IEEE 802.11
Wireless Access Method and Physical Layer Specifications

Title: Proposed Updates to the D1 Draft, Section 3

Presented by: Tom Siep
Texas Instruments Incorporated
13510 N. Central Expressway, m/s 446
Dallas, Texas 75243
Tel: (214) 995-3675
Fax: (214) 995-6194
Email: siep@hc.ti.com

Abstract: **This paper proposes changes to the D1 Draft to reflect the resolution of comments on Section 3 during the May 95 meeting.**

Action: **Adopt the changes in this paper to update the relevant portions of P802.11/D1**

Introduction

The text of section 3 is modified by this document to reflect work done at the May 1995 meeting. The changes are described by the following categories

- Removal of references to 802.10
- Removal of "dead" editorial text
- Restructing of the section to reflect its simpler content

Other Contributors

David Bagby
Michael Fischer
Leon Scaldeferri
Jeff Abramowitz

1. MAC Service Definition

1.1. Overview of MAC Services

~~1.1.1.General Description of Services Provided~~

1.1.2. Asynchronous Data Service

This service provides peer LLC entities with the ability to exchange MAC Service Data Units. To support this service, the local MAC will use the underlying PHY-level services to transport an MSDU to a peer MAC entity, where it will be delivered to the peer LLC. Such asynchronous MSDU transport is performed on a best-effort connectionless basis. There are no guarantees that the submitted MSDU will be delivered successfully. Broadcast and multicast transport is part of the asynchronous data service provided by the MAC. All Stations are required to support the AsynchronousAsynchronlus Data Service.

1.1.3. Time-bounded Services

Time-Bounded services are implemented within the Point Coordination Function (PCF) as connection based data transfers. The access point adds connections to the polling-list in a best attempt to maintain the requested connection. Maintaining time bounded services within an ESS shall be supported.

Since the PCF is optional, support for Time-bounded Services are also optional.

1.1.4. Security Services

Security services in 802.11 shall be provided by the Wired Equivalency Privacy mechanisma subset of the service described in IEEE Std 802.10-1992, Secure Data Exchange (SDE), (clause 2) [2], hereafter referred to as WEPSDE. The scope of the security services provided is limited to Station-to-Station associationsdata exchange. The confidentialityminimum service offered by any 802.11 WEP implementation shall be the encipherment of the MSDU payload. For the purposes of this standard, the WEPSDE is viewed as a logical sub-layer located at the top of the above the MAC sub-layer as shown in the reference model - section 2.4. Actual implementations of the WEPSDE sub-layer is considered transparent to the LLC or other layers above the MAC sub-layer.

The security services provided by the WEPSDE into 802.11 are:

