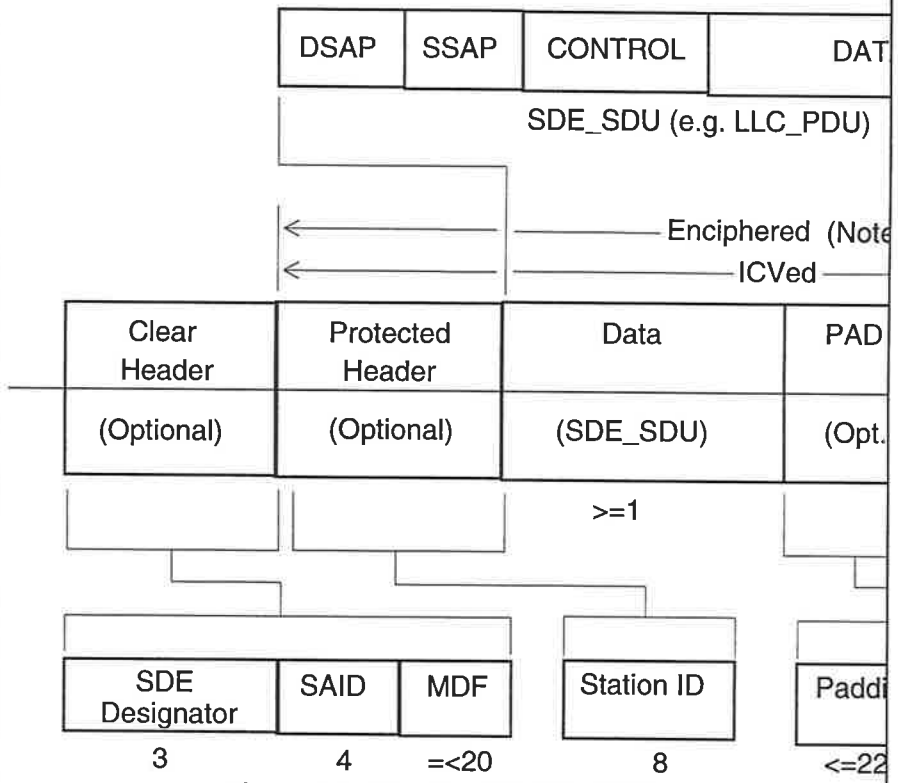
Collected comments on Section 3 of draft standard D1

3	Rick White	T	Must add more detailed information on Data and Management Services	The Section is dominated by Security services with very little information on Data and Management services.
3.1.1.1	CHRIS ZEGELIN		NO MENTION IS MADE OF THE STORE AND FORWARD SERVICE PROVIDED FOR POWER CONSERVING STATIONS	THIS IS VERY MUCH A MAC SERVICE THAT EFFECTS THE WAY MSDU'S ARE SENT.
3.1.1.1	Jon Rosdahl	E	...MAC Service Data Units (MSDU)	The abbreviation needs to be added as it is used later in this section. This seemed to be where it is defined.
3.1.1 1	David Bagby	T	provided by the MAC. All Stations are required to support the Asynchronous Data Service.	See imbeded comments and annotations
3.1.1.1	Rick White	T	Need to define both contention and contention-free Data Services.	Not defined.
3.1.1.2	CHRIS ZEGELIN		THIS SECTION NO LONGER ACCURATELY DESCRIBES THE TIME BOUNDED SERVICE.	
3.1.1.2	Glen Sherwood	E	Define Time-bounded services before using.	Time-bounded service is referenced before being defined.
3.1.1.2	A. Bolea	T		The requirement that Time Bounded Services shall not be interrupted when a station reassociates may not be achievable. The reason is that scanning for a new AP and then associating with this AP will probably take longer than the time bounded service period. I believe that this requirement should be removed.
3.1.1.2	David Bagby	T	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. The adoption of 94/252 (see 252a slide 5) indicates that the following language should be added here: Time bounded services are supported by a PCF (see section 5). The ability of a Station to operate as the PCF is optional.	See imbeded comments and annotations
3.1.1.2	Dean Kawaguchi	T	Time-bounded Services The peer-to-peer Time-bounded services shall be provided at the MAC/LLC boundary (MAC-SAP to MAC-SAP). Time-bounded services is provided on a best-effort basis given the channel conditions and load. Time bounded services shall not be interrupted when a station reassociates with a new access point in its current ESS...	Time bounded services cannot be guaranteed in all channel conditions, e.g., excessive interference or edge of range. Even after determining conditions are sufficient, channel conditions may change to unsuitable in a short period of time.
3.1.1.2	Fischer, Mike.	T	last sentence: change Ôtime bounded servicesÓ to Òany network servicesÓ	correctness, this subjet applies to all network services

