IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 11bi D1.0 12.16.5 comments | | | | |
| Date: 2025-03-25 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | Email |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |

Abstract

This submission resolves the following CIDs:

675, 676, 847, 848, 965

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Revision based on the discussion during the meeting

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 TGbi D1.0 Draft. This introduction is not part of the adopted material.

Editing instructions formatted like this are intended to be copied into the TGbi D1.0 Draft. (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents). TGbi Editor: Editing instructions preceded by “TGbi Editor” are instructions to the TGbi editor to modify existing material in the TGbi draft. As a result of adopting the changes, the TGbi editor will execute the instructions rather than copy them to the TGbi Draft.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 675 | 122.42 | 12.16.5 | "Include the AKM Suite Selector element indicating the selected IEEE 802.1X AKM." -- include where? This duplicates Clause 9 anyway. Ditto 123.4 | Delete the cited text | Rejected –  The main bullets says “The originator then constructs the first Authentication frame of the exchange as follows:”. Hence, it is in the first Authentication frame. For 123.4, the main bullet says “The responder then constructs the second Authentication frame of the exchange as follows:”. Hence, it is in the second Authentication frame. The text in clause 9 does not say it include what AKM. As a result, we need the texts in 12.16.5. |
| 676 | 0.00 | 12.16.5 | This subclause is lacking in "shall"s | Use "shall"s rather than just the present simple | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0536 under all headings that include CID 676 |
| 847 | 123.27 | 12.16.5 | The text indicates that the encapsulation length is 0 if the status is invalid, but does not indicate (as the earlier messages do) that the message might carry an EAPOL PDU. | Add bullet item listing possible EAPOL PDU | Rejected –  If the encapsulation length is 0, then there is no encapsulated EAPOL PDU. |
| 848 | 123.57 | 12.16.5 | Text describing the handling of status code should explicitly state that this is for all messages with sequence numbers of X or greater. | Change text to "If the processing status returned in any frame where the sequence number is X or greater is not SUCCESS, the originator or the responder shall terminate the authentication. | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0536 under all headings that include CID 848 |
| 965 | 123.56 | 12.16.5 | It is not described how the EAPOL exchange using Authentication frames is completed. Is Status Code 0 used in all cases? Even with EAP-Failure? Is the non-AP STA support to upper layer information (i.e., EAP-Success or EAP-Failure) to determine when authentication has been completed? If so, that needs to be specified. If not, there needs to be lower layer information (e.g., one new Status Code to indicate EAP exchange continues and Status Code 0 to indicate that EAP completed successfully and new Status Code to indicate that EAP resulted in failure). | Describe the exact rules based on which a non-AP STA or a non-AP MLD concludes that authentication succeeded or failed and can move to the next step (i.e., association in the success case). | Revised –  Agree in principle with the commenter. EAP success will indicate the authentication is successful to move to the next stage. EAP failure will indicate no further change is needed. Both will have status code 0 means processing successfully with EAPOL PDU sent  Note that when EAPOL PDU is exchange with the data frame, there is no specific status code in data frame for EAP continue and EAP success. Hence, non-AP STA already has ways to know when to move to the next step from EAP exchange  TGbi editor to make the changes shown in the latest version of 11-25/0536 under all headings that include CID 965 |

***Discussion:***

***Proposal:***

**TGbi Editor: *Instruction: Modify 12.16.5 as follows***

* IEEE 802.1X authentication utilizing Authentication frames

If an AP sets the IEEE 802.1X Authentication Utilizing Authentication Frame Support field in the RSNXE that it transmits to 1, then a non-AP STA (originator) with dot11EDPIEEE8021XAuthenticationUtilizingAuthenticationFrameActivated equal to true may signal its Supplicant to authenticate with the AP (responder) using IEEE Std 802.1X-2020 utilizing Authentication frames.

If any AP affiliated with an AP MLD sets the IEEE 802.1X Authentication Utilizing Authentication Frame Support field in the RSNXE that it transmits to 1, then a non-AP MLD (originator) with dot11EDPIEEE8021XAuthenticationUtilizingAuthenticationFrameActivated equal to true may signal its Supplicant to authenticate with the AP MLD (responder) using IEEE Std 802.1X-2020 utilizing Authentication frames by transmitting the Authentication frames to the AP through a non-AP STA affiliated with the non-AP MLD.

When the originator is a non-AP MLD and the responder is an AP MLD, the RA field of an Authentication frame in response to an Authentication frame from the peer shall be set to the TA field of the Authentication frame from the peer.

