IEEE P802.11
Wireless LANs

|  |
| --- |
| RSN overriding |
| Date: 2024-01-05 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm Technologies, Inc. |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

This document proposed text changes to address IEEE P802.11-REVme/D4.0 CID 6087. This introduces new elements that allow the contents of the RSNE and the RSNXE to be overridden for STAs that have capability for the new mechanism while allowing already deployed devices to use the RSNE and the RSNXE. This targets deployment cases where already deployed STAs do not follow the rules for negotiating RSN parameters correctly and have issues connecting to an AP that enables multiple AKMs or pairwise ciphers and the deployed STA might not recognize some the advertized values, but instead of ignoring the unrecognized values, it might reject the full RSNE/BSS.

### Proposed changes for CID 6087

**9.3.3.2 Beacon frame format**

*Add two rows to Table 9-62 (Beacon frame body) before the Last-1 row (D4.1 P718 L19) as shown:*

|  |  |  |
| --- | --- | --- |
| 93 | RSNE Override | The RSNE Override element is present as defined in 12.14 (Overriding of RSN parameters). |
| 94 | RSNXE Override | The RSNXE Override element is present as defined in 12.14 (Overriding of RSN parameters). |
| Last – 1 | Vendor Specific | One or more Vendor Specific elements are optionally present. |

**9.3.3.5 Association Request frame format**

*Add a row to Table 9-64 (Association Request frame body) before the Last row (D4.1 P722 L29) as shown:*

|  |  |  |
| --- | --- | --- |
| 60 | RSNE Override | The RSNE Override element is present as defined in 12.14 (Overriding of RSN parameters). |
| Last | Vendor Specific | One or more Vendor Specific elements are optionally present. These elements follow all other elements. |

**9.3.3.7 Reassociation Request frame format**

*Add a row to Table 9-66 (Reassociation Request frame body) before the Last row (D4.1 P731 L24) as shown:*

|  |  |  |
| --- | --- | --- |
| 64 | RSNE Override | The RSNE Override element is present as defined in 12.14 (Overriding of RSN parameters). |
| Last | Vendor Specific | One or more Vendor Specific elements are optionally present. These elements follow all other elements. |

**9.3.3.10 Probe Response frame format**

*Add two rows to Table 9-69 (Probe Response frame body) before the Last-1 row (D4.1 P747 L15) as shown:*

|  |  |  |
| --- | --- | --- |
| 112 | RSNE Override | The RSNE Override element is present as defined in 12.14 (Overriding of RSN parameters). |
| 113 | RSNXE Override | The RSNXE Override element is present as defined in 12.14 (Overriding of RSN parameters). |
| Last – 1 | Vendor Specific | One or more Vendor Specific elements are optionally present. These elements follow all other elements, except the Requested elements.  |

**9.4.2 Elements**

**9.4.2.1 General**

*Add two rows to Table 9-130 as shown, obtain an assignment from ANA for <ANA-1> and <ANA-2>, and update the Reserved row accordingly.*

 **Table 9-130—Element IDs**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Element** | **Element ID** | **Element ID Extension** | **Extensible** | **Fragmentable** |
| Known STA Identification (see 9.4.2.298 (Known STA Identification element)) | 255 | 136 | Yes | No |
| RSNE Override (see 9.4.2.311 (RSNE Override element)) | 255 | <ANA-1> | Yes | No |
| RSNXE Override (see 9.4.2.312 (RSNXE Override element) | 255 | <ANA-2> | Yes | No |
| Reserved | 255 | 137-255 |  |  |

*Add two new subclauses at the end of 9.4.2, i.e., just before the start of 9.4.3 (REVme-D4.1 P1532 L9):*

**9.4.2.311 RSNE Override element**

The RSNE Override element contains an alternative RSNE. See Figure 9-XYZ (RSNE Override element format).

|  |  |  |  |
| --- | --- | --- | --- |
|  Element ID |  Length | Element ID Extension |  Payload |

 Octets: 1 1 1 variable

 **Figure 9-XYZ—RSNE Override element format**

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1 (General).

The Payload field contains the Information field of the RSNE as defined in 9.4.2.23 (RSNE), when this element is included in a Beacon or Probe Response frame. This field is empty when this element is included in a (Re)Association Request frame.

**9.4.2.312 RSNXE Override element**

The RSNXE Override element contains an alternative RSNXE. See Figure 9-XYZ+1 (RSNXE Override element format).

|  |  |  |  |
| --- | --- | --- | --- |
|  Element ID |  Length | Element ID Extension |  Payload |

 Octets: 1 1 1 variable

 **Figure 9-XYZ+1—RSNXE Override element format**

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1 (General).

The Payload field contains the Information field of the RSNXE as defined in 9.4.2.240 (RSNXE).

