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

May 17th, 2023

# Content

[1 Content 2](#_Toc135075250)

[2 Definitions and Terms 3](#_Toc135075251)

[3 General 5](#_Toc135075252)

[4 DPP Air Interface Protocol (AIP) 6](#_Toc135075253)

[5 Channel Access 11](#_Toc135075254)

[6 DPP SS States 17](#_Toc135075255)

[7 DPP link Connectivity Establishment and Maintenance Procedures 19](#_Toc135075256)

[8 Relay Station 26](#_Toc135075257)

[9 Messages format 27](#_Toc135075258)

# Definitions and Terms

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

**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 SS which AIRs can use for transmission.

**CTS**: Clear to Send

**CTS Deferral:** A period after CTS reception in which a non-intended receiver willnot access the channel.

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

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

**DPP SS**: Each of the two SSs of the DPP link.

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

**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.

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

**Link Adaptation (LA):** A process by which a DPP SS is notified by its peer DPP SS, what MCS it can use for transmission.

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

**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 number of slots.

**Non-Intended Receiver:** Any DPP SS other than the intended DPP SS receiver as identified by the destination Ethernet address in the burst.

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

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

**Random Back-Off Duration:** A duration in which a DPP SS avoids channel access following an access attempt in which the channel was busy. The backoff is random so that if multiple DPP SSs are trying to access the channel at the same time, the probability of collision next time is minimized.

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

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

**RSSI Threshold:** The measured RSSI is compared with the configurable RSSI Threshold parameter for use by the CSMA mechanism to determine whether or not the channel is in use.

**RTS**: Request to Send

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

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

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

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

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

# General (DPP Should be a new clause 9 at same level as PHY

**this section General would be 9.1, and so on.**

## This document presents the Direct Peer-to-Peer (DPP) communication between two DPP SSs, which is peer-to-peer operation without the use of base station infrastructure. A Relay Station, however, may be used in DPP mode for range extension. The two DPP SSs of a DPP link are peers (i.e., there is 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 SSs 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 SS shall only transmit when needed. The CSMA/CA mechanism is used to resolve contention between the two DPP SSs of the DPP link and resolve possible contention with DPP SSs of other in-range DPP links.

## An DPP SS employs the same PHY layer for transmit and receive. The PHY layer is identical to the uplink of the WirelessMAN-NB PHY

## Each DPP SS employs CSMA/CA before the start of a transmission. In this mode, a DPP link may interfere with a nearby ieee802.16 PtMP system if operated on the same frequency. Moreover, if operated on the same frequency, the DPP SSs 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 whenever it is in range of a PtMP ieee802.16 system.

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

## The 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 SS 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 SS may automatically establish Packet Header Suppression (PHS) rules with its peer.

# DPP Air Interface Protocol (AIP) (9.2)

## The DPP SS shall generate 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 directions. The waveform is as described in the WirelessMAN-NB PHY specification section “8.6.8 Uplink”. The Control Message and the Data PDUs waveform generation follows the procedure described in the WirelessMAN-NB 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 if more than one subchannel is used (aggregated) between a pair of radios for DPP operation.

## 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.

Table

Description automatically generated

Figure 1. Burst structure

## Burst Structure:

### **Gain Adjustment Period**: The DPP SS shall begin each burst by transmitting one slot worth of alternate 1’s and 0’s as a BPSK modulated signal for a receiver to adjust the gain.

### **Synchronization:** Following the Gain Adjustment Period,the DPP SS shall transmit a preamble to be used as a synchronization signal carrying a Gold sequence of length 63 as described in WirelessMAN-NB PHY specification document, refer to the section “*8.6.7 Downlink Preamble Transmission”.*

### **Control Message:** The DPP SS shall transmit a control message (CTRL MSG) using the robust MCS. Table 4 describes the CTRL MSG structure. The control message type field shall indicate whether the CTRL MSG is used to convey information about PDUs that follow the CTRL MSG in the burst or is used to indicate an RTS, CTS, or Ack message. An ACK indication is set based on the presence of any PDU which needs an ACK. A non-intended receiver shall use the ACK indication for ACK-based deferral.

