH-ID shall be unique within the same mobility domain. This is a strict security requirement for a STA to distinguish between multiple entities that it will be executing the key hierarchy with. R0KH-ID and R1KH-ID uniqueness cannot be mere assumptions.
(Originally LB98/387 submitted by Sood, Kapil, during LB98 with ID Sood/036)

SuggestedRemedy

Change "Each R0KH-ID and R1KH-ID is assumed to be expressed as a unique identifier within the Mobility Domain." to "Each R0KH-ID and R1KH-ID shall be a unique identifier within the Mobility Domain."

Response *Response Status* **U**

REJECT.
IEEE 802.11-2007 has requirements stated as assumptions.

Cl **11A** *SC* **11A.2.2** *P* **49** *L* **43** # 177

Sood, Kapil

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

The R0KH-ID and R1KH-ID shall always be unique within the mobility domain. This is a strong security requirement. Without this uniqueness property, the STA and AP cannot assure themselves that they are communicating with the right entity. This uniqueness is also a strongly desired property that this FT security protocol is based upon.

SuggestedRemedy

Change: "Each R0KH-ID and R1KH-ID shall be expressed as a unique identifier within the Mobility"

Response *Response Status* **U**

REJECT.
IEEE 802.11-2007 has requirements stated as assumptions.

Cl **11A** *SC* **11A.2.2** *P* **49** *L* **44** # 178

Sood, Kapil

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

Not any STA, a non-AP STA

SuggestedRemedy

Change: "This identifier is communicated to the non-AP STA and other key"

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.2.2** *P* **49** *L* **54** # 303

Malinen, Jouni

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

Typo

SuggestedRemedy

Replace "R0H-ID" with "R0KH-ID".

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.2.2** *P* **49** *L* **55** # 179

Sood, Kapil

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

Typo on R0H-ID

SuggestedRemedy

Change: R0KH-ID

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.2.2** *P* **50** *L* **13** # 119

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Typo
(Originally LB105/11 submitted by Malinen, Jouni, during LB105 with ID Malinen/09)

SuggestedRemedy

Replace "dot11FTR0eyHolderID" with "dot11FTR0KeyHolderID".

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.2.2** *P* **50** *L* **13** # 129

HEUBAUM, KARL F

Comment Type **E** *Comment Status* **A**

The letter "K" is missing in "The MIB variables dot11FTR0eyHolderID and..."

SuggestedRemedy

Change to "The MIB variables dot11FTR0KeyHolderID and..."

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.2.2** *P* **50** *L* **13** # 180

Sood, Kapil

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

The MIB variable is not dot11FTR0eyHolderID" - maybe, a typo

SuggestedRemedy

Change: "dot11FTR0KeyHolderID"

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.2.2** *P* **50** *L* **13** # 304

Malinen, Jouni

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

Typo

SuggestedRemedy

Replace "dot11FTR0eyHolderID" with "dot11FTR0KeyHolderID".

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.2.2** *P* **50** *L* **17** # 140

Chaplin, Clint F

Comment Type **TR** *Comment Status* **R** *Key distribution*

The document is deficient in not specifying some type of key transfer from the R0KH to the R1KH. A default mechanism needs to be defined in 11r. While AP-AP communication is outside the scope of the MAC/PHY, the definition of the MIB is within scope of 802.11. A MIB-based key transfer should be included in 11r. (submitted by Bill Marshall)

SuggestedRemedy

Incorporate latest revision of 11-06-1677-xx-000r-key-distribution-via-snmp.doc into the amendment

Response *Response Status* **U**

REJECT
From a system point of view, key distribution should be done by a layer three protocol. Any layer three protocol would be out of scope for IEEE 802.11r; the PAR only authorizes MAC changes. Assumed requirements for the key distribution are given in 11A.2.2.

Cl **11A** *SC* **11A.2.2** *P* **50** *L* **19** # 51

CHAPLIN, CLINT F

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

"&includes the PMK-R1,&" is insufficient as all other components of SA are also needed to be transferred which are stated in the PMK-R1 PMKSA definition".
(Originally LB98/444 submitted by Sood, Kapil, during LB98 with ID Sood/041)

SuggestedRemedy

Change to "&includes the PMK-R1 PMKSA, &"

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.2.2** *P* **50** *L* **32** # 346

Sood, Kapil

Comment Type **TR** *Comment Status* **A** *Security assumptions*

"The mutual authentication between the R0KH and a R1KH authorizes the R1KH to obtain and hold
the PMK-R1. If the mutual authentication is separate from the authentication to authorize an R1KH,
then the R1KH shall bind the same identity with the mutual authenticated protection channel" - the first sentence is a repeat of the previous bullet. The second sentence is obscure - I could not unambiguously parse what was being conveyed through the 2nd sentence. This is mentioning a second authenication scheme that is not being defined in this draft - why is this not an EAP issue, entirely. The second authorization scheme is desired, but is out of scope. (This is revision of similar comment)

SuggestedRemedy

Delete the entire bullet, OR, Change the second sentence, as there seems to be a specific dependency that this sentence is trying to convey: "The mutual authentication between the R0KH and a R1KH authorizes the R1KH to obtain and hold the PMK-R1. An authorization scheme is outside the scope, but it is assumed that if the mutual authentication for secure channel is separate from the authentication to authorize an R1KH, then the R1KH shall bind the authorization identity of R1KH with the mutual authenticated protection channel."

Response *Response Status* **U**

ACCEPT.
Entire bullet deleted.

Cl **11A** *SC* **11A.2.2** *P* **50** *L* **32** # 181

Sood, Kapil

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

"The mutual authentication between the R0KH and a R1KH authorizes the R1KH to obtain and hold
the PMK-R1. If the mutual authentication is separate from the authentication to authorize an R1KH,
then the R1KH shall bind the same identity with the mutual authenticated protection channel" - the first sentence is a repeat of the previous bullet. The second sentence is obscure - I could not unambiguously parse what was being conveyed through the 2nd sentence.

SuggestedRemedy

Change the second sentence, as there seems to be a specific dependency that this sentence is trying to convey: "The mutual authentication between the R0KH and a R1KH authorizes the R1KH to obtain and hold the PMK-R1. If the mutual authentication for secure channel is separate from the authentication to authorize an R1KH, then the R1KH shall bind the authorization identity of R1Kh with the mutual authenticated protection channel."

Response *Response Status* **U**

ACCEPT.
Entire bullet deleted.

Cl **11A** *SC* **11A.2.2** *P* **50** *L* **32** # 52

CHAPLIN, CLINT F

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

"&the same identity with the&" is ambiguous. No clear what the "same" is referring to? (Originally LB98/447 submitted by Sood, Kapil, during LB98 with ID Sood/042)

SuggestedRemedy

Change "the same identity used in authentication to authorize with the&"

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.2.2** *P* **50** *L* **35** # 53

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

Do you mean "integrity protection" when the draft states "authenticity"? We already have plenty of bullets on authentication so I am pretty sure by now that authenticity is present! (Originally LB98/448 submitted by Sood, Kapil, during LB98 with ID Sood/043)

SuggestedRemedy

Change "authenticity" to "integrity protection".

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.2.2** *P* **50** *L* **43** # 182

Sood, Kapil

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

"The S0KH interacts with 802.1X to receive the MSK resulting from an EAP authentication. The S1KH
interacts with 802.1X to open the controlled port. Both the S0KH and S1KH interactions with 802.1X occur
within the SME of a STA." - they interact with the 802.1X functional block of Fig 5-10 of 802.11 reference model. This fact is missing.

SuggestedRemedy

Change: "The S0KH interacts with 802.1X functional block (Fig 5-10) to receive the MSK resulting from an EAP authentication. The S1KH interacts with 802.1X functional block (Fig 5-10) to open the controlled port. Both the S0KH and S1KH interactions with 802.1X occur within the SME of a STA."

Response *Response Status* **U**

ACCEPT.
In proposed change, "Fig 5-10" changed to "see Figure 5-10 in 5.9", and "802.1X functional block" changed to "the 802.1X functional block"

Cl **11A** *SC* **11A.2.2** *P* **50** *L* **43** # 347

Sood, Kapil

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

"The S0KH interacts with 802.1X to receive the MSK resulting from an EAP authentication. The S1KH
interacts with 802.1X to open the controlled port. Both the S0KH and S1KH interactions with 802.1X occur
within the SME of a STA." - they interact with the 802.1X functional block of Fig 5-10 of 802.11 reference model. This fact is missing. (This is revision of similar comment)

SuggestedRemedy

Change: "The S0KH interacts with 802.1X functional block (Fig 5-10) to receive the MSK resulting from an EAP authentication. The S1KH interacts with 802.1X functional block (Fig 5-10) to open the controlled port. Both the S0KH and S1KH interactions with 802.1X occur within the SME of a STA."

Response *Response Status* **U**

ACCEPT.
In proposed change, "Fig 5-10" changed to "see Figure 5-10 in 5.9", and "802.1X functional block" changed to "the 802.1X functional block"

Cl **11A** *SC* **11A.2.2** *P* **50** *L* **5** # 50

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

Bullet 2 is too wordy and repetitive. We know from previous paragraphs that R1KH is part of Authenticator.
(Originally LB98/391 submitted by Sood, Kapil, during LB98 with ID Sood/040)

SuggestedRemedy

Change bullet 2 on line 50 as "The R1KH shall derive and distribute the GTK to all connected STAs."

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.2.2** *P* **50** *L* **5** # 148

Mccann, Stephen

Comment Type **E** *Comment Status* **R**

The use of the term "IEEE 802.11" is not required within this amendment

SuggestedRemedy

Remove all references to IEEE 802.11

Response *Response Status* **C**

REJECT.
IEEE Style Manual, clause 13.9 states "When referring to the document, i.e. the standard that is published, IEEE Std 1234 should be used. When referring to the technology that the document standardizes, IEEE 1234 should be used."

Cl **11A** *SC* **11A.2.3** *P* **50** *L* **54** # 120

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A** *Other*

S0KH and S1KH identities should be defined as a "shall". Each key holder should be mandated as having a specific identify, otherwise the security does not work.
(Originally LB105/12 submitted by Sood, Kapil, during LB105 with ID Sood/10)

SuggestedRemedy

Change "S0KH and S1KH are identified" to "S0KH and S1KH shall be identified"

Response *Response Status* **C**

ACCEPT

Cl **11A** *SC* **11A.2.3** *P* **50** *L* **55** # 121

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

S0KH and S1KH are defined as 2 separate sub-entities within the Supplicant. Therefore, the key scope should also be at the same level.
(Originally LB105/13 submitted by Sood, Kapil, during LB105 with ID Sood/11)

SuggestedRemedy

Change "and shall not expose the PMK-R0 or PMK-R1 to parties outside the supplicant" to ". S0KH shall not expose the PMK-R0 to other parties, and shall not expose the PMK-R1 to parties other than the authorized S1KH. S1KH shall not expose the PMK-R1 to other parties."

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.3** *P* **50** *L* **60** # 327

Sood, Kapil

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

The use of MDIE in the beacons/probes is sufficient to indicate that FT is supported by the AP. There is no technical reason or technical justification to have MDIE and then additional bits within the MDIE policy field to indicate FT support. From STA implementation standpoint, having to check multiple fields results in complexity and requires additional error cases to be validated/conveyed to AP. In addition, I do not see TGu using the MDIE (which was the original reason for making MDIE extensible), and so, no reason to keep this generality at the expense of TGr implementation complexity. (This is a revision of similar comment)

SuggestedRemedy

Clause 11A.3, pg 50, line 61-62 change "The Fast BSS Transition capability is advertised in the Beacon and Probe Response frames by including the MDIE."

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.3** *P* **50** *L* **60** # 152

Sood, Kapil

Comment Type **TR** *Comment Status* **A** *DIE indication of FT capability*

The use of MDIE in the beacons/probes is sufficient to indicate that FT is supported by the AP. There is no technical reason or technical justification to have MDIE and then additional bits within the MDIE policy field to indicate FT support. From STA implementation standpoint, having to check multiple fields results in complexity and requires additional error cases to be validated/conveyed to AP. In addition, I do not see TGu using the MDIE (which was the original reason for making MDIE extensible), and so, no reason to keep this generality at the expense of TGr implementation complexity.

SuggestedRemedy

Clause 11A.3, pg 50, line 61-62 change "The Fast BSS Transition capability is advertised in the Beacon and Probe Response frames by including the MDIE."

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.3** *P* **50** *L* **63** # 54

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Suggested wording
(Originally LB98/451 submitted by Malinen, Jouni, during LB98 with ID Malinen/34)

SuggestedRemedy

Replace "Beacons and Probe Response frames" with "Beacon and Probe Response frames".

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.3** *P* **50** *L* **65** # 56

CHAPLIN, CLINT F

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

"When MDIE is used without the Fast BSS Transition Capability(Fast &" is insufficient. This standard is not describing any situations (besides errors) when this MDIE is not used. A direct statement is much clearer to developers and eliminates confusion.
(Originally LB98/453 submitted by Sood, Kapil, during LB98 with ID Sood/044)

SuggestedRemedy

Change "When Fast BSS Transition over air and Fast BSS Transition over DS are both set to zero, then all other bits of the Fast BSS Capability and Policy field shall be ignored."

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Statement deleted

Cl **11A** *SC* **11A.3** *P* **50** *L* **65** # 55

CHAPLIN, CLINT F

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

MDIE is only included if FT is supported, so there is no need for specifying contents of the IE for a case where FT is not supported.
(Originally LB98/452 submitted by Malinen, Jouni, during LB98 with ID Malinen/10)

SuggestedRemedy

Remove "When MDIE is used without the Fast BSS Transition Capability (Fast BSS Transition over air and Fast BSS Transition over DS both set to zero), then all other bits of the Fast BSS Capability and Policy field shall be ignored." In addition, replace "If Fast BSS Transition is supported, at least" with "At least" on line 29.

