IEEE P802.11
Wireless LANs

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
| Clarification on GMAC AAD |
| Date: 2025-09-12 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel  |  |  | po-kai.huang@intel.com |
| Nehru Bhandaru | Broadcom |  |  | nehru.bhandaru@broadcom.com |

 |

Abstract

This submission proposes resolutions for the following comments from comment collection on P802.11-REVmf D1.0:

195

**Revision History:**

R0: Initial version.

R1: Editorial revision of the note.

R2: Change note to normative behaviors based on the received feedbacks. Align with D1.1. Changes are marked with green.

# CID 195

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page.Line** | **Comment** | **Proposed Change** | **Resolution** |
| 195 | 12.5.3.3 | 3295.46 | IEEE defines specific BIP AAD, which is is not the same as the AAD defintion in GMAC. The AAD of GMAC uses the entire frame that needs to be authenticated. To differentiate, it is good to always say BIP AAD, so it will not be confused with the GMAC AAD. The current spec sometimes says BIP AAD and sometimes just says AAD. | Clarify all relevant place of AAD to BIP AAD. Similar comments apply to CIP AAD. Contibution 11-25-1444 will be submitted to resolve this CID. | REVISED – Agree in principle with the commenter. Instruction to TGmf Editor:Instructions to the editor:  Please make the changes as shown under CID 195 in 11-25/1444r2 |

## Discussion:

GMAC is used for BIP and CIP, and IEEE defines specific AAD construction for BIP AAD and CIP AAD. However, NIST Special Publication 800-38D also defines AAD for GMAC, and the BIP/CIP AAD concatenated with he authented body is the AAD for the GMAC. To differentiate the two AAD instnaces, we should clearly label the “AAD” defined under BIP and CIP to be BIP AAD and CIP AAD. This has been done in certain instances but not all the instances. We propose clarification in all instances.

## Proposed Text:

**TGmf Editor: *Instruction: Modify 12.5.3 as follows:***

* Broadcast/multicast integrity protocol (BIP)
* BIP overview

BIP provides data integrity and replay protection for group addressed robust Management frames after establishment of an IGTKSA (see 12.6.1.1.9 (IGTKSA)). For non-S1G STAs, BIP provides data integrity and replay protection for Beacon frames after establishment of a BIGTKSA (see 12.6.1.1.11 (BIGTKSA)). For S1G STAs, BIP provides data integrity and replay protection for S1G Beacon frames after establishment of a BIGTKSA (see 12.6.1.1.11 (BIGTKSA)). BIP also provides integrity and replay protection for individually addressed and group addressed WUR frames (see 29.10 (WUR frame protection)).

BIP-CMAC-128 provides data integrity and replay protection, using AES-128 in CMAC Mode with a 128-bit integrity key and a CMAC TLen value of 128 (16 octets). BIP-CMAC-256 provides data integrity and replay protection, using AES-256 in CMAC Mode with a 256-bit integrity key and a CMAC TLen value of 128 (16 octets). NIST Special Publication 800-38B defines the CMAC algorithm, and NIST Special Publication 800-38D defines the GMAC algorithm. BIP processing uses AES with a 128-bit or 256-bit integrity key and a CMAC TLen value of 128 (16 octets). The CMAC output for BIP-CMAC-256 is not truncated and shall be 128 bits (16 octets). The CMAC output for BIP-CMAC-128 is truncated to 64 bits:

MIC = Truncate-64(CMAC Output).

BIP-GMAC-128 uses AES with a 128-bit integrity key, and BIP-GMAC-256 uses AES with a 256-bit integrity key. The authentication tag for both BIP-GMAC-128 and BIP-GMAC-256 is not truncated and shall be 128 bits (16 octets).

BIP uses the IGTK or BIGTK to compute the MMPDU MIC, uses the WTK to compute the MIC for protecting individually addressed WUR Wake-up frames, and uses the WIGTK to compute the MIC for protecting broadcast or group addressed WUR Wake-up frames. The Authenticator shall, if management frame protection is negotiated, distribute one new IGTK and IGTK PN (IPN) whenever it distributes a new GTK. The IGTK is identified by the MAC address of the transmitting STA plus an IGTK key ID that is encoded in the MME Key ID field. If beacon protection is enabled, the Authenticator may distribute one new BIGTK and BIPN when it distributes a new GTK. The BIGTK is identified by the MAC address of the transmitting STA plus:

* a BIGTK key ID that is encoded in the S1G Beacon Compatibility element, in S1G Beacon frames that use BCE or
* a BIGTK key ID that is encoded in the MME Key ID field, in Beacon frames and S1G Beacon frames that do not use BCE.

