802.11bi Draft Specification

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed spec texts for protected version of unicast management frames | | | | |
| Date: 2022-11-07 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |
| Danny Alexander |  |  |  |
| Ido Ouzieli |  |  |  |
| Johannes Berg |  |  |  |
| Ilan Peer |  |  |  |

Abstract

This submission proposes spec text based on the following passed requirement.

*11bi shall define an optional protected version of the following unicast management frames between a CPE AP and an associated CPE Client:*

* *Notify Channel Width frame*
* *SM Power save frame*
* *CSI frame*
* *Noncompressed Beamforming frame*
* *Compressed Beamforming frame*
* *VHT Compressed Beamforming frame*
* *Group ID Management frame*
* *Operating Mode Notification frame*
* *HE Compressed Beamforming/CQI frame*
* *Quiet Time Period Action frame*
* *EHT Compressed Beamforming/CQI frame*

Revision History:

* Rev 0: Initial version of the document

***Editing instructions formatted like this are intended to be copied into the TGbi 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 or insert 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.***

**TGbi Editor: *Instruction: Modify 3.4 Abbreviations and acronyms as shown below***

**3.4 Abbreviations and acronyms**

***Insert the following acronym definitions (maintaining alphabetical order):***

EDP enhanced data privacy

CPE client privacy enhancements

**TGbi Editor: *Instruction: Modify 9.4.2.1 General as shown below***

* + 1. **Elements**
       1. **General**

***Insert the following new rows to*** [***Table 9-128 (Element IDs)***](#bookmark99)***:***

**Table 9-128—Element IDs**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Element** | **Element ID** | **Element ID Extension** | **Extensible** | **Fragmentable** |
| EDP Capabilities (see 9.4.2.xxx (EDP [Capabilities element)](#bookmark180)) | 255 | <ANA> | Yes | No |

**TGbi Editor: *Instruction: Insert 9.4.2.xxx EDP Capabilities element as shown below***

9.4.2.xxx EDP Capabilities element

**9.4.2.xxx.1 General**

A STA declares that it is an EDP STA by transmitting the EDP Capabilities element.

The EDP Capabilities element contains a number of fields that are used to advertise the EDP capabilities of  
an EDP STA. The EDP Capabilities element is defined in Figure 9-xxxx (EDP Capabilities element format).

|  |  |  |  |
| --- | --- | --- | --- |
| Element | Length | Element ID Extension | CPE  Capabilities Information |

Octets: 1 1 1 1

**Figure 9-xxxx— EDP Capabilities element format**

The Element ID, Length, and Element ID Extension fields are defined in [9.4.2.1 (General)](#bookmark98).

The CPE Capabilities Information are defined in the subclauses below.

**9.4.2.xxx.2 CPE Capabilities Information field**

The format of the CPE Capabilities Information field is defined in [Figure 9-xxx](#bookmark182) (CPE [Capabilities Information field format)](#bookmark182).

B0 B1 B7

|  |  |
| --- | --- |
| EDP Robust Individually Addressed Management Frame Support(#13482) | Reserved |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Bits: | 1 |  | 7 |  |

**Figure 9-xxxx—CPE Capabilities Information field format**

The subfields of the CPE Capabilities Information field are defined in [Table 9-xxx (Subfields of the](#bookmark183) [CPE Capabilities Information field)](#bookmark183).

**Table 9-xxx—Subfields of the CPE Capabilities Information field**

|  |  |  |
| --- | --- | --- |
| **Subfield** | **Definition** | **Encoding** |
| EDP Robust Individually Addressed Management Frame Support | Indicates whether or not EDP robust individually addressed management frame is supported. | (#11847)Set to 1 if dot11EDPRobustIndividuallyAddressedManagementFrameActivated is true.  Set to 0 otherwise. |

**TGbi Editor: *Instruction: Modify 9.4.1.11 Action field as shown below***

**9.4.1.11 Action field**

***Insert the following new rows to*** [***Table 9-79 (Category values)***](#bookmark83) ***while maintaining the numerical order and updating the reserved range(#12432):***.

**Table 9-79—Category values**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Code** | **Meaning** | **See subclause** | **Robust** | **Group addressed privacy** |
| <ANA> | Protected HT | [9.6.xx (Protected HT Action frame](#bookmark231) [details)](#bookmark231) | Yes | No |
| <ANA> | Protected VHT | [9.6.xx (Protected VHT Action](#bookmark234) [frame details)](#bookmark234) | Yes | No |

**TGbi Editor: *Instruction: Insert 9.6.xx Protected HT Action frame details as shown below***

**9.6.xx Protected HT Action frame details**

**9.6.xx.1 Protected HT Action field**

A Protected HT Action field, in the octet immediately after the Category field, differentiates the Protected  
HT Action frame formats. The Protected HT Action field values associated with each frame format within  
the (#2217)Protected HT category are defined in Table 9-xxx (Protected HT Action field values).