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.4.2** *P* **51** *L* **29** # 183

Sood, Kapil

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

Not any STA, a non-AP STA

SuggestedRemedy

Change: where the SME of the non-AP STA enables

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.4.2** *P* **51** *L* **32** # 348

Sood, Kapil

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

"Reassociation frames are supported to enable FT and non-FT APs in an ESS." - what does this mean? (This is revision of similar comment)

SuggestedRemedy

Delete this line, or clarify

Response *Response Status* **U**

ACCEPT
In addition to Association frames, Reassociation frames are supported in the Initial Mobility Domain Association to enable both FT and non-FT APs to be present in a single ESS.

Cl **11A** *SC* **11A.4.2** *P* **51** *L* **32** # 184

Sood, Kapil

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

"Reassociation frames are supported to enable FT and non-FT APs in an ESS." - what does this mean?

SuggestedRemedy

Delete this line, or clarify

Response *Response Status* **U**

ACCEPT
In addition to Association frames, Reassociation frames are supported in the Initial Mobility Domain Association to enable both FT and non-FT APs to be present in a single ESS.

Cl **11A** *SC* **11A.4.2** *P* **51** *L* **35** # 352

Sood, Kapil

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

The specification does not specify if a non-AP STA can execute a rekey procedure to refresh its key hierarchy, while the non-AP STA is currently associated with an AP. This is a missing functionality and an important use case for deployment - we have received this feedback from large WLAN enterprise customers. Regardless of the duration of the KeyLIfetime, non-AP STA will run out of KeyLifetime and disrupt ongoing user sessions - which is not an acceptable solution. If the non-AP STA has to disconnect from the AP and then execute the Initial Mobility Domain assoc procedures to referesh the key hierarchy, then this amendment would have failed to meet the user expectations. I understand that the non-AP STA can do the FT Initial Mobility Domain Assoc at any time (which will re-fresh the EAP key), but there ought to be text in this amendment to address this. (Look at DHCP for example) (This is revision of similar comment)

SuggestedRemedy

Add the following text in Clause 8.5.1.5.1 page 22 line 9 "FT Initial Mobility Domain Association procedure shall be used by a non-AP STA to create a fresh FT key hierarchy. After 50% of the KeyLifetime has passed, the non-AP STA will initiate the FT Initial Mobility Domain procedures."

Response *Response Status* **U**

REJECT.
The requirement to perform another Initial Mobility Domain Association is already stated in 11A.4.2, page 54 line 21.

Cl **11A** *SC* **11A.4.2** *P* **51** *L* **35** # 193

Sood, Kapil

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

The specification does not specify if a non-AP STA can execute an Initial Mobility Domain Association while it is currently associated with an AP. This is a missing functionality and an important use case. Regardless of the duration of the KeyLIfetime, Clients will run out of KeyLifetime and disrupt ongoing user sessions. If the client has to disconnect and then execute the Initial Mobility Domain assoc procedures, then this amendment would have failed to meet the user expectations.

SuggestedRemedy

Add the missing functionality by accepting my submission

Response *Response Status* **U**

REJECT.
The requirement to perform another Initial Mobility Domain Association is already stated in 11A.4.2, page 54 line 21.

Cl **11A** *SC* **11A.4.2** *P* **51** *L* **41** # 57

CHAPLIN, CLINT F

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

"&a modified 4-Way Handshake" - what does this mean? Where is this defined? This specification has been using "FT 4-Way Handshake " in previous clauses.
(Originally LB98/458 submitted by Sood, Kapil, during LB98 with ID Sood/045)

SuggestedRemedy

Change "&the FT 4-Way Handshake"

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.4.2** *P* **51** *L* **41** # 189

Sood, Kapil

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

The "modified" 4-way handshake is referred to as FT 4-way handshake elsewhere in this document.

SuggestedRemedy

Change "modified 4-way handshake" to "FT 4-way handshake"

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.4.2** *P* **52** *L* **15** # 58

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Typo
(Originally LB98/459 submitted by Malinen, Jouni, during LB98 with ID Malinen/36)

SuggestedRemedy

Replace "Anonce" with "ANonce" in Figure 204b.

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.4.2** *P* **52** *L* **38** # 202

Sood, Kapil

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

STA is not just any STA - it is a non-AP STA

SuggestedRemedy

Change on line 38: "non-AP STA -> AP" and on line 39: "AP -> non-AP STA"

Response *Response Status* **U**

REJECT.
Clause 11A is specific in applying only to an infrastructure BSS, and in such situations there is no ambiguity in the use of the term STA.

Cl **11A** *SC* **11A.4.2** *P* **52** *L* **53** # 203

Sood, Kapil

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

STA is not just any STA - it is a non-AP STA

SuggestedRemedy

Change on line 53: "non-AP STA -> AP" and on line 54: "AP -> non-AP STA"

Response *Response Status* **U**

REJECT.
Clause 11A is specific in applying only to an infrastructure BSS, and in such situations there is no ambiguity in the use of the term STA.

Cl **11A** *SC* **11A.4.2** *P* **53** *L* **13** # 186

Sood, Kapil

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

Supplicant is not the most precise component that does EAP. It is S0KH, as defined elsewhere in this document.

SuggestedRemedy

Make this document consistent by changing: "The S0KH shall use the value of R0KH-ID&"

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.4.2** *P* **53** *L* **19** # 188

Sood, Kapil

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

The key hierarchy in R0KH must exist for the same non-AP STA and within the same Mobility Domain ID => THEN only with the key hierarchy be deleted.

SuggestedRemedy

Change: "If a key hierarchy already exists for this non-AP STA belonging to same Mobility Domain (havind same MDID), the R0KH shall delete the existing"

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.4.2** *P* **53** *L* **19** # 187

Sood, Kapil

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

Not any STA, a non-AP STA

SuggestedRemedy

Change: "exists for this non-AP STA, the R0KH"

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.4.2** *P* **53** *L* **19** # 350

Sood, Kapil

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

The key hierarchy in R0KH must exist for the same non-AP STA and within the same Mobility Domain ID => THEN only with the key hierarchy be deleted. (This is revision of similar comment)

SuggestedRemedy

Change: "If a key hierarchy already exists for this non-AP STA belonging to same Mobility Domain (havind same MDID), the R0KH shall delete the existing"

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.4.2** *P* **53** *L* **41** # 59

CHAPLIN, CLINT F

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

EAPOL-Key frame notation is not followed correctly here. It looks like the new SM (SMK Message) parameter is missing here.
(Originally LB98/472 submitted by Malinen, Jouni, during LB98 with ID Malinen/77)

SuggestedRemedy

Replace "P, " with "P, 0, " in all four EAPOL-Key frames to add the new SM parameter.

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.4.2** *P* **53** *L* **47** # 190

Sood, Kapil

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

Insert a " " (space) between KeyLifetime, as elsewhere it is referred as "Key Lifetime"

SuggestedRemedy

Change "TIE[Key Lifetime]"

Response *Response Status* **U**

REJECT.
"TIE[KeyLifetime]" is consistently used in the document, as is "TIE[ReassociationDeadline]" (also without a space)

Cl **11A** *SC* **11A.4.2** *P* **53** *L* **8** # 185

Sood, Kapil

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

"The FTIE shall indicate a MIC information element count of zero (i.e., no MIC present), and have nonce and
MIC values of zero." - This statement is not accurate as it does not exactly and correctly specify the fields and values.

SuggestedRemedy

Change: "The FTIE shall set MIC Control field as zero to indicate MIC information element count of zero (i.e., no MIC present), and have Anonce, Snonce, and MIC fields set to values of zero."

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.4.2** *P* **53** *L* **8** # 349

Sood, Kapil

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

"The FTIE shall indicate a MIC information element count of zero (i.e., no MIC present), and have nonce and
MIC values of zero." - This statement is not accurate as it does not exactly and correctly specify the fields and values. (This is revision of similar comment)

SuggestedRemedy

Change: "The FTIE shall set MIC Control field as zero to indicate MIC information element count of zero (i.e., no MIC present), and have Anonce, Snonce, and MIC fields set to values of zero."

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.4.2** *P* **54** *L* **17** # 60

CHAPLIN, CLINT F

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

"Once the IEEE 802.1X controlled port is open, the PTK key lifetime timer is initiated to ensure that the lifetime of the PTKSA is no longer than the value provided in the Message 3 Key Lifetime TIE." - There is no connection between the controlled port ensuring the correct value of PTK is set in the timer. This implied connection is incorrect, so clearly de-lineate in 2 separete sentences.
(Originally LB98/473 submitted by Sood, Kapil, during LB98 with ID Sood/049)

SuggestedRemedy

Change "Once the IEEE 802.1X controlled port is open, the PTK key lifetime timer is initiated with the value provided in the Message 3 Key Lifetime TIE."

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Change "Once the IEEE 802.1X controlled port is open" to "Upon completion of a successful FT 4-Way Handshake"

Cl **11A** *SC* **11A.4.2** *P* **54** *L* **21** # 192

Sood, Kapil

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

All references to STA in lines 21-29 are for a non-AP STA.

SuggestedRemedy

Change in lines 21-29: "STA" to "non-AP STA"

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.4.2** *P* **54** *L* **25** # 351

Sood, Kapil

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

"If the AP sends a Deauthentication or Disassociation frame to the STA with reason code 2 ("Previous authentication
no longer valid"), then to continue its association in the Mobility Domain the STA shall perform the FT Initial
Mobility Domain Association procedures." What happens when an AP sends a disconnect (disassoc/deauth) to a non-AP STA with a reason code other than 2? If this AP is the one with which the non-AP STA performed Initial MD Assoc, then can the STA perform an FT with this AP using the existing key hierarchy? Different clients will make different assumptions and clients need to know if it needs to do full EAP, continue with the FT, or go away. This specification has not been proven inter-operable, and neither has this amendment specified any error branches - I would like to see detailed description of all error scenarios, as this would make all the difference between a successful and failed standard. (This is revision of similar comment)

SuggestedRemedy

At the end of this sentence, insert: "If an AP sends a deauthentication and disassociation to the non-AP STA, then the non-AP STA may reassociate with the same AP using the FT protocol.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
At end of sentence, insert "with any AP in the Mobility Domain."

Cl **11A** *SC* **11A.4.2** *P* **54** *L* **25** # 191

Sood, Kapil

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

"If the AP sends a Deauthentication or Disassociation frame to the STA with reason code 2 ("Previous authentication
no longer valid"), then to continue its association in the Mobility Domain the STA shall perform the FT Initial
Mobility Domain Association procedures." What happens when an AP sends a disconnect (disassoc/deauth) to a non-AP STA with a reason code other than 2? If this AP is the one with which the non-AP STA performed Initial MD Assoc, then can the STA perform an FT with this AP using the existing key hierarchy? This specification has not been proven inter-operable, and neither has this amendment specified any error branches - I would like to see detailed description of all error scenarios, as this would make all the difference between a successful and failed standard.

SuggestedRemedy

At the end of this sentence, insert: "If an AP sends a deauthentication and disassociation to the non-AP STA, then the non-AP STA may reassociate with the same AP using the FT protocol.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
At end of sentence, insert "with any AP in the Mobility Domain."

Cl **11A** *SC* **11A.4.3** *P* **55** *L* **1** # 204

Sood, Kapil

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

STA is not just any STA - it is a non-AP STA

SuggestedRemedy

Change on line 1: "non-AP STA -> AP" and on line 2: "AP -> non-AP STA"

Response *Response Status* **U**

REJECT.
Clause 11A is specific in applying only to an infrastructure BSS, and in such situations there is no ambiguity in the use of the term STA.

Cl **11A** *SC* **11A.4.3** *P* **55** *L* **17** # 205

Sood, Kapil

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

STA is not just any STA - it is a non-AP STA

SuggestedRemedy

Change on line 17: "non-AP STA -> AP" and on line 18: "AP -> non-AP STA"

Response *Response Status* **U**

REJECT.
Clause 11A is specific in applying only to an infrastructure BSS, and in such situations there is no ambiguity in the use of the term STA.

Cl **11A** *SC* **11A.5** *P* **55** *L* **40** # 122

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **R**

There's been a partial renaming of Fast BSS transition protocol to FT protocol. However it hasn't occurred in the heading of 11A.5
(Originally LB105/14 submitted by Stephens, Adrian, during LB105 with ID Stephens/10)

SuggestedRemedy

Rename to match changes make in the body text.

Response *Response Status* **C**

REJECT.
"FT" is defined as an acronym meaning "Fast BSS Transition", so the meaning is identical. IEEE Style Manual states that acronyms should be written out in their first usage in the text. Clause and subclause titles appear in the frontmatter, prior to any text. Therefore acronyms appearing in titles should be written out in full.

Note that the document will be professionally edited prior to publication, and the interpretation of the TGr technical editor may be overruled at that time.

Cl **11A** *SC* **11A.5.1** *P* **55** *L* **46** # 61

CHAPLIN, CLINT F

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

What does the word "systems" refer to?
(Originally LB98/474 submitted by Lemberger, Uriel, during LB98 with ID Lemberger/10)

SuggestedRemedy

Change "systems" to specific STA and/or AP as required

Response *Response Status* **U**

ACCEPT.
Changed to "STAs"

Cl **11A** *SC* **11A.5.1** *P* **55** *L* **46** # 62

CHAPLIN, CLINT F

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

What is the word "system" referring to?
(Originally LB98/475 submitted by Sood, Kapil, during LB98 with ID Sood/050)

SuggestedRemedy

Change "System" to "STA"

Response *Response Status* **U**

ACCEPT.
Changed to "STAs"

Cl **11A** *SC* **11A.5.2** *P* **56** *L* **21** # 63

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Typo
(Originally LB98/477 submitted by Malinen, Jouni, during LB98 with ID Malinen/37)

SuggestedRemedy

Replace "Snonce" with "SNonce" in Figure 204d.