If WUR frame protection is negotiated, the Authenticator may distribute one new WIGTK and WIPN when it distributes a new GTK. The WIGTK is identified by the MAC address of the transmitting STA plus the WIGTK key ID that is encoded in the Key ID field (see Figure 12-51 (WIGTK KDE format), Figure 9-1477 (Miscellaneous subfield format), 9.4.2.294 (WUR PN Update element) and 9.4.2.46 (FTE).

* BIP encapsulation format

The MME shall follow all of the other elements in the management frame body but precede the FCS. See 9.4.2.53 (MME) for the format of the MME. The frame format for a protected Management frame is shown in Figure 12-23 (BIP encapsulation).

|  |  |  |
| --- | --- | --- |
| MAC header | Management frame body with MME as last element | FCS |
| * BIP encapsulation
 |

For S1G Beacon frames using BCE, the MIC element shall follow all of the other elements in the frame body but precede the FCS. See 9.4.2.117 (MIC element)for the format of the MIC element. The frame format for an S1G Beacon frame using BCE is shown in Figure 12-24 (BIP compact encapsulation).

|  |  |  |
| --- | --- | --- |
| MAC header | S1G Beacon frame body with MIC element as last element | FCS |
| * BIP compact encapsulation
 |

* BIP AAD construction

For MPDUs that are not S1G Beacon frames, the BIP Additional Authentication Data (AAD) is constructed from the MPDU header. BIP(#195) AAD construction is performed as follows:

* FC—MPDU Frame Control field, with:
* Retry subfield (bit 11) masked out
* Power Management subfield (bit 12) masked out
* More Data subfield (bit 13) masked out
* No modifications to other subfields
* A1—MPDU Address 1 field.
* A2—MPDU Address 2 field.
* A3—MPDU Address 3 field.

Figure 12-25 (BIP AAD construction) depicts the format of the BIP(#195) AAD.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | FC | A1 | A2 | A3 |
| Octets: | 2 | 6 | 6 | 6 |
| * BIP AAD construction
 |

For S1G Beacon frames when BCE is not in use, the BIP Additional Authentication Data (AAD) is constructed from the MPDU header. BIP(#195) AAD construction is performed as follows:

* FC-MPDU Frame Control field.
* SA-address of the STA transmitting the S1G Beacon frame.
* Change Sequence.
* Next TBTT (if present).
* Short SSID (if present).
* Access Network Options (if present).

NOTE 1—S1G APs with dot11APPMActivated equal to true may enter Power Save mode. To prevent disruption of BSS traffic by an attacker setting the AP PM subfield (bit 15) in modified beacons, the AP PM subfield in S1G Beacon frames is protected by inclusion in the BIP(#195) AAD.

NOTE 2—The Frame Control field in S1G Beacons does not contain Retry or More Data subfields.

Figure 12-26 (BIP AAD construction for S1G Beacon frames without BCE) depicts the format of the BIP(#195) AAD. The length of the BIP(#195) AAD is 9-17 octets.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | FC | SA | ChangeSequence | Next TBTT | Short SSID | Access Network Options |
| Octets: | 2 | 6 | 1 | 0 or 3 | 0 or 4 | 0 or 1 |
| * BIP AAD construction for S1G Beacon frames without BCE
 |

For S1G Beacon frames when BCE is in use, the BIP Additional Authentication Data (AAD) is constructed from the MPDU header and the BIPN. BIP(#195) AAD construction is performed as follows:

* FC-MPDU Frame Control field.
* SA-address of the STA transmitting the S1G Beacon frame.
* Change Sequence.
* Next TBTT (if present).
* Short SSID (if present).
* Access Network Options (if present).
* BIPN.

Figure 12-27 (BIP AAD construction for S1G Beacon frames with BCE) depicts the format of the BIP(#195) AAD. The length of the BIP(#195) AAD is 15-23 octets.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | FC | SA | ChangeSequence | Next TBTT | Short SSID | Access Network Options | BIPN |
| Octets: | 2 | 6 | 1 | 0 or 3 | 0 or 4 | 0 or 1 | 6 |
| * BIP AAD construction for S1G Beacon frames with BCE
 |

* BIP replay counters and packet numbers

When management frame protection is negotiated, the receiver shall maintain a 48-bit replay counter for each IGTK. The receiver shall set the replay counter to the value of the IPN in the IGTK KDE (see 12.7.2 (EAPOL-Key frames)) provided by the Authenticator in the 4-way handshake, FT 4-way handshake, FT handshake, group key handshake, or FILS authentication. The transmitter shall maintain a single IPN for each IGTK. The IPN shall be implemented as a 48-bit strictly increasing integer, initialized to 1 when the corresponding IGTK is initialized.