**12. Security**

*Add a new subclause (and its subclauses) at the end of Clause 12, i.e., just before the start of Clause 13 (REVme-D4.1 P3099 L4):*

**12.14 Overriding of RSN parameters**

**12.14.1 General**

Extensions to the RSNE and RSNXE have resulted in issues with previously deployed non-AP STAs being unable to complete connection when the AP is enabling newer functionality, e.g., when advertising multiple AKM suite selectors. Since the likelihood of deployed devices getting updated to fix this type of issues is limited, some deployment cases depend on other mechanisms to avoid known interoperability issues. RSN overriding provides such a mechanism in a manner that allows an AP to advertise limited RSN parameters in the RSNE and the RSNXE (or fully omitting the RSNXE), so that the deployed STAs would not be exposed to the extensions that have resulted in issues. The extended set of RSN parameters is advertised in new elements to allow STAs capable of the override mechanism to use newer RSN options while the deployed STAs are more likely to ignore the new elements than changes to the contents of the previously defined RSNE.

Since the RSN overriding mechanisn hides the full set of available RSN options from STAs that do not support the mechanism and might result in them not being able to use the strongest commonly enabled option, the mechanism should be used only in cases where STAs are expected to have issues connecting with an RSNE that would advertise all the enabled options.

**12.14.2 Overriding mechanism**

The RSNE Override element uses the same format as the RSNE described in 9.4.2.311 (RSNE Override element) when transmitted in a Beacon frame and Probe Response frame. It may override the Pairwise Cipher Suite Count, Pairwise Cipher Suite List, AKM Suite Count, AKM Suite List, and RSN Capabilities fields. It may also specify the Group Management Cipher Suite field in cases where that field is not included in the RSNE. The RSNE Override element shall indicate the same Group Data Cipher Suite field as the Group Data Cipher Suite field in the RSNE. If the Group Management Cipher Suite field is present in the RSNE, the RSNE Override element shall indicate the same Group Management Cipher Suite field as the Group Management Cipher Suite field in the RSNE. If any of the MFPR, MFPC, Joint Multi-band RSNA, Extended Key ID for Individually Addressed Frames, or OCVC bits in the RSN Capabilities field in the RSNE are set to 1, the corresponding bits in the RSNE Override element shall be set to 1. If any of these bits are set to 0, the corresponding bit in the RSNE Override element may be set to 1. Other fields shall not be overridden.

The method of selecting which parameters to include in the RSNE and RSNXE versus the RSNE Override and RSNXE Override elements is outside the scope of this standard.

The RSNXE Override element uses the same format as the RSNXE as described in 9.4.2.312 (RSNXE Override element). It may override any value in the RSNXE (if present) or the omission of the RSNXE. If the RSNXE is included and the SAE Hash-to-element bit in the RSNXE is set to 1, the corresponding bit in the RSNXE Override element shall be set to 1.

An AP shall include the RSNE Override element in Beacon and Probe Response frames when dot11RSNAActivated and dot11RSNOverrideActivated are true. An AP shall include the RSNXE Override element in Beacon and Probe Response frames when dot11RSNAActivated and dot11RSNOverrideActivated are true, and any subfield of the Extended RSN Capabilities field in this element is nonzero, except the Field Length subfield.

NOTE 1—If an AP is configured to use the RSN overriding mechanism and the AP includes the RSNXE Override element, the RSNE Override element is also included based on the condition described above.

A non-AP STA with dot11RSNOverrideActivate set to true shall use the contents of the RSNE Override element instead of the constents of the RSNE when processing Beacon and Probe Response frames that include both elements.

A non-AP STA with dot11RSNOverrideActivate set to true shall use the contents of the RSNXE Override element instead of the contents of the RSNXE when processing Beacon and Probe Response frames that include both elements. A non-AP STA with dot11RSNOverrideActivate set to true shall use the contents of the RSNXE Override element when processing Beacon and Probe Response frames that include the RSNXE Overrride element and do not include the RSNXE. A non-AP STA with dot11RSNOverrideActivate set to true shall use the contents of the RSNXE (if present) when processing Beacon and Probe Response frames that do not include the RSNXE Overrride element.

A non-AP STA with dot11RSNAActivated and dot11RSNOverrideActivated set to true shall include the RSNE Override element with an empty Payload field in (Re)Association Request frames when associating with an AP that includes the RSNE Override element in Beacon and Probe Response frames. Otherwise, the RSNE Override element shall not be present in (Re)Association Request frames.

If the AP includes the RSNE Override element, the STA shall indicate its selected RSN parameters in the RSNE included in the (Re)Association Request frame even if the selection is based on the AP’s RSNE Override element instead of the RSNE. The STA shall indicate its extended RSN capabilities in the RSNXE included in the (Re)Association Request frame if any subfield of the Extended RSN Capabilities field in this element is nonzero, except the Field Length subfield.

