IEEE802.16t Direct Peer to Peer (DPP) Requirements

March 13th, 2023

# Content

[1 Content 2](#_Toc129605031)

[2 Definitions and Terms 3](#_Toc129605032)

[3 General 4](#_Toc129605033)

[4 DPP Air Interface Protocol (AIP) 5](#_Toc129605034)

[5 Channel Access in Mode 1 (HD with CSMA/CA) 8](#_Toc129605035)

[6 DPP Terminal States 12](#_Toc129605036)

[7 DPP link Connectivity Establishment and Maintenance Procedures 14](#_Toc129605037)

[8 Message formats 19](#_Toc129605038)

# Definitions and Terms

## **Direct Peer-to-Peer (DPP)**: Direct link between two terminals with no Base Station infrastructure in between.

## **DPP Terminal**: Each of the two terminals of the DPP link.

## **DPP Channel**: A continuous frequency range or an aggregation of multiple non-adjacent frequency ranges used for communication between DPP terminals.

## **Unpaired DPP Channel:** the same DPP channel is used for communication in both directions.

## **Paired DPP Channel:** Two distinct DPP channels are used, one for each direction.

## **DPP Sub-channel:** A partition of DPP channel in the frequency domain.

## **DPP Sub-channel group**: An aggregation of one or more adjacent or non-adjacent DPP sub-channels. A DPP link operates over one subchannel group.

## **Unpaired DPP Sub-channel group**: The same subchannel group is used for both directions of communication between two DPP terminals.

## **Paired DPP subchannel group:** Two distinct subchannel groups are used, one for each direction.

## **Half Duplex (HD):** Communication in both directions is not done at the same time.

## **Time Division Duplex (TDD):** The timeline is divided into frames. Each frame is divided into two subframes, each used for communication in one of the two directions.

## **CSMA/CA**: Carrier Sense Multiple Access with Collision Avoidance

## **RTS**: Request to Send

## **CTS**: Clear to Send

## **Slot**: The minimal duration usage within a subchannel.

## **Robust MCS**: The highest MCS that can reliably be decoded by the peer DPP terminal.

## **Transmit MCS**: The MCS used by the DPP terminal for transmission.

## **Receive MCS**: The MCS used by the DPP terminal for reception.

## **Over the Air (OTA)**

## **Air Interface Resource (AIR):** A two-dimensional entity with a frequency and a time range. Can be expressed in terms of slots.

## **Air Interface Resource Manager (AIRM):** An entity which may instruct a DPP terminal which AIRs it can use for transmission.

## **Air Interface Protocol (AIP):** A set of rules defining how two DPP terminals communicate with each other over the air.

## **Service Flow (SF):** A one direction virtual connection used to carry PDUs meeting certain classification rules.

# General

## This document presents the ieee802.16t Direct Peer to Peer (DPP) communication between two DPP terminals, with no base station infrastructure. The two DPP terminals of a DPP link are identical (no master slave relationship) and the DPP Air Interface Protocol (AIP) is symmetrical. Minimal a priori configuration as described in this document is needed to establish link connectivity.

## DPP terminals communicate over a paired or unpaired DPP sub-channel group.

## A DPP link operates in one of the following modes:

### HD mode with no strict framing using a CSMA/CA access mechanism. A DPP terminal operating in this mode will only transmit when needed. The CSMA/CA mechanism is used to resolve contentions between the two DPP terminals of the DPP link and resolve possible contentions with DPP terminals of other in range DPP links.

### TDD mode with configurable framing. In this mode, a DPP terminal may be controlled by an AIRM to avoid interfering with ieee802.16t PtMP systems. Also, this mode will support strict QOS scheduling, e.g., UGS.

## An ieee802.16t DPP terminal employs the same PHY layer for transmit and receive. The PHY layer is identical to the uplink PHY layer used in the ieee802.16t PtMP AIP.

