IEEE P802.11
Wireless LANs

|  |
| --- |
| RSN overriding |
| Date: 2023-12-08 |
| 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 two rows 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). |
| 61 | RSNXE Override | The RSNXE 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 two rows 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). |
| 65 | RSNXE Override | The RSNXE 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 contents of 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 fields defined for RSNE in 9.4.2.23 (RSNE) starting from the Version field when this element is included in a Beacon or Probe Response frame. This field is empty when this element is included in Association Request and Reassociation Request frames.

**9.4.2.312 RSNXE Override element**

The RSNXE Override element contains an alternative contents of 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 fields defined for RSNXE in 9.4.2.240 (RSNXE) starting from the Extended RSN Capabilities field.

**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 with the extensions that have resulted in issues. The extended set of RSN parameters are 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 is recommended to 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 when transmitted in Beacon frame and Probe Response frame. It can override the Pairwise Cipher Suite Count, Pairwise Cipher Suite List, AKM Suite Count, AKM Suite List, and RSNE Capabilities fields. It can also specify the Group Management Cipher Suite field in cases that field is not included in the RSNE. 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. It can override any value in the RSNXE or the omission of the RSNXE.

An AP includes the RSNE Override element in Beacon and Probe Response frames when dot11RSNAActivated is true and the AP is configured to use the RSN overriding mechanism. An AP includes the RSNXE Override element in Beacon and Probe Response frames when dot11RSNAActivated is true, the AP is configured to use the RSN overriding mechanism, and any of the Extended RSN Capabilities field in this element is nonzero, except the Field Length subfield.

A non-AP STA that supports RSN overriding shall use the contents of the RSNE Override and RSNXE Override elements instead of the constents of the RSNE and RSNXE when processing Beacon and Probe Response frames that include both variants.

A non-AP STA include the RSNE Override element with empty Payload field in Association Request and Reassociation Request frames when dot11RSNAActivated is true and the STA supports RSN overriding mechanism. The STA indicates its selected RSN parameters in the RSNE and RSNXE in these frames also in the case where the selection is based on the AP’s RSNE Override and RSNXE Override elements instead of the RSNE and RSNXE.

NOTE—There are no known issues related to non-AP STAs parsing of RSNE on the 6 GHz band and as such, the RSN override mechanism is not recommended to be used on that band.

**12.14.3 Downgrade protection**

When the AP is configured to use the RSN overriding mechanism and the non-AP STA indicated support for the RSN overriding mechanism, the contents of the RSNE and the RSNXE, if present, in the Key Data field of the 4-way handshake message 3 include the payload of the RSNE Override element and the RSNXE Override element, respectively. This provides downgrade protection for the overridden RSN parameters. The RSNE and RSNXE contents from the Beacon and Probe Response frames is not included in the 4-way handshake message 3 in this case. The non-AP STA shall verify that the RSNE and the RSNXE in the 4-way handshake message 3 match the override elements in Beacon or Probe Response frames in manner described in 12.7.6.4 (4-way handshake message 3) for the RSNE and RSNXE in Beacon or Probe Response frames.

There is no protected indication of the AP using the RSN overriding mechanism since adding such indication into 4-way handshake message 3 would risk introducing additional interoperability issues with deployed STAs. If a non-AP STA receives a Beacon frame containing an RSNE Override element from its associated AP when RSN overriding was not used for the association, the non-AP STA should log this as a potential indication of an attack, and it may try to reassociate with the AP using RSN overriding.