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.5.2** *P* **56** *L* **22** # 322

Malinen, Jouni

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

Inconsistent spelling of SNonce.

SuggestedRemedy

Replace "Snonce" with "SNonce" on page 56 line 22 (in Figure 11A-4) and on page 58 line 20 (in Figure 11A-5).

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.5.2** *P* **56** *L* **34** # 353

Sood, Kapil

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

"specify the PTKSA" - what does this mean? The STA and AP use the Authentication Sequence to indicate the PMK-R0 SA and then derive the PTKSA. (This is revision of similar comment)

SuggestedRemedy

Change: "specify the PMKR0Name"

Response *Response Status* **U**

REJECT.
The PTKSA includes numerous items (see 8.4.1.1.2), and more than just PMKR0Name is needed to derive it.

Cl **11A** *SC* **11A.5.2** *P* **56** *L* **34** # 194

Sood, Kapil

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

"specify the PTKSA" - what does this mean? The STA and AP use the Authentication Sequence to indicate the PMK-R0 SA and then derive the PTKSA.

SuggestedRemedy

Change: "specify the PMKR0Name"

Response *Response Status* **U**

REJECT.
The PTKSA includes numerous items (see 8.4.1.1.2), and more than just PMKR0Name is needed to derive it.

Cl **11A** *SC* **11A.5.2** *P* **56** *L* **34** # 64

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

Isn't FT Authentication sequence used to derive PTK and generate PTKSA; not just to "specify the PTKSA"? How does it "specify" the PTKSA? Or is this supposed to "specify" which PMK-R1 is used?
(Originally LB98/478 submitted by Malinen, Jouni, during LB98 with ID Malinen/38)

SuggestedRemedy

Replace "to specify the PTKSA" with "to specify the PMK-R1 SA".

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.5.2** *P* **56** *L* **43** # 201

Sood, Kapil

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

STA is not just any STA - it is a non-AP STA

SuggestedRemedy

Change on line 43: "non-AP STA -> Target AP" and on line 46: "Target AP -> non-AP STA"

Response *Response Status* **U**

REJECT.
Clause 11A is specific in applying only to an infrastructure BSS, and in such situations there is no ambiguity in the use of the term STA.

Cl **11A** *SC* **11A.5.2** *P* **56** *L* **50** # 367

Sood, Kapil

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

The FT protocols do not define the behavior of non-AP STA or AP in the scenario when a non-AP STA initiates an FT to its current AP. There can be scenarios due to buggy non-AP implementations or due to non-AP STA looking its current connection state, or due to non-AP STA not having processed the disconnect, or AP not having cleaned up non-AP STA's state - that a non-AP STA chooses to FT to an AP that currently holds state for this non-AP STA. (This is revision of similar comment)

SuggestedRemedy

Insert in Clause 11A.5.2 page 57 line 6 (also on 11A.5.3, page 58, line 65): "When a non-AP STA initiates an FT to an AP that currently holds association state for that non-AP STA, then the AP shall send a disassociate request to that non-AP STA with status code 57 ("New FT Initiated to same AP"). Clause 7.3.1.9, page 8, line 32 insert "57 New FT Initiated to same AP".

Response *Response Status* **U**

REJECT
P802.11r D7.0 allows the STA to initiate a Fast BSS Transition to its currently associated AP.

As a clarification in the draft, insert a paragraph break after the second sentence of the paragraph beginning "Upon a successful reassociation" on page 68 line 48. Change first sentence of the new paragraph from "The STA shall delete" to "Upon a successful reassociation, the STA shall delete"

Cl **11A** *SC* **11A.5.2** *P* **56** *L* **50** # 226

Sood, Kapil

Comment Type **TR** *Comment Status* **R** *Roam-to-self*

The FT protocols do not define the behavior of non-AP STA or AP in the scenario when a non-AP STA initiates an FT to its current AP. There can be scenarios due to buggy non-AP implementations or due to non-AP STA looking its current connection state, or due to non-AP STA not having processed the disconnect, or AP not having cleaned up non-AP STA's state - that a non-AP STA chooses to FT to an AP that currently holds state for this non-AP STA.

SuggestedRemedy

Insert in Clause 11A.5.2 page 57 line 6 (also on 11A.5.3, page 58, line 65): "When a non-AP STA initiates an FT to an AP that currently holds association state for that non-AP STA, then the AP shall send a disassociate request to that non-AP STA with status code 57 ("New FT Initiated to same AP"). Clause 7.3.1.9, page 8, line 32 insert "57 New FT Initiated to same AP".

Response *Response Status* **U**

REJECT
P802.11r D7.0 allows the STA to initiate a Fast BSS Transition to its currently associated AP.

As a clarification in the draft, insert a paragraph break after the second sentence of the paragraph beginning "Upon a successful reassociation" on page 68 line 48. Change first sentence of the new paragraph from "The STA shall delete" to "Upon a successful reassociation, the STA shall delete"

Cl **11A** *SC* **11A.5.2** *P* **57** *L* **10** # 196

Sood, Kapil

Comment Type **TR** *Comment Status* **A** *STA behavior*

The case of when an Authentication is failed, then what is a STA supposed to do is not defined. Problems occur when a STA is rejected from an AP but keeps coming back to the same AP. Or, STA may never come back to that AP. Both the AP and STA should know if the STA is coming back. This standard should define explicit behavior of failure cases.

SuggestedRemedy

Clause 11A.5.2 page 57 line 5: "Subsequent to an FT Authentication Request rejection, a STA may retry the FT Authentication Request with the correct set of parameters."

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Inserted "Subsequent to an FT Authentication Request rejection, a STA may retry the FT Authentication Request." The STA has no way of knowing the "currect set" of parameters, and the previous parameters may be acceptable to the AP at a different time.

Cl **11A** *SC* **11A.5.2** *P* **57** *L* **10** # 355

Sood, Kapil

Comment Type **TR** *Comment Status* **R** *STA behavior*

The case of when an Authentication is failed, then what is a STA supposed to do is not defined. Problems occur when a STA is rejected from an AP but keeps coming back to the same AP. Or, STA may never come back to that AP. Both the AP and non-AP STA should know if the non-AP STA is coming back. This standard should define explicit behavior of failure cases. (This is revision of similar comment)

SuggestedRemedy

Clause 11A.5.2 page 57 line 5: "For FT Authentication Request failures described above, a non-AP STA may re-issue a new FT Authentication Request to the same target AP after correcting the indicated error. If the AP rejected with status code 56 ("FT failed due to poor channel conditions"), then a non-AP STA shall not retry the FT Authentication Request with the same AP for a time indicated by the reassociation deadline time." Insert a new row in Table 7-23, Clause 7.3.1.9, page 8 line 30 "56 FT failed due to poor channel conditions."

Response *Response Status* **U**

REJECT
The base specification is rightly silent on the proper behavior of the STA in these situations. The proposed change given in this comment has no correlation to the situation described in the comment.

Cl **11A** *SC* **11A.5.2** *P* **57** *L* **24** # 197

Sood, Kapil

Comment Type **TR** *Comment Status* **R** *STA behavior*

Another case is when a STA times out trying to send an FT Authentication Request to the AP - then, what is the desired action for a STA? The STA may be timing out because of multiple reasons incl. channel conditions, collisions, interference, etc. What is the rate at which the STA should send these FT Authentication Request messages? Setting a rate is important because a STA may negotiate FT protocol at a lower rate, but then try to use the AP for data at a higher rate - leading to channel problems for itself and other STAs.

SuggestedRemedy

Insert in Clause 11A.5.2 page 57 line 30: "The non-AP STA and AP shall use their desired Tx data rate as the rate for sending FT Authentication messages. Each entity may retry the transmission 5 times before dropping the Tx rate. The Tx rate shall not be dropped beyond one rate lower than what is intended to be used for data packets." Similar sentence needs to be added to other sub-clauses in 11A.5 and 11A.6 and 11A.7

Response *Response Status* **U**

REJECT
The base specification does not specify rate adaption algorithms for the STA.

Cl **11A** *SC* **11A.5.2** *P* **57** *L* **24** # 356

Sood, Kapil

Comment Type **TR** *Comment Status* **R** *STA behavior*

Another case is when a STA times out trying to send an FT Authentication Request to the AP - then, what is the desired action for a STA? The STA may be timing out because of multiple reasons incl. channel conditions, collisions, interference, or maybe because AP to trying to contact the prescribed R0KH, etc. These cases is not new and happens in WLANs today - but the problems are exacerbated due to roaming when reducing rates and retries and backend connectivity and delays (as happen in distributed systems). Such steps need to be included in the amendment in order to address failure recovery scenarios - as, those are the most important ones. (This is revision of similar comment)

SuggestedRemedy

Insert in Clause 11A.5.2 page 57 line 6 "If a non-AP STA times out waiting for a FT Authentication Response from the target AP, then the non-AP STA shall abort FT to that AP."

Response *Response Status* **U**

REJECT.
This case is already covered in the paragraph starting on page 57 line 24.

Cl **11A** *SC* **11A.5.2** *P* **57** *L* **5** # 195

Sood, Kapil

Comment Type **TR** *Comment Status* **A** *PMK-R1 latency for pull*

The invalid PMKR0Name rejection should not be a "may". This should be a "shall" as the STA needs to know exactly under what conditions was the Auth failed. No inter-op has been done for this protocol, so I'dlike to see well defined failure cases.

SuggestedRemedy

Change "the AP shall reject the Authentication Request with status code 53 ("Invalid PMKID").

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
If the RSNIE in the Authentication Request frame contains an invalid PMKR0Name, and the Target AP has determined that it is an invalid PMKR0Name, the AP shall reject the Authentication Request with status code 53 ("Invalid PMKID"). If the Target 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 Authentication Request with status code 0. If the requested R0KH is not reachable, the AP shall respond to the Authentication Request with status code <ANA> ("R0KH unreachable").

Cl **11A** *SC* **11A.5.2** *P* **57** *L* **5** # 354

Sood, Kapil

Comment Type **TR** *Comment Status* **A** *PMK-R1 latency for pull*

The invalid PMKR0Name rejection should not be a "may". This should be a "shall" as the STA needs to know exactly under what conditions was the Auth failed. No inter-op has been done for this protocol, so I'dlike to see well defined failure cases. (This is revision of similar comment)

SuggestedRemedy

Change "the AP shall reject the Authentication Request with status code 53 ("Invalid PMKID").

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
If the RSNIE in the Authentication Request frame contains an invalid PMKR0Name, and the Target AP has determined that it is an invalid PMKR0Name, the AP shall reject the Authentication Request with status code 53 ("Invalid PMKID"). If the Target 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 Authentication Request with status code 0. If the requested R0KH is not reachable, the AP shall respond to the Authentication Request with status code <ANA> ("R0KH unreachable").

Cl **11A** *SC* **11A.5.3** *P* **57** *L* **33** # 357

Sood, Kapil

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

Mandating that the STA must see the MDIE from the Target AP to determine if an "over-the-DS" can be done to that Target AP completely defeats the purpose of the "over-the-DS". The over-the-DS scheme is most useful when the STA does not see those APs and does not need to waste important transition time scanning for those APs. There is a note in 11A.3 page 51 line 12, which says that the standard assumes that the FT Policy bits in MDIE are administered consistently across the MD - this should not be a note, it should be a "shall" requirement. From STA's perspective, FT will actually improve when it knows that alls APs within a MD are reachable over-the-DS when they all advertise exactly the same MDIE. (This is revision of similar comment)

SuggestedRemedy

Change Clause 11A.3, page 51 line 12: "The Fast BSS Transition policy bits in the MDIE is assumed to be administered consistently across the Mobility Domain" Change Clause 11A.5.3 page 57 line 33: "A non-AP STA shall not initiate a Fast BSS Transition over-the-DS to a target AP if the MDIE received from AP in FT 4-way handshake contains the Fast BSS Transition over DS bit set to zero." Insert this in Clause 11A.5.2 page 56 line 60 and Clause 11A.5.3 page 58 line 57 "The MDIE in the Authentication Request shall be the MDIE that was negotiated by the non-AP STA in the Initial Mobility Domain associaiton". OR, remove over-the-DS mechanisms as they will just not work.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
The 11k neighbor report indicates that the target AP is advertising an identical MDIE as the current AP, so over-the-air scanning is not required. It is assumed by the standard that the MDIE is administered consistently across the Mobility Domain (stated in 11A.3), so the settings obtained from the current AP are the same as those of the target AP, and are the same as those of the AP with which the non-AP STA did its Initial Mobility Domain Association. The requirement that the non-AP STA shall not initiate over-the-DS unless the MDIE bit is set is already present in 11A.5.3. No text changes needed.

Cl **11A** *SC* **11A.5.3** *P* **57** *L* **33** # 198

Sood, Kapil

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

Mandating that the STA must see the MDIE from the Target AP to determine if an "over-the-DS" can be done to that Target AP completely defeats the purpose of the "over-the-DS". The over-the-DS scheme is most useful when the STA does not see those APs and does not need to waste important transition time scanning for those APs. There is a note in 11A.3 page 51 line 12, which says that the standard assumes that the FT Policy bits in MDIE are administered consistently across the MD - this should not be a note, it should be a "shall" requirement. From STA's perspective, FT will actually improve when it knows that alls APs within a MD are reachable over-the-DS when they all advertise exactly the same MDIE.

SuggestedRemedy

Change Clause 11A.3, page 51 line 12: "The Fast BSS Transition policy bits in the MDIE shall be administered consistently across the Mobility Domain" Change Clause 11A.5.3 page 57 line 33: "A non-AP STA shall not initiate a Fast BSS Transition over-the-DS to a target AP if the MDIE received from AP in FT 4-way handshake contains the Fast BSS Transition over DS bit set to zero."