NOTE 2—The RSNXE Override element is not present in the (Re)Association Request frame.

NOTE 3—The RSNE Override element and the RSNXE Override element are not present in the (Re)Association Response frame.

If an AP with dot11RSNAActivated and dot11RSNOverrideActivated set to true receives an RSNE Override element with an empty Payload field in a (Re)Association Request frame, the AP shall use the indications in the RSNE Override element included in Beacon and Probe Response frames to construct the RSNE in the (Re)Association Response frame if the RSNE is included in the (Re)Association Response frame as defined in Table 9-65 (Association Response frame body) and Table 9-67 (Reassociation Response frame body) and to construct the RSNE in 4-way handshake message 3 as defined in 12.7.6 (4-way handshake). If an AP with dot11RSNAActivated and dot11RSNOverrideActivated set to true includes the RSNXE Override element in its Beacon and Probe Response frames and receives an RSNE Override element with an empty Payload field in the (Re)Association Request frame, the AP shall use the Information field of the RSNXE Override element included in Beacon and Probe Response frames to construct the RSNXE in the (Re)Association Response frame and to construct the RSNXE in 4-way handshake message 3 as defined in 12.7.6 (4-way handshake).

NOTE 4—The RSN override mechanism ought not to be used on the 6 GHz band.

NOTE 5—An AP with dot11RSNAOverrideActivated set to true might not advertise beacon protection to be enabled in the Beacon Protection Enabled bit of the Extended Capabilities field of the Extended Capabilities element. Non-AP STAs determine whether beacon protection is enabled based on receiving a BIGTK from the AP as described in Annex C for dot11BeaconProtetionEnabled. Beacon protection might be enabled even if the Beacon Protection Enabled bit in the Extended Capabilities element is set to 0.

**12.14.3 Downgrade protection**

When a non-AP STA indicates support for the RSN overriding mechanism by including an RSNE Override element with an empty Payload field in the (Re)Association Request frame sent to an AP, the Information fields of the RSNE and the RSNXE (if present) in the Key Data field of 4-way handshake message 3 shall be identical to the Information fields of the RSNE Override element and the RSNXE Override element (if present) in the AP’s Beacon and Probe Response frames, respectively. The RSNE and RSNXE contents from the Beacon and Probe Response frames are not included in 4-way handshake message 3 in this case. The non-AP STA shall verify that the RSNE and the RSNXE (if present) in 4-way handshake message 3 match the corresponding override elements in Beacon or Probe Response frames. This verification shall follow the rules described in 12.7.6.4 (4-way handshake message 3) for comparing the RSNE and RSNXE (if present) between 4-way handshake message 3 and Beacon and Probe Response frames. This provides downgrade protection for the overridden RSN parameters.

NOTE 1—There is no protected indication of the AP using the RSN overriding mechanism since adding such an indication into 4-way handshake message 3 would risk introducing additional interoperability issues with deployed STAs. A non-AP STA receiving a Beacon frame containing an RSNE Override element from its associated AP when RSN overriding was not used for the association might indicate a potential attack.

NOTE 2—A non-AP STA might log cases where an unexpected RSNE Override element was received from its associated AP. It might also try to reassociate with the AP using RSN overriding. While the non-AP STA might also deauthenticate in some cases, use of information from unprotected Beacon or Probe Response frames needs to be done with care to avoid opening possibilities for denial-of-service attacks.

**C.3 MIB detail**

*Modify Dot11PrivacyEntry as shown (REVme-D4.1 P5122 L47):*

Dot11PrivacyEntry ::=

 SEQUENCE {

 dot11PrivacyInvoked TruthValue,

 dot11WEPDefaultKeyID Unsigned32,

 dot11WEPKeyMappingLengthImplemented Unsigned32,

 dot11ExcludeUnencrypted TruthValue,

 dot11WEPICVErrorCount Counter32,

 dot11WEPExcludedCount Counter32,

 dot11RSNAActivated TruthValue,

 dot11RSNAPreauthenticationActivated TruthValue,

 dot11RSNOverrideActivated TruthValue }

*Add the following MIB variable after dot11RSNAPreauthenticationActivated (REVme-D4.1 P5124 L48):*

dot11RSNOverrideActivated OBJECT-TYPE

 SYNTAX TruthValue

 MAX-ACCESS read-write

 STATUS current

 DESCRIPTION

 "This is a control variable.

 It is written by an external management entity.

 Changes take effect for the next MLME-START.request primitive or MLME-

 JOIN.request primitive.

 This attribute, when true, indicates that RSN overriding is enabled on this entity.

 This object requires that dot11RSNAActivated also be equal to true."

 DEFVAL { false }

 ::= { dot11PrivacyEntry 9 }