When beacon protection is enabled at the non-SP STA, the receiver shall maintain a 48-bit replay counter for each BIGTK. The receiver shall set the replay counter to the value of the BIPN in the BIGTK key data encapsulation (KDE) (see 12.7.2 (EAPOL-Key frames)) provided by the Authenticator in the 4-way handshake, FT 4-way handshake, FT handshake, group key handshake, or FILS authentication. The transmitter shall maintain a single BIPN for each BIGTK. When beacon protection is enabled at an S1G AP and BCE is enabled, the BIPN shall be implemented as a 48-bit representation of the number of TSBTTs or TBTTs since TSF time 0. If dot11ShortBeaconInterval is true, the BIPN shall be initialized using Equation (12-1):

* BIPN = Floor (*TSF* / (1024 × *dot11ShortBeaconPeriod*))

If dot11ShortBeaconInterval is false, the BIPN shall be initialized using Equation (12-2):

* BIPN = Floor (*TSF* / (1024 × *dot11BeaconPeriod*)

When adding protection to, or checking protection on, an S1G Beacon frame, if dot11ShortBeaconInterval is true, the BIPN shall be calculated using Equation (12-3):

* BIPN = *CurrentTSBTT* / (1024 × *dot11ShortBeaconPeriod*)

where

*CurrentTSBTT* is the TSBTT of the S1G Beacon frame that is being protected, in µs.

When adding protection to, or checking protection on, an S1G Beacon frame, if dot11ShortBeaconInterval is false, the BIPN shall be calculated using Equation (12-4):

* BIPN = *CurrentTBTT* / (1024 × *dot11BeaconPeriod*)

where

*CurrentTBTT* is the TBTT of the S1G Beacon frame that is being protected, in µs.

NOTE 1—Calculation of CurrentTBTT or CurrentTSBTT is implementation dependent. One possible implementation is the transmitter could use Ceil(*TSF*/(1024 x *dot11ShortBeaconPeriod*)) and Ceil(*TSF*/(1024 x *dot11BeaconPeriod*)), and the receiver could use Floor(*TSF*/(1024 x *dot11ShortBeaconPeriod*)) and Floor(*TSF*/(1024 x *dot11BeaconPeriod*)).

When beacon protection is enabled at an S1G AP and BCE is disabled, the BIPN shall be implemented as a 48-bit strictly increasing integer, initialized to 1 when the corresponding BIGTK is initialized. For non-S1G STAs, the BIPN shall be implemented as a 48-bit strictly increasing integer, initialized to 1 when the corresponding BIGTK is initialized.

See 12.5.3.5 (BIP transmission) and 12.5.3.6 (BIP reception) for per frame BIP processing, including detection of replayed frames.

If the PN is larger than dot11PNExhaustionThreshold, an MLME-PN-EXHAUSTION.indication primitive shall be generated.

NOTE 2—When the IPN space is exhausted, the choices available to an implementation are to replace the corresponding key or to end communications. When the BIPN space is exhausted and BCE is not in use, the choices available to an implementation are to replace the corresponding key or to end communications. When the BIPN space is exhausted and BCE is in use, the choices available to an implementation are to replace the corresponding key and reset the TSF to 0 or to end communications (and the AP may restart the BSS).

When dot11QMFActivated is true, the receiver shall maintain an additional replay counter for each ACI for received group addressed robust Management frames that use QMF.

NOTE 3—QMF is not supported for PV1 Management frames (see 11.24.1.1 (Overview)).

When management frame protection is negotiated, the receiver shall maintain a single replay counter for received group addressed robust Management frames that do not use the QMF service. If dot11QMFActivated is also true, the receiver shall maintain an additional replay counter for each ACI for received group addressed robust Management frames that use the QMF service. When the QMF service is not used, the transmitter shall preserve the order of protected group addressed robust Management frames that are transmitted to the same RA. When the QMF service is used, the transmitter shall preserve the order of protected robust GQMFs within an AC that are transmitted to the same RA.

* BIP transmission

When a STA transmits a protected group addressed robust Management frame that is not an S1G Beacon using BCE, it shall

* Select the IGTK or BIGTK currently active for transmission of frames to the intended group of receivers and construct the MME (see 9.4.2.53 (MME)) with the MIC field masked out and the Key ID field set to the corresponding IGTK key ID. If the frame is not a GQMF, the transmitting STA shall insert a strictly increasing integer into the MME IPN/BIPN field. If the frame is a GQMF, then the transmitting STA shall maintain a 48-bit counter for use as the IPN, the counter shall be incremented for each GQMF until the two least significant bits of the counter match the ACI of the AC that is used to transmit the frame, and the counter value shall be inserted into the MME IPN/BIPN field of the frame. For BIP-GMAC-128 and BIP-GMAC-256, the initialization vector (as defined in NIST Special Publication 800-38D) (#195) passed to GMAC shall be:
* For S1G Beacons: a concatenation of the SA field from the MAC header of the MPDU and the non-negative integer inserted into the MME IPN/BIPN field.
* For all other frames: a concatenation of Address 2 from the MAC header of the MPDU and the non-negative integer inserted into the MME IPN/BIPN field.

