IEEE 802.11
Wireless Access Method and Physical Layer Specifications

Title: Proposed Updates to the D1.1 Draft, Sections 2, 3, 4 & 5 -- Security (WEP)

Author:
Dave Bagby
AMD
Email: david.bagby@amd.com

Other contributors:
Michael Fischer
Leon Scaldeferri
Tom Siep

Abstract: **This paper proposes changes to the D1.1 Draft to reflect the resolution of comments made during the May 95 meeting.**

Action: **Adopt the changes in this paper to update the relevant portions of P802.11/D1.1**

Description:

The following extracts from the D1.1 Draft have been modified to reflect changes made as a result of letter ballot comments on Wire Equivalency Privacy (WEP). See doc 95/112 for the comments addressed.

Section 2

Removal of 802.10 references. This section was distributed as document 95s124.

Section 3

This document contains onlyl the WEP changes for sections 3. Distributed at the May meeting as D95s3.doc. **This portion of the document should be superceeded by 95/102**, which has all of these changes plus others made for readability, completness, and notation of required text to be added.

Section 4

This section contains editor notes for changes needed for sec4 of D1.1. I believe that the actual text changes for sec 4 have been incorporated into the sec 4 file Simon Black is creating for D1.2.

Section 5

Subsection 5.4 (WEP) has been deleted so that its contents may be incorporated in a new section. No other changes for section 5 are reflected in this document.

1.

2. General Description

2.1. Architecture General Description

This section presents the concepts and terminology used within the 802.11 standard. Specific terms are defined in section 1. Illustrations convey key 802.11 concepts and the interrelationships of the architectural components. 802.11 uses an architecture to describe functional components of an 802.11 LAN. The architectural descriptions are not intended to represent any specific physical implementation of 802.11.

2.1.1.How Wireless LAN Systems are Different

Wireless networks have fundamental characteristics which make them significantly different from traditional wired LANs.

2.1.1.1. Destination Address Does Not Equal Destination Location

In wired LANs an address is equivalent to a physical location. This is implicitly assumed in the design of wired LANs. In 802.11, the addressable unit is a station (STA). The STA is a message destination, but not (in general) a fixed location.

2.1.1.2. The Media Impacts the Design

The PHY layers used in 802.11 are fundamentally different from wired media. 802.11 PHYs:

a) Uses a medium that has neither absolute nor readily obsrevable boundaries outside of which stations with conformant PHY transcievers are known to be unable to receive network frames
b) Are unprotected from outside signals.
c) Are significantly less reliable than wired PHYs.
d) Have dynamic topologies.
e) The assuption normally made that every STA can hear every other STA is invalid as 802.11 PHYs lack full connectivity.

Because of limitations on wireless PHY ranges, wireless LANs intended to cover reasonable geographic distances must be built from basic coverage building blocks.

2.1.1.3. Impact of Handling Mobile Stations

One of the requirements of 802.11 is to handle *mobile* as well as *portable* stations. A *portable* station is one that is moved from location to location, but is only used while at a fixed location. *Mobile* stations actually access the LAN while in motion.

For technical reasons, it is not sufficient to handle only portable stations. Propagation effects blur the distinction between portable and mobile stations (stationary stations often appear to be mobile due to propagation effects).

Another inportant aspect of mobile stations is that they will often be battery powered and hence power management is an important consideration. For example, it cannot be presumed that a station's reciever will always be powered on.

2.1.1.4. Interaction with Other 802 Layers

One of the requirements of 802.11 is to handle *mobile* as well as *portable* stations. A *portable* station is one that is moved from location to location, but is only used while at a fixed location. *Mobile* stations actually access the LAN while in motion.

For technical reasons, it is not sufficient to handle only portable stations. Propagation effects blur the distinction between portable and mobile stations (stationary stations often appear to be mobile due to propagation effects).

Another inportant aspect of mobile stations is that they will often be battery powered and hence power management is an important consideration. For example, it cannot be presumed that a station's reciever will always be powered on.

2.2. 802.11 Architecture Components.

The 802.11 architecture consists of several components which interact to provide a wireless LAN that supports station mobility transparently to upper layers.

Some definitions from section 1:

Wireless Medium (WM): The medium used to implement a wireless LAN.

Station (STA): Any *device* that contains an 802.11 conformant MAC and PHY interface to the wireless medium.

Station Services (SS): The set of services that support transport of MSDUs between Stations within a BSS.

Coordination Function (CF). That logical function which determines when a station operating within a Basic Service Set transmits and receives via the wireless medium.

Basic Service Set (BSS). A set of stations controlled by a single Coordination Function. A BSS can have one PCF and one DCF.

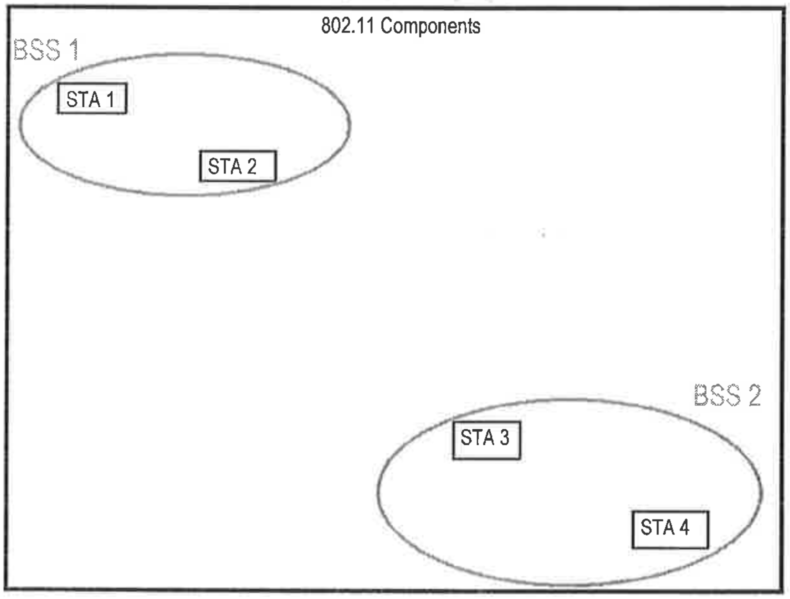


Figure 2-1: Basic Service Sets

The BSS is the basic building block of an 802.11 LAN. Figure 2-1 shows two BSSs, each of which has two stations which are members of the BSS.

It is useful to think of the ovals used to depict a BSS as the coverage area within which the member stations of the BSS can remain in communication. (The concept of area can lead one astray, and while not precise, is often good enough.) If a station moves out of it's BSS , it can no longer directly communicate with other members of the BSS.

2.2.1.The Independent BSS as an Ad-Hoc Network

The independent BSS is the most basic type of 802.11 LAN. A minimum 802.11 LAN can consist of only two stations.

Figure 2-1 shows two independent BSSs. This mode of operation is possible when 802.11 stations are able to communicate directly. Because this type of 802.11 LAN is often formed without pre-planning, for only as long as the LAN is needed, this type of operation is often referred to as an Ad-Hoc network.

2.2.1.1. STA to AP Association is Dynamic

The independent BSS is the most basic type of 802.11 LAN. A minimum 802.11 LAN can consist of only two stations.

Figure 2-1 shows two independent BSSs. This mode of operation is possible when 802.11 stations are able to communicate directly. Because this type of 802.11 LAN is often formed without pre-planning, for only as long as the LAN is needed, this type of operation is often referred to as an Ad-Hoc network.

2.2.2.Distribution System Concepts

PHY limitations determine the direct station to station distance which can be supported. For some networks this distance is sufficient, other networks require increased coverage.

Instead of existing independently, a BSS may also form a component of an extended form of network which is built with multiple BSSs. The architectural component used to interconnect BSSs is the Distribution System.

Distribution System (DS). A system used to interconnect a set of Basic Service Sets and integrated LANs to create an Extended Service Set.

Distribution System Medium (DSM). The medium used by a Distribution System (for Access Point interconnections).

802.11 logically separates the WM from the DSM. Each logical medium is used for different purposes, by a different component of the architecture. The 802.11 definitions neither preclude, nor demand, that the two media be either the same, or different.

Recognizing that the two media are *logically* different is key to understanding the flexibility of the architecture. The 802.11 LAN architecture is specified independently of the physical characteristics of any specific implementation.

The DS enables mobile device support by providing the logical services necessary to handle address to destination mapping and seamless integration of multiple BSSs.

Distribution System Services (DSS). The set of services provided by the distributions system which enable the MAC to transport MSDUs between stations that are not in direct communication with each other over a single instancfe of the WM. This includes transport of MSDUs between portals and BSSs within an ESS, and the transport of MSDUs between stations in the same BSS in cases where the station sending the MSDU chooses to involve DSS.

Access Point (AP). Any entity that has station functionality and provides access to the distribution services, via the WM for associated stations.

An AP is a STA which provides access to the DS by providing DS services in addition to acting as a Station.

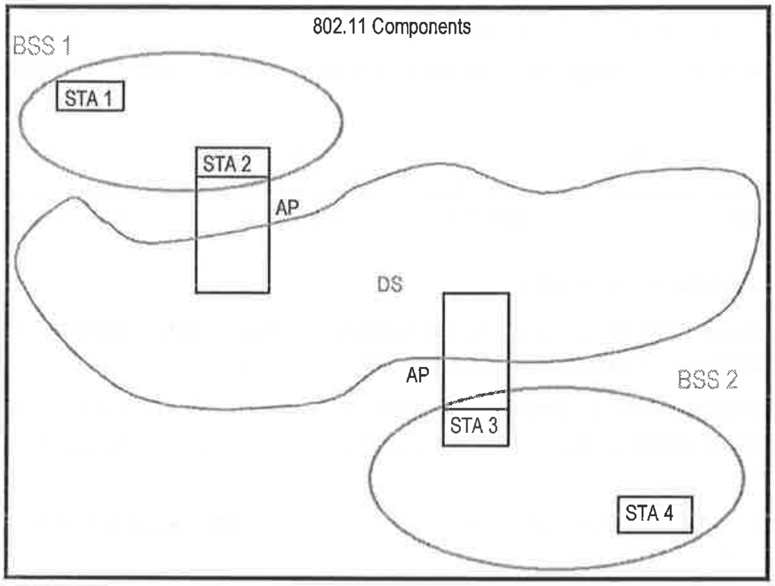


Figure 2-2: Distribution Systems and Access Points

Figure 2-2 adds the DS and AP components to the 802.11 architecture picture.

Data moves between a BSS and the DS via an Access Point (AP). Note that all APs are also STAs; thus they are addressable entities. The addresses used by an AP for sommunication on the WM and on the DSM are not necesarily the same.

2.2.2.1. ESS: The Large Coverage Network

The DS and BSSs allow 802.11 to create a wireless network of arbitrary size and complexity. 802.11 refers to this type of network as the ESS network.

Extended Service Set (ESS). A set of one or more interconnected Basic Service Sets and integrated LANs which appear as a single Basic Service Set to the logical link control layer at any station associated with on of those BSSs.