**Table 9-xxx—Protected HT Action field values**

|  |  |  |
| --- | --- | --- |
| **Value** | **Meaning** | **Time Priority** |
| 0 | Protected Notify Channel Width | No |
| 1 | Protected SM Power Save | No |
| 2 | Reserved |  |
| 3 | Reserved |  |
| 4 | Protected CSI | Yes |
| 5 | Protected Noncompressed Beamforming | Yes |
| 6 | Protected Compressed Beamforming | Yes |
| 7–255 | Reserved |  |

**9.6.xx.2 Protected Notify Channel Width frame format**

The Protected Notify Channel Width frame allows robust STA-STA communication of the same information that is conveyed in the Notify Channel Width frame that is not robust (see 9.6.11.1 (HT Action field)).

The Action field of the Protected Notify Channel Width frame has the same format as the Action field of the  
Notify Channel Width frame (see 9.6.11.2 (Notify Channel Width frame format)), except that the Order 2 item is the Protected HT Action field, which is defined in 9.6.xx.1 (Protected HT Action field), instead of the HT Action field.

**9.6.xx.3 Protected SM Power Save frame format**

The Protected SM Power Save frame allows robust STA-STA communication of the same information that is conveyed in the SM Power Save frame that is not robust (see 9.6.11.1 (HT Action field)).

The Action field of the Protected SM Power Save frame has the same format as the Action field of the  
SM Power Save frame (see 9.6.11.3 (SM Power Save frame format)), except that the Order 2 item is the Protected HT Action field, which is defined in 9.6.xx.1 (Protected HT Action field), instead of the HT Action field.

**9.6.xx.4 Protected CSI frame format**

The Protected CSI frame allows robust STA-STA communication of the same information that is conveyed in the CSI frame that is not robust (see 9.6.11.1 (HT Action field)).

The Action field of the Protected CSI frame has the same format as the Action field of the  
CSI frame (see 9.6.11.5 (CSI frame format)), except that the Order 2 item is the Protected HT Action field, which is defined in 9.6.xx.1 (Protected HT Action field), instead of the HT Action field.

**9.6.xx.5 Protected Noncompressed Beamforming frame format**

The Protected Noncompressed Beamforming frame allows robust STA-STA communication of the same information that is conveyed in the Noncompressed Beamforming frame that is not robust (see 9.6.11.1 (HT Action field)).

The Action field of the Protected Noncompressed Beamforming frame has the same format as the Action field of the Noncompressed Beamforming frame (see 9.6.11.6 (Noncompressed Beamforming frame format)), except that the Order 2 item is the Protected HT Action field, which is defined in 9.6.xx.1 (Protected HT Action field), instead of the HT Action field.

**9.6.xx.6 Protected Compressed Beamforming frame format**

The Protected Compressed Beamforming frame allows robust STA-STA communication of the same information that is conveyed in the Compressed Beamforming frame that is not robust (see 9.6.11.1 (HT Action field)).

The Action field of the Protected Compressed Beamforming frame has the same format as the Action field of the Compressed Beamforming frame (see 9.6.11.7 (Compressed Beamforming frame format)), except that the Order 2 item is the Protected HT Action field, which is defined in 9.6.xx.1 (Protected HT Action field), instead of the HT Action field.

**TGbi Editor: *Instruction: Insert 9.6.xx Protected VHT Action frame details as shown below***

**9.6.xx Protected VHT Action frame details**

**9.6.xx.1 Protected VHT Action field**

A Protected VHT Action field, in the octet immediately after the Category field, differentiates the Protected  
VHT Action frame formats. The Protected VHT Action field values associated with each frame format within  
the (#2217)Protected VHT category are defined in Table 9-xxx (Protected VHT Action field values).

**Table 9-xxx—Protected VHT Action field values**

|  |  |  |
| --- | --- | --- |
| **Value** | **Meaning** | **Time priority** |
| 0 | Protected VHT Compressed Beamforming | Yes |
| 1 | Protected Group ID Management | No |
| 2 | Protected Operating Mode Notification | No |
| 3–255 | Reserved |  |

**9.6.xx.2 Protected VHT Compressed Beamforming frame format**

The Protected VHT Compressed Beamforming frame allows robust STA-STA communication of the same information that is conveyed in the VHT Compressed Beamforming frame that is not robust (see 9.6.22.1 (VHT Action field)).