NOTE 1—QMF is not supported for PV1 Management frames (see 11.24.1.1 (Overview)).

* Compute BIP(#195) AAD as specified in 12.5.3.3 (BIP AAD construction).
* Compute an integrity value over the concatenation of BIP(#195) AAD and the management frame body including MME with:
* For protected Beacon frames: the Timestamp field masked out.
* For S1G Beacon Frames: the TSF Completion field of the S1G Beacon Compatibility element masked out, if the element is present.

 ca) For BIP-GMAC-128 and BIP-GMAC-256, the AAD (as defined in NIST Special Publication 800-38D) passed to GMAC shall be the concatenation defined in c), and the plaintext (as defined in NIST Special Publication 800-38D) passed to GMAC shall be empty. (#195)

Insert the output into the MME MIC field. For BIP-CMAC-128, the integrity value is 64 bits and is computed using AES-128-CMAC; for BIP-CMAC-256, the integrity value is 128 bits and is computed using AES-256-CMAC; for BIP-GMAC-128, the integrity value is 128 bits and is computed using  AES‑128-GMAC; and, for BIP-GMAC-256, the integrity value is 128 bits and is computed using AES-256-GMAC.

* Compose the frame as the MAC header, management frame body, including MME, and FCS. The MME shall appear last in the frame body.
* Transmit the frame.

When an S1G STA transmits a protected S1G Beacon frame using BCE, it shall:

* Select the BIGTK currently active for transmission of frames to the intended group of receivers.
* Set the BIGTK Key ID Index subfield in the S1G Beacon Compatibility element, if present, to the value that corresponds to the BIGTK key ID (see 9.4.2.195 (S1G Beacon Compatibility element)). If the S1G Beacon Compatibility element is not present, the BIGTK used to protect the frame shall be the same BIGTK used in the most recently transmitted protected S1G Beacon frame that contained an S1G Beacon Compatibility element. If that BIGTK is not available for use, or no previous protected S1G Beacon frame containing an S1G Beacon Compatibility element has been transmitted, then the frame shall be sent without BIP encapsulation.
* Construct the MIC element (see 9.4.2.117 (MIC element)) with the MIC field masked out.
* Derive the BIPN using Equation (12-3) if dot11ShortBeaconInterval is true, or Equation (12-4) if dot11ShortBeaconInterval is false. For BIP-GMAC-128 and BIP-GMAC-256, the initialization vector (as defined in NIST Special Publication 800-38D) (#195) passed to GMAC shall be a concatenation of the SA field from the MAC header of the MPDU and the non-negative integer inserted into the BIPN field. (#195)
* Compute BIP(#195) AAD as specified in 12.5.3.3 (BIP AAD construction).
* Compute an integrity value over the concatenation of BIP(#195) AAD and the management frame body including MIC element, with the TSF Completion field of the S1G Beacon Compatibility element masked out if the element is present.

fa) For BIP-GMAC-128 and BIP-GMAC-256, the AAD (as defined in NIST Special Publication 800-38D) passed to GMAC shall be the concatenation defined in f), and the plaintext (as defined in NIST Special Publication 800-38D) passed to GMAC shall be empty. (#195)

* Insert the output into the MIC field of the MIC element. For BIP-CMAC-128, the integrity value is 64 bits and is computed using AES-128-CMAC; for BIP-CMAC-256, the integrity value is 128 bits and is computed using AES-256-CMAC; for BIP-GMAC-128, the integrity value is 128 bits and is computed using AES-128-GMAC; and, for BIP-GMAC-256, the integrity value is 128 bits and is computed using AES-256-GMAC.
* Compose the frame as the MAC header, management frame body, including MIC element, and FCS. The MIC element shall appear last in the frame body.
* Transmit the frame.

A protected group addressed robust Management frame shall be protected using the group management cipher suite (see 9.4.2.23.2 (Cipher suites)).

NOTE 2—BIP does not provide protection against forgery by associated (if in an infrastructure BSS, and optionally in a PBSS) and authenticated STAs. A STA that has left the BSS can successfully forge group addressed robust Management frames until the IGTK is updated.

Once a STA transmits a protected Beacon frame or a protected S1G Beacon frame using a new BIGTK, the STA shall not transmit protected Beacon frames or protected S1G Beacon frames using the previous BIGTK. Once a STA transmits a protected group addressed robust Management frame using a new IGTK, the STA shall not transmit protected group addressed robust Management frames using the previously used IGTK.