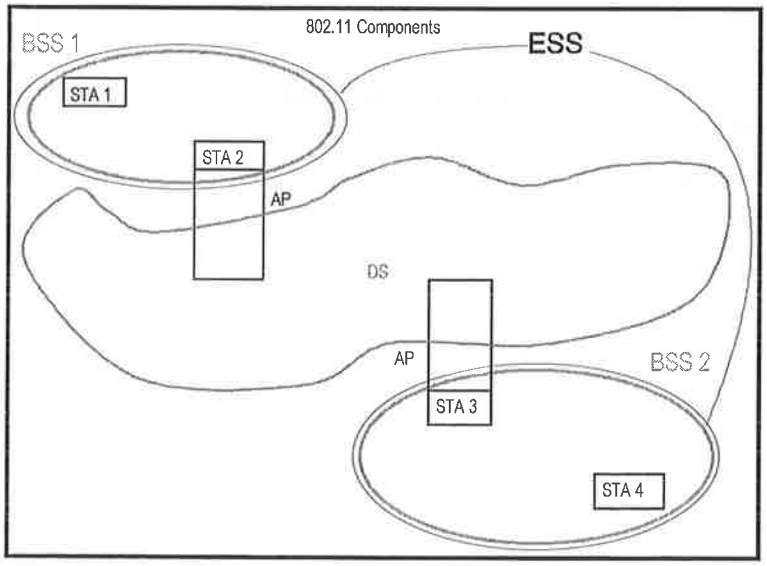


Figure 2-3: Extended Service Set

The key concept is that the ESS network appears the same to an LLC layer as an independent BSS network. Stations within an ESS can communicate and mobile stations may move from one BSS to another (within the same ESS) transparently to LLC.

Nothing is assumed by 802.11 about the relative physical locations of the BSSs in figure 2-3.

All of the following are possible:

a) The BSSs may partially overlap. This is commonly used to arrange contiguous coverage within a physical volume.

b) The BSSs could be physically disjoint. Logically there is no limit to the distance between BSSs.

c) The BSSs may be physically collocated. This might be done to provide redundancy.

d) One (or more) independent BSS, or ESS networks may be physically present in the same space as one (or more) ESS networks. This can arise for a number of reasons. Two of the most common are an Ad-hoc network is operating in a location which also has an ESS network and when physically adjacent 802.11 networks have been set up by different organizations.

2.2.3.Area Concepts

For wireless PHYs, well defined coverage areas simply do not exist. Propagation characteristics are dynamic and unpredictable. Small changes in position or direction can result in drastic differences in signal strength. Similar effects occur whether a station is stationary or mobile (as moving objects impact station to station propagation).

Figure 2-4 shows a signal strength map for a simple square room with a standard metal desk and an open door way. Figure 2-4 is a static snap shot, the propagation patterns change dynamically as stations and objects in the environment move. In figure 2-4 the red blocks in the lower left are a metal desk and there is a doorway at the top right of the figure. The figure indicates releative differences in field strength with different colors and indicate the variability of field strength even in a static environment.

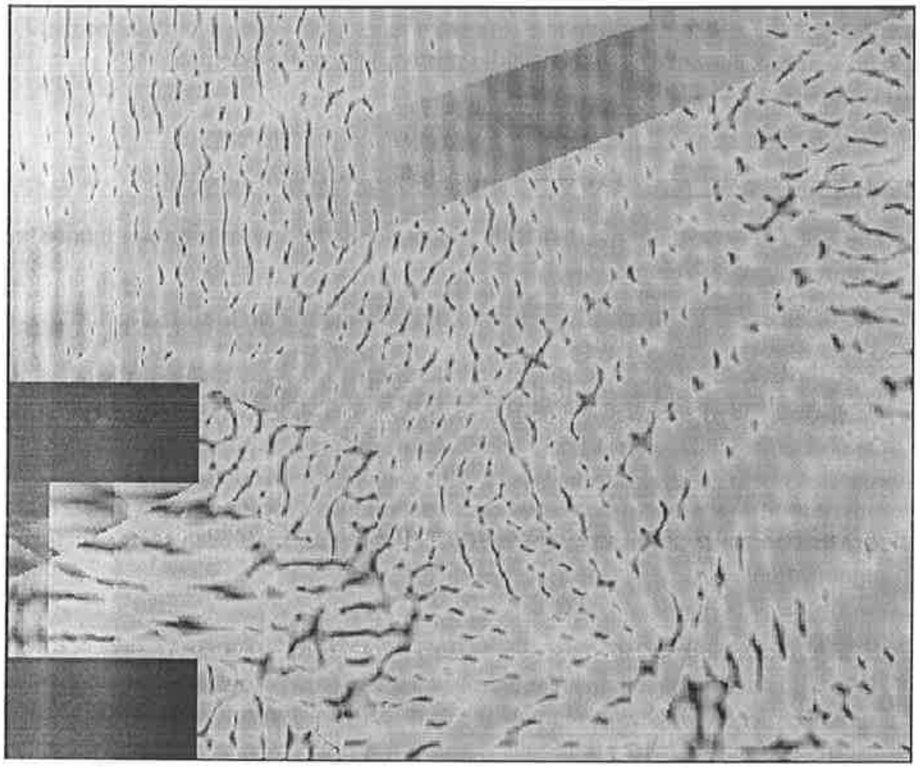


Figure 2-4: A Representative Signal Intensity Map

While the architecture diagrams show sharp boundaries for BSSs, this is an artifact of the pictorial representation, not a physical reality. Since dynamic three dimensional field strength pictures are difficult to draw, well defined shapes are used by 802.11 architectural diagrams to represent the coverage of a BSS.

Further description difficulties arise when attempting to describe collocated coverage areas. Consider figure 2-5, which BSS do stations 6 and 7 belong to?

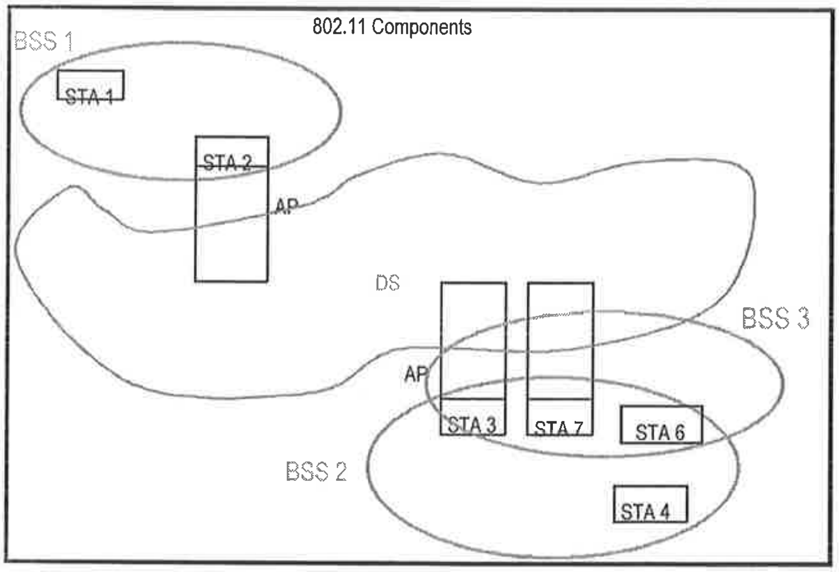


Figure 2-5: Collocated Coverage Areas

While sets of stations is the correct concept, it is often convenient to talk about areas. For many topics the concept of area is "good enough". Volume is a more precise term than area, though still not technically correct. For historical and convenience reasons the standard uses the common term "area".

The standard defines areas in terms of service sets.

Basic Service Area (BSA): The conceptual area within which members of a BSS can communicate.

Extended Service Area (ESA): The conceptual area within which members of an ESS can communicate. An ESA is larger than or equal to a BSA and may involve multiple, disjoint, BSAs

2.2.4.Integration with Wired LANs

To integrate the 802.11 architecture with a traditional wired LAN, a final *logical* architectural component is introduced; a "Portal".

Data from a wired LAN enters the 802.11 architecture via a Portal into the DS. The Portal is shown in figure 2-6 connecting to a wired 802 LAN.

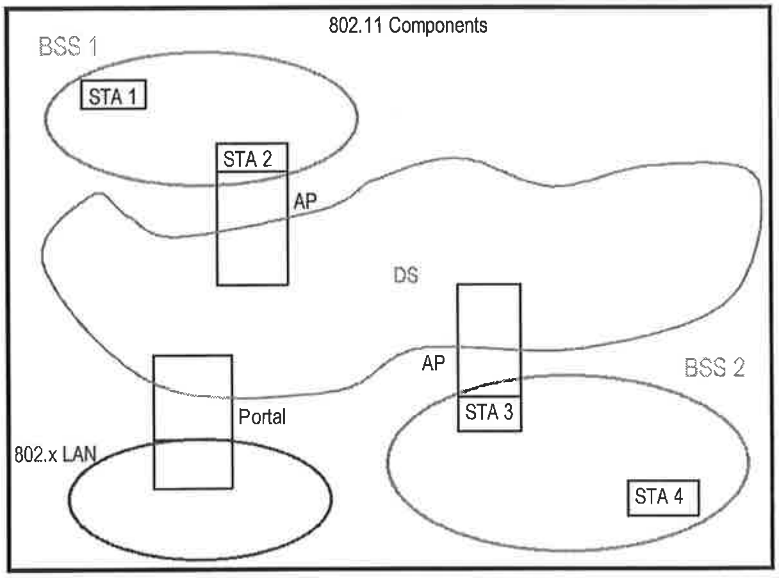


Figure 2-6: Connecting to Other 802 LANs

All data from non-802.11 LANs enters the 802.11 architecture via a Portal. The Portal provides logical integration between the 802.11 architecture and existing wired LANs. It is possible for one device to offer both the functions of an Ap and a Portal; this could be the case when a DS is implemented from 802 LAN components.

2.2.4.1. Portals and Bridges

As the 802.11 architecture contains more than one distinct logical medium, it is possible to become confused when comparing Portals with traditional 802 bridges.

Bridges were originally designed to provide range extension between like-type MAC layers. In 802.11, arbitrary range (coverage) is provided by the ESS architecture (via the DS and APs) making the PHY range extension aspects of bridges unnecessary.

Bridges (or bridge like devices) are also used to interconnect MAC layers of different types. Bridging to the 802.11 architecture raises the question of which logical medium to bridge to; the DSM or the WM?

Logical connections between 802.11 and other LANs are via the Portal. Portals connect between the DSM and the LAN media that is to be integrated. This is required by the unique aspects of 802.11 operation, particularly the dynamic membership of BSSs and the mapping of address and location required by mobility. Physically, a Portal may, or may not, include bridging functionality depending upon the physical implementation of the DS and the wired LAN.

2.3. Logical Service Interfaces

The 802.11 architecture allows for the possibility that the DS may not be identical to an existing wired LAN. A DS can be created from many different technologies including current 802.x wired LANs. 802.11 does not constrain the DS to be either Data Link or Network layer based. Nor does 802.11 constrain a DS to be either centralized or distributed in nature. This generality allows the 802.11 architecture to satisfy the diverse interests represented by the members of 802.11.

802.11 explicitly decided not to specify specific DS implementations. Instead 802.11 specifies services. The services are associated with different components of the architecture. There are two categories of 802.11 services; Station Services (SS) and Distribution System Services (DSS). Both categories of services are used by the 802.11 MAC layer.

The complete set of 802.11 architectural services are:

a) Authentication
b) Association
c) Deauthentication
d~~c~~) Disassociation
e~~d~~) Distribution
f~~e~~) Integration
g~~f~~) Privacy
h~~g~~) Reassociation

i~~h~~) MSDU delivery

This set of services is divided into two groups: those that are part of every station and those that are part of a distribution system.

2.3.1.Station Services

The services provided by stations are known as the Station Services.

Station Services (SS): The set of services which support transport of MSDUs between Stations within a BSS.

The Station Services are present in every 802.11 station (including APs; as APs include station functionality). Station Services are specified for use by MAC layer entities. All conformant stations provide Station Services.

The Station Services subset is:

a) Authentication
b) Deauthentication
c) Privacy

2.3.2.Distribution System Services

The services provided by the DS are known as the Distribution Systems Services (DSS).