## When operating in HD mode with no strict framing, each TDD terminal employs CSMA/CA before start of transmission. In this mode, a DPP link may interfere with a nearby ieee802.16 PtMP system if operated in the same frequency. Moreover, if operated in the same frequency, the DPP terminals may be starved due to high utilization activity in a nearby ieee802.16 system. It is therefore required to use a dedicated frequency for DPP operating in this mode whenever it is in range of a PtMP ieee802.16 system.

## DPP Terminals employ various connectivity management messages with their peer for power control, MCS selection (this is also referred to as “Link Adaptation”) and automatic PHS rules establishment.

## The ieee802.16t DPP MAC PDU structure is described paragraph 4.1.6. It is optimized for the DPP requirements. The PDU can be used to encapsulate one SDU, concatenate multiple SDUs, encapsulate a fragment of concatenated SDUs or concatenate fragments of multiple SDUs.

## A DPP link may employ multiple service flows in each direction with a unique SFID carried in the MAC PDU header. Each service flow carries SDUs which meet a classification rule at the DPP terminal at which the SDU is received. Each service flow has an associated traffic priority between 1 to 7 (the lower the number, the higher the priority). Higher priority SDUs are transmitted before lower priority SDUs.

## Each DPP terminal may automatically establish Packet Header Suppression (PHS) rules with its peer.

# DPP Air Interface Protocol (AIP)

## **DPP AIP mode 1 (no framing)**

### In this mode, the DPP terminal generates bursts as described in Figure 1 below. The burst consists of a Gain Adjustment, Synchronization, Control Message and one or more PDU fields. The gain adjustment field is added in this mode to support connectionless operation.

### A SC-FDMA waveform is used for communication in both the directions. The waveform is as described in the 802.16t PHY specification section “3.4.2 Uplink”. The Control Message and the Data PDUs waveform generation follows the procedure described in the 802.16t PHY specification document, section “3.8 Uplink transmitter”.

### The waveform generation for the Gain Adjustment and the Synchronization fields, skips the channel coding and slot formation part of the procedure described in the 802.16t PHY specification document, section “3.8 Uplink transmitter”. These signals are transmitted in the lowest subchannel in the subchannel group.

### One transmission cycle constitutes one burst and a burst can have multiple PDUs.

Table

Description automatically generated

Figure 1 OTA burst structure in mode 1

### OTA Burst structure:

1. **Gain Adjustment Period**: the transmitter shall transmit the one slot worth alternate 1’s and 0’s BPSK modulated signal for a receiver to adjust the gain.
2. **Synchronization:** the preamble is used as a synchronization signal carrying Gold sequence of length 63, details are mentioned in 802.16t PHY specification document, refer to the section “*3.7.2 Downlink Preamble Transmission”.*
3. **Control Message:** The control message (CTRL MSG) shall carry the characteristics of the burst such as the MCS, length of the burst in slots etc. The CTRL MSG shall be transmitted with the robust MCS. Refer 8.1.4 for message structure.
4. **PDU**: The PDUs will be transmitted over the air in the same manner as it is processed in the 802.16t. Refer to 802.16t PHY specification document, section “*3.8* *Uplink transmitter” except the Ranging section.*

The total duration of the burst will not exceed the value of the configurable Max TX duration. This parameter will be specified in slots.

### PDU structure

1. The complete PDU structure has 6 Bytes Header followed by the variable length payload and the 4 bytes CRC as shown in Figure 2

Diagram

Description automatically generated

Figure 2 PDU Structure

PDU header is as shown in and described in

1. Table 4‑1.

Table

Description automatically generated

Figure 3 PDU Header Structure

|  |  |  |
| --- | --- | --- |
| 1. Syntax | Size(bit) | Notes |
| PDU\_header () { | --- | ---- |
| Header Type | 1 | 0 : Control PDU 1:Data PDU |
| Encryption indication | 1 | 0: Off 1:On |
| PHS indication | 1 | 0: Off 1: On |
| ACK indication | 1 | 0: Off 1: On |
| Reserved | 4 |  |
| Length | 16 | Length in bytes of the PDU including the header and the 4 Byte CRC. |
| Payload data ID or type | 8 | Indicates the type of message and sub headers are present in the message payload or not. |
| If (PHS indication == 1) PHS index | 8 | If PHS Indication is 0 set to 0. |
| HCS | 8 | CRC for the above 5 bytes |

