IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolution for WEP/TKIP removal | | | | |
| Date: 2022 - 11 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technology | Sunrise FL | 916 799 9563 | gsmith@srtrl.com |

Abstract

Green indicates material agreed to in the group,

yellow material to be discussed, red material rejected by the group and

cyan material not to be overlooked.

The “Final” view should be selected in Word.

R1 – Comments from Mark R. TSN and pre-RSNA added to search list and edits accordingly.

R2 – Remove “MIC michael”

R3 – check for “group cipher suite” 00-OF-AC:0 as well as :1 and :2

HISTORY

12.3 Pre-RSNA security methods

*2787.31 Except for Open System authentication, all pre-RSNA security mechanisms are obsolete. Support for them might be removed in a later revision of the standard. TSN security mechanisms are deprecated.*

Proposal back in 2018 was to delete WEP/TKIP and keep only the section on Open Authentication.

See 18/0162r1 for history of discussions in Berlin, and Orlando

The ‘killer” points in Orlando were:

* “This one gets complicated”. Certified devices are not supposed to accept WEP connections, but we have a mixed mode WPA2/WPA mixed mode, then you have to do the group key using TKIP, but that would be hard because we still need TKIP. While this is the case, we cannot take TKIP out.
* We know that there known implementation of WEP and TKIP in the market. We should not remove at this time.
* The Group did not come to consensus on removal of these two features. Agreed to add a non-consensus sentence to the REJECT resolution.
* The need to make a decision by the close out in January, and so we could reject for now, and then bring it up at a later time if we feel it appropriate.

It is now time to bite the bullet.

Following terms were searched for:WEP, TKIP, TSC, TTAK, ARC4, TSN, Pre-RSNA, MIC/micheal

Also group cipher suite 00-0F-AC:0

NOTE – 12.3 Non-RSNA security methods

TSN security mechanisms are deprecated

Jouni – “That concern on removing TKIP is still valid since TKIP is still implemented in more or less all new products. I think the appropriate step to take in REVme is to remove WEP as a standalone cipher while leaving TKIP (now obsoleted and subject to removal in the \_next\_ maintenance cycle). I've identified the changes needed for doing that.”

Dan – “removing TKIP from the standard will not prevent people from implementing it. Actually, I don't think there's anything we can do to stop people from implementing it. I would, I guess, like to hear what the issue is if it is removed, and people continue to put it in product”

The only point of Michael was to create TKIP. There is no use of Michael outside of TKIP so if your proposal is to do away with TKIP in its entirety (again, I applaud this) then all mention of Michael should be removed as well.

You should only remove MIC when it is specifically in the context of Michael, not when it's used for a generic message integrity code.

Thanks to Mark R for comments and pointers.

**RESOLUTION**

**REVISED**

***Note to Editor: 802.11REVme\_D2.0 is the base.***

Make changes as per below:

**NOTE: After implementing all the changes herein a check for WEP, TKIP, TSC, TTAK, TSN, pre-RSNA, michael, and ARC4 should be made to see if any references are still there where they should not be, i.e., only appear in “deprecated” MIBS.**

**218.6**

delete **~~message integrity code (MIC) key:~~** ~~Temporal key integrity protocol (TKIP) only: The portion of a transient key used to validate the integrity of medium access control (MAC) service data units (MSDUs) or MAC~~

~~protocol data units (MPDUs).~~

**218.15**

**~~michael:~~** ~~The message integrity code (MIC) for the temporal key integrity protocol (TKIP).~~

**228.18**

**robust security network** (RSN) “A security network that allows only the creation of robust security network associations (RSNAs). ~~An RSN can be identified by the indication in the RSN element (RSNE) of Beacon frames that the group cipher suite specified is not wired equivalent privacy (WEP).~~”

**234.6**

**temporal key (TK):** Temporal key integrity protocol. ~~(TKIP) only~~: ~~The combination of temporal encryption~~

~~key and a message integrity code (MIC) key. Non-TKIP only:~~ A temporal encryption key.(#1505)When

abbreviated this is, unless explicitly shown otherwise, specifically the key used to protect individually

addressed frames, as distinct from e.g., the TK that is the group temporal key (GTK).

**234.35**

**~~transition security network (TSN):~~** ~~A security network that allows the creation of pre-robust security~~

~~network associations (pre-RSNAs) as well as RSNAs.~~ ~~A TSN is identified by the indication in the robust~~

~~security network element (RSNE) of Beacon frames that the group cipher suite in use is wired equivalent~~

~~privacy (WEP).~~

**240.57**

delete **~~wired equivalent privacy (WEP)~~**~~” An obsolete cryptographic data confidentiality algorithm specified bythis standard.~~

**254.4**

delete ~~TKIP temporal key integrity protocol~~

**254.28**

delete ~~TSC TKIP sequence counter~~

**254.32**

Delete~~TSN transition security network~~

**254.35**

delete ~~TTAK TKIP mixed transmitter address and key~~

**255.20**

delete ~~WEP wired equivalent privacy~~

**311.50**

“IEEE Std 802.11 defines ~~five~~ four IEEE 802.11 authentication methods: Open System authentication, ~~Shared~~

~~Key authentication,~~ FT authentication, simultaneous authentication of equals (SAE), and FILS authentication. Open System authentication admits any STA to the DS. ~~Shared Key authentication relies on WEP to demonstrate knowledge of a WEP encryption key~~.