These services are represented in the 802.11 architecture by arrows within the APs, indicating that the services are used to cross media and address space logical boundaries. This is the convenient place to show the services in the picture. The physical embodiment of various services may or may not be within a physical AP.

Distribution System Services (DSS): The set of services provided by the DS which enable the MAC to transport MSDUs between BSSs within an ESS.

The Distribution System Services are provided by the Distribution System. They are accessed via a STA which also provides Distribution System Services. A station that is providing access to DSS is an AP.

The Distribution System Services subset is:

a) Association
b) Disassociation
c) Distribution
d) Integration
e) Reassociation

DS Services are specified for use by MAC layer entities.

Figure 2-7 combines the components from previous figures with both types of services to show the complete 802.11 architecture.

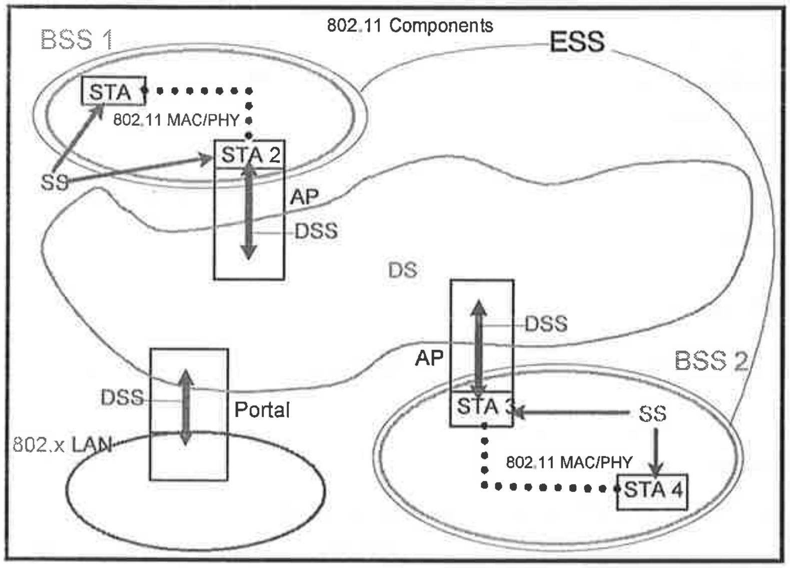


Figure 2-7: Complete 802.11 Architecture

2.3.3.Multiple Logical Address Spaces

Just as the 802.11 architecture allows for the possibility that the WM, DSM and an integrated wired LAN may all be different physical media, it also allows for the possibility that each of these components may be operating within different address spaces.

802.11 only uses and specifies the use of the WM address space.

Each 802.11 PHY operates in a single medium; the WM. The 802.11 MAC operates in a single address space. MAC addresses are localized to the WM in the 802.11 architecture. Therefore it is unnecessary for the standard to explicitly specify that it's addresses are "WM addresses". This is assumed throughout the 802.11 standard.

802.11 has chosen to use the IEEE 802 48 bit address space (see section 4). Thus 802.11 addresses will be compatible with, and unique within, the address space used by the 802 LAN family.

The 802.11 choice of address space implies that for many instantiations of the 802.11 architecture, the wired LAN MAC address space and the 802.11 MAC address space will be the same. In those situations where a DS which uses MAC level 802 addressing is appropriate, all three of the logical address spaces used within a system could be identical. While this is a common case, it is not the only combination allowed by the architecture. The 802.11 architecture allows for all three logical address spaces to be different.

A multiple address space example is one where the DS implementation chose to use network layer addressing. In this case the WM address space and the DS address space would be different.

The ability of the architecture to handle multiple logical media and address spaces is key to the ability of 802.11 to be independent of the DS implementation and to cleanly interface with network layer mobility approaches (e.g. Layer 3 mobility standards such as IETF mobile IP).

2.4. Overview of the Services

There are seven services specified by 802.11. Five of the services are used to support MSDU delivery between Stations. Two of the services are used to control 802.11 LAN access and confidentiality.

This section will introduce the various services, provide an introduction to how each service is used, and describe how it relates to the other services and the 802.11 architecture. The services are presented in an order designed to help build an understanding of the operation of an 802.11 ESS network. As a result, station services and distribution system services are intermixed in order (rather than being grouped by category).

Each of the services is supported by one or more MAC frame types. Some of the services are supported by MAC Management messages and some by MAC Data messages. All of the messages gain access to the WM via the 802.11 MAC layer media access methods specified in section 5 of the standard.

The 802.11 MAC layer uses three types of messages, Data, Management and Control (see section 4 frame formats). The Data messages are handled via the MAC data service path.

MAC Management messages are used to support the 802.11 Services and are handled via the MAC Management Service data path.

The examples in this section assume an ESS network environment. The differences between the ESS and the independent BSS network environments are provided separately at the end of this section.

2.4.1.Distribution of Messages Within a DS

2.4.1.1. Distribution

Distribution: The service which (by using Association information) delivers MSDUs within the DS.

This is the primary service used by 802.11 stations. It is conceptually invoked by every data message to or from an 802.11 station operating in an ESS when the frame is sent via the DS. Distribution is a Distribution System Service.

Refer to the ESS network in figure 2-7 and consider a data message being sent from STA 1 to STA 4. The message is sent from STA 1 and received by STA 2 (the "input" AP). The AP gives the message to the Distribution Service of the DS.

It is the job of the Distribution Service to deliver the message within the DS in such a way that it arrives at the appropriate DS destination for the intended recipient.

In this example the message is distributed to the STA 3 (the "output" AP) and STA 3 accesses the WM to send the message to STA 4 (the intended destination).

<u>How</u> the message is distributed within the Distribution System is not specified by 802.11. All 802.11 is required to do is to provide the DS with enough information for the DS to be able to determine the "output" point which corresponds to the desired recipient. The necessary information is provided to the DS by the three Association related (Association, Reassociation, and Disassociation) services.

The previous example was a case where the AP which invoked the Distribution service was different from the AP which received the distributed message. If the message had been intended for a station which was a member of the same BSS as the sending station, then the "input" and "output" APs for the message would have been the same.

In either example, the Distribution service was logically invoked. Whether the message actually had to traverse the physical DSM or not is a DS implementation matter and not specified by 802.11.

While 802.11 does not specify DS implementations, it does recognize and support the use of the WM as the DSM. This is specifically supported by the 802.11 frame formats. (Refer to section 4 for details).

2.4.1.2. Integration

Integration: The service which enables delivery of MSDUs between the DS and an existing network.

If the Distribution Service determines that the intended recipient of a message is a member of an integrated LAN, the "output" point of the DS would be a Portal instead of an AP.

Messages which are distributed to a Portal cause the DS to invoke the Integration service (conceptually after the Distribution Service). The Integration service is responsible for accomplishing whatever is needed to deliver a message from the DSM to the integrated LAN media (including any required media or address space translations). Integration is a Distribution System Service.

Messages received from an integrated LAN (via a Portal) by the DS for an 802.11 STA will invoke the Integration Service before the message is distributed by the Distribution Service.

The details of an Integration service are dependent on a specific DS implementation and are not further specified by 802.11.

2.4.2.Services Which Support the Distribution Service

The primary purpose of a MAC layer is to transfer MSDUs between MAC layer entities. The information required for the Distribution Service to operate is provided by the Association services. Before a data message can be handled by the Distribution service, a STA must be "Associated".

Before understanding the concepts of Association it is necessary to define mobility. There are three degrees of mobility defined by 802.11.

2.4.2.1. Mobility Types

There are three transition types of significance to this standard that describe the mobility of stations within a network:

a) ***No-transition:*** In this type, two-subclasses that are logically indistinguishable are identified:
   1) Static - no motion
   2) Local movement - movement within the PHY range of the communicating Stations (i.e. movement within a Basic Service Area).

b) ***BSS-transition:*** This type is defined as a station movement from one Basic Service Set in one Extended Service Set to another Basic Service Set within the same Extended Service Set.

c) ***ESS-transition:*** This type is defined as station movement from a Basic Service Set in one Extended Service Set to a Basic Service Set in an independent Extended Service Set. This case is supported only in the sense that the Station can move. Maintenance of upper layer connections cannot be guaranteed by 802.11, in fact disruption of service is likely to occur.

The different Association services support the different categories of mobility.

2.4.2.2. Association

Association: The service which establishes an initial Association between a station and an access point.

To deliver a message within a DS, the Distribution Service needs to know which AP to access for the given 802.11 STA. This information is provided to the DS by the concept of Association. Association is necessary, but not sufficient, to support BSS-transition mobility. Association is sufficient to support "no-transition" mobility. Association is a Distribution System Service.

Before a STA is allowed to send a data message via an AP, it must first become associated with the AP. The act of becoming associated invokes the Association service which provides the STA to AP mapping to the DS. The DS uses this information to accomplish it's message distribution service. How the information provided by the Association service is stored / managed within the DS is not specified by 802.11.

At any given instant, a STA may be associated with no more than one AP. This ensures that the DS can determine a unique answer to the question "which AP is serving STA X?" Once an association is completed, a STA may make full use of a DS (via the AP) to communicate.

An AP may be associated with many STAs at one time.

A station learns what APs are present and then requests to establish an association by invoking the Association Service.

For the details of how a station learns about what APs are present see section 7.xx on scanning.

Association is always initiated by the mobile STA.

2.4.2.3. Reassociation

Reassociation: The service which enables an established Association (of a STA) to be transferred from one AP to another AP (within an ESS).

Association is sufficient for No-transition message delivery between 802.11 stations. Additional functionality is needed to support BSS-transition mobility. The additional required functionality is provided by the Reassociation service. Reassociation is a Distribution System Service.

The Reassociation service is invoked to "move" a current association from one AP to another. This keeps the DS informed of the current mapping between AP and STA as the station moves from BSS to BSS within an ESS. Reassociation also enables changing association attributes of an established association while the STA remains associated the same AP.

Reassociation is always initiated by the mobile STA.

2.4.2.4. Disassociation

Disassociation: The service which voids an existing Association.

The Disassociation Service is invoked whenever an existing Association must be terminated. Disassociation is a Distribution System Service.

In an ESS this tells the DS to void existing association information. Attempts to send messages to a disassociated STA will be unsuccessful.

The Disassociation Service can be invoked by either party to an Association (STA or AP). Disassociation is a notification, not a request. Disassociation can not be refused by either party to the association.

APs might need to disassociate STAs to enable the AP to be removed from a network for service or for other reasons.

STAs are encouraged to Disassociate whenever they leave a network. However, the MAC protocol does not depend on STAs invoking the Disassociation service (MAC management always protects itself against STAs which simply die or go away).

2.4.3.Access and Confidentiality Control Services

Two services are required for 802.11 to provide functionality equivalent to that which is inherent to Wired LANs. The design of wired LANs assumes the physical attributes of wire. In particular wired LAN design assumes the closed, non-shared nature of wired media. The open, shared medium nature of an 802.11 LAN violates those assumptions.

Two services are provided to bring the 802.11 functionality in line with wired LAN assumptions; Authentication and Privacy. Authentication is used instead of the wired media physical connection. Privacy is used to provide the confidential aspects of closed wired media.

2.4.3.1. Authentication

Authentication: The service used to establish the identity of Stations to each other.

In a wired LAN it is generally assumed that access to a physical connection conveys authority to connect to the LAN. This is not a valid assumption for a wireless LAN. With a shared medium (that is not constrained by physical connection limitations), there is no equivalent to the wired LAN physical medium connection.

An equivalent ability to control LAN access is provided via the Authentication service. This service is used by all stations to establish their identity with stations they wish to communicate with. If a mutually acceptable level of authentication has not been established between two stations, an Association shall not be established. Authentication is a Station Service.