3.1.1.2	Rick White	T	Must define what is meant by time bounded? Must define time bounded.	Not defined.
3.1.1.2	Stuart Kerry	T	Time-bounded Services The peer-to-peer Time-bounded services shall be provided at the MAC/LLC boundary (MAC-SAP to MAC-SAP). Time-bounded services is provided on a best-effort basis given the channel conditions and load. Time bounded services shall not be interrupted when a station reassociates with a new access point in its current ESS...	Time bounded services cannot be guaranteed in all channel conditions.
3.1.1.2	Tim Phipps	T	The peer-to-peer Time-bounded services shall be provided at the MAC/LLC boundary (MAC-SAP to MAC-SAP). Time bounded services **may be interrupted (by loss of MSDUs)** 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.	It it not possible to preserve both the ordering of MSDUs and avoid packet loss on re-association. Consider a station which is associated with an AP that has buffered MSDUs for it. That station associates with some other AP, and the DS immediately routes MSDUs via the new AP before the old AP has received notification of the deassociation and while it still holds buffered MSDUs.
3.1.1.2.	Fischerma:Time-bounded services	T	...Time bounded services shall not be interrupted for more than X microseconds when a station reassociates with a new access point in its current ESS...	Current wording indicates that NO interruption is allowed during reassociation. Since this condition, read literally, means that ZERO dropped frames, & ZERO additional latency & ZERO change in throughput is required in order to be conformant, no real system could meet this portion of the specificaiton as worded. Wording needs to include a realistic limit in order to insure consistency of quality of service throughout conformant devices.
3.1.1.3	CHRIS ZEGELIN		DELETE THE SENTENCE THAT SAYS " ALL IMPLEMENTATIONS OF 802.11 SHALL PROVIDE FOR ENCIPHERMENT OF DATA USING THE DEFAULT ALGORITHMS"	TILL THE WHOLE MECHANISM OF KEY MANAGEMENT IS RESOLVED, IT IS NOT POSSIBLE TO REQUIRE ENCIPHERMENT.
3.1.1.3	CHRIS ZEGELIN		THE PICTURE IS INCONSISTENT WITH THE WEP ALGORITHM SHOWN LATER AND USES TERMS THAT ARE NOT DEFINED. FURTHER THERE ARE OPTIONS SHOWN WITH NO DEFINITION OF WHEN THEY ARE USED. THIS WHOLE DRAWING SHOULD BE DELETED FROM THE TEXT TILL ALL THE INCONSISTENCIES WITH THE SECURITY PROVISIONS ARE WORKED OUT.	THERE IS INSUFFICIENT CLEAR DETAIL TO IMPLEMENT THE SECURITY PROVISIONS. THEY CURRENTLY CONFUSE MORE THAN HELP.
3.1.1.3	A. Bolea	E	reference to section 2.4 should be to section 2.9 (or figure 2-11)	
3.1.1.3	Glen Sherwood	E	Error in Figure 3-1: the SDE_SDU right bracket should point back to the right edge of the Data field.	SDE_SDU is the data in the SDE_PDU frame.
3.1.1.3	Jim Panian	E	Describe how access control works in conjunction with layer management.	
3.1.1.3	Joe Kubler	E	default encipherment algorithm is Wired Equivalency Privacy (WEP) section 5.4	
3.1.1.3	MLT	E	'[2] describes five parts ...' --- only four parts are listed in this sentence	
3.1.1.3	Rick White	E	Reference Model is shown in Section 2.9 not 2.4.	
3.1.1.3	A. Bolea	T		The default encipherment algorithm needs to be specified. In addition it is not clear whether encipherment is optional or not. I recommend that it be optional since not all applications are transmitting sensitive data.

