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

April 18th, 2023

# Content

[1 Content 2](#_Toc132660676)

[2 Definitions and Terms 3](#_Toc132660677)

[3 General 5](#_Toc132660678)

[4 DPP Air Interface Protocol (AIP) 6](#_Toc132660679)

[5 Channel Access in HD with CSMA/CA 9](#_Toc132660680)

[6 DPP Terminal States 14](#_Toc132660681)

[7 DPP link Connectivity Establishment and Maintenance Procedures 16](#_Toc132660682)

[8 Messages format 22](#_Toc132660683)

# Definitions and Terms

## **Direct Peer-to-Peer (DPP)**: Direct link between two terminals with no Base Station infrastructure in between nor required for operation.

## **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.

## **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.

## **MAX RBC:** Maximum Random Backoff Count, a configuration parameter used to declare the transmission failure once the random backoff count exceeds the configured value.

## **MAX CO:** Maximum Channel Occupancy, a configuration parameter defining the maximum duration of the burst in terms of the slots.

## **LA Hold Timer:** Link Adaptation hold timer is a timer which starts/restarts once the measurement report is received and resets once maximum duration time is reached which is configured in terms of seconds between 1 to 60 seconds.

# General

## This document presents the ieee802.16t Direct Peer to Peer (DPP) communication between two DPP terminals, which is peer to peer operation without the use of 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 HD mode with no strict framing using a CSMA/CA access mechanism. A DPP terminal shall 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.

## 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.

## Each DPP 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 4.6. 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 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 the beginning of the burst 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. The maximum number of PDUs in a burst shall not exceed 16.



Figure 1 OTA burst structure

## OTA Burst structure:

1. **Gain Adjustment Period**: the transmitter shall transmit one slot worth of 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 a Gold sequence of length 63 as described 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 be transmitted using the robust MCS. Table 3 describes the CTRL MSG structure. The control message type field is used to identify whether the CTRL MSG is used to convey information about PDUs which follow the CTRL MSG in the burst or is used to indicate an RTS, CTS or Ack message. ACK indication is set based on the presence of any PDU which needs an ACK. This indication shall be used by non-intended receiver for ACK based deferral.
4. **PDU**: The PDUs shall be transmitted in accordance with 802.16t PHY specification document, section “*3.8* *Uplink transmitter” except the Ranging section.*

The total duration of the burst shall not exceed the value of the configurable Maximal Channel Occupancy. This parameter will be specified in slots.

## PDU structure

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



Figure 2 PDU Structure

1. The PDU header is shown in Figure 3 and described in Table 1.

 

Figure 3 PDU Header Structure

|  |  |  |
| --- | --- | --- |
| 1. Syntax
 | Size(bit) | Notes |
| PDU header () { | --- | ---- |
| Header Type | 1 | 0 : Management PDU 1:Data PDU |
| Encryption indication | 1 | 0: Off 1:On |
| PHS indication | 1 | 0: Off 1: On |
| Sub Header indication  | 1 | 0:Absent 1:Present |
| ACKI | 1 | 0: Off 1: ACK to be sent. |
| Length | 11 | 0 to 2047 Length in bytes of the PDU including the header and the 4-Byte CRC. |
| If (PHS indication == 1) PHS index   | 8 | If PHS Indication is set to 0, PHS is turned off and there is no PHS index. |
| HCS  | 8 | CRC for the above 3 bytes |
| } |  |  |

Table 1 : PDU Header fields

1. The PDU header shall contain the following fields:
2. The Header Type indicates two types of PDU:
3. The value 0 indicates it is a Management PDU used to carry management messages mentioned below,
4. Association Messages, refer Table 4 and Table 5
5. Measurement Report, refer Table 6
6. Automatic PHS, refer Table 7 and Table 8
7. The value 1 indicates it is Data PDU
8. An encryption indication. The value 0 indicates the data is not encrypted. The value 1 indicates the data is encrypted.
9. A PHS indication. The value 0 indicates PHS is disabled and the value 1 indicates PHS is enabled.
10. SDUs mapped to the same service flow shall be packed in the single PDU as these will have same PHS index value and ACK requirements. This is subject to the value of the Maximum Channel Occupancy.
11. A Sub Header indication. The value 0 indicates there are no sub-headers present and 1 indicates there are sub-headers present. Sub-header is present at the start of the SDU, Sub-headers describe the SDUs with either packing or fragmentation. The sub-headers format is described in Table 2.

