CI <b>00</b>	SC (	)	Р	L	# 276	C/ 00	SC	0	Р	L	# 288
Chaplin, C	Clint F					Chaplin	, Clint F				
Comment	Type	TR	Comment Status A		Crypto-agility	Comme	nt Type	TR	Comment Status A		Compromised AP
l also possil specil versic comp reaso algori neces (From	wonder bility that fic crypto on numbe atible. Bu ns, such thm (or a ssary in the othe sec	if enough it may at graphic a ers buried ut even w as the Pl algorithm he future. urity revie	consideration has been give some point become necess Igorithms used in the protoc in the protocol that a new v here the spec mandates spe RF and MIC calculations, it r suite) identifiers in those pla w of Dan Simon)	en to "crypto-agi ary to replace o ol. I assume tha ersion could ease crific algorithms night be worthw ces, to allow for	lity"that is, to the ne or more of the t there are enough sily be made backward for interoperability hile to consider adding easier revision if	In the able who thus netv moi con Fro	ne event to enter ble Mobili s spoof co work. For re secure sequence m the rev	that an Ac a Mobility ty Domain ommunica efficiency ones. Ho es of a cor vised secu	cess Point is completely comp Domain, it appears that this w . In particular, any AP can get a tion with any Mobile Station. The and deployment reasons, this wever, potential users of 802.1 npromise of any access point. rity review of John Mitchell	romised or a ould be a ma access to an hus one bad architecture 1r should be	I "rogue" Access Point is ajor compromise of the ay PMKR1 from the AS and AP can disrupt the whole might be favored over a aware of the
Suggester	dRomod					Sugges	tedReme	edy			
See	omment	y				See	e Comme	nt			
50000	Johnmenn					Respon	se		Response Status U		
ACCE P802. select the ve	11r has tor in the ersion su	RINCIPLI defined a RSN info bmitted fo	E mechanism to provide "cryp rmation element. This was or external security review.	oto-agility" throug added in D6.0, a	gh the AKM suite and was not present in # 137	C/ 00	s text in 1 R1KH m s for othe SC	1A.2.2 spenay receive or R1KHs.	ecities requirements for the aut e any keys. Even if one R1KH i Any statements beyond this ar <i>P</i>	hentication of s compromise outside the	t potential R1KHs before sed, it cannot obtain the e scope of 802.11. # 287
Chaplin, C	Clint F	•		-	" 101	Comme	, Clint F	TR	Comment Status R		Security Review
Comment	Type	ER	Comment Status A			Also	o, due to	the same	reason, the first message seen	ns to provide	an "oracle" for
Peopl (subm	le who su nitted by	ubmitted s Bill Marsh	security reviews need to be a nall)	acknowledged a	s contributors.	eav is n	esdroppe ot MAC'd	ers, that id I, an attack	entifies the next location of a M ker could spoof this message in	lobile Statior	n - since the first message o which the AP will reveal
Suggeste	dRemed	Y				the	m the rev	ised secu	rity review of John Mitchell	scenario is p	revented.
Incluc	le anothe	er three-c	olumn list on page v, at line	52, "The following	ng security experts	Sugges	tedReme	edv.	,		
Scott	ved this ( Kellv.	aocument	Include in the list Bill Burr	, Charles Clanc	y, Katrin Hoeper, and	See	e Comme	ent.			
Response	)		Response Status U			Respon	se		Response Status II		
ACCE	EPT.		,			RE Wh exc the the una	JECT ile it is teo hange, w content is target AF uthentica	chnically for re have ch s still visib P will revea ated STA.	easible to protect the first mess osen not to do so. Even if the f le and still an "oracle". If an att al the R1KH-ID, which is also a	age of the F irst message acker were to vaiable for th	Tast BSS Transition were to contain a MIC, o spoof the first message, ne probing by any

Page 1 of 89

C/ 00 SC 0		Р	L	# 286	C/ 00 SC	C 0	Р	L	# 280		
Chaplin, Clint F					Chaplin, Clint F						
Comment Type T Since the first tw service attack co would have to ca Note that injectir attack, as sugge	R o message ould be mo ache the no ng custom sted by a r	Comment Status R es are unsecured, they c unted by flooding AP2 w onces, and possibly have 802.11r messages is like recent presentation on 80 oviou of John Mitchell	ould be spoofed ith bogus auther to talk to the A by to be more th 02.11 security te	I. Further, a denial-of- ntication requests. AP2 S to get key information. an just a theoretical esting [1].	Comment Type In the event able to ente that this wor (From the so SuggestedRemo	TR that an Ac r a Mobility uld be a ma ecurity revi edy	Comment Status A scess Point is completely com / Domain, what capabilities we ajor compromise of the whole lew of John Mitchell)	promised or a ould an attacke Mobility Doma	"rogue" Access Point is r have? It would appear in.		
SuggestedRemedy					See comme	nt					
See Comment					Response		Response Status U				
Response REJECT While it is techni	F cally feasit	Response Status U	ssage of the Fa	st BSS Transition	ACCEPT IN PRINCIPLE The text in 11A.2.2 specifies requirements for the authentication of potential R1F that R1KH may receive any keys. Even if one R1KH is compromised, it cannot c keys for other R1KHs. Any statements beyond this are outside the scope of 802						
exchange, we hat the content is sti the target AP will unauthenticated	ave choser Il visible ar I reveal the STA	n not to do so. Even if the nd still an "oracle". If an a e R1KH-ID, which is also	e first message wattacker were to avaiable for the	were to contain a MIC, spoof the first message, probing by any	C/ <b>00</b> SC Chaplin, Clint F	0 0	Р	L	# 279		
	• • •				Comment Type	TR	Comment Status A		Security Review		
Chaplin, Clint F Comment Type <b>1</b> The first messag location of a Mol (From the securi	<b>R</b> Je seems to bile Station ty review c	P Comment Status <b>R</b> o provide an "oracle" for i. of John Mitchell)	L eavesdroppers,	# 281 Security Review that identifies the	Since the fir service attac would have Note that inj attack, as si L. Butti. Wi- https://www. (From the co	st two mes ck could be to cache the ecting cus uggested the Fi Advance blackhat.co	ssages are unsecured, they co e mounted by flooding AP2 wi ne nonces, and possibly have tom 802.11r messages is like by a recent presentation on 80 ed Fuzzing. Black Hat Europe icom/presentations/bh-europe- icom of John Mitsboll	build be spoofed th bogus auther to talk to the A ly to be more th 2.11 security to , 2007. 07/ Butti/Prese	d. Further, a denial-of- entication requests. AP2 \S to get key information. han just a theoretical esting. ntation/bh-eu-07-Butti.pdf.		
SuggestedRemedy					(FIOH the S						
See comment					Suggesteurreine See comme	ent					
Response	F	Response Status U			Response		Pasnonsa Status II				
While it is techni exchange, we ha the content is sti the target AP wil unauthenticated	cally feasil ave choser Il visible ar I reveal the STA.	ble to protect the first me n not to do so. Even if the nd still an "oracle". If an a e R1KH-ID, which is also	ssage of the Fa e first message v attacker were to avaiable for the	st BSS Transition were to contain a MIC, spoof the first message, probing by any	ACCEPT IN We acknow flooding and susceptible introduces r unlicensed s interference	PRINCIPI ledge that l similar at to similar o no new typ spectrum is	LE this is a potential attack, and i tacks. The existing 802.11-20 denial-of-service attacks. To o es of vulnerabilities beyond th s always susceptible to denial	implementatior 07 security me our knowledge, e existing 802. -of-service atta	ns need to be resistant to chanism is already this amendment 11-2007. In addition, acks through radio		

C/ 00 SC 0 Chaplin, Clint F	Р	L	# 277	<i>CI</i> <b>00</b> Chaplin, Cl					
Comment Type <b>TR</b> When handling a Mobile associated with the stat cached? (From the security revie	Comment Status A e Station transition, AP2 mu ion. How is this handled? F ew of John Mitchell)	ust be able to ge Pulled by AP2 fro	Key distribution at access to the PMKR1 om the AS, and then	Comment One of the sec to obta concer					
SuggestedRemedy See comment	third ar a malic essent about v STA ha MIC to (From								
Response ACCEPT This comment reflects a information. This inform									
				Suggested					
C/ 00 SC 0	Р	L	# 275	See co					
Chaplin, Clint F				Response					
Comment Type TR My only recommendation string, "802.11r", or som keys for some other pur (From the security review	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				exchar					
Response ACCEPT IN PRINCIPL Include "FT" in all of the	Response Status U E. alabels.								

C/ 00	SC O	Р	L	# 274
Chaplin, Clir	nt F			
Comment Ty	vpe TR	Comment Status R		MIC message 2

One other area of concern is the lack of a MIC on the Authentication Response message, or he 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 hird and fourth messages of the FT protocol are in the critical path. By not including a MIC, 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)

#### gestedRemedy

See comment

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. n 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.

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Page 3 of 89 09/27/2007 06:28

Kev distribution

C/ 00	SC O	Ρ	L	# 273
Chaplin, Clin	tF			

### Comment Type TR Comment Status R

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 multivendor 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

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.

Response Status U

C/ 00	SC O	Р	L	# 272
Chaplin, Clir	nt 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.

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Comment ID # 272

Page 4 of 89 09/27/2007 06:28

C/ 00	SC (	)	Р	L	# 270	C/ 00 SC	C 0	Р	L	# 268
Chaplin, Clir	nt F					Chaplin, Clint F	•			
Comment Ty PTK and " Output docume Hence F transien KCK = L The des PTK>= 3 This is c (From th	ype d Pairv t lengtl nt: CC PTK is t keys (PTK, cribed 3* 128 clearly he sec	TR vise tran PTKLe MP (128 128, 250 (KCK, k 0, 128) derivati bits. Ho a mistal urity revi	Comment Status A nsient Keys (KCK, KEK, TK) Di en depends on negotiated CS. 8 bits), TKIP (256), WEP-40 (4 6, 40, or 104 bits long. This is (EK,TK) with , KEK = L(PTK, 128, 128), TK ion of KCK, KEK, TK (Section a powever PTK<= 256 bits and thu ke in the description! iew of Bill Burr)	scussion From Table 60 0), WEP-104 ( not long enoug = L(PTK, 256, 3.5.1.5.5) requ is never suffici	<i>PTKLen</i> in Section 8.5.2 in core 104) h to derive the pairwise 128) res ently long!	Comment Type PMK-R0 Dis "Here KDF- generate 12 problems? (From the se SuggestedReme See comme Response	TR scussion 384 is use 8 bits as s ecurity rev edy nt	Comment Status R ed, as opposed to KDF-256 as salt for the key identifier. Does iew of Bill Burr) Response Status U	for the other ket this asymmetry	Security Review eys. This is done to y introduce any security
SuggestedR See con	emed	/				REJECT At this point by virtue of t	the group	does not see any new vulnera	ability being intr	roduced into the protocol
specifica defined At page At page value of	ally, it cipher 24 line 24 line PTKL	s 256+le from 8.9 25 cha 54 inse en) depe	ength(TK). However, use of P 5.2. anged cross reference from "Ta erted "For vendor specific ciph end on the vendor specific alog	TKLen is confu able 60" to "Tal er suites, the le prithm."	sing with only a single ble 8-2". ength of TK (and the					
C/ 00	SC (	)	P	L	# 269					
Chaplin, Clir	nt F									
Comment Ty PMK-R1 " Asymm (From th	vpe I Discu netry in ne sec	TR Ission name urity revi	Comment Status R derivation compared to PMK-R iew of Bill Burr)	80	Security Review					
SuggestedR	Remed	/								
See con	nment									
Response			Response Status U							
REJECT At this p by virtue	F oint th e of thi	e group s asymn	does not see any new vulnera netry.	bility being intr	oduced into the protocol					

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID Comment ID 268

Page 5 of 89 09/27/2007 06:28

-											
C/ <b>00</b>	SC O	Р	L	# 265	CI <b>00</b>	SC	0	Р	L	# 278	
Chaplin, (	Clint F				Chaplin,	Clint F					
Commen	t Type TR	Comment Status A		Security Review	Commen	t Type	TR	Comment Status A		Security Review	
Broad additi additi Beac (DoS 1. Ad In tha will e:	dcasted beacons ional information ional information on signals (by na ) attacks. The ne versary changes at case, STAs wo xecute a full re-at a case disable th	of APs that support FT within about the mobility domain an is contained in a Mobility Dor ture) cannot be protected an w MDIE element enables the bit indicating the FT ability of n't request FT even though it association and authentication of ET forture.	n the mobility dou d the FT capabil main Information d are thus vulner following DoS a f an AP to zero. is supported by . Hence, an adve	nain contain some ities of the AP. This Element (MDIE). able to Denial of Service ttacks: the AP. Instead the STA ersary modifying the	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 n 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						
This 2. Ad In tha This 3. Ad Detec	may not be detect versary changes at case, a STA ma will be detected b versary changes cted if STA reque	this service. "invalid MDIE"). ode 54, not detected if	Respons ACC The estal Tran	e EPT IN F first two r plishmen sitions.	PRINCIPI message t. P802.1	Response Status U E s cannot be protected as they 1w will protect the Action fram	are exchanged es for over-the	d prior to key -DS Fast BSS			
Conc able t	does not request lusions: no sever to disable the FT	F I due to wrong information e security risk. However, we service.	should note that	an adversary may be	<i>Cl</i> <b>00</b> Chaplin,	SC Clint F	0	Р	L	# 264	
Suggeste	dRemedy		Comment Type ER Comment Status A People who submitted security reviews need to be acknowledged as contributor								
566 (	Johnmenn				Suggeste	edRemed	dy				
Response ACCI We a	e EPT IN PRINCIPI cknowledge that	Response Status U INCIPLE e that this is a potential attack, and implementations need to be resistant t			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, Katr Hoeper, Srinivas Inguya, Scott Kelly, John C, Mitchell, Arnab Roy, Dan Simon.						
simila authe	ar attacks. The co entication exchan	ontents of the MDIE from the ge, where they are covered b	Beacon are repe ov a MIC. The ex	ated in the FT isting 802,11-2007	Respons	е		Response Status U			
secu	ity mechanism is	already susceptible to simila	ar denial-of-servi	ce attacks. To our	ACC	EPT.					

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

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

Page 6 of 89 09/27/2007 06:28

Submission

attacks through radio interference.

Bill Marshall, ATT Labs Research

		# 200	C/ 00 SC	0	P	L	# 271
			Chaplin, Clint F				
Comment Status A 5.1.5.2) e as in SP800-108, KDF ered being secure guideline that can be cit F computations: i and la 302.11r must specify en bel" is explicitly describe of Bill Burr) Response Status U paragraph in 8.5.1.5.2 ' ordering conventions of during the Sponsor Ballo	F in counter moded ed? ength encoded a coding for K, lat d, however exp K, label, and Co 7.1.1." of period of this	# 1200 KDF specification de with prf=HMAC-SHA- according to Section 7.1.1 bel, and content. In licit encoding for key K	Cr uu Sc Chaplin, Clint F Comment Type Based on my perspective. only one sec R0KH-R1KH communicati "The R0KH a be used to exchange cr assumes tha key transfer authorization for distribution standard." I understand that such a protocol shou sort of thing typically cover most in the security direc I won't attem the following cryptogray must be great than or equa That is, if the 802.11i keys distribution of should be of if digital co example EAI then I think this way to sum t and the prev link in the se chain. Other Of course, it stronger than	TR / limited re I have unity-related ions secur and the R1 yptograph it the includes th includes th that the 1 uld remain is ered in oth ctorate woo ipt to rewriti- is includes th includes th is includes th is includes th is is is ot alw is is not alw is not alw is not alw is not alw is not alw is not alw	<i>Comment Status</i> <b>A</b> eview, I also think the overall of ed concern, and that relates to rity. Here is the current text fro 1KH are assumed to have a s nic keys without exposure to an the PMK-R1, the PMK-R1 con- otocol ing material from the R0KH to the 11r group does not want to dea in outside the scope of this wo her IEEE documents. However build agree that the current text ite the text myself, but I think is edence": the cryptographic pro- yptographic properties of the of ES-CCM, then the crypto-inte- r better) strength. are used for 802.1X (i.e. as p -R1KH authentication should it is where attackers will aim. rays possible to say whether of and it's occur to get into ratio.	design is quite so o the attempt to orm section 11A.2 ecure channel b ny intermediate p text, and the ass the R1KH is outs sign a capwap-li rk. Also, I don't k or, were this an IB t comes up shor it would be good operties of the ke channels for whi grity mechanism part of the 802.11 arguably be simi ribution channel one algorithm is s	# <u>[2/1</u> <i>Key distribution</i> olid from a security completely punt on 2.2: etween them that can parties. This standard sociated key side the scope of this ke protocol, and I agree know how thoroughly this ETF document, I think t. I if the text addressed ay exchange channel ch the keys will be used. a employed for the Ii key derivation, for ilarly strong. A simple must not be the weak stricly equivalent to (or
	Comment Status A 5.1.5.2) e as in SP800-108, KDF lered being secure guideline that can be cit DF computations: i and le 802.11r must specify end bel" is explicitly describe of Bill Burr) Response Status U paragraph in 8.5.1.5.2 " ordering conventions of during the Sponsor Ballo	Comment Status A 5.1.5.2) e as in SP800-108, KDF in counter model lered being secure guideline that can be cited? DF computations: i and length encoded a 802.11r must specify encoding for K, lab bel" is explicitly described, however expl of Bill Burr) Response Status U paragraph in 8.5.1.5.2 "K, label, and Co ordering conventions of 7.1.1." during the Sponsor Ballot period of this a	Comment Status A KDF specification 5.1.5.2) e as in SP800-108, KDF in counter mode with prf=HMAC-SHA- lered being secure guideline that can be cited? F computations: i and length encoded according to Section 7.1.1 302.11r must specify encoding for K, label, and content. In bell is explicitly described, however explicit encoding for key K of Bill Burr) Response Status U paragraph in 8.5.1.5.2 "K, label, and Context are bit strings, and ordering conventions of 7.1.1." during the Sponsor Ballot period of this amendment, we will	Comment Status A       KDF specification         5.1.5.2)       e as in SP800-108, KDF in counter mode with prf=HMAC-SHA- lered being secure       Based on my         guideline that can be cited?       Communication         >DF computations: i and length encoded according to Section 7.1.1       Communication         302.11r must specify encoding for K, label, and content. In       be used to         paragraph in 8.5.1.5.2       W, label, and Context are bit strings, and       moderstand."         paragraph in 8.5.1.5.2       K, label, and Context are bit strings, and       protocol sho         ordering conventions of 7.1.1."       understand       that such a         during the Sponsor Ballot period of this amendment, we will       security direc       security direc         during the Sponsor Ballot period of this amendment, we will       cox of thing       typically cov         c - if digital c       example EA       that is if the         socurity direc       is with be reve       should be of         if digital c       example EA       then I think t	Comment StatusKDF specification5.1.5.2)e as in SP800-108, KDF in counter mode with prf=HMAC-SHA- lered being secure guideline that can be cited?Based on my limited n perspective. I have only one security-relat ROKH-R1KH communications secu in and length encoded according to Section 7.1.1 of 6 Bill Burr)Based on my limited n perspective. I have only one security-relat ROKH-R1KH to communications secu authorizations. The pr for distribution of keyin standard." I understand that the 4 that such a protocol should remain sourced in off that such a protocol should remain sourced in off that such a protocol should remain sourced in off most in the security directorate wull won't attempt to rew the following: cryptographic "imper must be greater than or equal to the cr That is, if the 802.11 i keys are for A distribution of samel and the ROKH way to sum this and the Previous bulle link in the security chain. Otherwise, that Of communication security chain. Otherwise, that Of course, it is not alw stronger than) arctificates	Comment Status A KDF specification 5.1.5.2) eas in SP800-108, KDF in counter mode with prf=HMAC-SHA- lared being secure guideline that can be cited? F computations: i and length encoded according to Section 7.1.1 302.11r must specify encoding for K, label, and content. In beil" is explicitly described, however explicit encoding for key K are fill Burr) Response Status U are grangraph in 8.5.1.5.2 "K, label, and Context are bit strings, and ardering conventions of 7.1.1." Response Ballot period of this amendment, we will during the Sponsor Ballot period of this amendment. during the Sponsor Ballot period of this amendment,	Comment StatusAKDF specification5.1.5.2)as in SP800-108, KDF in counter mode with prf=HMAC-SHA- lered being secure quideline that can be cited?Based on my limited review, I also think the overall design is quite s perspective. I have only one security-related concern, and that relates to the attempt to ROKH-R1KH70.2.11r must specify encoding for K, label, and content. In 1 is explicitly described, however explicit encoding for key K if Bill Burr)The ROKH and the R1KH are assumed to have a secure channel b be used to exchange cryptographic keys without exposure to any intermediate assumes that the key transfer includes the PMK-R1, the PMK-R1 context, and the ass authorizations. The protocol for distribution of theying material from the R0KH to the R1KH is out standard.*that such a protocol should remain outside the scope of this work. Also, I don't is sort of thing is typically covered in other IEEE documents. However, were this an II most in the security directorate would agree that the current text comes up shor sort of thing is typically covered in other IEEE documents. However, were this an II most in the security directorate would agree that the current text comes up shor sort of thing is typically covered in other IEEE documents. However, were this an II most in the security directorate would agree that the current text comes up shor sort of thing is typically covered in other IEEE documents. However, were this an II most in the security directorate would agree that the current text comes up shor that is, if the eagree in than or equal to the cryptographic properties of the channels should be of similar (or better) strength. if digital certificates are used for 802.11% (exe as part of the 802.11% example EAP-TLS), then I think the OKHH current

 TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general
 Page 7 of 89

 COMMENT STATUS: D/dispatched A/accepted R/rejected
 RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn
 Comment ID
 Page 7 of 89

 SORT ORDER: Comment ID
 09/27/2007 06:28

Submission

this key distribution channel and the associated risks. # 1 C/ 00 SC 0 P0 L27 (From the security review of Scott Kelly) CHAPLIN, CLINT F SuggestedRemedy Comment Type T Comment Status A See comment pre-auth & key-caching are not necessarily coupled Response Response Status U (Originally LB98/21 submitted by Ciotti, Frank, during LB98 with ID Ciotti/09) ACCEPT SuggestedRemedy 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 Change text from: cryptographic strength of the channels for which the keys will be used". Inserted text at page "pre-authentication and key caching" 50 line 27, "The cryptographic strength of the authentication is assumed to be greater than to: or equal to the cryptographic strength of the authentication between the STA and AS." "pre-authentication or key caching" Response Response Status C Ρ 1 C/ 00 SC 0 # 267 ACCEPT. Chaplin, Clint F Comment Type TR Comment Status A Security Review C/ 00 SC 0 P0 L 30 # 2 PMK-R0 Discussion CHAPLIN. CLINT F " What is R0KH-ID = identifier of PMK-R0 holder in authenticator? Specification needed for Comment Type E Comment Status A proper encoding and computation. The identifier is probably the NAS address of the authenticator; however this is not Tvpo mentioned here! (Originally LB98/22 submitted by Ciotti, Frank, during LB98 with ID Ciotti/10) (From the security review of Bill Burr) SuggestedRemedy SugaestedRemedv "Install the key" --> "Install the keys" See comment Response Response Status C Response Response Status U ACCEPT. ACCEPT IN PRINCIPLE The definition of R0KH-ID is given in 11A.2.2. Text has been added in the definition of the C/ 00 SC 0 P0 L41 # 3 kdf function that defines this as a bit string. CHAPLIN. CLINT F C/ 00 SC 0 PO LO # 317 Comment Type T Comment Status A Coordination, Editorial 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". Comment Status A Comment Type **GR** (Originally LB98/23 submitted by Ciotti, Frank, during LB98 with ID Ciotti/11) Please submit seperate file for figures, if they weren't created in Framemaker. SuggestedRemedv SuggestedRemedy Consider changing: "transmission of the last/first acknowledged data frame" Response Response Status U "receipt of the last/first data frame" ACCEPT. Response Response Status C ACCEPT.

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general Page 8 of 89 COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn Comment ID # 3 SORT ORDER: Comment ID 09/27/2007 06:28

Bill Marshall, ATT Labs Research

Submission

<i>CI</i> <b>00</b> Chaplin, C	SC Clint F	0	Р	1	L18	# 135		C/ <b>00</b> Edney, Jona	SC athan	0	P <b>49</b>	L <b>25</b>	# 294		
Comment	Туре	ER	Comment Status	5 <b>A</b>				Comment T	ype	TR	Comment Status A		Security assumptions		
title in Suggester	ncorrect, dRemed	should be ly ification" t	e "specifications" (pl	ural) (s	ubmitted by Bill Ma	rshall)		Clause a list of Line 26: implies	11A.2 proble "R1K	2.2: This c ems: (H in the <i>i</i>	lause is very poorly written an AP" This is the only place whe	Id should be re	evised or deleted. Here is R1KH is in the AP and		
Response ACCE	ept.		Response Status	U			Line 302 with equ Line 302 authent Line 402 Does it so what Line 452 Earier it DS. So Line 522 term an Running Page 50 underst term tha Page 50 Page 50	"ROK ilpme 1st s catior Wha is? "Eac said "ROK d yet g of th b: Line and 8 d yet g of th b: Line and 8 d yet g of th b: Line	KH interact int sentence: in result vi- t is the int that have that have that have that have that have this is a n the same p e 5: "sha 02.1X aut ow. 13: Typo agraph at	ts with 802.1X": 802.1X is a s what does this mean? How ca a 802.1X. I just don't understa ent of this statement? How co a to do it at the same moment der name is mapped to a phys eyholders were part of the SM here? e co-resident" What does "co ormative statement. Does it m rocessor? In the same buildin Il provide the IEEE802.11 Aut henticator function but I am n "dot11FTR0eyHolderID" line 17 seems to be pretty red	an the R0KH re ind this senten ould they derive in time? I don' sical entity in the IE on the STA co-resident'' me tean in the sar ig? I have no id thenticator fund ot familiar with	ot capable of interaction eceive the EAP nee e the PTK non-mutually? 't think that is intended - he DS where it resides" which is not part of the ean. This is not a defined me mechanical box? dea ction" What is this? I n this. It is not a defined			
								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 ACCEP Page 49 Page 49 Ine) Page 49 R1KH a Page 49 where it Page 49 Page 50 derive a typo fixe Page 50	T ) line : ) line : ) line : ) line : ) line : ) line : nd dis ed. ) line :	26, delete 30, chang 31, chang 40, chang IKH each 46, delete les. 52, chang 5, delete stribute th 17 is stati	Response Status U ed "in the AP" le "802.1X" to "the IEEE 802.1 le "with 802.1X" to "with the IE le "The R1KH shall derive the derive the PTK." "Each key holder name is ma le "co-resident" to "co-located 'provide the IEEE 802.11 Auti e GTK") ng different requirements than	1X Authenticat EE 802.1X Au PTK mutually apped to a phy " henticator func n the paragrap	tor" uthenticator" (twice on this with the S1KH" to "The vsical entity in the DS ction to" (leaving "shall wh at line 23.		

CI 00 Edney, Jon	SC <b>0</b> athan	P <b>50</b>	L 63	# 295	<i>CI</i> <b>00</b> Ptasinski,	SC <b>0</b> Henry S	P51	L 35	# 316
Comment Clause	<i>Type</i> <b>E</b> 11A.3: talks ab	Comment Status A	tion over DS"		<i>Comment</i> Remo	<i>Type</i> <b>TR</b> ove dependent	Comment Status <b>R</b> cy on 802.11i 4-way handshake	e for initial assoc	Initial MD Association
Suggested insert t Response	Remedy he word "field" c ⊃⊤	or similar to clairfy meaning Response Status <b>C</b>			Suggester Use n occur using	dRemedy nodified over-t between FT & data frames v	the-air fast BSS transition proto 302.11 Authentication exchange vith ToDS = 0, FromDS = 0 for	col instead. 802 ∋ and FT 802.11 EAPOL-Key me	.1X/EAP exchange can Reassociation exchange, ssages.
ACCEI	1.				Response	)	Response Status U		
CI <b>00</b> Hansen, C Comment T Initial a	SC <b>0</b> J <i>Type</i> <b>TR</b> association shou	P 51 Comment Status R Ild not require 4-way handshak	L <b>35</b> ke.	# 319	REJE Multip The c Furthe within	CI ble alternatives hosen result v er, the focus o the Mobility I	s were considered for the initial was selected because it reused of TGr is on the transitions, and Domain.	authentication, i many of the exis the initial associ	including this mechanism. sting RSN mechanisms. iation is not a transition
Suggested	Remedy				C/ 00	SC 0	P61	L <b>23</b>	# 318
Modifie exchar Reasso messa	ed over-the-air fange can occur be ociation exchang ges.	ast BSS transition protocol can etween the FT 802.11 Authent ge, using data frames with ToI	n be employed. ication exchan DS = 0, FromD	The 802.1X/EAP ge and the FT 802.11 S = 0 for EAPOL-Key	Hansen, C Comment The re	CJ <i>Type</i> <b>TR</b> esource reque	Comment Status R est protocol is adds extra time to	o the fast transiti	reservation protocol ion setup, and is unable to
Response		Response Status U			Suggester	d Domodu	guarantees. It's benefits are ut	JUIUUS.	
REJEC Multiple	CT e alternatives w	ere considered for the initial a	uthentication in	ocluding this mechanism	Remo	ove.			
The ch	osen result was	selected because it reused m	any of the exis	ting RSN mechanisms.	Response	9	Response Status U		
Further, the focus of TGr is on the transitions, and the initial association is not a transition within the Mobility Domain.					REJE The 6 specif tolera	CT -message exc fically carrier g nce data strea	change is critical in some deplo grade deployments that use HC ams, to accomodate TSPEC pro	yments of Fast E CA and high bai ocessing.	3SS Transition, ndwidth/low jitter

Page 10 of 89 09/27/2007 06:28

Bill Marshall, ATT Labs Research

<i>CI</i> <b>00</b> Ptasinski,	SC <b>0</b> Henry S	P61	L <b>23</b>	# 315	<i>CI</i> <b>02</b> Mccann, S	SC <b>2</b> Stephen	P1	L <b>49</b>	# 143
Comment Resor transi	<i>Type</i> <b>TR</b> urce Request pro tion" setup, and i	Comment Status <b>R</b> btocol is overly complex, adds a is unable to provide any service	extra processino e guarantees.	reservation protocol g time to the "fast	<i>Comment</i> The ir and d	<i>Type</i> <b>E</b> nitial reference late be also add	Comment Status <b>R</b> "FIPS PUB 180-2-2002" appear ded	s to be rather w	eak. Could a full title
Suggeste	dRemedy				Suggeste	dRemedy			
Delete	e the protocol.				Add t	he full title of th	is reference and publication date	e	
Response REJE The 6 specif tolera	e CT -message excha fically carrier gra nce data stream	Response Status U inge is critical in some deployments that use HCC/ s, to accomodate TSPEC proce	nents of Fast BS A and high band essing.	SS Transition, Iwidth/low jitter	Response REJE This r Secui acqui	e CT. reference follow re Hash Standa ring copies of F	Response Status <b>C</b> vs the style used in 802.11-2007 ard." 802.11-2007 includes a for TPS publications.	7, specifically "F otnote providing	IPS PUB 180-1-1995, information for
CI 00	SC 0	P <b>97</b>	L37	# 136	C/ 03	SC 3	P <b>2</b>	L 27	# 6
Chaplin, C	Clint F				CHAPLIN	, CLINT F			
Comment MIB v Suggester chang	t <i>Type</i> <b>ER</b> variable wrong (si <i>dRemedy</i> ge "Spectrummar	Comment Status A ubmitted by Bill Marshall) nagementTable" to "SpectrumN	<i>I</i> anagementTal	ble"	Comment Add a speci guide (Origi	t <i>Type</i> <b>TR</b> a definition of th fication. The de nally LB98/26 s	Comment Status A e "FT 4-Way Handshake" as thi finition of "4-Way Handshake" in submitted by Sood, Kapil, during	is term has been n 802.11-REVm g LB98 with ID S	n used frequently in this na9.0 can be used as a Sood/046)
Response	9	Response Status U	-		Suggeste	dRemedy			,
ACCE	SC 1	P1	L 29	# [132	Insert BSS maste Editor	t "3.XX FT 4-Wa Transition is en er key (PMK-R1 r: Please numb	ay Handshake: A pairwise key n abled. This handshake confirms I) by two parties and distributes er XX appropriately.	nanagement prosses a mutual posses a group tempor	otocol used when Fast sion of a pairwise al key (GTK)"
Comment Refer	ediger E <i>Type E</i> ence should be r	Comment Status A nade to 802.11k-D8.0			Response ACCE	e PT.	Response Status U		
Suggester chang "(base	<i>dRemedy</i> ge reference to ed on P802.11k-l	D8.0)"			<i>Cl</i> <b>03</b> Kays, Rue	SC 3 ediger	P2	L 37	# 134
Response ACCE	e EPT.	Response Status C			Numb Suggeste	oers 3.95a alrea dRemedy	ady used in 802.11k D8.0		
					Chan Chan	ge "3.95a" to "3 ge "3.95b" to "3	3.95b". 3.95c"		
					Response ACCE All oth	e EPT. her changes ma	Response Status <b>C</b> ade in P802.11k in D8.0 (and 80	)2.11-2007) also	o tracked in P802.11r.