802.11 supports several ~~a general~~ authentication processes. The 802.11 authentication mechanism also allows expansion of the supported authentication schemes. ~~ability which is sufficient to handle authentication protocols ranging from "unsecured" to public key cryptographic authentication schemes.~~ 802.11 does not mandate the use of any particular authentication scheme.

802.11 provides link level authentication between 802.11 stations. 802.11 does not provide either end-to-end (message origin to message destination) or user-to-user authentication. 802.11 authentication is simply used to bring the wireless link up to the assumed physical standards of a wired link. (This use of authentication is independent of any authentication process that may be used at upper levels of a network stack.)

If desired, an 802.11 network can be run without authentication. 802.11 cautions against this as it may violate implicit assumptions made by higher network layers. This is referred to as an "Open System". In an Open System, anyone is allowed to become authenticated.

802.11 also supports shared key authentication. This is referred to as "shared key authentication". Use of this authentication mechanism requires implementation of the WEP option (see section X.X). In a shared key authentication system, identity is demonstrated by knowledge of a secret, shared WEP encryption key.

~~802.11 provides support for challenge / response (C/R) authentication. The three steps of a C/R exchange are:~~

~~a) Assertion of identity.~~
~~b) Challenge of Assertion.~~
~~c) Response to Challenge.~~

~~Examples of a C/R exchange are:~~

~~An open system example:~~
~~a) Assertion: I'm station 4~~
~~b) Challenge: null~~
~~c) Response: null~~
~~d) Result: Station becomes Authenticated.~~

~~A password based example:~~
~~a) Assertion: I'm station 4~~
~~b) Challenge: Prove your identity~~
~~c) Response: Here is my password.~~
~~d) Result: If password OK, station becomes Authenticated.~~

~~A Cryptographic challenge / response based example:~~
~~a) Assertion: I'm station 4~~
~~b) Challenge: Here is some information (X) I encrypted with your public key, what is it?~~

~~c) Response: The contents of the challenge is X (only station 4's private key could have recovered the challenge contents).~~

~~d) Result: OK, I believe that you are station 4.~~

~~Details of the usage of cryptographic authentication schemes are outside the scope of this standard.~~

~~A~~ Management Information Base (MIB) functions are~~is~~ provided to support ~~inquiries into~~ the standardized authentication schemes ~~authentication algorithms supported by a STA~~.

802.11 requires mutually acceptable, successful, ~~bi-directional~~ authentication.

A STA can be authenticated with many other STAs (and hence APs) at any given instant.

2.4.3.1.1. Pre-authentication

Because the authentication process could be time consuming (depending on the authentication protocol in use), the Authentication service can be invoked independently of the Association service.

Pre-authentication is typically done by a STA while it is already associated with an AP (which it previously authenticated with). 802.11 does not require that STAs pre-authenticate with APs. However, Authentication is required before an Association can be established.

If the authentication is left until Reassociation time, this may impact the speed with which a STA can Reassociate between APs, limiting BSS-transition mobility performance. The use of Pre-authentication takes the authentication service overhead out of the time critical Reassociation process.

2.4.3.2. Deauthentication

Deauthentication: The service which voids an existing Authentication.

The Deauthentication Service is invoked whenever an existing Authentication must be terminated. Deauthentication is a Station Service.

I~~i~~n an ESS, since Authentication is a prerequisite for Association, the act of Deauthentication can cause and explicit Disassociation.

The Deauthentication Service can be invoked by either authenticated party (mobile STA or AP). Deauthentication is not a request, it is a notification. Deauthentication can not be refused by either party.

2.4.3.3. Privacy

Privacy: The service used to prevent the contents of messages from being read by other than the intended recipient.

In a wired LAN only those stations physically connected to the wire can hear LAN traffic. With a wireless shared medium, this is not the case. Any 802.11 compliant adapter can hear all 802.11 traffic that it is within range of. Thus the connection of a single wireless link (without privacy) to an existing wired LAN may seriously degrade the security level of the wired LAN.

To bring the functionality of the wireless LAN up to the level assumed by wired LAN design, 802.11 provides the ability to encrypt the contents of messages. This functionality is provided by the Privacy service. Privacy is a Station Service.

802.11 uses the WEP mechanism (see section X.X) to ~~IEEE 802.10 SDE clause 2 to~~ perform the actual encryption of messages. ~~A~~ MIB functions are~~is~~ provided to support WEP.~~inquire the encryption algorithms supported by a station.~~

~~A mutually acceptable privacy algorithm must be agreed upon before an Association can be established.~~

Note that privacy may ~~is~~ only~~not~~ be invoked for Data frames and some Authentication Management frames.~~until the frame following the Privacy Response frame.~~ All stations initially start "in the clear" in order to set up the Authentication and Privacy services.

The default privacy state~~algorithm~~ for all 802.11 Stations is "in the clear". If the Privacy Service is not invoked ~~to set up a privacy algorithm~~, all messages will be sent unencrypted. If this~~e~~ default is not acceptable to one party or the other, Data frames will not be successful (they won't be acked)~~then the Association will fail.~~ .

~~If a privacy algorithm (default or otherwise) is set up, then that algorithm will be used for all subsequent Reassociations. Even if an Association is successful, a later Reassociation may be refused. This could occur if not all APs support the same privacy algorithms.~~

IEEE 802.11 specifies an optional privacy algorithm (WEP) that is designed to satisfy the goal of wired LAN "equivalent" privacy. The algorithm is not designed for ultimate security but rather to be "at least as secure as a wire". See section 5.4 for more details.

2.5. Relationships Between Services

As noted previously some services must be completed successfully before others can be invoked. This requires keeping track of two state variables for a station:

Authentication State:
The values are: Unauthenticated and Authenticated.
Association State:
The values are: Unassociated and Associated.

These two variables create three station states:

State 1:
Initial start state, Unauthenticated, Unassociated.

State 2:
Authenticated, not Associated

State 3:
Authenticated and Associated.

The relationships between these state variables and the Services are given by figure 2-8.

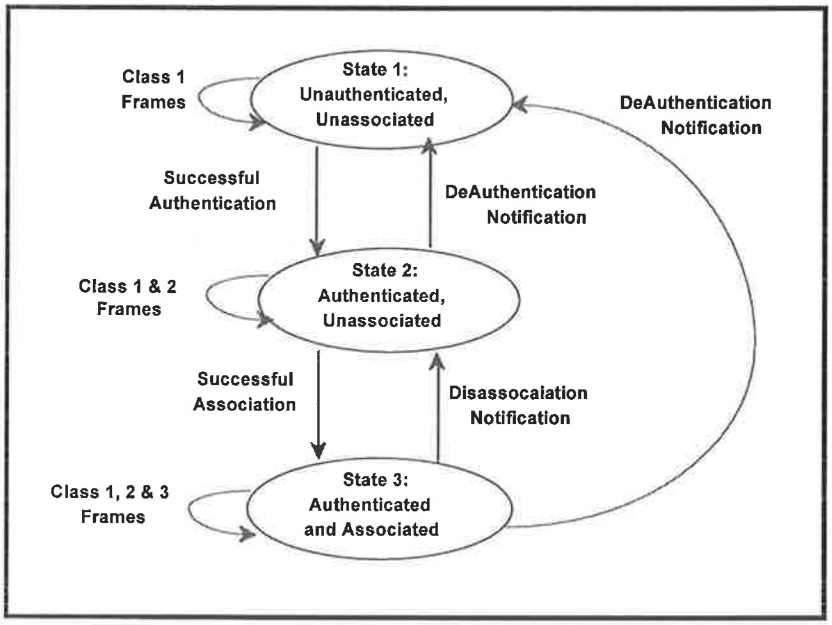


Figure 2-8: Relationship Between State Variables and Services

These states determine the 802.11 frame types which may be sent by a Station. The allowed frame types are grouped into classes and the classes correspond to the Station State. In State 1 only Class 1 frames are allowed. In State 2 either Class 1 or Class 2 frames are allowed. In State 3 All frames are allowed (Class 1, 2 and 3). The frame classes are defined as follows:

Class 1 frames (Legal from within States 1, 2 and 3):

a) Control Frames:
1) RTS
2) CTS
3) ACK

b) Management Frames:
1) Probe Request/Response
2) Beacon
3) Authentication
Successful Authentication enables a station to exchange Class 2 frames. Unsuccessful Authentication leaves the Station in State 1.

Class 2 frames (IFF Authenticated; allowed from within States 2 and 3 only):

a) Data frames:
1) Asynchronous data
Direct data frames only (FC control bits "To DS and From DS" both false).

b) Management frames:
~~1) Privacy Request/Response~~
1~~2~~) ATIM
2~~3~~) Association R/R
Successful Association enables Class 3 frames.
Unsuccessful Association leaves STA in state 2.
34) Deauthentication

Class 3 frames (IFF Associated; allowed only from within State 3):

a) Data frames:
1) Asynchronous Data
Indirect Data frames allowed. I.e. the "To Ds" and "From DS" FC control bits may be set to utilize DS Services.

b) Management frames:
1) Reassociation Request/Response
2) Disassociation
Disassociation notification changes a Stations state from 3 to 2. Thus a Station must become Associated again if it wishes to utilize the DS.
3) Deauthentication

c) Control frames:
1) CF END
2) Poll

2.6. Differences Between ESS and Independent BSS LANs

In section 2.2.1 the concept of the independent BSS LAN was introduced. It was noted that an independent BSS is often used to support an "Ad-Hoc" network. In an independent BSS network, a STA communicates directly with one or more other STAs.

The independent BSS LAN is a logical subset of an ESS LAN.

Consider the full 802.11 architecture as shown in figure 2-9.

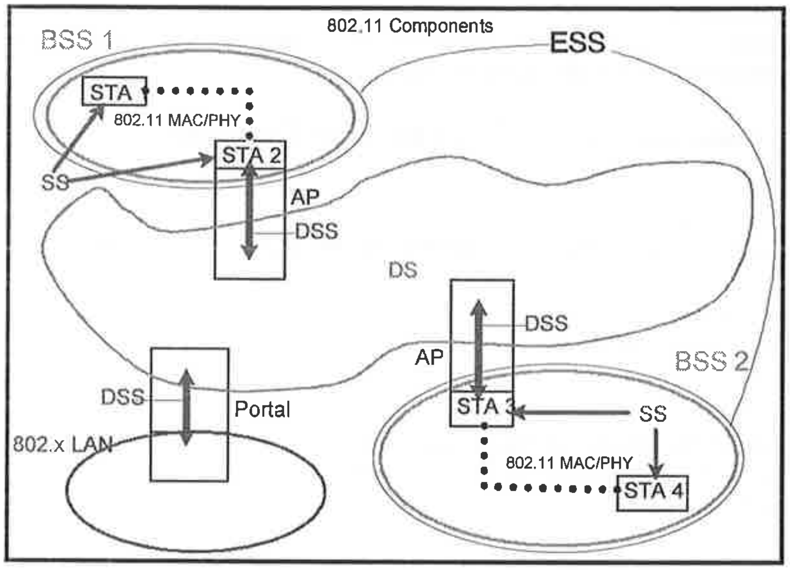


Figure 2-9: 802.11 Architecture (again)

An independent BSS consists of STAs which are directly connected. Thus there will (by definition) only be one BSS. Further, since there is no physical DS, there cannot be a Portal, an integrated wired LAN, or the DS services. The logical picture reduces to figure 2-10.