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
The 11k neighbor report indicates that the target AP is advertising an identical MDIE as the current AP, so over-the-air scanning is not required. It is assumed by the standard that the MDIE is administered consistently across the Mobility Domain (stated in 11A.3), so the settings obtained from the current AP are the same as those of the target AP, and are the same as those of the AP with which the non-AP STA did its Initial Mobility Domain Association. The requirement that the non-AP STA shall not initiate over-the-DS unless the MDIE bit is set is already present in 11A.5.3. No text changes needed.

Cl **11A** *SC* **11A.5.3** *P* **58** *L* **20** # 65

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Typo
(Originally LB98/485 submitted by Malinen, Jouni, during LB98 with ID Malinen/39)

SuggestedRemedy

Replace "Snonce" with "SNonce" in Figure 204e.

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.5.3** *P* **58** *L* **36** # 199

Sood, Kapil

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

The STA and TargetAP are addresses of these entities as defined in 7.4.7. This should be clarified here.

SuggestedRemedy

Change Clause 11A.5.3 page 58 lines 36-41 in the parameter list only: "STA" to "STA Address" and "TargetAP" to "Target AP Address"

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.5.3** *P* **58** *L* **36** # 200

Sood, Kapil

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

STA is not just any STA - it is a non-AP STA

SuggestedRemedy

Change on line 36: "non-AP STA -> Target AP" and on line 39: "Target AP -> non-AP STA"

Response *Response Status* **U**

REJECT.
Clause 11A is specific in applying only to an infrastructure BSS, and in such situations there is no ambiguity in the use of the term STA.

Cl **11A** *SC* **11A.5.3** *P* **58** *L* **43** # 206

Sood, Kapil

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

STA is not just any STA - it is a non-AP STA

SuggestedRemedy

Lines 42-51 change: "STA" to "non-AP STA"

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.5.3** *P* **58** *L* **45** # 123

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

"(Action frame of category[#488] Fast BSS Transition)" - I'm not sure the change was adequate - i.e. it is not definitive.
(Originally LB105/15 submitted by Stephens, Adrian, during LB105 with ID Stephens/11)

SuggestedRemedy

Quote both category and action

Response *Response Status* **C**

ACCEPT.
Changed to "Action frame of category Fast BSS Transition and Action field Fast BSS Transition Request". Similar change at line 49.

Cl **11A** *SC* **11A.5.3** *P* **58** *L* **65** # 358

Sood, Kapil

Comment Type **TR** *Comment Status* **A** *PMK-R1 latency for pull*

The invalid PMKR0Name rejection should not be a "may". This should be a "shall" as the STA needs to know exactly under what conditions was the Auth failed. No inter-op has been done for this protocol, so I'd like to see well defined failure cases. (This is revision of similar comment)

SuggestedRemedy

Change "the AP shall reject the Authentication Request with status code 53 ("Invalid PMKID").

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
If the RSNIE in the Authentication Request frame contains an invalid PMKR0Name, and the Target AP has determined that it is an invalid PMKR0Name, the AP shall reject the Authentication Request with status code 53 ("Invalid PMKID"). If the Target 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 Authentication Request with status code 0. If the requested R0KH is not reachable, the AP shall respond to the Authentication Request with status code <ANA> ("R0KH unreachable").

Cl **11A** *SC* **11A.5.3** *P* **58** *L* **65** # 207

Sood, Kapil

Comment Type **TR** *Comment Status* **A** *PMK-R1 latency for pull*

The invalid PMKR0Name rejection should not be a "may". This should be a "shall" as the STA needs to know exactly under what conditions was the Auth failed. No inter-op has been done for this protocol, so I'd like to see well defined failure cases.

SuggestedRemedy

Change "the AP shall reject the Authentication Request with status code 53 ("Invalid PMKID").

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
If the RSNIE in the Authentication Request frame contains an invalid PMKR0Name, and the Target AP has determined that it is an invalid PMKR0Name, the AP shall reject the Authentication Request with status code 53 ("Invalid PMKID"). If the Target 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 Authentication Request with status code 0. If the requested R0KH is not reachable, the AP shall respond to the Authentication Request with status code <ANA> ("R0KH unreachable").

Cl **11A** *SC* **11A.5.3** *P* **59** *L* **1** # 208

Sood, Kapil

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

STA is not just any STA - it is a non-AP STA

SuggestedRemedy

Line 1 change: "STA" to "non-AP STA"

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.5.3** *P* **59** *L* **10** # 209

Sood, Kapil

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

STA is not just any STA - it is a non-AP STA

SuggestedRemedy

Line 10-12 change 2 occurances of "STA" to "non-AP STA". Line 13: change "non-AP STA". Line 18 change "non-AP STA"

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.5.3** *P* **59** *L* **18** # 364

Sood, Kapil

Comment Type **TR** *Comment Status* **R** *STA behavior*

What if multiple FT Request frames are issued by a non-AP STA to the same Target AP. The scenario being that a response to first never came back, and then non-AP STA issued another FT Request. Will both be accepted by the Target AP? Will second one be rejected, and if so, with what status code? Also, it is very important for a non-AP STA to commit to the same SNonce value - as to avoid a flooding attack on that AP. Seeing the same SNonce from the non-AP STA tells the target Ap that these are not floods - just retries. Of course, no source authenication can be done until 3rd message, but commiting to an SNonce for a specific time avoids AP flooding attacks. (This is revision of similar comment)

SuggestedRemedy

Insert a new line at line 24: "The non-AP STA shall commit to the same SNonce for executing the FT protocol with the target AP. If multiple FT Requests are sent to the target AP, then the non-AP STA shall use the same SNonce value for all FT Requests issued within the time specified by the reassociation deadline. If one FT Request has been processed at the Target AP, and multiple FT Requests are received at the Target AP from the same non-AP STA, then the Target AP shall reject the subsequent FT Request with status code 56 ("over-the-DS Limit")."

Response *Response Status* **U**

REJECT
The base specification is rightly silent on the proper behavior of the STA in these situations. Both changes proposed will lead to critical failures of the STA in certain roaming situations.

Cl **11A** *SC* **11A.5.3** *P* **59** *L* **18** # 217

Sood, Kapil

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

What if multiple FT Request frames are issued by a non-AP STA to the same Target AP. The scenario being that a response to first never came back, and then non-AP STA issued another FT Request. Will both be accepted by the Target AP? Will second one be rejected, and if so, with what status code?

SuggestedRemedy

Insert a new line at line 24: "If one FT Request has been processed at the Target AP, and multiple FT Requests are received at the Target AP from the same non-AP STA, then the Target AP shall reject the subsequent FT Request with status code 56 ("over-the-DS Limit")."

Response *Response Status* **U**

REJECT
The base specification is rightly silent on the proper behavior of the STA in these situations. Both changes proposed will lead to critical failures of the STA in certain roaming situations.

Cl **11A** *SC* **11A.5.3** *P* **59** *L* **19** # 359

Sood, Kapil

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

Over-the-DS lends itself to an interesting problem - a non-AP STA being always an opportunistic fella may want to execute FT Requests to multiple APs that it cannot see. An AP controller being more intelligent may want to limit these to a limited set. Moreover, it is possible that an AP may successfully execute the FT Request/Response with non-AP STA knowing well that Reassoc Request from that non-AP STA will likely be rejected (I have seen many reassoc failures in enterprise deployments for no justifiable reason!). So, in order to deter a non-AP STA from coming to that AP, the FT Request should be rejected by those Target AP. (This is revision of similar comment)

SuggestedRemedy

Add the following at the end of line 65 on page 58 Clause 11A.5.3: "The Target AP may reject the FT Authentication Request for limiting the non-AP STA's Reassociation to this Target AP by using the status code 56 ("over-the-DS Limit"). Clause 7.3.1.9, page 8 line 29 Add a row: "56 over-the-DS limit". Feel free to change the reason code to something more generic, if desired.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Inserted "The target AP may reject the FT Request for limiting the non-AP STA's reassociation to this target AP by using the status code 37 ("This request has been declined")."

Cl **11A** *SC* **11A.5.3** *P* **59** *L* **19** # 210

Sood, Kapil

Comment Type **TR** *Comment Status* **A** *Resource limit*

Over-the-DS lends itself to an interesting problem - a non-AP STA being always an opportunistic fella may want to execute FT Requests to multiple APs that it cannot see. An AP controller being more intelligent may want to limit these to a limited set. Moreover, it is possible that an AP may successfully execute the FT Request/Response with non-AP STA knowing well that Reassoc Request from that non-AP STA will likely be rejected (I have seen many reassoc failures in enterprise deployments for no justifiable reason!). So, in order to deter a non-AP STA from coming to that AP, the FT Request should be rejected by those Target AP.

SuggestedRemedy

Add the following at the end of line 65 on page 58 Clause 11A.5.3: "The Target AP may reject the FT Authentication Request for limiting the non-AP STA's Reassociation to this Target AP by using the status code 56 ("over-the-DS Limit"). Clause 7.3.1.9, page 8 line 29 Add a row: "56 over-the-DS limit". Feel free to change the reason code to something more generic, if desired.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Inserted "The target AP may reject the FT Request for limiting the non-AP STA's reassociation to this target AP by using the status code 37 ("This request has been declined")."

Cl **11A** *SC* **11A.5.4** *P* **59** *L* **26** # 211

Sood, Kapil

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

The over-the-air procedures defined in this clause are exactly the same as those defined in 11A.5.2 with the exception of non-RSN. Model this clause as done in 11A.6.2.

SuggestedRemedy

Delete entire text in clause 11A.5.4. Do not delete the Fig 11A-6. Move Fig 11A-6 into Clause 11A.5.2. Change Clause 11A.5.2 title page 55 line 58 "Over-the-air fast BSS transition protocol authentication". Change Clause 11A.5.2 page 55 line 65: "The over-the-air FT protocol in an RSN is shown in Figure 11A-4 and in a non-RSN is shown in Fig 11A-6. RSNIE and FTIE shall not be present in non-RSN protocol, and references to RSNIE, FTIE, and Key Holders in this sub-clause are applicable to RSN only."

Response *Response Status* **U**

REJECT.
The differences between 11A.5.2 and 11A.5.4 are significant, such as message contents and error handling. The combination of RSN and non-RSN in 11A.6 was possible only because 11A.6 could refer back to 11A.5 for the differences

Cl **11A** *SC* **11A.5.4** *P* **59** *L* **26** # 360

Sood, Kapil

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

The over-the-air procedures defined in this clause are exactly the same as those defined in 11A.5.2 with the exception of non-RSN. Model this clause as done in 11A.6.2. (This is revision of similar comment)

SuggestedRemedy

Delete entire text in clause 11A.5.4. Do not delete the Fig 11A-6. Move Fig 11A-6 into Clause 11A.5.2. Change Clause 11A.5.2 title page 55 line 58 "Over-the-air fast BSS transition protocol authentication". Change Clause 11A.5.2 page 55 line 65: "The over-the-air FT protocol in an RSN is shown in Figure 11A-4 and in a non-RSN is shown in Fig 11A-6. RSNIE and FTIE shall not be present in non-RSN protocol, and references to RSNIE, FTIE, and Key Holders in this sub-clause are applicable to RSN only."

Response *Response Status* **U**

REJECT.
The differences between 11A.5.2 and 11A.5.4 are significant, such as message contents and error handling. The combination of RSN and non-RSN in 11A.6 was possible only because 11A.6 could refer back to 11A.5 for the differences

Cl **11A** *SC* **11A.5.4** *P* **59** *L* **28** # 66

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

"..in a non-RSN&" is not consistent with the referencing text for the following procedure. (Originally LB98/508 submitted by Sood, Kapil, during LB98 with ID Sood/057)

SuggestedRemedy

Change "The over-the-air Fast BSS Transition protocol in a non-RSN (dot11RSNAEnabled is set False) is shown in Figure 204f."

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.5.5** *P* **60** *L* **25** # 361

Sood, Kapil

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

The over-the-DS procedures defined in this clause are exactly the same as those defined in 11A.5.3 with the exception of non-RSN. Restructure this clause as done in 11A.6.3 (This is revision of similar comment)

SuggestedRemedy

Delete entire text in clause 11A.5.5. Do not delete the Fig 11A-7. Move Fig 11A-7 into Clause 11A.5.3. Change Clause 11A.5.3 title page 55 line 58 "Over-the-DS fast BSS transition protocol authentication". Change Clause 11A.5.3 page 57 line 37: "The over-the-DS FT protocol in an RSN is shown in Figure 11A-5 and in a non-RSN is shown in Fig 11A-7. RSNIE and FTIE shall not be present in non-RSN protocol. Protocol description and references to RSNIE, FTIE, Key Holders, and Key derivations in this sub-clause are applicable to RSN only."

Response *Response Status* **U**

REJECT.
The differences between 11A.5.3 and 11A.5.5 are significant, such as message contents and error handling. The combination of RSN and non-RSN in 11A.6 was possible only because 11A.6 could refer back to 11A.5 for the differences

Cl **11A** *SC* **11A.5.5** *P* **60** *L* **25** # 212

Sood, Kapil

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

The over-the-DS procedures defined in this clause are exactly the same as those defined in 11A.5.3 with the exception of non-RSN. Restructure this clause as done in 11A.6.3

SuggestedRemedy

Delete entire text in clause 11A.5.5. Do not delete the Fig 11A-7. Move Fig 11A-7 into Clause 11A.5.3. Change Clause 11A.5.3 title page 55 line 58 "Over-the-DS fast BSS transition protocol authentication". Change Clause 11A.5.3 page 57 line 37: "The over-the-DS FT protocol in an RSN is shown in Figure 11A-5 and in a non-RSN is shown in Fig 11A-7. RSNIE and FTIE shall not be present in non-RSN protocol. Protocol description and references to RSNIE, FTIE, Key Holders, and Key derivations in this sub-clause are applicable to RSN only."