### **PDU**: The DPP SS shall transmit PDUs 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 terms of a number of slots.

## PDU structure

1. The PDU shall begin with 4 bytes of header followed by a variable length payload and a 4-byte CRC as shown in Figure 2.

Diagram

Description automatically generated

Figure 2. PDU Structure

1. The PDU header shall be as shown in Figure 3 and described in Table 1.

A picture containing box and whisker chart

Description automatically generated

Figure 3. PDU Header Structure

|  |  |  |
| --- | --- | --- |
| 1. Syntax | Size(bits) | 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 |
| ACK Indication | 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 DPP SS shall include the following fields in the header of each PDU it transmits:
2. A Header Type, indicating the type of the PDU:
3. The value 0 indicates it is a Management PDU used to carry management messages mentioned below,
4. Association Messages, refer to Table 5 and Table 6
5. Measurement Report, refer to Table 7
6. Automatic PHS, refer to Table 8 and Table 9
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 a single PDU, SDU sub header type shall indicate the packing, subject to the limit of the Maximum Channel Occupancy, as these will have the same PHS index value and ACK requirements. If the number of SDUs exceeds the limit of the Maximum Channel Occupancy, the remaining SDUs shall be sent in the next burst. If the SDU needs to be fragmented, the SDU sub header type shall indicate fragmentation. Refer to Table 2 for the sub header details.
11. A Sub-Header indication. The value 0 indicates there are no sub-headers and 1 indicates there are sub-headers present within the PDU. The sub-header is present immediately after the PDU header and then onwards at the beginning of the next SDU. Withing the sub-header, sub-header type field describes the SDUs as either packed i.e., value 0, or fragmented i.e., value 1. The sub-header format is described in Table 2.

|  |  |  |
| --- | --- | --- |
| 1. Syntax | Size(bits) | Notes |
| Sub header () { | --- | ---- |
| Sub header Type | 1 | 0: Packing 1: Fragmentation |
| Fragmentation state | 2 | Indicates the fragmentation state of the payload:  00 = No fragmentation  01 = Last fragment  10 = First fragment  11 = 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 format

1. ACK Indication field (ACKI). The value 0 indicates that an ACK is not needed for the PDU. The value 1 indicates that an ACK is needed.
2. A PDU length field. The value can be from 0 to 2047 referring to the number of bytes comprising the PDU.
3. A PHS index field. If the PHS indication is 1 this field indicates the PHS index. Otherwise, it is 0. Refer to section 7.3 for PHS related details.
4. The HCS is computed in 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 a transmission opportunity and packets to be transmitted get queued, the packets can be concatenated into single PDU and transmitted, provided it is to be transmitted 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

## General

### The following configurable channel/sub-channel access schemes shall be supported by the DPP SS:

## Half Duplex non-persistent CSMA with the same frequency used in both directions.

## Half Duplex non-persistent CSMA with a distinct frequency used in each direction. In this case, sensing is done on both transmit and receive frequencies.

## In addition to the above, the channel access procedure can be configured to use Request to Send (RTS) and Clear to Send (CTS) messages.

### The DPP SS shall support the division of a channel dedicated to DPP service into sub-channels, the same as is done in the WirelessMAN-NB PHY.

### A configurable Maximum Channel Occupancy (MAX CO) parameter in the DPP SS shall limit each burst to an integer multiple of the slot duration. This parameter will be configured by the user based on the application/deployment scenario. This feature helps to avoid excessive usage of the channel by one DPP SS.

### When the DPP SS has data to transmit and the channel is free, it shall compute the total duration of the burst in slots, based on the length of the SDUs in the buffer and the MCS, if the duration is less than the Maximum Channel Occupancy parameter then all available SDUs shall be sent immediately in the same burst else when duration exceeds, then remaining SDUs will be sent in next burst. If needed, fragmentation may be used such that the burst duration does not exceed the configured Maximum Channel Occupancy parameter.

