IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 802.11bi EPP Reassociation  Reassociation to same AP or AP MLD | | | | |
| Date: 2025 - Sept | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SRT BlueHalo | Sunrise, FL, USA. | 916 799 9563 | gsmith@bluehalo.com |

Abstract

A proposal to resolve CID 2023.

Presentation 25/1632r0 made a case that a simple reassociation by a non-AP or non-AP MLD could serve as a privacy protection as an alternative to a full Frame Anonymization especially in large scale networks. Also, as FA is only for MLO devices, this can be used for non-MLO.

A proposal for non-APs and non-AP MLDs to use reassocation to change paraameters.

“EPP Reassociation”

**DISCUSSION**

Presentation 25/1632r0 made a case that a simple reassociation by a non\_AP STA or a non-AP MLD could serve as a privacy protection as an alternative to Frame Anonymization especially in large scale networks.

Normally a reassociation to the same AP or AP-MLD is used to reset certain agreements, e.g., TWT or block ack agreements. In the case that the non-AP MLD is reassociationg in order to change its MAC address and reset SN, it does not want to reset any agreements.

Note that FA only applies to MLO and hence simple reassociation adds some privacy for non-MLO devices.

Of course, the non-AP STA/MLD may want to reassociate in order to reset agreements. In that case it does not use EPP Reassociation.

Therefore, a method is required such that the non-AP STA can indicate if it is reassociating solely for privacy purposes,

The section in 11mf that covers what is deleted or reset for a standard reassociation is:

**11.3.5.4 Non-AP STA, non-AP MLD, and non-PCP STA reassociation initiation procedures**

If the MLME-REASSOCIATION.request primitive has the new (#11be)AP’s, AP MLD’s, or PCP’s MAC address in the CurrentAPAddress parameter (reassociation to the same AP, AP MLD, or PCP), the following states, agreements and allocations shall be deleted or reset to initial values:

BTW It should be “MLME-REASSOCIATE.request”, AND there is no “CurrentAPAddress” in that MLME. There is a “Current AP Address”in the Reassociate request. Need to edit this in 11mf.

1) All EDCAF state

2) Any block ack agreements that are not GCR agreements

3) Sequence number

4) Duplicate detection caches

5) Anything queued for transmission

6) Fragmentation and reassembly buffers

7) Power management mode

8) WNM sleep mod

9) TDLS agreements

10) TPKSAs established with any peers

11) TSPECs

12) DMG TSPECs

13) GLK-GCR agreement

14) MSCS

15) SCS

16) (#11be)TWT

**Proposal**

In the proposed case of a CPE non-AP or a non-AP MLD reassociating solely for privacy, only the following should change:

1. Non-AP address (new)
2. Sequence number (reset)
3. AID allocation (new)
4. PN (reset)

This reassociation can be used for non-MLO devices (FA is for MLO only). For MLO devices it would be an alternative to using frame anonymization. A non-AP STA, or a non-AP MLD could signal that this is a “privacy reassociation” by setting “EPP ReassociationActivated” bit in the RSNXE.

The EPP Reassociation is carried out if the following is true:

* The Reassociation Request frame is encrypted,
* The Reassociation Request frame is for reassociation to the same AP or AP MLD,
* The DS MAC Address is present,
* Dot11EPPReassociationActivated is true for the AP or AP MLD and the non-AP STA of non-AP MLD.

Then the AP or AP MLD knows that this is a reassociation to change the MAC Address and reset SN, and PN, and re-allocate AID, only. No existing agreements are to be torn down.

**PROPOSAL**

**4.5.4.10a Enhanced Privacy Protection (EPP) enhancements**

At P29L44, add text as shown:

Examples of unencrypted fields and elements that contain static or predictable values assigned to the transmitter or receiver include: transmitter address (TA), receiver address (RA); sequence number (SN); packet number (PN); timestamp; association identifier (AID) and fields and elements derived from the AID. A third-party observer can monitor these values and, as long as the values remain static or predictable, the third-party observer can determine that the corresponding 802.11 device continues to be present at that location. In some cases, the location could be fixed (relative to the ground) while in other cases the location could be in motion, e.g. the device is moving, or the AP is installed in a vehicle and both the AP and the device are moving.