Response *Response Status* **U**

REJECT.
The differences between 11A.5.3 and 11A.5.5 are significant, such as message contents and error handling. The combination of RSN and non-RSN in 11A.6 was possible only because 11A.6 could refer back to 11A.5 for the differences

Cl **11A** *SC* **11A.5.5** *P* **60** *L* **27** # 67

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

"..in a non-RSN&" is not consistent with the referencing text for the following procedure. (Originally LB98/511 submitted by Sood, Kapil, during LB98 with ID Sood/058)

SuggestedRemedy

Change "The over-the-DS Fast BSS Transition protocol in a non-RSN (dot11RSNAEnabled is set False) is shown in Figure 204g."

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.6** *P* **61** *L* **23** # 282

Epstein, Joseph

Comment Type **TR** *Comment Status* **A** *reservation protocol*

The six-message resource request protocol mentioned in 11A.6 is seriously flawed and must be removed. These flaws are generally of the nature that the protocol cannot be successfully implemented in such a way as to perform the desired function without nasty or debilitating effects. Among the problems are as follows. Establishing resource allocations without commitment by the allocator leads to binding shop-around behavior. Shop-around behavior leads to known race conditions, resulting in poor convergence behavior at best, and deadlock at worst. Multiple allocations cannot be forcably prohibited in this model. Shop-around behavior is subject to game-theoretic problems that reward the aggressive client in low-usage cases while shutting down the network in high-usage cases. Global effects such as network failure, or per-station convergence times averaging above 50ms (or around there--calculations based on reasonable assumptions have exceeded this number when modelling the 6-message exchange) fails to eliminate or reduce data absense, and thus does not meet the goal mentioned in the scope of the PAR. No implementation has been shown to work with this 6-message exchange. Furthermore, a number of potential implementers of this standard have suggested that the 6-message exchange is flawed and have removed it from being required or being tested in a testplan being constructed around what will ultimately become the 11r amendment, adding doubt that the protocol is needed or implementable.

SuggestedRemedy

Delete section 11A.6, and all references to the 6-message FT resource request protocol throughout the draft. Delete the Authentication and FT Confirm and ACK messages.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changes given in submission 11-07-2516-01.

Cl **11A** *SC* **11A.6** *P* **61** *L* **23** # 313

Myles, Andrew F

Comment Type **TR** *Comment Status* **A** *reservation protocol*

The Resource Request protocol (requesting resources prior to association) is overly complex. It will lead to under-utilziation of resources in the network since a STA may be able to reserve resources at multiple APs, thus tying down the resources. The QBSS Load IE in the beacons gives a good idea of if TSPECs will get accepts at a particular AP. The STA should use this information to deterimine if it should initiation an association with it, rather than trying Admission control at multiple APs. Thus the resource request protocol should be removed from the draft.

SuggestedRemedy

Remove Section 11A.6

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changes given in submission 11-07-2516-01.

Cl **11A** *SC* **11A.6** *P* **61** *L* **23** # 379

Sood, Kapil

Comment Type **TR** *Comment Status* **A** *reservation protocol*

The FT resource request 6-msg protocol (reservation of resources prior to reassociation) does not solve any additional problems beyond those solved by the FT 4-message protocol. The FT Resource Request protocol adds too much complexity and cost to the implementation of this amendment, and as such, can be a great dis-incentive to never get implemented. This scheme is counter to the field experience with WLAN deployments and the behavior of clients in both managed and unmanaged WLANs - for starters, clients never have the luxury of apriori knowing which APs will be the best new targets - AP's channel characteristics change continually made worse by Clients rate adaptation, frame retries and signal power. It is impossible for a client to know which potential APs should it target as candidates for FT - mostly because signal strength is a weak measure of channel capacity at an AP. Say this scheme was implemented - it is easy to see why this will fail - A client being always opportunistic, it will continually keep on executing over-the-DS resource pre-reservation with ALL its known APs because it doesn't know which AP will look favorable when it has to roam and when that happens, then client will have tens of msecs to execute FT. If client floods all the APs in its cache (say, average 10 from our study), then one will start seeing artificial resource exhaustion at every AP. Limiting the reservation times does not help, as the client would like to renew that as soon as the previous reservation expires! The APs have very little idea on how to manage this artificial over-subscription and maintain accurate availability stats (QBSS) and accurately advertised to the clients. If the client executes this 6-msg protocol over-the-air, then that will rapidly drain it power as client would have to continually hop between channels. Moreover, studies from existing proprietary fast roaming WLAN protocols show that the bare latency of executing 6 messages will be over 70 msecs in 30% of cases on very lightly loaded APs in an over-provisioned AP environment. Removing the 6-msg scheme will lend much greater simplicity to this amendment, and hence, enable develors to implement this feature corerctly. (This is revision of similar comment)

SuggestedRemedy

Accept my submission (11-07-2351-00-000r-FT-resource-request-protocol-removal) that addresses the removal of the complex 6-message FT Resource Request protocol scheme.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changes given in submission 11-07-2516-01.

Cl **11A** *SC* **11A.6** *P* **61** *L* **23** # 251

Sood, Kapil

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

The exclusive FT resource request 6-msg protocol (reservation of resources prior to reassociation) does not solve any additional problems beyond those solved by the FT 4-message protocol. This scheme adds too much complexity and cost to the implementation of this amendment, and as such, can be a great dis-incentive to never get implemented. This scheme is counter to the field experience with WLAN deployments and the behavior of clients in both managed and unmanaged WLANs - for starters, clients never have the luxury of apriori knowing which APs will be the best new targets - AP's channel characteristics change continually made worse by Clients rate adaptation, frame retries and signal power. It is impossible for a client to know which potential APs should it target as candidates for FT - mostly because signal strength is a weak measure of channel capacity at an AP. Say this scheme was implemented - it is easy to see why this will fail - A client being always opportunistic, it will continually keep on executing over-the-DS resource pre-reservation with ALL its known APs because it doesn't know which AP will look favorable when it has to roam and when that happens, then client will have 10s of msecs to FT. If client floods all the APs in its cache (say, average 10 from our study), then one will start seeing artificial resource exhaustion at every AP. Limiting the reservation times does not help, as the client would like to renew that as soon as it expires! The APs have very little idea on how to manage this over-subscription and keep the availability accurately advertised to the clients. If the client executes this 6-msg protocol over-the-air, then that will rapidly drain it power as client would have to continually hop between channels. Moreover, studies from existing proprietary fast roaming WLAN protocols show that the bare latency of executing 6 messages will be over 70 msecs in 30% of cases on very lightly loaded APs in an over-provisioned AP environment. Removing the 6-msg scheme will lend much greater simplicity to this amendment, and hence, enable develors to implementat this feature corerctly.

SuggestedRemedy

Accept my submission that addresses the removal of the complex 6-message reservation prior to reassociation scheme.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changes given in submission 11-07-2516-01.

Cl **11A** *SC* **11A.6** *P* **61** *L* **24** # 325

Sood, Kapil

Comment Type **TR** *Comment Status* **A** *reservation protocol*

Resource Request protocol described in Clause 11A.6 and elsewhere in the document does not solve any problem. In fact, the open-endedness of this protocol lends it to be too vaguely defined and will result in poor interoperability among STAs and APs, degraded user experience, and much larger transition latencies. Among other things, this protocol does not define (1) how APs are supposed to allocate resources, (2) does not define the failure state machines of numerous error scenarios, (3) does not describe how an AP can prevent the resources from being consumed by existing or new STAs, (4) how the AP informs a STA that the channel has degraded and that the STA should look for other APs...and, so on. At 15msec average for a roundtrip, this protocol execution by itself will approach the 50 msecs FT time that is the L2 transition budget for voice - leading to a not-so-fast-transition. This comment is on Clause 11A.6 and all text related to FT Resource Request protocol in D7.0. (This is a revision of similar comment)

SuggestedRemedy

Remove clause 11A.6 and Accept my submission (11-07-2351-00-000r-FT-resource-request-protocol-removal) that prescribes all the changes in this draft that remove the FT Resource Request protocol.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changes given in submission 11-07-2516-01.

Cl **11A** *SC* **11A.6** *P* **61** *L* **24** # 150

Sood, Kapil

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

Resource Request protocol described in Clause 11A.6 and elsewhere in the document does not solve any problem. In fact, the open-endedness of this protocol lends it to be too vaguely defined and will result in poor interoperability among STAs and APs, degraded user experience, and much larger transition latencies. Among other things, this protocol does not define (1) how APs are supposed to allocate resources, (2) does not define the failure state machines of numerous error scenarios, (3) does not describe how an AP can prevent the resources from being consumed by existing or new STAs, (4) how the AP informs a STA that the channel has degraded and that the STA should look for other APs...and, so on. At 15msec average for a roundtrip, this protocol execution by itself will approach the 50 msecs FT time that is the L2 transition budget for voice - leading to a not-so-fast-transition. This comment is on Clause 11A.6 and all text related to FT Resource Request protocol in D7.0.

SuggestedRemedy

Remove clause 11A.6 and Accept my submission that prescribes all the changes in this draft that remove the FT Resource Request protocol.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changes given in submission 11-07-2516-01.

Cl **11A** *SC* **11A.6.2** *P* **64** *L* **13** # 215

Sood, Kapil

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

The "it" is dangling - is "it" refering to the response or to MIC.

SuggestedRemedy

Change: "shall disregard the response if the MIC is incorrect".

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.6.2** *P* **64** *L* **8** # 214

Sood, Kapil

Comment Type **T** *Comment Status* **A**

"In a non-RSN, a Timeout Information Element may appear" - this reads like a misplaced sentence lending more intrigue than giving substantial value to implementers. A better description appears on lines 31-34, so this sentence is redundant.

SuggestedRemedy

Delete this line.

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.6.2** *P* **64** *L* **8** # 363

Sood, Kapil

Comment Type **T** *Comment Status* **A**

"In a non-RSN, a Timeout Information Element may appear" - this reads like a misplaced sentence lending more intrigue than giving substantial value to implementers. A better description appears on lines 31-34, so this sentence is redundant. (This is revision of similar comment)

SuggestedRemedy

Delete this line.

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.6.3** *P* **65** *L* **20** # 382

Amann, Keith

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

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.

SuggestedRemedy

One of two solutions seems acceptable:
1) Allow the station to provide the "Reassociation Deadline Time" value to the AP indicating when it will return. In this situation the AP can then drop any state that has been setup as a result of the previous authentication transactions once the timeout has been reached. Since the AP is having to maintain these timers anyway (one per station for the existing solution) this doesn't appear to add any additional complexity on the part of the AP.
2) Add a mechanism that would allow the station to query the AP ahead of time for this value, or include it as "public" information in the beacon or probe responses so that a station can determine if it can actually meet the "Reassociation Deadline Time" requirements specified.
I suspect that there are some potential security issues related to #2, so would be more in favor of #1.

Response *Response Status* **U**

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.

Cl **11A** *SC* **11A.6.3** *P* **67** *L* **21** # 216

Sood, Kapil

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

The "it" is dangling - is "it" refering to the response or to MIC.

SuggestedRemedy

Change: "disregard the response if the MIC is incorrect".

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.7** *P* **67** *L* **50** # 248

Sood, Kapil

Comment Type **TR** *Comment Status* **A** *RIC format*

When a non-AP STA moves from a WMM-AP to a target AP supporting 11e-only TSPECs, then its resource requirements will not be met at the Target AP. A non-AP STA only learns after a RIC failure, but ends up associated with an AP that does not support its resource type. The non-AP STA then has to look for another AP, which increases the transition time for that non-AP STA to an appropriate AP. Same problems occur when current AP supports 11e and target AP supports only WMM. TGr must be made to co-exist with 11e and WMM TSPECs. The industry has implemented WMM and 11r devices will be tested/certified with WMM. It is, therefore, a strong requirement that no change be necessary to this specification when 11r is tested/certified with WMM TSPEC/resources.

SuggestedRemedy

Adopt my submission that allows non-AP STA to identify the supported resource types on the target AP prior to making a FT attempt to that AP.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Insert row in Table 11A-3 with Resource Type "Vendor Specific" and Resource Descriptor definition "RDIE is followed by any Vendor-specific information elements required to specify this resource."

Cl **11A** *SC* **11A.7** *P* **67** *L* **50** # 376

Sood, Kapil

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

When a non-AP STA moves from a WMM-AP to a target AP supporting 11e-only TSPECs, then its resource requirements will not be met at the Target AP. A non-AP STA only learns after a RIC failure, but ends up associated with an AP that does not support its resource type. The non-AP STA then has to look for another AP, which increases the transition time for that non-AP STA to an appropriate AP. Same problems occur when current AP supports 11e and target AP supports only WMM. TGr must be made to co-exist with 11e and WMM TSPECs. The industry has implemented WMM and 11r devices will be tested/certified with WMM. It is, therefore, a strong requirement that no change be necessary to this specification when 11r is tested/certified with WMM TSPEC/resources. (This is revision of similar comment)

SuggestedRemedy

Adopt my submission that allows non-AP STA to identify the supported resource types on the target AP prior to making a FT attempt to that AP.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Insert row in Table 11A-3 with Resource Type "Vendor Specific" and Resource Descriptor definition "RDIE is followed by any Vendor-specific information elements required to specify this resource."

Cl **11A** *SC* **11A.7.1** *P* **67** *L* **54** # 218

Sood, Kapil

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

STA is not just any STA - it is a non-AP STA

SuggestedRemedy

Change lines 54, 57, 59, 60, 62: "STA" to "non-AP STA"

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.7.1** *P* **68** *L* **13** # 220

Sood, Kapil

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

The "it" is dangling - is "it" refering to the request or to MIC.

SuggestedRemedy

Change: "disregard the request if the MIC is incorrect".