CI 03	SC 3.54b	P <b>2</b>	L 23	# 5	C/ <b>04</b>	SC 4	P <b>3</b>	L 56	# 7
CHAPLIN	, CLINT F				CHAPLIN,	CLINT F			
Comment	t Type <b>T</b>	Comment Status A			Comment	Type E	Comment Status A		
"The fails a first	first association or a association, or a	reassociation procedure&" first/second/any) reassociat	s confusing. It in ion. This is not the	nplies that we either do ne intent of the	Missir (Origir	ng PMKR0Name anally LB98/46 sub	and PMKR1Name abbreviatic omitted by Sood, Kapil, during	ons in this list LB98 with ID \$	Sood/013)
defini that th	tion. It is an assoc	iation procedure or a reasso	ciation procedure	e, in which the result is	Suggested	dRemedy			
(Origi	nally LB98/25 sub	mitted by Sood, Kapil, during	g LB98 with ID S	ood/010)	Add a	bbreviations for "	PMKR0Name First level Pairv	wise Master Ke	y name" and
Suggeste	dRemedy				"PMK	R1Name Second	l level Pairwise Master Key Na	ame" to this list	
Chan OR.	ge "first associatio	n or reassociation procedure	e" to "first associa	ation procedure"	Response ACCE	PT IN PRINCIPL	Response Status <b>C</b> .E.		
Chan reass	ge "first associatio ociation procedure	n or reassociation procedure	e" to "first associa	ation or first	PMKR PTKN	0Name is not an ame. For consist	acroynm. PMKR1Name is als ency, PTKName deleted from	so not an acror i clause 4.	nym. Neither is
Response	è	Response Status C							
ACCE Chan	EPT. ged to "first associ	ation or first reassociation:							
C/ 03	SC 3.89a	P <b>2</b>	L <b>34</b>	# 133					
Kays, Rue	ediger								
Comment Numb	t <i>Type</i> <b>E</b> ber 3.89a is alread	Comment Status A y used in 802.11k-D8.0							
Suggeste Not p	<i>dRemedy</i> ossible in this draf	t, if alphabetic order has to t	be kept						
Response	9	Response Status <b>C</b>							
ACCE Chan	EPT. ged 3.89a to "3.89	-5" and added an Editorial N	lote below explai	ning the required action					
C/ 03	SC 3 99	P <b>2</b>	17	# 1					
CHAPLIN	, CLINT F	12	L1	$\pi$ 4					
Comment	t Type <b>T</b>	Comment Status A							
"PMK (Origi	C-R1 value" is redu nally LB98/24 sub	ndant. mitted by Sood, Kapil, during	g LB98 with ID S	ood/009)					
Suggeste	dRemedy								
Chan	ge "PMK-R1 value	" to "PMK-R1".							
Response	e	Response Status C							
ACCE	EPT.								

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Comment ID # 7

Page 12 of 89 09/27/2007 06:28 Clause5

C/ <b>05</b>	SC 5	Р	L	# 321
Malinen.	Jouni			

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

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.

C/ 05	SC :	5		P <b>4</b>	L <b>2</b>	5	#	138		
Chaplin, C	lint F									-
<b>.</b> .	-		~						~	_

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 ACCE	PT.	Response Status U		
CI <b>05</b>	SC 5.4.2.1	P <b>4</b>	L <b>25</b>	# 296
Montemur	ro, Michael			
Comment	Туре Т	Comment Status A		Clause5
There	should be a shore	t description of Fast BS	S-Transition in this cla	ause.
Suggestee	dRemedy			
Add th The F BSS-1 enable	ne following text to ast BSS-Transitio Fransition betwee ed in the ESS.	o this subclause as a ne on protocol provides a m n access points in an R	ew paragraph following nechanism for a non-A SN, or when QoS Adr	g the first paragraph: P STA to perform a nission Control is
Response	,	Response Status C		
ACCE	PT.			
Cl <b>05</b> Montemur	SC <b>5.4.3.4</b> ro, Michael	P <b>4</b>	L <b>25</b>	# 297
Comment The F assoc	<i>Type</i> <b>T</b> ast-BSS Transitio iation.	Comment Status A on protocol adds an add	itional mechanism to	<i>Clause5</i> establish a new security
Suggestee	dRemedy			
Modify define the 4-	y the second sent d in this standard Way Handshake,	tence of the first paragra I provide fresh keys by r the Fast BSS-Transitio	aph of 5.4.3.4 as follow means of protocols ca n protocol, and Group	vs: The procedures lled Key Handshake.
Response		Response Status C		

ACCEPT.

CI 05 Montemu	SC <b>5.8</b> rro, Michael	P4	L <b>25</b>	# 298	<i>CI</i> <b>06</b> Malinen, J	SC ( Iouni	6.1.2	Р	L	# 320
Comment The F assoc	<i>Type</i> <b>T</b> ast-BSS Transiti iation.	Comment Status <b>A</b> on protocol adds an additional	mechanism to	Clause5 establish a new security	Comment 802.1 Claus	<i>Type</i> 1r introd e 11A. H	ER uces a ne lowever,	Comment Status <b>A</b> w authentication exchange (f 6.1.2 was not updated to poin	T protocol) w t to this clause	hich is described in e.
Suggeste Modif 802.1 Trans Hand Response	dRemedy y the first sentend 1 depends upon ition protocol, an shake, described PT.	ce of the second paragraph of IEEE Std 802.1X-2004 and the d Group Key in Clauses 8 and 11A, to esta <i>Response Status</i> <b>C</b>	clause 5.8.1 as 4-Way Hands blish and chan	follows: IEEE Std hake, the Fast BSS- ge cryptographic keys.	Suggester Modif authe Claus inform Response ACCE	dRemed y the thin ntication e 8" with nation as PT.	y ed paragra exchang "During describe	aph of 6.1.2 by adding a refere le, both parties exchange auth the authentication exchange, ed in Clause 8 and Clause 11/ Response Status <b>U</b>	ence to Clause nentication info both parties e A."	e 11A: replace "During the ormation as described in exchange authentication
<i>CI</i> 05 Montemu	SC <b>5.8.2.1</b> rro, Michael	P <b>4</b>	L <b>25</b>	# 299	<i>Cl</i> <b>06</b> Malinen, J	SC ( Iouni	6.1.2	Р	L	# 308
Comment The F assoc Suggeste Add ti BSS- Response ACCE	Type <b>T</b> Fast-BSS Transiti- ciation. dRemedy he following text a Transition, derive EPT.	Comment Status A on protocol adds an additional after the second bullet of the se PMK-R0 and PMK-R1 keys. <i>Response Status</i> <b>C</b>	mechanism to	<i>Clause5</i> establish a new security oh: "- In the case of Fast	Comment IEEE Howe alread be ne cipher Suggestee Add fo "The u	Type 802.11r/ ver, TKI dy reached eded to for new dRemed blowing use of TI	TR D7.0 see P was de ed the es allow smo deploym deploym y paragrap KIP as a	Comment Status <b>R</b> ms to allow TKIP to be negoti signed as a temporary solutio timated end of that lifetime. W both transition to more secure tents should be deprecated. h to the end of 6.1.2 (just afte pairwise cipher when using Fa	ated as a pair n with limited /hile use of TK solutions, use not the paragrap ast BSS Trans	TKIR wise cipher with FT. lifetime and we have KIP as a group cipher may e of TKIP as the pairwise oh that deprecates WEP): sition is deprecated. TKIP
<i>CI</i> <b>05</b> Montemu	SC <b>5.8.2.1</b> rro, Michael	P5	L <b>25</b>	# 300	was d deploy not all comm	esigned yments.' lowing it	as a tem More ge to be neg	porary solution with a limited neral deprecation of TKIP for gotiated for FT would also be a	ifetime and it IEEE 802.11 an acceptable	is unsuitable for new or strict requirement of way of addressing this
Comment The F assoc Suggeste Modif transi Response ACCE	Type <b>T</b> Fast-BSS Transiticiation. <i>dRemedy</i> y the third bullet of ent key (PTK) from PT.	Comment Status A on protocol adds an additional of the second paragraph as fol m the PMK, or the PMK-R1 in <i>Response Status</i> C	mechanism to ows: Derive the case of Fa	<i>Clause5</i> establish a new security a fresh pairwise st BSS-Transition.	Response REJE There Trans	CT are exis	sting depl	Response Status U	AES but would	d benefit from Fast BSS

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Page 14 of 89 09/27/2007 06:28

Submission

RIC format

C/ 07	SC 7	P14	L <b>26</b>	#	142
Chaplin, Clin	t F				

Comment Type TR Comment Status A

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." Figure 7-95x, "Length" (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).-qp>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 7.3.1.5, 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."

C/ 07	SC 7.3.2.45	P10	L 63	# 8
CHAPLIN, C	LINT 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"

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Comment ID # 8

Page 15 of 89 09/27/2007 06:28

Submission

C/ 07	SC 7.3.2.45	P11	L <b>4</b>	#	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

C/ 07 SC 7.3.2.45 P11 L4 # 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 ACCEPT		Response Status U			
C/ <b>07</b> Sood, Kar	SC <b>7.3.2.46</b>	P11	L <b>64</b>	# 154	j
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).

 TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general

 COMMENT STATUS: D/dispatched A/accepted R/rejected
 RESPONSE STATUS: O/open W/written C/closed
 U/unsatisfied Z/withdrawn

 SORT ORDER: Comment ID
 Comment ID
 154

Page 16 of 89 09/27/2007 06:28

Submission

C/ 07 Sood, Kapi	SC 7.3.2.46	P11	L 64	# 328	C/ <b>07</b> Sood, Kar	SC 7.3.2.46	P12	L <b>50</b>	# 153
Comment It is no Inform include	<i>Type</i> <b>TR</b> t clear where the ation element co ed in the FTIE. (T	Comment Status <b>R</b> e number of optional paramet unt should also include the c This is a revision of similar co	ters is accounted count of all option omment)	for, in the FTIE. The al parameters that are	Comment TGw GTK updat	<i>Type</i> <b>T</b> D2.1 is using an l sub-element form ed to account for	Comment Status A IGTK with a keyid of 2 octets. hat are inadequate to handle 1 2 octets for Fig 7-95u and 7-	This seems to i IGw defined IGT 95v.	mply that the fields in the Ƙ. This needs to be
Suggested Chang field co include	Remedy the Clause 7.3.2.4 contains the total r ad in the MIC cal	6, pg 11 line 64 "The Informa number of information eleme culation."	ation Element Co nts and optional	ount of the MIC Control parameters that are	Suggeste Chan to be Response	<i>dRemedy</i> ge Clause 7.3.2.4 2 octets, as well.	i6, pg 12-13, Figs 7-95u with Response Status C	Key Info length	to be 2 and in Fig 7-95v
Response REJEC Option in the I its opti	CT. al parameters ar MIC Control field onal parameters	Response Status <b>U</b> e included in the length of th is a count of information ele as a single IE).	e FTIE. The Info ments (which co	ormation element count unts the FTIE with all of	ACCE C/ 07 Edney, Jo Comment	SC 7.3.2.46	P13	L16	# 291
Cl <b>07</b> Edney, Jor	SC 7.3.2.46 nathan	P12	L14	# 290	There	e is inconsistent n to a "Key RSC" t	aming. Fig 7-95u shows a "R field. What field is this?	SC" and "Key" fi	eld but the text here
Comment Figure	<i>Type</i> <b>T</b> 7-95t suggest th	Comment Status A at only one optional parame	ter is allowed. Ins	serting the field show	Suggester Clarif	<i>dRemedy</i> y naming in this p	paragraph		
Suggested The fie	Figure 7-95r do <i>Remedy</i> eld show be show	es not allow for mulotiple op n as optionally repeating or	tional parameters	s ear from the text	Response ACCE Chan	e EPT. ged "The Key RS	Response Status <b>C</b>		
Response ACCEI Chang line 9 t	PT. e "Optional para o "The format of	Response Status <b>C</b> meters" in Figure 7-95r to "O an optional parameter is sho	ptional paramete wn in Figure 7-9	er(s)". Changed page 12 5t."	CI <b>07</b> HEUBAUI Comment The w Suggeste Chan	SC 7.3.2.46 M, KARL F Type E vord "it" is missing dRemedy ge to "for CCMI	P13 Comment Status A g in "for CCMP is the Packe P it is the Packet Number (PN	L 22 et Number (PN)	# [ <u>127</u> ].
					Response ACCE	, EPT.	Response Status C		

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Page 17 of 89 09/27/2007 06:28

CI <b>07</b> CHAPLIN,	SC <b>7.3.2.47</b> CLINT F	P13	L <b>36</b>	# 9	<i>Cl</i> <b>07</b> Sood, Kap	SC <b>7.3.2.48</b> pil	P14	<b>1</b>	L 38	# 156
Comment The de (Origin Suggested	Type TR escription of TI IE nally LB98/175 sul IRemedy	Comment Status <b>A</b> is not clear:'specifies various bmitted by Zaks, Artur, during	types of time in LB98 with ID Z	tervals and timeouts" aks/10)	Comment Typo ' Suggested	<i>Type</i> <b>ER</b> "to uniquely ider <i>dRemedy</i>	Comment Status	A		
Define	the purpose of th	nis IE in a concise manner.			Response		Response Status			
Response ACCE	PT.	Response Status U			ACCE	PT.	nesponse otatas	0		
Chang	sc 7224	me intervals and timeouts."	1.20	# 000	 <i>CI</i> <b>07</b> Sood, Kap	SC <b>7.3.2.48</b> bil	P14	<b>1</b>	L 38	# 157
Malinen, Jo	ouni	F 14	L 30	# 283	Comment	Type <b>TR</b>	Comment Status	R		
Comment Typo	Туре Е	Comment Status A			The so being same	cope of the uniq that the same n AP.	ue RDIE Identifier shou umber (say, RDIE Id =:	uld be larger th 2) may be use	han the current F ed in different res	RIC. The reason source requests to
Suggested	lRemedy				Suggested	dRemedy				
Replac	ce "to uniquely ide	entifies" with "to uniquely iden	tify".		Chang	ge "to uniquely i	dentify the RDIE within	the RIC" to "to	o uniquely identi	ify the RDIE for all
Response ACCE	PT.	Response Status C			Response		Response Status	U		
CI 07 Edney, Jor	SC 7.3.2.48	P14	L 38	# 292	REJE Proce outsta	CT. dures in 11A.11 Inding at an AP,	state that a non-AP ST so there is no confusio	TA can only ha	ave a single RIC	-Request
Comment Typo:	<i>Type</i> <b>E</b> "identities" should	Comment Status <b>A</b> be "identify"			<i>Cl</i> <b>07</b> Sood, Kap	SC <b>7.3.2.48</b> bil	P14	<b>1</b>	L 38	# 330
Suggested Correc	<i>IRemedy</i> ct typo				Comment The so being	<i>Type</i> <b>TR</b> cope of the uniq that the same n	Comment Status ue RDIE Identifier shou umber (say, RDIE Id =:	R uld be larger th 2) may be use	han the current f	RIC. The reason
Response		Response Status C			same	AP.(This is revis	sion of similar commen	it)		
ACCE	PI.				Suggested	dRemedy				
					Chang resour	ge "to uniquely in rce requests iss	dentify the RDIE within ued by the STA to a sp	the RIC" to "to ecific AP".	o uniquely identi	ify the RDIE for all
					Response		Response Status	U		
					REJE Proce outsta	CT. dures in 11A.11 Inding at an AP,	state that a non-AP ST so there is no confusio	TA can only ha	ave a single RIC	-Request

Cl 07 Sood, Kapil	SC 7.3.2.48	P <b>14</b>	L <b>43</b>	# 158		<i>CI</i> <b>07</b> Sood, Kap	SC	7.4.7	P14	L	.64	# 159
Comment T	ype E	Comment Status R				Comment	Туре	TR	Comment Status	Α		
"Resou even 10	rce Descriptor" s )th!), and gives a	sounds too ominous for son an impression of yet anothe	neone reading this r complex protoco	s for the first time (c ol structure.	or,	lt is no STA a	ot certai ind AP i	n that the	e action frames will not ly. I do not see what va	impact the op	eration of the ctive stateme	link between the nt is adding to the
Suggested	Remedy					protoc	ol defin	ition.				
Renam	e "Resource De	scriptor" to "Resource"throu	ghout the draft			Suggested	dRemed	dy				
Response		Response Status C				Chang	ge: "The	FT actic	on frames are sent over	r the air betwe	en the STA a	nd the current AP."
REJEC	т.	·				Response			Response Status	U		
"Resou	rce descriptor" is	s a much more accurate ter	m for the field tha	n "Resource"		ACCE	PT.					
C/ 07	SC 7.3.2.48	P14	L <b>43</b>	# 331		C/ 07	SC	7.4.7	P14	L	. 65	# 10
Sood, Kapil						CHAPLIN,	CLINT	F				
Comment T	ype E	Comment Status R				Comment	Туре	т	Comment Status	Α		
"Resou even 10 revision	rce Descriptor" s Oth!), and gives a o of similar comm	sounds too ominous for son an impression of yet anothe nent)	neone reading this r complex protoco	s for the first time (c ol structure. (This is	or,	"&do r (the la (Origir	not affeo ist "in ar nally LB	ct the ope ny way" i 98/196 s	eration of the link betwe s not needed). ubmitted by Cam-Wing	een the STA a jet, Nancy, du	nd the currer ring LB98 wit	t AP in any way." h ID Cam-Winget/11)
Suggested	Remedy					Sugaested	dRemed	lv		•	-	<b>.</b> ,
Renam	e "Resource De	scriptor" to "Resource"throu	ghout the draft			Remo	ved "in	any way"	from this sentence.			
Response		Response Status C				Response			Response Status	с		
REJEC "Resou	T. rce descriptor" is	s a much more accurate ter	m for the field tha	n "Resource"		ACCE	PT.			-		
C/ 07	SC 7.4.7	P14	L 64	# 332		<i>ci</i> <b>07</b> Chaplin,	SC CLINT	<b>7.4.7</b> F	P14	L	. 65	# 11
Sood, Kapli						Comment	Tvpe	т	Comment Status	Δ		
Comment T	ype TR	Comment Status A				Strictly	v speak	ing, FT a	ction frames can affect	the operation	of the link b	etween the STA and
It is not STA an what va	certain that the d AP in any way alue this subiecti	action frames will not impace In fact, they certainly will i ve statement is adding to th	ct the operation of mpact channel co le protocol definit	f the link between the hold between the	ne ee	the cu PwrMe	rrent Al gt flag ir	P, so it is n the fran	not correct to claim the ne control field in the a	em not to affect ction frames c	ct this "in any ould be used	way". For example, to move the STA
Sugaested	, Remedv	Ū	·			param	en pow	t the curr	ent AP, but "operation	of the link" so	unds more ge	eneral than that.
Change	e: "The FT action	n frames are sent over the a	ir between the S	A and the current	AP."	(Origir	nally LB	98/197 s	ubmitted by Malinen, J	ouni, during L	B98 with ID N	lalinen/12)
Response		Response Status II				Suggested	dRemec	dy				
ACCEP	ΥТ.					Repla way" v	ce "do r vith "do	not affect not affec	the operation of the lin at the FT association st	k between the ate between the	e STA and the ne current AF	e current AP in any and the STA".
						Response			Response Status	с		
						ACCE Chang	PT IN F	PRINCIPI do not aff	_E. fect the state of the link	between the	STA and the	current AP."
			,									
ITPE: IR/te	ecnnical require	u ER/editorial required GR	/general required	i/technical E/edit	unai G/g	eneral						Dage 10 of 90

COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Page 19 of 89 09/27/2007 06:28

Submission

Bill Marshall, ATT Labs Research

C/ 07 SC 7.4.7.1 P15 L42 # 128 HEUBAUM, KARL F	C/ 08 SC 8.4.1.1 CHAPLIN, CLINT F	P18	L 58	# 12
Comment Type E Comment Status A "Frames" in "for Fast BSS Transition Action Frames." should be lower case	Comment Type E Co There is a "." after Handshake (Originally LB98/212 submitte	omment Status <b>A</b> e" ed by Sood, Kapil, dur	ing LB98 with ID :	Sood/020)
SuggestedRemedy Change to "for Fast BSS Transition Action frames."	SuggestedRemedy	· · <b>,</b> · · · · <b>,</b> · · · ·	<b>J</b>	
Response Response Status C ACCEPT.	Response Res	sponse Status C		
C/ 08 SC 8.4.1.1 P18 L 52 # 114 CHAPLIN, CLINT F	C/ 08 SC 8.4.1.1.1a	P19	L17	# 334
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)	Comment Type TR Co "This can include parameters authorized SSID is not correc is a "STA's Authorized SSID" similar comment) SuggestedRemedy	omment Status <b>A</b> such as the STA's au t, as SSID shall alway ? Indicate some other	thorized SSID" - s be part of the F example, if need	The example of STA's PMK-R0 SA. BTW, what ed. (This is revision of
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 guided phrase errors up</something></something>	Delete "This can include para first component of the PMK-R Response Res ACCEPT.	imeters such as STA's 20 SA. sponse Status U	s authorized SSIE	" and add "- SSID" as
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 8.4.1.1.1a Sood, Kapil Comment Type TR Co "This can include parameters authorized SSID is not correc is a "STA's Authorized SSID" SuggestedRemedy Delete "This can include para first component of the PMK-R Response Res ACCEPT.	P19 omment Status A such as the STA's au t, as SSID shall alway ? Indicate some other meters such as STA's to SA. sponse Status U	L 17 athorized SSID" - vs be part of the F example, if need s authorized SSID	# 161 The example of STA's PMK-R0 SA. BTW, what ed. " and add "- SSID" as

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID Comment ID 101

Page 20 of 89 09/27/2007 06:28

C/ 08 Sood, Kap	SC 8.4.1.1.1a	P19	L <b>43</b>	# 335	<i>Cl</i> <b>08</b> Sood, Kap	SC 8.4.1.1.1	a P	19 L	.7 #	333
Comment This c author is a "S similar	<i>Type</i> <b>TR</b> an include parame rized SSID is not c STA's Authorized S r comment)	Comment Status A eters such as the STA's auth orrect, as SSID shall always SID"? Indicate some other	norized SSID - Th s be part of the P example, if need	ne example of STA's MK-R1 SA. BTW, what ed. (This is revision of	Comment SSID (This i Suggested Add "-	Type <b>TR</b> is missing from F s revision of sim dRemedy SSID" as the fir	Comment Status PMK-R0 SA, but is (c ilar comment)	SA orrectly) include	⊧d in the PMK-R0 k	ey derivation
Suggested	dRemedy				Response		Posponso Status			
Delete first co	e "This can include omponent of the Pl	parameters such as STA's MK-R1 SA.	authorized SSID	" and add "- SSID" as	ACCE	PT.	Response Status	0		
Response ACCE	PT.	Response Status U			<i>CI</i> <b>08</b> Chaplin,	SC 8.4.1.1.2 CLINT F	P	19 L	. 56 #	13
Cl 08 Sood, Kap Comment This ci author is a "S	SC 8.4.1.1.1a bil <i>Type</i> TR an include parame rized SSID is not o STA's Authorized S	P19 Comment Status A eters such as the STA's auth orrect, as SSID shall always SID"? Indicate some other	L 43 horized SSID - Th s be part of the P example, if need	# 162 ne example of STA's MK-R1 SA. BTW, what ed.	Comment "There Suppli define ambig (Origin Suggested	Type <b>TR</b> e shall be only or icant and Auther d additional com uous for FT key hally LB98/219 s dRemedy	Comment Status ne PTKSA with the s tricator MAC address ponents to be part o hierarchy design. ubmitted by Sood, K	s <b>A</b> ame ses." is not true f f the Auth and S apil, during LB98	ior FT. This is beca Suppl, and this state 8 with ID Sood/022	ause we have ement become ?)
Suggested Delete	dRemedy = "This can include propert of the Plane	parameters such as STA's	authorized SSID	" and add "- SSID" as	Chang shall b	ge sentence to "F be only one PTK	For the PTKSA derive SA with the same Su	ed as a result of pplicant and Au	the 4-Way Handsh thenticator MAC ad	hake, there ddresses."
Response ACCE	PT.	Response Status U			Response ACCE After r Mobili	PT IN PRINCIPL equested senter ty Domain Assoc	Response Status E. Ice, also inserted "Fo iation or Fast BSS T	or the PTKSA de ransition, there	erived as a result o shall be only one F	f an Initial PTKSA with the
C/ 08	SC 8.4.1.1.1a	P <b>19</b>	L <b>7</b>	# 160	same	non-AP STA MA	C address and BSS	ID."		
Comment SSID i Suggested Add "-	Type <b>TR</b> is missing from PN <i>dRemedy</i> SSID" as the first	Comment Status A IK-R0 SA, but is (correctly) component of the PMK-R0	included in the P SA list	MK-R0 key derivation	C/ <b>08</b> CHAPLIN, <i>Comment</i> The P (Origin	SC 8.4.1.1.2 CLINT F <i>Type</i> <b>TR</b> TKName is miss nally LB98/221 s	Comment Status ing from the PTKSA ubmitted by Cam-Wi	20 <i>L</i> s <b>A</b> nget, Nancy, du	.3 #	14 Cam-Winget/16)
Response ACCE	PT.	Response Status U			Suggested Includ	dRemedy e PTKName in tl	ne PTKSA list.			
					Response ACCE Inserte	PT. ed bullet item "If	Response Status	<b>U</b> key hierarchy is	; used, PTKName"	

 TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general
 Page 21 of 89

 COMMENT STATUS: D/dispatched A/accepted R/rejected
 RESPONSE STATUS: O/open W/written C/closed
 U/unsatisfied Z/withdrawn
 Page 21 of 89

 SORT ORDER: Comment ID
 09/27/2007 06:28

Submission

CI 08 Chaplin	SC <b>8.4.1.1.2</b> CLINT F	P <b>20</b>	L <b>3</b>	# 15		<i>CI</i> <b>08</b> Chaplin,	SC <b>8.4.3</b> CLINT F	ŀ	<sup>⊃</sup> 20	L12	# 116
Comment PTKS a nam not re (Origin	<i>Type</i> <b>T</b> A does not include the for the key. Sho ally used for anyth hally LB98/222 sub	Comment Status A e PTKName even though uldn't PTKName be adde ing in the current draft, so pomitted by Malinen, Journ	both PMK-R0 and d into PTKSA? Th o it could be remov , during LB98 with	PMK-R1 SAs do ir en again, PTKNam ed completely. ID Malinen/14)	nclude ne is	Comment In D5. FT wit appros (Origin	<i>Type</i> <b>T</b> 0, 8.4.3 include h TKIP. As TKII ach. Change the nally LB105/8 su	Comment State d text that required of P has passed its des e text to specifically ubmitted by Stanley,	us <b>R</b> use of CCM sign goal, m prokibit use Dorothy, de	P with FT, spenoving past TKI oving past TKI of TKIP as the uring LB105 wi	<i>TKIP</i> cifically prohibiting use of P seems to be the right pairwise cipher. th ID Stanley/09)
Suggester Either the P <sup>-</sup> Response ACCE Insert	dRemedy remove PTKNam rKSA by inserting PT. ed bullet item "If F	e completely (per my con a new item after PTK: "P <i>Response Status</i> <b>C</b> ast BSS Transition key hi	nment on 8.5.1.5.5 TKName". erarchy is used, P	) or add PTKName TKName''	to	Suggested Re-ins Repla the pa suite, cipher the as	Remedy sert the text from ce "STA shall us irwise cipher su and reject the a suite is selecte sociation with s	n 8.4.3 D5.0, and ap se CCMP as the pai uite" and replace (on issociation with statu id' with 'does not sel tatus code 42 ("Inva	pply the char irwise ciphe line 50) 'als us code 42 ( ect TKIP as lid pairwise	nges suggeste r suite" with "S so selects CCM ("Invalid pairwis s the pairwise c cipher") if TKII	d by Comment 233: TA shall not use TKIP as IP as the pairwise cipher se cipher") if any other ipher suite, and reject P is selected'.
C/ 08 CHAPLIN Comment Remo pairwi cipheu the cu and w quest this co langu (Origin Suggester Add fo "The u was d deploy	SC 8.4.3 CLINT F Type T val of 8.4.3 and re se cipher for FT us rs to be used, the p urrent state of TKIF re are at the end of onable. While it m build be done even age in 802.11 to di nally LB105/7 subi dRemedy blowing paragraph use of TKIP as a p esigned as a temp yments."	P20 Comment Status R lated changed in D6.0 br se. While the other change part of allowing TKIP as a p. TKIP was designed as f its designed lifetime. As ay still be desirable for so if the 802.11 standard w iscourage the use of TKIF mitted by Malinen, Jouni, to the end of 6.1.2 (just airwise cipher when using borary solution with a limit	L 12 bught back TKIP a les were necessary fully supported cip a temporary solution such, its use in an ome deployments the ere to deprecate T would be a good during LB105 with after the paragraph g Fast BSS Transit ed lifetime and it is	# 115 s a fully supported y to allow vendor sp oher does not fit we on with a limited life y new amendment o be able to use Th (IPs use. Having s thing to do now. ID Malinen/11) that deprecates W ion is deprecated.	TKIP pecific ell with etime is KIP, some VEP): TKIP	Response REJE There Transi	CT are existing de tion.	Response Statu	is C	AES but would	benefit from Fast BSS
Response REJE There Trans	CT are existing deplo ition.	Response Status C	ort AES but would	benefit from Fast B	355						

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Comment ID # 116

Page 22 of 89 09/27/2007 06:28

CI 08 CHAPLIN,	SC <b>8.5.1.1</b> CLINT F	P <b>2</b>	20	L <b>50</b>	# 16	C/ ( Hou	<b>8</b> S sley, Russe	C <b>8.5.1.5.1</b> ell D		P <b>21</b>	L 58	# 285	
Comment Comm (Origin Suggested (a) In 4 "Wher the AF are as PRF-1 PRF-2 PRF-3 PRF-5 Other (b) In 4 "Wher the AF PMKII Here, Other (c) In 4 "Wher peer S SMKII Here, Other	Type TR nent: Changes hally LB98/243 <i>(Remedy</i> ) 3.5.1.1, insert to the RSNA Ca P and the non- defined below 28(K, A, B) = 92(K, A, B) = 92(K, A, B) = 92(K, A, B) = 92(K, A, B) = 12(K,	Comment Status to remove use of SHA- submitted by Stanley, I the following text prior t spabilities field B6 is set AP STA, or between pe (where KDF is as defin KDF-128(K, A, B, 128) KDF-192(K, A, B, 129) KDF-256(K, A, B, 256) KDF-384(K, A, B, 384) KDF-512(K, A, B, 512) tions are as defined be the following text prior t spabilities field B6 is set AP STA, a PMK identifi A256-128(PMK, "PMK 6-128 is the first 128 bi dentifier is defined as A256-128(SMK, "SMK 6-128 is the first 128 bi dentifier is&	R 1 are incom Dorothy, dur o the senter t to 1 in the l er STAS (for hed in 8.5.1. clow." In the o the senter t to 1 in the l er is defined Name"    AA its of the HM o the senter t to 1 in the l	plete ing LB98 w nce beginnir RSNA inforr r PeerKey d 5.2: following&. ce beginnir RSNA inforr I as .   SPA) IAC-SHA25 nce beginnir RSNA inforr IAC-SHA25	SHA-1 vs SHA-2 ith ID Stanley/09) ng "In the following" mation element of both lerivations) PRF function ng "A PMK identifier is&" mation element of both 6 of its argument list. ng "A PMK identifier is&" mation element of both C_P    INonce    MAC_I) 6 of its argument list.	56 Con ns ' Res	ment Type The docum Jpon a suc PMK-R0 S created be came Mobi This is ven PMK-R0 S he supplic These work Part of the refering to gestedRen Rewite the bonse ACCEPT Text chang R0 SA for f R1 SAs de	E E enent says: ccessful aut A and all PN tween the S ility Domain y confusing A and any S ant that was ds do not pr confusion c the same en nedy few senten ged to "Uppor this Mobility rived from th	Comme nentication, /IK-R1 SAs i 0KH and S1 to me. I thinl (As that were just authen owide this m omes from S titly in this s ces. Respons a successf Domain for nat prior PM	nt Status <b>A</b> the R0KH shall of its possession KH and any oth the goal is to control e derived from it ticated for this Meaning to me. STA, Supplicant ection. <b>B</b> <b>C</b> and authentication the supplicant the K-R0 SA."	delete the prior a which were prev er R0KH and R1H lelete the prior that are related t Aobility Domain. , S0KH, and S1KH	iously KH in the o H all delete any prio enticated, and a	Editor or PMK- all PMK-
response		Response Status	U										

### Response

REJECT

Submission

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

Page 23 of 89 09/27/2007 06:28

CipherSuites

C/ 08	SC 8.5.1.5.1	P 22	L13	#	166
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.