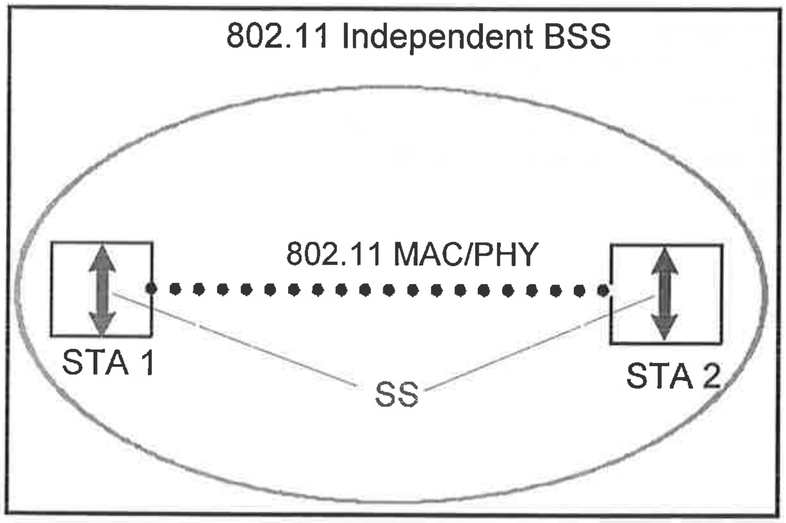


Figure 2-10: Logical Architecture of an Independent BSS

Only the minimum two stations are shown in figure 2-10. An IBSS can have an arbitrary number of members. In an IBSS, only class 1 and class 2 frames are allowed since there is no DS in an IBSS.

The Services which apply to an independent BSS are the Station Services.

2.7. Message Information Contents That Support the Services

Each Service is supported by one or more 802.11 messages. This section specifies the information items which must be present in the messages to support the service.

Information items are given by name, for corresponding values, see section 4.

2.7.1.Data Distribution

When a Station wishes to send data to another Station it sends a Data message. In the ESS the message will be handled by the Distribution Service.

Data Messages

- Message type:
  - Data
- Message sub-type:
  - Asynchronous Data
- Information Items:
  - IEEE source address of message.
  - IEEE destination address of message.
  - BSS ID
- Direction of message:
  - From STA to STA

2.7.2.Association

When a STA wishes to Associate, the Association service causes the following message to occur.

Association-request

- Message type:
  - Management
- Message sub-type:
  - Association-request
- Information Items:
  - IEEE address of the station initiating the association.
  - IEEE address of the AP the initiating station desires to associate with.
  - ~~Privacy algorithm number.~~
  - ESSID
- Direction of message:
  - From STA to AP.

Association-response

- Message type:
  - Management
- Message sub-type:
  - Association-response
- Information Items:
  - Result of the requested association. This is a fixed length item with values "successful" and "unsuccessful".
  - If the association is successful, the response shall include the SID
- Direction of message:
  - From AP to STA.

2.7.3.Reassociation

When a STA wishes to Reassociate, the Reassociation service causes the following message to occur.

Reassociation-request

Message type:
Management
Message sub-type:
Reassociation-request
Information Items:
IEEE address of the station initiating the reassociation.
IEEE address of the AP the initiating station desires to reassociate with.
IEEE address of the AP that the initiating station is currently associated with.
~~The current privacy algorithm number being used by the reassociating station. This is a fixed length field.~~
ESSID
Direction of message:
From STA to AP (The AP with which the STA is requesting reassociation.)

The address of the current AP is included for efficiency. The inclusion of the current AP address facilitates MAC reassociation to be independent of the DS implementation.

Reassociation-response

Message type:
Management
Message sub-type:
Reassociation-response
Information Items:
Result of the requested Reassociation. This is a fixed length item with values "successful" and "unsuccessful".
If the reassociation is successful, the response shall include the SID
Direction of message:
From AP to STA.

2.7.4.Disassociation

When a STA wishes to terminate an active association, the Disassociation service causes the following message to occur.

Disassociation

Message type:
Management
Message sub-type:
Disassociation
Information Items:
IEEE address of the station which is being disassociated.
IEEE address of the AP which the Station is currently associated with.
Direction of message:
From STA to STA (e.g. STA to AP or AP to STA).

2.7.5.Privacy

When two STAs wish to ~~negotiate and set up a~~ invoke the WEP privacy algorithm ~~for use~~ (as controlled by the related MIB variables, see section 7.X), the privacy service causes MSDU encryption and sets the WEP frame header bit apprpriately (see section 4.X)~~the following message sequence to occur~~.

~~In an independent BSS environment either station may be the initiating STA. In an ESS environment STA 1 would be the mobile STA and STA 2 would be the AP.~~

~~Privacy Request~~

~~Message type:~~
~~Management~~
~~Message sub-type:~~

~~Privacy Request~~

~~Information Items:~~

~~List of acceptable privacy algorithms supported. This is a variable length list of fixed length items.~~

~~Direction of message:~~

~~From STA 1 to STA 2.~~

~~Privacy Response~~

~~Message type:~~

~~Management~~

~~Message sub-type:~~

~~Privacy Response~~

~~Information Items:~~

~~Result of the requested privacy setup. This is a fixed length item with values "successful" and "unsuccessful".~~

~~The mutually supported privacy algorithm selected. This is a fixed length field. The contents of this field are valid only if the previous field contained the value "successful".~~

~~Direction of message:~~

~~From STA 2 to STA 1.~~

Note: ~~802.10 does not specify specific cryptographic algorithms for privacy. P802.11 has registered the following algorithms with 802.10:~~

~~**No Privacy Algorithm in use:** Value = ??~~

~~**Wired Equivalent Privacy (WEP) algorithm**: Value = ??~~

~~This satisfies the minimal operational needs of 802.11.~~

~~Additional privacy algorithms, which have been registered with 802.10 for use within 802.11 implementations, and were known at the time of publication are contained in appendix XX.~~

2.7.6.Authentication

When a ~~two~~ STA~~s~~ wishes to ~~mutually~~ authenticate with anouther STA~~each other~~, the authentication service causes one or more Authentication Management frames to be exchanged. The exact sequence of the frames and thier contents is dependent on the authentication scheme invoked.~~the following message sequence to occur.~~ For all authentiaciton schemes, the authentication algorithm is identified wihtin the Management frame body.

~~In an ESS environment STA 2 would be an AP.~~

In an independent BSS environment either station may be the initiating STA (STA 1). In an ESS environment STA 1 would be the mobile STA and STA 2 would be the AP.

~~In both cases, STA 2 had to have previously asserted it's identity as part of STA 1 finding out that STA 2 existed.~~

Authentication ~~(message 1)~~(First frame of sequence)

Message type:

Management

Message sub-type:

Authentication

Information Items:

Authentication Algorithm Identification.

Station Identity Assertion.

Authentication transaction sequence number.
Authentication algortithm dependent infromation.
~~List of acceptable authentication algorithms supported. This is a variable length list of fixed length items.~~

Direction of message:
First frame in the tranaciton sequence is always From STA 1 to STA 2.

The first frame is an authentication sequence shall always be unencrypted.

Authentication ~~(message 2)~~(intermediate sequence frames)

Message type:
Management

Message sub-type:
Authentication

Information Items:
Authentication Algorithm Identification.
Authentication transaction sequence number.
~~Identity assertion by STA 2.~~
~~Result of the requested authentication algorithm setup. This is a fixed length item with values "successful" and "unsuccessful".~~
~~The mutually supported authentication algorithm selected. This is a fixed length field. The contents of this field are valid only if the previous field contained the value "successful".~~
Authentication algortithm dependent infromation.

Direction of message:
Even transaction sequence numbers: from STA 2 to STA 1
Odd transaction sequence numbers: from STA 1 to STA 2
~~STA 2 to STA 1.~~

~~Authentication (message 3)~~

~~Message type:~~
~~Management~~

~~Message sub-type:~~
~~Authentication~~

~~Information Items:~~
~~Authentication transaction sequence number.~~
~~STA 1 Challenge of STA 2 identity assertion. This is a variable length item the contents of which are determined by the authentication algorithm selected.~~
~~STA 1 assertion of identity. This is the IEEE address of STA 1.~~

~~Direction of message:~~
~~STA 1 to STA 2.~~

~~Authentication (message 4)~~

~~Message type:~~
~~Management~~

~~Message sub-type:~~
~~Authentication~~

~~Information Items:~~
~~Authentication transaction sequence number.~~
~~STA 2 response to STA 1 challenge of STA 2's identity assertion. This is a variable length item the contents of which are determined by the authentication algorithm selected.~~
~~STA 2 challenge of STA 1 identity assertion. This is a variable length item the contents of which are determined by the authentication algorithm selected.~~

~~Direction of message:~~

~~STA 2 to STA 1.~~

~~Authentication (message 5)~~

~~Message type:~~

~~Management~~

~~Message sub-type:~~

~~Authentication~~

~~Information Items:~~

~~Authentication transaction sequence number.~~

~~STA 1 response to STA 2's challenge of STA 1's identity assertion. This is a variable length item the contents of which are determined by the authentication algorithm selected.~~

~~The result from STA 1 of STA 2's challenge response. This is a variable length item the contents of which are determined by the authentication algorithm selected.~~

~~Direction of message:~~

~~STA 1 to STA 2.~~

Authentication ~~(message 6)~~Final frame of sequence.

Message type:

Management

Message sub-type:

Authentication

Information Items:

Authentication Algorithm Identification.

Authentication transaction sequence number.

Authentication algortithm dependent infromation.

The result of the requested authentication. This is a fixed length item with values "successful" and "unsuccessful".

~~result from STA 2 of STA 1's challenge response. This is a variable length item the contents of which are determined by the authentication algorithm selected.~~

Direction of message:

STA 2 to STA 1.

~~Note: 802.10 does not specify specific cryptographic algorithms for authentication or privacy. However the algorithm numbers must be known for proper operation of 802.11. P802.11 has registered the following algorithms with 802.10:~~

~~No Authentication algorithm in use: Value = ??~~

~~This satisfies the minimal operational needs of 802.11.~~

~~Additional authentication algorithms which have been registered with 802.10 for use within 802.11 implementations and were known at the time of publication are contained in appendix XX.~~

2.7.7.Deauthentication

When a STA wishes to cancel an active authentication, the following message is sent.

Deauthentication

Message type:

Management

Message sub-type:

Deauthentication

Information Items:

IEEE address of the station which is being deauthenticated.

IEEE address of the AP which the Station is currently authenticated with.

Direction of message:

From STA to STA (e.g. STA to AP or AP to STA).

2.8. Reference Model

The standard presents the architectural view, emphasizing the separation of the system into two major parts: the MAC of the data link layer and the PHY. These layers are intended to correspond closely to the lowest layers of the ISO Basic Reference Model of OSI (ISO 7498 [1]).