### Higher priority SDUs shall be transmitted first while the lower priority SDUs may be left in the queue and transmitted in the next burst., SDUs shall be discarded when their TTL expire.

### The DPP SS shall set the Random Backoff Count (RBC) to zero before the beginning of each transmission attempt. The RSSI threshold shall be used to compare the measured RSSI with the 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 shall be incremented, and a Random Back-Off Duration shall be selected based on the integer random function output with the range of values between one to MAX CO in terms of slots. After waiting for the Random Back-Off Duration, the DPP SS shall repeat the process of channel sensing and transmit if channel is free or incrementing the RBC count and do the Random Back-Off as mentioned above. In case the RBC exceeds the MAX RBC then it shall be considered as a transmission failure. A vendor specific failure indication will be provided to the operator.

### The DPP SS 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 SS shall set the Ack Indication bit to 1 in the CTRL MSG (refer to Table 4 for CTRL MSG) if the transmitted burst requires any of the PDUs to be acknowledged.

### Upon receiving a PDU, if the CRC check passes successfully for this PDU, the receiving DPP SS shall transmit a CTRL MSG to the sender DPP SS with type ACK (value 3) along with the ACK bit map indicating the order of the PDU and corresponding bit set.

### Upon receiving a PDU, if the CRC check for the PDU does not pass successfully, the receiving SS shall transmit a CTRL MSG to the sender DPP SS with type ACK (value 3) along with the ACK bit map indicating the order of the PDU and corresponding bit set to zero. The sending SS shall wait for the ACK message for a configurable duration (this should equal the maximum round trip delay) before retransmitting the PDU if no ACK is received.

## Half Duplex CSMA

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

### The DPP SS shall conform with the flowchart behavior shown in Figure 4 when initiating a transmission.

Diagram

Description automatically generated

Figure 4. CSMA flowchart for transmitting radio

### Intended receiver behavior

1. The DPP SS shall determine that it is the intended receiver if it identifies its MAC address in an incoming CTRL MSG.
2. The intended DPP receive SS shall decode the PDUs based on the MCS identified within the CTRL MSG.
3. If an ACK is required, the intended DPP receive SS shall perform the CSMA procedure to send the ACK. The DPP receive SS shall transmit ACK messages using Robust MCS.

### Non-Intended Receiver behavior

The DPP SS shall determine that it is a non-intended receiver if it does not identify its MAC address in the incoming message. The DPP SS shall discard a message for which it is a non-intended receiver. If an ACK is required based on an ACK indication in the incoming CTRL MSG, a non-intended receiver shall avoid transmission within the ACK Deferral duration as defined in 5.4.3.

## CSMA/CA with RTS, CTS

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

### The access procedure described in this paragraph includes an RTS message transmitted by the DPP SS with SDU(s) queued to transmit, referred to as the “initiating SS”, and a CTS response by the intended receiver. RTS and CTS are short messages that precede the data transmission. Upon having one or more SDUs queued to send and CSMA-sensing that the channel is clear, the DPP SS shall transmit an RTS message that specifies the requested number of bytes including the PDU and SDU overheads. The intended receiver specifies within the CTS message the allocated number of slots to be transmitted and the MCS to be used which is based on the measured CINR. Refer Table 4 for RTS/CTS message details.

### The initiating SS shall conform with the flowchart behavior shown in Figure 5.

### Intended Receiver behavior:

1. The intended DPP receiver shall detect its MAC address in CTRL MSG as described in Table 4.
2. Upon receiving an RTS message, the intended DPP receiver configured for CA operation shall convert the number of bytes that were requested in the CTRL MSG into the number of slots that it is allocating at the MCS which it determines based on the CINR measured in the received RTS message, plus the additional slots required to transmit the CTRL MSG, using the Robust MCS.
3. Upon CSMA-sensing that the channel is clear after receiving an RTS message, the intended DPP receiver shall transmit a CTS message identifying the number of slots it has allocated along with the MCS to be used in accordance with Table 4.
4. When the intended DPP receiver transmits a CTS message, it shall delay any subsequent transmission by the CTS Deferral time as defined in 5.4.2.
5. The intended DPP receiver shall decode a message without errors when received and upon CSMA-sensing that the channel is clear, send an ACK to the sender if indicated in the CTRL MSG.