**313.26** 4.5.4.4

IEEE Std 802.11 provides several cryptographic algorithms to protect data traffic, including ~~TKIP,~~

CCMP~~,~~ and GCMP. ~~TKIP is based on the ARC4~~~~20~~ ~~algorithm, and~~ CCMP and GCMP are based on the

advanced encryption standard (AES). A means is provided for STAs to select the algorithm(s) to be used for

a given association.

**313.62**

Delete Footnote 20

**343.46**

5.1.2 Security services

~~WEP is obsolete. The WEP algorithm is unsuitable for the purposes of this standard.~~

~~The use of TKIP is (#1643)obsolete. The TKIP algorithm is unsuitable for the purposes of this standard.~~

~~A STA that has associated with management frame protection enabled shall not use pairwise cipher suite~~

~~selectors WEP-40, WEP-104, TKIP, or “Use group cipher suite.”~~

~~A mesh STA with dot11MeshSecurityActivated equal to true shall not use the pairwise cipher suite selectors~~

~~WEP-40, WEP-104, or TKIP.~~

~~An S1G STA shall not use the pairwise cipher suite selectors WEP-40, WEP-104, TKIP, or “Use group~~

~~cipher suite”.~~

**368.47**

Delete row ~~MIC (michael) failure event MICHAELMICFAILURE 7 etc.~~

**491.22** MLME-SETKEYS.request

0–3 shall be used

with ~~WEP, TKIP,~~

CCMP, and

GCMP;

4–5 with BIP for

IGTK; 6-7 with

BIP for BIGTK;

(11ba)8–9 with

BIP for WIGTK;

and 10–4095 are

reserved

**492.10**

When the Key Type parameter is Pairwise or PeerKey, and the Key, Key ID, and Address (where

valid) parameters identify a new key to be set, the MAC shall initialize the transmitter ~~TSC/~~PN

counter and the receiver replay counter(s) to 0. When the Key Type parameter is not Pairwise or

PeerKey, and the Key, Key ID, and Address (where valid) parameters identify a new key to be set,

the MAC shall initialize, depending on the direction of the traffic, the transmitter ~~TSC/~~PN/IPN/

BIPN/WIPN counter to 0 or 1 (see Clause 12 (Security) and Clause 29 (Wake-Up Radio (WUR)

MAC specification(11ba))) or the receiver replay counter(s) to the value in the Receive Sequence

Count parameter. When the Key Type, Key, Key ID, and Address (where valid) parameters identify

an existing key, the MAC shall not change the transmitter ~~TSC/~~PN/IPN/BIPN/WIPN counter or the

receiver replay counter(s) associated with that key

**493.3** MLME-DELETEKEYS.request

0–3 shall be used

with ~~WEP, TKIP,~~

CCMP, and

GCMP;

4–5 with BIP for

IGTK; 6-7 with

BIP for BIGTK;

(11ba)8–9 with

BIP for WIGTK;

and 10–4095 are

reserved

**525.10**

6.6.7 ESS status reporting 6.6.7.1.3 When generated

This primitive is generated when the ESS link to a network of APs is available to exchange Data frames. The

generation of this primitive may vary depending on ~~the contents of dot11WEPDefaultKeysTable and~~

~~dot11WEPKeyMappingsTable and~~ the setting of dot11RSNAOptionImplemented.

If ~~there are no entries in the dot11WEPDefaultKeysTable, no entry for the current AP in~~

~~dot11WEPKeyMappingsTable, and~~ dot11RSNAOptionImplemented is false, then the network does not use

encryption. This event is generated upon receipt of an MLME-ASSOCIATE.confirm primitive with a result

code of success.

If ~~there are entries in the dot11WEPDefaultKeysTable, or an entry for the current AP in~~

~~dot11WEPKeyMappingsTable, or~~ dot11RSNAOptionImplemented is true, then the network requires the use

of encryption on the link. Before declaring that the link is ready to exchange Data frames, the convergence

function receives an MLME-ASSOCIATE.confirm primitive with a result code of success and the SME emits

an MLME-SETKEYS.request primitive. The latter primitive is used to determine ~~that a WEP key is available,~~

~~or~~ that the RSN 4-way handshake has completed.

**526.23**

Table 6-2 and 527.32 Table 6-3

KEY\_EXPIRATION (#1382 A security association has expired due to time or traffic limitations~~,~~

~~or TKIP countermeasures have invalidated the key hierarchy~~.

**583.2**

The Protected Frame subfield is set to 0 in Data frames of subtype Null, QoS Null,

QoS CF-Poll, and QoS CF-Ack +CF-Poll (see, for example, ~~12.3.4.2 (TKIP MPDU formats) and~~ 12.5.2.1

(General) that show that the frame body needs to be 1 octet or longer to apply the encapsulation).

**620.61**

— The presence of security encapsulation (e.g., ~~TKIP,~~ CCMP or GCMP header and MIC).