* BIP reception

When a STA with management frame protection negotiated receives a group addressed robust Management frame, a protected Beacon frame, or a protected S1G Beacon frame that is not using BCE, it shall

* Identify the appropriate IGTK or BIGTK and associated state based on the MME Key ID field. If the frame is a robust Management frame and no such IGTK exists, silently discard the frame and terminate BIP processing for this reception. If the frame is a protected S1G Beacon frame, and the Encapsulation Mode for the key is BCE, the receiver shall silently discard the frame and optionally transmit to the AP a WNM Notification Re-quest frame to report beacon protection failure. If the frame is a protected Beacon frame and no such BIGTK exists, terminate BIP processing for this reception, and
* If beacon protection is enabled at the non-AP STA, silently discard the frame and optionally transmit to the AP a WNM Notification Request frame to report beacon protection failure.
* Perform replay protection on the received frame. The receiver shall interpret the MME IPN/BIPN field as a 48-bit unsigned integer.
* If the frame is a robust Management frame but not a GQMF, the receiver shall compare this MME IPN/BIPN to the value of the replay counter for the IGTK identified by the MME Key ID field. If the value from the received MME IPN/BIPN field is less than or equal to the replay counter value for this IGTK, the receiver shall discard the frame and increment the dot11RSNAStatsCMACReplays counter by 1.

NOTE 1—QMF is not supported for PV1 Management frames (see 11.24.1.1 (Overview)).

* If the frame is a robust Management frame and also a GQMF, the receiver shall compare this MME IPN/BIPN to the value of the replay counter for the IGTK identified by the MME Key ID field and the AC represented by the value of the ACI subfield of the received frame. If the value from the received MME IPN/BIPN field is less than or equal to the replay counter value for this IGTK and AC, the receiver shall discard the frame and increment the dot11RSNAStatsCMACReplays counter by 1.
* If the frame is a protected Beacon frame or a protected S1G Beacon frame, the receiver shall compare this MME IPN/BIPN to the value of the replay counter for the BIGTK identified by the MME Key ID field. If the integer value from the received MME IPN/BIPN field is less than or equal to the replay counter value for this BIGTK, the receiver shall discard the frame and increment the dot11RSNAStatsCMACReplays counter by 1.
* Compute BIP(#195) AAD for this Management frame, as specified in 12.5.3.3 (BIP AAD construction). For BIP-GMAC-128 and BIP-GMAC-256, an initialization vector (as defined in NIST Special Publication 800-38D) (#195) for GMAC is constructed as:
* For S1G Beacons: a concatenation of the SA field from the MAC header of the MPDU and the non-negative integer inserted into the MME IPN/BIPN field.
* For all other frames: a concatenation of Address 2 from the MAC header of the MPDU and the non-negative integer inserted into the MME IPN/BIPN field.
* Extract and save the received MIC value, and compute a verifier over the concatenation of BIP(#195) AAD, the management frame body, with:
* For protected Beacon frames: the Timestamp field masked out
* For S1G Beacon Frames: the TSF Completion field of the S1G Beacon Compatibility element masked out if the element is present,

and MME, with the MIC field masked out in the MME. For BIP-CMAC-128, the integrity value is 64 bits and is computed using AES-128-CMAC; for BIP-CMAC-256, the integrity value is 128 bits and is computed using AES-256-CMAC; for BIP-GMAC-128, the integrity value is 128 bits and is computed using AES-128-GMAC; and, for BIP-GMAC-256, the integrity value is 128 bits and is computed using AES-256-GMAC. If the result does not match the received MIC value, then the receiver shall discard the frame, increment the dot11RSNAStatsBIPMICErrors counter by 1, and terminate BIP processing for this reception.

 da) For BIP-GMAC-128 and BIP-GMAC-256, the AAD (as defined in NIST Special Publication 800-38D) passed to GMAC shall be the concatenation defined in d), and the plaintext (as defined in NIST Special Publication 800-38D) passed to GMAC shall be empty. (#195)

* If the frame is a robust Management frame but not a GQMF, update the replay counter for the IGTK identified by the MME Key ID field with the value of the MME IPN/BIPN field.
* If the frame is a robust Management frame and also a GQMF, update the replay counter for the IGTK identified by the MME Key ID field and the AC represented by the value of the ACI subfield of the received frame with the value of the MME IPN/BIPN field.
* If the frame is a protected Beacon frame or a protected S1G Beacon frame, update the replay counter for the BIGTK identified by the MME Key ID field with the value of the MME IPN/BIPN field.

