### IEEE P802.11 Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed TBD fix for MLD Association – SA Query | | | | |
| Date: 2020-10-20 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel Corporation | 2200 Mission College Blvd, Santa Clara, CA 950542200 |  | po-kai.huang@intel.com |
| Robert Stacey |  |  |  |  |
| Daniel Bravo |  |  |  |  |
| Ido Ouzieli |  |  |  |  |
| Danny Alexander |  |  |  |  |

Abstract

We propose to complete the SA query procedure which is an important component of the association procedure. We revise the specific text to enable SA Query for MLD association.

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Revision based on the comments received offline that SA Query Maximum Timeout is MLD level, and introduce dot11MLDAssociationSAQueryMaximumTimeout to clarify the confusion

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbe 0.1 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbe D0.1 Draft (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***TGbe Editor: Editing instructions preceded by “TGbe Editor” are instructions to the TGbe editor to modify existing material in the TGbe draft. As a result of adopting the changes, the TGbe editor will execute the instructions rather than copy them to the TGbe Draft.***

**Discussion:**

SA query is an important component of the association procedure in the baseline.

STA can send SA query after receiving unprotected disassocaiton or disauthentication due to association state mismatch to verify the disassocaiton is from legit AP.

AP can send SA query after receiving reassociation request to verify that the reassociation is from legit STA.

We revise the specific text to enable SA Query related to MLD association.

**Propose:**

***TGbe editor: Modify clause 11.13 SA Query procedures as follows(track change on):***

* SA Query procedures

If dot11RSNAProtectedManagementFramesActivated is true, then the STA or MLD shall support the SA Query procedure.

To send an SA Query Request or SA Query Response frame to a peer STA or a peer MLD, the SME shall issue an MLME-SA-QUERY.request or MLME-SA-QUERY.response primitive respectively. Reception of an SA Query Request or SA Query Response frame is signaled to the SME with an MLME-SA-QUERY.indication or MLME-SA-QUERY.confirm primitive respectively.

A STA or a MLD that supports the SA Query procedure and receives an SA Query Request frame shall respond with an SA Query Response frame (M58)if none of the following are true:

* the STA or the non-AP MLD is not currently associated to the STA or the AP MLD that sent the SA Query Request frame
* the STA has sent a (Re)Association Request frame within dot11AssociationResponseTimeOut but has not received a corresponding (Re)Association Response frame
* (M58)dot11RSNAOperatingChannelValidationActivated is true and the sending STA had indicated OCVC capability in its association and either:
* OCI element is not present in the request
* Operating channel information indicated does not match the current channel information (see 12.2.9 (Requirements for Operating Channel Validation(M58)))

(…existing texts….)

If a non-AP and non-PCP STA that has an SA with its AP or PCP for an association that negotiated management frame protection receives an unprotected Deauthentication or Disassociation frame with reason code INVALID\_CLASS2\_FRAME or INVALID\_CLASS3\_FRAME from the AP or PCP, the non-AP and non-PCP STA may use this as an indication that there might be a mismatch in the association state between itself and the AP or PCP. In such a case, the non-AP and non-PCP STA’s SME may initiate the SA Query procedure with the AP or PCP to verify the validity of the SA by issuing one MLME-SA-QUERY.request primitive every dot11AssociationSAQueryRetryTimeout TUs until a matching MLME‑SA‑QUERY.confirm primitive is received or dot11AssociationSAQueryMaximumTimeout TUs from the beginning of the SA Query procedure has passed. If the AP or PCP responds to the SA Query request with a valid SA Query response, the non-AP STA should continue to use the SA. If no valid SA Query response is received, the non-AP and non-PCP STA’s SME may delete the SA and temporal keys held for communication with the STA by issuing an MLME-DELETEKEYS.request primitive and the non-AP and non-PCP STA may move into State 1 (or State 2, for a DMG STA) with the AP.