### Non-Intended Receiver behavior

1. A DPP SS is considered to be a non-intended receiver for a message it receives in which it does not recognize its MAC address.
2. If a received CTRL MSG indicates RTS, the non-intended receiver shall avoid transmission within the RTS Deferral duration as defined in 5.4.1.
3. If a received CTRL MSG indicates CTS, the non-intended receiver shall avoid transmission within the CTS Deferral duration as defined in 5.4.2.
4. If CTRL MSG is received with ACK indication, then non-intended receiver will avoid transmission within the ACK deferral duration as defined in 5.4.3.

## Deferrals

### RTS Deferral: When the non-intended receiver receives a CTRL MSG with indication of RTS, it shall compute the deferral time using the number of slots requested plus the duration of the CTRL MSG, gain adjustment, synchronization signal, and maximum round trip duration.

### CTS Deferral:

1. When the non-intended receiver sees a CTRL MSG with the indication of CTS, it shall compute the CTS Deferral Time using the number of slots allocated in the CTS message plus the duration of the CTRL MSG, gain adjustment, synchronization signal, and maximum round trip duration.
2. When the intended receiver sends a CTRL MSG with the indication of CTS, it shall compute the CTS Deferral Time using the number of slots allocated in the CTS message plus the duration of the CTRL MSG, gain adjustment, synchronization signal, and maximum round trip duration.

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

Diagram

Description automatically generated

Figure 5. CSMA/CA RTS CTS flowchart for DPP SS initiating transmission

# DPP SS States

## Offline state

## The DPP SS when turned ON shall enter the Offline state by default.

## Each DPP SS will have a unique MAC Address and public/private key pair configured during production.

## A X509 certificate may also be installed during production or later by a Certificate Authority under customer responsibility.

## The DPP SS shall 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, DPP SS Name and specific DPP parameters as described in this document.

## Each DPP SS shall be configured with a pairing method. Two pairing methods are supported:

## Automatic Pairing: In automatic pairing, A DPP SS identifies its peer using the peer’s MAC address.

## List Selection Pairing: In list selection pairing, a DPP SS filters and presents a list of available DPP SSs Names within its range. The list contains DPP SS name received in the ASSOCIATE Request message. The user manually selects the desired peer from the list to complete the association process. The filtering parameters is the certificate issuer name that is transmitted in the ASSOCIATE Request message.

## For ‘automatic’ pairing method, each DPP SS shall be configured with parameters of its peer DPP SS as follows:

## MAC address of peer SS.

## public key of its peer SS.

## For ‘list selection’ pairing method each DPP SSshall be configured with parameters of valid peer DPP SSs as follows:

## certificate issuer, as appears in the certificate issuer Name field.

## public key of the certificate issuer.

## When configured to use two distinct frequencies in ‘automatic’ pairing mode, the DPP SS shall compare its own MAC address with the MAC address of its peer and use the higher frequency for TX and the lower frequency for RX if its MAC address is higher than the peer DPP SS’s MAC address, otherwise, it selects the lower frequency for TX and the higher frequency for RX.

## When configured to use two distinct frequencies in ‘list selection’ pairing mode, DPP SSs shall operate in the lower frequency while in Online state and Association state. While in Operational state, the DPP will compare its own MAC address with the MAC address of its peer and use the higher frequency for TX and the lower frequency for RX if its MAC address is higher than the peer DPP SS’s MAC address, otherwise, it selects the lower frequency for TX and the higher frequency for RX.

## The DPP SS shall switch to the online state based on a vendor-specific manual trigger.

## Online state

1. While in the online state, the DPP SS shall transmit periodically an ASSOCIATE Request message indicating its MAC address and in the case of ‘list selection’ pairing mode its name and issuer, as appear in its certificate.

## Association state

## The DPP SS shall enter the association state following the receipt of an ASSOCIATE Response or ASSOCIATE Request message from its peer.