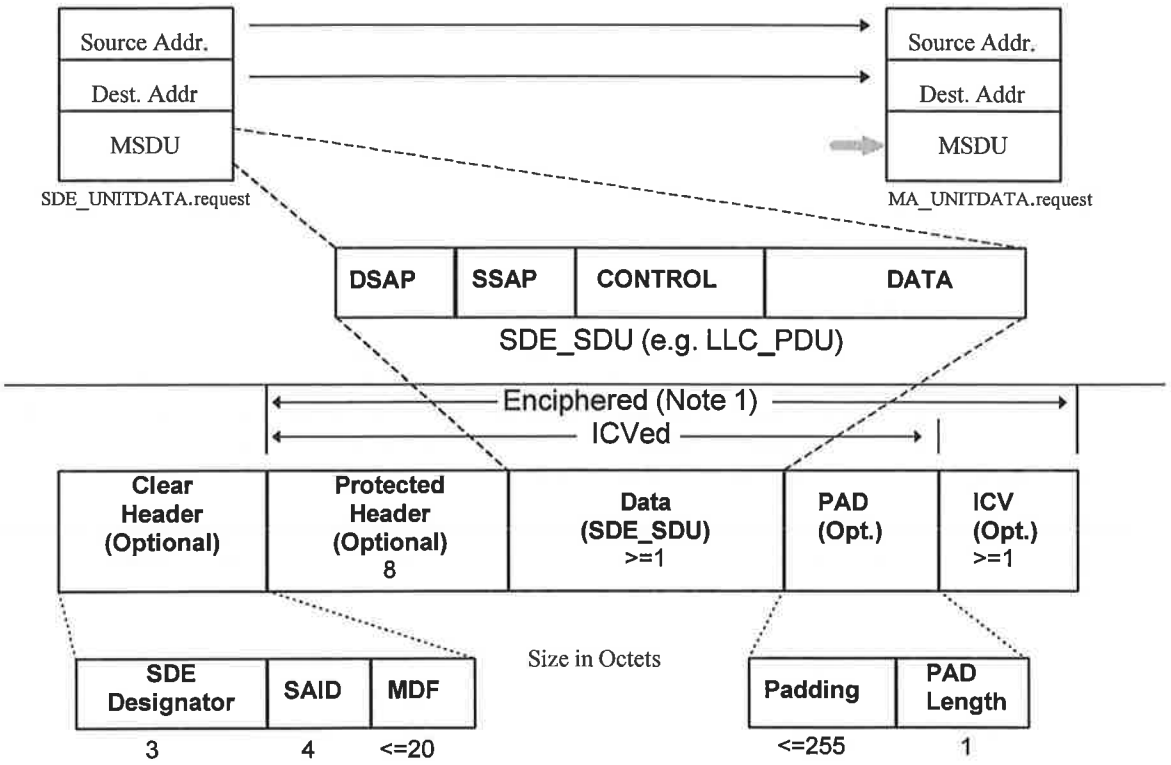
1) confidentiality;
2) authentication; and
3) access control in conjunction with layer management.

Threats protected against are:

1) unauthorized disclosure;
2) unauthorized resource use; and
3) masquerade.

The IEEE 802.10 SDE [2] describes five parts to the SDE_PDU: Clear Header, Protected Header, Data, Pad, and Integrity Check Value (ICV).

Only the data is required, all other parts are optional to the particular implementation and the security services provided by the application of the SDE. All implementations of 802.11 shall provide for encipherment of data using the default algorithm(s). The default encipherment algorithm is specified in section 5.4.

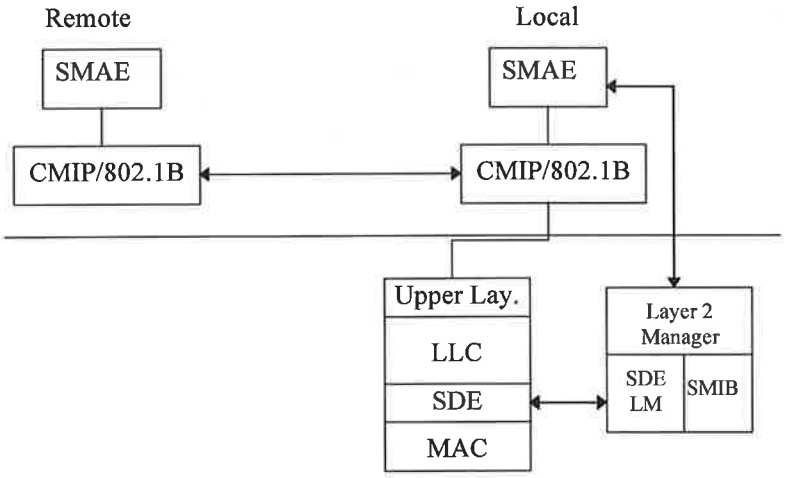


~~Figure 3-1: Construction of the SDE_PDU~~

~~Note 1 - The enciphered data may include expansion and/or cryptographic information.~~

During the authentication exchange, parties A and B exchange authentication information as described in section y.y.