If an affiliated non-AP STA of a non-AP MLD that has an SA with its AP MLD for an association that negotiated management frame protection receives an unprotected Deauthentication or Disassociation frame with reason code INVALID\_CLASS2\_FRAME or INVALID\_CLASS3\_FRAME from the corresponding affiliated AP of the AP MLD in a setup link, the non-AP MLD may use this as an indication that there might be a mismatch in the association state between itself and the AP MLD. In such a case, the SME may initiate the SA Query procedure with the AP MLD to verify the validity of the SA by issuing one MLME-SA-QUERY.request primitive every dot11AssociationSAQueryRetryTimeout TUs until a matching MLME‑SA‑QUERY.confirm primitive is received or dot11MLDAssociationSAQueryMaximumTimeout TUs from the beginning of the SA Query procedure has passed. If the AP MLD responds to the SA Query request with a valid SA Query response, the non-AP MLD should continue to use the SA. If no valid SA Query response is received, the SME may delete the SA and temporal keys held for communication with the AP MLD by issuing an MLME-DELETEKEYS.request primitive and the non-AP MLD may move into State 1 with the AP MLD.

(…existing texts….)

***TGbe editor: Modify 11.3.5.3 AP, AP MLD, or PCP association receipt procedures as follows (track change on):***

***Change the title of the subclause***

* AP, AP MLD, or PCP association receipt procedures

***Change as follows:***

The following procedure shall be used by an AP or PCP ~~U~~upon receipt of an Association Request frame from a STA ~~the AP or PCP shall use the following procedure~~ or by an AP MLD upon receipt of an Association Request frame with Multi-Link element indicates the AP MLD from a non-AP STA affiliated with a non-AP MLD:

* The MLME shall issue an MLME-ASSOCIATE.indication primitive to inform the SME of the association request. The SME shall issue an MLME-ASSOCIATE.response primitive addressed to the STA or MLD identified by the PeerSTAAddress parameter of the MLME-ASSOCIATE.indication primitive. If the association is not successful, the SME shall indicate a specific reason for the failure to associate in the ResultCode parameter. Upon receipt of the MLME-ASSOCIATE.response primitive, the MLME shall transmit an Association Response frame.
* If the state for the STA is 1 and the STA is a non-DMG STA or the state of the non-AP MLD is 1, the SME shall refuse the association request by issuing an MLME-ASSOCIATE.response primitive with ResultCode NOT\_AUTHENTICATED.
* AP with dot11InterworkingServiceActivated true only: If the MLME-ASSOCIATE.indication primitive has the EmergencyServices parameter set to true and the RSN parameter does not include an RSNE, the SME shall not reject the association request on the basis that dot11RSNAActivated is true, thereby granting access, using unprotected frames (see 9.2.4.1.9 (Protected Frame subfield)), to the network for emergency services purposes.
* Otherwise, in an RSNA the SME shall check the values received in the RSN parameter to see whether the values received match the security policy. If they do not, the SME shall refuse the association by issuing an MLME-ASSOCIATE.response primitive with a ResultCode indicating the security policy mismatch.
* Otherwise, if the state for the STA or the non-AP MLD is 4, the STA or the non-AP MLD has a valid security association, the STA or the non-AP MLD has negotiated management frame protection, the STA or the non-AP MLD has not performed a successful SAE authentication after the current association was established, and there has been no earlier, timed out SA Query procedure with the STA or the non-AP MLD (which would have allowed a new association process to be started, without an additional SA Query procedure):
* The SME shall refuse the association request by issuing an MLME-ASSOCIATE.response primitive with ResultCode REFUSED\_TEMPORARILY and TimeoutInterval containing a Timeout Interval element with the Timeout Interval Type field set to 3 (Association Comeback time). If the SME is in an ongoing SA Query with the STA or the non-AP MLD, the Timeout Interval Value field shall be set to the remaining SA Query period, otherwise it shall be set to dot11AssociationSAQueryMaximumTimeout or dot11MLDAssociationSAQueryMaximumTimeout.
* The state for the STA or the non-AP MLD shall be left unchanged.
* Following this, if the SME is not in an ongoing SA Query with the STA or the non-AP MLD, the SME shall issue one MLME-SA-QUERY.request primitive addressed to the STA or the non-AP MLD every dot11AssociationSAQueryRetryTimeout TUs until an MLME-SA-QUERY.confirm primitive for the STA or the non-AP MLD is received or dot11AssociationSAQueryMaximumTimeout TUs or dot11MLDAssociationSAQueryMaximumTimeout TUs from the beginning of the SA Query procedure have passed. The SME shall increment the TransactionIdentifier by 1 for each MLME-SA-QUERY.request primitive, rolling it over the value to 0 after the maximum allowed value is reached.
* If no MLME-SA-QUERY.confirm primitive for the STA or the non-AP MLD is received within the dot11AssociationSAQueryMaximumTimeout period or the dot11MLDAssociationSAQueryMaximumTimeout, the SME shall allow a subsequent association process with the STA or the non-AP MLD to be started without starting an additional SA Query procedure, except that the SME may deny a subsequent association process with the STA or the non-AP MLD if an MSDU was received from the STA or any affiliated STA of the non-AP MLD within this period.