**621.7**

Delete ~~NOTE 2—TKIP is not allowed with A-MSDUs (see 12.2.5 (RSNA assumptions and constraints)) or MMPDUs (see 12.5.3.1 (BIP overview)) and, therefore, need not be taken into account if a maximum A-MSDU or MMPDU size constraint applies~~.

**683.63** 9.3.2.1.1

NOTE 1—The maximum frame body size shown in Figure 9-111 (Data frame format) is for GCMP encryption of a maximum-size A-MSDU (note that ~~TKIP encryption is not allowed in this case and~~ any Mesh Control fields are part of the A-MSDU subframes). The corresponding maximum for CCMP encryption is 7951 octets. The maximum frame body size if A-MSDUs are not used is 2346 octets for GCMP encryption of a maximum-size MSDU, 2338 octets for CCMP encryption of a maximum-size MSDU ~~and 2342 octets for TKIP encryption of a maximum-size MSDU~~, including in both cases an 18-octet Mesh Control field.

**752.46 Table 9-77 Reason codes**

18 ~~REASON\_INVALID\_GROUP\_CIPHER~~ ~~Invalid group cipher~~ Reserved

**757.23 Table 9-78 Status codes**

41 ~~STATUS\_INVALID\_GROUP\_CIPHER~~ ~~Invalid group cipher~~ Reserved

**At 967.15 and 967.26**,

IEEE 802.1X authentication, CCMP-128 pairwise and group data cipher suites ~~(WEP-40, WEP-104, and~~

~~TKIP not allowed)~~:

**967.37**

IEEE 802.1X authentication, Use GTK for pairwise cipher suite, ~~WEP-40 group data cipher suites,~~ optional

RSN Capabilities field omitted:

30, // Element id, i.e., 48 in decimal(#1849)(#1850)

12, // Length in octets, i.e., 18 in decimal(#1849)(#1850)

01 00, // Version 1

~~00 0F AC 01, // WEP-40 as group data cipher suite~~

01 00, // Pairwise cipher suite count(#1850)

~~00 0F AC 00, // Use group cipher suite as pairwise cipher suite~~

01 00, // Authentication count(#1850)

00 0F AC 01 // IEEE 802.1X authentication

**968.61**

Table 9-189- Cipher suite selectors

Delete following rows in Table 9-189

~~“00-0F-AC 0 Use group cipher suite”~~

~~“00-0F-AC 1 WEP-40”~~

~~“00-0F-AC 2 TKIP”~~

~~“00-0F-AC 5 WEP-104”~~

**969.52**

~~The cipher suite selectors 00-0F-AC:1 (WEP-40) and 00-0F-AC:5 (WEP-104) are only valid as a group~~

~~cipher suite in a transition security network (TSN) to allow pre-RSNA STAs to join an IBSS or to associate~~

~~with an infrastructure BSS.~~

~~Use of any group cipher suite other than TKIP, WEP-104, or WEP-40 with TKIP as the pairwise cipher suite~~

~~is not supported.~~

~~The cipher suite selector 00-0F-AC:0 (Use group cipher suite) is valid only as the pairwise cipher suite. An~~

~~AP specifies the selector 00-0F-AC:0 (Use group cipher suite) for a pairwise cipher suite if it does not~~

~~support any pairwise cipher suites. If an AP specifies 00-0F-AC:0 (Use group cipher suite) as the pairwise~~

~~cipher selection, this is the only pairwise cipher selection the AP advertises.~~

**970.1**

If an AP advertises a group cipher suite ~~other than TKIP, WEP-104, or WEP-40,~~ then the AP supports

pairwise keys~~, and thus the pairwise suite selector 00-0F-AC:0 (Use group cipher suite) is not a valid option.~~

**970.13**

Table 9-187 – Cipher suite usage

Delete rows:

~~“WEP-40 Yes No No”~~

~~“WEP-104 Yes No No”~~

~~“TKIP Yes Yes No”~~

**978.1**

9.4.2.24.4 RSN capabilities

Bit 1: No Pairwise. ~~If a STA supports WEP default key 0 simultaneously with a pairwise key~~

~~(see 12.7.1 (Key hierarchy)), then the STA sets the No Pairwise subfield(#1801) to 0~~.

~~If a STA does not support WEP default key 0 simultaneously with a pairwise key (see 12.7.1 (Key~~

~~hierarchy)), then the STA sets the No Pairwise subfield(#1801) to 1.~~

The No Pairwise subfield describes a capability of a non-AP STA. IBSS STAs and APs set the No

Pairwise subfield to 0.

~~The No Pairwise subfield is set to 1 only in a TSN and when the pairwise cipher suite selected by the~~

~~STA is TKIP~~.

Bits 2–3: PTKSA Replay Counter. A STA sets the PTKSA Replay Counter subfield(#1801) to the

value contained in dot11RSNAConfigNumberOfPTKSAReplayCounters(#1391). See ~~12.3.4.6~~

~~(TKIP replay protection procedures) and~~ 12.5.2.4.4 (PN and replay detection). The meaning of the

value in the PTKSA/GTKSA Replay Counter subfield is defined in Table 9-189 (PTKSA/GTKSA/

TPKSA replay counters usage).