## The DPP SS shall perform the following activities during the Association state:

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

## Authenticate its peer SS as described in section 7.2.

## Automatic PHS configuration as described in section 7.3.

## The DPP SS in the Association 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 SS shall enter the Operational state automatically, following the completion of the activities described in the Association state.

## The DPP SS shall perform the following activities during the Operational state:

## Exchange data messages with the peer DPP SS.

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

### 1. If configured for ‘automatic’ pairing method, the DPP SSs shall exchange their MAC addresses using ASSOCIATE Request/Response messages. The DPP SS receiving an ASSOCIATE Request message shall compare the received MAC address with the MAC address(es) of its configured peer DPP SS(s) and send an ASSOCIATE Response message to the sender of the ASSOCIATE Request message if a match is found. If there is no match, the DPP SS shall not respond to the ASSOCIATE request message and will return to online state. The identity verification process is shown in Figure 6 below.

2. If configured to ‘list selection’ pairing method, the DPP SS receiving an ASSOCIATE Request message shall compare the received certificate issuer with its configured peer DPP SS(s) certificate issuer and if matched will add the SS’s name and MAC address, as appears in the ASSOCIATE Request message, to the list of available DPP SSs.

3. If configured to ‘list selection’ pairing method, the DPP SS shall include a function to display the list of filtered available DPP SS names, and a function to configure the MAC address of the manually selected peer SS. If no SS is selected, the DPP SS will return to online state.

Timeline

Description automatically generated

Figure . Association message flow

## Authentication

### Authentication and Key management

1. Each DPP SS in the network shall include a unique private / public key pair.
2. Each DPP SS shall have a X.509 certificate that has been signed by a trusted Certificate Authority (CA).
3. A DPP SS configured to ‘list selection’ pairing method shall have a configured DPP SS Name.

### Each DPP SS shall support both client and server TLS v1.3. If TLS authentication fails, the DPP SS will return to online state.

### At minimum, a DPP SS shall support the following TLS v1.3 cipher suites options:

1. Key exchange: Elliptic Curve Diffie-Hellman (ECDH) [RFC 4492] or ephemeral Elliptic Curve Diffie-Hellman (ECDHE)
2. Authentication: Elliptic Curve Digital Signature Algorithm (ECDSA)
3. Encryption: AES-128 or AES-256

### Message authentication: HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512.

### Upon sending an ASSOCIATE Response message, the DPP SS shall compare its own MAC address with the MAC address of its peer and shall operate as a TLS server if its MAC address is higher than the peer DPP SS’s MAC address, otherwise, it shall operate as a TLS client.

### Upon receiving an ASSOCIATE Response message, the receiving SS shall compare its own MAC address with the MAC address of its peer and shall operate as a TLS server if its MAC address is higher than the peer DPP SS’s MAC address, otherwise, it shall operate as a TLS client.

### When operating as a TLS server, if the DPP terminal does not receive a ClientHello message within TBD msec, it shall return to online state.

### A DPP SS operating as TLS server, shall include in the ServerHello optional fields: Certificate, CertificateRequest and CertificateVerify, to support mutual authentication.

### Upon receiving a certificate from another DPP SS, if configured to ‘automatic’ pairing, the receiving SS shall authenticate the sending SS identity using its configured public key.

### Upon receiving a certificate from another DPP SS, if configured to ‘list selection’ pairing, the receiving SS shall authenticate the issuing CA using its configured CA public key and then authenticate the SS by the public key sent with the certificate.

## 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 size, PHS field, PHS mask and PHS index. All these parameters are used during PHS rule creation.

**PHS Size**

This indicates the size of the PHS Field. Since this is just one byte, only a maximum of 255 bytes can be suppressed.

**PHS Index**

This is unique per service flow. This is used to identify the PHS rule. It precedes the higher layer PDU when PHS is enabled. It does not exist when PHS is disabled. If PHS is enabled and suppression is not done, PHS Index=0 is used. It has the range 1-255.