<< editors please remove the box labeled "802.10b SDE in the followign figure - we did not have MSDRAW avail to do the edit - db>>

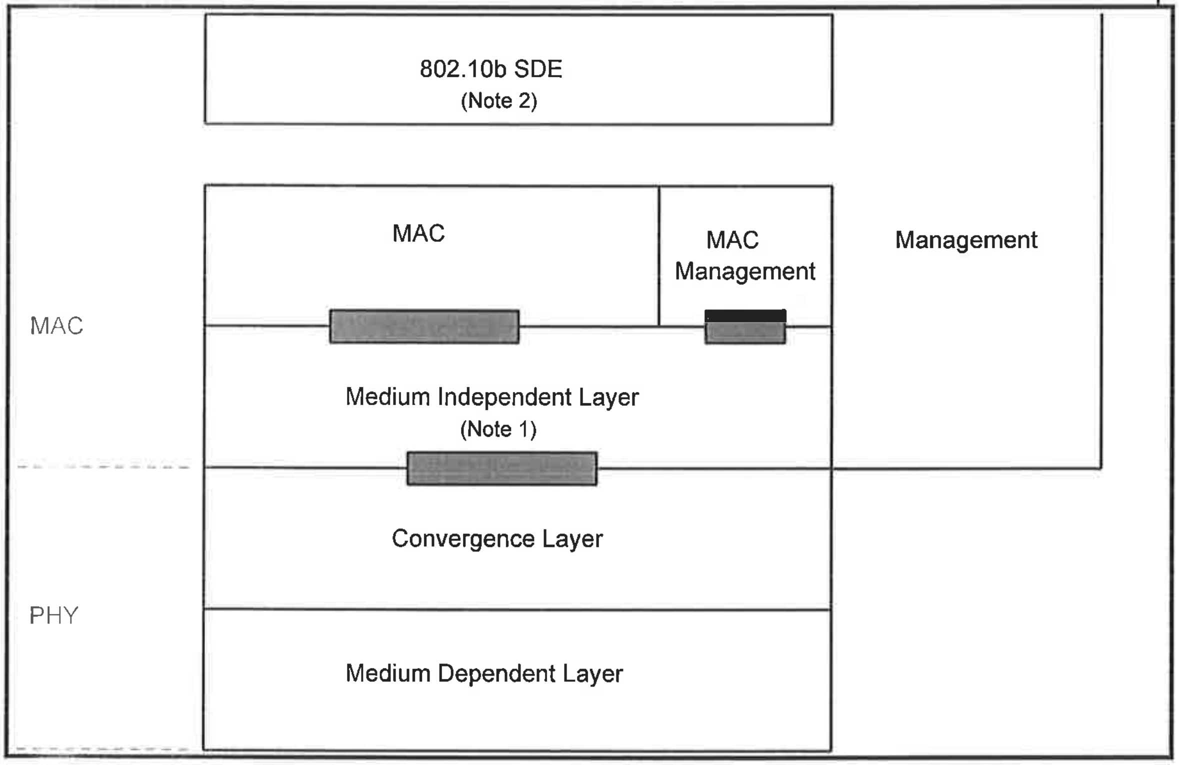


Figure 2-11, Portion of the ISO Basic Reference Model Covered in this Standard

>>> editor note - the interface shown in the above figure between MAC and Phy was supposed to have been removed as part of the April LB votes. Please correct the figure to remove this interface. <<<

~~Note 2 - 802.10 SDE: IEEE 802.10 - Secure Data Exchange [2]~~

2.9. Service Primitives

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.

3.1.1.3. Security Services

Security services in 802.11 shall be provided by the Wired Equivalency Privacy mechanism~~a subset of the service described in IEEE Std 802.10-1992, Secure Data Exchange (SDE), (clause 2) [2~~], hereafter referred to as WEP~~SDE~~. The scope of the security services provided is limited to Station-to-Station Data Exchange~~associations~~. The ~~minimum~~ privacy service offered by an~~y~~ 802.11 WEP implementation shall be the encipherment of the MSDU payload. For the purposes of this standard, the WEP~~SDE~~ 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 WEP~~SDE~~ sub-layer is considered transparent to the LLC or other layers above the MAC sub-layer.

The security services provided by the WEP~~SDE~~ in~~to~~ 802.11 are:

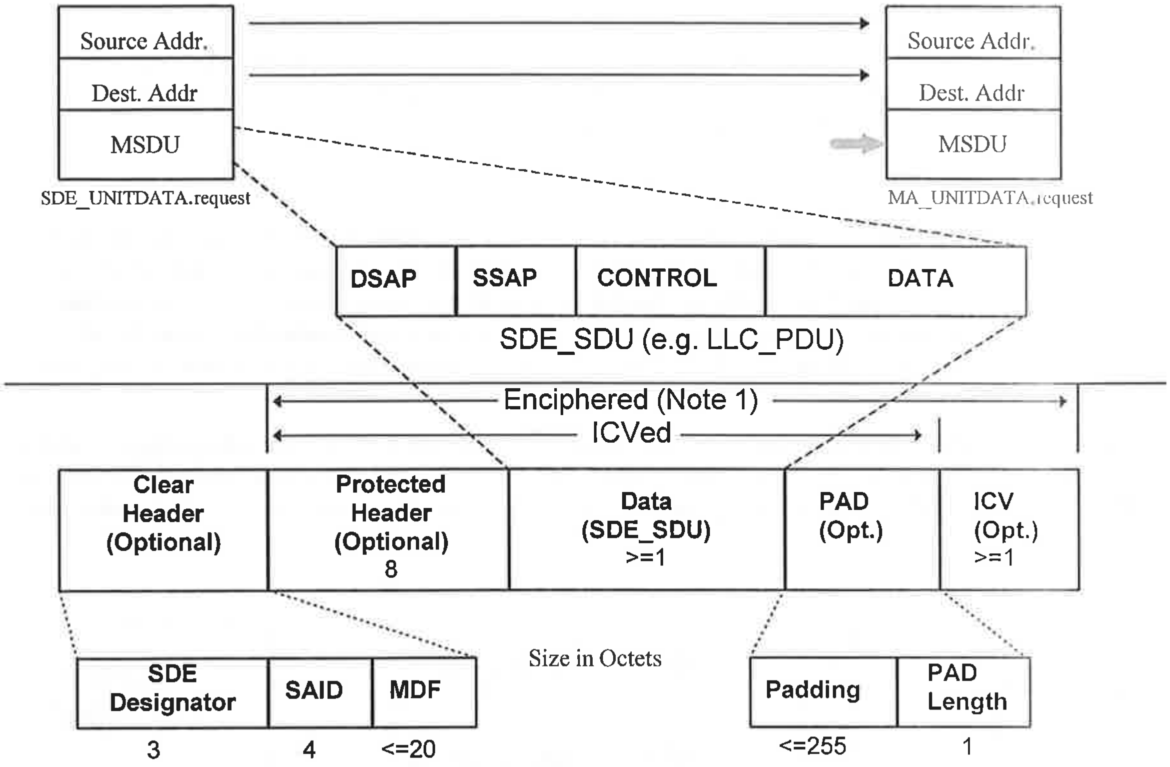
1) confidentiality;
2) authentication; and
3) access control in conjunction with layer management.

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).~~

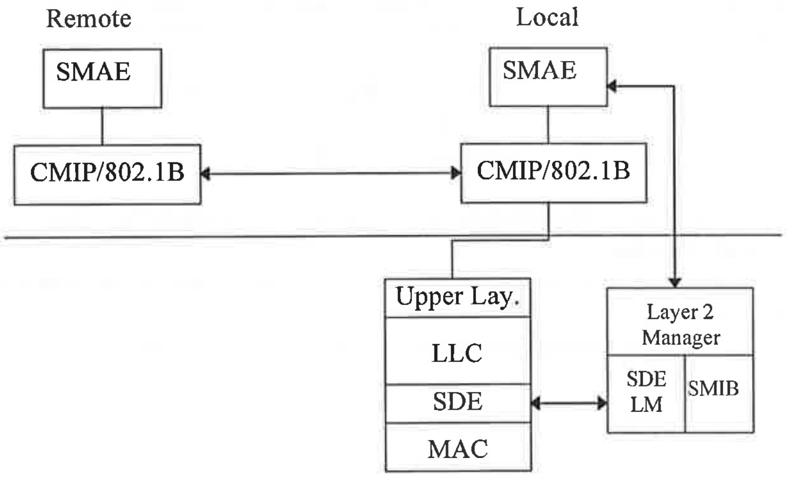
_~~Only the data is required, all other parts are optional to the particular implementation and the security services provided by the application of the SDE. All implementations of 802.11 shall provide for encipherment of data using the default algorithm(s). The default encipherment algorithm is specified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



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

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

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~~

3.1.2. Basic Service and Options

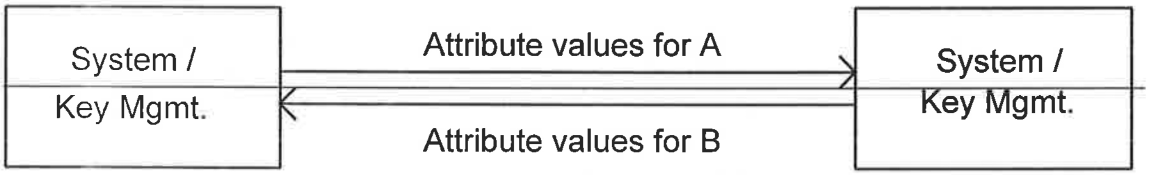
3.1.3. Reordering of MPDUs

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.

3.1.4.Security Service

As described in Section 3.1.1.3 above, all 802.11 Stations may ~~Wireless LANs shall~~ provide for data encipherment ~~in accordance~~ as described in section xx (was 5.4)~~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 authentication~~ssociation~~ exchange, parties A and B exchange authentication information (as described in section X.Xyy). ~~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.~~

3.2. Detailed Service Specification

3.2.1. MAC Data Services

3.2.1.1. MA_UNITDATA.request

3.2.1.1.1. 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.

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

3.2.1.1.3. 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.

3.2.1.1.4. 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.

3.2.1.2. MA_UNITDATA.indication

3.2.1.2.1. 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.

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

3.2.1.2.3. 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.

3.2.1.2.4. Effect of Receipt

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

3.2.2. MAC Management Services

To facilitate the three distribution system services:

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

3.2.3. 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).

3.2.3.1.

3.2.3.2.

3.2.3.3.

3.2.3.4.

3.2.3.5.

3.2.3.6. 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?}

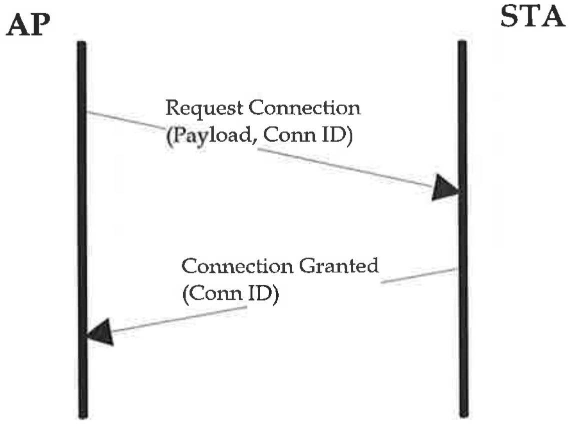


Figure 3-5: Connection Initiated by AP

3.2.3.7. 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).

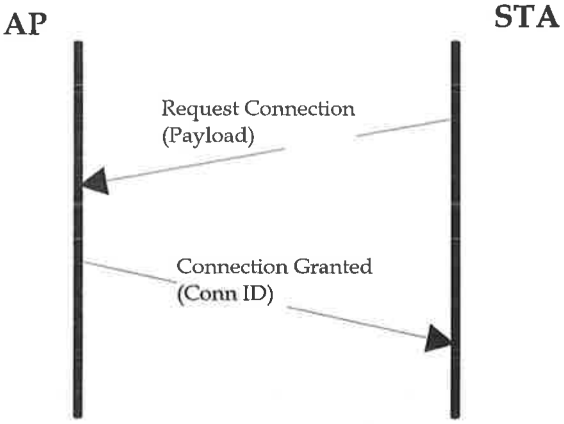


Figure 3-6: Connection Initiated by STA

3.2.3.8. 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.