The Action field of the Protected VHT Compressed Beamforming frame has the same format as the Action field of the VHT Compressed Beamforming frame (see 9.6.22.2 (VHT Compressed Beamforming frame format)), except that the Order 2 item is the Protected VHT Action field, which is defined in 9.6.xx.1 (Protected VHT Action field), instead of the VHT Action field.

**9.6.xx.3 Protected Group ID Management frame format**

The Protected Group ID Management frame allows robust STA-STA communication of the same information that is conveyed in the Group ID Management frame that is not robust (see 9.6.22.1 (VHT Action field)).

The Action field of the Protected Group ID Management frame has the same format as the Action field of the Group ID Management frame (see 9.6.22.3 (Group ID Management frame format)), except that the Order 2 item is the Protected VHT Action field, which is defined in 9.6.xx.1 (Protected VHT Action field), instead of the VHT Action field.

**9.6.xx.4 Protected Operating Mode Notification frame format**

The Protected Operating Mode Notification frame allows robust STA-STA communication of the same information that is conveyed in the Operating Mode Notification frame that is not robust (see 9.6.22.1 (VHT Action field)).

The Action field of the Protected Operating Mode Notification frame has the same format as the Action field of the Operating Mode Notification frame (see 9.6.22.4 (Operating Mode Notification frame format)), except that the Order 2 item is the Protected VHT Action field, which is defined in 9.6.xx.1 (Protected VHT Action field), instead of the VHT Action field.

**TGbi Editor: *Instruction: Modify 9.6.32.1 Protected HE Action field as shown below (Track change on)***

**9.6.32 Protected HE Action frame details(11ax)  
9.6.32.1 Protected HE Action field**

A Protected HE Action field, in the octet immediately after the Category field, differentiates the Protected HE Action frame formats. The Protected HE Action field values associated with each frame format within the (#2217)Protected HE category are defined in Table 9-619 (Protected HE Action field values(11ax)).

|  |  |
| --- | --- |
| * **Protected HE Action field values(11ax)** | |
| **Value** | **Meaning** |
| 0 | HE BSS Color Change Announcement |
| 1 | MU EDCA Reset |
| 2 | Protected HE Compressed Beamforming/CQI |
| 3 | Protected Quiet Time Period Action |
| 4–255 | Reserved |

**TGbi Editor: *Instruction: Insert 9.6.32.3 Protected HE Compressed Beamforming/CQI frame format***

***and 9.6.32.4 Protected Quiet Time Period Action frame format as shown below***

**9.6.32.3 Protected HE Compressed Beamforming/CQI frame format**

The Protected HE Compressed Beamforming/CQI frame allows robust STA-STA communication of the same information that is conveyed in the HE Compressed Beamforming/CQI frame that is not robust (see 9.6.31.1 (HE Action field)).

The Action field of the Protected HE Compressed Beamforming/CQI frame has the same format as the Action field of the HE Compressed Beamforming/CQI frame (see 9.6.31.2 (HE Compressed Beamforming/CQI frame format)), except that the Order 2 item is the Protected HE Action field, which is defined in 9.6.32.1 (Protected HE Action field), instead of the HE Action field.

**9.6.32.4 Protected Quiet Time Period Action frame format**

The Protected Quiet Time Period Action frame allows robust STA-STA communication of the same information that is conveyed in the Quiet Time Period Action frame that is not robust (see 9.6.31.1 (HE Action field)).

The Action field of the Protected Quiet Time Period Action frame has the same format as the Action field of the Quiet Time Period Action frame (see 9.6.31.3 (Quiet Time Period Action frame format)), except that the Order 2 item is the Protected HE Action field, which is defined in 9.6.32.1 (Protected HE Action field), instead of the HE Action field.

**TGbi Editor: *Instruction: Modify 9.6.34.1 Protected EHT Action field as shown below (Track change on)***

* + 1. **Protected EHT Action frame details**
       1. **Protected EHT Action field**

A Protected EHT Action field, in the octet immediately after the Category field, differentiates the Protected EHT Action frame formats. The Protected EHT Action field values associated with each frame format within the EHT category are defined in [Table 9-623c (Protected EHT Action field values)](#bookmark236).