NOTE 1—Reception of an MSDU implies reception of a valid protected frame, which obviates the need for the SA Query procedure.

* The SME shall refuse an association request from a STA or a non-AP MLD that does not support all of the rates in the BSSBasicRateSet parameter and all of the membership selectors in the BSSMembershipSelectorSet parameter of the AP or of the corresponding AP in each setup link, respectively, in the MLME-START.request primitive.
* The SME shall refuse an association request from an HT STA or a non-AP MLD that does not support all of the MCSs in the Basic HT-MCS Set field of the HT Operation parameter of the AP or of the corresponding AP in each setup link, respectively, in the MLME-START.request primitive.
* The SME shall refuse an association request from a VHT STA or a non-AP MLD that does not support all of the <VHT-MCS, NSS> tuples indicated by the Basic VHT-MCS And NSS Set field of the VHT Operation parameter of the AP or the corresponding AP in each setup link, respectively, in the MLME-START.request primitive.
* The SME shall refuse an association request from a HE STA or a non-AP MLD that does not support all of the <HE-MCS, NSS> tuples indicated by the Basic HE-MCS And NSS Set field of the HE Operation parameter of the AP or the corresponding AP in each setup link, respectively, in the MLME-START.request primitive.
* An AP or PCP may refuse GLK association based on local policy and, if so, shall return the GLK\_NOT\_AUTHORIZED ResultCode.

NOTE 2—For example, there might be a list of authorized GLK peers or clients or a limit on the number of GLK peers or clients and the peer or client is not on that list or its acceptance would exceed the limit.

* The SME shall generate an MLME-ASSOCIATE.response primitive with the PeerSTAAddress parameter set to the MAC address of the STA or the non-AP MLD identified by the PeerSTAAddress parameter of the MLME-ASSOCIATE.indication primitive. If the ResultCode in the MLME-ASSOCIATE.response primitive is SUCCESS, the SME has an existing SA with the STA or the non-AP MLD, and an SA Query procedure with that STA or the non-AP MLD has failed to receive a valid response (i.e., has not received an MLME-SA-QUERY.confirm primitive within the dot11AssociationSAQueryMaximumTimeout period or dot11MLDAssociationSAQueryMaximumTimeout period), the SME shall issue an MLME-DISASSOCIATE.request primitive addressed to the STA or the non-AP MLD with ReasonCode INVALID\_AUTHENTICATION.

NOTE 3—This MLME-DISASSOCIATE.request primitive generates a protected Disassociation frame. If the association request was genuine, the STA has deleted the PTKSA by this point and so the protected Disassociation frame is ignored. The purpose is to inform a STA which has for some reason failed to respond to an SA Query procedure triggered by a forged association request.