When an S1G STA with management frame protection negotiated receives a protected S1G Beacon frame that is using BCE, it shall

* Identify the appropriate BIGTK and associated state based on the BIGTK Key ID Index subfield in the S1G Beacon Compatibility element, if present (see 9.4.2.195 (S1G Beacon Compatibility element)). If the S1G Beacon Compatibility element is not present, the BIGTK used to check the frame shall be the same BIGTK used in the most recently received protected S1G Beacon frame that contained an S1G Beacon Compatibility element. If the Encapsulation Mode for the key is Normal, the receiver shall silently discard the frame and optionally transmit to the AP a WNM Notification Request frame to report beacon protection failure.
* If no such BIGTK exists, terminate BIP processing for this reception, and
* If beacon protection is enabled at the non-AP STA, silently discard the frame and optionally transmit to the AP a WNM Notification Request frame to report beacon protection failure.
* Otherwise, process the frame.
* Derive the BIPN using Equation (12-3) if dot11ShortBeaconInterval is true, or Equation (12-4) if dot11ShortBeaconInterval is false. For BIP-GMAC-128 and BIP-GMAC-256, the initialization vector (as defined in NIST Special Publication 800-38D) (#195) passed to GMAC shall be a concatenation of the SA field from the MAC header of the MPDU and the BIPN.
* Perform replay protection on the received frame. The receiver shall compare the derived BIPN to the value of the replay counter for the identified BIGTK. If the integer value from the derived BIPN is less than or equal to the replay counter value for this BIGTK, the receiver shall discard the frame and increment the dot11RSNAStatsCMACReplays counter by 1.

NOTE 2—A STA should synchronize to the TSF prior to processing the first protected S1G Beacon frame using BCE.

* Compute BIP(#195) AAD for this Management frame, as specified in 12.5.3.3 (BIP AAD construction).
* Extract and save the received MIC value, and compute a verifier over the concatenation of BIP(#195) AAD, the management frame body, with the TSF Completion field of the S1G Beacon Compatibility element masked out if the element is present, and MIC element, with the MIC field masked out in the MIC ele-ment. For BIP-CMAC-128, the integrity value is 64 bits and is computed using AES-128-CMAC; for BIP-CMAC-256, the integrity value is 128 bits and is computed using AES-256-CMAC; for BIP-GMAC-128, the integrity value is 128 bits and is computed using AES-128-GMAC; and, for BIP-GMAC-256, the integrity value is 128 bits and is computed using AES-256-GMAC. If the result does not match the received MIC value, then the receiver shall discard the frame, increment the dot11RSNAStatsBIPMICErrors counter by 1, and terminate BIP processing for this reception.

g) For BIP-GMAC-128 and BIP-GMAC-256, the AAD (as defined in NIST Special Publication 800-38D) passed to GMAC shall be the concatenation defined in f), and the plaintext (as defined in NIST Special Publication 800-38D) passed to GMAC shall be empty. (#195)

**TGmf Editor: *Instruction: Modify 12.5.5 as follows:***

* Control integrity protocol (CIP)(#M7)
* Overview

The control integrity protocol (CIP) provides integrity and replay protection for the Control frames that are defined to be protected.

The cipher suite that is used for individually addressed Control frames in CIP is determined based on the negotiated pairwise cipher suite for individually addressed Data and Management frames. When GCMP-256 is used as the pairwise cipher suite, GMAC-256 shall be used for CIP of individually addressed Control frames. CIP cannot be used if another pairwise cipher suite is negotiated.

GMAC-256 shall be used for CIP of group addressed Control frames.

NIST Special Publication 800-38D defines the GMAC algorithm. GMAC-256 for CIP uses AES with a 256-bit integrity key. The authentication tag is not truncated and shall be 128 bits (16 octets).

If CIP is used, the same TK is used both for protecting individually addressed Data and Management frames with GCMP-256 and for protecting individually addressed Control frames with GMAC-256. The 4 most significant bits of the PN for protecting individually addressed Data and Management frames shall be set to a value that is less than 15 and the 4 most significant bits of the PN for protecting individually addressed Control frames shall be set to all 1s.

CIP uses the TK to compute the MIC of individually addressed Control frames that are defined to be protected.

CIP uses the control integrity group temporal key (CIGTK) and CIGTK packet number (CIPN) delivered by the AP to compute the MIC of group addressed Control frames that are defined to be protected. In a multiple BSSID set, all APs in the multiple BSSID set deliver and use the same CIGTK.

* Encapsulation format

To provide integrity and replay protection, CIP utilizes the Key ID, PN, and MIC in the Control frames that are defined to be protected.

The frame format is described in 9.3.1.7 (BlockAckReq frame format), 9.3.1.8 (BlockAck frame format), and 9.3.1.22 (Trigger frame format).