3.1.1.3	Bob O'Hara	T	Delete all of 3.1.1.3	If security services are to be provoded by 802.10, this section is not needed. All security will already have been done above the MAC (where 802.10 lives).

3.1.1.3	David Bagby	T	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(s) are for further study.~~ The 802.11 document should not attempt to duplicate the contents of other standards documents, thus I have removed the excerpts from 802.10 and left the relevant references.  ~~**Figure 3-1: Structure of SDE_PDU**~~ ~~Note 1 - The enciphered data may include expansion and/or cryptographic information.~~	See imbeded comments and annotations

3.1.1.3	Geiger	T	encryption option	
3.1.1.3	Miceli	T	must supply the default encipherment algorithm	needed for interoperabilty
3.1.1.3	Renfro	T		If all users must support encipherment of MSDU payload, then default algorithm must be defined.
3.1.1.3	Rick White	T	States that minimum service offered by 802.11 is encipherment but earlier in draft it states encryption is optional. Must be resolved.	
3.1.1.3	Rick White	T	Paragraph 5 states that encipherment is required but earlier in draft states that it is optional Must be resolved.	
3.1.1.3	Wim Diepstraten	T	If we use authentication services provided by 802.10 SDE, as specified under bullet item 2, why do we then need to support this in the MAC?	
3.1.1.3 and 2.8	Fischer, Mike.	T	Add the following regarding 802.10 subset: The use of the 802.10 subset for privacy is optional. If privacy (WEP) is in use, that fact is indicated by a bit in the frame header. When this bit is set, the algorithm number, from the list of (initially 1) algorithm(s) supported by 802.11 for WEP, is indicated as part of the IV (see section 5.4). Privacy only applies to the MSDU, not to the MAC header nor CRC. When MSDUs are fragmented, the privacy algorithm is applied to the MSDU before fragmentation, and validated on the MSDU after reassembly. When privacy is in use, data frames are always encrypted, control frames are never encrypted, and management frames are never encrypted other than as needed for authentication. If the ICV of an encrypted data frame does not check, the existence of the MSDU shall not be indicated to the LLC at the receiving station, and the contents of the MSDU shall not be passed to the LLC. The 802.10 SDE settings for 802.11 WEP shall be: clear header length = 0, protected header length = 0, pad = none, and ICV = 32 bits. The data field shall include a 32Ðbit IV field immediately preceding the MSDU. This field shall contain an 8Ðbit privacy algorithm number followed by a 24Ðbit initialization vector value. The length of the IV field is never less than 32 bits. If the designated algorithm requires an IV longer than 24 bits, a longer IV field may be used, subject to the restriction that the IV must always contain an even number of octets. There shall be an ESSÐwide, default key to permit implict authentification and lowÐoverhead mobility transitions. Any station in possession of the default key is considered to be preÐauthenticated. Stations may, optionally, maintain receive privacy tables that associate stationÐspecific, nonÐdefault keys with station addresses. The default key is used in cases where this table not used and where the table has no station specific key corresponding to the source address of the received MSDU. The 802.10 SDE mechanism allows for more than one SDE entity to be operating in the same protocol stack. If a user chooses to deploy an SDE environment that requires SDE settings more comprehensive than those in the WEP subset, and/or based on an encryption algorithm not supported for the WEP function, that user may disable the WEP function, thereby avoiding the overhead of performing encryption and security processing twice on the same MSDU. This is consistent with the 802.10 model, in which lowerÐlayer SDE entities are generally disabled when higherÐlayer SDE entities are present. Replace figure 3Ð1 with one that shows the 802.10 subset listed above rather than the full generality of the 802.10 SDE_PDU. Replace the text after the first paragraph of 3.1.1.3 with a reference to 802.10 and its use above the MAC in cases where security functions beyond WEP are desired by a user of 802.11.	This embodies the recommendations made at the MAC group meeting on WEP held during the January, 1995 Interim Meeting. (The minutes of that meeting are document 95/06.)
3.1.1.3, 2.4.3.2,	Jim Panian	E	Specify privacy flows for the ad-hoc case where associations are not performed.	There is no description of privacy flows for the ad-hoc case.