Table 4‑1 : PDU Header fields

1. Header contains below details:
2. Header Type indicates two types of PDU.
3. Value 0 indicates it is Control PDU
   * RTS, CTS,
   * Security, SF, LA related
4. Value 1 indicates it is Data PDU
5. Encryption indication, value 0 indicates the Data is not encrypted 1 indicates data is encrypted.
6. PHS indication, value 0 indicates PHS is disabled and 1 indicates enabled.
7. ACK indication, value 0 indicates ACK is not needed for the PDU, value 1 indicates DPP terminal has to send ACK for the PDU received on CRC pass.
8. PDU length, value can be from 0 to 65535.
9. Payload ID or Data type, Indicates the type of message and sub headers are present in the message payload or not.
10. PHS index if PHS indication is 1 this field indicates the PHS index.
11. HCS is computed same as Table 6-3 HCS mentioned in the 802.16.
12. One or more control messages and SDUs can be encapsulated in one PDU. For example, a node is waiting for transmission and packets get queued, then the packets can be concatenated to single PDU and transmitted, provided it is under tolerable latency.
13. PDU CRC is computed in same manner as described in 802.16 section 6.3.3.5 CRC calculation.

## **DPP AIP mode 2 (TDD)**

### The DPP terminals will be configured with TDD frame parameters including, frame duration, subframes durations and gaps durations. The default frame configuration will be symmetrical, i.e., the two subframes and the two gaps will have identical durations. Non-symmetrical frame configuration can be done manually.

### The DPP terminal will support automatic subframe selection during the association state as described in this document.

### DPP AIP mode 2 is connection oriented. Connectivity between the two DPP terminals is maintained with a Sync and CTRL MSG transmitted by each DPP terminal at the beginning of their respective subframes. The receive gain will be calculated based on the Sync and CTRL message and the adjustment slot will not be required in this mode.

### The structure of the burst in DPP mode 2 is shown in Figure 4 below. The sync, CTRL and PDU fields are the same as for mode 1 as described above.

### 

Table

Description automatically generated with medium confidence

Figure 4 OTA burst structure in mode 2

### The total duration of the burst will not exceed the duration of the respective subframe.

### A DPP node operating in mode 2 may be controlled by a AIRM. In this case, the DPP terminal will only transmit as per BSC allocations.

# Channel Access in Mode 1 (HD with CSMA/CA)

## General

### The following channel/sub-channel access schemes shall be supported by a DPP terminal:

## Half Duplex CSMA/CA with the same frequency used in both directions.

## Half Duplex CSMA/CA with a distinct frequency used in each direction. In this case, sensing is done against both transmit and receive frequencies.

## The CSMA/CA mechanism will be optionally augmented with Request to Send (RTS) and Clear to Send (CTS) messages. This is applicable to both cases above.

### A channel dedicated to the DPP service can be divided into sub-channels, same as it is done in the ieee802.16t Point to Multipoint AIP.

### A Max TX duration parameter shall be configured in a DPP terminal to avoid excessive usage of the channel by one DPP terminal. This parameter is an integer multiple of the slot duration. This parameter will be configured based on the application/deployment scenario.

### When the DPP terminal has data to transmit, the total duration of the burst in slots is computed, based on the length of the SDUs in the buffer and the MCS. The lowest priority SDUs may be left out if needed and fragmentation may be used such that the burst duration does not exceed the configured maximum TX duration.

### Random Backoff Count (RBC) is set to zero before the beginning of each transmission attempt. RSSI threshold is used to compare the RSSI measured, and channel access is taken if the measured RSSI is less than the threshold. In case the channel is busy, RBC count is incremented, and the random back-off duration is selected as a value between the one slot duration to the MAX TX Duration which is integer multiple of the slot duration. In case RBC exceeds the MAX RBC then transmission failure is declared.