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.7.1** *P* **68** *L* **21** # 249

Sood, Kapil

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

A significant processing capability is missing from this Clause and from Clause 11A.7.2. A non-AP STA desiring to move to a target AP shall not be rejected by the target AP if the requested resources in the RIC-Request in the reassoc request message cannot be made available by the target AP. The reason why this should be allowed is that a non-AP STA spends expensive resources to attempt reassociation with a target AP and many a times, will be facing an emergency re-connection situation. Decoupling the reassoc response status from the success/failure of the RIC gives much greater flexibility to a non-AP STA. From numerous data studies: A failed reassociation adds 100s of msecs to the transition time, and reassoc attempts should be failed only under dire circumstances (as mentioned in this clause). This specification is way too complex to comprehend and implement correctly (ask anyone strating to implement this!) - Anyhow, this remediation should be added in these clauses.

SuggestedRemedy

Insert the following in Clause 11A.7.1, page 68 line 20: "The target AP shall not reject the reassociation request from a non-AP STA if the target AP was unable to allocate the requested resources in the RIC-Request." Insert the same sentence in Clause 11A.7.2 page 69 line 18

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Page 93 line 17 changed "The Status Code shall be set" to "The Status Code in the RDIE shall be set". Inserted after line 27 "A non-zero Status Code in an RDIE shall not cause a non-zero Status Code in the frame containing the RIC Request."

Cl **11A** *SC* **11A.7.1** *P* **68** *L* **21** # 377

Sood, Kapil

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

A significant processing capability is missing from this Clause and from Clause 11A.7.2. A non-AP STA desiring to move to a target AP shall not be rejected by the target AP if the requested resources in the RIC-Request in the reassoc request message cannot be made available by the target AP. The reason why this should be allowed is that a non-AP STA spends expensive resources to attempt reassociation with a target AP and many a times, will be facing an emergency re-connection situation. Decoupling the reassoc response status from the success/failure of the RIC gives much greater flexibility to a non-AP STA. From numerous data studies: A failed reassociation adds 100s of msecs to the transition time, and reassoc attempts should be failed only under dire circumstances (as mentioned in this clause). This specification is way too complex to comprehend and implement correctly (ask anyone strating to implement this!) - Anyhow, this remediation should be added in these clauses. (This is revision of similar comment)

SuggestedRemedy

Insert the following in Clause 11A.7.1, page 68 line 20: "The target AP shall not reject the reassociation request from a non-AP STA if the target AP was unable to allocate the requested resources in the RIC-Request." Insert the same sentence in Clause 11A.7.2 page 69 line 18

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Page 93 line 17 changed "The Status Code shall be set" to "The Status Code in the RDIE shall be set". Inserted after line 27 "A non-zero Status Code in an RDIE shall not cause a non-zero Status Code in the frame containing the RIC Request."

Cl **11A** *SC* **11A.7.1** *P* **68** *L* **22** # 222

Sood, Kapil

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

STA is not just any STA - it is a non-AP STA

SuggestedRemedy

Change lines 22, 27, 31: "STA" to "non-AP STA".

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.7.1** *P* **68** *L* **28** # 221

Sood, Kapil

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

The "it" is dangling - is "it" refering to the response or to MIC.

SuggestedRemedy

Change: "disregard the response if the MIC is incorrect".

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.7.1** *P* **68** *L* **36** # 223

Sood, Kapil

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

STA is not just any STA - it is a non-AP STA

SuggestedRemedy

Change lines 36, 43, 48, 50, 51: "STA" to "non-AP STA"

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.7.1** *P* **68** *L* **43** # 224

Sood, Kapil

Comment Type **TR** *Comment Status* **R** *STA behavior*

"...then the STA shall abandon this transition attempt. Handling of other errors returned in the Status Code shall be as specified in 11.3." -a non-AP STA has received a non-zero status code, so the FT attempt has failed and STA shall abandon this FT attempt on ANY failure. A STA has no other recourse but to try the entire FT again. I do not understand why the STA shall abandon on only these failures, and not others. If there are other outcomes please list them.

SuggestedRemedy

Change: "If the Status Code returned by the target AP in the response is 1 ("unspecified failure"), 14 ("Authentication transaction sequence number out of sequence"), 16 ("Authentication rejected due to timeout waiting for next frame in sequence"), or any other non-zero status code, then the STA shall abandon this fast transition attempt. Handling of other errors returned in the Status Code shall be as specified in 11.3." Same change in Clause 11A.7.2 page 69 line 38.

Response *Response Status* **U**

REJECT
The existing text lists specific reasons (14, 16) caused by failures in the FT, and the third (unspecified failure) enables the AP to indicate other relevent failures requiring the STA to abandon the transition attempt.

Cl **11A** *SC* **11A.7.1** *P* **68** *L* **43** # 365

Sood, Kapil

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

"...then the STA shall abandon this transition attempt. Handling of other errors returned in the Status Code shall be as specified in 11.3." -a non-AP STA has received a non-zero status code, so the FT attempt has failed and STA shall abandon this FT attempt on ANY failure. A STA has no other recourse but to try the entire FT again. I do not understand why the STA shall abandon on only these failures, and not others. If there are other outcomes please list them. (This is revision of similar comment)

SuggestedRemedy

Change: "If the Status Code returned by the target AP in the response is 1 ("unspecified failure"), 14 ("Authentication transaction sequence number out of sequence"), 16 ("Authentication rejected due to timeout waiting for next frame in sequence"), or any other non-zero status code, then the STA shall abandon this fast transition attempt. Handling of other errors returned in the Status Code shall be as specified in 11.3." Same change in Clause 11A.7.2 page 69 line 38.

Response *Response Status* **U**

REJECT
The existing text lists specific reasons (14, 16) caused by failures in the FT, and the third (unspecified failure) enables the AP to indicate other relevent failures requiring the STA to abandon the transition attempt.

Cl **11A** *SC* **11A.7.1** *P* **68** *L* **47** # 69

CHAPLIN, CLINT F

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

Both 11A.6.2 and 11A.6.3 seem to include a paragraph that describes that PTKSA has been proven live and lists some operations to be done at this point. However, such text is not included in the description of reassociation for FT protocol. Shouldn't the same description and steps apply to FT protocol, too?
(Originally LB98/560 submitted by Malinen, Jouni, during LB98 with ID Malinen/48)

SuggestedRemedy

Copy this paragraph into 11A.7.1 with "Fast BSS Transition Confirm/Acknowledgement" replaced with "reassociation" and with the last two sentence ("The PTKSA shall be deleted .. specified in 11A.10") deleted.

Response *Response Status* **U**

ACCEPT.
Only text missing is "the PTKSA has been established and proven live." Change first sentence at 67.47 to "Upon a successful reassociation, the PTKSA has been established and proven live. The SME of the AP."

Cl **11A** *SC* **11A.7.1** *P* **68** *L* **47** # 68

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

"unblock" is used here, but "open" is used elsewhere in this amendment. Be consistent.
(Originally LB98/504 submitted by Sood, Kapil, during LB98 with ID Sood/055)

SuggestedRemedy

Change "unblock" to "open"

Response *Response Status* **C**

ACCEPT.
Also changed at 52.01 and 63.37.

Cl **11A** *SC* **11A.7.1** *P* **68** *L* **48** # 366

Sood, Kapil

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

"If the target AP is distinct from the previous AP, the STA
shall enter State 1 with respect to the previous AP" - can a non-AP STA do an FT to the same AP that it is currently associated with? If so, then why would we allow such an operation. If not, then why do we have this statement? (This is revision of similar comment)

SuggestedRemedy

Change: "The non-AP STA shall enter State 1 with respect to the previous AP." Same change on Clause 11A.7.2 page 69 line 46.

Response *Response Status* **U**

REJECT.
This change makes a reassociation with the current AP impossible

Cl **11A** *SC* **11A.7.1** *P* **68** *L* **48** # 225

Sood, Kapil

Comment Type **TR** *Comment Status* **R** *Roam-to-self*

"If the target AP is distinct from the previous AP, the STA
shall enter State 1 with respect to the previous AP" - can a non-AP STA do an FT to the same AP that it is currently associated with? If so, then why would we allow such an operation. If not, then why do we have this statement?

SuggestedRemedy

Change: "The non-AP STA shall enter State 1 with respect to the previous AP." Same change on Clause 11A.7.2 page 69 line 46.

Response *Response Status* **U**

REJECT.
This change makes a reassociation with the current AP impossible

Cl **11A** *SC* **11A.7.1** *P* **68** *L* **53** # 70

CHAPLIN, CLINT F

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

"The PTK key lifetime timer shall be initialized to ensure that the lifetime of the PTKSA is no longer than the value provided in the Key Lifetime TIE obtained during the FT Initial Mobility Domain Association." - Is not specific and does not give any specific information to the implementers. This is a potential bug in the interoperability aspect of this amendment. (Originally LB98/506 submitted by Sood, Kapil, during LB98 with ID Sood/056)

SuggestedRemedy

Change "Once the IEEE 802.1X controlled port is open, the PTK key lifetime timer is initialized with the value calculated as the difference between the TIE[KeyLifetime] sent in Message 3 of FT Initial Mobility Domain association and the time duration in seconds since the 802.1X controlled port was opened when the STA executed the FT Initial Mobility Domain Association."

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Change to "The PTK key lifetime timer shall be initialized with the value calculated as the difference between the TIE[KeyLifetime] sent in Message 3 of the FT Initial Mobility Domain association and the time since the completion of the FT 4-Way Handshake during the FT Initial Mobility Domain Association."

Cl **11A** *SC* **11A.7.2** *P* **69** *L* **1** # 227

Sood, Kapil

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

STA is not just any STA - it is a non-AP STA

SuggestedRemedy

Change lines 1, 2, 5, 11, 21, 31, 38, 45, 46 "STA" to "non-AP STA"

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.7.2** *P* **69** *L* **18** # 250

Sood, Kapil

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

A significant processing capability is missing from this Clause and from Clause 11A.7.2. A non-AP STA desiring to move to a target AP shall not be rejected by the target AP if the requested resources in the RIC-Request in the reassoc request message cannot be made available by the target AP. The reason why this should be allowed is that a non-AP STA spends expensive resources to attempt reassociation with a target AP and many a times, will be facing an emergency re-connection situation. Decoupling the reassoc response status from the success/failure of the RIC gives much greater flexibility to a non-AP STA. From numerous data studies: A failed reassociation adds 100s of msecs to the transition time, and reassoc attempts should be failed only under dire circumstances (as mentioned in this clause). This specification is way too complex to comprehend and implement correctly (ask anyone strating to implement this!) - Anyhow, this remediation should be added in these clauses.

SuggestedRemedy

Insert the following in Clause 11A.7.2, page 69 line 18: "The target AP shall not reject the reassociation request from a non-AP STA if the target AP was unable to allocate the requested resources in the RIC-Request." Insert the same sentence in Clause 11A.7.1 page 68 line 20.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Page 93 line 17 changed "The Status Code shall be set" to "The Status Code in the RDIE shall be set". Inserted after line 27 "A non-zero Status Code in an RDIE shall not cause a non-zero Status Code in the frame containing the RIC Request."

Cl **11A** *SC* **11A.7.2** *P* **69** *L* **18** # 378

Sood, Kapil

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

A significant processing capability is missing from this Clause and from Clause 11A.7.2. A non-AP STA desiring to move to a target AP shall not be rejected by the target AP if the requested resources in the RIC-Request in the reassoc request message cannot be made available by the target AP. The reason why this should be allowed is that a non-AP STA spends expensive resources to attempt reassociation with a target AP and many a times, will be facing an emergency re-connection situation. Decoupling the reassoc response status from the success/failure of the RIC gives much greater flexibility to a non-AP STA. From numerous data studies: A failed reassociation adds 100s of msecs to the transition time, and reassoc attempts should be failed only under dire circumstances (as mentioned in this clause). This specification is way too complex to comprehend and implement correctly (ask anyone strating to implement this!) - Anyhow, this remediation should be added in these clauses. (This is revision of similar comment)

SuggestedRemedy

Insert the following in Clause 11A.7.2, page 69 line 18: "The target AP shall not reject the reassociation request from a non-AP STA if the target AP was unable to allocate the requested resources in the RIC-Request." Insert the same sentence in Clause 11A.7.1 page 68 line 20.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Page 93 line 17 changed "The Status Code shall be set" to "The Status Code in the RDIE shall be set". Inserted after line 27 "A non-zero Status Code in an RDIE shall not cause a non-zero Status Code in the frame containing the RIC Request."

Cl **11A** *SC* **11A.7.2** *P* **69** *L* **41** # 368

Sood, Kapil

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

"If the AP has dot11RSNAEnabled set to true, upon a successful reassociation the SME shall unblock the
IEEE 802.1X Controlled Port." - Isn't this clause describing a non-RSN case? There is no 802.1X in non-RSN. An AP may have a RSN enabled, but if this is the case this is trying to say, then re-word accordingly. (This is revision of similar comment)

SuggestedRemedy

Delete this line. (lines 41-42 on page 69).

Response *Response Status* **U**

REJECT.
This sentence is needed to cover the case of a non-RSN STA associated to a RSN-capable AP (called TSN in 802.11-2007)

Cl **11A** *SC* **11A.7.2** *P* **69** *L* **41** # 228

Sood, Kapil

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

"If the AP has dot11RSNAEnabled set to true, upon a successful reassociation the SME shall unblock the
IEEE 802.1X Controlled Port." - Isn't this clause describing a non-RSN case? There is no 802.1X in non-RSN. An AP may have a RSN enabled, but if this is the case this is trying to say, then re-word accordingly.

SuggestedRemedy

Delete this line. (lines 41-42 on page 69).