EPP Reassociation allows a non-AP STA or non-AP MLD to reassociate to the same AP or AP MLD in order to change its MAC address, reset SN and PN, and receive a new AID. When using EPP Reassociation, no existing states and agreements are deleted.

Frame anonymization, available when MLO is enabled, improves user privacy by restricting the periods

within which unencrypted fields and elements remain static or predictable, thereby increasing the effort

required for a third party to determine the long-term presence of the person. The periods, called EPP epochs, can be relatively short in duration when compared to the typical lifetime of an association.

*At P75L59, add new row to Table 9-373 as shown:*

**Table 9-373—Extended RSN Capabilities field *(continued)***

|  |  |  |
| --- | --- | --- |
| 31 | DS MAC Address Support | The DS MAC Address Support field is set to 1 when dot11DSMACAddressActivated is true and is set to 0 otherwise |
| 32 | EPP Robust Individually Addressed Beamforming/CSI/CQI Frame Non-TB Tx Support | An EPP STA sets the EPP Robust  Individually Addressed Beamforming/CSI/  CQI Frame Non-TB Tx Support field to 1 if  dot11EPPRobustIndividuallyAddressedBea  mformingCSICQIFrameNonTBTxActivate  d is true. Otherwise, this field is set to 0.  See 12.16.3 (EPP Robust Individually  Addressed Management Frames and Robust  Individually Addressed Beamforming/CSI/  CQI Frames). |
| 34 | SAE Password Identifier Change Support | A non-AP STA that supports changing the  SAE Password Identifier sets this to 1.  Otherwise, this is set to 0. |
| ANA | EPP Reassociation Support | The EPP Reassociation Support field is set to 1 when dot11EPPReassociation Activated is true and set to 0 otherwise. |

**12.16.6 (Re)Association Request/Response Frame Encryption**

*At P153L63, make edits as shown below:*

This subclause defines rules to encrypt the Frame Body field of the (Re)Association Request/Response frame, ~~and to~~ include a DS MAC Address element in the encrypted (Re)Association Request frame in the encrypted (Re)Association Request frame. and to perform EPP Reassociation.

**12.16.6.1 Non-MLO procedure**

*At P155L1, add text as shown below:*

The EPP non-AP STA may randomize the DS MAC address. To construct a random DS MAC address, the EPP non-AP STA shall select the randomized DS MAC address according to IEEE Std 802-2014 and IEEE Std 802c-2017. If dot11DSMACAddressActivated is true, the EPP non-AP STA shall use the same DS MAC address for the duration of its connection across an ESS.

NOTE 2—Detection and remediation of possible DS MAC address collisions are outside the scope of this standard.

A non-AP STA can change its MAC address, reset SN and PN and be allocated a new AID by reassociating to the same EPP AP using EPP Reassociation. If dot11EPPReassociationActivated is true, an EPP AP sets the EPP Reassociation Support field in the RSNXE to 1 to indicate support for EPP Reassociation. The non-AP STA is reassociating using EPP Reassociation if the Reassociation Request frame is encrypted, the EPP Reassociation Support field in the RSNXE is set to 1, the Current AP Address is the same as the new AP’s address (reassociating to the same AP), and the DS MAC Address element is present.