**PHS Field**

This is a specified number of bytes containing header information to be suppressed. It is stored and used on both sending and receiving sides. The number of bytes is the same as the value of PHS Size.

**PHS Mask**

This is a mask that determines which parts of the PHS Field needs to be suppressed. A value of 1 indicates a byte to be suppressed. Otherwise, the byte is included in the transmission. This has a maximum length of 8 bytes to cover the range of PHS Size. Bit 0 is related to the first byte of the PHS Field.

### PHS rules shall be automatically created by the sending SS when there is a repetitive portion of data in a packet. In a PHS rule, the sending SS shall specify the field values that can be suppressed in that packet and the associated PHS index to identify the PHS rule in the PHS request message sent to receiving SS. Please refer to ieee802.16-2017 section 5.2.3 and section 5.2.3.1 for details on PHS specification and operation.

### A sending SS shall trigger a new rule when any repetitive field value in the traffic is observed and the field values are not matching with any of the already existing PHS rule field values stored.

### A sending SS shall apply PHS after creation of a rule. Comment: Until a PHS rule is created, the message header data it specifies will be unsuppressed.

### A sending SS shall include a PHS index as a prefix to PDU data to indicate when PHS is applied.

### A receiving SS shall identify each PHS rule using a PHS Index (PHSI) as specified in Table 1 .

Diagram

Description automatically generated

Figure PHS Creation Flow

.

### Automatic PHS-related messages are described in section 9.1.4.

## Link Adaptation (LA)

### Link adaptation is the process of dynamic selection for transmission of the highest MCS and repetition rate that can support reliable communications subject to the CINR at the peer SS receiver.

### At the beginning of the LA process, the DPP SS shall transmit all packets with the Robust MCS. To initiate the LA process, each DPP SS shall send an unsolicited Measurement Report message to its peer DPP SS at the beginning of the Association phase. To reinitiate the LA process, the DPP SS shall send an unsolicited Measurement Report message to its peer DPP SS whenever it detects a significant change in CINR measurements indicating that the current MCS is not the highest that can support reliable communications.

### Table 3 describes the MCS table with repetition factor.

### The Measurement Report message shall indicate the sequence number of the burst for which the measurement was taken.

### After receiving a Measurement Report message, the DPP SS shall start/restart its LA hold timer and use the MCS as per the report until the timer expires.

### In case the LA hold timer expires, the DPP SS shall use Robust MCS for transmission until the LA process has reoccurred and determined that a different MCS should be applied.

### The measurement report structure is described in section 9.1.3. Figure 8 shows the flow of the LA process.

Chart, diagram

Description automatically generated

Figure 8. Link Adaptation (LA) Procedure

Table 3 MCS table

|  |  |
| --- | --- |
| MCS | Value |
| QPSK 1/2 R128 | 0 |
| QPSK 1/2 R64 | 1 |
| QPSK 1/2 R32 | 2 |
| QPSK 1/2 R16 | 3 |
| QPSK 1/2 R8 | 4 |
| QPSK 1/2 R4 | 5 |
| QPSK 1/2 R2 | 6 |
| QPSK 1/2 | 7 |
| QPSK 3/4 | 8 |
| 16 QAM 1/2 | 9 |
| 16 QAM 3/4 | 10 |
| 64 QAM 3/4 | 11 |
| 64 QAM 5/6 | 12 |
| 256 QAM 7/8 | 13 |

## Power Control

### Power control is an optional DPP process. When power control is not enabled, the DPP SS is configured for fixed TX power (typically Max TX power) and the Automatic Gain Control (AGC) at the peer DPP SS adjusts its gain to attempt to optimize its 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 SS. The criteria is vendor specific. The receiving DPP SS sends a Measurement Report message (the same message type as used for LA) which includes the RSSI, so that the transmitting SS can use this RSSI measurement to compare it with the target RSSI and do the delta power correction in the next transmission. The power control process (if present) must be designed to work synergistically with the LA process.

### The measurement report structure is defined in section 9.1.3 .

# Relay Station

## General

### The CTRL-MSG within the burst shall indicate if the burst shall be relayed using the field Relay Status as described in Table 4.

