Proposed Text for Section 3, Based on responses to Draft D1 Letter Ballot processed at March 1995 Meeting

Tom Siep
Texas Instruments
13510 N. Central Expressway, m/s 446
Dallas TX 75243, USA
Phone: 214 995 3675
Fax: 214 995 6194
E-Mail: siep@hc.ti.com

Abstract: This paper presents the changes to section 3 in the Draft Standard P802.11/D1 as a result of the Response to Draft D1 Letter Ballot processed at the March 1995 Meeting as shown in the companion Document P802.11-95/64. Not all Letter Ballot comments were processed at the March 1995 Meeting.

Action: Adopt the changes in this paper to replace the relevent portions of Section 3 of P802.11/D1.

1. 1.

2.

3. MAC Service Definition

3.1 Overview of MAC Services

3.1.1 General Description of Services Provided

3.1.1.1 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 Asynchronlus Data Service.*

3.1.1.2 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.
~~The peer-to-peer Time-bounded services shall be provided at the MAC/LLC boundary (MAC-SAP to MAC-SAP). Time bounded services shall not be interrupted when a station reassociates with a new access point in its current ESS. No requirement is made upon the continuance of time bounded services when a station associates with an access point that is not a member of its current ESS.~~

3.1.1.3 Security Services

{For d1.1: any changes to section 5.4 take precidence to text contained in this section}

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

The security services provided by the SDE to 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.* ~~(s) are for further study~~.