**978.31**

Bits 4–5: GTKSA Replay Counter. A STA sets the GTKSA Replay Counter subfield(#1801) to the

value contained in dot11RSNAConfigNumberOfGTKSAReplayCounters(#1391). See ~~12.3.4.6~~

~~(TKIP replay protection procedures) and~~ 12.5.2.4.4 (PN and replay detection). The meaning of the

value in the GTKSA Replay Counter subfield is defined in Table 9-189 (PTKSA/GTKSA/TPKSA

replay counters usage).

**1038.53**

The RSC ~~for TKIP is the TKIP sequence counter (TSC);~~ for CCMP and GCMP ~~it~~ is the packet number (PN); see Table 12-9 (RSC field(#1406)).

**1038.58**

~~For WEP, the RSC (#1406)field is reserved.~~

**1045.58**

**Delete 9.4.2.54 MME in its entirety**

**1158.58**

The (#1406)RSC denotes the last ~~TSC or~~ PN sent using the GTK and is specified in Table 12-9 (RSC

field(#1406)) of 12.7.2 (EAPOL-Key frames)

**1264.48** 9.4.2.185

The RSC ~~for TKIP is the TKIP sequence counter (TSC);~~ for CCMP and GCMP ~~it~~ is the packet number (PN); see Table 12-9 (RSC field(#1406)).

**1633.60**

The RSC ~~for TKIP is the TKIP sequence counter (TSC);~~ for CCMP and GCMP ~~it~~ is the packet number (PN); see Table 12-9 (RSC field(#1406)).

**2780.21**

12.2.1 Classes of security algorithm

This standard defines ~~two~~ a class~~es~~ of security algorithms for IEEE 802.11 networks~~:—~~ ~~Algorithms~~ for creating and using an RSNA, called *RSNA algorithms.*

~~— Pre-RSNA algorithms~~

~~NOTE—This standard does not prohibit STAs from simultaneously operating pre-RSNA and RSNA algorithms.~~

~~WEP is obsolete. The WEP algorithm is unsuitable for the purposes of this standard.~~

~~The use of TKIP is (#1643)obsolete. The TKIP algorithm is unsuitable for the purposes of this standard.~~

**2780.33**

Security Methods

12.2.2 Security methods

~~Pre-RSNA security comprises the following algorithms and procedures:~~

~~— WEP, described in 12.3.2 (Wired equivalent privacy (WEP))~~

~~— IEEE 802.11 entity authentication, described in 12.3.3 (Pre-RSNA authentication)~~

RSNA security comprises the following algorithms and procedures:

~~— TKIP, described in 12.5.2 (CTR with CBC-MAC protocol (CCMP))~~

~~(#1433)NOTE—TKIP is not however considered a robust security network mechanism.~~

— CCMP, described in 12.5.2 (CTR with CBC-MAC protocol (CCMP))

— GCMP, described in 12.5.4 (GCM protocol (GCMP))

— BIP, described in 12.5.3 (Broadcast/multicast integrity protocol (BIP))

— RSNA establishment and termination procedures, including use of IEEE 802.1X authentication,

described in 12.6 (RSNA security association management), SAE authentication described in 12.4

(Authentication using a password), and OWE described in IETF RFC 8110(#1084).

— Key management procedures, described in 12.7 (Keys and key distribution)

**2781.6 12.2.3**

When dot11RSNAActivated is true, a STA uses the RSNE to advertise support for RSNAs. When

dot11RSNAActivated is true, a DMG STA shall set the DMG Privacy subfield to 1 within transmitted DMG

Beacon frames. ~~A pre-RSNA STA is not capable of creating RSNAs.~~

**2784.49**

~~An HT STA shall not use either of the pairwise cipher suite selectors: “Use group cipher suite” or TKIP to~~

~~communicate with another HT STA.~~

~~NOTE—Because a VHT STA is also an HT STA, the elimination of TKIP also applies to VHT STAs.~~

***2787.22, editor- rename 12.3 as shown and then make the following changes***

**12.3 ~~Non-RSNA security methods~~ Open System authentication**

***Editor – delete and renumber as follows***

**Delete 12.3.1 to 12.3.2.4 and heading 12.3.3. in their entirety**

**Renumber 12.3.3.1 as 12.3.1 “Overview”**

**Delete heading 12.3.3.2 “Open System authentication” and Renumber 12.3.3.2 as 12.3.2 “General”**

**Renumber 12.3.3.2.2 as 12.3.3 “Open System authentication (first frame)”**

**Renumber 12.3.3.2.3 as 12.3.4 “Open System authentication (final frame)”**

**Delete 12.3.3.3 in its entirety**

**Delete 12.3.4 Temporal key integrity protocol (TKIP) in its entirety**

***Editor – make edits as shown***

**2834.62**

**2835.52**

The ExtIV subfield (bit 5) of the Key ID octet signals that the CCMP Header field extends the MPDU header

by a total of 8 octets~~, compared to the 4 octets added to the MPDU header when WEP is used~~. The ExtIV

subfield is always set to 1 for CCMP.