* CIP AAD construction

The CIP additional authentication data (AAD) is constructed from the Control frame header. CIP(#195) AAD construction is performed as follows without any bits masked out:

* Frame Control field
* Duration field
* RA field
* TA field

Figure 12-32 (CIP AAD construction) depicts the format of the CIP(#195) AAD.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Frame Control | Duration | RA | TA |
| Octets: | 2 | 2 | 6 | 6 |
| * CIP AAD construction
 |

* Replay counters and packet numbers

When CIP is negotiated between an AP and a non-AP STA:

* The non-AP STA and the AP shall maintain a single PN (48-bit counter) for each PTKSA for protecting individually addressed Control frames. The PN shall be implemented as a 48-bit strictly increasing integer. The 4 most significant bits of the PN shall be set to all 1s. The 44 least significant bits of the PN shall be initialized to 0.
* The non-AP STA and the AP shall maintain a 48-bit replay counter for each PTKSA to check replay of individually addressed Control frames between them that are defined to be protected.
* The AP shall maintain a single PN (48-bit counter) for each CIGTK. The PN shall be implemented as a 48-bit strictly increasing integer, initialized to 0 when the corresponding CIGTK is initialized. A single PN space shall be maintained for all APs in a multiple BSSID set.
* The non-AP STA shall maintain a 48-bit replay counter for each CIGTK to check replay of group addressed Control frames from the AP that are defined to be protected.
* Transmission

When a STA transmits a Control frame that is defined to be protected, it shall:

* Select the TK (if the Control frame is individually addressed) or CIGTK (if the Control frame is group addressed) currently active for transmission of individually addressed Control frames or group addressed Control frames, respectively.
* Increment the PN to obtain a fresh nonzero PN.
* Set the Key ID field to the corresponding key ID and set the PN0 field, the PN1 field, the PN2 field, the PN3 field, the PN4 field, and the PN5 field based on the corresponding PN. The initialization vector (as defined in NIST Special Publication 800-38D) passed to GMAC shall be a concatenation of the TA field and the non-negative integer value of the PN (#195)
* Compute the CIP(#195) AAD as specified in 12.5.5.3 (CIP AAD construction).
* For the Trigger frame, compute an integrity value over the concatenation of the CIP(#195) AAD and its contents after the TA field up to and including the last User Info field that precedes the first User Info field that carries the MIC (see Figure 9-107 (Formats of User Info fields with AID12 subfield equal to 2010(#M7))) and excluding anything from any of the User Info fields that carry the MIC or other subsequent User Info fields (if any) that follow the User Info fields that carry the MIC. Otherwise, compute an integrity value over the concatenation of the CIP(#195) AAD and contents after the TA field and before the MIC field. Insert the output into the MIC field.

 ea) The AAD (as defined in NIST Special Publication 800-38D) passed to GMAC shall be the concatenation defined in e), and the plaintext (as defined in NIST Special Publication 800-38D) passed to GMAC shall be empty. (#195)

* Include padding if needed to satisfy the padding requirement(s) of the intended recipient(s).
* Transmit the frame.
* Reception

When a STA receives a Control frame that is defined to be protected, it shall:

* Identify the appropriate TK (if the Control frame is individually addressed) or CIGTK (if the Control frame is group addressed) and associated state based on the Key ID field. If no such TK or CIGTK exists, silently discard the frame and terminate CIP processing for this reception.
* Perform replay protection on the received frame. The receiver shall interpret the PN field (constructed from the PN0 field, the PN1 field, the PN2 field, the PN3 field, the PN4 field, and the PN5 field if needed) as a 48-bit unsigned integer. The receiver shall compare the PN to the value of the replay counter identified by the Key ID field and the RA field. If the value from the PN field is less than or equal to the replay counter value, the receiver shall discard the frame and increment the dot11RSNAStatsCIPReplays counter by 1.
* The initialization vector (as defined in NIST Special Publication 800-38D) passed to GMAC shall be a concatenation of the TA field and the non-negative integer inserted into the PN field. (#195)
* Compute the CIP(#195) AAD as specified in 12.5.5.3 (CIP AAD construction).
* Extract and save the received MIC value. If the MIC value does not exist, silently discard the frame and terminate CIP processing for this reception. For the Trigger frame, compute a verifier over the concatenation of the CIP(#195) AAD and its contents after the TA field up to and including the last User Info that precedes the first User Info field that carries the MIC (see Figure 9-107 (Formats of User Info fields with AID12 subfield equal to 2010(#M7))) and excluding anything from any of the User Info fields that carry part of the MIC value or other subsequent User Info fields (if any) that follow the User Info fields that carry the MIC value. Otherwise, compute a verifier over the concatenation of the CIP(#195) AAD and contents following the TA field and before the MIC field. If the computed verifier is not equal to the received MIC value, then the receiver shall discard the frame, increment the dot11RSNAStatsCIPMICErrors counter by 1, and terminate CIP processing for this reception.