|  |  |  |
| --- | --- | --- |
| 1. Syntax
 | Size(bit) | Notes |
| Sub header () { | --- | ---- |
| Sub header Type | 1 | 0 : Packing 1:Fragmentation |
| Fragmentation state | 2 | Indicates the fragmentation state of the payload:00 = No fragmentation01 = Last fragment10 = First fragment11 = Continuing (middle) fragment |
| FSN | 2 | Sequence number of the current SDU fragment. The value shall increment by one (modulo 4) for each fragment. |
| If (Sub Header Type == 1) { |  |  |
| Reserved | 3 |  |
| } else { |  |  |
| Length  | 11 | 0 to 2047 Length in bytes of the SDU including the Sub header. |
| } |  |  |
| } |  |  |

Table 2 Sub Header

1. ACK indication field (ACKI). The value 0 indicates ACK is not needed for the PDU. The value 1 indicates ACK is needed.
2. A PDU length filed. The value can be from 0 to 2047 in bytes.
3. A PHS index field. If the PHS indication is 1 this field indicates the PHS index. Otherwise, it is 0.
4. The HCS is computed the same manner as described in Table 6-3 of 802.16-2017.
5. One or more SDUs can be encapsulated in one PDU. For example, if a node is waiting for transmission and packets get queued, the packets can be concatenated into single PDU and transmitted, provided it is within tolerable latency.
6. The 4 byte PDU CRC is computed in the same manner as described in 802.16 section 6.3.3.5 CRC calculation.

# Channel Access in 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, the same as is done in the ieee802.16t Point to Multipoint AIP.

### A Maximal Channel Occupancy 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 Channel Occupancy.

### The Random Backoff Count (RBC) is set to zero before the beginning of each transmission attempt. The RSSI threshold is used to compare the measured RSSI with a threshold and the channel is accessed if the measured RSSI is less than the threshold. In case the channel is busy as indicated by the measured RSSI being greater than the threshold, the RBC count is incremented, and the random back-off duration is selected based on the integer random function output with the range of values between one to MAX CO in slots. In case the RBC exceeds the MAX RBC then it is a transmission failure, how it is indicated to an operator is vendor specific.

### A DPP terminal shall indicate to its peer the need to acknowledge proper receipt of one or more PDUs in the burst as shown in Table 1. The DPP terminal will set the Ack Indication bit to 1 in the CTRL MSG (refer to Table 3 for CTRL MSG) if the transmitted burst requires any of the PDUs to be acknowledged, At the receiving terminal, if the CRC passes for the PDU, then a CTRL MSG with type ACK (value 3) along with the ACK bit map indicating the order of the PDU and corresponding bit set if CRC is passed else set to zero is sent to the sender DPP terminal. The terminal waiting for the ACK message shall wait for a configurable duration (this should equal the maximum round trip delay) before retransmitting the PDU (if no ACK is received).

## Half Duplex CSMA/CA

### This paragraph describes the behavior of DPP terminals using HD CSMA/CA with the same TX and RX frequency as well as the case in which distinct TX and RX frequencies are used.

### Figure 4 shows a flowchart for the behavior of the DPP terminal initiating the transmission.

 

Figure 4 CSMA/CA flowchart for transmitting radio

### Intended receiver behavior

1. The intended receiver will identify its MAC address in the incoming CTRL MSG.
2. The intended receiver will decode the CTRL MSG based on the MCS received within the CTRL MSG.
3. If ACK is required, the intended receiver terminal will perform CSMA/CA procedure to send the ACK. The ACK message is transmitted using the Robust MCS.

### Non-Intended Receiver behavior

When a non-intended receiver does not identify its MAC address in the incoming message, it discards the message. If an ACK is required based on Ack indication in the incoming CTRL MSG , it will not access the channel for an ACK deferral in slots.

## CSMA/CA with RTS, CTS

### The CSMA/CA mechanism has the known problem of hidden nodes. This is addressed by the exchange of RTS and CTS Messages between the two DPP terminals.

### The modified access procedure described in this paragraph includes an RTS message transmitted by the initiating terminal and a CTS response by the intended receiver. RTS and CTS are short messages that precede the data transmission. The initiating node specifies within the RTS message the number of slots to be transmitted and the MCS. The intended receiver specifies within the CTS message number of slots and the MCS to be used which is based on the measured CINR. Refer Table 1 for RTS/CTS message details.