The Layer 2 security services provided by the WEP~~SDE~~ rely on information from non-Layer 2 management or system entities. Management entities communicate the information to the WEP~~SDE~~ entity through a set of MIB variables.~~Security Management Information Base (SMIB). The implementation of the SMIB is a local issue; however, IEEE 802.10f, SDE Sublayer Management, provides information on the managed object classes and attributes. The SMIB provides the interface between the local System Management Application Entity (SMAE) and the LM of the protocol stack. This is illustrated in Figure 3-2:~~



~~Figure 3-2: SDE Management Architecture~~

~~1.1.5. Basic Service and Options~~

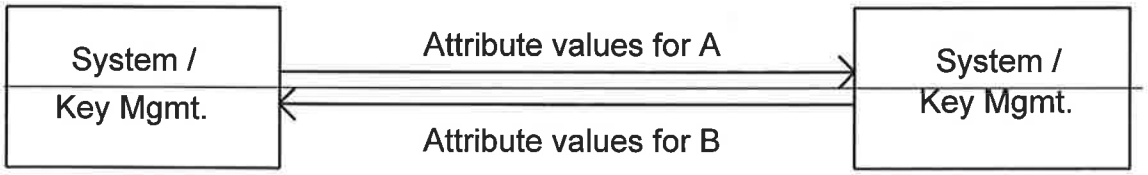
1.1.6. Reordering of MPDUs

The services provided by the MAC Sublayer permit the reordering of MSDUs. The MAC does not intentionally reorder MSDUs. However, since MSDUs can transit a DS, and a DS might reorder~~reoder~~ MSDUs, it is not possible for the MAC to guarantee MSDU ordering.

~~1.1.7.Security Service~~

~~As described in Section 3.1.1.3 above, all 802.11 Wireless LANs shall provide for data encipherment in accordance to the appropriate sections of SDE [2]. Elements of the SDE procedures applicable to 802.11, including transmission and reception processing, are defined in this sub-clause. Other elements including management architecture, addressing, Security Management Information Base (SMIB), and the definitions of the managed objects are contained in section 2.3 of IEEE 802.10 SDE [2].~~

~~During the association exchange, parties A and B exchange of the attribute values of the security association managed objects defines in IEEE 802.10 SDE [2]. These values specify the security parameters (e.g. algorithm, key, etc.) that will be needed for the association.~~



~~Figure 3-3: Initial Exchange~~

~~The management entity enters the values for the association objects into the SMIB. This may be done by a secure exchange between stations using a higher layer protocol or the SMIB may be pre-established by other techniques (e.g. SmartCard).~~

~~Simple Example of Security Management Information Base (SMIB)~~

~~Station ID (N-bit ID)~~ ~~(Note 1)~~	~~Remote_SDE (True = 1, False = 0)~~	~~Data Privacy Mask (M-bit Data "Key")~~ ~~(Note 2)~~	~~Algorithm Number~~ ~~(Note 3)~~
~~Sta (a)~~	~~1~~	~~abcd12987fed...~~	~~0=Default~~
~~Sta (b)~~	~~0~~	~~None~~	~~0~~
~~Sta (c)~~	~~1~~	~~abcdef0123456789~~	~~2~~
~~...~~	~~...~~	~~...~~	~~...~~

~~Note 1 - The station ID could be 48 bit "Ethernet like" address or other type (this is not necessicarily the same as the SID)~~

~~Note 2 - The Data Privacy Mask can be either fixed or variable (max) length to accommodate a variety of algorithms.~~

~~Note 3 - Algorithm Number is an algorithm number registered per IEEE 802.10.~~

1.2. Detailed Service Specification

1.2.1. MAC Data Services

1.2.1.1. MA_UNITDATA.request

~~1.2.1.1.1.~~ **Function**

This primitive defines the transfer of a MSDU from a Local LLC sublayer entity to a single peer LLC sublayer entity, or multiple peer LLC sublayer entities in the case of group addresses.

~~1.2.1.1.2.~~ **Semantics of the Service Primitive**

The semantics of the primitive are as follows:

```
MA_UNITDATA.request (
                        source_address,
                        destination_address,
                        routing_information,
                        data,
                        priority,
                        service_class
                        )
```

The source_address parameter (SA) shall specify an individual MAC sublayer entity address, this SA shall be replaced in the MPDUs resulting from this request with the individual MAC sublayer address of the MAC entity to which the request is made. The destination_address parameter (DA) shall specify either an individual or a group MAC sublayer entity address. The routing_information parameter specifies the route desired for the data transfer (a null value indicates source routing is not to be used). The data parameter specifies the MAC service data unit (MSDU) to be transmitted by the MAC sublayer entity. The length of the MSDU shall be less-than or equal to 2304 octets. The priority parameter specifies the priority desired for the data unit transfer (contention~~conention~~ or contention-free). The service_class parameter specifies the service_class desired for the data unit transfer (asynchronous or time-bounded).

