Proposed Text for Sections 1, 2 (& a few lines in Section 4), Based on responses to Draft D1 Letter Ballot processed at March 1995 Meeting

Abstract: This paper (95/56) presents the changes to sections in the Draft Standard P802.11/D1 as a result of the Response to Draft D1 Letter Ballot processed at the March 1995 Meeting as shown in the companion Document P802.11-95/62 (sec 1), 95/63 (sec 2) and 95/60 (sec 5.4).

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

1. 1.General

1.1 Purpose

The original Project Authorization Request (PAR) defines the scope of the IEEE 802.11 work as follows:

> To develop a medium access control (MAC) and Physical Layer (PHY) specification for wireless connectivity for fixed, portable and moving stations within a local area.

The PAR further defines the purpose as follows:

> To provide wireless connectivity to automatic machinery, equipment or, stations that require rapid deployment, which may be portable, or hand-held or which may be mounted on moving vehicles within a local area.
>
> To offer a standard for use by regulatory bodies to standardize access to one or more frequency bands for the purpose of local area communication.
>
> The various RF phy groups working within a given band must return to the drawing board and decide what their PHY specificaiton reccomendation should be. To accompliosh this they must forego the temptation to continue operating in splinter groups which become smaller and smaller as a means of avoiding internal controversy and tough decisions. Note that I make no comment on which of the currently proposed PHYs should be selected. What is important is that the group reach a technical concensus on a reccomendation of a **single** phy for the 2.4 Ghz ISM band.

Specifically the 802.11 standard:

- Ddescribes the functions and services required by an 802.11 compliant device to operate within ad-hoc and infrastructure networks as well as the aspects of station mobility (transition) within those networks.
- Ddescribes the medium access control (MAC) procedures to support the asynchronous and time-bounded MAC service data unit (MSDU) delivery services.
- Ssupports the operation of an 802.11 compliant device within a wireless LAN which may coexist with multiple overlapping wireless LANs.
- Ddescribes the requirement and service to provide security, privacy and authentication of 802.11 compliant devices.

1.2 Definitions

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

Ad-hoc network. An ad-hoc network is a network created for a specific purpose, typically in a spontaneous manner. The principal characteristic of an ad-hoc network is that the act of creating and dissolving the network is sufficiently straightforward and convenient so as to be achievable by non-technical users of the network facilities (i.e. no specialized 'technical skills' are required with little and/or no investment of time or additional resources required beyond the stations which are to participate in the (ad-hoc) network. The term "Ad-Hoc" is often used as slang to refer to an Independent BSS (IBSS).

Access control. The prevention of unauthorized usage~~e~~ of resources., ~~including the prevention of use of resource in an unauthorized manner.~~

Association. The service used to ~~that~~ establish~~es~~ AP/STA mapping and enables STA invocation of the D~~d~~istribution S~~system~~ S~~services~~.

Authentication. The service used to positively establish the identity of one station to another station~~s to each other~~.

Basic Service Area (BSA). The conceptual area within which members of a B~~b~~asic S~~s~~ervice S~~s~~et can communicate.

Basic Service Set (BSS). A set of stations controlled by a single C~~c~~oordination F~~f~~unction. A BSS can have one PCF and one DCF.

Channel. An instance of medium use for the purpose of passing protocol data units that can be used simultaniously, in the same voliume of space, with other instances of medium use on other channels by instances of the same PHY, with an acceptably low frame error rate due to mutual interference. Some PHYs only provide one channel, whereas others provide multiple channels.~~coexist with other instances of medium use.~~

single channel	n-channel
1-narrowband channel	FDM channels
DSS with 1 code	DSS with CDMA

Confidentiality. The property of information that is not made available or disclosed to unauthorized individuals, entities or processes.

Coordination Function (CF). That logical function which determines when a station operating within a B~~b~~asic S~~s~~ervice S~~s~~et transmits and receives~~d~~ via the wireless medium.

Disassociation. The service which removes an existing A~~a~~ssociation.

Distributed Coordination Function (DCF). A class of possible coordination functions where the same coordination function logic is active in every station in the BSS at any ~~at~~ any given time that the network is in operation.

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

Distribution System (DS). A system used to interconnect a set of Bbasic Sservice Ssets and integrated LANs to create an Eextended Sservice Sset.

Distribution System Medium (DSM). The medium used by a Ddistribution Ssystem (for Access Point(~~for basic service set~~ interconnections).

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.

~~The set of services provided by the distribution system which enable the MAC to transport MAC service data units between basic service sets within an extended service set.~~

ESS_BASIC_RATE_SET: A set of rates that all the stations on the given ESS are required to be capable to receive. According to the PHYs definitions the default ESS BASIC RATE SETs for the different PHYs will be:

For 2,4 Ghz ISM DS PHY : {1Mbs,2MBs}
For 2,4 Ghz ISM FH PHY: {1Mbs}
For IR PHY: {1Mbs, 2Mbs}Note that this value is preset for all stations in the ESS.

EXTENDED_RATE_SET: The set of rates beyond the BASIC_RATE_SET that a station supports. This can be a speed that is defined in future PHY standards.

Extended Service Area (ESA). The conceptual area within which members of an Eextended Sservice Sset can communicate. An Eextended Sservice Aarea is larger or equal to a Bbasic Sservice Aarea and may involve multiple, disjoint, BSAs.

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

Gaussian Frequency Shift Keying (GFSK). A modulation scheme where the data is first filtered by a Gaussian filter in the base band and then modulated with a simple frequency modulation.