***TGbe editor: Modify 11.3.5.5 A P, AP MLD, or PCP reassociation receipt procedures as follows (track change on):***

* AP, AP MLD, or PCP reassociation receipt procedures

***Change as follows:***

The following procedure shall be used by an AP or PCP u~~U~~pon receipt of a Reassociation Request frame from a STA ~~the AP or PCP shall use the following procedure~~ or by an AP MLD upon receipt of a Reassociation Request frame with Multi-Link element indicates the AP MLD from a non-AP STA affiliated with a non-AP MLD:

* The MLME shall issue an MLME-REASSOCIATE.indication primitive to inform the SME of the reassociation request. The SME shall issue an MLME-REASSOCIATE.response primitive addressed to the STA or the non-AP MLD identified by the PeerSTAAddress parameter of the MLME-REASSOCIATE.indication primitive. If the reassociation is not successful, the SME shall indicate a specific reason for the failure to reassociate in the ResultCode parameter. Upon receipt of the MLME-REASSOCIATE.response primitive, the MLME shall transmit a Reassociation Response frame.
* If the state for the STA is 1 and the STA is a non-DMG STA or the state for the non-AP MLD is 1, the SME shall refuse the reassociation request by issuing an MLME REASSOCIATE.response primitive with ResultCode NOT\_AUTHENTICATED.
* AP with dot11InterworkingServiceActivated true only: If the MLME-REASSOCIATE.indication primitive has the EmergencyServices parameter set to true and the RSN parameter does not include an RSNE, the SME shall not reject the reassociation request on the basis that dot11RSNAActivated is true and dot11PrivacyInvoked is true thereby granting access, using unprotected frames (see 9.2.4.1.9 (Protected Frame subfield)), to the network for emergency services purposes.
* Otherwise, in an RSNA the SME shall check the values received in the RSN parameter to see whether the values received match the security policy. If they do not, SME shall refuse the reassociation by issuing an MLME-REASSOCIATE.response primitive with a ResultCode indicating the security policy mismatch.
* Otherwise, if the state for the STA or the non-AP MLD is 4, the STA or the non-AP MLD has a valid security association, the STA or the non-AP MLD has negotiated management frame protection, the reassociation is not a part of a fast BSS/ML transition, the STA or the non-AP MLD has not performed a successful SAE authentication after the current association was established, and there has been no earlier, timed out SA Query procedure with the STA or the non-AP MLD (which would have allowed a new reassociation process to be started, without an additional SA Query procedure):
* The SME shall refuse the reassociation request by issuing an MLME-REASSOCIATE.response primitive with ResultCode REFUSED\_TEMPORARILY and TimeoutInterval containing a Timeout Interval element with the Timeout Interval Type field set to 3 (Association Comeback time). If the SME is in an ongoing SA Query with the STA or the non-AP MLD, the Timeout Interval Value field shall be set to the remaining SA Query period, otherwise it shall be set to dot11AssociationSAQueryMaximumTimeout or dot11MLDAssociationSAQueryMaximumTimeout.
* The state for the STA or the non-AP MLD shall be left unchanged.
* Following this, if the SME is not in an ongoing SA Query with the STA or the non-AP MLD, the SME shall issue one MLME-SA-QUERY.request primitive addressed to the STA or the non-AP MLD every dot11AssociationSAQueryRetryTimeout TUs until an MLME-SA-QUERY.confirm primitive for the STA or the non-AP MLD is received or dot11AssociationSAQueryMaximumTimeout TUs or dot11MLDAssociationSAQueryMaximumTimeout TUs from the beginning of the SA Query procedure have passed. The SME shall increment the TransactionIdentifier by 1 for each MLME-SA-QUERY.request primitive, rolling it over to 0 after the maximum allowed value is reached.
* If no MLME-SA-QUERY.confirm primitive for a STA or a non-AP MLD is received within the dot11AssociationSAQueryMaximumTimeout period or dot11MLDAssociationSAQueryMaximumTimeout period, the SME shall allow a subsequent reassociation process to be started without starting an additional SA Query procedure, except that the SME may deny a subsequent reassociation process with the STA or the non-AP MLD if an MSDU was received from the STA or any affiliated STA of the non-AP MLD within this period.