**Table 9-623c—Protected EHT Action field values**

|  |  |  |
| --- | --- | --- |
| **Value** | **Meaning** | **Time priority** |
| 0 | TID-To-Link Mapping Request | No |
| 1 | TID-To-Link Mapping Response | No |
| 2 | TID-To-Link Mapping Teardown | No |
| 3 | EPCS Priority Access Enable Request | No |
| 4 | EPCS Priority Access Enable Response | No |
| 5 | EPCS Priority Access Teardown | No |
| 6 | EML Operating Mode Notification | No |
| (#12808)7 | Link Recommendation | No |
| 8 | Protected EHT Compressed Beamforming/CQI frame | Yes |
| 9–255 | Reserved |  |

**TGbi Editor: *Instruction: Insert 9.6.35.10 Protected EHT Compressed Beamforming/CQI frame format***

***format as shown below***

**9.6.35.10 Protected EHT Compressed Beamforming/CQI frame format**

The Protected EHT Compressed Beamforming/CQI frame allows robust STA-STA communication of the same information that is conveyed in the EHT Compressed Beamforming/CQI frame that is not robust (see 9.6.34.1 (EHT Action field)).

The Action field of the Protected EHT Compressed Beamforming/CQI frame has the same format as the Action field of the EHT Compressed Beamforming/CQI frame (see 9.6.34.2 (EHT Compressed Beamforming/CQI frame format)), except that the Order 2 item is the Protected EHT Action field, which is defined in 9.6.35.1 (Protected EHT Action field), instead of the EHT Action field.

**TGbi Editor: *Instruction: Insert the following to the end of 12.6.20 Robust management frame selection procedure ncement as shown below***

**12.6.20 Robust management frame selection procedure**

(…existing texts…)

The selection rules for individually addressed Protected TWT Setup, Protected TWT Teardown, and Protected TWT Information frames are described in 10.47.1 (TWT overview).

The selection rules for EDP robust individually addressed management frames are described in 12.13.1 (EDP Robust Individually Addressed Management Frame).

**TGbi Editor: *Instruction: Insert 12.13 Client Privacy Enhancement as shown below***

**12.13 Client Privacy Enhancement**

**12.13.1 EDP Robust Individually Addressed Management Frame**

This subclause defines rules for the individually addressed management frames described in Table 9-xxx (EDP robust individually addressed management frame and its corresponding unrobust individually addressed management frame).

|  |  |  |
| --- | --- | --- |
| Robust | Unrobust | Protected Beamforming/CSI/CQI frame |
| Protected Notify Channel Width frame | Notify Channel Width frame | No |
| Protected SM Power save frame | SM Power save frame | No |
| Protected CSI frame | CSI frame | Yes |
| Protected Noncompressed Beamforming frame | Noncompressed Beamforming frame | Yes |
| Protected Compressed Beamforming frame | Compressed Beamforming frame | Yes |
| Protected VHT Compressed Beamforming frame | VHT Compressed Beamforming frame | Yes |
| Protected Group ID Management frame | Group ID Management frame | No |
| Protected Operating Mode Notification frame | Operating Mode Notification frame | No |
| Protected HE Compressed Beamforming/CQI frame | HE Compressed Beamforming/CQI frame | Yes |
| Protected Quiet Time Period Action frame | Quiet Time Period Action frame | No |
| Protected EHT Compressed Beamforming/CQI frame | EHT Compressed Beamforming/CQI frame | No |

**Table 9-xxx—EDP robust individually addressed management frame and its corresponding unrobust individually addressed management frame**

When performing operations that need to use any unrobust individually addressed management frame described in Table 9-xxx (EDP robust individually addressed management frame and its corresponding unrobust individually addressed management frame), if management frame protection is negotiated and both STAs set the EDP Robust Individually Addressed Management Frame Support subfield of the CPE Capabilities Information field in the EDP Capabilities element that they transmit to 1, the STAs shall

* use the corresponding robust individually addressed frame described in Table 9-xxx (EDP robust individually addressed management frame and its corresponding unrobust individually addressed management frame) instead of the unrobust individually addressed frame and
* discard any unrobust individually addressed management frame described in Table 9-xxx (EDP robust individually addressed management frame and its corresponding unrobust individually addressed management frame) from the peer STA, with which management frame protection is negotiated.

If management frame protection is not negotiated or the EDP Robust Individually Addressed Management Frame Support Support subfield of the CPE Capabilities Information field in the EDP Capabilities element by either STA is set to 0, the STAs shall not use any robust individually addressed frame described in Table 9-xxx (EDP robust individually addressed management frame and its corresponding unrobust individually addressed management frame).