#### 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.

C/ 08	SC 8.5.1.5.1	P <b>22</b>	L13	#	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.

Comment ID # 338

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Page 24 of 89 09/27/2007 06:28

Bill Marshall, ATT Labs Research

Submission

C/ 08	SC 8.5.1.5	.1 P22	L <b>14</b>	# 117
CHAPLIN, C	LINT F			
Comment Ty	pe 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 REJECT From a system poi layer three protoco changes. Assumed	Response Status U nt of view, key distribution shou I would be out of scope for IEEE d requirements for the key distrib	ld be done by a la E 802.11r; the PAF pution are given in	yer three protocol. Any R only authorizes MAC 11A.2.2.	PMKR0Name altogether in 8 128(SHA-256 23, line 57), a to derive the P
C/ 08 SC 8.5.1	.5.2 P 22	L <b>31</b>	# 17	Response
CHAPLIN, CLINT F				REJECT
Comment Type E	Comment Status A			Government r
Suggested wording	) 77 aukasittad ku Malinan Jauni	durin a I DOQ with I	ID Maliana (40)	and ban all us
(Originally LB98/2)	7 submitted by Malinen, Jouni,	during LB98 with	ID Malinen/19)	CI 08 SC :
SuggestedRemedy	out with "OFC bit kout"			CHAPLIN, CLINT
				Comment Type
ACCEPT.	Response Status C			Adding extra ( any real value adding extra c (Originally LB
				SuggestedRemed
				Remove "0x0

CI 08	SC 8.5.1.5.2	P <b>22</b>	L <b>42</b>	# 302
Malinen, J	ouni			

Comment Status R

Comment Type TR

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 algorithms, 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 Status U erned about the political problem of SHA-1 vs SHA-256; that the US may overreact to the problems identified in SHA-1 (for its use in certificates) ses of SHA-1. 8.5.1.5.2 P 22 L42 # 18 F TR Comment Status A 0x00 after 'label' into KDF() data for HMAC-SHA256() does not seem to add e. It is not needed here since 'i' and 'label' are of fixed length. As such, it is just complexity and making KDF slower. 98/278 submitted by Malinen, Jouni, during LB98 with ID Malinen/20) ly 0 ||" from HMAC-SHA256() parameters. Response Response Status U

ACCEPT.

 TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general
 Page 25 of 89

 COMMENT STATUS: D/dispatched A/accepted R/rejected
 RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn
 Comment ID
 Page 25 of 89

 SORT ORDER: Comment ID
 09/27/2007 06:28

Submission

Cl <b>08</b> Malinen, Jo	SC <b>8.5.1.5.2</b> puni	P <b>22</b>	L <b>42</b>	# 301	<i>CI</i> <b>08</b> CHAPLIN,	SC <b>8.5.1.5.3</b> CLINT F		P <b>22</b>	L 58	# 20
Comment T 0x00 at more c benefit	Type <b>TR</b> fter label in the HM omplex to implem Remedy	Comment Status A MAC-SHA256 data serves no p ent and uses more CPU to run	urpose in KDF. derive the keys	It just makes this without any added	Comment Use o shorte opera (Origin	<i>Type</i> <b>TR</b> f a long label "R0 r label would me tion which is alrea nally LB98/283 su	Comment S Key Derivation et that requirem ady quite CPU o ubmitted by Mal	Status <b>A</b> " is not neede nent. Long strir expensive. inen, Jouni, du	d to keep key d ng here is just a uring LB98 with	erivations unique; dding extra cost to KDF ID Malinen/22)
Delete	"0x00    " from HN	AC-SHA256 data in the KDF.			Suggested	Remedy				
Response ACCEF	рТ	Response Status U			Repla replac 0x523 replac	ce "R0 Key Deriv e '"R0 Key Deriv 0'. On page 24 lii e '"R0 Key Name	ation" with "R0" ation" is 0x5230 ne 25, replace " e" is 0x5230204	' in R0-Key-Da 204B6579204 R0 Key Name b6579204e61	ata derivation. C 465726976617 " with "R0N". O 6d65' with "R0I	Dn page 24 line 7, '4696F6E' with "'R0" is n page 24 line 30, N" is 0x52304E'.
Cl <b>08</b> Stanley, Do	SC <b>8.5.1.5.2</b> prothy V	P <b>22</b>	L <b>42</b>	# 130	Response ACCE	PT IN PRINCIPL	Response S E.	tatus U		
Comment T Use of	Type <b>TR</b> SHA256 introduce	Comment Status <b>R</b> es a computational burden on t	he STA which is	SHA-1 vs SHA-256 not warranted	Chang <i>Cl</i> 08	ged to "FT-R0" (0 SC 8.5.1.5.3	x46542d5230)	in calculation of P22	of PMK-R0 and L <b>58</b>	PMKR0Name. # 21
Suggested	Remedy				CHAPLIN,	CLINT F				
Change	e to use HMAC-SI	HA-1, as in IEEE 802.11-2007.			Comment	Туре Т	Comment S	Status A		
Response REJEC We are Govern	CT concerned about iment may overrea	Response Status <b>U</b> the political problem of SHA-1 act to the problems identified in	vs SHA-256; th SHA-1 (for its u	at the US ise in certificates)	During meetir see ar (Origir	g the evaluation on ng, it was clear th ny loss of cryptog nally LB98/284 su	of s-PRF versus at we can redu raphic security ubmitted by Soc	v-PRF and Al ce a SHA oper in doing so. od, Kapil, durin	ES versus SHA ration if we sho ng LB98 with ID	256 KDFs in last rten the label. I do not Sood/025)
and ba	IT all uses of SHA-	·I.			Suggested	Remedy			( ) ) Do	
CI <b>08</b>	SC 8.5.1.5.2	P 22	L <b>47</b>	# 19	Chang	ge "R0 Key Deriv	ation" to "RU Ke	ey" in formulae	for deriving RU	-Key-Data.
CHAPLIN, Comment 7 Sugges (Origina	CLINT F <i>Type</i> <b>E</b> sted wording ally LB98/279 sub	Comment Status <b>A</b>	a LB98 with ID I	Malinen/21)	Response ACCE Chanç	PT IN PRINCIPL ged to "FT-R0" (0	Response S E. x46542d5230)	tatus <b>C</b>	of PMK-R0 and	PMKR0Name.
Suggested	Remedy	· · · · ·	0	,						
Replac	e "16 bit unsigned	l integers" with "16-bit unsigne	d integers".							
Response ACCEF	РТ.	Response Status C								

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID Comment ID Comment ID

Page 26 of 89 09/27/2007 06:28

Submission

C/ 08 Edney, Jor	SC 8.5.1.5.3 nathan	P <b>22</b>	L <b>7</b>	# 293	<i>ci</i> <b>08</b> Chaplin	SC <b>8.5.1.</b> , CLINT F	5.4	P 23	L <b>39</b>	# 24
Comment	Type <b>TR</b>	Comment Status R			Comment	Type E	Con	nment Status A		
The us as is n	se of this long inte ormal for 802.11.	ger is confusing or, worse, This long number format ap	vrong if encodeo pears here and	d using little endianism in the following two	Sugge (Origi	ested wording nally LB98/29	6 submitted	by Malinen, Jouni, c	during LB98 with	ID Malinen/24)
clause	s S				Suggeste	dRemedy				
Suggester	Remedy	tten) electristic en electrice ef			Repla	ice "256 bit ke	y" with "256	S-bit key".		
Clarity	endianism or (be	tter) show this as a string of	octets		Response	)	Resp	onse Status <b>C</b>		
Response	~	Response Status U			ACCE	PT.				
REJE This is minimi	not a long intege ze confusion abo	r. It is shown as a string of out string termination.	octets, twice, in t	wo different formats to	<i>CI</i> <b>08</b> Chaplin	SC <b>8.5.1.</b> , CLINT F	5.4	P <b>23</b>	L <b>42</b>	# 25
C/ 08	SC 8.5.1.5.3	P 23	L <b>7</b>	# 22	Comment	Type TR	Con	ment Status A		
CHAPLIN,	CLINT F				Use o	f a long label	"R1 Key De	rivation" is not need	ed to keep key de	erivations unique;
Comment Reduc	<i>Type</i> <b>T</b> e label length of " ally I B98/289 sul	Comment Status A R0 Key Derivation" bmitted by Sood, Kapil, duri	ng I B98 with ID	Sood/026)	shorte opera (Origi	er label would tion which is a nally LB98/29	meet that re already quite 8 submitted	equirement. Long str e CPU expensive. by Malinen, Jouni, c	ing here is just ad	dding extra cost to KDF ID Malinen/25)
Suggester	IRemedy		.g	00000,020)	Suggeste	dRemedy				
Chanc	ie as follows: "- "F	0 Kev" is 0x5230204B6579	n		Repla	ce "R1 Key D	erivation" w	ith "R1" in PMK-R1 (	derivation. On line	e 49, replace "R1 Key
Response		Response Status <b>C</b>			56, re 0x523	place "R1 Key 31204b657920	/ Name" wit /4e616d65'	h "R1N". On line 61, with '"R1N" is 0x523	replace "R1 Key 14E'.	v Name" is
Chanc	PT IN PRINCIPLE led to "FT-R0" (0x	=. (46542d5230) in calculation	of PMK-R0 and	PMKR0Name.	Response	)	Resp	onse Status U		
					ACCE	PT IN PRINC	IPLE.			
C/ 08	SC 8.5.1.5.3	P 23	L <b>9</b>	# 23	Chan	ged to "FT-R1	" (0x465420	d5231) in calculation	of PMK-R1 and	PMKR1Name.
CHAPLIN, Comment	CLINTF Type E	Comment Status A			CI <b>08</b> Chaplin	SC <b>8.5.1.</b> , CLINT F	5.4	P <b>23</b>	L <b>42</b>	# 26
Sugge (Origin	sted wording ally I B98/290 sul	bmitted by Malinen Jouni d	urina I B98 with	ID Malinen/23)	Comment	Туре Т	Con	nment Status A		
Suggester	IRemedy		ag _200 mm		During	g the evaluation	on of s-PRF	versus v-PRF and A	AES versus SHA2	256 KDFs in last
Replac	ce "Beacons and	Probe Responses" with "Be	acon and Probe	Response frames".	meeti	ng, it was clea	r that we ca	an reduce a SHA ope	eration if we shor	ten the label. I do not
Resnonse		Response Status C			(Origi	nally LB98/29	9 submitted	by Sood, Kapil, duri	ng LB98 with ID	Sood/027)
	PT	Response Status C			Sugaeste	dRemedv			0	,
AUOL					Chan	ae "R1 Kev D	erivation" to	"R1 Kev" in formula	e for derivina PM	K-R1.
					Response	9	Resp	onse Status <b>C</b>	0	
					ACCE	EPT IN PRINC	IPLE. " (0x465420	d5231) in calculation	of PMK-R1 and	PMKR1Name.

C/ 08 CHAPLIN,	SC 8.5.1.5.4 CLINT F	P 23	L <b>50</b>	# 27	<i>CI</i> <b>08</b> Chaplin, C	SC <b>8.5.1.5.5</b> LINT F	P <b>24</b>	L10	# 28
Comment Reduc (Origin Suggested Chang	<i>Type</i> <b>T</b> nally LB98/300 sub <i>Remedy</i> ne as follows: "- "R	Comment Status A R1 Key Derivation" pritted by Sood, Kapil, during 11 Key" is 0x5231204B6579"	JLB98 with ID	Sood/028)	Comment Ty Use of a shorter I operatio (Origina SuggestedB	ope TR long label "PT abel would mee n which is alrea lly LB98/310 su emedy	Comment Status <b>A</b> K Key derivation" is not need at that requirement. Long strin dy quite CPU expensive. bmitted by Malinen, Jouni, du	ed to keep key d ng here is just ad uring LB98 with I	lerivations unique; Iding extra cost to KDF D Malinen/26)
Response ACCE Chang	PT IN PRINCIPLE jed to "FT-R1" (0x	Response Status <b>C</b> 46542d5231) in calculation o	f PMK-R1 and	PMKR1Name.	Replace derivatio <i>Response</i>	"PTK Key deri n" is 0x50544B	vation" with "PTK" in PTK der 204B6579206465726976617 Response Status <b>U</b>	rivation. On line 74696F6E' with "	18, replace '"PTK Key 'PTK" is 0x50544B'.
<i>Cl</i> <b>08</b> Sood, Kap	SC 8.5.1.5.4	P23	L <b>52</b>	# 163	ACCEP Change	T IN PRINCIPL d to "FT-PTK" (	E. 0x46542d50544b) in calculat	ion of PTK and I	PTKName.
Comment All AP	<i>Type</i> <b>TR</b> s have an R1KH,	Comment Status <b>A</b> including the first AP with whi	ch the STA per	formed Initial Auth. So,	<i>Cl</i> <b>08</b> Housley, Ru	SC <b>8.5.1.5.5</b> ssell D	P <b>24</b>	L 10	# 284
Suggested Chang the AF the Ini Response ACCE First a	IRemedy je: "R1KH-ID is a " OR "R1KH-ID is tial or target AP" PT. Iternative taken.	MAC address of the holder of a MAC address of the holde <i>Response Status</i> <b>U</b>	the PMK-R1 ir r of the PMK-R	the Authenticator of 1 in the Authenticator of	The doc the P' PTK = K The doc KCK = L KEK = L TK = L(F If the PT flexibility	ument says: TK derivation is IDF-PTKLen(Pf ument also say (PTK, 0, 128) (PTK, 128, 128) PTK, 256, 128) TK will always b of PTKLen car that this flavibil	as follows: MK-R1, "PTK Key derivation" s: ) e composed of three 128-bit n be removed from the specif ity is needed and that the der	, keys, then the fication. I	
CI <b>08</b> Sood, Kap Comment	SC <b>8.5.1.5.4</b> il <i>Type</i> <b>TR</b>	P 23 Comment Status A	L <b>52</b>	# 336	the KCK SuggestedR Change	, KEK, and TK emedy the text derivat	ion of the KCK. KEK. and TK	(need to reflect	
All AP "R1KH AP" is	s have an R1KH, I-ID is a MAC add not accurate. (Th	including the first AP with whi ress of the holder of the PMK is is revision of similar comme	ch the STA per -R1 in the Auth ent)	formed Initial Auth. So, enticator of the target	the poss Response ACCEP	sibility of more t	han one PTK key size. <i>Response Status</i> <b>U</b>		
Suggested Chang the AF the Ini	<i>IRemedy</i> je: "R1KH-ID is a '" OR "R1KH-ID is tial or target AP"	MAC address of the holder of a MAC address of the holde	the PMK-R1 ir r of the PMK-R	the Authenticator of 1 in the Authenticator of	At page value of	24 line 54 inse PTKLen) depe	rted "For vendor specific ciph nd on the vendor specific alg	er suites, the ler orithm."	ngth of TK (and the
Response ACCE First a	PT. Iternative taken.	Response Status U							

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Comment ID # 284

Page 28 of 89 09/27/2007 06:28

PTKLen

Submission

CI <b>08</b> CHAPLIN,	SC <b>8.5.1.5.5</b> CLINT F	P <b>24</b>	L 10	# 29	CI <b>08</b> Chaplin	SC <b>8.5.1.5.5</b> I, CLINT F	P <b>24</b>	L18	# 30
Comment <sup>7</sup> During meetin see an (Origin Suggested Chang	Type <b>T</b> the evaluation of g, it was clear tha y loss of cryptogra ally LB98/311 sub Remedy e "PTK Key deriva	Comment Status <b>A</b> s-PRF versus v-PRF and Af t we can reduce a SHA oper aphic security in doing so. imitted by Sood, Kapil, durin	ES versus SHA2 ation if we short g LB98 with ID S a for deriving PT	56 KDFs in last en the label. I do not Sood/029) TK	Commen Redu (Orig Suggeste Char Respons	<i>t Type</i> <b>T</b> ice length of "PTK inally LB98/313 su edRemedy nge " "PTK Key" i e	Comment Status A Key derivation" bmitted by Sood, Kapil, duri s x50544B204B6579." Response Status C	ing LB98 with ID	Sood/030)
Response	PT IN PRINCIPI F	Response Status C	Ū		ACC Char	EPT IN PRINCIPL nged to "FT-PTK" (	E. 0x46542d50544b) in calcula	ation of PTK and	PTKName.
Chang	ed to "FT-PTK" (0	x46542d50544b) in calculati	on of PTK and F	PTKName.	C/ <b>08</b> Sood, Ka	SC 8.5.1.5.5 pil	P <b>24</b>	L <b>24</b>	# 337
Cr us Chen, Lido Comment Accorc 802.11 allower 802.11 Otherw Suggested Response ACCEI At pag value o	<i>Type</i> <b>T</b> ling to the main do r, KCK and KEK a d, then TK is 128 l m. vise, PTKLen show <i>Remedy</i> PT. e 24 line 54 insert of PTKLen) depen	Comment Status A Document, 802.11m, PTKLen are both 128 bits. TK depend bits and the PTKLen must be uld be modified in 11r. Response Status C ed "For vendor specific ciphe d on the vendor specific algo	L 11 depends on the ls on cipher suit e 384 bits. It mus er suites, the ler prithm."	# 149 PTKLer cipher suite. In e. If only CCMP is st be consistent with hgth of TK (and the	Commen "The "The 8.5.2 certa comr Suggeste Char mess Respons ACC C/ 08 Sood, Ka	t Type TR KEK is used to pro "falsely implies the in fields within the nent) edRemedy nge: "The KEK is u sages, as defined i e EPT. SC 8.5.1.5.5 pil t Type TR	Comment Status A ovide data confidentiality in l at the EAPOL-Key message EAPOL-Key are confidentia sed to provide data confider n 8.5.2" Response Status U P24 Comment Status A	EAPOL-Key mess es have data conf lity protected. (Th ntiality for Key Da	sages, as defined in identiality. In fact, nis is revision of similar nta field in EAPOL-Key # 165
Cl 08 Sood, Kapi Comment Typo " Suggested Chang Response ACCEI	SC 8.5.1.5.5 I Type ER S1KHand" <i>Remedy</i> e: "S1KH and" PT.	P24 Comment Status A Response Status U	L 17	# 164	The 8.5.2 certa Suggeste Char EAPO Respons ACC	KEK is used to pro- "falsely implies the in fields within the edRemedy age: "The KEK is u DL-Key messages e EPT.	ovide data confidentiality in at the EAPOL-Key message EAPOL-Key are confidentia sed to provide data confider , as defined in 8.5.2" <i>Response Status</i> <b>U</b>	EAPOL-Key mesas have data conf lity protected. ntiality for certain	sages, as defined in identiality. In fact, fields (Key Data) in

CI 08	SC 8.5.1.5.5	P 24	L <b>59</b>	# 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
		<u> </u>

#### REJECT.

The current text does not require the calculation of PTKName.

C/ 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 P38 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.

C/ 10	SC 10.3.34.2.3	P 38	L <b>30</b>	# 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.

C/ 10	SC 10.3.34.4.4	P <b>40</b>	L12	# 33
CHAPLIN, C	LINT 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.

Page 30 of 89

09/27/2007 06:28

C/ 10 Sood, Kapi	SC <b>10.3.35</b>	P <b>41</b>	L <b>56</b>	# 340
Comment The M standa indepe comple	<i>Type</i> <b>TR</b> LME's defined in t and amendment hat andent entities - so ex functions. (This	Comment Status <b>A</b> this clause are confusing, an as not seen a single proof of b, all steps much be taken to s is revision of similar comme	d need further nter-operable ensure very lu nt)	<i>MLME diagram</i> clarification. This behavior between 2 ucid description of
Suggested Add a entities diagran essent my cor	Remedy MLME interface of s for Fast BSS Tra m has been drawi ial to make this s ntribution (11-07-2	liagram indicating which MLN ansition protocol (4-message n in multiple TGr adhoc meet pec more comprehensible an 2352-00-000r-FT-MLME-Figu	IE functions a flow) using ov ings, and addi d hence, easid re) to address	re invoked at which /er-the-DS. A similar ng one such diagram is er to inter-operate. Accept this comment.
Response ACCE Chang shown	PT IN PRINCIPLE es to 11A.5.3 as to 11A.10.	Response Status U E given in 11-07-2352-02-000r	ft-mlme-figure	.doc; not the changes
C/ 10 Sood, Kapi	SC 10.3.35	P <b>41</b>	L <b>56</b>	# 170
Comment The M standa indepe comple	Type <b>TR</b> LME's defined in t and amendment hat andent entities - so ex functions.	Comment Status <b>A</b> this clause are confusing, an as not seen a single proof of b, all steps much be taken to	d need further nter-operable ensure very lu	clarification. This behavior between 2 ucid description of

#### 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.

C/ 10	SC 10.3.35.1.2	P <b>42</b>	L17	# 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.

C/ 10	SC 10.3.35.1.2	P <b>42</b>	L <b>36</b>	# 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"?

### SuggestedRemedv

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

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

2 P 42	L <b>36</b>	# 339	C/ 10 Sood Kapi	SC 10.3.35.2.1	P <b>42</b>	L <b>44</b>	# 171
Commont Status			Commont I		mmont Statua		
the response is delivered to means that the MAC of nor prect? Is this response "MLI ment)	o the SME for proc n-AP STA sends a ME-REMOTE-REC	essing." - what does ι "response" to the QUEST.confirm"? (This	"This p Subtyp entire M differer	rimitive is used by the S e&" - only non-AP STA MLME clause for MLME nt messages. The text, a	SME to request the M can send this messa -Remote_Request is as written, is very con	IAC to send a Ma age. This must be s used on non-AP nfusing and shoul	nagement Frame of indicated clearly. The STA and on AP for Id be clarified.
			Suggestedi	Remedy			
. At the non-AP STA, the M e SME for processing." OR,	AC delivers the M delete this senter	LME-REMOTE- nce, as this is covered	Change and SM Frame	<ul> <li>"This primitive is used IE of AP (to send over- of Subtype&amp;"</li> </ul>	d by the SME of non- the-DS response) to	-AP STA (to send request the MAC	l over-the-DS Request) to send a Management
Response Status U			Response ACCEF	Resµ ²T.	bonse Status U		
I P <b>42</b>	L 44	# 341	<i>Cl</i> <b>10</b> Sood, Kapil	SC 10.3.35.2.2	P <b>42</b>	L <b>39</b>	# 169
y the SME to request the M/ ? STA can send this message MLME-Remote_Request is text, as written, is very con- .ent) is used by the SME of non	AC to send a Mana ge. This must be in used on non-AP S fusing and should AP STA (to send c	agement Frame of ndicated clearly. The STA and on AP for be clarified. (This is over-the-DS Request)	The dei Suggested/ Change Response ACCEF C/ <b>10</b>	finition of ".request" sho Remedy e 10.3.35.2 to 10.3.35.1 <i>Res</i> PT. SC <b>10.3.35.3.1</b>	, and change 10.3.3 ponse Status U	L <b>28</b>	# [342
over-the-DS response) to r	equest the MAC to	5 send a management	Sood, Kapil	1			
Response Status U			Comment 7 "This p Frame{ revisior	Type         TR         Con-           rimitive is used by the MAC         MAC         MAC           a of similar comment)         Comment         Comment	mment Status <b>R</b> MAC to indicate that i c of non-AP STA to it	it has completed s s SME. Make this	sending a Management s explicit. (This is
			Suggested Change sending	Remedy e: "This primitive is user g a Management Frame	d by the MAC of non-	-AP STA to indica	ate that it has completed
			<i>Response</i> REJEC This pr	Resp T. imitive is also used by t	bonse Status U	to the standard field in the	
	Comment Status A the response is delivered to means that the MAC of nor- prect? Is this response "MLM mment) a. At the non-AP STA, the M e SME for processing." OR, <i>Response Status</i> U the non-AP STA" deleted 1 P42 <i>Comment Status</i> A y the SME to request the M. P STA can send this message MLME-Remote_Request is a text, as written, is very con- nent) is used by the SME of non-/ d over-the-DS response) to r <i>Response Status</i> U	Comment Status A         at the response is delivered to the SME for processing that the MAC of non-AP STA sends a prect? Is this response "MLME-REMOTE-REComment)         at the non-AP STA, the MAC delivers the Mace SME for processing." OR, delete this senter         Response Status U         the non-AP STA" deleted         1       P42         L44         Comment Status A         y the SME to request the MAC to send a Mana P STA can send this message. This must be in MLME-Remote_Request is used on non-AP S text, as written, is very confusing and should tent)         is used by the SME of non-AP STA (to send c to end)         is used by the SME of non-AP STA (to send c to end)         Response Status U	Comment Status A         the response is delivered to the SME for processing." - what does is means that the MAC of non-AP STA sends a "response" to the procet? Is this response "MLME-REMOTE-REQUEST.confirm"? (This ment)         a. At the non-AP STA, the MAC delivers the MLME-REMOTE-es SME for processing." OR, delete this sentence, as this is covered <i>Response Status</i> U         the non-AP STA' deleted       1         1       P42       L44       # 341         Comment Status A         Y he SME to request the MAC to send a Management Frame of PSTA can send this message. This must be indicated clearly. The MLME-REquest is used on non-AP STA and on AP for exet, as written, is very confusing and should be clarified. (This is text)         the used by the SME of non-AP STA (to send over-the-DS Request)       to ver-the-DS response) to request the MAC to send a Management         tower the-DS response) to request the MAC to send a Management       This is text)	Comment Status A       Sood, Kapii         a. the response is delivered to the SME for processing." - what does a means that the MAC of non-AP STA sends a "response" to the processing." I bits response "MLME-REMOTE-REQUEST.confirm"? (This is subtypentive of Processing." OR, delete this sentence, as this is covered       "This p Subtypentive of the Change and SM Frame         a. At the non-AP STA, the MAC delivers the MLME-REMOTE-ee SME for processing." OR, delete this sentence, as this is covered       Response Status U         b. the non-AP STA' deleted       C/ 10         1       P42       L44       # 341         Y the SME to request the MAC to send a Management Frame of PSTA can send this message. This must be indicated clearly. The MLME-Remote_Request is used on non-AP STA and on AP for text, as written, is very confusing and should be clarified. (This is is used by the SME of non-AP STA (to send over-the-DS Request)       Comment T         is used by the SME of non-AP STA (to send over-the-DS Request)       Comment I       This p Frame         is used by the SME of non-AP STA (to send over-the-DS Request)       Comment I       This p Frame         is used by the SME of non-AP STA (to send a Management Prame)       Sood, Kapii       Sood, Kapii         Response Status U       Comment I       This p Frame       This p Frame         Response Status U       Comment I       This p Frame       This p Frame         Response Status U       Comment I       This p Frame       This p Frame <td>Comment Status A       Sood, Kapil         Comment Status A       Comment Status A         The response is delivered to the SME for processing." - what does means that the MAC of non-AP STA sends a "response" to the mement       This primitive is used by the S         Soud, Kapil       Subtype&amp;" - only non-AP STA entry is primitive is used by the S         Soud Mapping       Subtype "- only non-AP STA entry is primitive is used and set of the mon-AP STA, the MAC delivers the MLME-REMOTE-ee is SME for processing." OR, delete this sentence, as this is covered         Mapping       P42       L44       # 341         Comment Status A       The AP42       L44       # 341         Comment Status A       Subtype&amp;" only non-AP STA (adeleted different message). This must be indicated clearly. The MLME-Remote Request is used on non-AP STA and on AP for text, as written, is very confusing and should be clarified. (This is isent)       Comment Type TR Core The edition of ".request" should be clarified. (This is isent)         Response Status U       Change 10.3.35.2 to 10.3.35.1       Sood, Kapil         Response Status U       Comment Type TR Core The edition of singla comment)       Coursent Type TR Core The edition of singla comment)         SuggestedRemedy       Change 10.3.35.2.1 to 10.3.35.3.1       Sood, Kapil         Comment Type TR Core The edition of singla comment)       Comment Type TR Core The edition of singla comment)         SuggestedRemedy       Change "This primitive is useed by the MA</td> <td>Comment Status A       Sood, Kapil         Comment Status A       This primitive is used by the SME for processing." - what does is response is delivered to the SME for processing." - what does is response is delivered the MAC of non-AP STA and the MAC of non-AP STA and the non-AP STA, the MAC delivers the MLME-REMOTE-ee SME for processing." OR, delete this sentence, as this is covered       This primitive is used by the SME to request the MLME-REMOTE-ee SME for processing." OR, delete this sentence, as this is covered         Response Status U       Change: "This primitive is used by the SME of non-AP STA and of AP (to send over-the-DS response) to Fame of Subtype&amp;"         Response Status A       The definition of ".request" should appear before the SME to request the MAC to send a Management Frame of S STA can send this message. This must be indicated clearly. The MLME-Remote. Request is used on nAP STA and on AP For and or and SME of non-AP STA (to send over-the-DS response) to request the MAC to send a Management is over-the-DS response) to request the MAC to send a Management frame of Subgreated/Remedy         C/ 10       SC 10.3.35.1       P43         Sood, Kapil       Comment Status R       "This primitive is used by the MAC to indicate that Frame&amp;" is issued by the MAC of non-AP STA to inversion of similar comment)         Suggested/Remedy       Change: "This primitive is used by the MAC</td> <td>Comment Status A         the response is delivered to the SME for processing." - what does imment be MAC of non-AP STA sends a "response" to the imment of the MAC of non-AP STA sends a "response" to the entire MLME clause for MLME-REMOTE- REQUEST.confirm"? (This is espense Status U         A the non-AP STA, the MAC delivers the MLME-REMOTE- e SME for processing." OR, delete this sentence, as this is covered Response Status U         A the non-AP STA, the MAC delivers the MLME-REMOTE- e SME for processing." OR, delete this sentence, as this is covered         Response Status U         the non-AP STA" deleted         1       P42         L44       # [341]         Comment Status A         y the SME to request the MAC to send a Management Frame of PSTA can send this message. This must be indicated clearly. The MLME-Remote_Request is used on non-AP STA and on AP for PSTA can send this message. This must be indicated clearly. The MLME-Remote_Request is used on non-AP STA and on AP for PSTA can send this message. This must be clarified. (This is tent)         is used by the SME of non-AP STA (to send a Management Frame of PSTA can send this message. This must be indicated clearly. The MLME-Remote_Request is used on non-AP STA and on AP for PSTA can send this message. This must be indicated clearly. The MLME-Remote_Request is used on non-AP STA to indicate the definition of *.request* should appear before the definition of *.ir SuggestedRemedy         Change 10.3.35.1       P43       L28         Sood, Kapil       Comment Type TR       Comment Status R         This primitive is used by the MAC to indicate</td>	Comment Status A       Sood, Kapil         Comment Status A       Comment Status A         The response is delivered to the SME for processing." - what does means that the MAC of non-AP STA sends a "response" to the mement       This primitive is used by the S         Soud, Kapil       Subtype&" - only non-AP STA entry is primitive is used by the S         Soud Mapping       Subtype "- only non-AP STA entry is primitive is used and set of the mon-AP STA, the MAC delivers the MLME-REMOTE-ee is SME for processing." OR, delete this sentence, as this is covered         Mapping       P42       L44       # 341         Comment Status A       The AP42       L44       # 341         Comment Status A       Subtype&" only non-AP STA (adeleted different message). This must be indicated clearly. The MLME-Remote Request is used on non-AP STA and on AP for text, as written, is very confusing and should be clarified. (This is isent)       Comment Type TR Core The edition of ".request" should be clarified. (This is isent)         Response Status U       Change 10.3.35.2 to 10.3.35.1       Sood, Kapil         Response Status U       Comment Type TR Core The edition of singla comment)       Coursent Type TR Core The edition of singla comment)         SuggestedRemedy       Change 10.3.35.2.1 to 10.3.35.3.1       Sood, Kapil         Comment Type TR Core The edition of singla comment)       Comment Type TR Core The edition of singla comment)         SuggestedRemedy       Change "This primitive is useed by the MA	Comment Status A       Sood, Kapil         Comment Status A       This primitive is used by the SME for processing." - what does is response is delivered to the SME for processing." - what does is response is delivered the MAC of non-AP STA and the MAC of non-AP STA and the non-AP STA, the MAC delivers the MLME-REMOTE-ee SME for processing." OR, delete this sentence, as this is covered       This primitive is used by the SME to request the MLME-REMOTE-ee SME for processing." OR, delete this sentence, as this is covered         Response Status U       Change: "This primitive is used by the SME of non-AP STA and of AP (to send over-the-DS response) to Fame of Subtype&"         Response Status A       The definition of ".request" should appear before the SME to request the MAC to send a Management Frame of S STA can send this message. This must be indicated clearly. The MLME-Remote. Request is used on nAP STA and on AP For and or and SME of non-AP STA (to send over-the-DS response) to request the MAC to send a Management is over-the-DS response) to request the MAC to send a Management frame of Subgreated/Remedy         C/ 10       SC 10.3.35.1       P43         Sood, Kapil       Comment Status R       "This primitive is used by the MAC to indicate that Frame&" is issued by the MAC of non-AP STA to inversion of similar comment)         Suggested/Remedy       Change: "This primitive is used by the MAC	Comment Status A         the response is delivered to the SME for processing." - what does imment be MAC of non-AP STA sends a "response" to the imment of the MAC of non-AP STA sends a "response" to the entire MLME clause for MLME-REMOTE- REQUEST.confirm"? (This is espense Status U         A the non-AP STA, the MAC delivers the MLME-REMOTE- e SME for processing." OR, delete this sentence, as this is covered Response Status U         A the non-AP STA, the MAC delivers the MLME-REMOTE- e SME for processing." OR, delete this sentence, as this is covered         Response Status U         the non-AP STA" deleted         1       P42         L44       # [341]         Comment Status A         y the SME to request the MAC to send a Management Frame of PSTA can send this message. This must be indicated clearly. The MLME-Remote_Request is used on non-AP STA and on AP for PSTA can send this message. This must be indicated clearly. The MLME-Remote_Request is used on non-AP STA and on AP for PSTA can send this message. This must be clarified. (This is tent)         is used by the SME of non-AP STA (to send a Management Frame of PSTA can send this message. This must be indicated clearly. The MLME-Remote_Request is used on non-AP STA and on AP for PSTA can send this message. This must be indicated clearly. The MLME-Remote_Request is used on non-AP STA to indicate the definition of *.request* should appear before the definition of *.ir SuggestedRemedy         Change 10.3.35.1       P43       L28         Sood, Kapil       Comment Type TR       Comment Status R         This primitive is used by the MAC to indicate

COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Bill Marshall, ATT Labs Research

09/27/2007 06:28

C/ 10 SC 10.3.35.3 Sood, Kapil	.1 P43	L <b>28</b>	# 172	C/ 11 CHAPLIN	SC <b>11.3.2.1</b> , CLINT F	P <b>45</b>	L13	# 37
Comment Type <b>TR</b> "This primitive is used I Frame&" is issued by th	Comment Status R by the MAC to indicate that ne MAC of non-AP STA to it	it has completed s s SME. Make this	ending a Management explicit.	<i>Comment</i> As fai used	<i>Type</i> <b>TR</b> as FT is concerr for FT protocol. T	Comment Status A ned, Association is only use aken into account how initi	ed during the initial al MD association	MD association; it is not works, it is more or less
SuggestedRemedy Change: "This primitive sending a Managemen	is used by the MAC of non t Frame"	-AP STA to indica	e that it has completed	identi descr case (Origi	cal process to the iption of how PTH of FT. The chang nally LB98/355 st	802.11i association and a (SA is to be deleted. This d e to PTKSA deletion is only ubmitted by Malinen, Jouni,	s such, there is no leletion can, and s y needed for reass , during LB98 with	need to modify the hould, happen also in ociation procedure. ID Malinen/30)
Response REJECT. This primitive is also us the response.	Response Status U ed by the MAC of the AP to	indicate that it ha	s completed sending	Suggester Remo Response	dRemedy we changes to 17	I.3.2.1. Response Status U		
Cl 11 SC 11.3.1.1 CHAPLIN, CLINT F Comment Type TR	P44	L <b>24</b>	#  34	ACCE <i>Cl</i> 11 CHAPLIN	EPT. SC <b>11.3.2.1</b> , CLINT F	P <b>45</b>	L13	# 36
It is mentioned that Fas (Originally LB98/352 su SuggestedRemedy	t BSS Transition is possible botted by Zaks, Artur, duri	e in IBSS - which is ng LB98 with ID Z	s not true aks/11)	<i>Comment</i> The F (Origi	<i>Type</i> <b>TR</b> TKSA should be nally LB98/354 si	Comment Status A deleted even on an FT. Jomitted by Cam-Winget, N	lancy, during LB98	3 with ID Cam-Winget/19)
Remove IBSS from the Response	definition. State clearly tha <i>Response Status</i> <b>U</b>	t FT is not applical	ble to IBSS	Suggester Remo	dRemedy ove the added "Ex	cept when " clause of this	s sentence.	
ACCEPT. Change second dash li	st item to "If in an ESS, and	the Authentication	n Algorithm."	Response ACCE	P PT IN PRINCIPL	Response Status U E.	Domain Associatio	on and not for the FT
C/ 11 SC 11.3.1.2 CHAPLIN. CLINT F	P <b>44</b>	L <b>64</b>	# 35	protoc	cols. Changes to	11.3.2.1 deleted.	Domain Associatio	
Comment Type TR The PTKSA should be (Originally LB98/353 su SuggestedRemedy Remove the added "If"	Comment Status R deleted even on an FT. Ibmitted by Cam-Winget, Na	ancy, during LB98	with ID Cam-Winget/18)	C/ 11 CHAPLIN Comment The F (Origi	SC 11.3.2.2 , CLINT F <i>Type</i> <b>TR</b> PTKSA should be nally LB98/356 st	P 45 Comment Status A deleted even on an FT. ubmitted by Cam-Winget, N	L <b>23</b> Jancy, during LB98	# 38
Response REJECT. Text changes to 11.3.1 associations created by describe the 11r condit	Response Status U .2 are to insure that the pre- v 11r. Current text in 11A.4.3	11r behavior does 2 (at 53.24) and 17 sociations.	not delete security A.5.4 (at 60.22)	Suggester Remo Response ACCE Assoc protoc	dRemedy we the added "Ex PT IN PRINCIPL ciation is only use cols. Changes to	ccept when" clause of this Response Status U .E. d during the Initial Mobility 11.3.2.2 deleted.	s sentence. Domain Associatio	on, and not for the FT

 TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general
 Page 33 of 89

 COMMENT STATUS: D/dispatched A/accepted R/rejected
 RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn
 Comment ID
 Page 33 of 89

 SORT ORDER: Comment ID
 09/27/2007 06:28

Submission

C/ 11 CHAPLIN	SC <b>11.3.2.2</b> , CLINT F	P <b>45</b>	L <b>23</b>	# 39	<i>CI</i> 11 CHAPLIN	SC <b>11.3.2.3</b> I, CLINT F	P <b>45</b>	L <b>44</b>	# 41
Comment As far used identi descr case (Origi Suggester Remo	t Type <b>TR</b> r as FT is concerned for FT protocol. Ta cal process to the iption of how PTKS of FT. The change inally LB98/357 su dRemedy prove changes to 11	Comment Status <b>A</b> ed, Association is only used aken into account how initial 802.11i association and as SA is to be deleted. This de to PTKSA deletion is only is bmitted by Malinen, Jouni, of 3.2.2.	during the initial MD association v such, there is no letion can, and sh needed for reasso luring LB98 with I	MD association; it is not works, it is more or less need to modify the ould, happen also in ociation procedure. D Malinen/31)	Comment The F (Origi Suggeste Remo Response REJE Text	t Type <b>TR</b> PTKSA should be inally LB98/359 st dRemedy bye the added "Es e ECT. changes to 11.3.2	Comment Status R deleted even on an FT. ubmitted by Cam-Winget, Na ccept when" clause of this Response Status U	ancy, during LB9 sentence. 11r behavior do	8 with ID Cam-Winget/21) es not delete security
Response	9	Response Status U			asso	ciations created b	y 11r. Current text in 11A.4.2	2 (at 53.24) and	11A.5.4 (at 60.22)
ACCE	EPT.				C/ 11	SC 11.3.2.4	P <b>45</b>	/ 54	# 42
Cl 11 CHAPLIN Comment Per 1 over-t STAs behav (Origi Suggester Remo	SC 11.3.2.3 , CLINT F t Type TR 1A.5 State 2 is entitle- the-air and over-th will already be in vior to ignore State inally LB98/358 su dRemedy ove changes to point P	P45 Comment Status A tered after successful comp e-DS FT. In other words, wil State 2 and as such, the ch e 1 verification is not needed bmitted by Malinen, Jouni, of ant (a) of the lettered list in the Response Status U	<i>L</i> <b>36</b> letion of authentic nen reassociation ange for MLME-R I for FT. during LB98 with I ne first paragraph	# 40 eation phase in both request is sent, the EASSOCIATE.request D Malinen/32) of 11.3.2.3.	CHAPLIN Comment The F (Origi Suggeste Remo Response REJE Text associ descr	I, CLINT F t Type <b>TR</b> PTKSA should be inally LB98/360 so the added "Ex- pove the added"	Comment Status R deleted even on an FT. ubmitted by Cam-Winget, Na accept when" clause of this Response Status U 2.4 are to insure that the pre- y 11r. Current text in 11A.4.2 ions for deleting security as	ancy, during LB9 sentence. 11r behavior do 2 (at 53.24) and sociations.	es not delete security 11A.5.4 (at 60.22)
					Cl 11 CHAPLIN Comment Missi reass (Origi Suggeste Chan Response ACCI	SC 11.4.1 I, CLINT F t Type <b>T</b> ng function that T cociation message inally LB98/363 st <i>dRemedy</i> nge "&initiating a tr e EPT.	P46 Comment Status A raffic Stream can be created ubmitted by Sood, Kapil, duri ransition to that AP, or in the Response Status C	L 4 I when the TSPE ing LB98 with ID reassociation re	# 43 EC is sent in the 9 Sood/033) equest to that AP"

C/ <b>11</b> CHAPLIN	SC <b>11.4.4a</b> I, CLINT F	P 47	L18	# 44	C/ 11 CHAPLIN	SC , CLINT	11.4.4a F	P <b>47</b>	L <b>27</b>	# 46
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         Q         ACCEPT.				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						
C/ 11 CHAPLIN Comment	SC <b>11.4.4a</b> I, CLINT F <i>t Type</i> <b>E</b>	P47 Comment Status A	L 22	# 45	take i accou <i>Response</i> ACCI Chan	nto acco unt", hov e EPT IN F ges give	PRINCIPL	us, equivalent to "may take ir alid.) <i>Response Status</i> <b>U</b> E hission 11-07-2516-01.	nto account". "Sr	iali not take into
Gram (Origi <i>Suggeste</i> Repla this re	imar inally LB98/370 su ed <i>Remedy</i> ace "Each TS esta esource request is	bmitted by Malinen, Jouni, dur blished by this resource reque	ing LB98 with I st are" with "Ea	D Malinen/33) ch TS established by	C/ <b>11A</b> Sood, Ka Comment	SC pil t Type	11A TR	P 47 Comment Status R	L 44	# 329
Response ACCI	e EPT.	Response Status C	Atus C 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.

Comment ID # 329

Response

Response Status U

REJECT

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

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Page 35 of 89 09/27/2007 06:28

C/ 11A	SC 11A	P 47	L <b>44</b>	# 219	С				
Sood, Kapi	I				Μ				
Comment	Type <b>TR</b>	Comment Status R		out-of-order IEs	С				
The FT AP ST IE is no	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.								
Suggested	Remedy								
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							
REJEC Subcla the ord Genera needed	CT. use 11A.8 specifi ler of the IEs in th al ordering of IEs d to 802.11r.	es the order for IEs for the MI e frame. The order of the IEs in the frames is covered in ba	C calculation, within the RIC se specification	which is independent of s specified in 11A.11. on in 7.2.3. No changes	С М С				
C/ 11A	SC 11A	P <b>47</b>	L 44	# 155	S				
Sood, Kapi	I								
Comment	Type <b>TR</b>	Comment Status R		Wait for Interoperability	R				
No inte demon the bes all corr withour results protoco	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.								
Suggested	Remedy								
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			R				
REJEC The IE	REJECT The IEEE procedure for publishing standards is not the subject of this ballot.								

C/ 11A	SC 11A.1	P <b>47</b>	L <b>50</b>	# 144
Mccann, St	ephen			
Comment T Typo "o	<i>Type</i> <b>E</b> connectivity is lo	Comment Status A st"		
Suggested conne	R <i>emedy</i> ctivity that is los	t"		
Response ACCEF Change	PT IN PRINCIPL	Response Status <b>C</b> .E. connectivity is lost."		
C/ 11A Mccann, St	SC 11A.1 ephen	P <b>47</b>	L <b>51</b>	# 145
Comment T Specifi	<i>Type</i> <b>E</b> cally what "prote	Comment Status A cools" are referred to		
Suggested Add "F	R <i>emedy</i> ast Transition P	rocotols"		
Response ACCEF Change	PT IN PRINCIPL = "These protoc	Response Status <b>C</b> E. ols" to "The Fast BSS Transi	tion protocols"	
C/ 11A Sood, Kapi	SC 11A.1	P <b>47</b>	L 55	# 173
Comment T "First" i	<i>Type</i> <b>TR</b> s inconsistent w	Comment Status A vith the use of "Initial" elsewh	ere in the docume	ent.
Suggested Change	Remedy e: first to Initial			
Response ACCEF	РТ.	Response Status U		

 TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general

 COMMENT STATUS: D/dispatched A/accepted R/rejected
 RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn

 SORT ORDER: Comment ID
 Comment ID
C/ 11A	SC 11A.1	P 48	L1	# 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.

-

CI	11A	SC 11A.1	

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.

P48

L47

# 146

### 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

C/ 11A	SC 11A.10	P 84	L1	# 314
Myles, Andre	w F			

#### Comment Type TR Comment Status A

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

### 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."

Response Status U

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.

RRB

C/ 11A SC 11 Malinen, Jouni	IA.10	P <b>86</b>	L1	# 324		C/ <b>11A</b> Chaplin, C	SC 11 <b>A.</b> CLINT F
Comment Type 11A.10 describe Action frames a and the AP des the non-AP STA than new Actior communication to wait for 802.1	TR Comment St es a new component, re ind data frames with a s ign could be simplified I As could send and recei n frames. In addition, thi to be protected since d I 1w to add managemen	tatus <b>R</b> emote request brippecific Ethertype by removing RRE ve data frames a s allows the non ata frames are e t frame protection	oker, that is use a. This functional b frame converses as easily, if not -AP STA <-> cu ncrypted in the n.	ed to convert betw ality is unnecessa sion completely s even more easily urrent AP RSNA without ha	RRB ween ary ince ', aving	Comment T Expand (Origina SuggestedF Change Response	ype E ACK ally LB98/62 Remedy a "ACK" to "
SuggestedRemedy Remove RRB fr defined in 11A. the destination data frames, the	rame conversion (Actior 10.3 by sending and rec AP. The frames will still ere is no need to have s	n <-> data) from eiving them dire go through the o pecific RRB pro	802.11r and ins ctly from/to the current AP, but cessing in the c	tead, use the fra non-AP STA to/f since they are no current AP.	mes rom ormal	Cl <b>11A</b> CHAPLIN, C Comment T	SC 11A. CLINT F
Response REJECT Use of Action fr	Response St ames is consistent with	atus <b>U</b> the over-the-air	FT methods			Make S (Origina SuggestedF	TA more s ally LB98/62 Remedy
C/ 11A SC 11 Chaplin, Clint F	IA.10	P86	L1	# 141	RRB	Change Response ACCEP	e "STA" to " 'T.
The Remote Re MAC/PHY scop fast BSS transit to define a spec the target AP to	equest Broker, and the A be of 802.11. While som ion, it needs to be defin cial format data frame so accomplish this. (subn	AP-AP protool de e mechanism is ed with the scop ent over-the-air t hitted by Bill Mars	fined in 11A.10 needed to perfo e of the project o the current Al shall)	), are outside the orm the over-the- . One such desig > that is directed	DS in is to	Cl 11A Sood, Kapil Comment T	SC 11A. Type ER es it" - who
SuggestedRemedy Incorporate late the amendment	st revision of 11-06-162	22-xx-000r-CID-1	835-General-E	ncapsulation.doc	into	SuggestedF Change	Remedy e "Fast BSS
Response REJECT AP to AP comm The design dec consistent with AP protocol is c	Response St nunication is in scope to ision is to use Action fra use of Authentication fra lefined here, but any su	atus <b>U</b> facilitate Fast B ames to enable c ames in over-the ch protocol can I	SS Transitions over-the-DS trar air transitions. De used.	over-the-DS sitions to remain One sample AP-	ı to-	Response ACCEP	т.

<i>CI</i> <b>11A</b> CHAPLIN, C	SC 11 <b>A.10.1</b> LINT F	P 80	6	L11	# 88
Comment Ty Expand (Original	<i>rpe</i> <b>E</b> ACK Ily LB98/621 sub	Comment Status mitted by Sood, Ka	A pil, during LB	98 with ID Sood/(	081)
SuggestedR Change	<i>emedy</i> "ACK" to "Ackno	owledgement"			
Response ACCEP	Г.	Response Status	С		
C/ <b>11A</b> CHAPLIN, C	SC <b>11A.10.1</b> LINT F	P8	6	L 15	# 89
Comment Ty Make S <sup>-</sup> (Original	/pe <b>T</b> FA more specific Ily LB98/622 sub	Comment Status mitted by Sood, Ka	<b>A</b> pil, during LB	98 with ID Sood/(	082)
SuggestedR Change	<i>emedy</i> "STA" to "non-A	P STA"			
Response ACCEP	г.	Response Status	С		
C/ <b>11A</b> Sood, Kapil	SC 11A.10.1	P 8	6	L 31	# 255
Comment Ty "it passe	<i>pe</i> <b>ER</b> es it" - who passe	Comment Status es what? Clarify	Α		
SuggestedR Change	<i>emedy</i> "Fast BSS Trans	sition, the MAC pas	ses the Actio	n Frame to the SM	ME"
Response ACCEP	г.	Response Status	U		

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Comment ID # 255

Page 38 of 89 09/27/2007 06:28

C/ 11A SC 11A.10.1 Sood, Kapil	P86	L <b>54</b>	# 256	<i>Cl</i> <b>11A</b> <i>SC</i> <b>11A.10.1</b> Sood, Kapil	P86	L <b>6</b>	# 253
Comment Type <b>TR</b> Which AP will forward	Comment Status A it - clarify.			Comment Type <b>TR</b> STA is not just any STA	Comment Status A		non-AP STA
SuggestedRemedy Change "the current A	P will forward the Request to	that target AP"		SuggestedRemedy Change line 6, 7, 11, 15	5, 49, 51, 62, : "STA" to "non <sup>.</sup>	-AP STA"	
Response ACCEPT.	Response Status U			Response ACCEPT	Response Status U		
<i>CI</i> <b>11A</b> SC <b>11A.10.1</b> CHAPLIN, CLINT F	P86	L <b>6</b>	#  87	<i>Cl</i> <b>11A</b> SC <b>11A.10.1</b> Sood, Kapil	P <b>86</b>	L <b>6</b>	# 252
Comment Type <b>T</b> The "STA" in the introd (Originally LB98/620 s SuggestedRemedy Change "STA" to "non	Comment Status A duction of RRB should be mor ubmitted by Sood, Kapil, durir -AP STA"	e specific. Ig LB98 with ID 3	Sood/080)	Comment Type ER "This" is not the correct SuggestedRemedy Change "Remote Requ	Comment Status A way to start a new section. est Broker (RRB) mechanism	n allows&"	
Response ACCEPT.	Response Status C			Response ACCEPT IN PRINCIPLI Changed to "The Remo	Response Status U E. te Request Broker (RRB) me	echanism allows	
C/ 11A SC 11A.10.1 Sood, Kapil	P86	L <b>6</b>	# 254	<i>CI</i> <b>11A</b> SC <b>11A.10.2</b> CHAPLIN, CLINT F	P86	L 38	# 90
Comment Type ER "its" - who does its refe	Comment Status <b>A</b> er to? Clarify.			Comment Type <b>T</b> There are Responses, ( (Originally LB98/634 su	Comment Status A Confirm, Acks, besides Requ bmitted by Sood, Kapil, durir	uests. ng LB98 with ID \$	Sood/094)
Change "AP through n	oon-AP STA's existing"			SuggestedRemedy Change "Requests" to "	'protocol messages"		
Response ACCEPT.	Response Status U			Response ACCEPT.	Response Status C		

C/ <b>11A</b> CHAPLIN,	SC <b>11A.10.2</b> CLINT F	P 86	L <b>48</b>	# 91		<i>CI</i> <b>11A</b> CHAPLIN,	SC 11A.10.2 CLINT F	P86	L <b>55</b>	# 94
Comment Make S (Origin	<i>Type</i> <b>T</b> STA more specific nally LB98/640 sub	Comment Status A mitted by Sood, Kapil, during	g LB98 with ID \$	Sood/095)		Comment This se Reque (Origin	<i>Type</i> <b>T</b> ection don't do a g est/Response mes nally LB98/643 su	Comment Status A good job in connecting Act ssages bmitted by Sood, Kapil, du	ion Frames and R Iring LB98 with ID	emote Sood/098)
Suggested	<i>Remedy</i> ie "STA" to "non-A	P STA"				Suggested	IRemedy		0	,
Response		Response Status C				Add a into Re	sentence at end emote Requests,	of line 54, pg 86: "The RRI and converts Remote Res	3 on Current AP co ponse into Action	onverts Action Frames Frames"
C/ 11A	SC 11A.10.2	P86	L 51	# 92		Response ACCEI	PT.	Response Status C		
CHAPLIN,	CLINT F					C/ 11A	SC 11A.10.2	P <b>87</b>	L3	# 257
Comment Make S (Origin	<i>Type</i> <b>T</b> STA more specific nally LB98/641 sub	Comment Status A	g LB98 with ID \$	Sood/096)		Sood, Kapi <i>Comment</i>	il Type <b>TR</b>	Comment Status A		non-AP STA
Suggested Chang	IRemedy je "STA" to "non-A	P STA"				STA is Suggested	not just any STA	- It is non-AP STA		
Response ACCEI	PT.	Response Status C				Chang Response	je line 3, : "STA" t 	o "non-AP STA" Response Status <b>U</b>		
C/ 11A CHAPLIN,	SC 11A.10.2 CLINT F	P86	L <b>52</b>	# 93		ACCEI	PT			
Comment <sup>-</sup> This se (Origin	<i>Type</i> <b>T</b> entence is confusin nally LB98/642 sub	Comment Status A ng imitted by Sood, Kapil, during	g LB98 with ID \$	Sood/097)						
Suggested	Remedy		-							
Chang "over-t	je "directed to a <sup>-</sup> the-DS" communic	Target AP in the same Mobil ations) the Current AP will for	ity Domain (and prward the mess	I therefore supporting ages to that target A	) .P"					
Response ACCEI Chang forward above.	PT. Je indicated in the d". Also deleted th	Response Status <b>C</b> proposed resolution changes e parenthesized phrase, as	s "AP will forwar it is repeated fro	d" to "Current AP will m two paragraphs	I					

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Comment ID # 257

Page 40 of 89 09/27/2007 06:28

C/ 11A	SC 11A.10.3	P <b>87</b>	L <b>40</b>	# 323	
Malinen, Jo	uni				
Comment T	ype TR	Comment Status A		I	RRB
IEEE 8	02.11r is introduc	cing a new Ethertype for AP-	to-AP communic	ation 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

#### ACCEPT

C/ 11A	SC 11A.10.3	P <b>87</b>	L <b>45</b>	# 306
Malinen .	louni			

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.

C/ 11A Sood, Kapil	SC 11A.11.1	P88	L <b>34</b>	# 258
Comment T STA is r	/pe <b>TR</b> not just any STA -	Comment Status A It is non-AP STA		non-AP STA
SuggestedF Change	<i>emedy</i> lines 34, 35, 50,	44, :"STA" to "non-AP STA"		
Response ACCEP	Т	Response Status U		
<i>CI</i> <b>11A</b> CHAPLIN, C	SC <b>11A.11.1</b> CLINT F	P 88	L <b>34</b>	#  95
Comment T	vpe 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			
ACCE Chanç	PT IN PRINCIPLE	sion 11-07-2516-01.			
C/ 11A CHAPLIN,	SC 11A.11.1 CLINT F	P 88	L <b>34</b>	# 96	
<i>Comment</i> Make (Origin	<i>Type</i> <b>T</b> STA more specific nally LB98/649 sub	Comment Status A mitted by Sood, Kapil, durir	ng LB98 with ID S	Sood/102)	
Suggested Chano	dRemedy ge "STA" to "non-Al	P STA"			

Response Response Status C

ACCEPT.

 TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general

 COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn

 SORT ORDER: Comment ID

Page 41 of 89 09/27/2007 06:28

CI 11A SC 11A.11. CHAPLIN, CLINT F	1 <i>P</i> 88	L <b>43</b>	# 97	<i>CI</i> <b>11A</b> CHAPLIN,	SC 1 CLINT I	11 <b>A.11.1</b> F	P88	L <b>54</b>	# 100
Comment Type TR	Comment Status A			Comment	Tvpe	т	Comment Status A		
The text emphasing th muddled. Allowing sta manner before associ was previously accept (Originally LB98/650 s	hat resource requests don't ta titions to request resources to ation, leads to instability beca ted by the group, but someho submitted by Epstein, Joseph	ke place until rea more than one Al use of overreque w, the text becam during LB98 with	ssociation has become P at a time, in a binding sting of resources. This e unclear. ID Epstein/11)	Make (Origir Suggested Chang	STA mo nally LBS <i>Remedy</i> ge "STA"	ore specific 98/655 sub y ' to "non-A	mitted by Sood, Kapil, duri P STA"	ing LB98 with ID	Sood/105)
SuggestedRemedy		U U	. ,	Response			Response Status C		
Change to "The RIC of reservation after the tr discard any previous resource request shal the AP discards any p	contains a complete list of res ransition. An AP that receives resource request from that SI I first be authenticated by the revious resource request."	ources requested a resource reque A. In an RSN, thi AP through check	by the STA, for est from a STA shall s king of the MIC before	ACCE C/ 11A CHAPLIN,	SC 1 CLINT	11 <b>A.11.2</b> F	Р <b>8</b> 9	L1	#  101
Response	Response Status U			Comment	Туре	Е	Comment Status A		
ACCEPT IN PRINCIP Changes given in sub	LE mission 11-07-2516-01.			We ha (Origir	ave estat nally LBS	blished an 98/661 sub	abbreviation for "Resource mitted by Sood, Kapil, duri	e Information Co ing LB98 with ID	ntained" Sood/101)
C/ 11A SC 11A.11.	1 P88	L <b>43</b>	# 98	Suggested Use "F	dRemedy RIC" inst	y ead of "Re	source Information Contai	ner"	
Comment Type T "after the transition" is transition?	Comment Status A	pefore the transiti	on? During the	Response ACCE Cl 11A	PT.	11A.11.2	Response Status C	L 24	# 131
(Originally LB98/651 s	submitted by Sood, Kapil, dur	ng LB98 with ID \$	Sood/100)	Trainin, So	olomon				
SuggestedRemedy Delete this phrase from	m the sentence			Comment	Туре	TR	Comment Status A	;	RIC format
Response ACCEPT.	Response Status C			eleme WMM resour	nt. It ma QoS sp rces. Mo	etery clear by be imporecification ore explanation	tant in case if an AP support as well. In this case the ST tion may be very useful.	orts QoS in para FA may request	an alternative of both
C/ 11A SC 11A.11.	1 P88	L <b>49</b>	# 99	Suggested	dRemed	y			
CHAPLIN, CLINT F				Provid	le explar	nation, cha	nge format of the Resourc	e Information Co	ontainer if needed
Comment Type <b>T</b> Make STA more spec (Originally LB98/654 s	Comment Status A ific submitted by Sood, Kapil, duri	ng LB98 with ID \$	Good/104)	Response ACCE Insert	PT row in T	able 11A-3	Response Status U	ndor Specific" an	d Resource Descriptor
SuggestedRemedy Change "STA" to "nor	n-AP STA"			definit this re	ion "RDI source."	E is follow	ed by any Vendor-specific	information eler	nents required to specify
Response ACCEPT.	Response Status C								
		, , , ,	<b>-</b>	, .					