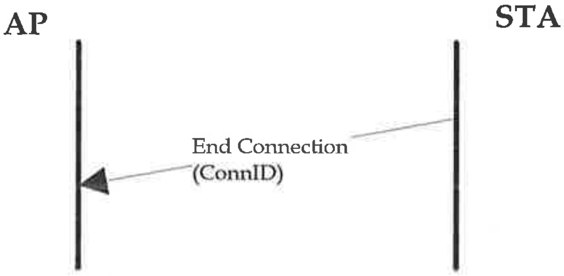


Figure 3-7: End Connection

4. Security Services

~~The security services in 802.11 shall be provided by a sub-set of the services described in IEEE Std 802.10-1992 standard - Secure Data Exchange (SDE); Clause 2 [2]. Therefore, the security service sections of IEEE 802.11 standard are used in conjunction with the applicable sections of IEEE 802.10 standard [2] specified above.~~

<<<editor's NOTE: This is a new section that should probably be placed after D1.2 sec 3 and before sec 4. >>>

4.1. Authentication Services

802.11 defines two subtypes of authentication service: “Open System” and “Shared Key”. The subtype invoked is indcated in the body of authentication management frames. Thus authentication frames are self idenfitfying witherspect to authentication algorithm.

4.1.1. Open System Authentication

Open System authentication is the simplest of the available authentication algotithms. Essentially it is a null authentication algorithm. Anyone who requests authentication with this algorithm becomes authentcated.

Open syetem authentication involves a two step authentication transaction sequence. The first step in the sequence is Identity assertion and request for authentication. The second frame in the sequence is a (usually) successful authentication result.

4.1.1.1. Open System Authentication (First frame)

Message type:
 Management
Message sub-type:
 Authentication
Information Items:
 Authentication Algorithm Identification = “open system”
 Station Identity Assertion (in SA field of header)
 Authentication transaction sequence number = 1
 Authentication algortithm dependent infromation (none)
Direction of message:
 From authentication initiating STA

This frame shall be sent with WEP OFF.

4.1.1.2. Open System Authentication (second and final frame).

Message type:
 Management
Message sub-type:
 Authentication
Information Items:
 Authentication Algorithm Identification = “open system”
 Authentication transaction sequence number = 2
 Authentication algortithm dependent infromation. (none)
 The result of the requested authentication. This is a fixed length item with values "successful" and "unsuccessful".
Direction of message:
 From authenticatiing station to initiating station.

This frame shall be sent with WEP OFF.

4.1.2. Shared Key Authentication

Shared Key authentication supports authentication of Stations as either a member of those who know a shared secret key or a member of those who do not. 802.11 shared key authentication accomplishes this without the need to transmit the secret key in the clear; requiring the use of the WEP privacy mechanism.

Therefore, this authentication scheme is only available if the WEP option is implemented. Additionally, the Shared Key authentication facility shall be implemented if WEP is implemented.

The required secret, shared key is presumed to have been delivered to participating stations via a secure channel wich is independnt of 802.11. This shared key is stored in a read-only MIB variable via the MAC management path.

4.1.2.1. Shared Key Authentication (First frame)

Message type:
  Management
Message sub-type:
  Authentication
Information Items:
  Station Identity Assertion (in SA field of header)
  Authentication Algorithm Identification = "shared key"
  Authentication transaction sequence number = 1
  Authentication algortithm dependent infromation (none)
Direction of message:
  From authentication initiating STA

This frame shall be sent with WEP OFF.

4.1.2.2. Shared Key Authentication (Second frame)

Before sending the second frame in the shared key authentication sequence, the sender shall use WEP to generate a string of octets which shall be used as the authentication challenge text.

Message type:
  Management
Message sub-type:
  Authentication
Information Items:
  Authentication Algorithm Identification = "shared key"
  Authentication transaction sequence number = 2
  Authentication algortithm dependent infromation = Challlenge text.
    This filed shall be of fixed length of 128 octets. The field shall be filled with octets generated by the WEP mechanism.

Direction of message:
  To authentication initiating STA

This frame shall be sent with WEP OFF.

4.1.2.3. Shared Key Authentication (Third frame)

The station which recieved the second frame in the sequence shall copy the challenge text from the second frame into the third frame. The third frame shall be transmitted after encryption by WEP using the shared secret key.

Message type:
  Management
Message sub-type:
  Authentication
Information Items:

Authentication Algorithm Identification = "shared key"
Authentication transaction sequence number = 3
Authentication algortithm dependent infromation = challenge text from sequence two frame.

Direction of message:
From authentication initiating STA

This frame shall be sent with WEP ON.

4.1.2.4. Shared Key Authentication (Fourth and final frame).

The stations which recieves the third frame of the authentication sequence shall attempt to decrypt it using what it believes to be the shared WEP key. It shall then compare the challenge text recovered to that sent in frame 2 of the sequence. If they are the same then the two stations must have the same shared key. This is then presumed to be suffcient proof that the authentication requesting station shall become succesfully authenticated.

Message type:
Management
Message sub-type:
Authentication
Information Items:
Authentication Algorithm Identification = "open system"
Authentication transaction sequence number = 4
Authentication algortithm dependent infromation. = the authentication result.
The result of the requested authentication.
This is a fixed length item with values "successful" and "unsuccessful".

Direction of message:
To authentication initiating station.

This frame shall be sent with WEP OFF.

4.2. The Wired Equivalent Privacy Algorithm (WEP)

4.2.1. Introduction

Eavesdropping is a familiar problem to users of other types of wireless technology. P802.11 specifies a wired LAN equivalent data confidentiality algorithm. Wired equivalent privacy is defined as protecting authorized users of a wireless LAN from casual eavesdropping. This service is intended to provide functionality for the Wireless LAN equivalent to that provided by the physical security attributes inherent to a wired media.

Data confidentiality depends on an external key management service to authenticate users and distribute data enciphering/deciphering keys. P802.11 specifically recommends against running an 802.11 with privacy but without authentication. While this combination is possible, it leaves the system open to significant security threats.

4.2.2. Properties of the WEP Algorithm

The WEP algorithm has the following properties:

Reasonably Strong:

The security afforded by the algorithm relies on the difficulty of discovering the secret key through a brute-force attack. This in turn is related to the length of the secret key and the frequency of changing keys. WEP allows for the changing of the key (*k*) and frequent changing the Initialization Vector (IV).

Self Synchronizing:

WEP is self-synchronizing for each message. This property is critical for a data-link level encryption algorithm, where "best effort" delivery is assumed and packet loss rates can be high.

Efficient:

The WEP algorithm is efficient and can be implemented in either hardware or software.

Export:

Every effort has been made to design the WEP system operation so as to maximize the chances of approval of export from the U.S. of products containing a WEP implementation via the Commerce Department. However, due to the legal and political climate toward cryptography at the time of publication, no guarantee can be made that any specific 802.11 implementations that use WEP will be exportable from the United States.

Optionality:

~~Therefore, t~~The implementation and use of WEP is an 802.11 option.

4.2.3. WEP Theory of Operation

The process of disguising (binary) data in order to hide its information content is called **encryption**[1]. Data that is not enciphered is called **plaintext** (denoted by *P*) and data that is enciphered is called **ciphertext** (denoted by *C*). The process of turning ciphertext back into plaintext is called **decryption**. A **cryptographic algorithm**, or cipher, is a mathematical function used for enciphering or deciphering data. Modern cryptographic algorithms use a key sequence (denoted by *k*) to modify their output. The encryption function *E* operates on *P* to produce *C:*

$$E_k(P) = C$$

[1] Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", John Wiley & Sons, Inc. 1994

In the reverse process, the decryption function *D* operates on *C* to produce *P:*

$$D_k(C) = P$$

As illustrated in Figure 5-21, note that if the same key is used for encryption and decryption then

$$D_k(E_k(P)) = P$$

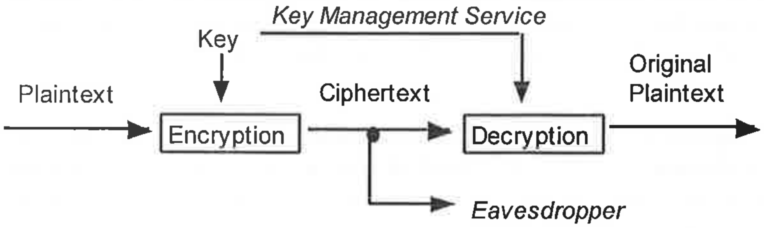


Figure 5-21: A Confidential Data Channel

The WEP algorithm is a form of electronic code book in which a block of plaintext is bitwise XOR'd with a pseudo random key sequence of equal length. The key sequence is generated by the WEP algorithm.

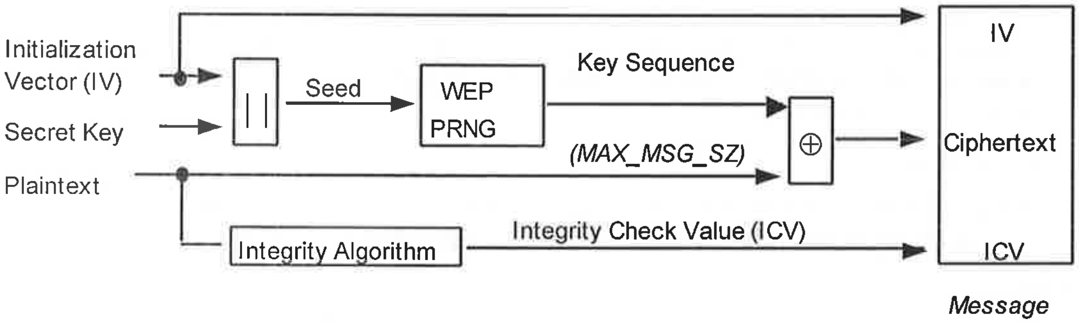


Figure 5-22: WEP Encipherment Block Diagram

Referring to Figure 5-22 and following from left to right, encipherment begins with a **secret key** that has been distributed to cooperating stations by an external key management service. WEP is a symmetric algorithm in which the same key is used for encipherment and decipherment.

The secret key is concatenated with an **initialization vector** (IV) and the resulting **seed** is input to a **pseudo random number generator** (PRNG). The PRNG outputs a **key sequence** *k* of pseudo-random bits equal in length to the largest possible MSDU. Two processes are applied to the plaintext MSDU. To protect against unauthorized data modification, an integrity algorithm operates on *P* to produce an **integrity check value** (ICV). Encipherment is then accomplished by mathematically combining the key sequence with *P*. The output of the process is a **message** containing the resulting ciphertext, the IV, and the ICV.

The WEP PRNG is the critical component of this process, since it transforms a relatively short secret key into an arbitrarily long key sequence. This greatly simplifies the task of key distribution as only the secret key needs to be communicated between stations. The IV extends the useful lifetime of the secret key and provides the self-synchronous property of the algorithm. The secret key remains constant while the IV changes periodically. Each new IV results in a new seed and key sequence, thus there is a one-to-one correspondence between the IV and *k*. The IV may be changed as frequently as every MSDU and, since it travels with the message, the receiver will always be able to decipher any message. The IV may be transmitted in the clear since it does not provide an attacker with any information about the secret key.

Because IV and the ICV must be transmitted with the MSDU, fragmentation may be invoked. The WEP algorithm is applied to an MSDU. The {IV, MSDU, ICV} triplet forms the actual data to be sent in the data frame.

For WEP protected frames, the first four octets of the frame contain the IV field for the MSDU. This field shall contain two sub-fields: A 1-octet field that contains the confidentiality algorithm ID, followed by a 3-octet field that contains the initialization vector The WEP IV is 16 bits. The 64-bit PRNG seed is formed using the secret key as the most significant 40 bits and the initialization vector as the least significant 24 bits. The WEP IV is 16 bits. The IV is followed by the MSDU, which is followed by the ICV. The WEP ICV is 32 bits. The WEP Integrity Check algorithm is CRC-32.