**2864.58**

~~In an RSN, an AP shall not associate with pre-RSNA STAs, i.e., with STAs that fail to include the RSNE in the~~

~~(Re)Association Request frame.~~

**2865.4** 12.6.3.

~~An HT STA shall eliminate TKIP as a choice for the pairwise cipher suite if CCMP-128 or CCMP-256 is advertised by the AP or if the AP included an HT Capabilities element in its Beacon and Probe Response frames. The elimination of TKIP as a choice for the pairwise cipher suite may result in a lack of overlap of the remaining pairwise cipher suite choices, in which case the STA shall decline to create an RSN association with that AP~~.

**2864.18**

In order to accommodate local security policy, a STA may choose not to associate with an AP that does not

support any pairwise cipher suites. ~~An AP may indicate that it does not support any pairwise keys by~~

~~advertising 00-0F-AC:0 (Use group cipher suite) as the pairwise cipher suite selector.~~

**2867.38**

Delete 12.6.4 TSN policy selection in an infrastructure BSS. In its entirety

**2868.1** 12.6.5

~~An HT STA that is in an IBSS or that is transmitting frames through a (#2152)TDLS direct link shall eliminate~~

~~TKIP as a choice for the pairwise cipher suite if CCMP-128 or CCMP-256 is advertised by the other STA or if~~

~~the other STA included an HT Capabilities element in any of its Beacon or Probe Response frames.~~

~~NOTE 1—The elimination of TKIP as a choice for the pairwise cipher suite might result in a lack of overlap of the~~

~~remaining pairwise cipher suite choices, in which case the STAs do not exchange encrypted frames.~~

**2869.40**

Delete 12.6.6 TSN policy selection in an IBSS, in its entirety

**2869.56** 12.6.7

RSNA policy is advertised in Beacon frames and Probe Response frames. A mesh STA identifies a candidate

peer by parsing its neighbor STA’s Beacon frames and Probe Response frames (see 14.2 (Mesh discovery)).

~~An HT mesh STA shall eliminate TKIP as a choice for the pairwise cipher suite if CCMP-128 or CCMP-256 is~~

~~advertised by the peer or if the peer included an HT Capabilities element in any of its Beacon or Probe~~

~~Response frames.~~

**2885.18** 12.7.1.1

In an infrastructure BSS, the IEEE 802.1X Authenticator MAC address (AA) and the AP’s MAC address are

the same, and the Supplicant’s MAC address (SPA) and the STA’s MAC address are equal. For the purposes of

comparison in this standard, the MAC address is encoded as 6 octets, taken to represent an unsigned integer.

The first octet of the MAC address shall be used as the most significant octet. The bit numbering conventions

in 9.2.2 (Conventions) shall be used within each octet. This results in a sequence of 48 bits represented such

that bit 0 is the first transmitted bit (Individual/Group bit) and bit 47 is the last transmitted bit.

An RSNA STA shall support at least one pairwise key for any <TA,RA> pair for use with RSNA

mechanisms. ~~The <TA,RA> identifies the pairwise key, which does not correspond to any WEP key identifier~~

(#432)~~In a a mixed environment, an AP may simultaneously communicate with some STAs using WEP with~~

~~shared WEP keys and to STAs using RSNA mechanisms with pairwise keys. The STAs running WEP use~~

~~default keys 0–3 for shared WEP keys; the important point here is that WEP can still use WEP default key 0.~~

~~The AP might be configured to use the WEP key in WEP default key 0 for WEP; if the AP is configured in this~~

~~way, STAs that cannot support WEP default key 0 simultaneously with a TKIP pairwise key shall specify the~~

~~No Pairwise subfield in the RSN Capabilities field. If an AP is configured to use WEP default key 0 as a WEP~~

~~key and a “No Pairwise” STA associates, the AP shall not set the Install bit in the 4-way handshake. In other~~

~~words, the STA does not install a pairwise temporal key and instead uses WEP default key 0 for all traffic.~~

~~NOTE 2—The behavior of “No Pairwise” STAs is intended only to support the migration of WEP to RSNA.~~

~~TKIP STAs in a mixed environment are expected to support a single pairwise key either by using a key~~

~~mapping key or by mapping to default key 0. The AP uses a pairwise key for individually addressed traffic~~

~~between the AP and the STA. If a key mapping key is available, the <RA,TA> pair identifies the key; if there is~~

~~no key mapping key, then the default key 0 is used because the key index in the message is 0.~~

~~A STA that cannot support TKIP keys and WEP default key 0 simultaneously advertises this deficiency by~~

~~setting the No Pairwise subfield in the RSNE it sends in the (Re)Association Request frame to the AP. In~~

~~response, the AP sets the Install bit to 0 in message 3 of the 4-way handshake to notify the STA not to install~~

~~the pairwise key. The AP instead sends the WEP shared key to the STA to be plumbed as the WEP default~~

~~key 0; this key is then used with WEP to send and receive individually addressed traffic between the AP and~~

~~the STA.~~

~~The TKIP STA that has this limitation might not know that it will be forced to use WEP for all transmissions~~

~~until it has associated with the AP and been given the keys to use. (The STA cannot know that the AP has been~~

~~configured to use WEP default key 0 for WEP communication.) If this does not satisfy the security policy~~

~~configured at the STA, the STA’s only recourse is to disassociate and try a different AP.~~

~~(#432)STAs using RSNA mechanisms in a TSN shall support pairwise keys and WEP default key 0~~