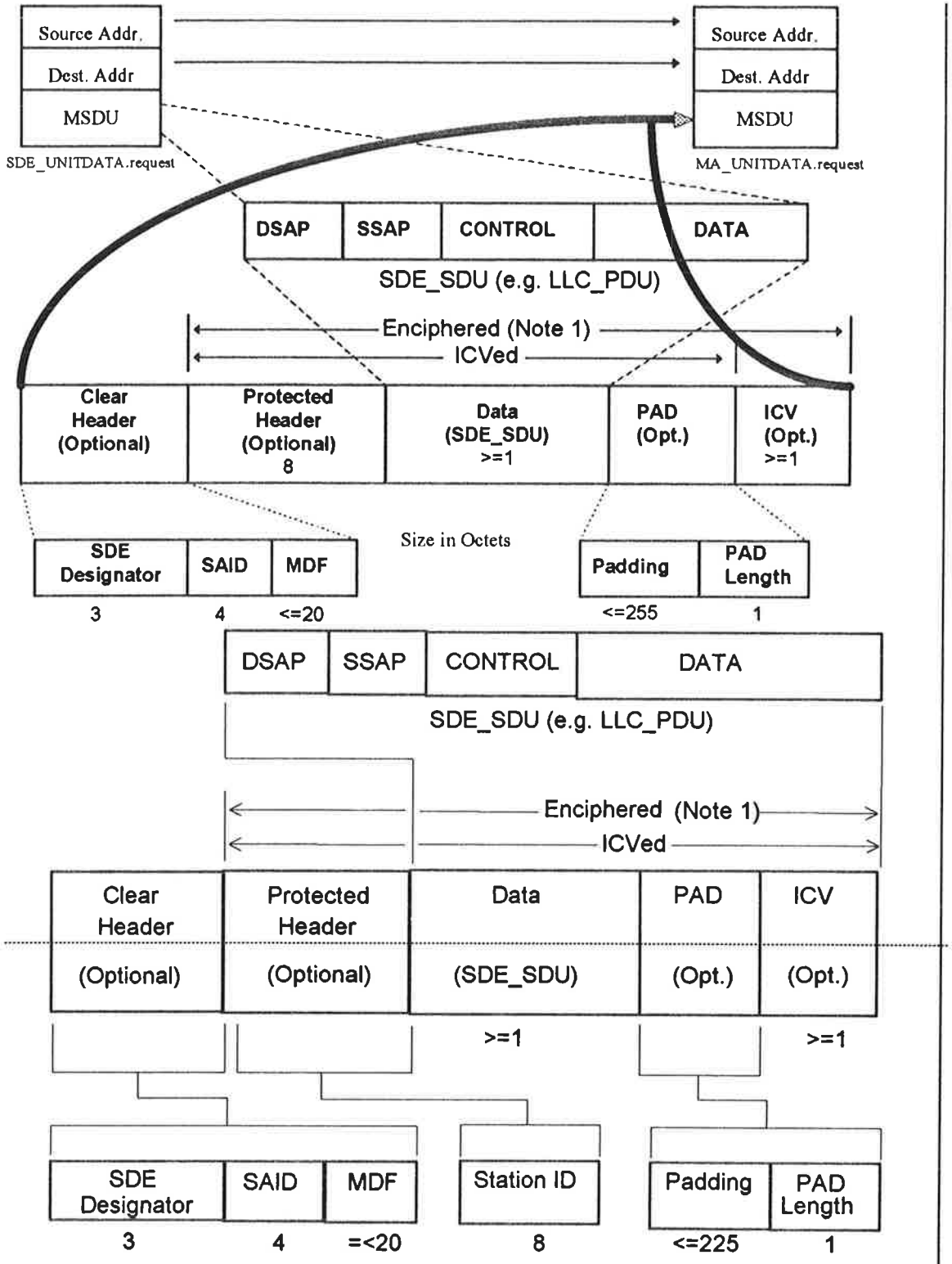


Figure 3-1: *Construction of the* Structure of SDE_PDU

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

The Layer 2 security services provided by the SDE rely on information from non-Layer 2 management or system entities. Management entities communicate the information to the SDE entity through a 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:

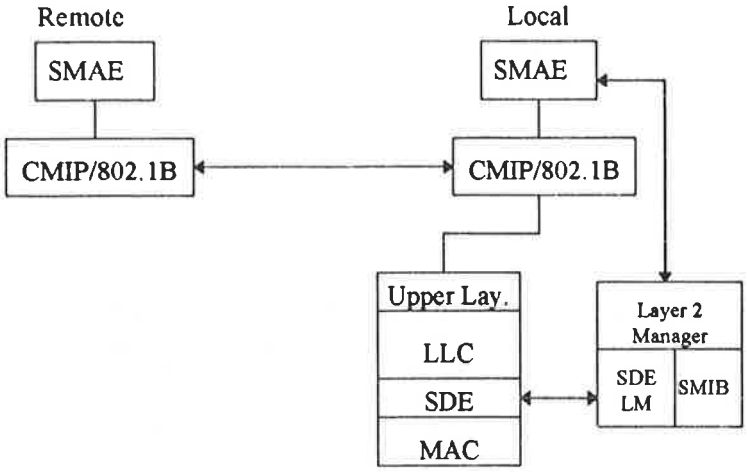


Figure 3-2: SDE management architecture

3.1.2 Basic Service and Options

{For d1.1: text needed}

3.1.2.1 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 reoder MSDUs, it is not possible for the MAC to guarantee MSDU ordering.

~~The service provided by the MAC Sublayer does not permit the reordering of MPDUs transmitted with a given user priority. MA_UNITDATA.indication service primitives corresponding to MA_UNITDATA.request primitives with the same requested priority are received in the same order as the request primitives were processed.~~

3.1.2.2 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.

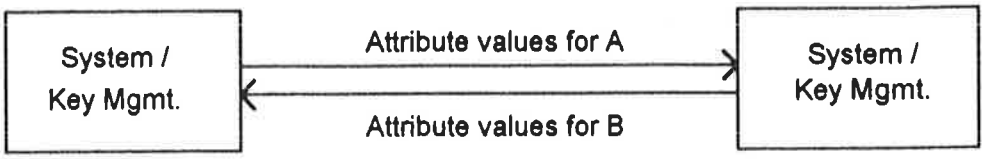


Figure 3-32: Initial Exchange

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.