### A DPP terminal shall indicate to its peer the need to acknowledge proper receipt of the PDU. The DPP terminal will set the Ack Indication bit if the transmitted PDU requires acknowledgement, based on the Service Flow (SF) profile associated with the respective SDU SF. At the receiving terminal, if the CRC passes for the burst PDU, then same CRC is sent in the ACK message to the sender DPP terminal indicated successful reception refer Table 8‑6 for ACK message.

## Half Duplex CSMA/CA

Figure 5 shows a flowchart of HD CSMA/CA with the same TX and RX frequency and distinct TX and RX frequencies.

Diagram

Description automatically generated

Figure 5 CSMA/CA flowchart

CSMA/CA has the known problem of hidden nodes hence it is preferred in a scenario characterized by bi-directional traffic flows with gaps. In case only one directional traffic is there then the hidden node who is not detecting the signal might consider the channel is idle and transmit resulting in collision. In case we make sure the concerned receiving node does the transmission this might help in hidden node detecting the signal and considering channel is busy. The bi-directional traffic increases the probability of hidden nodes sensing the channel is busy avoiding further collisions.

To reduce the probability of collisions, an Acknowledgement (ACK) message can be added as a configurable option. Sending of the ACK makes communication bi-directional and can help the hidden node to sense the channel is busy.

In case ACK has not been received, the transmitter must do the random back-off and initiate the channel access procedure again before doing the re-transmission.

## CSMA/CA with RTS, CTS

In addition to CSMA/CA, before transmitting the actual data, the DPP terminal sends a RTS message and waits for a CTS message. RTS and CTS messages are transmitted using the Robust MCS. This helps resolve the hidden node problem. With the CTS response, automatic MCS selection converges faster due to the bidirectional traffic. With RTS/CTS, larger packets can be sent, RTS CTS can be used to inform other listening nodes about the transaction details to avoid further collisions. The below Figure 6 shows the flowchart:

Diagram

Description automatically generated

Figure 6 CSMA/CA RTS CTS flowchart

# DPP Terminal States

## **Offline state**

## Each DPP terminal when turned ON will enter the Offline state by default.

## Configuration happens during this state. Each DPP terminal will have a unique ID (MAC Address).

## Each DPP terminal will have a priori information about its peer DPP terminal. This information includes:

## MAC address and Name

## Private and public key

## When there are two distinct frequencies available the DPP terminal will compare its own MAC ID with the MAC ID of its peer and use the highest frequency for TX and lower frequency for RX in case its MAC ID is higher than the peer DPP terminal’s MAC ID, otherwise it selects lower frequency for TX and higher frequency for RX.

## When the DPP terminal employs AIP mode 2 (TDD), the DPP terminal will use the first TDD subframe to transmit if its MAC ID is higher than its peer and the second TDD subframe to transmit if its MAC ID is lower than its peer. DPP terminals shall switch to an online state based on any trigger like an external command.

## **Online state**

## During this state the DPP terminal starts to transmit periodic ASSOCIATE Request message indicating its own ID and the peer node ID with which it wants to communicate.

## On receiving a response from the other DPP terminal, the DPP terminal enters the Association state.

## **Association state**

## The DPP terminal in this state shall receive and transmit internal control messages (non-traffic) but will not transmit any user data until it reaches the Operational state.

## The DPP terminal will perform the following activities during the association phase:

## Verify the DPP terminal ID of its peer terminal.

## Authenticate its peer terminal.

## Select frequency in the case of paired subchannel group. This is skipped in the case of unpaired subchannel group.

## Select subframe in the case of mode 2 operation. This is skipped in the case of mode 1 operation.

## Automatic PHS configuration

## **Operational state**

## Data exchange between the two DPP terminals

1. Perform continuous link adaptation to adjust MCS and repetitions based on the channel conditions (CINR).
2. Perform continuous receive gain adjustments as needed to bring the CINR to the optimal level.
3. Perform power control to minimize the TX power subject to the performance meeting RSSI criteria.
4. Continuously adjust automatic PHS rules

# DPP link Connectivity Establishment and Maintenance Procedures

## **Identity verification**

### The DPP terminals shall exchange their IDs (MAC address or Name) using ASSOICATE Request/Response/Reject/Ack messages. DPP terminal receiving the ASSOCIATE request message shall match the received MAC ID of the peer DPP terminal and send the ASSOCIATE Response if a match is found. If there is no match the DPP terminal shall send ASSOCIATE Reject message. Shown below in Figure 7, DPP terminal 1 is the transmitter, and it is associating with DPP terminal 2 the receiver. Similarly, DPP terminal 2 shall associate with DPP terminal 1 for its transmission.