Response *Response Status* **U**

REJECT.
This sentence is needed to cover the case of a non-RSN STA associated to a RSN-capable AP (called TSN in 802.11-2007)

Cl **11A** *SC* **11A.8.1** *P* **69** *L* **59** # 229

Sood, Kapil

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

STA is not just any STA - it is a non-AP STA

SuggestedRemedy

Change lines 59, 61, 65: "STA" to "non-AP STA"

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.8.1** *P* **70** *L* **18** # 231

Sood, Kapil

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

"In all cases" - what all cases are being referred to here. No value is being added by this term - just adding confusion.

SuggestedRemedy

Delete "In all cases"

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.8.1** *P* **70** *L* **45** # 232

Sood, Kapil

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

Snonce and Anonce are together the Instance Identifiers.

SuggestedRemedy

Change: "The non-AP STA includes a fresh SNonce as its contribution to the association instance identifier and to provide key"

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.8.1** *P* **70** *L* **48** # 233

Sood, Kapil

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

The entire paragraph (lines 40-48) clearly defines all data is being sent by the non-AP STA. So, the last line "This information is sent from the STA to the target AP" is not adding any value.

SuggestedRemedy

Delete the line: "This information is sent from the STA to the target AP".

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.8.1** *P* **70** *L* **48** # 369

Sood, Kapil

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

The entire paragraph (lines 40-48) clearly defines all data is being sent by the non-AP STA. So, the last line "This information is sent from the STA to the target AP" is not adding any value. (This is revision of similar comment)

SuggestedRemedy

Delete the line: "This information is sent from the STA to the target AP".

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.8.1** *P* **70** *L* **5** # 230

Sood, Kapil

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

STA is not just any STA - it is a non-AP STA

SuggestedRemedy

Change lines 5, 11, 40, 45, 50, 56, 57, 60: "STA" to "non-AP STA"

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.8.1** *P* **70** *L* **52** # 234

Sood, Kapil

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

Target AP provides the Anonce, but this is also the target AP contribution to the assoc instance id. Make this consistent with the SNonce in previous paragraph.

SuggestedRemedy

Change: "The target AP also includes a fresh ANonce as its contribution to the association instance identifier and to provide key separation of the derived PTK."

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.8.1** *P* **70** *L* **52** # 370

Sood, Kapil

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

Target AP provides the Anonce, but this is also the target AP contribution to the assoc instance id. Make this consistent with the SNonce in previous paragraph. (This is revision of similar comment)

SuggestedRemedy

Change: "The target AP also includes a fresh ANonce as its contribution to the association instance identifier and to provide key separation of the derived PTK."

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.8.1** *P* **70** *L* **53** # 235

Sood, Kapil

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

The entire paragraph (lines 50-54) clearly defines all data is being sent by the target AP. So, the last line "This information is sent from the target AP to the STA" is not adding any value.

SuggestedRemedy

Delete the line: "This information is sent from the target AP to the STA".

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.8.1** *P* **70** *L* **53** # 371

Sood, Kapil

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

The entire paragraph (lines 50-54) clearly defines all data is being sent by the target AP. So, the last line "This information is sent from the target AP to the STA" is not adding any value. (This is revision of similar comment)

SuggestedRemedy

Delete the line: "This information is sent from the target AP to the STA".

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.8.1** *P* **70** *L* **57** # 372

Sood, Kapil

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

The entire paragraph (lines 56-58) clearly defines all data is being sent by the non-AP STA. So, the last line "This information is sent from the STA to the target AP" is not adding any value. (This is revision of similar comment)

SuggestedRemedy

Delete the line: "This information is sent from the STA to the target AP". Change: "In an RSN, the third message is used by the non-AP STA to assert to the target AP that the non-AP STA has a valid PTK."

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.8.1** *P* **70** *L* **57** # 236

Sood, Kapil

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

The entire paragraph (lines 56-58) clearly defines all data is being sent by the non-AP STA. So, the last line "This information is sent from the STA to the target AP" is not adding any value.

SuggestedRemedy

Delete the line: "This information is sent from the STA to the target AP". Change: "In an RSN, the third message is used by the non-AP STA to assert to the target AP that the non-AP STA has a valid PTK."

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.8.1** *P* **70** *L* **65** # 373

Sood, Kapil

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

The entire paragraph (lines 60-65) clearly defines all data is being sent by the target AP. So, the last line "This information is sent from the target AP to the STA" is not adding any value. (This is revision of similar comment)

SuggestedRemedy

Delete the line: "This information is sent from the target AP to the STA".

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.8.1** *P* **70** *L* **65** # 237

Sood, Kapil

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

The entire paragraph (lines 60-65) clearly defines all data is being sent by the target AP. So, the last line "This information is sent from the target AP to the STA" is not adding any value.

SuggestedRemedy

Delete the line: "This information is sent from the target AP to the STA".

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.8.2** *P* **71** *L* **15** # 238

Sood, Kapil

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

Making the non-AP STA send the MDIE from the beacons/probes of the target AP defeats the purpose of using 11k discovery and over-the-DS. MDIE should be consistently the same in the entire MD, and as such, the non-AP STA should include the MDIE that it got from the AP with which it performed the Initial MD Association.

SuggestedRemedy

Change: "The MDIE shall contain the Mobility Domain Identifier, the Fast BSS Transition Capability and policy
settings obtained from the AP with which the non-AP STA performed the Initial Mobiloity Domain Association. The MDIE shall be the same as received in message 3 of the FT 4-way handshake of the Initial Mobility Domain Association. All APs within the same Mobility Domain shall advertise the same MDIE."

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
The 11k neighbor report indicates that the target AP is advertising an identical MDIE as the current AP, so the 11k discovery is not being defeated. It is assumed by the standard that the MDIE is administered consistently across the Mobility Domain (stated in 11A.3), so the settings obtained by the non-AP STA during Initial Mobility Domain Association are the same as those of the target AP. However, the target AP is unable to verify that the MDIE is identical to the initial one, but can verify that it is identical to its own. No text changes needed.

Cl **11A** *SC* **11A.8.2** *P* **71** *L* **15** # 374

Sood, Kapil

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

Making the non-AP STA send the MDIE from the beacons/probes of the target AP defeats the purpose of using 11k discovery and over-the-DS. MDIE should be consistently the same in the entire MD, and as such, the non-AP STA should include the MDIE that it got from the AP with which it performed the Initial MD Association. (This is revision of similar comment)

SuggestedRemedy

Change: "The MDIE shall contain the Mobility Domain Identifier, the Fast BSS Transition Capability and policy
settings obtained from the AP with which the non-AP STA performed the Initial Mobiloity Domain Association. The MDIE shall be the same as received in message 3 of the FT 4-way handshake of the Initial Mobility Domain Association. All APs within the same Mobility Domain shall advertise the same MDIE."

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
The 11k neighbor report indicates that the target AP is advertising an identical MDIE as the current AP, so the 11k discovery is not being defeated. It is assumed by the standard that the MDIE is administered consistently across the Mobility Domain (stated in 11A.3), so the settings obtained by the non-AP STA during Initial Mobility Domain Association are the same as those of the target AP. However, the target AP is unable to verify that the MDIE is identical to the initial one, but can verify that it is identical to its own. No text changes needed.

Cl **11A** *SC* **11A.8.2** *P* **71** *L* **23** # 239

Sood, Kapil

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

STA is not just any STA - it is a non-AP STA

SuggestedRemedy

Change lines 23, 26, 55 : "STA" to "non-AP STA"

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.8.3** *P* **71** *L* **48** # 241

Sood, Kapil

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

It is the target AP - just to be clear.

SuggestedRemedy

Change: "MDIE advertised by the target AP in &"

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.8.3** *P* **71** *L* **56** # 240

Sood, Kapil

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

It is the target AP - just to be clear.

SuggestedRemedy

Change: "R1 Key Holder Identifier of the target AP, from the&"

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.8.4** *P* **72** *L* **26** # 124

CHAPLIN, CLINT F

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

I think there is a misunderstanding to LB98 CID 587&the resolution states: "(resolution to this comment agreed as part of LB87)
Rejected. The Group and Pairwise cipher selection is used in 8.5.2 to determine the MIC algorithm, and the same algorithm is being specified here." However, my comment is to the MIC algorithm in the FTIE. There has been a current update in D6.0 to state that it is now based on the AKM, which may be acceptable....but the implication is that for every new cipher, a new AKM will be required. Is this the desired effect?
(Originally LB105/17 submitted by Cam-Winget, Nancy, during LB105 with ID Cam-Winget/10)

SuggestedRemedy

The reserved bits in the MIC control field of the FTIE could be used to allow for a security parameter index. For now it can be set to 0 to signal AES-CMAC but can be used to provide the necessary crypto agility should other ciphers be allowed.

Response *Response Status* **U**

REJECT.
The intent is that a new AKM would be used to select a different MIC algorithm. This approach was chosen for the following reasons: (1) To consolidate all the security algorithm into the RSN information element; (2) To provide enough flexibility for vendor specific MIC algorithms; using the FTIE available bits provides very limited flexibility whereas using the AKM allows for vendor specific MIC algorithms.

Cl **11A** *SC* **11A.8.4** *P* **72** *L* **30** # 242

Sood, Kapil

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

STA is not just any STA - it is a non-AP STA

SuggestedRemedy

Change lines 30, : "STA" to "non-AP STA"

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.8.4** *P* **72** *L* **40** # 243

Sood, Kapil

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

The correct item is RIC-Request to be consistent with prior usage and figures.

SuggestedRemedy

Change: "Contents of the RIC-Request (if present)

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.8.4** *P* **72** *L* **45** # 244

Sood, Kapil

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

The correct item is RIC-Request to be consistent with prior usage and figures.

SuggestedRemedy

Change: "&forming the RIC-Request shall be included."

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.8.5** *P* **72** *L* **60** # 245

Sood, Kapil

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

It is the target AP - just to be clear.

SuggestedRemedy

Change: "&advertised by the target AP in Beacon&"

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.8.5** *P* **73** *L* **26** # 246

Sood, Kapil

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

STA is not just any STA - it is a non-AP STA

SuggestedRemedy

Change lines 26, 50 : "STA" to "non-AP STA"

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.9** *P* **75** *L* **1** # 125

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **R** *SDL State Machines*

The state machine diagrams are overloaded and poorly drawn.
(Originally LB105/18 submitted by Hiertz, Guido, during LB105 with ID Hiertz/9)

SuggestedRemedy

SDL provides the necessary functionality of a well defined programming language. The state machine diagrams should be redrawn using SDL-92.

Response *Response Status* **C**

REJECT
State machines are drawn in a manner and form consistent with the existing ones in 802.11-2007.

Cl **11A** *SC* **11A.9.2** *P* **75** *L* **34** # 312

Malinen, Jouni

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

Typo

SuggestedRemedy

Replace "Derive-Keu-PMK-R1()" with "Derive-Key-PMK-R1()" in the FT-R0-SEND-PMKR1SA state in Figure 11A-12.

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.9.3** *P* **76** *L* **45** # 139

Chaplin, Clint F

Comment Type **TR** *Comment Status* **A** *State Machines*

State machines in 11A.9.3 for R1KH and 11A.9.5 for S1KH show far more than the portions in the Authenticator/Supplicant, rather they show much of the SME algorithms as well. Requiring all of the operations shown in the state machines to be in the Authenticator/Supplicant is not right, and (I think) not part of the intention when the state machines were first written.
Either remove the SME portions from the figures 11A-13, 11A-14, 11A-16, and 11A-17, or re-title them to indicate they show SME actions as well as R1KH/S1KH actions. I recommend the latter. (submitted by Bill Marshall)

SuggestedRemedy

11A.9.3, page 76 line 45 change "The R1KH authenticator FT state machine defined in Figure 11A-13 and Figure 11A-14 consists" to "The R1KH authenticator FT state machine, along with other portions of the SME, are defined in Figure 11A-13 and Figure 11A-14, and consist...". Change title of Figure 11A-13/14 to "Authenticator R1KH state machine, including portions of the SME (part 1/2)". In 11A.9.5, page 81 line 41 change "The Supplicant S1KH state machine defined in Figure 11A-16 and Figure 11A-17 consists..." to "The Supplicant S1KH state machine, along with other portions of the SME, are defined in Figure 11A-16 and Figure 11A-17, and consist...". Change title of Figure 11A-16/17 to "Supplicant S1KH FT state machine, including portions of the SME (part 1/2)".

Response *Response Status* **U**

ACCEPT
In addition to proposed change, page 76 line 45 change to "The Authenticator R1KH state machine."

Cl **11A** *SC* **11A.9.3** *P* **76** *L* **54** # 71

CHAPLIN, CLINT F

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

R1KH state machine lifetime is somewhat unclear. Will this state machine instance continue to live after the STA has transitioned to another AP? What about when the transition is back to the same AP? In the current design, the state machine would be stuck in FT-PTK-INIT-DONE or SKIP-EAP state if nothing triggers the "Init" signal to restart the state machine when the STA roams back to the same AP.
(Originally LB98/596 submitted by Malinen, Jouni, during LB98 with ID Malinen/51)

SuggestedRemedy

Add a new IDLE state into R1KH state machine (either Figure 204m or 204n depending on which is easier for the editor) and add UCT transitions from FT-PTK-INIT-DONE and SKIP-EAP into this new IDLE state. The IDLE state does not do anything (empty box), but it has following transitions to other states: MLME-AUTHENTICATE.indication(FT, SNonce, R0KH-ID, PMKR0Name) to FT-AUTH; MLME-AUTHENTICATE.indication(Open) to FT-INIT-AUTH; MLME-ASSOCIATE.indication() || MLME-REASSOCIATE.indication() to FT-INIT-ASSOC. Add "IDLE: This state is entered upon successfully completed initial MD association or FT protocol." into 11A.8.3.1.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE.
Insert a new paragraph at end of 11A.9.3 "A new instance of the Authenticator R1KH state machine is created each time Initial Mobility Domain association or Fast BSS Transition is initiated."