~~Transmission procedures. The transmission procedures are those involved in processing an UNITDATA-request. The functions are represented as a flow chart shown below, (Object values are contained in the SMIB).~~

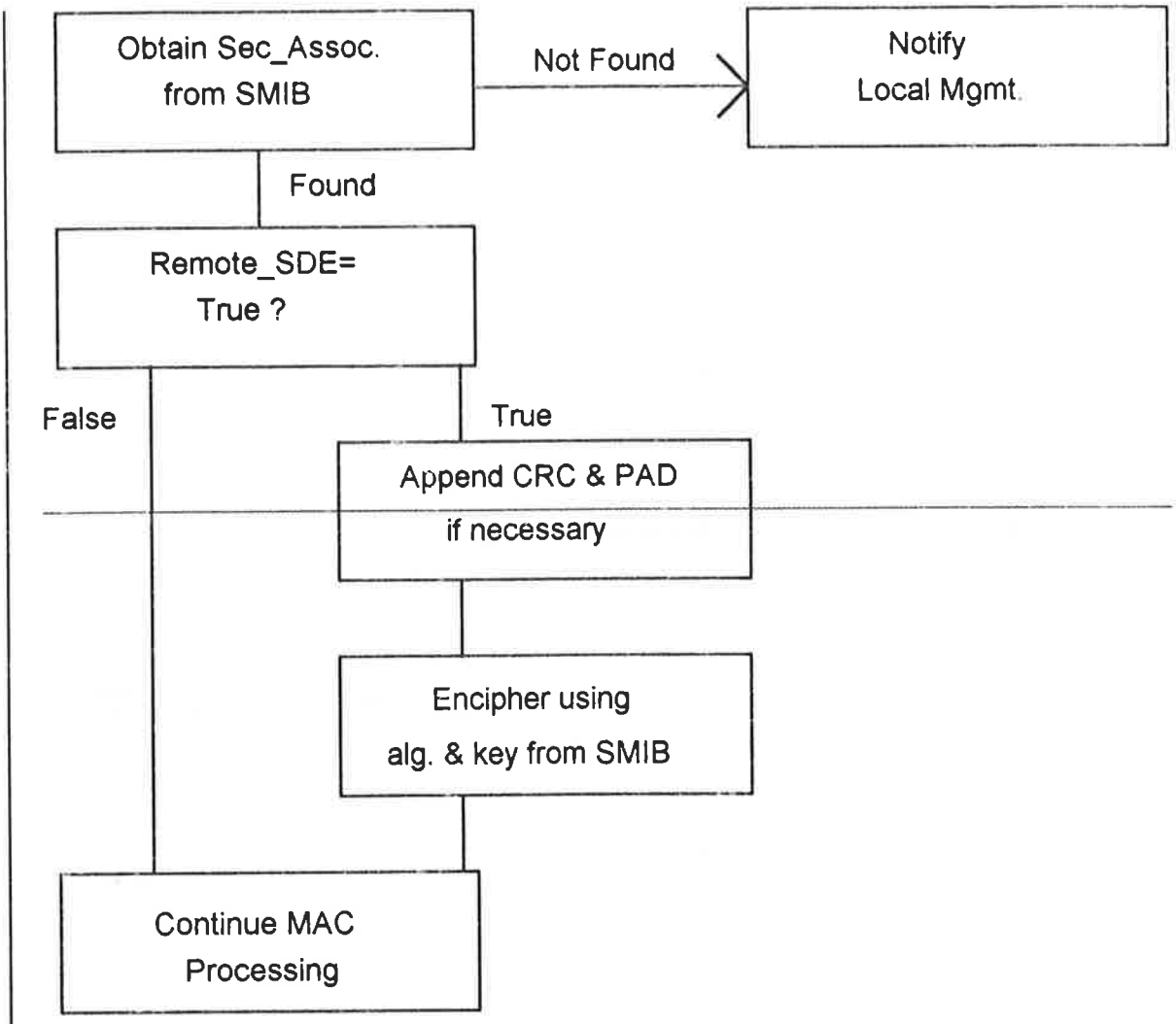
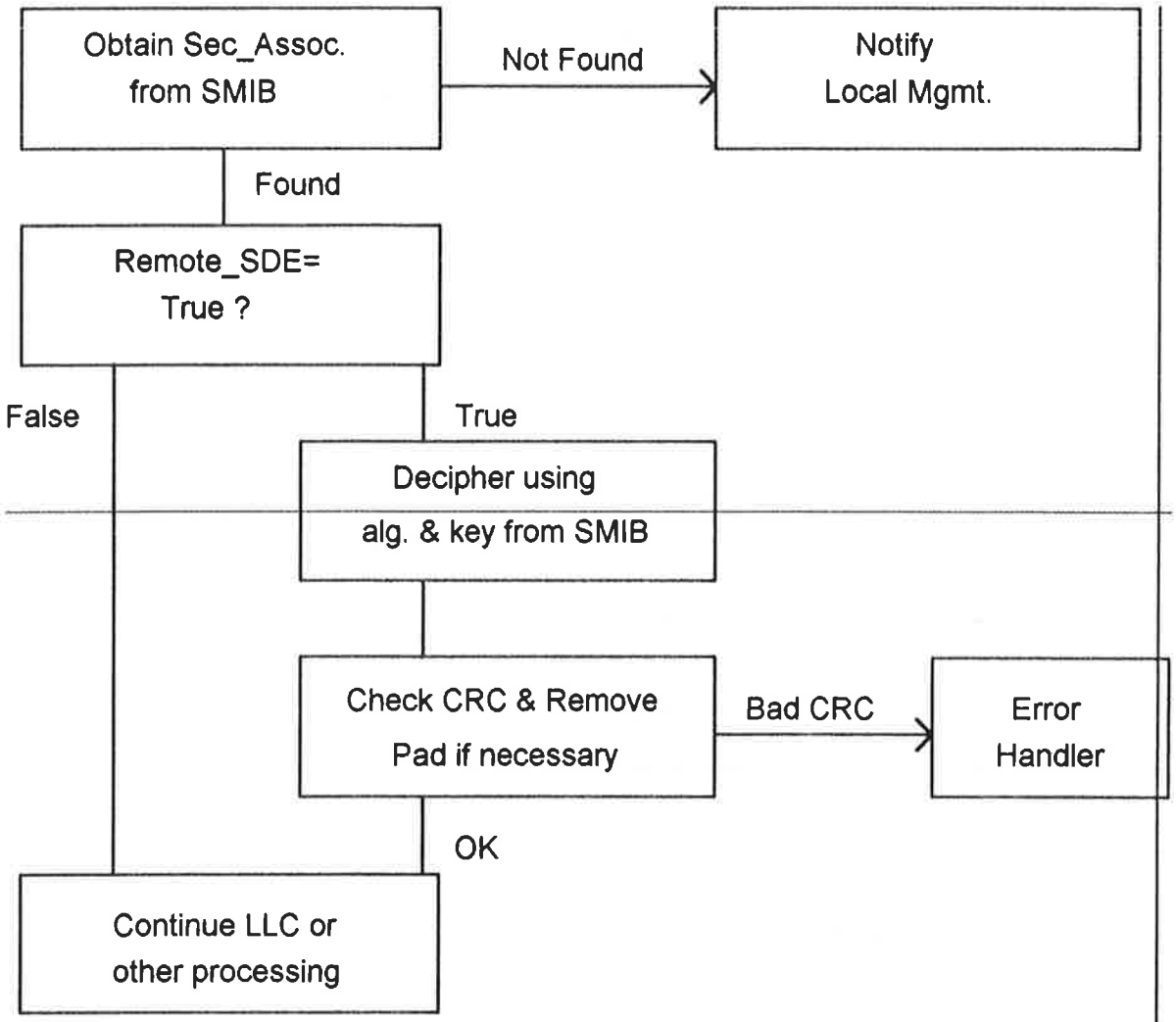


