IEEE P802.11
Wireless LANs

|  |
| --- |
| SA Query improvements for low-transmit devices |
| Date: 2025-04-29 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Henry Ptasinski | Morse Micro |  |  | henry@e78com.com |
| David Halasz | Morse Micro |  |  | dave.halasz@ieee.org |

Abstract

The SA query mechanism used to detect association state mismatch assumes the non-AP STA is initiating frames that will trigger a Deauthentication or Disassociation frame. For low power STAs that rarely transmit, such as sensor devices, or for STAs that do not initiate any transmission until queried by the AP or another network device, this assumption leads to long times before the association state recovers, if ever.

## Discussion:

With respect to the SA Query procedure, the standard assumes that non-AP STAs will typically send protected traffic to the AP. If the security state is out of sync (e.g. the AP does not have an appropriate security association for the protected traffic from the non-AP STA), that will then trigger a Deauthentication or Disassociation. At that

point, the non-AP STA may perform an SA Query to check the security state. Non-AP STAs initiate the SA Query procedure after receipt of a Deauth or Disassoc frame with specific reason codes:

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 individually addressed 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. (11.13 SA Query procedures)

but these reason codes will only be used in response to a frame transmitted from the non-AP STA to the AP. If the non-AP STA rarely (or never) initiates a Class 2 or Class 3 frame transmission to the AP, the SA Query procedures will never be invoked and the non-AP STA will not be able to recover.

Some devices may operate primarily as a data sink, and hence never have any data frames to transmit. Other devices, such as some sensor devices, may wait to transmit until queried by a received frame from the AP or a device deeper in the network. If, for example, the AP resets while one of these low power STAs is not awake, the AP will stop forwarding frames to the STA. However, the STA will not have any indication that the assiciaiton is no longer valied. Following the procedure as quoted above, the device will not initiate an SA Query and will never re-establish the association.

Note that the non-AP STA could also be out of sync with the AP merely by missing a (protected) Deauthentication or Disassociation message, due to not being awake or operating off-channel.

A possible workaround is for the non-AP STA to periodically transmit a protected frame that would trigger a Deauthentication or Disassociation with one of the above reason codes if the state is out of sync, for no reason other than to see if it triggers the Deauthentication or Disassociation. However, that would require an additional frame transmission from the non-AP STA at some regular interval. This approach has numerous issues:

* The extra frame transmission would be unwelcome in power-sensitive devices. Transmitting consumes many times more power than passively receiving.
* The extra frame transmission would also be unwelcome in large scale installations (e.g. containing thousands of S1G stations), particularly when bandwidth is very limited.
* It's not clear what a generic protected data frame could contain that would not trigger a warning message, additional downstream traffic, or an unwanted action at some layer on the AP or upstream device.

A lower-traffic approach is for the STA to use the SA Query proecdure directly whenever it wants to verify that the security association is still valid, eliminating the need for an additional data frame transmission and subsequent deauthentication frame. A STA may want to use the SA Query to satisfy other requirements, such as sending keepalive traffic during a BSS Max Idle period. While there is no prohibition on a STA initiating an SA Query procedure, it is not explicitly stated that a STA can initiate the procedure whenever desired.

Additionally, clarification is needed regarding the SA Query procedures for S1G STAs and for the RSNA security association recovery procedures in general.

## Proposed Resolution:

### 4.5.4.4 Data confidentiality

Insert the following note after the 6th paragraph:

The default data confidentiality state for all IEEE 802.11 STAs is “in the clear,” i.e., without protection. If the data confidentiality service is not invoked, all frames are sent unprotected. If this policy is unacceptable to the sender, it does not send Data frames; and if the policy is unacceptable to the receiver, it discards any received Data frames. Unprotected Data frames and unprotected robust Management frames received at a STA configured for mandatory data confidentiality, as well as protected Data frames and protected robust Management frames using a key not available at the receiving STA, are discarded without an indication to LLC (or without indication to distribution system services in the case of “To DS” frames received at an AP). These frames are acknowledged on the WM [if received without frame check sequence (FCS) error] to avoid wasting WM bandwidth on retries of frames that are being discarded.

NOTE—Null and QoS (+)Null frames are not protected.

### 9.6.9.1 SA Query Action field

*Note: There is no “Association Lockout” problem defined in the standard.*

Delete the note:

Two Action frame formats are defined for the SA Query procedure. An SA Query Action field, in the field immediately after the Category field, differentiates the formats. The Action field values associated with each frame format are defined in Table 9-515 (SA Query Action field values).

