IEEE P802.11
Wireless LANs

|  |
| --- |
| Security parameter constraints |
| Date: 2019-11-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm, Inc. |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

This document discusses LB 244 (P802.11ax/D5.0) comment CID 22018 and proposes a resolution to it. The proposed changes introduce a new Clause 12 subclause to specify constraints on which security parameters cannot be used in various cases. This subclause is easily extensible to cover other cases, but the changes in this document address the specific item discussed in CID 22018 to cover operation in the new 6 GHz band.

r1:

* add forgotten PSK AKMs 00-0F-AC:19 and 00-0F-AC:20 to the shall-not-use list
* clarify language for the use-something-as-a-replacement descriptions to make them easier to understand
* add discussion on should vs. shall on the recommended replacement AKMs

**CID 22018**

LB 244 (P802.11ax/D5.0) CID 22018

Clause: 12 (no page/line identified)

Comment:

Disallow legacy security suites and smaller key sizes in 6 GHz including Pre-RSNA and TKIP

Proposed Change:

Disallow legacy security suites and smaller key sizes in 6 GHz including Pre-RSNA and TKIP

Discussion:

The comment is requesting legacy security options to be disallowed in the new 6 GHz band. While many of the legacy security options are already explicitly or implicitly disallowed for HE in general, such constraints on what can be enabled and negotiated are listed in various different locations in the standard and it may be helpful to provide a clear location for listing specific constraints on what shall not be used. Furthermore, 6 GHz makes it easier to push for stronger security since there is no legacy STAs to consider on the new band and as such, there is no need to allow legacy security options to be used for backwards compatibility.

The cleanest approach for addressing this comment seems to be introduction of a new subclause under Clause 12 (Security). P802.11ax can start this by defining the constraints for the new 6 GHz band. Future amendments may consider extending this to other bands and cases that place additional constraints on which security parameters are appropriate. This allows the standard to maintain description of legacy security functionality for backwards compatibility while still allowing clear push for more secure options by disabling legacy parameters where appropriate.

These subclauses can also recommend or require replacement mechanism to use instead of a legacy option. For the 6 GHz band, this case covers replacement of Open System authentication (without encryption) with Opportunistic Wireless Encryption and replacement of PSK with SAE. These replacements are described with “should” instead of “shall” since the IEEE 802.11 standard allows vendor specific AKMs to be used and it might be considered to be outside the scope of the standard to enforce a single option for these cases. However, if there is preference for using “shall” instead, that could be acceptable with the justification being that the standard itself does not provide acceptable other options.

**Proposed Resolution for CID 22018:**

REVISED – Agree with the commenter in principle. Introduce a new subclause to define which legacy security options are not allowed in 6 GHz.

TGax editor, please make changes as shown in <*this document*> in the “Proposed changes to the amendment” section.

**Proposed changes to the amendment**

**2. Normative references**

*Add the following reference into Clause 2:*

IETF RFC 8110, Opportunistic Wireless Encryption, D. Harkins, W. Kumari, March 2017.

**12. Security**

*Add the following subclauses at the end of Clause 12:*

**12.13 Constraints on allowed security parameters**

This standard defines various security mechanisms of which some are deprecated or obsolete and are not considered to meet current requirements for security. Such mechanisms enable interoperability with legacy devices, but are not suitable for new uses where legacy support is not needed. This subclause describes constraints on security parameter selection for some use cases.

**12.13.1 Security constraints in the 6 GHz band**

A STA operating in the 6 GHz band,

* shall not use the following pre-RSNA security methods: WEP, Open System authentication without encryption, Shared Key authentication
* shall not use cipher suite selector 00-0F-AC:0 (Use group cipher suite)
* shall not use cipher suite selector 00-0F-AC:1 (WEP-40)
* shall not use cipher suite selector 00-0F-AC:2 (TKIP)
* shall not use cipher suite selector 00-0F-AC:5 (WEP-104)
* should use Opportunistic Wireless Encryption, as specified in IETF RFC 8110, when connecting in an infrastructure BSS without authentication (as a replacement for Open System authentication without encryption)
* shall not use AKM suite selector 00-0F-AC:2 (PSK)
* shall not use AKM suite selector 00-0F-AC:4 (FT authentication using PSK)
* shall not use AKM suite selector 00-0F-AC:6 (PSK with SHA-256)
* shall not use AKM suite selector 00-0F-AC:19 (FT authentication using PSK with SHA-384)
* shall not use AKM suite selector 00-0F-AC:20 (PSK with SHA-384)
* should use SAE (AKM suite selectors 00-0F-AC:8 and/or 00-0F-AC:9) when authenticating using a password where IEEE Std 802.1X is not used (as a replacement for PSK)
* shall use management frame protection (MFPR=1) when using RSN