~~simultaneously. It is invalid for the STA to negotiate the No Pairwise subfield when an RSNA mechanism~~

~~other than TKIP is one of the configured ciphers.~~

**2888.38**

**Editor - Delete NOTE 2 and renumber NOTE 3 to NOTE 2**

**2900.21** 12.7.2 EAPOL-Key frames

1) Key Descriptor Version (bits 0–2) shall be set to 0 on all transmitted (#1836)EAPOL-Key

PDUs indicating that the (#1836)EAPOL-Key PDU is constructed and processed according to

the negotiated AKM as described in Table 12-11 (Integrity and key wrap algorithms) ~~except~~

~~under the following circumstances:~~

~~i) The value 1 shall be used for all (#1836)EAPOL-Key PDUs to a STA when the negotiated~~

~~AKM is 00-0F-AC:1 or 00-0F-AC:2 and the pairwise cipher is TKIP or “Use group cipher~~

~~suite”. In this case, the “Deprecated” row in Table 12-11 (Integrity and key wrap algorithms)~~

~~is used.~~

~~ii) (#432)The value 2 shall be used for all (#1836)EAPOL-Key PDUs to a STA when the~~

~~negotiated AKM is 00-0F-AC:1 or 00-0F-AC:2 and either the pairwise or the group cipher~~

~~is an RSNA mechanism other than TKIP. In this case, the matching row in Table 12-11~~

~~(Integrity and key wrap algorithms) is used~~.

**2901.13**

8) Error (bit 10) is set to ~~1 by a Supplicant to report that a MIC failure occurred in~~

~~a TKIP MSDU (in which case the Request (bit 11) is also set to 1); it is set to~~ 0 ~~otherwise~~.

**2902**

“Table 12-8—Cipher suite key lengths”

Delete row – ~~“TKIP 32 256.”~~

**2903.6**

g) (#1406)**RSC**. This field contains the current receive sequence counter (RSC) for the GTK being

installed. It is used in message 3 of the 4-way handshake and message 1 of the group key handshake,

where it is used to synchronize the IEEE 802.11 replay state. ~~It may also be used in the Michael MIC~~

~~Failure Report frame, to report the TSC field value of the frame experiencing a MIC failure.~~ It shall

contain 0 in other messages. If the RSC is less than 8 octets in length, it is stored in the first octets

and the remaining octets are set to 0. The least significant octet of the RSC is in the first octet of the

(#1406)RSC field. The RSC ~~for TKIP is the TKIP sequence number (TSC);~~ for CCMP and GCMP it

is the packet number (PN); see Table 12-9 (RSC field(#1406)).

**2903.26**

Just after “Table 12-5 Key RSC field”, delete “~~For WEP the field is reserved~~.”

**2908.34** 12.7.3 EAPOL-Key frame construction and processing

edit as shown

Table 12-11 (Integrity and key wrap algorithms) indicates the particular algorithms to use when constructing

and processing EAPOL-Key frames and FT authentication sequence. ~~The AKM of “Deprecated” indicates an~~

~~AKM of 00-0F-AC:1 or 00-0F-AC:2 when either TKIP or “Use group cipher suite” is the negotiated pairwise~~

~~cipher.~~ For ~~all other~~ AKMs the negotiated pairwise cipher suite does not influence the algorithms used to

process EAPOL-Key frames.

**2909.8 Table 12-11**

**Delete Row ~~“~~**~~Deprecated HMAC-MD5 128 16 ARC4 128 0 0”~~

**2913.12**

Key Descriptor Version = ~~1 (ARC4 encryption with HMAC-MD5) or~~ 2 (NIST AES key wrap

with HMAC-SHA-1-128) or 3 (NIST AES key wrap with AES-128-CMAC), in all other

cases 0

**2914.4**

Key Descriptor Version = ~~1 (ARC4 encryption with HMAC-MD5) or~~ 2 (NIST AES key wrap

with HMAC-SHA-1-128) or 3 (NIST AES key wrap with AES-128-CMAC), in all other

cases 0 – same as message 1

**2915.50 12.7.6.4**

Key Descriptor Version = ~~1 (ARC4 encryption with HMAC-MD5) or~~ 2 (NIST AES key wrap

with HMAC-SHA-1-128) or 3 (NIST AES key wrap with AES-128-CMAC), in all other

cases 0 – same as message 1

**2916.13**

RSC = ~~Starting TSC or~~ PN that the Authenticator’s STA uses in MPDUs protected by GTK.

**2918.18**

Key Descriptor Version = ~~1 (ARC4 encryption with HMAC-MD5) or~~ 2 (NIST AES key wrap

with HMAC-SHA-1-128) or 3 (NIST AES key wrap with AES-128-CMAC), in all other

cases 0 – same as message 1

**2919.29**  12.7.6.6 4-way handshake implementation considerations

**edit as shown**

An implementation should save the KCK and KEK beyond the 4-way handshake, as they are needed for group

key handshakes~~, and recovery from TKIP MIC failures~~.

**2922.49**

RSC denotes the last ~~TSC or~~ PN sent using the GTK.