~~1.2.1.1.3.~~ **When Generated**

This primitive is generated by the LLC sublayer entity whenever a MSDU must be transferred to a peer LLC sublayer entity or entities. This can be as a result of a request from higher layers of protocol, or from a MSDU generated internally to the LLC sublayer, such as required by Type 2 operation.

~~1.2.1.1.4.~~ **Effect of Receipt**

The receipt of this primitive shall cause the MAC sublayer entity to append all MAC specified fields, including DA, SA, and any fields that are unique to the particular media access method, and pass the properly formatted frame to the lower layers for transfer to peer MAC sublayer entity or entities.

1.2.1.2. MA_UNITDATA.indication

~~1.2.1.2.1.~~ **Function**

This primitive defines the transfer of a MSDU from the MAC sublayer entity to the LLC sublayer entity, or entities in the case of group addresses. In the absence of error, the contents of the data parameter are logically complete and unchanged relative to the data parameter in the associated MA_UNIT_DATA-Request primitive.

~~1.2.1.2.2.~~ **Semantics of the Service Primitive**

The semantics of the primitive are as follows:

```
MA_UNITDATA.indication(
                        source_address,
                        destination_address,
```

routing_information,
data,
reception_status,
priority,
service_class
)

The source_address parameter must be an individual address as specified by the SA field of the incoming frame. The destination_address parameter shall be either an individual or a group address as specified by the DA field of the incoming frame. The routing_information parameter specifies the route desired for the data transfer (null for 802.11 MACs). The data parameter specifies the MAC service data unit (MSDU) as received by the local MAC entity, and shall be less than or equal to 2304 octets in length. The reception_status parameter indicates the success or failure of the incoming frame. The priority parameter specifies the priority desired for the data unit transfer (contentionconention or contention-free). The service_class parameter specifies the service_class desired for the data unit transfer (asynchronous or time-bounded).

~~1.2.1.2.3.~~ **When Generated**

The MA_UNIT_DATA-Indication primitive is passed from the MAC sublayer entity to the LLC sublayer entity or entities to indicate the arrival of a frame at the local MAC sublayer entity. Frames are reported only if at the MAC sublayer they are validly formatted, received without error, received with valid (or null) privacy encryption, and their destination address designates the local MAC sublayer entity as either an individual or group member. When the receiving MAC sublayer entity is operating with a null privacy function, frames that are received in error may be reported, at the option of LLC; however, when operating with WEP enabled, erroneous reception (e.g. CRC failure) precludes validation of the ICV, so to report such frames when operating with WEP enabled could constitute a breach of security.

~~1.2.1.2.4.~~ **Effect of Receipt**

The effect of receipt of this primitive by the LLC sublayer is dependent on the validity and content of the frame.

1.2.2. MAC Management Services

To facilitate the three distribution system services:

a) Association
b) Reassociation
c) Disassociation - including the detection of link outage

1.2.3. Contention Free Connection Services

Contention Free Connections (CFCs) Services is a set of optional connection-oriented services. Connection setup is done once per association with an ESS, and is maintained across BSS transitions (reassociations) but must be reestablished if a disassociation occurs (either due to explicit disassociation or timeout).

1.2.3.1. Function

Semantics of the Service Primitive

MA_CONNECTION_START.request (
maximum_msdu_size,
normal_request_interval
)

When Generated

Effect of Receipt

1.2.3.2. Function

Semantics of the Service Primitive

MA_CONNECTION_END.request(
connection_id
)

When Generated

Effect of Receipt

1.2.3.3. Function

Semantics of the Service Primitive

MA_CONNECTION_END.indication (
connection_id
)

When Generated

Effect of Receipt

1.2.3.4. Function

Semantics of the Service Primitive

MA_CONNECTION_GRANT.indication (
connection_id
)

When Generated

Effect of Receipt

1.2.3.5. Function

Semantics of the Service Primitive

MA_CONNECTION_NOT_GRANTED.indication()

When Generated

Effect of Receipt

1.2.3.6. Access Point Initiates Connection Set-up Illustration

The following exchange will be used when an AP wants to establish a connection.