### The behavior of the initiating terminal is shown in Figure 5.

### Intended Receiver behavior:

1. The intended receiver shall detect its MAC address in CTRL MSG as described in Table 3.
2. The intended receiver shall convert the requested number of slots along with MCS into the number of slots that shall be allocated based MCS which is decided based on the measured CINR, plus the additional slots required to transmit the other header and CTRL MSG in robust MCS. The number of slots is transmitted along with the MCS within the CTS message which is described in the Table 3.
3. The intended receiver shall transmit the CTS message and defer transmission for CTS deferral.
4. The intended receiver shall decode the message when received and send an ACK if indicated in the CTRL MSG. ACK message is sent using the robust MCS.

### Non-Intended Receiver behavior

1. The non intended receiver is a receiver which does not recognize its MAC address in any of the messages.
2. If the received CTRL MSG indicates RTS, the non-intended receiver shall avoid transmission within the RTS deferral duration.
3. If the received CTRL MSG indicates CTS, the non-intended receiver shall avoid transmission within the CTS deferral duration.
4. If CTRL MSG is received with ACK indication, then non intended receiver will avoid transmission within the ACK deferral duration.

### Deferrals

1. RTS deferral: When the non-intended receiver sees the CTRL MSG with the RTS it shall compute the deferral time using the number of slots requested plus the CTRL MSG, gain adjustment, synchronization signal, and maximum round trip duration.
2. CTS deferral: When the non-intended receiver sees the CTRL MSG with the CTS it shall compute the deferral time using the number of slots allocated plus the CTRL MSG, gain adjustment, synchronization signal, and maximum round trip duration.
3. ACK deferral: When the non-intended receiver sees the CTRL MSG with the ACK indication ON, it shall compute the deferral time using the number of slots allocated plus twice the duration of CTRL MSG, gain adjustment, synchronization signal, and maximum round trip duration.

 

Figure 5 CSMA/CA RTS CTS flowchart for transmitting radio

# DPP Terminal States

## **Offline state**

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

## Each DPP terminal will have a unique MAC Address, public/private key pair and a X509 certificate that binds the MAC address to the private key and a Name. This is configured during production.

## The DPP Terminal will be configured with various operational parameters including frequency (one or two frequencies), channel parameters (including subchannel bandwidth, subchannel bitmap and subchannel group), Service Flows with their QOS profiles, Name and specific DPP parameters as described in this document.

## Each DPP terminal will be configured with parameters of its peer DPP terminal. This information includes:

## MAC address and Name.

## 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.

## DPP terminals shall switch to an online state based on any trigger like an external command.

## **Online state**

## The DPP terminal transitions to the online state following a manual operation (an external hardware trigger like push button or a software command).

## During this state the DPP terminal starts to transmit periodic ASSOCIATE Request messages indicating its own unique MAC address or Name. This DPP terminal is referred to as terminal 1.

## **Association state**

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

## Verify the DPP terminal ID of its peer terminal as described in section 7.1.

## Authenticate its peer terminal as described in section 0.

## Automatic PHS configuration as described in section 7.3.

## 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.

## **Operational state**

## The DPP terminal shall enter the operational state automatically, following the completion of the Association process.

## The DPP terminal shall perform the following activities during the operational state:

## Data exchange with the peer DPP terminals

## Perform continuous link adaptation to adjust MCS and repetitions based on the on CINR at the peer DPP terminal. Link Adaptation is performed in each direction independent of the other direction. Refer to section 7.4 for link adaptation process description.

## Perform continuous receive gain adjustments as needed to attempt to bring the CINR to the optimal level.

## Perform power control to minimize the TX power subject to the performance meeting RSSI criteria. Refer to section 7.5 for power control process description.

## Continuously adjust automatic PHS rules. Refer to section 7.3 for the automatic PHS process description.

# 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. The 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 not respond to the ASSOCIATE request message. The identity verification process is shown in Figure 6 below.



Figure Association message flow

## **Authentication**

### Authentication and Key management

1. Each DPP terminal in the network shall include a unique private / public RSA key pair.
2. Each DPP terminal shall be pre-configured with its peer MAC address and the peer’s public RSA key.
3. Each DPP terminal shall have a X.509 certificate that shall include the fields defined in 802.16-2017, section 7.3.

### Each DPP terminal shall authenticate its peer terminal 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 of that document. Attributes of the different messages shall be TLV encoded as per these tables.