Timeline

Description automatically generated

Figure 7 Association message flow

## **Link Adaptation (LA)**

### Link adaptation is the process of dynamic selection for transmission of the highest MCS and repetition rate subject to the CINR at the peer terminal receiver.

### A DPP terminal shall begin the transmission with the Robust MCS. Each DPP terminal shall send an unsolicited measurement report to its peer DPP terminal during the association phase and whenever there is a significant change in measurements (when the MCS needs to be changed).

### The report shall indicate the time frame of data for which the measurement was taken.

### After receiving the measurement report LA hold timer shall be started/restarted and the MCS as per the report shall be used till the timer expiry.

### In case LA hold timer expires then the DPP terminal shall use the Robust MCS for transmission.

### The measurement report structure is described in section 8.1.6. Figure 8 shows the flow of LA procedure.

Chart, diagram

Description automatically generated

Figure 8 LA Procedure

### :

## **Power Control**

### Power control is an optional DPP procedure. A DPP terminal may be configured for fixed TX power (typically Max TX power) and the Automatic Gain Control (AGC) at the peer DPP terminal, adjusts its gain to optimize it CINR.

### The objective of the power control is to minimize self-interference by reduction in TX power as much as possible subject to CINR and/or RSSI criteria at the peer DPP terminal. The criteria is vendor specific. Receiving DPP terminal sends the measurement report which includes the RSSI, transmitting terminal can use this RSSI measurement to compare it with the target RSSI and do the delta power correction in the next transmission.

### The measurement report structure is defined in section 8.1.6 .

## **Authentication**

### Authentication and Key management

## Each DPP terminal in the network will include a unique private / public RSA key pair.

## Each DPP terminal will be pre-configured with its peer MAC address and the peer’s public RSA key.

## Each DPP terminal will have a X.509 certificate which shall include the following fields:

|  |  |
| --- | --- |
| Field | Content |
| MAC address | The node’s owned MAC address |
| Manufacturer | A string indicating the node’s manufacture (e.g., “Ondas Inc.) |
| Owner | A string indicating the node’s owner (e.g., “railroad A”) |

Table 7‑1: Required X.509 attributes.

### Each node shall authenticate the other node independently.

### Key management shall employ two MAC message types: PKM-REQ and PKM-RSP, as per section 6.3.2.3.9 in 802.16-2017 and with the format listed in table 6-66 and table 6-67 there. Attributes of the different messages shall be TLV encoded as per these tables.

### The keying materials (AK, KEK, TEK) shall be directional. The sending node of each direction shall be the generator of the AK from which a KEK and message authentication keys are derived. Pre-PAK generation is per section 7.2.2.2.1 of 802.16-2017. AK derivation is per section 7.2.2.2.3 of 802.16-2017. KEK derivation is per section 7.2.2.2.4 of 802.16-2017 and TEK is per section 7.2.2.2.6 of 802.16-2017.

### A DPP terminal (terminal 1), after identifying its peer (DPP terminal 2), will send a PKMv2 RSA-Request to terminal 2 to request RSA authentication.

### Upon receiving a PKMv`2 RSA-Request, terminal 2 will authenticate terminal 1 by using terminal 1 public RSA key. If authenticated, terminal 2 will reply to the sending terminal with a PKMv2 RSA-Reply message.