The entire {IV, MSDU, ICV} package may be split into several fragments (depending on the realtive values of the MSDU and the active MPDU size).

As stated previously, WEP combines *k* with *P* using bitwise XOR.

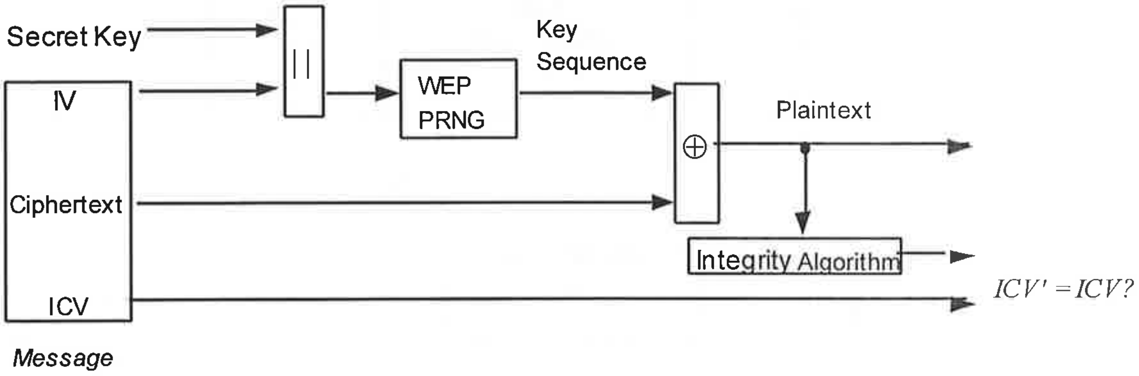


Figure 5-23: WEP Decipherment Block Diagram

Referring to Figure 5-23 and following from left to right, decipherment begins with the arrival of a message. The IV of the incoming message is used to generate the key sequence necessary to decipher the incoming message. Combining the ciphertext with the proper key sequence yields the original plaintext. Correct decipherment is verified by performing the integrity algorithm on the recovered plaintext and comparing the output ICV' to the ICV transmitted with the message. If ICV' is not equal to ICV, the received MSDU is not passed to LLC and and error indication is sent to MAC management.

4.2.4. WEP Algorithm Specification

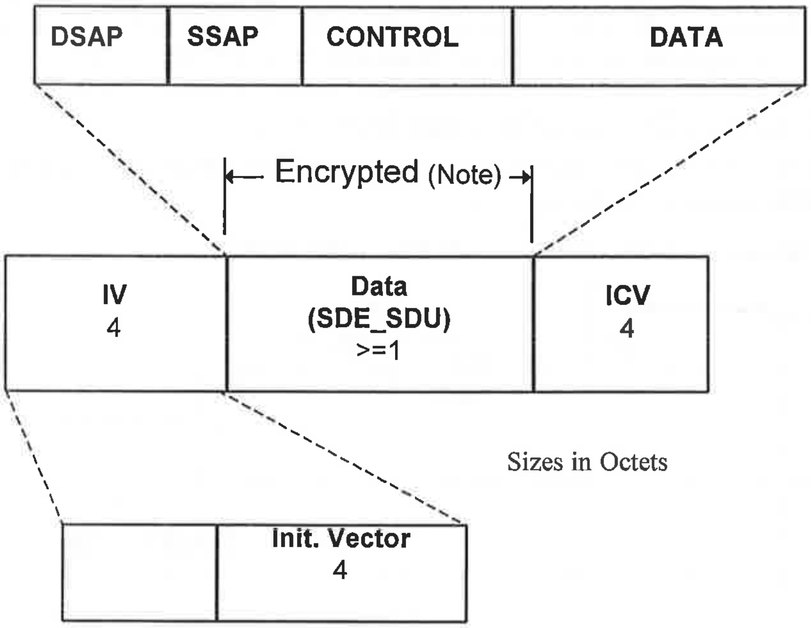
The specific PRNG algorithm is unspecified at present. Reviewers of this draft are encouraged to comment on appropriate PRNG algorithms for adoption by 802.11.

4.2.5. ~~Relationship of~~ WEP MSDU Expanison~~to IEEE 802.10, Secure Data Exchange (SDE)~~:

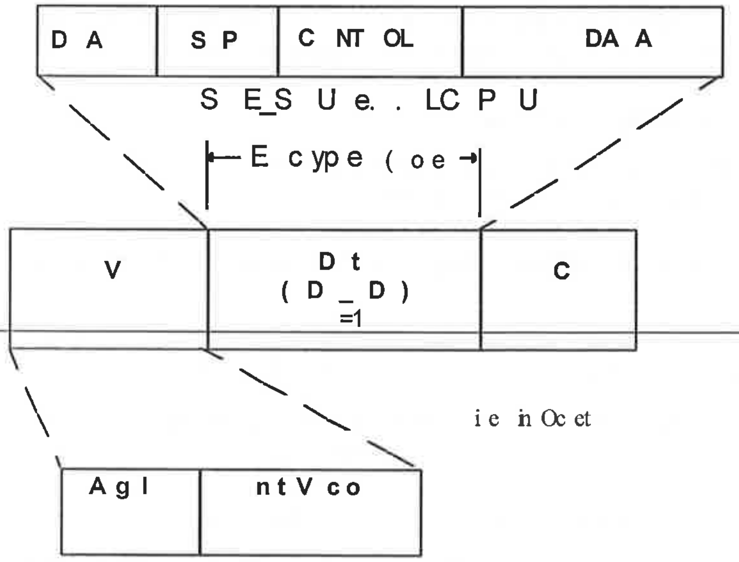
~~The WEP uses a subset of the IEEE 802.10 SDE structure shown in Figure 3-1 of section 3.1.1.3.~~ Figure 5-24 shows the encrypted MSDU~~SDE_PDU~~ as constructed by the WEP.

The WEP~~802.10 SDE settings for 802.11 WEP shall be clear header length =null, protected header length =null, pad =null, and~~ ICV = 32 bits. The expanded MSDU ~~data field~~ shall include a 32~~D~~ bit IV field immediately preceding the MSDU. This field shall contain one~~two~~ sub-fields: A ~~1-octet field that contains the confidentiality algorithm ID, and a~~ 4~~3~~-octet field that contains the initialization vector.

The ~~802.10~~ WEP mechanism is invisible to entities outside the 802.11 MAC. ~~allows for 802.10 SDE entities 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 twice on the same MSDU. This is consistent with the 802.10 model, in which lowerDlayer SDE entities are generally disabled when higherDlayer SDE entities are present.~~



Note: The encipherment process has expanded the original MSDU by8 Octets, 4 for the Initialization Vector (IV) field and 4 for the Integrity Check Value (ICV). The ICV is calculated on the Data field only.



Note: The encipher ent proc s ha exp nded th DE_ DU by 8 Oc e s 4 for th ni ia iz ion V c or (I) field and 4 for th nt gr ty he k a ue (I V The I V s a cul ed on the Da a f eld on y.

Figure 5-24: Construction of expanded WEP MSDU~~SDE_PDU~~

4.3. Security services related MIB variables

The 802.11 security mechanisms are controlled via the MAC management path and related MIB variables. This section gives an overview of the security related MIB variables and how they are used. For details of the MIB variable definitions, refer to section 7.X.

4.3.1. Authentication related MIB variables

The type of authentication invoked when authentication is attempted is controlled by the MIB variable Authentication_Type. This variable may have the following values:

1 = Open System
2 = Shared Key
All other values are reserved.

4.3.2. Privacy related MIB variables.

The default value for all WEP keys shall be Null. This indicates an invalid WEP key. An attempt to use WEP with a Null key shall result in an error condition.

To support shared key configurations, the MIB contains a variable called "Default_WEP_Key". The default value for this variable is Null. If not null, this variable contains the deafault key to be used with WEP.

An additional variable called "WEP_Default" is a boolean. If set True then on transmit, Data frames shall be encypted using Default_WEP_Key and on receive they shall be decrypted using Default_WEP_Key. The MIB shall not allow WEP_DEfault to be set to TRUE if Dfault_WEP_Key is Null. The default value of WEP_Default is False.

802.11 does not require that the same WEP key be used for all stations. The MIB supprts the ability to have a separate WEP key for each station which which a Station directly communicates. This is supported by a MIB variable which is a two dimensional array called "WEP_Key_Mapping". The array is indexed by MAC address and contains two fields for each entry: "WEP_ON" and the corresponding WEP_Key. The MIB shall not allow WEP_ON to be set to TRUE if the corresponding WEP_key entry is Null. The default value for all WEP_ON fields is False. This variable is always indexed by either RA to TA addresses (since WEP is applied only to the wireless link).

The values in this array variable take precedence over the WEP_Default and Default_WEP_Key variables.

The minimal length of WEP_Key_Mapping shall be 10. This value represents a minimum capability that may be assumed for any station which implements the WEP option.

The maximum length of WEP_Key_Mapping shall be implmementation dependant and the actual length of the array can be inquired from the read only MIB variable "WEP_Key_Mapping_Length".

The interactions between these variables is described below:

```
Transmit case:
        if WEP_Key_Mapping(RA, WEP_On) = Ture then use WEP_KEY_Mapping(RA,
            WEP_Key) for encryption,
        if WEP_Default = Ture then Use WEP_Default for encryption,
        otherwise do no encypt the frame.

Receive case:
        if WEP_Key_Mapping(TA, WEP_On) = Ture then use WEP_KEY_Mapping(TA,
            WEP_Key) for decryption,
        if WEP_Default = Ture then Use WEP_Default for decryption,
        otherwise do no attempt to decypt the frame.
```

>>>>>>>>>>>>>>>> <<<<<<<<<<<<<<<<<<<<<

Editing notes for section 4 to complete a self consistent set of changes re security for draft 1.2.

Draft 1.1 will have the WEP bit in the frame header - these changes are assumed as part of the base text that these changes apply to.

Since Draft 1.2 text for section 4 was not available at the time this document was created, the changes required relative to draft 1.0 are shown below - the editor's are requested to apply these changes to draft 1.1 text when creating draft 1.2.

The changes required in section 4 are:

Delete the Privacy and privacy request mgt frame types from table 4.1

Delete sections 4.2.3.10 (privacy frame desc), 4.2.3.11 (privacy response frame desc), 4.4.11 (privacy alg number structure), 4.4.16 (supported alg list), sections 4.4.18, 4.4.19 and 4.4.20 (the challenge and response structure descriptions).

Note: the sec 4 gang has tried to incorporte these changes in their revised text work as of 5/10/95.

>>>>>>>>>>>>>>>> <<<<<<<<<<<<<<<<<<<<<<

5. MAC Sub-layer Functional Description

5.1.

802.11 defines two subtypes of authentication service; “Open System” and “Shared Key”. The subtype invoked is indcated in the body of authentication management frames. Thus authentication frames are self idenfitfying witherspect to authentication algorithm.

5.2.

802.11 defines two subtypes of authentication service: “Open System” and “Shared Key”. The subtype invoked is indcated in the body of authentication management frames. Thus authentication frames are self idenfitfying witherspect to authentication algorithm.

5.3.

802.11 defines two subtypes of authentication service; "Open System" and "Shared Key". The subtype invoked is indcated in the body of authentication management frames. Thus authentication frames are self idenfitfying witherspect to authentication algorithm.

5.4. The Wired Equivalent Privacy Algorithm

{section deleted}

802.11 defines two subtypes of authentication service: "Open System" and "Shared Key". The subtype invoked is indcated in the body of authentication management frames. Thus authentication frames are self idenfitfying witherspect to authentication algorithm.