**2923.31 12.7.7.2**

Key Descriptor Version = ~~1 (ARC4 encryption with HMAC-MD5) or~~ 2 (NIST AES key wrap

with HMAC-SHA-1-128) or 3 (NIST AES key wrap with AES-128-CMAC), in all other

cases 0

**2923.55**

RSC denotes the last ~~TSC or~~ PN sent using the GTK.

**2924.45 12.7.7.3**

Key Descriptor Version = ~~1 (ARC4 encryption with HMAC-MD5) or~~ 2 (NIST AES key wrap

with HMAC-SHA-1-128) or 3 (NIST AES key wrap with AES-128-CMAC), in all other

cases 0 – same as message 1

**2925.57**

It sends an (#1836)EAPOL-Key PDU containing the GTK, IGTK and BIGTK (message 1), along with the last ~~TSC or~~ PN used with the GTK (RSC), the last IPN used with the IGTK and the last BIPN used with the BIGTK.

**2926.39**

The TPK security protocol is executed between the two non-AP STAs that intend to establish an RSNA for

(#2152)TDLS direct link(#1356) communication. If any security method (~~pre-RSNA or~~ RSNA) is enabled on

the connection between a STA and the AP, the STA shall require that the TPK security protocol complete

successfully before using a (#2152)TDLS direct link.

**2926.46**  12.7.8.1

Delete “~~NOTE—A STA might refuse to set up a TDLS direct link(#2152) when the STA link to the AP is~~

~~secured with WEP-40, WEP-104 or TKIP, or is unsecured~~”

**2926.62** 12.7.8.2

a STA may refuse to initiate the TDLS direct link if ~~a) Tt~~he AP does not include an RSNE in its Beacon and Probe Response frames to advertise the availability of security~~;~~ .

~~b) The AP’s RSNE indicates that WEP-40 (00-0F-AC:1) or WEP-104 (00-0F-AC:5) or TKIP (00-0FAC:~~

~~2) are enabled as either pairwise or group cipher suites;(#223) or~~

~~c) The AP’s RSNE indicates that Use group cipher suite (00-0F-AC:0) is used as the pairwise cipher~~

~~suite~~

12.7.8.4.2 TPK handshake message 1

**2929.9**

The pairwise cipher suite list field shall indicate the pairwise cipher suites the TDLS

initiator STA is willing to use with the TPKSA. ~~WEP-40, WEP-104, and TKIP shall not be~~

~~included in this list.~~

**2929.52**

If none of the pairwise cipher suites are acceptable~~, or pairwise ciphers include WEP-40,~~

~~WEP-104, or TKIP,~~ then the TDLS responder STA shall reject the TDLS Setup Request frame

with status code STATUS\_INVALID\_PAIRWISE\_CIPHER.

12.7.9.3 Supplicant state machine variables

**2933.47**

~~—~~ *~~IntegrityFailed.~~* ~~The Supplicant sets this variable to true when its STA reports that a fatal data~~

~~integrity error (e.g., michael failure) has occurred~~.

~~NOTE—A michael failure is not the same as MICVerified because IntegrityFailed is generated if the michael integrity check fails; MICVerified is generated from validating the EAPOL-Key integrity check. Note also the STA does not generate this event for ciphers other than TKIP because countermeasures are not required.~~ “.”

**2943.3 Delete subclause “12.8.1 Mapping PTK to TKIP keys”**

**2943.18 Delete subclause “12.8.2 Mapping GTK to TKIP keys”**

**2943.47 Delete subclause “12.8.5 Mapping GTK to WEP-40 keys”**

**2943.54** **Delete subclause “12.8.6 Mapping GTK to WEP-104 keys”**

**2963.27** 12.12.2 Security constraints in the 6 GHz band

The following apply to a STA operating in the 6 GHz band:

— The STA shall not use Open System authentication without encryption. ~~the following pre-RSNA security methods:~~

~~— WEP~~

~~— Open System authentication without encryption~~

~~— Shared Key authentication~~

~~— The STA shall not use 00-0F-AC:0 (Use group cipher suite).~~

~~the following cipher suite selectors:~~

~~— 00-0F-AC:0 (Use group cipher suite)~~

~~— 00-0F-AC:1 (WEP-40)~~

~~— 00-0F-AC:2 (TKIP)~~

~~— 00-0F-AC:5 (WEP-104~~)

14.5.2.1 Instance Pairwise Cipher Suite selection

**3032.41** Delete as shown

“~~Pairwise cipher suite selectors WEP-40, WEP-104, and TKIP shall not be used as the pairwise cipher suite when dot11MeshSecurityActivated, dot11ProtectedTXOPNegotiationActivated, or~~

~~dot11ProtectedQLoadReportActivated is true.”.~~

14.5.2.2 Group cipher suite selection

**3033.18** Delete as shown

~~“Group cipher suite selectors WEP-40, WEP-104, and TKIP shall not be used as the group cipher suite when dot11MeshSecurityActivated is true.”~~

B.4.4.1 MAC protocol capabilities

**4633.16**

**Delete PC2 PC2.1 and PC2.2 entry**

**4640.9**

**Delete rows PC34.1.2.2, PC34.1.2.2.1, PC34.1.2.2.2, PC34.1.2.2.3, PC34.1.2.2.4**

Item PC 34.1.10

**4642.6 in “References” column, delete the following:**

12.5.2.1.2 (TKIP cryptographic encapsulation),

12.5.2.1.3 (TKIP decapsulation),

12.5.2.2 (TKIP MPDU formats),”