3.1.1.4	Fischer, Mike.	T	replace this section with a reference to 802.10 for the full security model and to section 5.4 for the WEP process	We donÕt need to repeat 802.10 general mechanisms in 802.11. We only need to describe the portions of 802.10 that we use or provide SMIB compatibility with and to refer the reader to 802.10 for the more general version of the security model.
3.1.2	Jeff Rackowitz	E	Add notes about intentionally left blank or To be specified.	
3.1.2	McKown	E	this is a header with no text below it	typo
3.1.2	Mark Demange	t	Need to define reordering rules for MSDU's.	802.11 should allow MSDU reordering. This would allow an AP to go ahead and forward an MSDU to one device that is awake while another device that is asleep has it's MSDU buffered by the AP. This would also allow for the situation where one MPDU of an MSDU is in back-off due to poor coverage by the destination station while another MPDU of another MSDU is forwarded to a station that is in good coverage. However, MSDU reordering should not be allowed on a per destination basis since this could cause incompatibilities with existing NOS'.
3.1.2	Rick White	T	Must define what are the Service and Options.	There is no text or subsections to this section. Must define all basic data services (contention, contention-free, time bounded).
3.1.2.	Fischerma:Basic Services and Options	T	committee shall provide text	This section is empty. I do not know what the intention of the committee was in including this section and therefore am unable to provide the text necessary to correct the problem.
3.1.3	A. Bolea	E		It not clear what MA_UNITDATA stands for at this point in the text. It should be clearly specified or referenced to section 3.2.
3.1.3	Wim Diepstraten	E	Exchange MPDU by MSDU.	

3.1.3	David Bagby	T	**1. Reordering of MSPDUs** The para as written is factually incorrect. It is not possible for the MAC to guarantee ordering of MSDUs (MPDUs we could do) the unit_data request is at the top of the mac and therefore this para really ment the MSDU. Since MSDUs are sent thru a DS, and a DS *might* reorder MSDUs, we can not guarantee MSDU order within the 802.11 MAC. Therefore the para must be replaced by: 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.~~ [DB4]	See imbeded comments and annotations
3.1.3	Rick White	T	The MAC must be able to handle more than one outstanding frame.	This indicates that there can only be a single outstanding frame in the MAC. This could be a very sever performance problem for an AP. If an AP is having a problem (retransmission) sending a frame to a STA, this will impact the traffic to all other STAs within the BSS. This must be resolved, i.e., MAC must handle multiple frames if in the process of retransmitting a frame.
3.1.3	Wim Diepstraten	T	Sinse privacy is optional, there should be an indication in the MAC Header as to whether privacy has been applied. It should be made clear which fields are used by the 802.11 WEP. These settings and other WEP aspects should follow the recommendations as discussed during the January MAC meeting and documented in the minutes IEEE P802.11-95/06. It should be made clear that the 802.11 SDE uses an ESS wide security association, and not a station to station association.	The WEP privacy provisions should be more embedded in the 802.11 MAC independent of 802.10. The main difference is that the WEP should assume a ESS wide security association to allow ESS wide roaming. The approach should allow for efficient implementation so as to promote its use as much as possible. As a default an approach should be used that does allow a SW implementation on the MSDU level, aswell as a "on-the-fly" implementation on a per fragment basis.
3.1.4	CHRIS ZEGELIN		THIS SECTION CONTAINS DETAILS ABOUT THE WORKINGS OF THE SECURITY SERVICE THAT IS INAPPROPRIATE FOR SECTION 3.	MOST OF THIS INFORMATION BELONGS IN SECTION 5.4 WITH THE WEP ALGORITHM. ALTERNATIVELY A NEW MAJOR SECTION COULD BE DEDICATED TO THE SECURITY SERVICE.
3.1.4	Glen Sherwood	E	Don't know--can't figure out what it is trying to say (last par. on pg. 41).	Unreadable.