### A DPP SS shall be configured with one of three relay options as follows:

* + 1. Direct transmission only: when relay station receives the CTRL-MSG with relay option value as 0 it shall not relay.
    2. Relay: When Relay station receives the CTRL-MSG with relay option value as 1 it shall relay the burst.
    3. Relay based on ACK failure: For this option, the ACK indication shall be set to value 1 in the CTRL-MSG. When the Relay station receives the CTRL-MSG with relay option value as 2, it shall decode the burst and wait for the ACK bit map to be received till the configurable wait time duration. If ACK bit map is not received, the whole burst is relayed. If ACK bit map is received, depending on the bitmap status, only the PDUs whose bit status is zero shall be relayed in the burst. ACK bitmap is present in the CTRL-MSG when control message type option value is 3.

### A relay station shall relay the burst if required by the CTRL MSG. The relay station shall change the relay status to 1 in CTRL-MSG when it does the relay transmission.

### Relay station shall perform the channel access as per the procedure described in section 5.2.

# Messages format

All data fields are little endian.

### Control Message (CTRL MSG)

|  |  |  |
| --- | --- | --- |
| Syntax | Size(bits) | Notes |
| Control message () { | --- | ---- |
| Control message Type | 2 | This field indicates the type of CTRL MSG based on what description it is carrying.  Value 0: PDU,  1: RTS  2: CTS  3: ACK |
| Relay Status | 1 | 0: Original transmission, 1: Relay Transmission |
| Relay option | 2 | Value 0: Direct transmission only, No Relay  1: Relay  2: Relay based on ACK failure |
| Sender ID | 48 | MAC address |
| Receiver ID | 48 | MAC address |
| If (control message Type == 1) { |  |  |
| Requested bytes | 16 | Total bytes to transmit including PDU and SDU overheads. |
| Reserved | 11 |  |
| } |  |  |
| ElseIf (control message Type == 3) { |  |  |
| ACK Bit Map | 16 | LSB applies to first PDU and MSB to last. Bit value 1 indicates ACK. Maximum number of PDUs in burst shall not exceed 16. |
| Reserved | 11 |  |
| } else { |  |  |
| MCS | 4 | MCS includes the Repetition. Refer Table 3. |
| 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 | 2 |  |
| Sequence number | 7 | Transmission sequence number |
| AUTHI | 1 | Authentication. 0: Disabled 1: Valid CMAC/HMAC is present. |
| } |  |  |
| CRC | 8 | CRC for above bytes computed per 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 4.: CTRL Message

### Association Message (ASSOCIATE Request, ASSOCIATE Response)

|  |  |  |
| --- | --- | --- |
| Syntax | Size(bit) | Notes |
| Associate Request () { | --- | ---- |
| Message Type | 8 | Value: 1 |
| Initiator MAC addr | 48 | MAC address of initiating SS |
| Receiver MAC addr | 48 | MAC address of peer SS |
| SS name length | 8 |  |
| SS name |  | As appears in certificate.subjectName |
| Certificate issuer length | 8 |  |
| Certificate issuer |  | As appears in certificate.issuerName |
| } |  |  |

Table 5. Associate Request

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

Table 6. Associate Response

### Measurement Report Message

|  |  |  |
| --- | --- | --- |
| Syntax | Size(bit) | Notes |
| Measurement\_report () { | --- | ---- |
| Message Type | 8 | Value: 3 |
| CINR | 8 | Averaged CINR measurement report |
| RSSI | 16 | Averaged RSSI measurement report |
| MCS | 4 | MCS includes Repetition. Refer Table 3. |
| Reserved | 4 |  |
| } |  |  |
|  |  |  |

Table 7. Measurement report

### Automatic PHS Message

|  |  |  |
| --- | --- | --- |
| Syntax | Size(bit) | Notes |
| PHS Request () { | --- | ---- |
| Message Type | 8 | Value: 4 |
| PHSI | 8 | PHS Index, 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. PHS Request

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

Table 9. PHS Response

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

Table 10. PHS ACK