### The keying materials (AK, KEK, TEK) shall be directional. The sending terminal 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.

### After receiving an ASSOCIATE Response message, the receiving node will send a PKMv2 RSA-Request to terminal 2 to request RSA authentication.

### Upon receiving a PKMv2 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 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’s identity by:

1. Verifying the peer terminal RSA Signature.
2. Comparing the pre-configured peer MAC address in the X.509 with the sender’s MAC address
3. 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 Signature attribute indicates a RSA signature over all the other attributes in this message, and the terminal 2 private key is used to create an 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 Signature attribute in a PKMv2 RSA-Acknowledgment indicates a RSA signature over all the other attributes in this message, and terminal 1’s private key is used to create an RSA signature.
2. After achieving initial authorization, each DPP terminal shall comply with PKMv2 requirements as per section 7.2.2 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 an MS shall be populated with the sending terminal attributes, and attributes related to a BS shall be populated with the receiving terminal attributes. In PKMv2 RSA-Reply and PKMv2 RSA-Reject, attributes related to a BS shall be populated with the sending terminal attributes, and attributes related to an 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 a new rule when any repetitive field value 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).



Figure 6 PHS Creation Flow

### Automatic PHS related messages are described in section 8.1.4.

## **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 message 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 sequence number of the burst for which the measurement was taken.

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

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

### The measurement report structure is described in section 8.1.3. Figure 7 shows the flow of LA procedure.



Figure 7 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 attempt to optimize it’s 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. The receiving DPP terminal sends the measurement report which includes the RSSI, so that the 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 8.1.3 .

# Messages format

### CTRL MSG

|  |  |  |
| --- | --- | --- |
|  Syntax | Size(bit) | Notes |
| Control message () { | --- | ---- |
| Control message Type | 3 | This field indicates the type of CTRL MSG based on what description it is carrying.Value 0: PDU,  1: RTS 2: CTS 3: ACK |
| Sender ID | 48 | MAC address |
| Receiver ID  | 48 | MAC address |
| If (control message Type == 3) { |  |  |
| ACK Bit Map | 16 | LSB for first PDU and MSB for last. Bit value 1 indicates ACK. Max PDUs in burst shall not exceed 16. |
| Reserved | 13 |  |
| } else { |  |  |
| MCS | 4 | MCS includes the Repetition. |
| ACKI | 1 | ACK Indication. 0: disabled, 1: enabled |
| Number of slots | 12 | Number of slots requested (for RTS) or allocated (for CTS/PDU) post CTRL MSG. |
| Reserved | 4 |  |
| Sequence number | 7 | Transmission sequence number |
| AUTHI | 1 | Authentication. 0: Disabled 1: Valid CMAC/HMAC is present. |
| } |  |  |
| CRC | 8 | CRC for above bytes computed 802.16 section 6.3.3.5 CRC calculation |
| CMAC/HMAC Digest | 128 | Message integrity code of the message. Must be last field in the message. If AUTHI is 0 then this field is not transmitted, when AUTHI is set to 1 this will be present after the CRC. |
|  } |  |  |

Table 3 : CTRL Message

### 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 4 Associate Request

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

Table 5 Associate Response

### Measurement Report

|  |  |  |
| --- | --- | --- |
| Syntax | Size(bit) | Notes |
| Measurement\_report () { | --- | ---- |
| Message Type | 8 | Value: 3 |
|  CINR | 8 | Averaged CINR measurement report |
|  RSSI | 16 | Averaged RSSI measurement report |
| MCS | 8 | MCS includes the Repetition. |
|  } |  |  |
|  |  |  |

Table 6 : Measurement report

### Automatic PHS messages

|  |  |  |
| --- | --- | --- |
| Syntax | Size(bit) | Notes |
| PHS Request () { | --- | ---- |
| Message Type | 8 | Value: 4 |
| 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 7 PHS Request

|  |  |  |
| --- | --- | --- |
| Syntax | Size(bit) | Notes |
| PHS Response () { | --- | ---- |
| Message Type | 8 | Value: 5 |
| Response | 8 | 0: Reject 1 : Accept |
|  } |  |  |

Table 8 PHS Response

|  |  |  |
| --- | --- | --- |
| Syntax | Size(bit) | Notes |
| PHS\_Ack () { | --- | ---- |
| Message Type | 8 | Value: 6 |
|  } |  |  |

Table 9 PHS ACK