ea) The AAD (as defined in NIST Special Publication 800-38D) passed to GMAC shall be the concatenation defined in e), and the plaintext (as defined in NIST Special Publication 800-38D) passed to GMAC shall be empty. (#195)

* Update the corresponding replay counter identified by the Key ID field and the RA field with the value of the PN field.
* Padding

A STA transmitting a BCC-encoded PPDU that contains a protected Control frame shall ensure that for each target STA, the number of bits in the PSDU following *Vlast* is at least *MPAD,MAC* as defined in Equation (12-5), which is based on the MIC padding delay indicated by the target STA (see 9.4.2.316 (CIP Capabilities element(#M7))), where *Vlast* is:

* MIC[127] if the frame is a BlockAckReq frame or a Multi-STA BlockAck frame.
* The last bit of the User Info field containing MIC[127] (see Figure 9-107 (Formats of User Info fields with AID12 subfield equal to 2010(#M7))) if the frame is a Trigger frame.
* *MPAD,MAC* = *NDBPSMPAD*

where

*NDBPS* is defined in Table 17-4 (Modulation-dependent parameters) for a non-HT and non-HT duplicate PPDU, Table 19-7 (Frequently used parameters) for an HT PPDU, Table 21-6 (Frequently used parameters) for a VHT PPDU, and Table 27-16 (Frequently used parameters) for an HE PPDU. If the protected Control frame is carried in an HE MU PPDU, *NDBPS* is replaced by *NDBPS,u* of the target user in Equation (12-5).

*MPAD* is defined as follows:

 —  For a non-HT PPDU, HT PPDU, or VHT PPDU, *MPAD* is:

 - 0 if the MIC padding delay is 0 µs.

 - 1 if the MIC padding delay is 4 µs.

 - 2 if the MIC padding delay is 8 µs.

 - 3 if the MIC padding delay is 12 µs.

 - 4 if the MIC padding delay is 16 µs.

 - 5 if the MIC padding delay is 20 µs.

 - 6 if the MIC padding delay is 24 µs.

 - 7 if the MIC padding delay is 28 µs.

 - 8 if the MIC padding delay is 32 µs.

 —  For an HE PPDU, *MPAD* is:

 - 0 if the MIC padding delay is 0 µs.

 - 1 if the MIC padding delay is less than or equal to 16 µs.

 - 2 if the MIC padding delay is less than or equal to 32 µs.

Define *VProc* as the duration of the PPDU that is after the OFDM symbol containing the last coded bit of the LDPC codeword that encodes *Vlast* minus *TPE, nominal* defined in 27.3.13 (Packet extension) for an HE PPDU.

A STA transmitting an LDPC-encoded PPDU that contains a protected Control frame shall ensure that for each target STA, *VProc* is greater than or equal to the MIC padding delay indicated by the target STA (see 9.4.2.316 (CIP Capabilities element(#M7))).

In an A-MPDU, a STA shall not use other MPDUs that are different from the protected Control frame as the padding to satisfy the requirements of the MIC padding delay.

A STA transmitting a BCC-encoded PPDU that contains the last frame soliciting a protected Control frame shall ensure that for each target STA, the number of bits in the PSDU following *Clast* is at least *MPAD,MAC*, which is based on the MIC padding delay indicated by the target STA (see 9.4.2.316 (CIP Capabilities element(#M7))), where *Clast* is:

* The last bit of the FCS of the frame if the frame is not a protected Control frame
* *Vlast* if the frame is a Trigger frame (see 9.3.1.22.1 (General)) or a BlockAckReq frame (see 9.3.1.7.1 (Overview))

Define *CProc* as the duration of the PPDU that is after the OFDM symbol containing the last coded bit of the LDPC codeword that encodes *Clast* of the frame soliciting a protected Control frame minus *TPE, nominal* defined in 27.3.13 (Packet extension) for an HE PPDU.

A STA transmitting an LDPC-encoded PPDU that contains the last frame soliciting a protected Control frame shall ensure that for each target STA, *CProc* is greater than or equal to the MIC padding delay indicated by the target STA (see 9.4.2.316 (CIP Capabilities element(#M7))).

Except for the exception specified in this subclause, a STA may use any type of padding to satisfy the requirements, such as using the Padding field in a Trigger frame, a Compressed BlockAckReq frame or a Multi-TID BlockAckReq frame, using one or more Per-AID TID Info subfields with the AID11 subfield equal to 2047 in a Multi-STA BlockAck frame, using pre-EOF A-MPDU padding, using post-EOF A-MPDU padding, or aggregating other MPDUs in the A-MPDU.