1. The message includes a pre-primary authorization key (Encrypted pre-Pak). The pre-Pak shall be encrypted with terminal 1 public key.
2. The pre-PAK shall be encrypted with terminal 1 public key. The received Random number is returned from the PKMv2 RSA-Request message, along with a random number supplied by the sending terminal, thus enabling assurance of key liveness.
3. The primary authorization key will be used to generate keys to encrypt all traffic from terminal 2 to terminal 1.

### A DPP terminal shall authentication it’s peer terminal identity by:

## Verifying the peer terminal RSA Sig.

## Comparing the pre-configured peer MAC address in the X.509 with the sender MAC address

## Validating the Manufacture and the Owner strings in the X.509 certificate

### Upon receiving a PKMv2 RSA-Request, if the receiving terminal (terminal 2) fails to authenticate the sending terminal (terminal 1), the receiving terminal (terminal 2) will reply to the sending terminal with a PKMv2 RSA-Reject message.

Comments:

* 1. The Error-Code and Display-String attributes describe to the requesting terminal 1 the reason for the RSA-based authorization failure.
  2. The Sig attribute indicates a RSA signature over all the other attributes in this message, and the terminal 2 private key is used to make a RSA signature

### Terminal 1 sends a PKMv2 RSA-Acknowledgment message in response to a PKMv2 RSA-Reply message. Only if the value of the Auth Result Code attribute is failure, then the Error-Code and Display-String attributes can be included in this message.

Comments:

1. The Sig attribute in a PKMv2 RSA-Acknowledgment indicates a RSA signature over all the other attributes in this message, and terminal 1 private key is used to make a RSA signature.
2. After achieving initial authorization, each DPP terminal periodically seeks reauthorization with its peer terminal; reauthorization is initiated for each direction by the receiving terminal. The directional authorization and reauthorization is managed by the terminal’s PKMv2 Authorization state machine. A DPP terminal shall maintain its authorization status with the other terminal to be able to refresh aging TEKs.
3. Reauthentication period shall be a configurable parameter (typically, 24 hours).
4. TEK state machines manage the refreshing of TEKs as per section 7.2.2.9 of 802.16-2017.

### PKMv2 Messages shall be as in tables 6-80, 6-81, 6-82 and 6-83 of 802.16-2017. In PKMv2 RSA-Request and PKMv2 RSA-Acknowledgement messages, attributes related to MS shall be populated with the sending terminal attributes, and attributes related to BS shall be populated with the receiving terminal attributes. In PKMv2 RSA-Reply and PKMv2 RSA-Reject, attributes related to BS shall be populated with the sending terminal attributes, and attributes related to MS shall be populated with the receiving terminal attributes.

## **Automatic Packet Header Suppression**

### A repetitive portion of the data in the packet is suppressed by the sender and restored by the receiver depending on known rules called PHS rules. PHS rules help in reconstructing the packet correctly at the receiving end.

### PHS parameters include PHS depth, PHS field, PHS mask and PHS index.

### PHS rules shall be automatically created by any of the nodes and the rules specify the field values that can be suppressed. Multiple values for the same field will be supported.

### Nodes shall learn the traffic and will trigger new rule when any repetitive field values in the traffic is observed.

### PHS suppression will be applied after creation of rule, until then the traffic will go unsuppressed.

### PHS index will be prefixed to PDU data and the PDU header will indicate when PHS is applied.

### Each PHS rule will be identified using PHS index (PHSI).

Diagram

Description automatically generated

Figure 6 PHS Creation Flow

### Automatic PHS related messages are described in section 8.1.7.

# Message formats

### Association Messages

|  |  |  |
| --- | --- | --- |
| Syntax | Size(bit) | Notes |
| ASSOCIATE Request () { | --- | ---- |
| Message Type | 8 | Value: 1 |
| Initiator Terminal ID | 48 | MAC address of initiating Terminal |
| Receptor Terminal ID | 48 | MAC address of partner terminal |
| } |  |  |

Table 8‑1 Associate Request

|  |  |  |
| --- | --- | --- |
| Syntax | Size(bit) | Notes |
| ASSOCIATE \_Response () { | --- | ---- |
| Message Type | 8 | Value: 2 |
| Response | 8 | 0: Reject 1 : Accept |
| } |  |  |