3.1.4	Jim Panian	E	Align this text with the Clause 2.4 , Overview of the Services (Association, Access and Confidentiality Control Services).	"During the association exchange, parties A and B exchange attribute values of the security managed objects defined in IEEE 802.10 SDE. These values specify the security parameters (e.g. algorithm, key, etc.,) that will be needed for the association." Is this text out of date?
3.1.4	Joe Kubler	E	figure 3-3 and 3-4, CRC should be ICV	
3.1.4	MLT	E	the next to last sentence on page 41 is very difficult to understand -- maybe should read as 'During the association exchange, parties A and B exchange the attribute values of the security association managed objects defined in IEEE 802.10 SDE [2].'	
3.1.4	bdobyns	T	This disagrees with 4.4.5 about the length of Station ID. Here it is arbitrarily long, e.g. 48 bits, but in 4.4.5 it is 16 bits.	
3.1.4	Bob O'Hara	T	Delete all of 3.1.4	If security services are to be provoded by 802.10, this section is not needed. All security will already have been done above the MAC (where 802.10 lives).
3.1.4	David Bagby	T	~~2. Security Service~~ <<< entire section removed >>>> could not show in this table as WORD refuses to do the paste from the review documnet!.	See imbeded comments and annotations
3.1.4	Greg Ennis	T	Move the material from the end of paragraph 2 to the end of the section to Section 5 of the document.	This material is not describing services but is describing mechanisms.
3.1.4	Marvin Sojka	T	Remmove Section 3.1.4. This information is covered in 802.10 and should not be reexplained/ specfiied in the 802.11 standard.	
3.1.4	Rick White	T	MAC must provide some level of privacy independent of 802.10 and its overhead. i.e., 802.11 must have a "built-in" privacy that can be turned on / off. If a user requires more privacy/security, then 802.10 is used above 802.11.	Customers will require privacy on their WLANs. They will not what to be required to use another standard to implement it.
3.2	Bob O'Hara	E	delete "_" from all "UNIT_DATA" occurrences	Proper standard language
3.2	Glen Sherwood	E	Define all protocol primitives before using. (see chap. 11 for examples).	Protocol primitives are not defined before being referenced. For example, what is MA_UNIT_DATA? How is it distinguished from MA_DATA described later?
3.2	Rick White	T	Management services must be defined	The Management Services are not defined. This only defines Data services. Management Service primitives must be defined.
3.2 (general), also 1.4	Fischer, Mike.	T	The service specification details should match those in section 2.2 of IEEE 802.2Ð1989 (ISO 8802Ð2) and this document should appear on the references list in 1.4	consistency with existing IEEE 802 standards of the adjacent protocol layer
3.2, 1.1, 2.4.2, 5.8	Jim Panian	T	Provide MAC service primitives to facilitate the three distribution system services: • Association • Reassociation • Disassociation - including the detection of link outage The above mentioned MAC service primitives will feed into the Association, Reassociation, and Disassocation services in the state machine descriptions as well.	Enough detail must be provided by the 802.11 standard to facilitate hand-off mechanisms on the distribution system.

3.2.1	Jeff Rackowitz	E	Sections 5.1.5, 5.1.7, 5.2.13.1.1 define MA_DATA.request and SM_MA.DATA.request and are not consitent with this section which defines MA_UNIT_DATA.-Request. There are either missing Primitives in this section or the other sections need to be corrected.	
3.2.1	Joe Kubler	T	priority/service_class should be enummerated since this is an external interface. If 802.2 defines this, then that reference should be made.	
3.2.1	Tim Phipps	T	*Change request to:* MA_UNIT_DATA.request(source_address, destination_address, data, priority/service_class, connection_id) *Add:* Connection_id shall specify the connection identifier for a connection based data transfer. Service_class shall distinguish between connection-based and non connection-based transfers.	Connection set up and data transfer have been specified, but the MAC user data request did not include a connection identifier, which is essential for a complete connection based data transfer service.
3.2.1, et seq	Bob O'Hara	E	change initial caps in ".Request", ".Indication" to lower case	Proper standard language
3.2.1.2	David Bagby	T	The semantics of the primitive are as follows: MA-UNIT_DATA-Request (source_address, destination_address, 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 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/service_class parameter specifies the priority/service_class desired for the data unit transfer~~.	See imbeded comments and annotations
3.2.1.2	Mark Demange	t	"2304 octets" should be changed to 16 K octets	Restricting MSDU to 2304 octets requires manufacturers to build source routing APs or to build a transparent bridge type AP and have customers manually configure a bridge elsewhere in the DS to negotiate 802.5 frame sizes down to a 2304 octets. Future higher data rate PHYs may also make it desirable to allow support for the larger 802.5 frames. 802.3 frames are acceptable using the current spec of 2304 octets.
3.2.1.2	Rick White	T	Must resolved editor's comments related to priority and service class	