Figure 3-3: Example of SDE Transmission Procedure

~~In response to an UNITDATA-request from the LLC sub-layer, the supplied address parameters are used to search for a security association in the SMIB.~~

~~1) If the search is successful, the data is processed or passed unprocessed if the SMIB indicates that Remote_SDE = False.~~
~~2) If no security association is found, the local management entity is notified. This may initiate the association procedure.~~

~~Reception Procedures. When an UNITDATA-indication is received, processing can vary depending on the local management functions. If any security relevant exceptions are encountered during processing by the SDE entity, the local management is notified.~~



~~Figure 3-4: Example of SDE Reception Procedure~~

~~Before a station can process an incoming PDU, a security association shall exist before communication is to be allowed. A bootstrap value shall have a security association in the SMIB to permit stations to become associated through a higher layer protocol or a pre-established association.~~

3.2 Detailed Service Specification

3.2.1 *MAC Management Services*

[text needed]

To facilitate the three distribution system services:

- *Association*
- *Reassociation*
- *Disassociation - including the detection of link outage*

3.2.2 *MAC Data Services*

3.2.2.1 MA_UNIT_DATA-Request

3.2.2.1.1 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.

3.2.2.1.2 Semantics of the Service Primitive

The semantics of the primitive are as follows:

~~MA-UNIT_DATA-Request (~~
~~source_address,~~
~~destination_address,~~
~~data,~~
~~priority/service_class~~
~~)~~

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. 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 (conention or contention-free).* The ~~priority~~/service_class parameter specifies the ~~priority~~/service_class desired for the data unit transfer *(asynchronous or time-bounded).*

{For d1.1:need enumeration types for priority and service_class}

3.2.2.1.3 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.

3.2.2.1.4 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.

3.2.3 MA_UNIT_DATA-Indication

3.2.3.1 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.

3.2.3.2 Semantics of the Service Primitive

The semantics of the primitive are as follows:

~~MA_UNIT-DATA-indication (~~
~~source_address,~~
~~destination_address,~~
~~data,~~
~~reception_status,~~
~~priority/service_class~~
~~)~~

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 (conention or contention-free).* The

~~priority~~/service_class parameter specifies the ~~priority~~/service_class desired for the data unit transfer *(asynchronous or time-bounded).*

{For d1.1: need enumeration types for reception_status, priority, and service_class}

3.2.3.3 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.* ~~Frames are reported only if at the MAC sublayer they are validly formatted, received without error, and their destination address designates the local MAC sublayer entity.~~

3.2.3.4 Effect of Receipt

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

3.2.4 Contention Free Connections

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).

3.2.4.1 Access Point Initiates Connection Set-up

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.

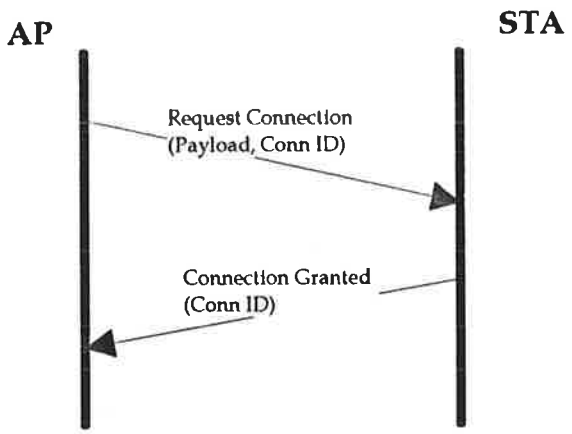


Figure 3-5: Connection Initiated by AP

3.2.4.2 Station Initiates Connection Set-up

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).

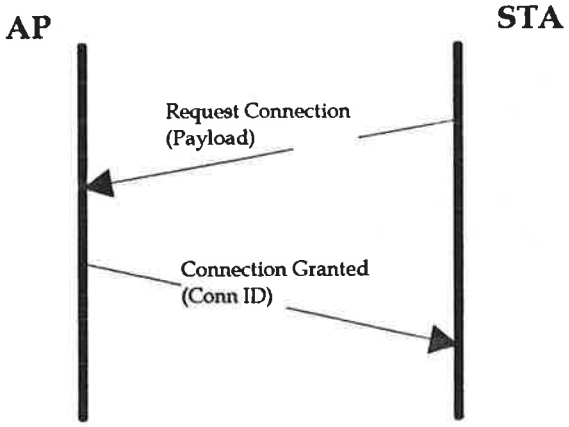


Figure 3-6: Connection Initiated by STA

3.2.4.3 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.

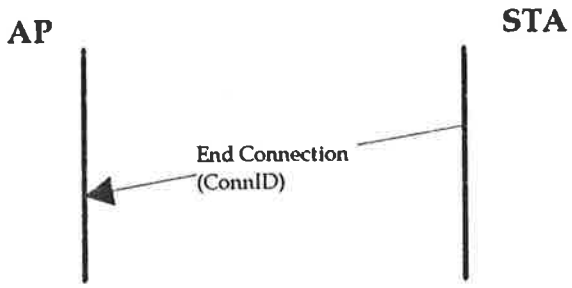


Figure 3-7: End Connection