1. AP MAC user makes Start Connection Request. If the AP MAC believes that it can support this connection then the AP MAC generates Start Connection Request frame (otherwise the AP MAC asserts a Connection Not Granted Indication).

2. If the STA MAC can support this connection then it generates a Grant Connection frame and a Grant Connection Indication. On receipt of the Grant Connection Frame a Grant Connection Indication is generated.

Note: Only one connection request may be outstanding, with any one station, at any given time. The exchange fails if no response is received before a time-out (connection set up time-out). This will result in a Connection Not Granted Indication.

{For d1.2: Should "connection not requested due to traffic congestion" be indicated back to the requester?}

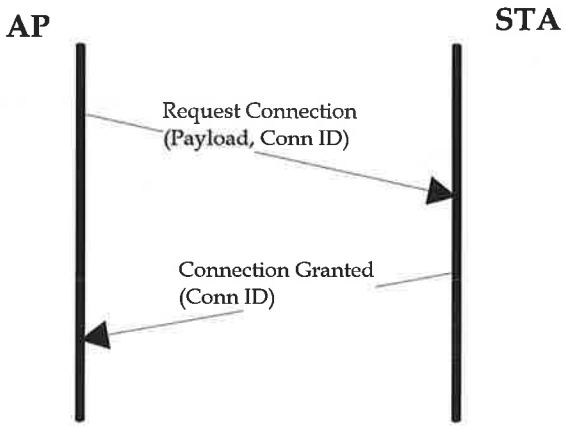


Figure 3-5: Connection Initiated by AP

1.2.3.7. Station Initiates Connection Set-up Illustration

The following exchange will be used when a STA wants to establish a connection.

1. STA MAC user makes a Start Connection Request. If the STA MAC can support this connection then it generates a Start Connection Request frame (otherwise it will assert the Connection Not Granted Indication).

2. If the AP MAC believes that it can support this connection request then it will generate a Grant Connection frame and a Grant Connection Indication.

Note: Only one connection request may be outstanding at any given time. The exchange fails if no response is received before a time-out (connection set up time-out).

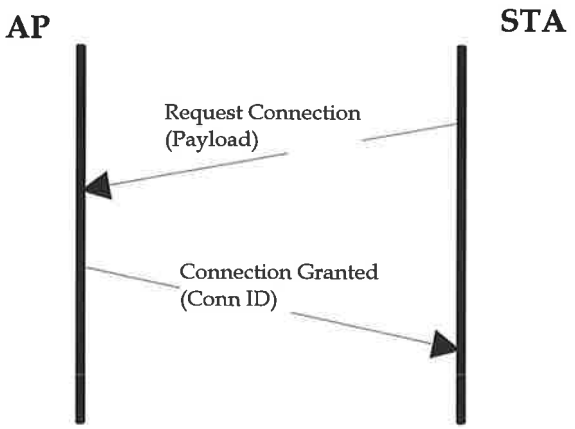


Figure 3-6: Connection Initiated by STA

1.2.3.8. End Connection

Either an AP or a station may end a connection in the following way:

1. End Connection.

No MAC layer negotiation is needed to end a connection.

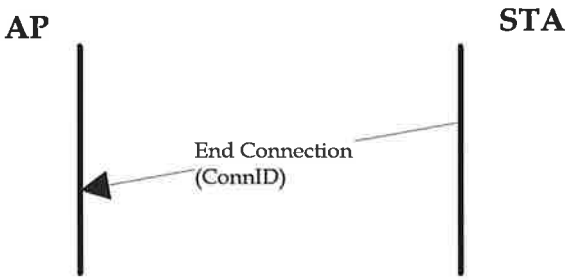


Figure 3-7: End Connection