**TGbi Editor: *Instruction: Modify 12.5.3.4.4 PN and replay detection as shown below (Track Change On)***

**12.5.3.4.4 PN and replay detection**

…

The following processing rules are used to detect replay:

…

c) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a single replay counter for received individually addressed robust Management frames except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)) and Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)) that are received with the To DS subfield equal to 0 and Protected Beamforming/CSI/CQI frame (see 12.13.1 (EDP Robust Individually Addressed Management Frame)), and a single replay counter for received individually addressed robust PV1 Management frames except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)), Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)), and Protected Beamforming/CSI/CQI frame (see 12.13.1 (EDP Robust Individually Addressed Management Frame)), and shall use the PN from the received frame to detect replays.

d) If dot11RSNAProtectedManagementFramesActivated is true and dot11QMFActivated is also true, the recipient shall maintain an additional replay counter for each ACI for received individually addressed robust Management frames and robust PV1 Management frames that are received with the To DS subfield equal to 1, except Protected Fine Timing frames (9.6.34 Protected Fine Timing Frame details), protected PV1 Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)), Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)), and Protected Beamforming/CSI/CQI frame (see 12.13.1 (EDP Robust Individually Addressed Management Frame)).

The QMF receiver shall use the ACI encoded in the Sequence Number field of the  
received frame to select the replay counter to use for the received frame, and shall use the  
PN from the received frame to detect replays. A replayed frame occurs when the PN from  
the frame is less than or equal to the current value of the management frame replay  
counter that corresponds to the ACI of the frame.

e) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a separate replay counter for receiving individually addressed Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)) and shall use the PN from the received frame to detect replays.

f) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a separate replay counter for receiving individually addressed Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)) and shall use the PN from the received frame to detect replays.

fa) For non-MLO, if dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a separate replay counter for receiving individually addressed Protected Beamforming/CSI/CQI frame (see 12.13.1 (EDP Robust Individually Addressed Management Frame)) and shall use the PN from the received frame to detect replays.

fb) For MLO, if dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a separate replay counter in each setup link for receiving individually addressed Protected Beamforming/CSI/CQI frame (see 12.13.1 (EDP Robust Individually Addressed Management Frame)) and shall use the PN from the received frame to detect replays.

….

**TGbi Editor: *Instruction: Modify 12.5.3.4.4 PN and replay detection as shown below (Track Change On)***

**12.5.5.4 GCMP decapsulation**

**12.5.5.4.4 PN and replay detection**

…

The following processing rules are used to detect replay:

…

c) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a single replay counter for received individually addressed robust Management frames except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)) and Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)) that are received with the To DS subfield equal to 0 and Protected Beamforming/CSI/CQI frame (see 12.13.1 (EDP Robust Individually Addressed Management Frame)), and a single replay counter for received individually addressed robust PV1 Management frames except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)), Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)), and Protected Beamforming/CSI/CQI frame (see 12.13.1 (EDP Robust Individually Addressed Management Frame)), and shall use the PN from the received frame to detect replays.

d) If dot11RSNAProtectedManagementFramesActivated is true and dot11QMFActivated is also true, the recipient shall maintain an additional replay counter for each ACI for received individually addressed robust Management frames and robust PV1 Management frames that are received with the To DS subfield equal to 1, except Protected Fine Timing frames (9.6.34 Protected Fine Timing Frame details), protected PV1 Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)), Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)), and Protected Beamforming/CSI/CQI frame (see 12.13.1 (EDP Robust Individually Addressed Management Frame)).

The QMF receiver shall use the ACI encoded in the Sequence Number field of the  
received frame to select the replay counter to use for the received frame, and shall use the  
PN from the received frame to detect replays. A replayed frame occurs when the PN from the frame is less than or equal to the current value of the management frame replay  
counter that corresponds to the ACI of the frame.

e) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a separate replay counter for receiving individually addressed Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)) and shall use the PN from the received frame to detect replays.

f) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a separate replay counter for receiving individually addressed Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)) and shall use the PN from the received frame to detect replays.

fa) For non-MLO, if dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a separate replay counter for receiving individually addressed Protected Beamforming/CSI/CQI frame (see 12.13.1 (EDP Robust Individually Addressed Management Frame)) and shall use the PN from the received frame to detect replays.

fb) For MLO, if dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a separate replay counter in each setup link for receiving individually addressed Protected Beamforming/CSI/CQI frame (see 12.13.1 (EDP Robust Individually Addressed Management Frame)) and shall use the PN from the received frame to detect replays.

…..