3.2.1.2	Tim Phipps	T	*Change:* "...or equal to 2304 octects", *To:* "...or equal to 2304 octects, **not including any 802.10 SDE overhead**",	It needs to be said whether the limit applies above the MAC, but below the notional 802.10 SDE layer, or above them both.
3.2.1.2	Wim Diepstraten	T	The service specification should be upward compatible with the 802.3 and Ethernet specification, so that a 802.11 MAC can run under a 802.3 and ethernet protocol stack. This requires the support of the 802.3 Length field, then can also be used to convey the Ethernet "type" field. This will also impact the MAC Header specification in section 4.	It will be very important for the market acceptance of the 802.11 standard that compatibility with existing higher layer protocol stacks (LLC and above) can be achieved, so that the MAC can directly be used with current implementations of LLC and higher.
3.2.1.2, 4.1.2.5	bdobyns	T	Requires explanation of source for 2304 as a value. e.g. $2304 = \left(\frac{7!}{2} - 6^3\right)$ where: 7 = the number of drafts of the standard before final approval 6 = the number of years to approve the standard 3 = the number of PHY types in the standard 2 = the maximum data rate the standard actually supports	another possible explanation is: $2304 = \left(\frac{2^5 + 2^6}{2}\right)^2$
3.2.1.2, last sentence, also 3.2.2.2, last sentence	Fischer, Mike.	T	The priority and service class are 2 separate parameters in 802.2. Here the statement on allowable parameter values should be more specific, as there are only two priorities currently defined (contentionÐbased and contentionÐfree) and two service classes (asynchronous data and timeÐbounded data).	There is no reason to omit the details for priority and service class when stating the details for SA, DA, and MSDU length restrictions.
3.2.1.2, source address	Fischer, Mike.	T	The inclusion of and LLCÐspecified SA in this service primitive is necessary due to the corresponding definition in 802.2. However, if possible we should add the statement either Òthe SA shall specify the individual MAC sublayer entity address of the MAC entity to which the request is madeÓ or Òthis SA shall be replaced in the MPDU(s) resulting from this request with the individual MAC sublayer entity address of the MAC entity to which the request is made.Ó	The 802.11 authentication, privacy, association, distribution and integration services (and duplicate frame filtering at the MAC receiver) are based on the existence of a set of Sas that can be assumed to be fixed identifiers of particular stations. Allowing an LLC entity to set another value that gets used in the SA of a frame transmitted by the MAC is potentially very dangerous. Unless 802 global rules forbid our placing one of these constraints on the SA, I suggest strongly that we do so.
3.2.2	Tim Phipps	T	*Change indication to:* MA_UNIT_DATA.indication(source_address, destination_address, data, reception_status, priority/service_class, connection_id) *Add:* Connection_id shall specify the connection identifier for a connection based data transfer. Service_class shall distinguish between connection-based and non connection-based transfers.	Connection set up and data transfer have been specified, but the MAC user data indication did not include a connection identifier, which is essential for a complete connection based data transfer service.
3.2.2.2	A. Bolea	T		The reception status parameter seems like it has no use. it is used to indicate whether the frame was correctly received or not, however in paragraph 3.2.2.3 it states that the indication is not generated if the message is not received correctly. It would seem that the reception status would always be set to success.

3.2.2.2	David Bagby	T	The semantics of the primitive are as follows: MA_UNIT-DATA-indication (source_address, destination_address, 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 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/service_class parameter specifies the priority/service_class desired for the data unit transfer~~.	See imbeded comments and annotations
3.2.2.2.	Fischerma:Semantics of the Service Primitive (MA_UNIT_DATA-indication)	T	delete all references to the "reception_status" parameter.	In section 3.2.2.3., it is sstated that 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." This implies that "reception_status" will always indicate "success", therefore, the "reception_status" parameter is unneeded.
3.2.2.3	Jon Rosdahl	T	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 and their destination address designates the local MAC sublayer entity.	Removed the "received without error" phrase to make it be consistent with 3.2.2.2 whereit states that the reception_status parameter indicates the success or failure of the incoming fram Either this change needs to be made, or the reference to the reception_status parameter needs to be omitted, like it is in the 802.2 spcification, and the original sentance here would match what is in 802.2. Consistency.
3.2.2.3, last sentence	Fischer, Mike.	T	replace with ÒFrames 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.	Specify the point at which WEP imposes privacy Ñ not reporting MSDUs with ICV failures to LLC. Also, 802.2 has requested that for some applications (e.g. multimedia audio/video streams) it is better to have erroneous data than no data and wishes to receive frames with errors. I believe a case can be made that the wireless PHYs will tend to loose frames, not a few bits here and there, so the reporting of erroneous receptions is a poor idea because even when they are detected, there is a good chance no station will be able to reliably decode the frame addresses. If this is true, we should resist providing the passÐwithÐerrors that 802.2 would like to have.