Cl **11A** *SC* **11A.9.3** *P* **77** *L* **29** # 310

Malinen, Jouni

Comment Type **TR** *Comment Status* **A** *State Machines*

FT-INIT-R1_SA state of Authenticator R1KH has a statement about checking PMK-R1 key lifetime. However, other state of this state machine do not seem to have similar validation (e.g., FT-PMK-R1-SA-RECD does not mention this even though it is also using PMK-R1). Implementation are expected to validate number of timeouts and explicitly listing all this validations in the state machine description would make the figures unnecessarily complex. The same comment applies to the S1KH state machine FT-INIT-R1-SA state.

SuggestedRemedy

Remove "Check PMK-R1 key lifetime" from FT-INIT-R1_SA in Figure 11A-13 and from FT-INIT-R1-SA in Figure 11A-16.

Response *Response Status* **U**

ACCEPT

Cl **11A** *SC* **11A.9.3** *P* **77** *L* **57** # 72

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Typo
(Originally LB98/595 submitted by Malinen, Jouni, during LB98 with ID Malinen/50)

SuggestedRemedy

Replace "MLME-SETPROTECTION.Request" with "MLME-SETPROTECTION.request" in Figure 204m.

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.9.3** *P* **78** *L* **24** # 126

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

My LB98 CID 597 was accepted, but it was not fully implemented in D6.0. This was likely due to the original comment being unclear on which "Reassoc-deadline" occurrences should be removed from FT-PMK-R1-SA-RECD in Figure 204n. The comment said that "both two cases" should be removed, but there were actually three occurrences.. Only one was removed. One of the two remaining once should also be removed to finish the cleanup: This state machine is clearly for RSN case (e.g., use of MIC-Verified) and as such, there is no reassociation deadline in the authentication frames in this case.
(Originally LB105/19 submitted by Malinen, Jouni, during LB105 with ID Malinen/10)

SuggestedRemedy

Remove ", Reassoc-deadline" parameter from MLME-AUTHENTICATE.response() in FT-PMK-R1-SA-RECD in Figure 204n.

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.9.3** *P* **78** *L* **24** # 305

Malinen, Jouni

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

The Authenticator R1KH state machine shown in the figure is for RSN case and consequently, the reassociation deadline is included only in the EAPOL-Key frames during the initial association (which is indeed shown correctly in the FT-PTK-CALC-NEGOTIATING3 state on the previous page). The authentication frames used during FT over-the-air do not include the reassociation deadline in this case and as such, the FT-PMK-R1-SA-RECD state should not show "Reassoc deadline" as a parameter to MLME-AUTHENTICATE.response() primitive.

SuggestedRemedy

Delete ", Reassoc-deadline" from the parameters to MLME-AUTHENTICATE.response() in FT-PMK-R1-SA-RECD state for Figure 11A-14.

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.9.3.1** *P* **78** *L* **57** # 73

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

FT-AUTH is also entered in case of resource request protocol.
(Originally LB98/598 submitted by Malinen, Jouni, during LB98 with ID Malinen/53)

SuggestedRemedy

Replace "FT protocol is invoked" with "FT protocol or FT resource request protocol is invoked" in the description of FT-AUTH.

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.9.3.1** *P* **79** *L* **10** # 75

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

FT-INIT-R1_SA is also entered when rekeying PTK.
(Originally LB98/600 submitted by Malinen, Jouni, during LB98 with ID Malinen/55)

SuggestedRemedy

Add to the end of the FT-INIT-R1_SA description: "and when rekeying PTK".

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.9.3.1** *P* **79** *L* **8** # 74

CHAPLIN, CLINT F

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

FT-INIT-GET-R1_SA is not entered on R0KH timeout as claimed here (that timeout would cause a transition to DISCONNECT state).
(Originally LB98/599 submitted by Malinen, Jouni, during LB98 with ID Malinen/54)

SuggestedRemedy

Remove ", or when the R1KH issues a timeout failing to get a response from the R0KH" from the description of FT-INIT-GET-R1_SA.

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.9.3.2** *P* **79** *L* **43** # 76

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Typo
(Originally LB98/601 submitted by Malinen, Jouni, during LB98 with ID Malinen/65)

SuggestedRemedy

Replace "to initialize R1KH the state machine" with "to initialize the R1KH state machine."

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.9.4** *P* **80** *L* **30** # 311

Malinen, Jouni

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

FT-Full-Auth(R1KH-ID) is described as coming from FT-INIT-AUTH state of S1KH SM even though it is actually coming from FT-INIT-START.

SuggestedRemedy

Replace "FT-INIT-AUTH" with "FT-INIT-START" on the second line of Figure 11A-15.

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.9.4** *P* **80** *L* **35** # 77

CHAPLIN, CLINT F

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

Unnecessary text in S0KH state machine: Describing that MDID, R0KH-ID, R1KH-ID are somehow set (to where?) does not really add any value here.
(Originally LB98/602 submitted by Malinen, Jouni, during LB98 with ID Malinen/56)

SuggestedRemedy

Remove "Set MDID, R0KH-ID, R1KH-ID" from FT-R0-AUTH in Figure 204o.

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.9.4** *P* **80** *L* **42** # 78

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Typo
(Originally LB98/603 submitted by Malinen, Jouni, during LB98 with ID Malinen/57)

SuggestedRemedy

Replace "Derive-key-PMK-R0()" with "Derive-Key-PMK-R0()".

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.9.4** *P* **80** *L* **55** # 79

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Typo
(Originally LB98/606 submitted by Malinen, Jouni, during LB98 with ID Malinen/60)

SuggestedRemedy

Replace "Derive-key-PMK-R1" with "Derive-Key-PMK-R1".

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.9.4.1** *P* **81** *L* **18** # 80

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Typo
(Originally LB98/608 submitted by Malinen, Jouni, during LB98 with ID Malinen/62)

SuggestedRemedy

Replace "PMKR0" with "PMK-R0".

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.9.5** *P* **82** *L* **1** # 81

CHAPLIN, CLINT F

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

S1KH state machine seems to get stuck into FT-PTK-INIT-DONE at the completion of initial MD association or into SKIP-EAP at the completion of FT. This state machine should have a way of re-starting itself for next transition.
(Originally LB98/610 submitted by Malinen, Jouni, during LB98 with ID Malinen/64)

SuggestedRemedy

Add a global transition to R1-START state with condition "Init" to Figure 204p and Figure 204q. Add description of "Init" variable into 11A.8.5.2: "This variable is set to true to initialize the S1KH state machine. In addition, this variable can be used to re-start the state machine when transitioning to a new AP."

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.9.5** *P* **82** *L* **20** # 309

Malinen, Jouni

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

Typo

SuggestedRemedy

Replace "802.1X::portValid-= FALSE" with "802.1X::portValid = FALSE" in the FT-INIT-START state of Figure 11A-16.

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.9.5** *P* **83** *L* **26** # 82

CHAPLIN, CLINT F

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

FT-PTK-CALC state is claimed to "Init. PMK-R1 lifetime". It does no such thing; PMK-R1 is derived by S0KH and the lifetime is set there, not in S1KH. Furthermore, this typo of extra information in the state machine does not add any value.
(Originally LB98/611 submitted by Malinen, Jouni, during LB98 with ID Malinen/70)

SuggestedRemedy

Remove "Init. PMK-R1 lifetime" from FT-PTK-CALC in Figure 204q.

Response *Response Status* **U**

ACCEPT.

Cl **11A** *SC* **11A.9.5** *P* **83** *L* **30** # 83

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Inconsistent capitalization of a variable name.
(Originally LB98/613 submitted by Malinen, Jouni, during LB98 with ID Malinen/69)

SuggestedRemedy

Replace "Over-the-air" with "Over-the-Air" (line 16), "over-the-air" with "Over-the-Air" (line 31), and "over-the-DS" with "Over-the-DS" (line 31) in Figure 204q.

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.9.5** *P* **83** *L* **36** # 84

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Typo
(Originally LB98/614 submitted by Malinen, Jouni, during LB98 with ID Malinen/66)

SuggestedRemedy

Replace "Timeoutctr" with "TimeoutCtr" in Figure 204q (at least 10 occurrences).

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.9.5** *P* **83** *L* **41** # 85

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

Inconsistent use of MDID or MD-ID in place of MDIE.
(Originally LB98/616 submitted by Malinen, Jouni, during LB98 with ID Malinen/67)

SuggestedRemedy

Replace "MDID" with "MDIE" in MLME-REASSOCIATE.confirm() parameters (twice on row 51) and "MD-ID" with "MDIE" in MLME-RESOURCE_REQUEST parameters (twice on row 41).

Response *Response Status* **C**

ACCEPT.

Cl **11A** *SC* **11A.9.5.1** *P* **84** *L* **61** # 86

CHAPLIN, CLINT F

Comment Type **T** *Comment Status* **A**

Reassociation request is sent from two different states in S1KH state machine so it would be better not to make FT-RESERVE-2 explanation sound like it is the state doing this.
(Originally LB98/617 submitted by Malinen, Jouni, during LB98 with ID Malinen/72)

SuggestedRemedy

Add "after completion of FT resource request" to the end of FT-RESERVE-2 description.

Response *Response Status* **C**

ACCEPT.

Cl **A** *SC* **A.4.3** *P* **94** *L* **1** # 110

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

What provisions are needed to be able to extract and use the PICS and ASN.1? Are there provisions for single use of PICS and ASN.1 for 802.11 PICS similar to what is in 802.3? If not, why not?
(Originally LB98/701 submitted by Kurihara, Thomas, during LB98 with ID Kurihara/9)

SuggestedRemedy

Consider adding a note to the PICS and ASN.1 annexes, similar to wht is in 802.3 that grants a copyright release for the purspose of extracting and using the PICS and ASN.1, assuming that this meets the requirements for Digital Right Management.

Response *Response Status* **C**

ACCEPT.
11ma D9.0 includes the statement "Copyright release for PICS proforma: Users of this standard may freely reproduce the PICS proforma in this annex so that it can be used for its intended purpose and may further publish the completed PICS." No changes needed in this amendment.

Cl **D** *SC* **D** *P* **97** *L* **37** # 307

Malinen, Jouni

Comment Type **E** *Comment Status* **A**

Typo

SuggestedRemedy

Replace "dot11SpectrummanagementTable" with "dot11SpectrumManagementTable" (capitalized 'M' in "Management").

Response *Response Status* **C**

ACCEPT.

Cl **D** *SC* **D** *P* **99** *L* **40** # 111

CHAPLIN, CLINT F

Comment Type **E** *Comment Status* **A**

After addition of authentication algorithm 3, the 1999 Edition of IEEE 802.11 is not going to work very well as a reference here. Could the edition be removed or at least updated to 2007?
(Originally LB98/706 submitted by Malinen, Jouni, during LB98 with ID Malinen/75)

SuggestedRemedy

Remove ", 1999 Edition".

Response *Response Status* **C**

ACCEPT IN PRINCIPLE.
Changed to ", 2007 Edition"

Cl **D** *SC* **D** *P* **99** *L* **58** # 112

CHAPLIN, CLINT F

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

dot11AuthenticationAlgorithm is an INTEGER, it is not "set of" anything like the description here is trying to say. While this error is already in the base standard we could fix this since we are anyway changing the description here.
(Originally LB98/707 submitted by Malinen, Jouni, during LB98 with ID Malinen/76)

SuggestedRemedy

Replace "a set of all the authentication algorithms supported by the STAs. The following are the default values and the associated algorithm" with "the authentication algorithm described by this entry in the table. The following values can be used here."

Response *Response Status* **U**

ACCEPT.

Cl **General** *SC* **General** *P* *L* # 289

Stephens, Adrian P

Comment Type **TR** *Comment Status* **A** *reservation protocol*

The resource reservation scheme has a number of flaws. But the main one is that the semantics are of reservation rather than enquiry.
The result is that a badly-designed STA which periodically "checks" neighboring candidate transition APs for QoS resources using this mechanism can tie up resources unnecessarily. This behavior, while dumb, is valid, and potentially results in denial of service to bona fide members of those BSSs.
So the question is whether to allow or protect against this behavior in some way - or to change the semantics of the reservation service.

SuggestedRemedy

Modify the semantics of the reservation service so that it is equivalent to "If I asked you for these TSPECs right now, what would your answer be?". The essential difference is that the candidate AP discounts these queries when responding to local requests.
The result is that a transitioning STA may occassionally be surprised to have its TSPECs refused, to the benefit of existing members of that BSS that are not unnecessarily denied access to local resources.

Response *Response Status* **U**

ACCEPT IN PRINCIPLE
Changes given in submission 11-07-2516-01.

Cl **General** *SC* **General** *P* **0** *L* **0** # 113

CHAPLIN, CLINT F

Comment Type **TR** *Comment Status* **R** *Key distribution*

There are numerous comments that deal with the lack of a 3 party protocol-- including 6, 8, 202, 413, 414, and 491. These were all improperly resolved. For example, CID 8 was "resolved" by accepting a document whose contents were later removed (there is no MDC anymore). CIDs 413 and 414 were "resolved" by accepting document 0637r0 which introduced a 3 party protocol but subsequently document 1612r2 was accepted which removed the 3 party protocol that 0637r0 introduced. If the document which addressed the comment (0637r0) was removed (by 1612r2) then it is illogical to claim the comments are still "accepted".
(Originally LB105/5 submitted by Harkins, Dan, during LB105 with ID Harkins/09)

SuggestedRemedy

Define a secure 3 party protocol.

Response *Response Status* **U**

REJECT.
The previous comments cited by this comment all require a 3 party protocol that attempts to provide a mechanism for the STA to verify the trust assumptions are actually implemented by the R0KH. Such a verification under all conditions is impossible; there is no way that the STA can always verify that the R0Key has not been disclosed to an unauthorized third party, nor is there any way for the STA to always detect that a rogue R1KH (or any other entity) has gained access to the R0Key.