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Page 42 of 89 09/27/2007 06:28

Submission

Bill Marshall, ATI Labs Research

Comment ID # 131

CI 11A SC 1 <sup>-</sup> CHAPLIN, CLINT F	1A.11.2	P <b>89</b>	L <b>30</b>	# 102	<i>Cl</i> <b>11A</b> Sood, Kapil	SC 11A.11.2	P <b>89</b>	L <b>30</b>	# 247
Comment Type Make STA mor (Originally LB98 SuggestedRemedy Change "STA" Response	T Comm e specific in "Note 8/665 submitted by to "non-AP STA" Respor	ent Status <b>A</b> s" column y Sood, Kapil, durir nse Status <b>C</b>	ng LB98 with ID S	Good/106)	Comment 1 The res has no adopted requirer 802.116 extensi	ype <b>TR</b> ource types cur accomodation f d and implemen ment that the 80 e, but all WMM ble to accomod	Comment Status A rently defined in the specific or WMM TSPECs as define ted the WMM resource form 02.11r procedure for resource (WFA) and other formats in ate co-existence of multiple	cation only mentio d by WiFi Alliance hats and processi ses be flexible to a future. This speci resource formats	RIC format ons 802.11 QoS, and e. The marketplace has ing, and it is an absolute accomodate not just ification should be made
ACCEPT.					Suggested	Remedy			
C/ 11A SC 1	1A.11.2	P 89	L <b>30</b>	# 375	Accept and adv	my submission /ertising correct	which addresses this proble resource support policies.	em, by extending	the resource identifiers
Sood, Kapil					Response		Response Status U		
Comment Type The resource ty has no accomo adopted and im requirement tha 802.11e, but all extensible to ac	TR Comm ypes currently defi idation for WMM T iplemented the Wi at the 802.11r prod I WMM (WFA) and cocomodate co-exis	ent Status <b>A</b> ned in the specifica 'SPECs as defined MM resource forma- cedure for resource d other formats in fu- stence of multiple re-	ation only mentior I by WiFi Alliance ats and processin as be flexible to a uture. This specif esource formats.	ns 802.11 QoS, and The marketplace has g, and it is an absolute ccomodate not just cation should be made (This is revision of	ACCEF Insert re definition this res C/ 11A CHAPLIN, 0	T IN PRINCIPL w in Table 11A in "RDIE is follo ource." SC 11A.11.3 CLINT F	E -3 with Resource Type "Ve wed by any Vendor-specific .1 P91	ndor Specific" and information elem	d Resource Descriptor ients required to specify # 103
similar commer	nt)				Comment 7	уре Т	Comment Status A		
SuggestedRemedy Accept my sub and advertising	, mission which adc I correct resource	Iresses this probler support policies.	m, by extending t	ne resource identifiers	"These This se which a	Resource Desc ntence is confus ire within a RIC	riptors are included in a Re sing and technically correct. request. A very good explai	source Informatio RDs are within a ination exists in 1	n Container (RIC)" - Resource Request, 1A.10.2, so why do we
Response	Respor	nse Status U			need th	is here. ally I B98/672 si	ibmitted by Sood Kapil du	ring I B98 with ID	Sood/107)
ACCEPT IN PR Insert row in Ta definition "RDIE	RINCIPLE able 11A-3 with Re E is followed by an	esource Type "Ven y Vendor-specific i	dor Specific" and information eleme	Resource Descriptor ents required to specify	Suggested Remov	Remedy e this sentence.			
this resource."	,			, , , , , , , , , , , , , , , , , , , ,	Response ACCEF	۲.	Response Status C		

Comment ID # 103

Page 43 of 89 09/27/2007 06:28

<i>ci</i> <b>11a</b> Chaplin,	SC 11A.11.3.1 , CLINT F	P <b>91</b>	L18	# 104	<i>CI</i> So	<b>11A</b> od, Kapil	SC 11A.11.3	.1	P <b>91</b>	L <b>44</b>	# 380
<i>Comment</i> Which (Origin	Type <b>T</b> is the "next" AP? T nally LB98/673 subi	Comment Status A This draft has used "Target" t mitted by Sood, Kapil, during	hroughout. LB98 with ID \$	Sood/108)	Co	mment Ty The use not cons	pe <b>TR</b> case of wheth idered here. (1	Comment St er a reassoc req This is revision o	atus <b>A</b> uest can be fa f similar comm	iled if resource nent)	e request were failed, is
Suggestee Repla Response ACCE	dRemedy ice "next" with "Targ PT.	get" Response Status <b>C</b>			Su	ggestedR Insert on by a targ requests	emedy line 44 page 9 let AP solely of from that non-	91 :"The non-AP n the basis of tar -AP STA."	STA shall not get AP not be	have its reass ing able to allo	ociation request rejected cate any resources
Cl <b>11A</b> Sood, Kap Comment This s	SC 11A.11.3.1 bil Type ER spec has used targe	P91 Comment Status A et AP, so why use next AP he	L <b>19</b> re	#   <mark>260</mark>		ACCEP Subclaus tells the 11A.11.3 the RDIE cause a	IN PRINCIPL se 11A.11.3.1 STA how to inf 3.2 page 93 lin shall be set". non-zero Statu	Response Sa E. is the STA proce terpret a zero sta e 17 changed "T Inserted after lir us Code in the fra	edures, not the atus in the fran he Status Coo he 27 "A non-z ame containin	AP procedure ne and a non-z le shall be set" ero Status Coo g the RIC Requ	s, and the text currently ero status in the RIC. In to "The Status Code in de in an RDIE shall not uest."
Suggested Chang Response ACCE	aRemeay ge "Next AP" to "tar e PT.	get AP" Response Status U			CI So Co	<b>11A</b> od, Kapil omment Ty STA is n	SC 11A.11.3 pe TR ot just any ST	.1 <i>Comment St</i> A - It is non-AP S	P <b>91</b> atus <b>A</b> STA	L <b>5</b>	# 259 non-AP STA
C/ 11A Sood, Kap	SC 11A.11.3.1	P <b>91</b>	L <b>44</b>	# 261	Su	ggestedR Change	emedy lines 6. 7. 9. 1	6. 21. 26. 30. 40	. 43. :"STA" to	"non-AP STA'	
Comment The u not cc	<i>Type</i> <b>TR</b> se case of whether onsidered here.	Comment Status <b>A</b> a reassoc request can be fai	led if resource	request were failed, is	Re	sponse ACCEPT	Γ	Response Sta	atus <b>U</b>		
Suggestee Insert by a ta reque	<i>dRemedy</i> on line 44 page 91 arget AP solely on t sts from that non-A	:"The non-AP STA shall not he basis of target AP not bei P STA.	have its reassong able to alloc	ociation request rejected cate any resources	b						
Response ACCE Subcli tells th 11A.1 the RI cause	PT IN PRINCIPLE. ause 11A.11.3.1 is ne STA how to inter 1.3.2 page 93 line DIE shall be set". In e a non-zero Status	Response Status <b>U</b> the STA procedures, not the pret a zero status in the fram 17 changed "The Status Codu serted after line 27 "A non-ze Code in the frame containing	AP procedure: e and a non-ze e shall be set" ero Status Cod the RIC Requ	s, and the text currently ero status in the RIC. In to "The Status Code in e in an RDIE shall not lest."							

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Comment ID # 259

Page 44 of 89 09/27/2007 06:28

C/ 11A CHAPLIN, (	SC 11A.11.3.1 CLINT F	P 91	L 62	# 105	Cl <b>11A</b> Sood, Kapil	SC 11A.11.3	.2	P <b>93</b>	L 12	# 262
Comment T The tex muddle manner was pre (Origina SuggestedF Change the tard	Type <b>TR</b> tt emphasing that d. Allowing station before association eviously accepted ally LB98/683 sub Remedy to "Failure to do use AP on behalf of	Comment Status <b>A</b> resource requests don't ta ns to request resources to on, leads to instability beca by the group, but someho mitted by Epstein, Joseph, so will result in the abando of the STA "	ke place until reas more than one Al ause of overreque w, the text becam , during LB98 with conment of any res	ssociation has become <sup>o</sup> at a time, in a binding sting of resources. This e unclear. ID Epstein/12) ource requests held by	Comment Typ The use of not consid SuggestedRe Insert on AP STA s from that Response	be <b>TR</b> case of wheth dered here. <i>medy</i> line 12 page olely on the non-AP STA	Commen er a reassoo 93 :"The targ basis of targe Respons	nt Status A c request can be get AP shall not et AP not being c e Status U	failed if resource reject a reassocia able to allocate ar	request were failed, is ation request from a non- ny resources requests
Response ACCEP Change	PT IN PRINCIPLE	Response Status U			ACCEPT Page 93 I shall be s non-zero	IN PRINCIP ine 17 chang et". Inserted Status Code	E. ed "The Stat after line 27 in the frame	us Code shall b "A non-zero Sta containing the F	e set" to "The Sta tus Code in an RI RIC Request."	tus Code in the RDIE DIE shall not cause a
C/ <b>11A</b> Chaplin, (	SC 11A.11.3.2 CLINT F	P <b>92</b>	L <b>30</b>	# 106	C/ <b>11A</b> Sood, Kapil	SC 11 <b>A.11.</b> 3	.2	P <b>93</b>	L12	# 381
Comment T The flov algorith is define (Origina SuggestedF Change	ype         TR           wchart's text does         m is for "acceptin ed in 11.4.           ally LB98/685 sub         Remedy           a "Able to allocate         Description	Comment Status A not match the text below i g" resource requests, not " mitted by Epstein, Joseph, these resources?" to "Abl	it, or the actual alg 'allocating" resour , during LB98 with e to accept these	gorithm all that well. The ceswhere "accepting" ID Epstein/13) resource requests?"	Comment Typ The use of not consid SuggestedRe Insert on AP STA s from that	be <b>TR</b> case of wheth dered here. ( <i>medy</i> line 12 page olely on the non-AP STA	Comment of a reassor This is revision 93 :"The targe basis of targe	nt Status <b>A</b> crequest can be on of similar con get AP shall not et AP not being a	failed if resource nment) reject a reassocia able to allocate ar	request were failed, is ation request from a non- ny resources requests
Response ACCEP	ΥТ.	Response Status U			<i>Response</i> ACCEPT Page 93 I shall be s	IN PRINCIP ine 17 chang et". Inserted	<i>Respons</i> E. ed "The Stat after line 27	e Status <b>U</b> us Code shall b "A non-zero Sta	e set" to "The Sta tus Code in an RI	itus Code in the RDIE DIE shall not cause a

non-zero Status Code in the frame containing the RIC Request."

Page 45 of 89 09/27/2007 06:28

C/ 11A CHAPLIN,	SC <b>11A.11.3.2</b> CLINT F	P <b>93</b>	L13	# 108	<i>CI</i> <b>11A</b> CHAPLIN,	SC <b>11A.11.3</b> . CLINT F	2 P93	L <b>5</b>	# 107
Comment Which (Origin	<i>Type</i> <b>T</b> response frame? nally LB98/688 sub	Comment Status A	ng LB98 with ID \$	Good/111)	Comment Clarify (Origir	<i>Type</i> <b>T</b> which SME? nally LB98/687 su	Comment Status A	ing LB98 with ID	Sood/110)
Suggested Chang	dRemedy ge: "∈ the fourth r	nessage (See 11A.7.5)."			Suggested Chang	<i>lRemedy</i> ge: "The Target A	P's SME examines the&"		
Response ACCE Delete	PT IN PRINCIPLE	Response Status <b>C</b> he response frame."			Response ACCE	PT.	Response Status C		
C/ 11A	SC 11A.11.3.2	P <b>93</b>	L <b>2</b>	# 263	<i>CI</i> <b>11A</b> CHAPLIN,	SC 11A.2.1 CLINT F	P <b>48</b>	L <b>32</b>	# 118
Comment STA is	<i>Type</i> <b>TR</b> s not just any STA	Comment Status A - It is non-AP STA		non-AP STA	<i>Comment</i> "Gene (Origir	<i>Type</i> <b>E</b> eral" is not an app nally LB105/10 su	Comment Status A ropriate title, as this sub-cla bmitted by Sood, Kapil, dur	use is introducine ing LB105 with II	g a new architecture. ጋ Sood/09)
Suggested Chang	dRemedy ge lines 2, :"STA" to	o "non-AP STA"			Suggested Chang	<i>lRemedy</i> ge "General" to "li	ntroduction"		
Response ACCE	PT	Response Status U			Response ACCE	PT.	Response Status C		
<i>CI</i> <b>11A</b> CHAPLIN,	SC 11A.11.3.2 CLINT F	P <b>93</b>	L <b>32</b>	# 109	C/ 11A Sood, Kap	SC 11A.2.1	P 48	L <b>34</b>	# 345
Comment What (Origin Suggestee	<i>Type</i> <b>E</b> is a "response RIC nally LB98/691 sub <i>dRemedy</i>	Comment Status A "? mitted by Sood, Kapil, durin	ng LB98 with ID \$	Good/113)	Comment "The F entitie: archite similar	<i>Type</i> <b>TR</b> T key holder arcl s" - sounds like e ecture? This relat	Comment Status <b>A</b> hitecture, shown in Figure 1 xists in a vaccum. How doe ionship is missing, and is a	1A-1, describes t s one relate this cause of comple:	the FT key management to the IEEE 802.11 xity. (This is revision of
Chang	ge "RIC response"				Suggester	Remedy			
Response ACCE	PT.	Response Status C			Chang	ge: "The FT key h gement entities a	older architecture, shown ir nd is defined in context of 8	ı Figure 11A-1, de 02.11 basic refer	escribes the FT key ence model (Fig 5-10)."
(Comi	ment reclassified a	s Editorial)			Response ACCE In prop referen	PT. posed change, "F nce model" chang	Response Status U ig 5-10" changed to "see Fi ged to "the IEEE 802.11 bas	gure 5-10 in 5.9", sic reference moc	, and "802.11 basic del".

C/ 11A SC 1 <sup>2</sup> Sood, Kapil	1A.2.1	P <b>48</b>	L <b>34</b>	# 176	C/ <b>11A</b> Sood, Kapil	SC 11A	2.2	P 49	L <b>30</b>	# 174
Comment Type "The FT key ho entities" - sound architecture? The SuggestedRemedy	TR Comm Ider architecture, s ds like exists in a his relationship is	ent Status <b>A</b> shown in Figure 1 <sup>-</sup> vaccum. How does missing, and is a d	A-1, describes the one relate this to cause of complex	ne FT key management o the IEEE 802.11 ity.	Comment 7 Line 26 distribu interact contrad R0KH a	ype <b>TF</b> in the 11A ted among s with 802 ictory? Fin and 802.1>	2.2 clau the R0k 1X to rea t says th are dist	Comment Status <b>A</b> ise reads "the functions of t H and R1KH". Then, line 3 ceive the MSK resulting fro nat 802.1X resides between inct. This needs to be fixed	he IEEE 802.1 0 in same clau m an EAP autl n R0KH and R1	IX Authenticator are ise reads "The R0KH hentication" - sounds 1KH; Second says that
management e	- I key holder arch ntities and is defin	ed in context of 80	Pigure 11A-1, de 02.11 basic refere	nce model (Fig 5-10)."	Suggested	Remedy				
Response ACCEPT. In proposed cha reference mode	Respor ange, "Fig 5-10" cl el" changed to "the	nse Status <b>U</b> nanged to "see Fig IEEE 802.11 bas	gure 5-10 in 5.9", ic reference mod	and "802.11 basic el".	Change 26: "the R0KH a <i>Response</i>	e: Line 30: functions and R1KH	The R0K of the Au	H receives the MSK resulti uthenticator (defined in IEE Response Status U	ng from an EA E 802.1X) are	NP authentication. Line distributed among the
C/ 11A SC 1 <sup>-</sup> Mccann, Stephen	1A.2.2	P <b>49</b>	L <b>26</b>	# 147	ACCEP Page 49 receive	9 line 30 c the MSK.	CIPLE. nanged t	o "The R0KH interacts with	the IEEE 802	.1X Authenticator to
Comment Type Both "IEEE 802	E Comm 2.1X" and "802.1X"	<i>ent Status</i> <b>A</b> ' are referred to.			C/ 11A Sood, Kapil	SC 11A	2.2	P <b>49</b>	L <b>30</b>	# 343
SuggestedRemedy Clarify this term ohter areas of t	n, based on the tra he document whe	ditional use within re this ambiguity a	IEEE 802.11-200 Iso appears.	)7. There are many	Comment 7 Line 26 distribu	<i>ype</i> <b>TF</b> in the 11 <i>F</i> ted among	2.2.2 clau the R0K	Comment Status <b>A</b> ise reads "the functions of t H and R1KH". Then, line 3	he IEEE 802.1 0 in same clau	IX Authenticator are use reads "The R0KH
ACCEPT.	Respon	se Status <b>C</b>	a correct form		contrad R0KH a	lictory? Firand 802.1	st says th are dist	hat 802.1X resides between inct. This needs to be fixed	ROKH and R . (This is revisi	1KH; Second says that ion of similar comment)
According to IE	EE Style Guide, "I		e correct form.		Suggested	Remedy				
					Change 26: "the	e: Line 30: functions	The R0K of the Au	H receives the MSK resulti thenticator (defined in IEE	ng from an EA E 802.1X) are	P authentication. Line distributed among the

R0KH and R1KH"

receive the MSK."

ACCEPT IN PRINCIPLE.

Response Status U

Page 49 line 30 changed to "The R0KH interacts with the IEEE 802.1X Authenticator to

Response

 TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general

 COMMENT STATUS: D/dispatched A/accepted R/rejected
 RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn

 SORT ORDER: Comment ID
 Comment ID # 343

Page 47 of 89 09/27/2007 06:28

Cl 11A Sood, Kapil	SC 11A.2.2	P <b>49</b>	L 31	# 175	<i>CI</i> <b>11A</b> CHAPLIN,	SC 1 CLINT F	1A.2.2	P4	9	L <b>43</b>	# 49
Comment T R1KH is contrad	<i>ype</i> <b>TR</b> s said to be part lictory	Comment Status R of 802.1X and then re-iterat	ed to be interact	ing with 802.1X - sounds	Comment R0KH securi	<i>Type</i> -ID and F ty require	<b>TR</b> R1KH-ID sl ement for a	<i>Comment Status</i> hall be unique with a STA to distinguis	R in the same h between i	e mobility dom multiple entitie	nain. This is a strict es that it will be
SuggestedF Change port. Bo	Remedy e: "The R1KH inte oth the R0KH and	eracts with 802.1X function I R1KH interactions with 80	al block (Fig 5-10 2.1X functional b	) to open the controlled lock occur within the	execu assum (Origir	ting the k options. oally LB9	key hierarc 8/387 subi	hy with. R0KH-ID a mitted by Sood, Ka	and R1KH-I apil, during I	ID uniqueness	s cannot be mere Sood/036)
SME of Response REJEC R1KH is	T T s not stated to be	Response Status U			Chang within within	ge "Each the Mobi the Mobi	R0KH-ID a ility Domai ility Domai	and R1KH-ID is as n." to "Each R0KH n."	sumed to b -ID and R1	e expressed a KH-ID shall be	as a unique identifier e a unique identifier
C/ 11A Sood, Kapil	SC 11A.2.2	P <b>49</b>	L <b>3</b> 1	#  344	Response REJE IEEE 8	CT. 302.11-2	007 has re	Response Status equirements stated	U as assump	otions.	
Comment T R1KH is contrad	<i>ype</i> <b>TR</b> s said to be part lictory. (This is re	Comment Status <b>R</b> of 802.1X and then re-iterat	ed to be interact	ing with 802.1X - sounds	C/ 11A Sood, Kap	SC 1	1A.2.2	P4	9	L <b>43</b>	# 177
SuggestedF Change port. Bo SME of	Remedy e: "The R1KH into th the R0KH and a STA.	eracts with 802.1X function d R1KH interactions with 80	al block (Fig 5-10 2.1X functional b	) to open the controlled lock occur within the	Comment The R strong assure a stror	<i>Type</i> 0KH-ID a security themse ngly desire	TR and R1KH- requireme lves that th red proper	Comment Status ID shall always be ent. Without this un ney are communica ty that this FT secu	R unique with iqueness p ating with th urity protoco	hin the mobilit roperty, the S ne right entity. ol is based up	ty domain. This is a TA and AP cannot This uniqueness is also on.
Response REJEC R1KH is	T s not stated to be	Response Status U			<i>Suggested</i> Chang Mobili	<i>lRemedy</i> je: "Each ty"	/ n R0KH-ID	and R1KH-ID shal	ll be expres	sed as a uniq	ue identifier within the
C/ <b>11A</b> CHAPLIN, (	SC <b>11A.2.2</b> CLINT F	P 49	L <b>35</b>	# 48	Response REJE IEEE 8	CT. 302.11-2	007 has re	Response Status	U as assume	otions.	
Comment T "The Pl be cach (Origina	<i>ype</i> <b>TR</b> MK-R0 in the Aut ned, when 8.5.1.4	Comment Status A thenticator shall be cached 5.1 states that it may be del	a." seems to imp eted (e.g. not ca	y that the PMK-R0 must ched).	C/ 11A Sood, Kap	SC 1	1A.2.2	P4	9	L 44	# [178
Suggestedf Change compor	Remedy to "The PMK-Rinent called the R	0 in the Authenticator shall 0KH."	be derived and n	hay be cached in a	Comment Not ar Suggested	Type iy STA, a IRemedy	TR a non-AP S ⁄	Comment Status STA	A		non-AP STA
Response		Response Status U			Chang	e: "This	identifier is	s communicated to	the non-Al	P STA and oth	ner key"
ACCEP Senten	PT IN PRINCIPLE	Ξ.			Response ACCE	PT.		Response Status	U		
TYPE: TR/te COMMENT	echnical required STATUS: D/disp ER: Comment II	ER/editorial required GR. batched A/accepted R/reje	general required	T/technical E/editorial G/ ISE STATUS: O/open W/v	general vritten C/closed	d U/uns	atisfied Z/	/withdrawn	Comment IE	0# <b>178</b>	Page 48 of 89 09/27/2007 06:28

A/accepted R/rejected JS: 0/oper SORT ORDER: Comment ID

C/ 11A SC 11A.2.2 Malinen, Jouni	P 49	L <b>54</b>	# 303	C/ 11A SC 11A.2.2 HEUBAUM, KARL F	P 50	L 13	# 129	
Comment Type ER Typo	Comment Status A			Comment Type E The letter "K" is missin	Comment Status A ig in "The MIB variables dot11	FTR0eyHolderID	) and"	
SuggestedRemedy Replace "R0H-ID" with	"R0KH-ID".			SuggestedRemedy Change to "The MIB v	ariables dot11FTR0KeyHolder	rID and"		
Response ACCEPT.	Response Status U			Response ACCEPT.	Response Status C			
C/ 11A SC 11A.2.2 Sood, Kapil	P <b>49</b>	L <b>55</b>	#  179	C/ 11A SC 11A.2.2 Sood, Kapil	P 50	L13	#  180	
Comment Type ER Typo on R0H-ID	Comment Status A			Comment Type <b>TR</b> The MIB variable is no	Comment Status A t dot11FTR0eyHolderID" - ma	ybe, a typo		
SuggestedRemedy Change: R0KH-ID				SuggestedRemedy Change: "dot11FTR0k	(eyHolderID"			
Response ACCEPT.	Response Status U			Response ACCEPT.	Response Status U			
C/ 11A SC 11A.2.2 CHAPLIN, CLINT F	P 50	L13	# 119	C/ 11A SC 11A.2.2 Malinen, Jouni	P 50	L13	# 304	
Comment Type E Typo (Originally LB105/11 st	Comment Status A	uring LB105 with	ID Malinen/09)	Comment Type ER Typo	Comment Status A			
SuggestedRemedy Replace "dot11FTR0ey	yHolderID" with "dot11FTR0K	eyHolderID".		Replace "dot11FTR0e	yHolderID" with "dot11FTR0K	eyHolderID".		
Response ACCEPT.	Response Status C			ACCEPT.	Response Status U			

Cl 11A Chaplin, Clint	SC 11A.2.2 F	P <b>50</b>	L17	# 140	C/ 11A SC 11A. Sood, Kapil	2.2	P <b>50</b>	L <b>32</b>	# 346
Comment Typ The docu R1KH. A outside th MIB-base SuggestedRe Incorpora amendme	the <b>TR</b> Iment is deficie default mecha he scope of the ed key transfer emedy the latest revisionent	Comment Status R nt in not specifying some type nism needs to be defined in 1 MAC/PHY, the definition of t should be included in 11r. (su	e of key transfe 1r. While AP-A he MIB is withir Ibmitted by Bill -distribution-via	Key distribution or from the R0KH to the AP communication is In scope of 802.11. A Marshall) a-snmp.doc into the	Comment Type TR "The mutual auther and hold the PMK-R1. If the R1KH, then the R1KH sha channel" - the first obscure - I could r sentence. This is r	Comment ntication between e mutual authentica all bind the same ic sentence is a repe iot unambiguously mentioning a secor	Status <b>A</b> the R0KH and tion is separa lentity with the cat of the prev parse what w id authenicati	d a R1KH authoriz ate from the authe e mutual authenti- rious bullet. The s ras being conveye on scheme that is	Security assumptions zes the R1KH to obtain entication to authorize an cated protection second sentence is ad through the 2nd s not being defined in this
Response REJECT From a sy layer thre changes.	ystem point of e protocol wou Assumed requ	Response Status U view, key distribution should t Id be out of scope for IEEE 8 irrements for the key distribut	be done by a la 02.11r; the PAF ion are given in	yer three protocol. Any R only authorizes MAC 11A.2.2.	draft - why is this r but is out of scope SuggestedRemedy Delete the entire b dependency that t	not an EAP issue, e . (This is revision o pullet, OR, Change his sentence is tryi	entirely. The s of similar comp the second so ng to convey:	econd authorizati ment) entence, as there "The mutual auth	on scheme is desired, seems to be a specific tentication between the
C/ 11A CHAPLIN, CL	SC <b>11A.2.2</b> LINT F	P50	L19	# 51	R0KH and a R1KH scheme is outside channel is separat the authorization in	I authorizes the R1 the scope, but it is e from the authent dentity of R1KH wit	KH to obtain assumed tha ication to auth h the mutual	and hold the PMI at if the mutual au norize an R1KH, t authenticated pro	K-R1. An authorization thentication for secure hen the R1KH shall bind tection channel."
Comment Typ "&include be transfe (Originally	be <b>TR</b> es the PMK-R1 erred which are y LB98/444 su	Comment Status A &" is insufficient as all other of e stated in the PMK-R1 PMKS pomitted by Sood, Kapil, during	components of SA definition". g LB98 with ID 3	SA are also needed to Sood/041)	Response ACCEPT. Entire bullet delete	Response	Status U		
SuggestedRe Change te	emedy o "&includes th	e PMK-R1 PMKSA, &"							
Response		Response Status U							

ACCEPT.

C/ 11A	SC 11A.2.2	P 50	L <b>32</b>	# 181		C/ 11A	SC	11A.2.2	P 50	L <b>35</b>	# 53
Sood, Kapi	I					CHAPLIN,	CLINT	ΓF			
Comment	Type <b>TR</b>	Comment Status A				Comment	Туре	т	Comment Status A		
"The m and ho the PM R1KH, then th channe obscur senten	nutual authentica ld IK-R1. If the mutu e R1KH shall bir e'' - the first sent e - I could not ur ce.	tion between the R0KH and a ual authentication is separate nd the same identity with the r ence is a repeat of the previo nambiguously parse what was	a R1KH authorize from the authent mutual authentica us bullet. The set being conveyed	s the R1KH to obtain ication to authorize ar ted protection cond sentence is through the 2nd	n	Do yo plenty (Origin Suggested Chang Response	u mear of bulle hally LE <i>IReme</i> e je "auth	n "integrity   ets on auth 398/448 su <i>dy</i> henticity" to	protection" when the draft sta entication so I am pretty sur- bmitted by Sood, Kapil, durin "integrity protection". Response Status <b>C</b>	ates "authenticity e by now that au ig LB98 with ID \$	"? We already have thenticity is present! Sood/043)
Suggested	Remedy					ACCE	PT.				
Chang senten authori	e the second ser ce is trying to co zes the R1KH to	ntence, as there seems to be nvey: "The mutual authentica obtain and hold the PMK-R1	a specific depend tion between the	lency that this R0KH and a R1KH thentication for secure	<del>a</del>	<i>Cl</i> <b>11A</b> Sood, Kap	SC il	11A.2.2	P <b>50</b>	L <b>43</b>	# 182
channe the aut	el is separate from horization identit	m the authentication to autho y of R1Kh with the mutual au	rize an R1KH, the thenticated prote	en the R1KH shall bine	d	Comment	Type	TR	Comment Status A	resulting from a	n FAP authentication
Response ACCEI Entire	PT. bullet deleted.	Response Status U				The S intera 802.1 within	1KH ts with coccur the SM	nteracts with 802.1X to r /F of a ST/	open the controlled port. Bo	th the S0KH and	S1KH interactions with
C/ 11A	SC 11A.2.2	P <b>50</b>	L 32	# 52		802.1	l refere	ence model	. This fact is missing.		
CHAPLIN,	CLINT F					Suggestee	Reme	dy			
Comment <sup>-</sup> "&the s (Origin	<i>Type</i> <b>TR</b> same identity with ally LB98/447 su	Comment Status <b>A</b> n the&" is ambiguous. No clea bmitted by Sood, Kapil, durin	ar what the "same Ig LB98 with ID S	e" is referring to? ood/042)		Chang resulti 5-10) within	ie: "The ng from to oper the SN	e S0KH into n an EAP a n the contro /IE of a ST/	eracts with 802.1X functiona uthentication. The S1KH inte led port. Both the S0KH and A."	l block (Fig 5-10) eracts with 802.1 d S1KH interaction	to receive the MSK X functional block (Fig ons with 802.1X occur
Suggested	Remedy					Response			Response Status U		
Chang	e "the same iden	tity used in authentication to	authorize with the	e&"		ACCE	PT.				
Response ACCEI	PT.	Response Status U				In pro block"	chang	change, "Fi ed to "the 8	g 5-10" changed to "see Fig 302.1X functional block"	ure 5-10 in 5.9",	and "802.1X functional

Comment ID # 182

Page 51 of 89

C/ 11A	SC 11A.2.2	P <b>50</b>	L <b>43</b>	# 347	C/ 11A	SC 11	IA.2.2	P <b>50</b>	L <b>5</b>	# 148
Sood, Kap	11				Mccann, S	stephen				
Comment "The S	<i>Type</i> <b>TR</b> S0KH interacts wi	Comment Status A th 802.1X to receive the MSI	K resulting from a	an EAP authentication.	<i>Comment</i> The u	<i>Type</i> se of the t	E term "IEI	Comment Status <b>R</b> EE 802.11" is not required wit	hin this amen	dment
The Sinteract 802.1) within 802.11	1KH cts with 802.1X to K occur the SME of a ST 1 reference mode	o open the controlled port. Bo A." - they interact with the 80 I. This fact is missing. (This i	oth the S0KH and 2.1X functional b s revision of sim	I S1KH interactions with block of Fig 5-10 of ilar comment)	Suggestee Remo Response	IRemedy ve all refe	erences	to IEEE 802.11 Response Status <b>C</b>		
Suggested	Remedy				IEEE	Style Man	nual, clau	use 13.9 states "When referrir	ng to the docu	ment, i.e. the standard
Chang resultii 5-10) t	ge: "The S0KH in ng from an EAP a to open the contro	teracts with 802.1X functiona authentication. The S1KH int olled port. Both the S0KH an	l block (Fig 5-10) eracts with 802.1 d S1KH interaction	) to receive the MSK IX functional block (Fig ons with 802.1X occur	that is docun	published nent stand	d, IEEE dardizes	Std 1234 should be used. Wi , IEEE 1234 should be used."	hen referring t	o the technology that the
within Response	the SME of a ST	A."			C/ 11A CHAPLIN	SC 11 CLINT F	IA.2.3	P 50	L <b>54</b>	# 120
ACCE In prop block	PT. bosed change, "F changed to "the	ig 5-10" changed to "see Fig 802.1X functional block"	ure 5-10 in 5.9",	and "802.1X functional	Comment S0KH manda	<i>Type</i> and S1Kl ated as ha	<b>T</b> H identit aving a s	Comment Status <b>A</b> ies should be defined as a "sh specific identify, otherwise the	nall". Each key security does	Other y holder should be s not work.
C/ 11A	SC 11A.2.2	P <b>50</b>	L <b>5</b>	# 50	(Origii	nally LB10	)5/12 su	bmitted by Sood, Kapil, during	g LB105 with I	D Sood/10)
CHAPLIN,	CLINT F				Suggester	IREMEDY	and S1	KH are identified" to "SOKH ar	nd S1KH shall	l be identified"
Comment	Туре Т	Comment Status A			Deserves	je Sukri				beidentined
Bullet Auther (Origin	2 is too wordy an nticator. nally LB98/391 su	d repetitive. We know from p Ibmitted by Sood, Kapil, durir	previous paragrap	ohs that R1KH is part of Sood/040)	ACCE	PT		Response Status C		
Suggested	Remedy		-		C/ 11A	SC 11	I A.2.3	P 50	L 55	# 121
Chang	e bullet 2 on line	50 as "The R1KH shall deriv	ve and distribute	the GTK to all	CHAPLIN,	CLINT F				
conne	cted STAs."				Comment	Туре	т	Comment Status A		
ACCE	PT.	Response Status <b>C</b>			S0KH key so (Origii	and S1Kl cope shou nally LB10	H are de Ild also b )5/13 su	fined as 2 separate sub-entiti be at the same level. bmitted by Sood, Kapil, during	es within the s g LB105 with I	Supplicant. Therefore, the ID Sood/11)
					Suggestee	Remedy				
					Chang ". SOK parties parties	ge "and sh H shall no s other tha s."	nall not e ot expos an the a	expose the PMK-R0 or PMK-F the PMK-R0 to other parties uthorized S1KH. S1KH shall r	R1 to parties o s, and shall no not expose the	utside the supplicant" to ot expose the PMK-R1 to e PMK-R1 to other
					Response			Response Status C		
					ACCE	PT.				