~~NOTE—The SA query functionality defined in this standard is used to prevent the Association Lockout problem(defined in 11.3 (STA authentication and association)).~~

### 9.6.9.2 SA Query Request frame

Change the 4th paragraph as shown:

The Transaction Identifier field is a ~~counter~~ value set by the STA sending the SA Query Request frame to identify any outstanding request/response transaction.

### 11.13 SA Query procedures

Change the first paragraph as shown:

If a STA and its peer negotiate management frame protection(#199), then the STA shall support the SA Query procedure. The STA or its peer may initiate an SA Query procedure at any point during an association to verify that the security association between the two devices is still valid.

Insert the following text after the 2nd paragraph:

The Transaction Identifier may be used for matching SA Query Responses with SA Query Requests when there are multiple, concurrent SA Query Requests.

Starting at the 7th paragraph, change the text as shown:

If a non-AP or non-PCP STA initiated an SA Query procedure following a channel switch and does not receive the SA Query Response frame from a STA that indicated OCVC within dot11AssociationSAQueryMaximumTimeout TUs from the beginning of the SA Query procedure, it shall deauthenticate from the BSS.

NOTE 1—A non-AP and non-PCP STA does not respond if it is trying to reassociate with the AP or PCP that sent the SA Query Request frame (since, except in the case of FT to the same AP, it no longer has the PTKSA) or to another AP or PCP (it could maintain the old association and PTKSA until the reassociation is completed). There is no such restriction for an AP or PCP.

If a non-AP and non-PCP STA that has ~~an SA~~a security association with its AP or PCP for an association that negotiated management frame protection receives an individually addressed 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~~security association 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~~security association. If no valid SA Query response is received, the non-AP and non-PCP STA’s SME may delete the ~~SA~~security association (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.

NOTE 2—The mechanism by which the MAC, MLME and SME coordinate the actions needed to effect these operations is outside the scope of this standard.

When an S1G STA in a power save mode wakes up with an interval longer than dot11AssociationSAQueryMaximumTimeout, an existing ~~SA~~security association can be destroyed. So, to maintain its valid ~~SA~~security association status, the S1G STA shall wake to listen ~~to~~for an SA Query Request frame with the interval specified by dot11AssociationSAQueryMaximumTimeout, relative to when the S1G STA received the (Re)Association Response frame for the current association. When dot11RSNAProtectedManagementFramesActivated is true, an S1G AP shall ~~provide~~ include a TIE ~~the timeout interval~~ with the Timeout Interval Type field indicating ~~(a~~Association comeback time~~, which is~~ and the Timeout Interval Value field set to dot11AssociationSAQueryMaximumTimeout~~)~~, in ~~an~~ Association Response frames and Reassociation Response frames with a status indicating success~~code 0 to the S1G STA~~.

### 12.6.16 RSNA security association termination

Delete NOTE 2 as shown:

NOTE 1—There is a race condition between when MLME-SETPROTECTION.request primitive is invoked on the Supplicant and when it is invoked on the Authenticator. During this time, the STA might receive an MPDU that it is unable to decrypt; and the MPDU is discarded without a deauthentication occurring.

~~NOTE 2—Null and QoS (+)Null frames are not protected.~~

### 12.6.17 Protection of robust Management frames.

Change the note as shown:

If management frame protection is negotiated for the link, a STA shall not transmit any of the following, and shall discard all of the following:

— An unprotected individually addressed Deauthentication or Disassociation frame.

NOTE 5—The STA might use this as an indication that there might be a mismatch in the association state between itself and the AP or PCP and might invoke the SA Query procedures (see 11.13 (SA Query procedures)) if received with a reason code of INVALID\_CLASS2\_FRAME or INVALID\_CLASS3\_FRAME.

### 12.7.6.3 4-way handshake message 2

*Note: Usage of the Transaction Identifier is only mentioned in 9.6.9.2 (SA Query Request frame):*

*The Transaction Identifier field is a counter value set by the STA sending the SA Query Request frame to identify any outstanding request/response transaction.*

*and 9.6.9.3 (SA Query Response frame):*

*The Transaction Identifier field is set to the same value as the Transaction Identifier field in the corresponding SA Query Request frame.*

*There does not appear to be any reason for this initialization step in 12.7.6.3, so we should either a) delete the step or b) provide some rules for usage and maintenance of this value.*

Delete item c as shown:

~~c) If management frame protection is being negotiated, the AP initializes the SA Query Transaction Identifier to an implementation specific non-negative integer value, valid for the current pairwise security association.~~

**References:**

[Draft P802.11REVme\_D7.0.pdf](https://grouper.ieee.org/groups/802/11/private/Draft_Standards/11me/Draft%20P802.11REVme_D7.0.pdf)