NOTE 1—Reception of an MSDU implies reception of a valid protected frame, which obviates the need for the SA Query procedure.

* The SME shall refuse a reassociation request from a STA or a non-AP MLD that does not support all the rates in the BSSBasicRateSet parameter and all of the membership selectors in the BSSMembershipSelectorSet parameter of the AP or of the corresponding AP in each setup link, respectively, in the MLME-START.request primitive.
* The SME shall refuse a reassociation request from an HT STA or a non-AP MLD that does not support all of the MCSs in the Basic HT-MCS Set field of the HT Operation parameter of the AP or of the corresponding AP in each setup link, respectively, in the MLME-START.request primitive.
* The SME shall refuse a reassociation request from a VHT STA or a non-AP MLD that does not support all of the <VHT-MCS, NSS> tuples indicated by the Basic VHT-MCS And NSS Set field of the VHT Operation parameter of the AP or of the corresponding AP in each setup link, respectively, in the MLME-START.request primitive.
* The SME shall refuse a reassociation request from a HE STA or a non-AP MLD that does not support all of the <HE-MCS, NSS> tuples indicated by the Basic HE-MCS And NSS Set field of the HE Operation parameter of the AP or of the corresponding AP in each setup link, respectively, in the MLME-START.request primitive.
* If the ResultCode in the MLME-REASSOCIATE.response primitive is SUCCESS, the SME has an existing SA with the STA or the non-AP MLD, and an SA Query procedure with that STA or the non-AP MLD has failed to receive a valid response (i.e., has not received an MLME-SA-QUERY.confirm primitive within the dot11AssociationSAQueryMaximumTimeout period or dot11MLDAssociationSAQueryMaximumTimeout), the SME shall issue an MLME-DISASSOCIATE.request primitive addressed to the STA or the non-AP MLD with ReasonCode INVALID\_AUTHENTICATION.

NOTE 2—This MLME-DISASSOCIATE.request primitive generates a protected Disassociation frame. If the reassociation request was genuine, the STA or the non-AP MLD has deleted the PTKSA by this point and so the protected Disassociation frame is ignored. The purpose is to inform a STA which has for some reason failed to respond to an SA Query procedure triggered by a forged reassociation request.

(…existing texts…)

***TGbe editor: Add 6.3.39.1 Introduct to 6.3.39 SA Query support as follows (track change on):***

6.3.39.1 General

In clause 6.3.39 SA Query support, the reference of a “STA” means the “STA” that is not affiliated with a MLD unless specified otherwise, and the reference of an “AP” means the AP that is not affiliated with a MLD unless specified otherwise. When referring to MLD management, the “SME” is the entity that manages the MLD. The peer MAC entity can be with a STA that is not affiliated with a MLD or a MLD depending on the context. The PeerSTAAddress can be the MAC address of the STA that is not affiliated with a MLD or the MLD MAC address depending on the context.

***TGbe editor: Modify 6.3.39 SA Query support as follows (track change on):***

* SA Query support
* MLME-SA-QUERY.request
* Function

This primitive requests that an SA Query(#1162) Request frame be sent to a specified peer STA to which the STA is associated or be sent to an affiliated STA of the specified peer MLD to which the MLD is associated.

* Semantics of the service primitive

The primitive parameters are as follows:

MLME-SA-QUERY.request(

PeerSTAAddress,  
TransactionIdentifier,  
VendorSpecificInfo  
)

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Valid range | Description |
| PeerSTAAddress(#2076) | MAC address(#5033) | Any valid individual MAC address(#5033) | Specifies the address of the peer MAC entity for the SA Query |
| TransactionIdentifier | 2 octets | As defined in 9.6.9.2 (SA Query Request frame) | The Transaction Identifier to identify the SA Query Request and Response transaction |
| VendorSpecificInfo | A set of elements | As defined in 9.4.2.25 (Vendor Specific element) | Zero or more elements. |

* When generated

This primitive is generated by the SME to request that an SA Query(#1162) Request frame be sent to a specified peer STA with which the STA is associated or be sent to a STA affiliated with the specified peer MLD with which the MLD is associated.

