IEEE P802.11
Wireless LANs

|  |
| --- |
| PeerKey Deletion Cleanup |
| Date: February 2, 2018 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Menzo Wentink | Qualcomm | Utrecht, The Netherlands | +31-65-183-6231 | mwentink@qualcomm.com |
| Adrian Stephens | Intel |  |  |  |
| Emily Qi | Intel |  |  |  |

Abstract

This document contains some remaining items related to the deletion of the PeerKey protocol. Changes shown are relative to REVmd draft 1.0.

383.45 delete clause 6.3.23 (MLME-PEERKEY-START) (ends 384.24)

2231.64 edit as shown:

An AP with dot11ProtectedTXOPNegotiationActivated true that does not have an active security association with a peer AP that indicates support for protected HCCA TXOP negotiation shall use the AP PeerKey protocol (as defined in 12.11.2 (AP PeerKey protocol)) and authenticated mesh peering exchange (AMPE) (as defined in 14.5 Authenticated mesh peering exchange (AMPE)) to negotiate security parameters and create a new PMKSA and PTKSA to secure the Protected HCCA TXOP Advertisement frames. The use of AMPE proves possession of the PMK (generated using the procedures described in 12.11.2 (AP PeerKey protocol)) and implicitly the private key that corresponds to the peer’s public key.

2371.44 delete "- SMKSA: A result of a successful initial SMK handshake."

2390.48 delete "SMKSA, "

2416.13 delete "/SMK"

2427.14 delete "/SMK"

2427.16 delete "SMK Message = 0"

2428.12 delete "/SMK"

2435.31 move 12.7.8.5 (Supplicant state machine procedures) to behind 12.7.9.3 (Supplicant state machine variables)

2437.57 delete 12.7.8.6 (Supplicant PeerKey state machine states) (ends 2439.29)

2439.30 delete 12.7.8.7 (Supplicant PeerKey state machine variables) (ends 2440.3)

The following are MIB cleanup instructions, which revert deletions to markings as deprecated. Instructions with thanks to Adrian Stephens and Emily Qi:

Instructions to the editor:

For each of the following variables:

dot11RSNAConfigSTKKeysImplemented

dot11RSNAConfigSTKCipher

dot11RSNAConfigSTKRekeyTime

dot11RSNAConfigSMKUpdateCount

dot11RSNAConfigSTKCipherSize

dot11RSNAConfigSMKLifetime

dot11RSNAConfigSMKReauthThreshold

dot11RSNAConfigNumberOfSTKSAReplayCounters

dot11RSNAPairwiseSTKSelected

dot11RSNASMKHandshakeFailures

dot11NonAPStationAuthDls

dot11LsigTxopProtectionOptionImplemented

dot11RMNeighborReportHTInfoLSIGTXOPProtectionSup

dot11RTSLSIGSuccessCount and dot11RTSLSIGFailureCount

dot11PCOOptionImplemented

dot11RMNeighborReportHTPCO

dot11RMNeighborReportHTPCOTransitionTime

dot11RMNeighborReportHTInfoPCOActive

dot11RMNeighborReportHTInfoPCOPhase

dot11PCOActivated

dot11PCOFortyMaxDuration

dot11PCOTwentyMaxDuration

dot11PCOFortyMinDuration

dot11PCOTwentyMinDuration

dot11CFPMaxDuration

Copy the OBJECT definition from D0.5 (note that some of them may still present in D1.0. if so, no copy is needed).

Change its STATUS to “Deprecated”.

Insert a new first line in the DESCRIPTION: “Deprecated as the related feature has been removed from the standard”.

In D0.5, find any reference to the variable in any GROUPs and re-instate this reference.

Change the group’s STATUS to “Deprecated”.

In the DESCRIPTION, insert a new first line: “Superseded by YYYY.” (Note that “YYYY” is the new GROUP name.)

Note the GROUP name.

For each of the groups noted above, copy the group, set its status to “Current” and increment (or add) a number after the name of the group name (e.g. dot11SMTbase11 -> dot11SMTbase12).

Make the corresponding changes (e.g. add or remove MIB varables) in the new group.

For each reference to one of the noted groups from a compliance statement, update it to refer to the new group.