C.3 MIB detail

**4891.6** Change “WEPKeytype ::= TEXTUAL-CONVENTION” STATUS to “Deprecated”

**4896.23** Change STATUS “dot11PrivacyOptionImplemented” to “Deprecated”

**4941.13** Change STATUS “dot11WEPDefaultKeysTable” to Deprecated

**4941.25** Change STATUS “dot11WEPDefaultKeysEntry” to Deprecated

**4941.37** Change STATUS “dot11WEPDefaultKeysIndex” to Deprecated

**4941.52** Change STATUS “dot11WEPDefaultKeyValue” to Deprecated

**4942.8** Change STATUS “dot11WEPKEYMappingsTable” to Deprecated

**4942.22** Change STATUS “dot11WEPKEYMappingsEntry” to Deprecated

**4942.51** Change STATUS “dot11WEPKEYMappingsAddress” to Deprecated

**4942.60** Change STATUS “dot11WEPKEYMappingsWEPOn” to Deprecated

**4943.5** Change STATUS “dot11WEPKEYMappingValue” to Deprecated

**4943.13** Change STATUS “dot11WEPKEYMappingStatus” to Deprecated

**4943.52** Edit as shown

Dot11PrivacyEntry ::=

SEQUENCE {

dot11PrivacyInvoked TruthValue,

~~dot11WEPDefaultKeyID Unsigned32,~~

~~dot11WEPKeyMappingLengthImplemented Unsigned32,~~

dot11ExcludeUnencrypted TruthValue,

~~dot11WEPICVErrorCount Counter32,~~

~~dot11WEPExcludedCount Counter32,~~

dot11RSNAActivated TruthValue,

dot11RSNAPreauthenticationActivated TruthValue }

**4944.8** Edit as shown

When this attribute is true, it indicates that some level of security is invoked for transmitting Data frames. ~~For WEP-only clients, the security mechanism used is WEP.~~

For RSNA non-AP STAs, an additional variable dot11RSNAActivated indicates whether RSNA is enabled. ~~If dot11RSNAActivated is false or the MIB attribute does not exist, the security mechanism invoked is WEP I~~f

dot11RSNAActivated is true, RSNA security mechanisms invoked are configured in the dot11RSNAConfigTable."

~~For WEP-only clients, the security mechanism used is WEP.~~

**4944.20** Change STATUS “WEPDefaultKeyID” to Deprecated

**4944.35** Change STATUS “WEPKeyMappingLengthImplemented” to Deprecated

**4944.63** Change STATUS “WEPICVErrorCount” to Deprecated

**4945.14** Change STATUS “WEPExcludeCount” to Deprecated

**4956.29** Change STATUS “RSNATKIPCounterMeasuresInvoked” to Deprecated

**4956.7 edit as shown**

This object indicates the length of the pairwise cipher key. This should be ~~256 for TKIP and~~ 128 or 256 for CCMP and 128 or 256 for GCMP."

**4961.7** dot11RSNAConfigPairwiseCipherSizeImplemented OBJECT-TYPE

This object indicates the length of the pairwise cipher key. This should be ~~256 for TKIP and~~ 128 or 256 for CCMP and 128 or 256 for GCMP.

**4962.43 delete from list the following**

~~dot11RSNAStatsTKIPICVErrors~~

~~dot11RSNAStatsTKIPLocalMICFailures~~

~~dot11RSNAStatsTKIPRemoteMICFailures~~

~~dot11RSNAStatsTKIPReplays~~

**4963.37** Change STATUS “dot11RSNAStatsTKIPICVErrors OBJECT-TYPE” to Deprecated

**4963.37** Change STATUS “dot11RSNAStatsTKIPICVErrors OBJECT-TYPE” to Deprecated

**4963.49** Change STATUS “dot11RSNAStatsTKIPLocalMICFailures OBJECT-TYPE” to Deprecated

**4963.61** Change STATUS “dot11RSNAStatsTKIPRemoteMICFailures OBJECT-TYPE” to Deprecated

**4964.31** Change STATUS “dot11RSNAStatsTKIPReplays OBJECT-TYPE” to Deprecated

**5619.1**

Delete “J.1 TKIP temporal key mixing function reference implementation and test vector” in its entirety.

**5631.15**

Delete “J.2 Michael reference implementation and test vectors” in its entirety

**5644.38**

Delete “J.6.2 WEP cryptographic encapsulation” in its entirety

**5645.39**

Delete “J.6.3 TKIP test vector” in its entirety

**5652.18**

**Delete as shown in J.7.1**

The test vectors in this subclause provide an example of PTK derivation for ~~both~~ CCMP-128 ~~and TKIP~~**.**

**5652.57**

**Delete J.7.3 TKIP pairwise key derivation” in its entirelty**

K2.2 Deriving Medium Time

**5679.1**

Security Encapsulation Size = 16 (CCMP), 20 (GCMP ~~and TKIP~~), ~~8 (WEP)~~ or 0 (open system)