* Effect of receipt

On receipt of this primitive, the MLME constructs an SA Query(#1162) Request frame. The STA then attempts to transmit this to the peer STA with which it is associated or a STA affiliated with the MLD attempts to transmit this to another STA affiliated with the peer MLD with which the MLD is associated on the corresponding link.

* MLME-SA-QUERY.confirm
* Function

This primitive reports the result of an SA Query(#1162) procedure.

* Semantics of the service primitive

The primitive parameters are as follows:

MLME-SA-QUERY.confirm(

PeerSTAAddress,  
TransactionIdentifier,  
VendorSpecificInfo  
)

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Valid Range | Description |
| PeerSTAAddress(#2076) | MAC address(#5033) | Any valid individual MAC address(#5033) | Specifies the address of the peer MAC entity for the SA Query |
| TransactionIdentifier | 2 octets | As defined in 9.6.9.2 (SA Query Request frame) | The Transaction Identifier to identify the SA Query Request and Response transaction |
| VendorSpecificInfo | A set of elements | As defined in 9.4.2.25 (Vendor Specific element) | Zero or more elements. |

* When generated

This primitive is generated by the MLME as a result of the receipt of a valid SA Query Response frame.

* Effect of receipt

On receipt of this primitive, the SME may use the response as a sign of liveness of the peer STA or the peer MLD.

* MLME-SA-QUERY.indication
* Function

This primitive indicates that an SA Query(#1162) Request frame was received.

* Semantics of the service primitive

The primitive parameters are as follows:

MLME-SA-QUERY.indication(

PeerSTAAddress,  
TransactionIdentifier,  
VendorSpecificInfo  
)

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Valid range | Description |
| PeerSTAAddress(#2076) | MAC address(#5033) | Any valid individual MAC address(#5033) | Specifies the address of the peer MAC entity for the SA Query |
| TransactionIdentifier | 2 octets | As defined in 9.6.9.2 (SA Query Request frame) | The Transaction Identifier to identify the SA Query Request and Response transaction |
| VendorSpecificInfo | A set of elements | As defined in 9.4.2.25 (Vendor Specific element) | Zero or more elements. |

* When generated

This primitive is generated by the MLME when a (#249)SA Query Request frame is received.

* Effect of receipt

On receipt of this primitive, the SME operates according to the procedure in 11.3 (STA authentication and association).

* MLME-SA-QUERY.response
* Function

This primitive is generated in response to an MLME-SA-QUERY.indication primitive requesting an SA Query(#1162) Response frame be sent to a STA or to a STA affiliaited with the peer MLD.

* Semantics of the service primitive

The primitive parameters are as follows:

MLME-SA-QUERY.response(

PeerSTAAddress,  
TransactionIdentifier,  
VendorSpecificInfo  
)

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Valid range | Description |
| PeerSTAAddress(#2076) | MAC address(#5033) | Any valid individual MAC address(#5033) | Specifies the address of the peer MAC entity for the SA Query |
| TransactionIdentifier | 2 octets | As defined in 9.6.9.2 (SA Query Request frame) | The Transaction Identifier to identify the SA Query Request and Response transaction |
| VendorSpecificInfo | A set of elements | As defined in 9.4.2.25 (Vendor Specific element) | Zero or more elements. |

* When generated

This primitive is generated by the SME, in response to an MLME-SA-QUERY.indication primitive, requesting an SA Query(#1162) Response frame be sent to a STA or to a STA affiliaited with the peer MLD.

* Effect of receipt

On receipt of this primitive, the MLME constructs an SA Query(#1162) Response frame. The STA then attempts to transmit this to the STA indicated by the PeerSTAAddress parameter or a STA affiliated with the MLD then attempts to transmit this to a STA affiliated with the peer MLD indicated by the PeerSTAAddress parameter.

**Straw Poll: Do you support to incorporate the proposed draft text in this document to the TGbe Draft 0.2?**

**Result: Yes/No/Abstain**