C/ 11A SC 11A	A.3 P50	L 60	# 327	C/ 11A CHAPLIN	SC 11A.3	P	50 Le	<b>3</b> # 54	
Comment Type T	R Comment Status A			Comment	Type E	Comment Status	s <b>A</b>		
The use of MDIE AP. There is no t bits within the ME standpoint, havin cases to be valid was the original r generality at the comment)	in the beacons/probes is suffic echnical reason or technical jus DIE policy field to indicate FT si g to check multiple fields result ated/conveyed to AP. In addition reason for making MDIE extension expense of TGr implementation	tient to indicate that stification to have MI upport. From STA in is in complexity and on, I do not see TGu bible), and so, no rea in complexity. (This is	FT is supported by the DIE and then additional plementation requires additional error using the MDIE (which son to keep this a revision of similar	Sugge (Origin Suggested Replac frames Response ACCE	sted wording ally LB98/451 s <i>IRemedy</i> ce "Beacons an s". PT.	submitted by Malinen, d Probe Response fra <i>Response Status</i>	, Jouni, during LB ames" with "Beac s <b>C</b>	98 with ID Malinen/34) on and Probe Respons	3e
Clause 11A.3, pg the Beacon and F	3 50, line 61-62 change "The Fa Probe Response frames by incl	ast BSS Transition c uding the MDIE."	apability is advertised in	<i>CI</i> <b>11A</b> CHAPLIN,	SC 11A.3 CLINT F	P	50 L G	<b>55</b> # 56	
Response ACCEPT	Response Status U			Comment "When	<i>Type</i> <b>TR</b> MDIE is used	Comment Status	s <b>A</b> Transition Capab	vility(Fast &" is insufficie	ent. This
C/ 11A SC 11A Sood, Kapil	A.3 P50	L <b>60</b>	# 152	direct s (Origin	statement is mu ally LB98/453	uch clearer to develop submitted by Sood, Ka	pers and eliminate apil, during LB98	en this MDIE is not use is confusion. with ID Sood/044)	3 <b>0.</b> A
Comment Type <b>T</b> The use of MDIE AP. There is no to bits within the ME standpoint, havin cases to be valid was the original r	R Comment Status A in the beacons/probes is suffic echnical reason or technical jus DIE policy field to indicate FT si g to check multiple fields result ated/conveyed to AP. In addition reason for making MDIE extension	DIE . sient to indicate that stification to have MI upport. From STA im is in complexity and on, I do not see TGu ible), and so, no rea	Indication of FT capability FT is supported by the DIE and then additional plementation requires additional error using the MDIE (which son to keep this	Suggested Chang to zerc Response ACCE Statem	IRemedy e "When Fast I o, then all other PT IN PRINCIF nent deleted	BSS Transition over a bits of the Fast BSS ( <i>Response Status</i> PLE.	ir and Fast BSS 1 Capability and Po : U	ransition over DS are l licy field shall be ignore	both set ed."
generality at the	expense of TGr implementatior	o complexity.		C/ 11A	SC 11A.3	P	50 L G	<b>55</b> # 55	
Clause 11A.3, pg	50, line 61-62 change "The Fa	ast BSS Transition c	apability is advertised in	CHAPLIN,	CLINT F	Comment Status	sΔ		
Response ACCEPT	Response Status U	uding the MDIE.		MDIE i IE for a (Origin	is only included a case where F ally LB98/452 s	if FT is supported, so T is not supported. submitted by Malinen,	o there is no need , Jouni, during LB	for specifying contents 98 with ID Malinen/10)	s of the
				Suggested	Remedy				
				Remov Transit the Fa Transit	ve "When MDIE tion over air an st BSS Capabil tion is supporte	is used without the F d Fast BSS Transitior ity and Policy field sh d, at least" with "At le	Fast BSS Transition over DS both se all be ignored." In ast" on line 29.	on Capability (Fast BSS t to zero), then all other addition, replace "If Fa	S r bits of ast BSS
				Response	DT	Response Status	U		

Bill Marshall, ATT Labs Research

Sood, Kapil	SC 11A.4.2	P <b>51</b>	L <b>29</b>	# 183
Comment Ty Not any	<i>rpe <b>TR</b></i> STA, a non-AP	Comment Status A STA		non-AP STA
SuggestedRe Change:	<i>emedy</i> where the SME	of the non-AP STA enabl	es	
Response ACCEP1	Г.	Response Status U		
C/ 11A Sood, Kapil	SC 11A.4.2	P51	L <b>32</b>	# 348
Comment Ty	vpe TR	Comment Status A		
"Reasso this mea	ciation frames a n? (This is revis	re supported to enable FT ion of similar comment)	and non-FT APs	in an ESS." - what does
SuggestedR Delete th	<i>emedy</i> nis line, or clarify	1		
Response		Response Status II		
ACCEPT In additio Domain	Г on to Associatio Association to е	n frames, Reassociation fr nable both FT and non-FT	ames are support APs to be preser	ed in the Initial Mobility It in a single ESS.
ACCEPT In additio Domain <i>Cl</i> <b>11A</b> Sood, Kapil	T on to Associatio Association to e SC <b>11A.4.2</b>	n frames, Reassociation fr nable both FT and non-FT P <b>51</b>	ames are support APs to be preser L 32	ed in the Initial Mobility at in a single ESS. # 184
ACCEPT In additic Domain C/ 11A Sood, Kapil Comment Ty "Reasso this mea SuggestedR Delete th	Ton to Associatio Association to e SC 11A.4.2 ype TR ciation frames a n? emedy his line, or clarify	n frames, Reassociation fr nable both FT and non-FT <b>P51</b> <i>Comment Status</i> <b>A</b> are supported to enable FT	ames are support APs to be preser <b><i>L</i> 32</b> and non-FT APs	ed in the Initial Mobility at in a single ESS. # <u>184</u> <i>Other</i> in an ESS." - what does

C/ 11A	SC 11A.4.2	P <b>51</b>	L35	# 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 KeyLlfetime, 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			
REJEC The rec 11A.4.1	CT. quirement to perf 2, page 54 line 21	orm another Initial Mobility	Domain Associati	on is already stated	in
C/ 11A	SC 11A.4.2	P <b>5</b> 1	L <b>35</b>	# 193	
Sood, Kapi	I				
Comment 7	Type <b>TR</b>	Comment Status R			
The sn	ecification does r	ot specify if a non-AP STA	can execute an I	nitial Mobility Domai	in

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 KeyLlfetime, 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.

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general Page 54 of 89 COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn Comment ID # 193 SORT ORDER: Comment ID

09/27/2007 06:28

Submission

Bill Marshall, ATT Labs Research

C/ <b>11A</b> CHAPLIN,	SC <b>11A.4.2</b> CLINT F	P51	L <b>41</b>	# 57	Cl 11A SC 11A Sood, Kapil	.4.2	P <b>52</b>	L 38	# 202
Comment 7 "&a mo specifio (Origina	<i>Type</i> <b>TR</b> odified 4-Way Ha cation has been ally LB98/458 s	Comment Status A andshake" - what does this m using "FT 4-Way Handshake ubmitted by Sood, Kapil, durin	ean? Where is ti " in previous cla ng LB98 with ID	nis defined? This auses. Sood/045)	Comment Type TF STA is not just an SuggestedRemedy Change on line 3	<b>R</b> y STA -	Comment Status R it is a non-AP STA	0. "AP -> non	non-AP STA
Suggested Change Response ACCEF	Remedy e "&the FT 4-W	ay Handshake" Response Status U			Response REJECT. Clause 11A is spe is no ambiguity in	ecific in the use	AP STA -> AP and on line 3 Response Status U applying only to an infrastruc of the term STA.	s. AP -> non-	d in such situations there
C/ 11A Sood, Kapi	SC 11A.4.2	P51	L <b>4</b> 1	# 189	Cl 11A SC 11A Sood, Kapil	.4.2	P <b>52</b>	L 53	# 203
Comment 7 The "m	<i>Type</i> <b>TR</b> nodified" 4-way I	Comment Status A nandshake is referred to as F	Γ4-way handsha	ake elsewhere in this	Comment Type <b>TF</b> STA is not just an	<b>R</b> y STA -	<i>Comment Status</i> <b>R</b> it is a non-AP STA		non-AP STA
docum Suggested Change Response ACCEF	ent. <i>Remedy</i> e "modified 4-w PT.	ay handshake" to "FT 4-way h <i>Response Status</i> <b>U</b>	andshake"		SuggestedRemedy Change on line 53 Response REJECT. Clause 11A is spe is no ambiguity in	3: "non-,	AP STA -> AP" and on line 5 <i>Response Status</i> <b>U</b> applying only to an infrastruc	4: "AP -> non- cture BSS, and	-AP STA" d in such situations there
C/ 11A CHAPLIN, COmment T	SC <b>11A.4.2</b> CLINT F <i>Type</i> <b>E</b>	P52 Comment Status A	L15	# <u> 58</u>	Cl 11A SC 11A Sood, Kapil Comment Type TF	.4.2 R	P 53 Comment Status A	L13	# 186
(Origina Suggested Replac Response ACCEF	ally LB98/459 s <i>Remedy</i> e "Anonce" with PT.	ubmitted by Malinen, Jouni, d n "ANonce" in Figure 204b. <i>Response Status</i> <b>C</b>	uring LB98 with	ID Malinen/36)	Supplicant is not a elsewhere in this SuggestedRemedy Make this docume Response ACCEPT.	the mos docume ent cons	it precise component that doe ent. sistent by changing: "The S0I <i>Response Status</i> <b>U</b>	es EAP. It is S KH shall use tl	OKH, as defined he value of R0KH-ID&"

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID Comment ID 186

Page 55 of 89 09/27/2007 06:28

<i>Cl</i> <b>11A</b> Sood, Kapil	SC 11A.4.2	P 53	L 19	# 188	C/ <b>11A</b> SC <sup>2</sup> CHAPLIN, CLINT
Comment T The key Mobility	ype <b>TR</b> hierarchy in RC Domain ID => <sup>-</sup>	Comment Status A IXH must exist for the same n IHEN only with the key hierar	on-AP STA and chy be deleted.	I within the same	Comment Type EAPOL-Key fr Message) par (Originally LB
Change	: "If a key hiera (havind same I	rchy already exists for this nor MDID), the R0KH shall delete	n-AP STA belon the existing"	iging to same Mobility	SuggestedRemed Replace "P, "
Response ACCEP	т	Response Status U			Response ACCEPT.
<i>Cl</i> <b>11A</b> Sood, Kapil	SC 11A.4.2	P 53	L 19	# 187	C/ <b>11A</b> SC Sood, Kapil
Comment T Not any	<i>ype</i> <b>TR</b> STA, a non-AP	Comment Status A STA		non-AP STA	<i>Comment Type</i> Insert a " " (sp
SuggestedF Change	Remedy :: "exists for this	non-AP STA, the R0KH"			SuggestedRemed Change "TIE[I
Response ACCEP	T	Response Status U	/ 19	# 250	Response REJECT. "TIE[KeyLifeti (also without a
Sood, Kapil	30 TT <b>A.4.2</b>	F 33	L 19	# 350	
Comment T	ype TR	Comment Status A			Sood, Kapil
The key Mobility similar o	v hierarchy in R0 Domain ID => comment)	NKH must exist for the same n THEN only with the key hierar	on-AP STA and chy be deleted.	d within the same (This is revision of	Comment Type "The FTIE sha have nonce a
Change	: "If a key hieral	rchy already exists for this nor	n-AP STA belon	iging to same Mobility	MIC values of specify the fie
Response	(navinu same i		the existing		SuggestedRemed
ACCEP	Т				Change: "The count of zero of zero."
					Response
					ACCEPT.

C/ <b>11A</b> CHAPLIN, C	SC <b>11A.4.2</b> CLINT F	P53	L 41	# 59			
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)							
SuggestedF	Remedy						
Replace	e "P, " with "P, 0,	" in all four EAPOL-Key fra	imes to add the n	ew SM parameter.			
Response ACCEP	Ϋ́Τ.	Response Status U					
Cl 11A Sood, Kapil	SC 11A.4.2	P <b>53</b>	L <b>47</b>	# 190			
<i>Comment T</i> Insert a	<i>ype</i> <b>ER</b> " " (space) betw	Comment Status <b>R</b> een KeyLifetime, as elsewh	nere it is referred	as "Key Lifetime"			
SuggestedF Change	Remedy e "TIE[Key Lifetim	ne]"					
Response		Response Status U					
REJEC "TIE[Ke (also wi	T. yLifetime]" is cor thout a space)	nsistently used in the docun	nent, as is "TIE[R	eassociationDeadlin	e]"		
Cl 11A Sood, Kapil	SC 11A.4.2	P <b>53</b>	L <b>8</b>	# 185			
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.							
Suggested	Remedy						
Change count o of zero.	e: "The FTIE shal f zero (i.e., no Mi "	I set MIC Control field as ze IC present), and have Anon	ero to indicate MI ace, Snonce, and	C information elemer MIC fields set to valu	nt Jes		
Response		Response Status U					

 TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general
 Page 56 of 89

 COMMENT STATUS: D/dispatched A/accepted R/rejected
 RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn
 Page 56 of 89

 SORT ORDER: Comment ID
 Comment ID # 185
 09/27/2007 06:28

Bill Marshall, ATT Labs Research

C/ 11A Sood, Kap	SC <b>11A.4.2</b> il	P 53	L 8	# 349	
Comment "The F have r MIC va specify	<i>Type</i> <b>TR</b> TIE shall indicate nonce and alues of zero." - T y the fields and va	Comment Status A a MIC information element his statement is not accurate alues. (This is revision of sim	count of zero (i.e e as it does not e illar comment)	e., no MIC present), a exactly and correctly	ind
Suggested Chang count of zero	<i>IRemedy</i> ge: "The FTIE sha of zero (i.e., no M o."	II set MIC Control field as ze IC present), and have Anon	ero to indicate MI ce, Snonce, and	C information elemer MIC fields set to valu	nt Jes
Response ACCE	PT.	Response Status U			
<i>CI</i> <b>11A</b> CHAPLIN,	SC <b>11A.4.2</b> CLINT F	P <b>54</b>	L17	# 60	
Comment "Once ensure Key Li value 2 sepa (Origir	Type <b>TR</b> the IEEE 802.1X that the lifetime fetime TIE." - The of PTK is set in the arete sentences. nally LB98/473 su	Comment Status A controlled port is open, the of the PTKSA is no longer the re is no connection between the timer. This implied connection bmitted by Sood, Kapil, during	PTK key lifetime han the value pro hat the controlled p tion is incorrect, ng LB98 with ID	timer is initiated to ovided in the Messag oort ensuring the corre so clearly de-lineate Sood/049)	e 3 ect in

#### 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"

<i>Cl</i> <b>11A</b> Sood, Kapi	SC 11A.4.2	P54	L <b>21</b>	# 192
Comment T All refe	<i>Type</i> <b>TR</b> rences to STA in	Comment Status A lines 21-29 are for a non-Al	P STA.	non-AP STA
Suggested Change	<i>Remedy</i> e in lines 21-29: "	STA" to "non-AP STA"		
Response ACCEF	РТ	Response Status U		
<i>Cl</i> <b>11A</b> Sood, Kapi	SC 11A.4.2	P <b>54</b>	L <b>25</b>	# 351
Comment 7	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."

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Comment ID # 351

Page 57 of 89 09/27/2007 06:28

<i>Cl</i> <b>11A</b> Sood, Kapil	SC 11A.4.2	P <b>54</b>	L <b>25</b>	# 191		Cl 11A SC 11A Sood, Kapil
Comment Ty "If the A ("Previo no longe perform Mobility (disasso with whi with this operable detailed success	P sends a Deau us authenticatio er valid"), then to the FT Initial Domain Associa oc/deauth) to a r ch the non-AP S AP using the e e, and neither ha description of a ful and failed sta	Comment Status <b>A</b> inthentication or Disassociation o continue its association in the ation procedures." What happ ion-AP STA with a reason co STA performed Initial MD Ass xisting key hierarchy? This sp as this amendment specified Il error scenarios, as this wor andard.	n frame to the S he Mobility Dom bens when an A de other than 2' soc, then can the becification has any error brancl uld make all the	TA with reason co ain the STA shall P sends a disconn If this AP is the o STA perform an I not been proven in nes - I would like to difference between	Other de 2 ect ne =T tter- o see n a	Comment Type TF STA is not just an SuggestedRemedy Change on line 17 Response REJECT. Clause 11A is spe is no ambiguity in C/ 11A SC 11A
SuggestedR At the ei the non- protocol Response ACCEP At end c	emedy nd of this senter AP STA, then th T IN PRINCIPLE of sentence, inse	nce, insert: "If an AP sends a ne non-AP STA may reassoc <i>Response Status</i> <b>U</b> E ert "with any AP in the Mobilit	deauthenticatio iate with the sar y Domain."	n and disassociation ne AP using the F	on to T	Comment Type E There's been a pa hasn't occurred in (Originally LB105) SuggestedRemedy Rename to match
Cl 11A Sood, Kapil Comment Ty STA is r SuggestedR Change Response REJECT	SC 11A.4.3 ype TR not just any STA <i>Remedy</i> on line 1: "non-	P55 Comment Status R - it is a non-AP STA AP STA -> AP" and on line 2 Response Status U	L1 : "AP -> non-AP	# <u>204</u> non-A STA"	P STA	Response REJECT. "FT" is defined as IEEE Style Manua Clause and subcl appearing in titles Note that the doct interpretation of th

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.

C/ 11A	SC 11A.4.3	P 55	L17	# 205
Sood, Kapil				
Comment Tvi	pe TR	Comment Status R		non-AP STA

STA is not just any STA - it is a non-AP STA

Change on line 17: "non-AP STA -> AP" and on line 18: "AP -> non-AP STA"

Response	Response Status	U
----------	-----------------	---

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.

C/ 11A	SC 11A.5	P 55	L <b>40</b>	# 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)

Rename to match changes make in the body text.

Response Status C

"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.

Comment ID # 122

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.

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Page 58 of 89 09/27/2007 06:28

C/ 11A CHAPLIN,	SC <b>11A.5.1</b> CLINT F	P <b>55</b>	L <b>46</b>	# 61	<i>Cl</i> <b>11A</b> Malinen, Jo	SC <b>11A.5.2</b> puni	P 56	L <b>22</b>	# 322		
Comment What o (Origin	<i>Type</i> <b>TR</b> does the word "sy hally LB98/474 su	Comment Status A stems" refer to? bmitted by Lemberger, Uriel,	during LB98 wit	h ID Lemberger/10)	Comment Incons	<i>Type</i> <b>ER</b> istent spelling c	Comment Status A of SNonce.				
Suggested Chang	IRemedy je "systems" to sp	pecific STA and/or AP as requ	uired		Replace "Snonce" with "SNonce" on page 56 line 22 (in Figure 11A-4) and on page 58 l 20 (in Figure 11A-5).						
Response ACCE Chang	PT. jed to "STAs"	Response Status U			Response ACCEI	PT.	Response Status U				
C/ 11A	SC 11A.5.1	P <b>55</b>	L <b>46</b>	# 62	C/ <b>11A</b> Sood, Kapi	SC 11A.5.2	P 56	L <b>34</b>	# 353		
Comment What i (Origir	<i>Type</i> <b>TR</b> s the word "syste nally LB98/475 su	Comment Status <b>A</b> m" referring to? bmitted by Sood, Kapil, durin	g LB98 with ID S	Sood/050)	Comment <sup>®</sup> "specif Seque similar	Type <b>TR</b> y the PTKSA" - nce to indicate comment)	Comment Status R what does this mean? The ST the PMK-R0 SA and then deriv	<sup>-</sup> A and AP use t ve the PTKSA. (	he Authentication This is revision of		
Suggested Chang	<i>IRemedy</i> je "System" to "S <sup>-</sup>	ΓΑ"			Suggested Chang	Remedy e: "specify the F	PMKR0Name"				
Response ACCE Chang	PT. jed to "STAs"	Response Status U			Response REJEC The PT needed	CT. IKSA includes r d to derive it.	Response Status U numerous items (see 8.4.1.1.2	), and more tha	n just PMKR0Name is		
C/ <b>11A</b> CHAPLIN,	SC 11A.5.2 CLINT F	P <b>56</b>	L <b>21</b>	# 63	C/ 11A	SC 11A.5.2	P <b>56</b>	L 34	# 194		
Comment Type E Comment Status A Typo (Originally LB98/477 submitted by Malinen, Jouni, during LB98 with ID Malinen/37)				Sood, Kapil Comment Type TR Comment Status R "specify the PTKSA" - what does this mean? The STA and AP use the Authentication							
Suggested Replac	<i>IRemedy</i> ce "Snonce" with	"SNonce" in Figure 204d.			Seque Suggested	nce to indicate	the PMK-RU SA and then deriv	/e the PTKSA.			
Response ACCE	PT.	Response Status C			Chang <i>Response</i> REJEC The P <sup>T</sup> needed	e: "specify the F CT. FKSA includes r d to derive it.	PMKR0Name" <i>Response Status</i> <b>U</b> numerous items (see 8.4.1.1.2	), and more that	n just PMKR0Name is		

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID Comment ID 194

Submission

Bill Marshall, ATT Labs Research

C/ 11A CHAPLIN	SC <b>11A.5.2</b> CLINT F	P <b>56</b>	L <b>34</b>	# 64	C/ 11A Sood Kapi	SC 11	A.5.2	P <b>56</b>	L <b>50</b>	# 367	
Comment <sup>-</sup> Isn't F <sup>-</sup> "specif	Type <b>T</b> Authentication set the PTKSA"? Ho	Comment Status A equence used to derive PTF w does it "specify" the PTK	( and generate P SA? Or is this ຣເ	TKSA; not just to pposed to "specify"	Comment Comment The Finon-Al	<i>Type</i> <b>1</b> protocols STA initi	r <b>R</b> s do not iates an	Comment Status R define the behavior of non-A FT to its current AP. There of to non AP STA looking its of	\P STA or AP ir can be scenario	n the scenario when a s due to buggy non-AP	
(Origin	ally LB98/478 sub	mitted by Malinen, Jouni, d	uring LB98 with I	D Malinen/38)	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						
Replac	Remedy e "to specify the P	TKSA" with "to specify the	PMK-R1 SA".		STA. ( Suggested	This is rev <i>Remedy</i>	ision of	similar comment)	·		
Response ACCEI	PT.	Response Status C			Insert i STA in the AP	n Clause itiates an shall sen	11A.5.2 FT to ar d a disa	page 57 line 6 (also on 11A AP that currently holds ass ssociate request to that non-	.5.3, page 58, li ociation state fo -AP STA with si	ne 65): "When a non-AP or that non-AP STA, then tatus code 57 ("New FT	
C/ 11A Sood, Kapi	SC 11A.5.2	P 56	L <b>43</b>	# 201	Initiate AP".	d to same	e AP"). C	Clause 7.3.1.9, page 8, line 3	2 insert "57 Nev	w FT Initiated to same	
Comment	Type TR	Comment Status R		non-AP STA	Response			Response Status U			
STA is	not just any STA	it is a non-AP STA			REJECT P802.11r D7.0 allows the STA to initiate a Fast BSS Transition to its currently associate					s currently associated AP.	
Suggested Chang	SuggestedRemedy Change on line 43: "non-AP STA -> Target AP" and on line 46: "Target AP -> non-AP STA"						As a clarification in the draft, insert a paragraph break after the second sentence of the paragraph beginning "I hop a successful reassociation" on page 68 line 48. Change first				
Response REJEC	CT.	Response Status U	icture BSS and	in such situations there	senten reasso	ce of the i ciation, th	new par le STA s	agraph from "The STA shall hall delete"	delete" to "Upo	n a successful	
is no a	mbiguity in the use	e of the term STA.	2012.0 D00, and								

Page 60 of 89 09/27/2007 06:28

Comment ID # 367

Cl 11A Sood, Kapil	SC	11A.5.2	P <b>56</b>	L <b>50</b>	# 226	C/ 11A Sood, Kapi	SC I	11A.5.2		P <b>57</b>	L 10	# 355
Comment T	уре	TR	Comment Status	ł	Roam-to-s	self Comment	Гуре	TR	Comment	Status R		STA behavio
The FT non-AP implem AP STA state - t STA.	protoc STA i entatio A not h hat a r	ols do not nitiates an ns or due aving proc non-AP ST	define the behavior of FT to its current AP. 1 to non-AP STA looking essed the disconnect, A chooses to FT to an	f non-AP STA or Al There can be scena g its current conner or AP not having o AP that currently I	P in the scenario when a arios due to buggy non-AF ction state, or due to non- cleaned up non-AP STA's holds state for this non-AF	The ca defined same / know it failure	se of v I. Prob AP. Or the no cases.	vhen an A lems occu , STA may on-AP STA (This is re dv	uthentication ir when a STA never come A is coming ba evision of simi	is failed, then w A is rejected fro back to that AF ack. This stand ilar comment)	vhat is a STA sup m an AP but kee P. Both the AP an ard should define	oposed to do is not ps coming back to the id non-AP STA should e explicit behavior of
Suggested	Remed	'y				Clause	11A 5	2 nage 5	7 line 5: "For	FT Authenticati	on Request failu	res described above a
Insert ir STA ini the AP Initiated AP".	n Claus tiates a shall s to sai	se 11A.5.2 an FT to ar end a disa me AP"). C	page 57 line 6 (also on AP that currently hole associate request to the Clause 7.3.1.9, page 8,	n 11A.5.3, page 58 ds association stat at non-AP STA with , line 32 insert "57 l	8, line 65): "When a non-A e for that non-AP STA, the n status code 57 ("New FT New FT Initiated to same	AP non-AF en correct T channe the sar Table	P STA ing the el cond ne AP 7-23, C	may re-iss indicated litions"), th for a time clause 7.3	ue a new FT error. If the A en a non-AP indicated by t 1.9, page 8 li	Authentication AP rejected with STA shall not r the reassociation ne 30 "56 FT fa	Request to the s status code 56 etry the FT Authe on deadline time. ailed due to poor	ame target AP after ("FT failed due to poor entication Request with " Insert a new row in channel conditions."
Response			Response Status	J		Response			Response	Status U		
REJEC P802.1 As a cla paragra	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						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.					STA in these situations. e situation described in
senteno	ce of the ciation,	the STA s	agraph from "The STA shall delete"	A shall delete" to "U	lpon a successful	C/ <b>11A</b> Sood, Kapi	SC	11A.5.2		P <b>57</b>	L <b>24</b>	# 197
C/ 11A	SC	11A.5.2	P <b>57</b>	L10	#  196	Comment	Гуре	TR	Comment	Status R		STA behavio
Sood, Kapil						Anothe	r case	is when a	STA times o	ut trying to sen	d an FT Authenti	cation Request to the
Comment T	уре	TR	Comment Status	N N	STA behav	/ior AP - th	AP - then, what is the desired action for a STA? The STA may be timing out because of multiple reasons include annual conditions, collisions, interference, etc. What is the rate at					
The cas defined same A	se of w . Probl .P. Or,	hen an Au ems occui STA may	thentication is failed, t when a STA is rejected never come back to the	hen what is a STA ed from an AP but hat AP. Both the AF	supposed to do is not keeps coming back to the and STA should know if	which to importa AP for	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.					ges? Setting a rate is but then try to use the nd other STAs.
the STA	A IS COI	ning back	. This standard should	define explicit beh	avior of failure cases.	Suggested	Reme	dy				
Suggested	Remed	У				Insert i	n Clau	se 11A.5.	2 page 57 line	30: "The non-	AP STA and AP	shall use their desired
Clause STA ma	11A.5 ay retry	2 page 57 / the FT A	' line 5: "Subsequent to uthentication Request	o an FT Authentica with the correct set	tion Request rejection, a t of parameters."	Tx data transm	a rate a ission	as the rate 5 times be	for sending F fore dropping	T Authentication the Tx rate. The Tx rate Tx r	on messages. Ea he Tx rate shall n	ach entity may retry the not be dropped beyond
Response			Response Status	J		one rat	e lowe	er than what	at is intended	to be used for	data packets." Si	milar sentence needs to
ACCEP	T IN F		an ET Authentication	Request rejection	a STA may retry the FT	Response			Response	Status <b>U</b>		
Authorit	tication	Request	" The STA has no way	of knowing the "ci	irroct cot" of parameters		т		•			

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general		Page 61 of 89
COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID	Comment ID # 197	09/27/2007 06:28
Submission		

Bill Marshall, ATT Labs Research

C/ 11A	SC	11A.5.2	P 57	L <b>24</b>	# 356
Sood, Kapil					
Comment T	уре	TR	Comment Status R		STA behavior
Anothou		ia when a	CTA times out trains to cond	on CT Authontic	ation Deguast to the

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

REJECT.

This case is already covered in the paragraph starting on page 57 line 24.

Response Status U

C/ 11A	SC 11A.5.2	P <b>57</b>	L <b>5</b>	# 195
Sood, Kapil				

Comment Type TR Comment Status A

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 l'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 <a href="https://www.awa.com">AWA</a> ("R0KH unreachable").

C/ 11A	SC 11A.5.2	P <b>57</b>	L <b>5</b>	# 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 Status U

Response

### 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").

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

PMK-R1 latency for pull

Comment ID # 354



#### 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 Reguest shall be the MDIE that was negotiated by the non-AP STA in the Initial Mobility Domain association". 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.

C/ 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.

#### SuggestedRemedv

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.