Table 8‑2 Associate Response

### RTS

1. Message includes type, Sender ID, Receiver ID, sequence number and Length of data in bytes.
2. Each node shall maintain a sequence number which will be incremented after every transmission.

|  |  |  |
| --- | --- | --- |
| Syntax | Size(bit) | Notes |
| Ready To Send () { | --- | ---- |
| Message Type | 8 | Value: 3 |
| Sender ID | 48 |  |
| Receiver ID | 48 |  |
| Sequence number | 8 | Transmission sequence number |
| Length of Data | 32 | Length of data waiting to be transmitted in bytes |
| } |  |  |

Table 8‑3 : RTS message

### CTS

Message includes type, Sender ID, Receiver ID, sequence number, MCS, expected duration of transmission in slots based on MCS, Received CINR and RSSI

|  |  |  |
| --- | --- | --- |
| Syntax | Size(bit) | Notes |
| Clear To Send () { | --- | ---- |
| Message Type | 8 | Value: 4 |
| Sender ID | 48 |  |
| Receiver ID | 48 |  |
| Sequence number | 8 | Transmission sequence number |
| MCS | 8 |  |
| Duration | 16 | Transmission duration in slots |
| CINR | 8 | Measured on received data |
| RSSI | 16 | Measured on received data |
| } |  |  |
|  |  |  |

Table 8‑4 : CTS message

### CTRL MSG

|  |  |  |
| --- | --- | --- |
| Syntax | Size(bit) | Notes |
| Control message () { | --- | ---- |
| Message Type | 8 | Value: 5 |
| Sender ID | 48 |  |
| Receiver ID | 48 |  |
| MCS | 8 | MCS includes the Repetition. |
| Length of Data | 32 |  |
| CINR | 8 | Measured on received data |
| RSSI | 16 | Measured on received data |
| } |  |  |
|  |  |  |

Table 8‑5 : CTRL Message

### ACK

|  |  |  |
| --- | --- | --- |
| Syntax | Size(bit) | Notes |
| Acknowledgement message () { | --- | ---- |
| Message Type | 8 | Value: 6 |
| Acknowledgement | 32 | Burst PDU CRC received for transmission is sent as ACK if the CRC passes. |
| } |  |  |

Table 8‑6 : ACK message

### Measurement Report

|  |  |  |
| --- | --- | --- |
| Syntax | Size(bit) | Notes |
| Measurement\_report () { | --- | ---- |
| Message Type |  | Value: 7 |
| Sender ID | 48 |  |
| Receiver ID | 48 | MAC address |
| Sequence number | 8 | Measurement report corresponding to the sequence number of the received data burst. |
| CINR | 8 | Averaged CINR measurement report |
| RSSI | 16 | Averaged RSSI measurement report |
| MCS | 8 | MCS includes the Repetition. |
| } |  |  |
|  |  |  |

Table 8‑7 : Measurement report

### Automatic PHS messages

|  |  |  |
| --- | --- | --- |
| Syntax | Size(bit) | Notes |
| PHS Request () { | --- | ---- |
| Message Type | 8 | Value: 8 |
| PHSI | 8 | Identifies the PHS rule |
| PHS size | 8 | Size of the PHS Field |
| PHS Mask | 48 | Bitmask that determines which bytes of the PHSF that needs to be suppressed |
| PHS Field | variable | Field values |
| } |  |  |

Table 8‑8 PHS Request

|  |  |  |
| --- | --- | --- |
| Syntax | Size(bit) | Notes |
| PHS Response () { | --- | ---- |
| Message Type | 8 | Value: 9 |
| Response | 8 | 0: Reject 1 : Accept |
| } |  |  |

Table 8‑9 PHS Response

|  |  |  |
| --- | --- | --- |
| Syntax | Size(bit) | Notes |
| PHS\_Ack () { | --- | ---- |
| Message Type | 8 | Value: 10 |
| } |  |  |

Table 8‑10 PHS ACK