*At P157L5, add text as shown below:*

On a successful (re)association,

* The EPP non-AP STA shall process the Key Delivery element in the (Re)Association Response frame if present.
* The EPP non-AP STA shall install the GTK and GTK RSC, and IGTK and IGTK RSC if management frame protection is enabled, and BIGTK and BIGTK RSC if present in the Key Delivery element and dot11BeaconProtectionEnabled is true, and WIGTK and WIGTK RSC if present in the Key Delivery element and dot11RSNAWURFrameProtectionActivated is true.
* The EPP AP and the EPP non-AP STA shall transition to State 4 (as defined in 11.3 (STA authentication and association)).
* If the DS MAC Address element is included in the (Re)Association Request frame, the EPP non-AP STA shall use the indicated DS MAC address rather than the MAC address of the EPP non-AP STA for the EPP non-AP STA to the EPP AP mapping to the DS.
* If the DS MAC Address element is included in the (Re)Association Request frame, the EPP AP shall process the DS MAC Address element and use the indicated DS MAC address rather than the MAC address of the EPP non-AP STA to establish the EPP non-AP STA to the EPP AP mapping to the DS.

NOTE 1—If the DS MAC Address element is included in the (Re)Association Request frame, the source address or destination address parameters of the MAC service tuples (see 5.2.4.2 (Semantics of the service primitive)) for the EPP non-AP STA are set to the DS MAC address, which is the identity of the non-AP STA known by the DS.

On a successful EPP Reassociation, the EPP AP and non-AP STA shall reset the SN and PN and the EPP AP MLD shall allocate a new AID to the non-AP STA but shall not change any pre-existing states or agreements.

**12.16.6.2 MLO procedure**

*At P157L 58 insert new text as shown below:*

The (Re)Association Request frame shall:

— Have the Address 1 field equal to the Address 1 field of the Authentication frame used by the non-

AP MLD to establish the PTKSA.

— Have the Address 2 field equal to the Address 2 field of the Authentication frame used by the non-

AP MLD to establish the PTKSA.

— Include the DS MAC Address element in the (Re)Association Request frame to indicate the DS

MAC address to be used by the EPP AP MLD for the mapping to the DS if

dot11DSMACAddressActivated is true and the APs affiliated with the EPP AP MLD set the DS

MAC Address Support field in the RSNXE to 1.

A non-AP MLD can change its MAC address, reset SN and PN and be allocated a new AID by reassociate to the same EPP AP MLD using EPP Reassociation. If EPPReassociationActivated is true, an EPP AP MLD sets the EPP Reassociation Support field in the RSNXE to 1 to indicate support for EPP Reassociation. A non-AP STA MLD is reassociating using EPP Reassociation. If a Reassociation Request frame is encrypted, the EPP Reassociation Support field in the RSNXE is set to 1, the Current AP Address is the same as the new AP’s address (reassociating to the same AP MLD), and the DS MAC Address element is present, the non-AP STA MLD is reassociating using EPP Reassociation.

*At P160l25 insert text as shown below:*

— If the DS MAC Address element is included in the (Re)Association Request frame, the EPP non-AP

MLD shall use the indicated DS MAC address rather than the MLD MAC address of the non-AP

MLD for the EPP non-AP MLD to the EPP AP MLD mapping to the DS.

— If the DS MAC Address element is included in the (Re)Association Request frame, the EPP AP

MLD shall process the DS MAC Address element and use the indicated DS MAC address rather

than the MLD MAC address of the EPP non-AP MLD to establish the EPP non-AP MLD to the EPP

AP MLD mapping to the DS.

NOTE 3—If the DS MAC Address element is included in the (Re)Association Request frame, the source address or destination address parameters of the MAC service tuples (see 5.2.4.2 (Semantics of the service primitive)) for the EPP non- AP MLD are set to the DS MAC address, which is the identity of the non-AP MLD known by the DS.

On a successful EPP Reassociation, the EPP AP MLD and non-AP MLD shall reset the SN and PN and the EPP AP MLD shall allocate a new AID to the non-AP MLD but shall not change any pre-existing states or agreements.

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-- \* dot11EPPStationConfig TABLE

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

*At P185L55 insert text as shown below:*

dot11EPPReassociationActivated OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity or the SME.

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

request primitive.

This attribute, when true, indicates the capability to support use of EPP Reassociation

is enabled. The capability is disabled otherwise."

DEFVAL { false }

::= { dot11EPPStationConfigEntry 14 }