C/ 11A	SC 11A	.5.3	P 58	L 20	# 65	
CHAPLIN,	CLINT F					
Comment <sup>-</sup>	Туре Е	Comment Sta	tus A			
Typo (Origin	ally LB98/4	85 submitted by Maline	en, Jouni, d	during LB98 with I	D Malinen/39)	
Suggested	Remedy					
Replac	e "Snonce'	' with "SNonce" in Figu	re 204e.			
Response		Response Stat	us <b>C</b>			
ACCE	>Τ.					

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

C/ 11A	SC 11A.5.3	B P58	L 36	# 199	C/ 11A	SC 11	A.5.3	P 58	L <b>45</b>	# 123
Sood, Kap	41				CHAPLIN,	CLINIF				
Comment	Type <b>TR</b>	Comment Status A			Comment	Туре Е		Comment Status A		
The S <sup>-</sup> clarifie	TA and Target. d here.	AP are addresses of these er	ntities as defined in	7.4.7. This should be	"(Actio adequ	n frame of ate - i.e. it	categ is not	ory[#488] Fast BSS Transition definitive.	n)" - I'm not su	re the change was
Suggested	Remedy				(Origir	ally LB10	5/15 su	bmitted by Stephens, Adrian,	during LB105	with ID Stephens/11)
Chang	ge Clause 11A.	5.3 page 58 lines 36-41 in th	e parameter list on	ly: "STA" to "STA	Suggestea	Remedy				
Addres	ss" and "Targe	tAP" to "Target AP Address"			Quote	both cates	gory ar	nd action		
Response		Response Status U			Response			Response Status C		
ACCE	PT.				ACCE	PT.				
C/ 11A	SC 11A.5.3	B P58	L 36	# 200	Chang Transi	ed to "Act tion Reque	ion frai est". Si	me of category Fast BSS Trai milar change at line 49.	nsition and Act	tion field Fast BSS
Sood, Kap	il				C/ 11A	SC 11	<b>453</b>	P58	/ 65	# 358
Comment	Type TR	Comment Status R		non-AP STA	Sood, Kap	il UC III		1.00	200	# 000
STA is	s not just any S	TA - it is a non-AP STA			Comment		R	Comment Status A		PMK-R1 latency for pull
Suggested	Remedy				The in	valid PMK	R0Nar	ne rejection should not be a "	may" This sho	uld be a "shall" as the
Chang	ge on line 36: "I	non-AP STA -> Target AP" a	nd on line 39: "Targ	get AP -> non-AP STA"	STA n	eeds to kn	ow exa	actly under what conditions w	as the Auth fai	led. No inter-op has been
Response		Response Status U			done f	or this pro ent)	tocol, s	so I'd like to see well defined f	ailure cases. (	This is revision of similar
REJE	CT.	a ta anna bitan an bata an tafaa		to such alternations thereas	Suaaestea	Remedv				
is no a	ambiguity in the	e use of the term STA.	structure BSS, and	In such situations there	Chang	e "the AP	shall r	eject the Authentication Requ	est with status	code 53 ("Invalid
C/ 11A	SC 11A.5.3	B P 58	L <b>43</b>	# 206	Response	, ).		Response Status U		
Sood, Kap	il				ACCE	PT IN PRI	NCIPL	, E		
<i>Comment</i> STA is	<i>Type</i> <b>TR</b> s not just any S	Comment Status A TA - it is a non-AP STA		non-AP STA	If the F Target Auther	RSNIE in to AP has d ntication R	ne Auti etermii eauesi	nentication Request frame co ned that it is an invalid PMKR t with status code 53 ("Invalid	ntains an inval 0Name, the Al PMKID"). If th	lid PMKR0Name, and the P shall reject the e Target AP has not
Suggested Lines	<i>Remedy</i> 42-51 change:	"STA" to "non-AP STA"			determ model	and the A	her the P doe	e PMKR0Name is valid (e.g., s not wait for the PMK-R1 key equest with status code 0. If t	key distribution / from the R0K	n is done via a "pull" (H), the AP may respond R0KH is not, reachable
Response ACCE	PT	Response Status U			the AP unread	shall resp hable").	ond to	the Authentication Request	with status cod	le <ana> ("R0KH</ana>

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Page 64 of 89 09/27/2007 06:28

Comment ID # 358

Cl 11A Sood, Kapil	SC 11A.5.3	P <b>58</b>	L <b>65</b>	# 207	C/ <b>11A</b> Sood, Kap					
Comment Ty The inva STA nee done for	ype <b>TR</b> alid PMKR0Nam eds to know exa r this protocol, so	Comment Status A e rejection should not be a " ctly under what conditions w o I'd like to see well defined f	may". This sho as the Auth fai failure cases.	<i>PMK-R1 latency for pull</i> build be a "shall" as the iled. No inter-op has been	Comment What i The so anothe					
SuggestedR Change PMKID	Remedy "the AP shall re ).	ject the Authentication Requ	est with status	code 53 ("Invalid	same from th source					
Response ACCEP If the RS Target A Authent determin model, a to the A the AP	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").</ana>									
Cl 11A Sood, Kapil	SC 11A.5.3	P 59	L1	# 208	Response REJE( The ba					
Comment Ty STA is r	ype <b>TR</b> not just any STA	Comment Status A - it is a non-AP STA		non-AP STA	C/ 11A Sood, Kap					
Line 1 c Response ACCEP	hange: "STA" to T	"non-AP STA" Response Status U			Comment What i The so anothe					
C/ 11A Sood, Kapil Comment Ty	SC 11A.5.3	P59 Comment Status A	L 10	# 209 non-AP STA	and in Suggested Insert multipl Target					
STAIST SuggestedR Line 10- Line 18 Response	not just any STA Remedy 12 change 2 oco change "non-AF	- It is a non-AP STA curances of "STA" to "non-A STA" Response Status	P STA". Line 1	3: change "non-AP STA".	Response REJEC The ba Both c					
ACCEP	Т									

C/ 11A	SC 11A.5.3	P 59	L18	# 364	
Sood, Kapi	I				

Comment Status R

Tvpe TR

STA behavior

if multiple FT Request frames are issued by a non-AP STA to the same Target AP. cenario being that a response to first never came back, and then non-AP STA issued er FT Request. Will both be accepted by the Target AP? Will second one be rejected. so, with what status code? Also, it is very important for a non-AP STA to commit to the SNonce value - as to avoid a flooding attack on that AP. Seeing the same SNonce he non-AP STA tells the target Ap that these are not floods - just retries. Of course, no e authenication can be done until 3rd message, but commiting to an SNonce for a fic time avoids AP flooding attacks. (This is revision of similar comment)

### dRemedv

a new line at line 24: "The non-AP STA shall commit to the same SNonce for ting the FT protocol with the target AP. If multiple FT Requests are sent to the target nen the non-AP STA shall use the same SNonce value for all FT Requests issued the time specified by the reassociation deadline. If one FT Request has been ssed at the Target AP, and multiple FT Requests are received at the Target AP from ame non-AP STA, then the Target AP shall reject the subsequent FT Request with code 56 ("over-the-DS Limit")."

#### Response Status U СТ ase specification is rightly silent on the proper behavior of the STA in these situations. changes proposed will lead to critical failures of the STA in certain roaming situations. SC 11A.5.3 P59 L18 # 217 TR Comment Status R Type if multiple FT Request frames are issued by a non-AP STA to the same Target AP. cenario being that a response to first never came back, and then non-AP STA issued er FT Request. Will both be accepted by the Target AP? Will second one be rejected. so, with what status code? dRemedy

a new line at line 24: "If one FT Request has been processed at the Target AP, and le FT Requests are received at the Target AP from the same non-AP STA, then the AP shall reject the subsequent FT Request with status code 56 ("over-the-DS Limit")."

Response Status U

### СТ

ase specification is rightly silent on the proper behavior of the STA in these situations. changes proposed will lead to critical failures of the STA in certain roaming situations.

Comment ID # 217

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general

COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Page 65 of 89 09/27/2007 06:28

C/ 11A	SC 11A.5.3	P 59	L19	# 359	ŀ
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")."

C/ 11A	SC 11A.5.3	P <b>59</b>	L 19	# 210
Sood, Kapil				

Comment Status A

#### Comment Type TR

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")."

C/ 11A	SC 11A.5.4	P 59	L <b>26</b>	# 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

Resource limit

C/ 11A SC 1	1A.5.4	P 59	L <b>26</b>	# 360	C/ 11A	SC 11A.5.5		P <b>60</b>	L <b>25</b>	# 361
Sood, Kapil					Sood, Kapi	I				
Comment Type	TR Comme	ent Status R			Comment 7	Type <b>TR</b>	Comment St	atus R		
The over-the-a 11A.5.2 with th revision of simi	ir procedures define e exception of non- ilar comment)	ed in this clause RSN. Model this	are exactly the sa clause as done ir	me as those defined in 11A.6.2. (This is	The ov 11A.5.3 revisior	er-the-DS proce 3 with the except n of similar com	edures defined in otion of non-RSN. iment)	this clause a Restructure	are exactly the sa this clause as do	me as those defined in one in 11A.6.3 (This is
SuggestedRemedy	/				Suggested	Remedy				
Delete entire te Clause 11A.5.2 transition proto air FT protocol 6. RSNIE and FTIE, and Key	ext in clause 11A.5. 2. Change Clause 1 col authentication". in an RSN is show FTIE shall not be pr Holders in this sub-	4. Do not delete 1A.5.2 title page Change Clause n in Figure 11A/ esent in non-RS clause are appli	the Fig 11A-6. Mo 55 line 58 "Over- 11A.5.2 page 55 and in a non-RS N protocol, and re cable to RSN only	ve Fig 11A-6 into the-air fast BSS line 65: "The over-the- N is shown in Fig 11A- ferences to RSNIE, ."	Delete Clause transiti DS FT 7. RSN referen applica	entire text in cla 11A.5.3. Chan on protocol auth protocol in an F IIE and FTIE sh ices to RSNIE, ible to RSN only	ause 11A.5.5. Do ge Clause 11A.5. nentication". Char RSN is shown in F nall not be present FTIE, Key Holder v."	not delete th 3 title page s ige Clause 1 igure 11A-5 in non-RSN s, and Key c	he Fig 11A-7. Mov 55 line 58 "Over-ti 11A.5.3 page 57 li and in a non-RS I protocol. Protoco Jerivations in this	ve Fig 11A-7 into he-DS fast BSS ine 37: "The over-the- N is shown in Fig 11A- ol description and sub-clause are
Response	Respons	se Status U			аррііса		y.			
The differences and error hand because 11A.6 <i>Cl</i> <b>11A</b> SC <b>1</b>	s between 11A.5.2 ; ling. The combinat could refer back to 1A.5.4	and 11A.5.4 are on of RSN and r 11A.5 for the di <b>P59</b>	significant, such a non-RSN in 11A.6 fferences <i>L</i> <b>28</b>	as message contents was possible only # 66	REJEC The dif and err becaus	CT. ferences betwe for handling. The se 11A.6 could not	en 11A.5.3 and 1 he combination of refer back to 11A.	1A.5.5 are s RSN and no 5 for the diff	ignificant, such as on-RSN in 11A.6 erences	s message contents was possible only
CHAPLIN, CLINT F	-				C/ 11A	SC 11A.5.5		P <b>60</b>	L 25	# 212
Comment Type	T Comme	ent Status A			Sood, Kapi	I				
"in a non-RSN	N&" is not consisten	t with the referer	ncing text for the for	ollowing procedure.	Comment 7	Type TR	Comment Sta	atus R		
(Originally LB9	8/508 submitted by	Sood, Kapil, dur	ing LB98 with ID \$	Sood/057)	The ov	er-the-DS proce	edures defined in	this clause a	are exactly the sa	me as those defined in
SuggestedRemedy	/				0			Restructure	e triis clause as ut	
Change "The c	over-the-air Fast BS	S Transition prot	ocol in a non-RSN	V (dot11RSNAEnabled	Suggesteal	Remedy		nat dalata ti		in Fig 11 A 7 into
Is set raise) is	Shown in Figure 20	41.			Clause	11A.5.3. Chan	ge Clause 11A.5.5. Do	3 title page 4	55 line 58 "Over-t	he-DS fast BSS
ACCEPT.	Respons	se Status C			transitio DS FT 7. RSN referen applica	on protocol auth protocol in an F IIE and FTIE sh ices to RSNIE, ible to RSN only	nentication". Char RSN is shown in F hall not be present FTIE, Key Holder y."	ige Clause 1 igure 11A-5 in non-RSN s, and Key c	11A.5.3 page 57 li and in a non-RS I protocol. Protocol derivations in this	ine 37: "The over-the- N is shown in Fig 11A- ol description and sub-clause are
					Response		Response Sta	tus <b>U</b>		

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

Page 67 of 89

09/27/2007 06:28

<i>CI</i> <b>11A</b> CHAPLIN,	SC CLINT	11 <b>A.5.5</b> F	P60	L <b>27</b>	# 67
Comment "in a (Origir	<i>Type</i> non-RS nally LB	<b>T</b> N&" is not 98/511 sul	Comment Status <b>A</b> t consistent with the referenci bmitted by Sood, Kapil, during	ng text for the g LB98 with ID	following procedure. 9 Sood/058)
Suggested Chang is set	<i>lRemed</i> je "The False) is	ly over-the-E s shown in	DS Fast BSS Transition proto h Figure 204g."	col in a non-R	SN (dot11RSNAEnabled
Response ACCE	PT.		Response Status C		
C/ 11A Epstein, Jo	SC oseph	11 <b>A</b> .6	P <b>61</b>	L <b>23</b>	# 282
Comment The si must b succe: debilit: withou behav and de around low-us as net there model does r shown impler	Type x-mession peremo ssfully in ating eff the commission lead behave age cas work fail -calcula ling the not meen to work	TR age resour- ved. Thes mplemente fects. Amo- itment by s to knowr at worst. I ior is subjo ses while s ilure, or pe- tions base 6-message t the goal < with this s to know the sta	Comment Status <b>A</b> rce request protocol mentione e flaws are generally of the ne ed in such a way as to perform ing the problems are as follow the allocator leads to binding n race conditions, resulting in Multiple allocations cannot be ect to game-theoretic problem shutting down the network in l er-station convergence times a ed on reasonable assumptions ge exchange) fails to eliminate mentioned in the scope of the 6-message exchange. Furthe	ed in 11A.6 is a ature that the p n the desired f vs. Establishin shop-around p forcably prohi is that reward nigh-usage ca averaging abo s have exceed or reduce da e PAR. No imp ermore, a num be 6-message	reservation protocol seriously flawed and protocol cannot be function without nasty or ig resource allocations behavior. Shop-around ence behavior at best, ibited in this model. Shop- the aggressive client in ses. Global effects such ve 50ms (or around ded this number when ta absense, and thus blementation has been ber of potential exchange is flawed and

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.

have removed it from being required or being tested in a testplan being constructed around

Response

Response Status U ACCEPT IN PRINCIPLE

Changes given in submission 11-07-2516-01.

C/ 11A	SC 11A.6	P <b>61</b>	L 23	# 313
Myles, Andı	rew F			

omment Type TR Comment Status A

reservation protocol

The Resource Request protocol (requesting resources prior to association) is overly complex. It will lead to under-utilization 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.

## uggestedRemedy

Remove Section 11A.6

esponse Response Status U

ACCEPT IN PRINCIPLE

Changes given in submission 11-07-2516-01.

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Comment ID # 313

Page 68 of 89 09/27/2007 06:28



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 prereservation 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.

C/ 11A	SC 11A.6	P <b>61</b>	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 4message 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 overprovisioned 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.

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Comment ID # 251

Page 69 of 89 09/27/2007 06:28

C/ 11A	SC 11A.6	P61	L <b>24</b>	# 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

Response

Remove clause 11A.6 and Accept my submission (11-07-2351-00-000r-FT-resourcerequest-protocol-removal) that prescribes all the changes in this draft that remove the FT Resource Request protocol.

#### Response Status U

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

#### 

### 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.

CI 11A	SC 11462	DEA	/ 13	# 215	
Sood, Kap	il	7 04	215	π 213	
Comment	Type <b>TR</b>	Comment Status A			
The a 114	" ie danalina - ie "	it" refering to the response o	or to MIC.		

ACCEPT.

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Comment ID # 215

Page 70 of 89 09/27/2007 06:28

CI 11A	SC 11462	Dea	1 9	# 214		·C 11 A 6 3	<b>P65</b>	/ 20	# 292
Sood, Kap	il	/ 04	20	$\pi$ Z14	Amann, Keith	0 114.0.5	7 05	20	# 302
Comment "In a n senter descri Suggested	Type <b>T</b> on-RSN, a Timed ace lending more ption appears on IRemedy	Comment Status <b>A</b> but Information Element may intrigue than giving substanti lines 31-34, so this sentence	appear" - this re al value to impl is redundant.	eads like a misplaced ementers. A better	Comment Type The state of by the stat This time is AP it force have a diff	e TR diagram indi on in attem s apparently s all stations erent "view"	Comment Status <b>A</b> icates that the "Reassociati pting to move from the auth defined by the target AP. s to conform to the same re of how their individual traff	on Deadline Time" nentication steps to By having this time equirement, even the fic needs to be deli	' is not to be exceeded o the association step. cout value defined by the hough they each may ivered, and when it might
Delete	this line.				be feasible configure t	to perform	the (re)association step. In er such that some stations	fact, it is conceiva	able that an AP could y can't work.
ACCE	PT.	Response Status C			SuggestedRen	nedy			,
Cl 11A Sood, Kap Comment "In a n senter descri comm Suggested Delete Response ACCE	SC 11A.6.2 il <i>Type</i> <b>T</b> on-RSN, a Timed ice lending more ption appears on ent) <i>IRemedy</i> this line. PT.	P64 Comment Status A out Information Element may intrigue than giving substanti lines 31-34, so this sentence Response Status C	L8 appear" - this re al value to impli- is redundant. (	# 363 eads like a misplaced ementers. A better This is revision of similar	One of two 1) Allow th when it will result of th the AP is h this doesn' 2) Add a m value, or ir can determ specified. I suspect th favor of #1 Response ACCEPT I The Reass Association	solutions s e station to return. In the previous a aving to ma t appear to echanism t clude it as hine if it can hat there are N PRINCIPI ociation De h, and is co	eems acceptable: provide the "Reassociation his situation the AP can the authentication transactions sintain these timers anyway add any additional complex hat would allow the station "public" information in the b actually meet the "Reasso e some potential security is <i>Response Status</i> <b>U</b> LE. adline is provided to the S <sup>-</sup> nsistent across the Mobility	Deadline Time" va en drop any state th once the timeout h v (one per station fo kity on the part of th to query the AP ah eacon or probe re- ciation Deadline Ti sues related to #2	alue to the AP indicating hat has been setup as a has been reached. Since or the existing solution) he AP. head of time for this sponses so that a station ime" requirements , so would be more in
					your secor security iss	d alternativ sues.	e. The value is protected b	y a MIC, which dea	als with the potential
					Cl 11A S Sood, Kapil Comment Type The "it" is o SuggestedRen Change: "o	C 11A.6.3 TR dangling - is nedy lisregard th	P67 Comment Status A "it" refering to the response e response if the MIC is inc	L 21 e or to MIC.	# 216
					Response ACCEPT.		Response Status U		

C/ 11A Sood, Kap	SC <b>11A.7</b> il	P67	L <b>50</b>	# 248
Comment When then it after a type. for tha TSPE WMM specif	Type <b>TR</b> a non-AP STA n s resource requi RIC failure, but The non-AP STA to not target AP sup Cs. The industry It is, therefore, a cation when 11r	Comment Status <b>A</b> noves from a WMM-AP to a tar rements will not be met at the ends up associated with an A then has to look for another A an appropriate AP. Same pro ports only WMM. TGr must be has implemented WMM and a strong requirement that no c is tested/certified with WMM	rget AP suppor Target AP. A n P that does not AP, which increa- blems occur wh blems occur wh a made to co-ex 11r devices will hange be nece ISPEC/resourc	RIC format ting 11e-only TSPECs, on-AP STA only learns support its resource ases the transition time nen current AP supports ist with 11e and WMM be tested/certified with ssary to this es.
Suggested	Remedy			
Adopt the ta	my submission t get AP prior to m	hat allows non-AP STA to ide naking a FT attempt to that AF	ntify the suppor 9.	ted resource types on
Response ACCE Insert definit this re	PT IN PRINCIPL row in Table 11A ion "RDIE is follo source."	Response Status U E -3 with Resource Type "Vend wed by any Vendor-specific ir	or Specific" and	d Resource Descriptor ients required to specify
C/ 11A	SC 11A.7	P <b>67</b>	L <b>50</b>	# 376
Sood, Kap Comment When then it after a type. for tha 11e a TSPE	il <i>Type</i> <b>TR</b> a non-AP STA n s resource requi RIC failure, but The non-AP STA to nd target AP sup Cs. The industry	Comment Status <b>A</b> noves from a WMM-AP to a ta rements will not be met at the ends up associated with an A then has to look for another <i>A</i> an appropriate AP. Same pro ports only WMM. TGr must be has implemented WMM and	rget AP suppor Target AP. A n P that does not AP, which increa blems occur wh made to co-ex 11r devices will	ting 11e-only TSPECs, on-AP STA only learns support its resource ases the transition time nen current AP supports ist with 11e and WMM 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)

Response Status U

### 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

## 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."

C/ 11A Sood, Kapil	SC 11 <b>A.7.1</b>	P <b>67</b>	L <b>54</b>	# 218
Comment Typ STA is not	e <b>TR</b> t just any STA - it	Comment Status A is a non-AP STA		non-AP STA
SuggestedRei Change lir	<i>medy</i> nes 54, 57, 59, 60	), 62: "STA" to "non- <i>i</i>	AP STA"	
Response ACCEPT	F	Response Status U		
C/ <b>11A</b> Sood, Kapil	SC 11A.7.1	P <b>68</b>	L13	# 220
<i>Comment Typ</i> The "it" is	e <b>TR</b> dangling - is "it" r	Comment Status A refering to the reques	t or to MIC.	
SuggestedRei Change: "	<i>medy</i> disregard the req	uest if the MIC is inco	orrect".	
Response	5	Pasnonsa Status II		

Response Response Status U ACCEPT.

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Page 72 of 89 Comment ID # 220

09/27/2007 06:28
C/ 11A	SC 11A.7.1	P 68	L <b>21</b>	# 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."

C/ 11A	SC 11A.7.1	P68	L <b>21</b>	# 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."

C/ <b>11A</b> Sood, Kapil	SC 11 <b>A.7.1</b>	P6	8	L <b>22</b>	# 222
Comment TypeTRComment StatusAnon-AP STASTA is not just any STA - it is a non-AP STA					
SuggestedRe Change	e <i>medy</i> lines 22, 27, 31:	"STA" to "non-AP S	STA".		
Response ACCEPT	г	Response Status	U		

C/ 11A SC 11A.7.1 Sood, Kapil	P 68	L <b>28</b>	# 221	C/ 11A SC 11A.7 Sood, Kapil	r.1 P68	L <b>43</b>	# 224
Comment Type TR The "it" is dangling - is SuggestedRemedy Change: "disregard the	Comment Status A "it" refering to the response o e response if the MIC is incorre	r to MIC. ect".		Comment Type TR "then the STA sha returned in the Stat non-zero status coo on ANY failure. A S understand why the	Comment Status <b>R</b> all abandon this transition atter us Code shall be as specified i de, so the FT attempt has failed TA has no other recourse but t s STA shall abandon on only th	npt. Handling of oth in 11.3." -a non-AP d and STA shall ab to try the entire FT lese failures, and n	STA behavior her errors STA has received a handon this FT attempt again. I do not hot others. If there are
ACCEPT. 	P68	L 36	# 223	other outcomes ple SuggestedRemedy Change: "If the Sta	ase list them. tus Code returned by the targe	t AP in the respons	se is 1 ("unspecified
Sood, Kapil <i>Comment Type</i> <b>TR</b> STA is not just any ST	Comment Status <b>A</b> A - it is a non-AP STA		non-AP STA	failure"), 14 ("Authe ("Authentication rej non-zero status coo other errors returne	entication transaction sequence ected due to timeout waiting fo de, then the STA shall abandor d in the Status Code shall be a to 69 line 38	<ul> <li>number out of sec r next frame in seq n this fast transition as specified in 11.3</li> </ul>	Juence"), 16 Juence"), or any other Attempt. Handling of 3." Same change in
SuggestedRemedy Change lines 36, 43, 4	18, 50, 51: "STA" to "non-AP S	TA"		Response REJECT	Response Status U		
Response ACCEPT	Response Status U			The existing text lis (unspecified failure abandon the transit	ts specific reasons (14, 16) can ) enables the AP to indicate oth ion attempt.	used by failures in t her relevent failures	the FT, and the third s requiring the STA to

C/ 11A	SC 11A.7.1	P68	L <b>43</b>	# 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.

C/ 11A	SC 11A.7.1	P68	L <b>47</b>	#	69
CHAPLIN, C	LINT 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."

C/ 11A	SC 11A.7.1	P 68	L 47	#	68
CHAPLIN, C	LINT 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	С
ACCEPT. Also changed at 52.01	and 63.37.	

C/ 11A	SC 11A.7.1	P 68	L <b>48</b>	#	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

C/ 11A	SC 11A.7.1	P68	L <b>48</b>	# 225
Sood, Kapi	I			
Comment	Type <b>TR</b>	Comment Status R		Roam-to-self
"If the t shall er same A operati	target AP is distin nter State 1 with AP that it is curre ion. If not, then w	nct from the previous AP, the respect to the previous AP" ntly associated with? If so, t /hy do we have this statement	e STA - can a non-AP S hen why would we nt?	TA do an FT to the e allow such an
Suggested	Remedy			

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.

Comment ID # 225

Response Response Status U

#### REJECT.

This change makes a reassociation with the current AP impossible

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general

COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

C/ 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."

C/ 11A	SC 11A.7.2	P69 L1	# 227
Sood, Kapil			
Comment T	ype TR	Comment Status A	non-AP STA
STA is	not just any STA	- it is a non-AP STA	
SuggestedF	Remedy		
Channe	1 A O F AA		

Change lines 1, 2, 5, 11, 21, 31, 38, 45, 46 "STA" to "non-AP STA"

Response Status U

```
Response
```

ACCEPT

C/ 11A SC 11A.7.2 P69 L18 # 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."

C/ 11A	SC 11A.7.2	P 69	L18	# 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."

<i>Cl</i> <b>11A</b> Sood, Kapi	SC 11A.7.2	P6	9	L 41	# 368
Comment 7 "If the J shall ut IEEE 8 802.1X say, th	Type TR C AP has dot11RSNAE nblock the .02.1X Controlled Por . in non-RSN. An AP en re-word according	Comment Status nabled set to tru rt." - Isn't this cla may have a RSN Ily. (This is revisi	<b>R</b> e, upon a suc use describin N enabled, bu on of similar o	ccessful reassocia g a non-RSN case t if this is the case comment)	ation the SME e? There is no e this is trying to
Suggested Delete	<i>Remedy</i> this line. (lines 41-42	on page 69).			
Response REJEC This se AP (ca	R CT. entence is needed to lled TSN in 802.11-20	esponse Status cover the case c 007)	U of a non-RSN	STA associated t	o a RSN-capable

C/ 11A	SC 11A.7.2	P 69	L <b>41</b>	# 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 Sood, Kapil	SC 11A.8.1	P <b>69</b>	L <b>59</b>	# 229
Comment 7 STA is	<i>Type</i> <b>TR</b> not just any STA	Comment Status A		non-AP STA
Suggestedl Change	R <i>emedy</i> e lines 59, 61, 65	: "STA" to "non-AP STA"		
Response ACCEF	РΤ	Response Status U		
<i>Cl</i> <b>11A</b> Sood, Kapil	SC 11A.8.1	P <b>70</b>	L 18	# 231
Comment 7 "In all c term - j Suggestedi Delete	<i>Type</i> <b>TR</b> cases" - what all oust adding confu <i>Remedy</i> "In all cases"	Comment Status A cases are being referred to sion.	here. No value is	being added by this
Response ACCEF	ΥТ.	Response Status U		

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID Comment ID 231

Page 77 of 89 09/27/2007 06:28

Submission

Bill Marshall, ATT Labs Research

C/ <b>11A</b> Sood, Kapil	SC 11 <b>A.8.1</b>	P <b>7</b>	0	L <b>45</b>	# 232
Comment 7 Snonce	<i>Type</i> <b>TR</b> e and Anonce ar	Comment Status e together the Instan	A ce Id	entifiers.	
Suggestedl Change instanc	R <i>emedy</i> e: "The non-AP \$ e identifier and t	STA includes a fresh to provide key"	SNo	nce as its contributio	n to the association
Response ACCEF	PT.	Response Status	U		
C/ <b>11A</b> Sood, Kapil	SC 11A.8.1	P <b>7</b>	0	L <b>48</b>	# 233
Comment 7 The en So, the value.	<i>Type</i> <b>TR</b> tire paragraph (I last line "This ir	Comment Status ines 40-48) clearly de nformation is sent from	A efines n the	s all data is being ser STA to the target Al	nt by the non-AP STA P" is not adding any
Suggestedl	Remedy	formation is cont from	n tha	STA to the target A	יכ
Response ACCEF	PT.	Response Status	U	STA to the target Ar	
C/ <b>11A</b> Sood, Kapil	SC 11A.8.1	P <b>7</b>	0	L 48	# 369
Comment 7 The en So, the value. ( Suggestedi	<i>Type</i> <b>TR</b> tire paragraph (I last line "This ir (This is revision <i>Remedy</i>	Comment Status ines 40-48) clearly de iformation is sent from of similar comment)	A efines n the	s all data is being ser STA to the target Al	nt by the non-AP STA P" is not adding any
Response	une line: " i nis in	Response Status	U U	STA to the target AF	

C/ 11A Sood, Kapil	SC 11 <b>A.8.1</b>	P <b>70</b>	L <b>5</b>	# 230
Comment 7 STA is	<i>Type</i> <b>TR</b> not just any STA	Comment Status A - it is a non-AP STA		non-AP STA
Suggested Change	R <i>emedy</i> e lines 5, 11, 40,	45, 50, 56, 57, 60: "STA" to	"non-AP STA"	
Response ACCEF	РТ	Response Status U		
C/ <b>11A</b> Sood, Kapil	SC 11A.8.1	P <b>70</b>	L <b>52</b>	# 234
Comment 7 Target instanc	<i>Type</i> <b>TR</b> AP provides the e id. Make this co	Comment Status <b>A</b> Anonce, but this is also the tonsistent with the SNonce in	arget AP contril	pution to the assoc raph.
Suggested Change instanc	R <i>emedy</i> e: "The target AP e identifier and to	also includes a fresh ANon provide key separation of t	ce as its contribute he derived PTK.	ution to the association ."
Response ACCEF	PT.	Response Status U		
C/ 11A Sood, Kapil	SC 11A.8.1	P <b>70</b>	L <b>52</b>	# 370
Comment 7 Target instanc similar	<i>Type</i> <b>TR</b> AP provides the e id. Make this co comment)	Comment Status A Anonce, but this is also the tonsistent with the SNonce in	arget AP contril previous parag	oution to the assoc raph. (This is revision of
Suggested Change instanc	Remedy e: "The target AP e identifier and to	also includes a fresh ANon provide key separation of t	ce as its contribute he derived PTK.	ution to the association ."
Response		Response Status U		

ACCEPT.