If an originator chooses to initiate IEEE 802.1X authentication utilizing Authentication frames, it first selects an IEEE 802.1X AKM that is supported by the responder.

The originator then shall construct(#676) the first Authentication frame of the exchange as follows:

* Authentication Algorithm Number field is set to 8 (IEEE 802.1X authentication).
* Authentication Transaction Sequence Number field is set to 1.
* The Encapsulation field carries an EAPOL PDU.
* Include the AKM Suite Selector element indicating the selected IEEE 802.1X AKM.

NOTE 1—The originator sends the EAPOL-Start Authentication frame as the first authentication frame to start the EAP authentication process.

The originator sends the first Authentication frame to the responder.

Upon receiving the first Authentication frame, the responder shall(#676):

* Validate(#676) that the AKM indicated in AKM Suite Selector element is an IEEE 802.1X AKM. Otherwise, processing status is set to STATUS\_INVALID\_AKMP.(#965)
* Validate(#676) that the selected IEEE 802.1X AKM indicated in AKM Suite Selector element is supported. Otherwise processing status is set to STATUS\_INVALID\_AKMP.
* Extract(#676) an EAPOL PDU from the Encapsulation field, and process(#676) it.

The responder then shall construct(#676) the second Authentication frame of the exchange as follows:

* Authentication Algorithm Number field is set to 8 (IEEE 802.1X authentication).
* Authentication Transaction Sequence Number field is set to 2.
* Status Code field indicates the processing status.
* The Encapsulation Length field indicates 0 if the status is set to STATUS\_INVALID\_AKMP.
* The Encapsulation field (if present) carries an EAPOL PDU.
* Include(#676) the AKM Suite Selector element indicating the same IEEE 802.1X AKM indicated in the first Authentication frame.

Once the processing is complete, the responder sends the second Authentication frame to the originator. If the processing status returned in the frame was not SUCCESS, the responder shall terminate the authentication.

Upon receiving the second Authentication frame, the originator shall(#676):

* Validate that the Status Code field is SUCCESS. Otherwise, the originator shall terminate the authentication. (#965)
* Validate(#676) that the AKM indicated in AKM Suite Selector element is the same as the one indicated in the first Authentication frame. Otherwise, processing status is set to STATUS\_INVALID\_AKMP.
* Extract(#676) an EAPOL PDU from the Encapsulation field, and process(#676) it.

The originator then shall construct(#676) the third Authentication of the exchange as follows:

* Authentication Algorithm Number field is set to 8 (IEEE 802.1X authentication).
* Authentication Transaction Sequence Number field is set to 3.
* Status Code field indicates the processing status.
* The Encapsulation Length field indicates 0 if the status is set to STATUS\_INVALID\_AKMP.
* The Encapsulation field (if present) carries an EAPOL PDU.(#965)

Once the processing is complete, the originator sends the third Authentication frame to the responder. If the processing status returned in the frame was not SUCCESS, the originator shall terminate the authentication.

Upon receiving the Authentication frame with Authentication Transaction Sequence Number field set to a value that(#848) is larger than or equal to 3, the originator or the responder shall(#676):

* Validate that the Status Code field is SUCCESS. Otherwise, the originator shall terminate the authentication. (#965)
* Extract(#676) an EAPOL PDU from the Encapsulation field, and process(#676) it.

If needed by the EAP method, the(#965) originator or the responder then shall construct(#676) the Authentication frame of the exchange in response to the Authentication frame with Authentication Transaction Sequence Number field set to a value that(#848) larger than or equal to 3, as follows:

* Authentication Algorithm Number field is set to 8 (IEEE 802.1X authentication).
* Authentication Transaction Sequence Number field is set to X+1.
* Status Code field indicates the processing status.
* The Encapsulation field (if present) carries an EAPOL PDU.

NOTE 2—The number of Authentication frame exchanges depends on the EAP method in use. Hence, X is a value as defined by the EAP method.

Once the processing is complete, the originator or the responder sends the Authentication frame in response to the Authentication frame with Authentication Transaction Sequence Number field set to a value that is larger than or equal to 3,(#848) to its peer (if needed by the EAP method). If the processing status returned in the frame was not SUCCESS, the originator or the responder shall terminate the authentication.

If the Supplicant does not have further EAPOL PDU to transmit, then the Supplicant concludes the authentication. (#965)

[status code for 802.1X on AP side]

[status code more texts for key derivation]