3.2.2.4	Geiger	T	Effect of Receipt The effect of receipt by the LLC sublayer is unspecified	We are defining the MAC not the LLC. The MAC doesn't care what the LLC does with the MA_UNIT-DATA.indicate
3.2.3	Bob O'Hara	E	move all of this paragraph and its subparagraphs to section 5	doesn't belong here
3.2.3	David Bagby	E	**3. Access Point Initiates Connection Set-up** is this for CF data? if so change all language to indicate optional nature... where does this go? it seems not to fit here.	See imbeded comments and annotations
3.2.3	Jeff Rackowitz	E	This section seems to be out of place. Does it belong in the Detailed Service Specification section? Seems like it should be listed in section 5.3.	
3.2.3	Rick White	E	Contention-Free is out of place in Section 3.2 which defines the Primitives.	If Contention-Free is part of 3.2, so should Contention and Time Bounded.
3.2.3	Wim Diepstraten	E/T	Clarify that Contention free Connections are optional in 802.11. The distinction between connectionless and Connection oriented service classes needsto be clarified. The relation to the LLC interface specification is also unclear. It should be made clear how the connection procedure is invoked by an LLC.	
3.2.3	Fischer, Mike.	T	There should be drawings of the exchanges between LLC and MAC (in addition to) the drawings regarding AP/STA exchanges, as well as listings of the LLC parameter settings needed to initiate a connection request, end a connection, etc.	This is a section on MAC services, not the air interface.
3.2.3	Tim Phipps	T	*Add:* MA_CONNECTION_START.request(maximum MSDU size, normal request interval) MA_CONNECTION_END.request(connection_id) MA_CONNECTION_END.indication(connection_id) MA_CONNECTION_GRANT.indication(connection_id) MA_CONNECTION_NOT_GRANTED.indication()	These MAC User requests and indications are referred to but not specified.
3.2.3, general	Fischer, Mike.	T	The section should state that connection setup is done once per association with an ESS, and is maintained across BSSÐtransitions (reassociations) but must be reestablished if a disassociation occurs (either due to explicit disassociation or timeout).	This makes an aspect of reassociation that is currently implicit very explicit in an area where improper understanding of the intent could lead to nonÐinteroperable implementations.
3.2.3.1	Glen Sherwood	E	Make terminology consistent with diagrams.	Inconsistent terminology. Is "Start Connection Request" the same as "Request Connection" in the diagram following?
3.2.3.1	Fischer, Mike.	T	The restriction in the ÒNoteÓ should be removed for APÐinitiated stations, or reworded to quantify the timeout and to identify the possibility that a connection request made by an AP on behalf of an entity on the DS may be rejected because other requests took too much time to process. If there is reason to retain this note (which there may be), there should be a result of Òconnection not requested due to traffic congestionÓ that can be indicated back to the requester.	To enforce a strict sequential processing on connection requests leaves the possibility that requests from the DS may never reach the intended recipient in time, leading to amibiguity over the reason for connection failure.
3.2.3.1	Mark Demange	t	"connection set up time-out" is undefined anywhere else in the draft. This needs to be defined and have a value assigned to it.	Undefined values for necessary variable is inappropriate for a standard.

3.2.3.2	Mark Demange	t	"connection set up time-out" is undefined anywhere else in the draft. This needs to be defined and have a value assigned to it.	Undefined values for necessary variable is inappropriate for a standard.
3.2.3.3.	Mahany	E	Show Acknowledges in Figures.	Readability