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

 Page 78 of 89

 Comment ID # 370
 09/27/2007 06

09/27/2007 06:28

C/ 11A Sood, Kapil	SC	11 <b>A.8.</b> 1	P <b>7</b>	0	L <b>53</b>	# 235	C/ <b>11A</b> Sood, Kapi	SC	11A.8.1	P <b>70</b>	L <b>57</b>	# 236
Comment T	Гуре	TR	Comment Status	Α			Comment	Туре	TR	Comment Status A		
The ent the last	tire par i line "T	ragraph (li This inform	nes 50-54) clearly d ation is sent from th	efines all data le target AP t	a is being sent b o the STA" is no	y the target AP. So, t adding any value.	The er So, the	itire pa e last li	ragraph (lir ne "This inf	nes 56-58) clearly defines ormation is sent from the	all data is being s STA to the target	ent by the non-AP STA. AP" is not adding any
Suggested	Remed	ly					value.	Domo	d.			
Delete	the line	e: "This inf	ormation is sent from	m the target A	AP to the STA".		Suggested	the lin	Jy o: "Thio inf	armation is cast from the	STA to the torget	D" Change: "In an
Response ACCEF	РТ.		Response Status	U			RSN, t AP ST	he thir A has	d message a valid PTK	is used by the non-AP S	TA to assert to the	target AP that the non-
C/ <b>11A</b> Sood, Kapil	SC	11 <b>A.</b> 8.1	P <b>7</b>	0	L <b>53</b>	#  371	Response ACCE	PT.		Response Status U		
Comment T	Гуре	TR	Comment Status	A Stinger all date			C/ 11A	SC	11A.8.1	P <b>70</b>	L 65	# 373
the last	ire par iine "T	his inform	ation is sent from th	ennes an data le target AP t	o the STA" is no	t adding any value.	Subu, Kapi					
(This is	revisio	on of simila	ar comment)	0		0 7	Comment	l ype	IR	Comment Status A		
Suggested# Delete	R <i>emed</i> the line	<i>ly</i> ə: "This inf	ormation is sent fro	n the target A	AP to the STA".		The er the las (This is	itire pa t line " s revisi	ragraph (lir This inform ion of simila	ation is sent from the targ ar comment)	s all data is being s get AP to the STA"	is not adding any value.
Response			Response Status	U			Suaaested	Reme	dv	·		
ACCEF	ΡT.			-			Delete	the lin	e: "This infe	ormation is sent from the	target AP to the S	ГА".
C/ 11A Sood, Kapil	SC	11A.8.1	P <b>7</b>	0	L <b>5</b> 7	# 372	Response ACCEI	PT.		Response Status U		
Comment T	rvpe	TR	Comment Status	Α			C/ 11A	SC	11A.8.1	P <b>70</b>	L 65	# 237
The ent	tire par	ragraph (li	nes 56-58) clearly d	efines all data	a is being sent b	y the non-AP STA.	Sood, Kapi	I				
So, the	last lin	e "This in	formation is sent fro	m the STA to	the target AP" is	s not adding any	Comment	Туре	TR	Comment Status A		
			or similar comment)				The er	itire pa	ragraph (lir	nes 60-65) clearly defines	all data is being s	ent by the target AP. So,
Delete	the line	y "This inf	ormation is cant from	m tha STA ta	the torget AD"	Changes "In an	the las	t line "	This inform	ation is sent from the targ	get AP to the STA"	is not adding any value.
RSN, th	ne thirc	l message	is used by the non-	AP STA to as	ssert to the targe	et AP that the non-	Suggested	Reme	dy			
AP STA	A has a	a valid PT	<."		0		Delete	the lin	e: "This info	ormation is sent from the	target AP to the S	ГА".
Response ACCEF	РТ.		Response Status	U			Response ACCE	PT.		Response Status U		
	echnic	al required	ER/editorial requi	ed GR/gene	ral required T/te	ochnical Eleditorial Glo	neneral					

I YPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Page 79 of 89 09/27/2007 06:28

Submission

Bill Marshall, ATT Labs Research

Comment ID # 237

L

C/ 11A	SC 11A.8.2	P <b>71</b>	L15	# 238		C/ 11A	SC 11A.8.2	P	71	L15	# 374
Sood, Kapil						Sood, Kapil					
Comment 7 Making the purj in the e AP with	ype <b>TR</b> the non-AP STA s pose of using 11k ntire MD, and as s which it performe	Comment Status A send the MDIE from the bea discovery and over-the-DS. such, the non-AP STA shoul d the Initial MD Association	ncons/probes of t MDIE should be Id include the ME	ne target AP defeats consistently the sam IE that it got from the	e	Comment 7 Making the pur in the e AP with	the non-AP ST cose of using 1 ntire MD, and a which it perfor	Comment Statu A send the MDIE fro 1k discovery and ov as such, the non-AP med the Initial MD A	s <b>A</b> om the beacc er-the-DS. M STA should i sssociation. ( <sup>-</sup>	DIS/probes of th DIE should be of include the MDI This is revision	e target AP defeats consistently the same IE that it got from the of similar comment)
Suggested	Remedy					Suggested	Remedy				
Change Capabi settings Domair handsh Domair	e: "The MDIE shall lity and policy s obtained from the a Association. The ake of the Initial N a shall advertise th	contain the Mobility Domain AP with which the non-AP MDIE shall be the same as lobility Domain Association. e same MDIE."	n Identifier, the F STA performed received in mes All APs within th	ast BSS Transition the Initial Mobiloity sage 3 of the FT 4-wa e same Mobility	у	Change Capabi settings Domair handsh Domair	: "The MDIE sl ity and policy obtained from Association. T ake of the Initia shall advertise	hall contain the Mob the AP with which t The MDIE shall be th al Mobility Domain A e the same MDIE."	ility Domain le ne non-AP S <sup>-</sup> e same as re ssociation. Al	dentifier, the Fa TA performed th ceived in mess II APs within the	st BSS Transition ne Initial Mobiloity age 3 of the FT 4-way ∋ same Mobility
Response		Response Status U				Response		Response Statu	S U		
ACCEF The 111 current the MD settings same a identica needed	PT IN PRINCIPLE. k neighbor report i AP, so the 11k dis IE is administered s obtained by the r s those of the targ al to the initial one,	ndicates that the target AP is scovery is not being defeate consistently across the Mol ion-AP STA during Initial Mo et AP. However, the target but can verify that it is iden	is advertising an d. It is assumed bility Domain (sta bility Domain As AP is unable to v tical to its own.	identical MDIE as the by the standard that ted in 11A.3), so the sociation are the erify that the MDIE is No text changes		ACCEF The 111 current the MD settings same a identica needed	T IN PRINCIPI c neighbor repo AP, so the 11k IE is administe c obtained by th s those of the t il to the initial o	LE. ort indicates that the discovery is not bei red consistently acro he non-AP STA durin arget AP. However, ne, but can verify th	target AP is a ng defeated. Iss the Mobili Ig Initial Mobi the target AP at it is identic	advertising an id It is assumed b ity Domain (stat ility Domain Ass ' is unable to ve al to its own. N	dentical MDIE as the y the standard that ed in 11A.3), so the sociation are the erify that the MDIE is o text changes
						<i>Cl</i> <b>11A</b> Sood, Kapil	SC 11A.8.2	Р	71	L <b>23</b>	# 239
						<i>Comment T</i> STA is	<i>ype</i> <b>TR</b> not just any ST	Comment Statu A - it is a non-AP ST	s <b>A</b> -A		non-AP STA
						Suggestedl Change	Remedy e lines 23, 26, 5	55 : "STA" to "non-Al	P STA"		
						Response ACCEF	т	Response Status	s U		

Comment ID # 239

Page 80 of 89 09/27/2007 06:28

C/ 11A SC 11A.8.3 Sood, Kapil	P <b>71</b>	L <b>48</b>	# 241	C/ <b>11A</b> CHAPLIN, (	SC <b>11A.8.4</b> CLINT F		P <b>72</b>	L <b>26</b>	# 124
Comment Type TR It is the target AP - just	Comment Status <b>A</b> st to be clear.			Comment 7 I think t	<i>Type</i> <b>TR</b> there is a misur	Comment St nderstanding to Ll	atus <b>R</b> B98 CID 5878	the resolution	states: "(resolution to
SuggestedRemedy Change: "MDIE adver	tised by the target AP in &"			this cor Rejecte algorith	mment agreed ed. The Group nm, and the sar	as part of LB87) and Pairwise ciph me algorithm is be	er selection is	s used in 8.5.2 here." Howeve	to determine the MIC r, my comment is to the
Response ACCEPT.	Response Status U			 MIC alg based o cipher, (Origina	gorithm in the F on the AKM, wi a new AKM wi allv LB105/17 s	TIE. There has b hich may be acce ill be required. Is t submitted by Cam	een a current ptablebut th his the desire -Winget, Nan	update in D6.0 he implication is d effect? cv. during LB10	to state that it is now s that for every new 05 with ID Cam-
C/ 11A SC 11A.8.3	P <b>71</b>	L <b>56</b>	# 240	Winget	/10)			-,,g	
Sood, Kapil				Suggested	Remedy				
Comment Type TR It is the target AP - just	Comment Status A st to be clear.			The res parame the nec	served bits in the ter index. For a constant of the served bits in the server of the server of the served bits in the served bi	he MIC control fiel now it can be set agility should othe	ld of the FTIE to 0 to signal er ciphers be a	could be used AES-CMAC bu allowed.	to allow for a security tt can be used to provide
SuggestedRemedy Change: "R1 Key Hole	der Identifier of the target AP, fr	om the&"		Response REJEC	CT.	Response Sta	atus U		
Response ACCEPT.	Response Status U			The internation approar into the algorith AKM al	ent is that a ne ich was chosen RSN informat ms; using the llows for vendo	w AKM would be for the following ion element; (2) T FTIE available bit or specific MIC alg	used to selec reasons: (1) T o provide end s provides ver orithms.	t a different MIC To consolidate a bugh flexibility for ry limited flexib	C algorithm. This all the security algorithm or vendor specific MIC ility whereas using the
				C/ <b>11A</b> Sood, Kapil	SC 11 <b>A.8.4</b>		P <b>72</b>	L <b>30</b>	# 242
				Comment 7 STA is	<i>Type</i> <b>TR</b> not just any ST	Comment St TA - it is a non-AP	atus <b>A</b> STA		non-AP STA
				Suggested Change	Remedy e lines 30, : "S <sup>-</sup>	TA" to "non-AP ST	ГА"		
				Response ACCEF	РТ	Response Sta	atus U		

Submission

C/ 11A SC Sood, Kapil	C 11A.8.4	P <b>72</b>	L <b>40</b>	# 243	C/ 11A SC 11A.8. Sood, Kapil	.5 P <b>7</b> 3	L <b>26</b>	# 246
Comment Type The correct	TR item is RIC-	Comment Status <b>A</b> Request to be consistent with	prior usage an	d figures.	Comment Type TR STA is not just any S	Comment Status A STA - it is a non-AP STA		non-AP STA
SuggestedReme Change: "Ce	edy contents of th	e RIC-Request (if present)			SuggestedRemedy Change lines 26, 50	) : "STA" to "non-AP STA"		
Response ACCEPT.		Response Status U			Response ACCEPT	Response Status U		
Cl 11A SC Sood, Kapil	C 11A.8.4	P <b>72</b>	L <b>45</b>	# 244	C/ 11A SC 11A.9 CHAPLIN, CLINT F	P <b>75</b>	L1	# 125
Comment Type The correct	TR item is RIC-	Comment Status A Request to be consistent with	prior usage an	d figures.	Comment Type <b>T</b> The state machine o (Originally LB105/18	Comment Status R diagrams are overloaded and p 3 submitted by Hiertz, Guido, d	boorly drawn. luring LB105 with	SDL State Machines
Change: "&f	eay forming the l	RIC-Request shall be included.	"		SuggestedRemedy			
Response	ioning the	Response Status U			SDL provides the ne machine diagrams s	ecessary functionality of a well should be redrawn using SDL-9	defined program 92.	ming language. The state
ACCEPT.					Response	Response Status C		
C/ 11A SC Sood, Kapil	C 11A.8.5	P <b>72</b>	L 60	# 245	REJECT State machines are 2007.	drawn in a manner and form c	consistent with th	e existing ones in 802.11-
Comment Type It is the targ	<b>TR</b> get AP - just t	Comment Status <b>A</b> to be clear.			C/ 11A SC 11A.9. Malinen, Jouni	.2 P75	L <b>34</b>	# 312
SuggestedReme Change: "&a	<i>edy</i> advertised b	y the target AP in Beacon&"			Comment Type ER Typo	Comment Status A		
Response ACCEPT.		Response Status U			SuggestedRemedy Replace "Derive-Ke PMKR1SA state in I	u-PMK-R1()" with "Derive-Key Figure 11A-12.	-PMK-R1()" in th	e FT-R0-SEND-
					Response	Response Status U		
					ACCEPT.			

Chapin, 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/Suppliciant, rather they show much of the SME algorithms as well.       Comment Type       TR       Comment Status A         Authenticator/Suppliciant, rather they show much of the SME algorithms as well.       Comment Type       TR       Comment Status A         R1KH state machine interime is somewhat unclear. Will this state machine instance continue the state instance of the state instance instance doe on sthe state instance of the state instance ins
Comment Type       TR
ACCEPT

C/ 11A CHAPLIN,	SC 11A.9.3 CLINT F	P <b>77</b>	L <b>57</b>	# 72	C/ <b>11A</b> Malinen, Je	SC <b>11A.9.3</b> ouni	P <b>78</b>	L <b>24</b>	# 305
Comment Typo (Origin Suggested Replac Figure Response ACCEI	<i>Type</i> <b>E</b> lally LB98/595 su <i>Remedy</i> ce "MLME-SETPI 204m. PT.	Comment Status A bmitted by Malinen, Jouni, du ROTECTION.Request" with " Response Status C	uring LB98 with I MLME-SETPRC	D Malinen/50) DTECTION.request" in	Comment The Ai conse the init NEGC over-th R1-SA AUTH Suggested	Type TR uthenticator R1KH quently, the reasso tial association (wh DTIATING3 state or ne-air do not includ -RECD state shoul ENTICATE.responsion IRemedy	Comment Status A state machine shown in the ciation deadline is included ich is indeed shown correc the previous page). The a e the reassociation deadlin d not show "Reassoc dead se() primitive.	e figure is for RS d only in the EAF ty in the FT-PTH outhentication fra ie in this case ar lline" as a param	N case and OL-Key frames during K-CALC- imes used during FT id as such, the FT-PMK- neter to MLME-
<i>CI</i> <b>11A</b> CHAPLIN,	SC <b>11A.9.3</b> CLINT F	P <b>78</b>	L <b>24</b>	# 126	FT-PM FT-PM	", Reassoc-deadili IK-R1-SA-RECD st	ate for Figure 11A-14. Response Status U	MLME-AUTHEI	NTICATE.response() In
My LBs due to be rem cases" remove state n reasso (Origin Suggested Remov PMK-F Response	98 CID 597 was a the original commoved from FT-PI should be removed. One of the two nachine is clearly ociation deadline hally LB105/19 su <i>Remedy</i> ye ", Reassoc-de R1-SA-RECD in F	accepted, but it was not fully ment being unclear on which MK-R1-SA-RECD in Figure 2 ved, but there were actually t o remaining once should also for RSN case (e.g., use of N in the authentication frames i bmitted by Malinen, Jouni, du adline" parameter from MLMI Figure 204n. <i>Response Status</i> <b>C</b>	implemented in "Reassoc-deadl 04n. The comme hree occurrence o be removed to /IC-Verified) and in this case. uring LB105 with E-AUTHENTICA	D6.0. This was likely ine" occurrences should ent said that "both two s Only one was finish the cleanup: This as such, there is no ID Malinen/10) TE.response() in FT-	Cl 11A CHAPLIN, Comment FT-AU (Origin Suggested Replac invoke Response ACCE	SC 11A.9.3.1 CLINT F Type T ITH is also entered hally LB98/598 subi IRemedy ce "FT protocol is in ed" in the descriptio PT.	P78 Comment Status A in case of resource reques nitted by Malinen, Jouni, d nvoked" with "FT protocol c n of FT-AUTH. Response Status C	L 57 st protocol. uring LB98 with or FT resource re	# [73
ACCEI	PT.				CI 11A CHAPLIN, Comment FT-INI (Origin Suggested Add to Response ACCE	SC 11A.9.3.1 CLINT F Type <b>T</b> T-R1_SA is also er hally LB98/600 subr <i>IRemedy</i> the end of the FT- PT.	P79 Comment Status A ntered when rekeying PTK. mitted by Malinen, Jouni, d INIT-R1_SA description: "a Response Status C	L 10 uring LB98 with and when rekeyin	# [ <u>75</u> ID Malinen/55) ng PTK".

<i>CI</i> <b>11A</b> CHAPLIN, CL	SC 11 <b>A.9.3.1</b> _INT F	P <b>79</b>	L <b>8</b>	# 74		<i>Cl</i> <b>11A</b> CHAPLIN,	SC <b>11A.9.4</b> CLINT F	P 80	L <b>35</b>	# 77
Comment Typ FT-INIT-C cause a t (Original)	be <b>TR</b> GET-R1_SA is ransition to DIS y LB98/599 sub	Comment Status A not entered on R0KH timeo SCONNECT state). mitted by Malinen, Jouni, d	ut as claimed her uring LB98 with I	e (that timeout would D Malinen/54)		Comment Unnec someh (Origin	<i>Type</i> <b>TR</b> essary text in SC how set (to where hally LB98/602 st	Comment Status A KH state machine: Describin ?) does not really add any va ubmitted by Malinen, Jouni, d	ng that MDID, R0 alue here. luring LB98 with	0KH-ID, R1KH-ID are ID Malinen/56)
SuggestedRe Remove from the o Response ACCEPT	emedy ", or when the F description of F	R1KH issues a timeout failin T-INIT-GET-R1_SA. <i>Response Status</i> <b>U</b>	g to get a respor	ise from the R0KH"		Suggested Remov Response ACCE	IRemedy ve "Set MDID, R PT.	DKH-ID, R1KH-ID" from FT-R Response Status U	0-AUTH in Figu	re 204o.
CI <b>11A</b> CHAPLIN, CL	SC 11A.9.3.2 LINT F	P <b>79</b>	L <b>43</b>	# 76		C/ <b>11A</b> CHAPLIN,	SC 11A.9.4 CLINT F	P80	L <b>42</b>	# 78
Comment Typ Typo (Originally SuggestedRe Replace Response ACCEPT	be E y LB98/601 sub emedy "to initialize R11	Comment Status A omitted by Malinen, Jouni, d KH the state machine" with Response Status C	uring LB98 with I "to initialize the F	D Malinen/65) 1KH state machine."		Comment Typo (Origin Suggested Replac Response ACCE	rype E hally LB98/603 su <i>Remedy</i> ce "Derive-key-P PT.	MK-R0()" with "Derive-Key-P Response Status C	MK-R0()".	ID Malinen/57)
Cl 11A Malinen, Jour	SC <b>11A.9.4</b> ni	P <b>80</b>	L <b>30</b>	# 311		CHAPLIN,	CLINT F	F 80	L 33	# [/9
Comment Typ FT-Full-A though it	be <b>TR</b> luth(R1KH-ID) i is actually com	Comment Status <b>A</b> s described as coming from ing from FT-INIT-START.	FT-INIT-AUTH	state of S1KH SM even	I	Comment Typo (Origin	<i>Type</i> E hally LB98/606 st	Comment Status A	luring LB98 with	ID Malinen/60)
SuggestedRe Replace ' Response ACCEPT	emedy "FT-INIT-AUTH	" with "FT-INIT-START" on Response Status U	the second line o	of Figure 11A-15.		Suggested Replac Response ACCE	i <del>rkemedy</del> ce "Derive-key-P PT.	MK-R1" with "Derive-Key-PN <i>Response Status</i> <b>C</b>	IK-R1".	

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID

Comment ID # **79** 09

Page 85 of 89 09/27/2007 06:28

Cl 11A CHAPLIN,	SC <b>11A.9.4.1</b> CLINT F	P81	L18	# 80	C/ 11A SC 11A.9.5 P83 L 26 # 82 CHAPLIN, CLINT F
Comment <sup>T</sup> Typo (Origin Suggested Replac	<i>Type</i> <b>E</b> ally LB98/608 sub <i>Remedy</i> re "PMKR0" with "	Comment Status A omitted by Malinen, Jouni, du PMK-R0".	Iring LB98 with I	D Malinen/62)	Comment Type <b>TR</b> Comment Status <b>A</b> 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) SuagestedRemedy
Response ACCEI	PT.	Response Status C			Remove "Init. PMK-R1 lifetime" from FT-PTK-CALC in Figure 204q.
C/ 11A	SC 11A.9.5	P82	L1	# 81	ACCEPT.
S1KH MD as way of (Origin Suggested Add a 204q. / the S1 when t Response ACCEI	state machine see sociation or into S re-starting itself fr ally LB98/610 sub Remedy global transition to Add description of KH state machine ransitioning to a n	ems to get stuck into FT-PTH KIP-EAP at the completion of or next transition. mitted by Malinen, Jouni, du 0 R1-START state with cond "Init" variable into 11A.8.5.2 . In addition, this variable ca ew AP." Response Status <b>U</b>	C-INIT-DONE at t of FT. This state uring LB98 with I ition "Init" to Figu t: "This variable i n be used to re-s	the completion of initial machine should have a D Malinen/64) re 204p and Figure s set to true to initialize start the state machine	CHAPLIN, CLINTF         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.       P83       L 36       # 84
Cl 11A Malinen, Jo Comment Typo Suggested Replac START Response ACCEI	SC 11A.9.5 ouni Type ER Remedy ee "802.1X::portVa state of Figure 1	P82 Comment Status A alid-= FALSE" with "802.1X:: 1A-16. Response Status U	L <b>20</b> portValid = FALS	# 309	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.

TYPE: TR/technical required ER/editorial required GR/general required T/technical E/editorial G/general COMMENT STATUS: D/dispatched A/accepted R/rejected RESPONSE STATUS: O/open W/written C/closed U/unsatisfied Z/withdrawn SORT ORDER: Comment ID Comment ID Comment ID

Submission

Bill Marshall, ATT Labs Research

C/ 11A SC 11A CHAPLIN, CLINT F	.9.5	P <b>83</b>	L <b>41</b>	# 85		<i>CI</i> <b>A</b> CHAPLIN,	SC CLINT	<b>A.4.3</b> F		P <b>94</b>	L1	# 110
Comment Type E Inconsistent use of (Originally LB98/6 SuggestedRemedy Replace "MDID" v 51) and "MD-ID" v 41). Response ACCEPT.	Comment Star of MDID or MD-ID in pla 16 submitted by Maline vith "MDIE" in MLME-R vith "MDIE" in MLME-R Response Stat	tus <b>A</b> ace of MDIE. m, Jouni, during I EASSOCIATE.cc ESOURCE_REC us <b>C</b>	LB98 with ID Ma onfirm() parame QUEST paramet	alinen/67) ters (twice on row ers (twice on row	1	Comment What p provisi not, wh (Origin Suggested Consid grants assum Response	Type provisic ions for hy not? hally LB <i>IRemec</i> der add a copy ning tha	E ons are new single use 998/701 su dy ling a note rright relea tt this mee	Comment S eded to be able e of PICS and <i>i</i> bmitted by Kur to the PICS ar ise for the purs ts the requirem Response S	Status <b>A</b> e to extract an ASN.1 for 802 ihara, Thomas ad ASN.1 anno pose of extract ents for Digita tatus <b>C</b>	d use the PICS .11 PICS simila s, during LB98 v exes, similar to cting and using t al Right Manage	and ASN.1? Are there r to what is in 802.3? If vith ID Kurihara/9) wht is in 802.3 that the PICS and ASN.1, ment.
Cl 11A SC 11A CHAPLIN, CLINT F Comment Type T Reassociation red	9.5.1 Comment Stat	P 84 tus A ifferent states in s	L <b>61</b> S1KH state mad	# 86	be	ACCE 11ma standa intendo ameno	PT. D9.0 in ard may ed purp dment.	icludes the / freely rep pose and r	e statement "Co produce the PIC nay further pub	pyright releas S proforma in lish the compl	e for PICS profe this annex so t leted PICS." No	orma: Users of this hat it can be used for its changes needed in this
better not to make (Originally LB98/6 SuggestedRemedy Add "after comple	FT-RESERVE-2 expla 17 submitted by Maline tion of FT resource req	anation sound like en, Jouni, during l uest" to the end o	e it is the state d LB98 with ID Ma of FT-RESERVE	loing this. alinen/72) E-2 description.		C/ <b>D</b> Malinen, Jo Comment	SC ouni <i>Type</i>	D E	Comment S	P <b>97</b> Status <b>A</b>	L 37	# 307
Response ACCEPT.	Response Stat	us C				Typo SuggestedRemedy Replace "dot11SpectrummanagementTable" with "dot11SpectrumManagementTa (capitalized 'M' in "Management").						lanagementTable"
						Response ACCE	PT.		Response S	tatus C		

Submission

C/ D       SC D       P99       L40       # [11]       C/ General SC General       P       L         CHAPLIN, CLINT F       Comment Type       E       Comment Status A       Stephens, Adrian P       Stephens, Adrian P         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?       Corriginally 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"       C         C/ D       SC D       P99       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       # [112]       Modify the semantics of the reservation service so that it is equivalent to " these TSPECs right now, what would your answer be?". The essential difficient of existing members of that BSS that are not unnect access to local resources.         CHAPLIN, CLINT F       Comment Type       TR       Comment Status A         dot11AuthenticationAlgorithm is an INTEGER, it is not "set of" anything like the description       Response       Response Status II	# 289 reservation protoc
Conment 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?       Comment Type       TR       Comment Status       A         (Originally LB98/706 submitted by Malinen, Jouni, during LB98 with ID Malinen/75)       SuggestedRemedy       The resource reservation scheme has a number of flaws. But the main or semantics are of reservation rather than enquiry.       The resource reservation scheme has a number of flaws. But the main or semantics are of reservation rather than enquiry.         Remove ", 1999 Edition".       Response Status       C         ACCEPT IN PRINCIPLE.       Changed to ", 2007 Edition"       SuggestedRemedy         C/ D       SC D       P99       L58       # 112         CHAPLIN, CLINT F       Comment Status       A       Modify the semantics of the reservation service so that it is equivalent to " these TSPECs right now, what would your answer be?". The essential difficand the at transitioning STA may occassionally be surprised to have refused, to the benefit of existing members of that BSS that are not unnect access to local resources.         Comment Type       TR       Comment Status       A         dot11AuthenticationAlgorithm is an INTEGER, it is not "set of" anything like the description       Response       Response Status       U	reservation protoc
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?       Comment Type       TR       Comment Status       A         (Originally LB98/706 submitted by Malinen, Jouni, during LB98 with ID Malinen/75)       SuggestedRemedy       The resource reservation scheme has a number of flaws. But the main or semantics are of reservation rather than enquiry.         Response       Response Status       C         ACCEPT IN PRINCIPLE.       Changed to ", 2007 Edition"       SuggestedRemedy         CHAPLIN, CLINT F       P99       L58       # 112         Comment Type       TR       Comment Status       A         Comment Type       TR       Comment Status       A         Comment Type       TR       Comment Status       B         Modify the semantics of the reservation service so that it is equivalent to " these TSPECs right now, what would your answer be?". The essential difficandidate AP discounts these queries when responding to local requests. The result is that a transitioning STA may occassionally be surprised to har refused, to the benefit of existing members of that BSS that are not unnect access to local resources.	reservation protoc
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?       The resource reservation scheme has a number of flaws. But the main or semantics are of reservation rather than enquiry. The result is that a badly-designed STA which periodically "checks" neigh transition APs for QoS resources using this mechanism can tie up resource This behavior, while dumb, is valid, and potentially results in denial of semembers of those BSSs. So the question is whether to allow or protect against this behavior in som change the semantics of the reservation service.         Response       Response Status         Ci       D       SC D       P99       L58       # 112         CHAPLIN, CLINT F       Comment Status       A         Comment Type       TR       Comment Status       A         dot11AuthenticationAlgorithm is an INTEGER, it is not "set of" anything like the description       Response       Response Status       U	
SuggestedRemedy         Remove ", 1999 Edition".         Response       Response Status C         ACCEPT IN PRINCIPLE.         Changed to ", 2007 Edition"         CI D SC D       P99         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	ne is that the nboring candidate rees unnecessarily
Remove ", 1999 Edition".       Response Status C         Response       Response Status C         ACCEPT IN PRINCIPLE.       So the question is whether to allow or protect against this behavior in som change the semantics of the reservation service.         Changed to ", 2007 Edition"       Modify the semantics of the reservation service so that it is equivalent to "         CI D       SC D       P99       L58       # 112         CHAPLIN, CLINT F       Comment Type TR       Comment Status A       Modify the description         dot11AuthenticationAlgorithm is an INTEGER, it is not "set of" anything like the description       Response       Response Status U	vice to bona fide
Response       Response Status       C         ACCEPT IN PRINCIPLE. Changed to ", 2007 Edition"       Modify the semantics of the reservation service so that it is equivalent to " these TSPECs right now, what would your answer be?". The essential difficant differences and the provide the semantics of the reservation service so that it is equivalent to " these TSPECs right now, what would your answer be?". The essential difficant difficant differences and the provide the semantics of the reservation service so that it is equivalent to " these TSPECs right now, what would your answer be?". The essential difficant difficant differences and the provide the semantics of the reservation service so that it is equivalent to " these TSPECs right now, what would your answer be?". The essential difficant difficant differences and the provide the semantics of the reservation service so that it is equivalent to " these TSPECs right now, what would your answer be?". The essential difficant difficant differences and the provide the semantics of the reservation service so that it is equivalent to " these TSPECs right now, what would your answer be?". The essential difficant difficant differences and the provide the semantics of the reservation service so that it is equivalent to " these TSPECs right now, what would your answer be?". The essential difficant difficant differences and the provide the semantics of the reservation service setting to be an experiment of the reservation service setting the semantics of the reservation service setting the semantis of the reservation service setting the semantics of	ne wav - or to
ACCEPT IN PRINCIPLE. Changed to ", 2007 Edition" C/ D SC D P99 L58 # 112 CHAPLIN, CLINT F Comment Type TR Comment Status A dot11AuthenticationAlgorithm is an INTEGER, it is not "set of" anything like the description Modify the semantics of the reservation service so that it is equivalent to " Modify the semantics of the reservation service so that it is equivalent to " these TSPECs right now, what would your answer be?". The essential diff candidate AP discounts these queries when responding to local requests. The result is that a transitioning STA may occassionally be surprised to he refused, to the benefit of existing members of that BSS that are not unnec access to local resources. Response Status U	
Changed to ", 2007 Edition" Changed to ", 2007 Edition" CI D SC D P99 L58 # 112 CHAPLIN, CLINT F Comment Type TR Comment Status A dot11AuthenticationAlgorithm is an INTEGER, it is not "set of" anything like the description	
CI D       SC D       P99       L 58       # 112         CHAPLIN, CLINT F       Comment Type       TR       Comment Status A       The essential difficult of existing members of that BSS that are not unnected access to local resources.         Comment Type       TR       Comment Status A       Response       Response       Status II	"If I asked you for
CHAPLIN, CLINT F Comment Type TR Comment Status A dot11AuthenticationAlgorithm is an INTEGER, it is not "set of" anything like the description $Response Status U$	ference is that the
Comment Type TR Comment Status A refused, to the benefit of existing members of that BSS that are not unnec access to local resources.	ave its TSPECs
dot11AuthenticationAlgorithm is an INTEGER, it is not "set of" anything like the description Response Status U	cessarily denied
dot induced on Algorithm is an introduct, it is not set of anything like the description Response Response Status I	
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.

reservation protocol

C/ General SC General	P <b>0</b>	L <b>0</b>	# 1	13
CHAPLIN, CLINT F			l	

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.

Page 89 of 89