Independent Basic Service Set (IBSS). A BSS which forms a self contained network independent of any other BSSs. ~~An IBSS is often the form an Ad-Hoc network takes.~~

Infrastructure. The infrastructure includes the logical Ddistribution Ssystem, Aaccess Ppoints and Pportals functions. An infrastructure contains one or more Aaccess Ppoints and zero or more Pportals in addition to thea Ddistribution Ssystem.

~~Within the infrastructure there are two exposed interfaces:~~

~~a) between stations and access points; and~~
~~b) between access points and distribution system.~~

~~Additionally,~~ DS services are provided between pairs of 802.11 MACs.

Integration. The service which enables delivery of MAC service data units between the Ddistribution Ssystem and an existing network (via a Portal).

MAC Protocol Data Unit (MPDU). The unit of data exchanged between two peer MAC entities using the services of the PHY. ~~The term "frame" is often used as a synonym for MPDU.~~

MAC Service Data Unit (MSDU). The MAC service data unit is information that is delivered as a unit between MAC service access points.

Masquerade. The pretense by an entity to be a different entity.

Mobile Station: A mobile station uses network communications while in motion.

Net Allocation Vector (NAV): An indicator, maintained by each station, of time periods when trasnmission onto the WM may not be initiated by the station whether or not the Station's CCA function senses the WM as being busy.

Point Coordination Function (PCF). A class of possible coordination functions where the coordination function logic is active in only one station in a BSS at any given time tat the network is in operation.

Portable Station: A portable station is one that may be moved from location to location, but only uses network communications while at a fixed location.

Portal: The logical point at which data from a non-802.11 LAN connects with an 802.11 LAN via ~~enters~~ the Ddistribution Ssystem.

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

Re-association. The service which enables an established association (between AP and ~~of a~~ station) to be transferred from one~~an~~ access point to another (or the same) access point.

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

STATION_BASIC_RATE: A value belonging to the ESS BASIC RATE SET, that is used by the station for specific transmissions (it could change dynamically, for example the Station Basic Rate on the IR depends on the Power Consumption Mode of the Station).

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

Unauthorized disclosure. The process of making information available to unauthorized individuals, entities or processes.

Unauthorized resource use. Use of resource not consistent with the defined security policy.

Wired Equivalent Privacy (WEP). The optional cryptographic privacy algorithm specified by 802.11 used to provide data confidentiality which is subjectively equivalent to the ~~a wired media~~ confidentiality of a wired LAN medium that does not employ cryptographic techniques to enhance privacy.

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

1.3 Abbreviations

AP	=	Access Point
BSA	=	Basic Service Area
BSS	=	Basic Service Set
CF	=	Coordination Function
DA	=	Destination Address
DCE	=	Data Communication Equipment
DCF	=	Distributed Coordination Function
DIFS	=	Distributed Inter-Frame Space
DLL	=	Data Link Layer
DS	=	Distribution System
DSAP	=	Destination Access Point
DSM	=	Distribution System Medium
DSS	=	Distribution System Services
DSSS	=	Direct Sequence Spread Spectrum
DTBS	=	Distributed Time Bounded Service
DTE	=	Data Terminal Equipment
ESA	=	Extended Service Area
ESS	=	Extended Service Set
FCS	=	Frame Check Sequence
FHSS	=	Frequency Hopping Spread Spectrum
GFSK	=	Gaussian Frequency Shift Keying
ICV	=	Integrity Check Value
IDU	=	Interface Data Unit
IFF	=	**IF And Only IF**
LLC	=	Logical Link Control
MAC	=	Medium Access Control
MDF	=	Management-Defined Field
MIB	=	Management Information Base
MPDU	=	MAC Protocol Data Unit
MSDU	=	MAC Service Data Unit
NAV	=	Network Allocation Vector
PAR	=	Project Authorization Request
PCF	=	Point Coordination Function
PDU	=	Protocol Data Unit
PhL	=	Physical Layer
PhS	=	Physical Service
PHY	=	Physical
PIFS	=	Priority Inter-Frame Space
PSNP	=	Power Save Non-Polling (mode)
PSP	=	Power Save Polling (mode)
SA	=	Source Address
SAID	=	Security Association Identifier
SAP	=	Service Access Point
SDE	=	Secure Data Exchange
SDU	=	Service Data Unit
SID	=	Station Identifier
SIFS	=	Short Inter-Frame Space
SMIB	=	Security Management Information Base
SS	=	Station Services
SSAP	=	Source Service Access Point
STA	=	Station

WAN	=	Wide Area Network
WDS	=	**Wireless Distribution System**
WEP	=	Wired Equivalent Privacy.
WM	=	Wireless Medium

1.4 References

1. ISO 7498:1984, Information Processing Systems - Open Systems Interconnection - Basic Reference Model.

2. IEEE Std 802.10-1992, Interoperable LAN/MAN Security (SILS)

3. ISO-7498 or CCITT Recommendation X.200 series - OSI Model and Notation Service Definition

4. IEEE Std 802-1990, IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture (ANSI).

5. <editor please add a correct formal ref to ISO 10039 here>

1.5 Conformance Requirements

This section for further study.

1.6 Conventions

1. This standard represents information fields as octet strings of various lengths. The least significant bit (LSB) of each octet is defined as bit zero (0) for that octet. All octets are represented in figures with the LSB on the right.

2. This standard represents fields longer than a single octet as strings of octets and fractions thereof. A field longer than a single octet is represented in figures with the most significant bit (MSB) on the left. Each octet to the right of the MSB is of correspondingly lesser significance.

2. 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) Have limited physical point to point connection ranges.~~
a~~b~~) Uses a ~~shared~~ 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~~.~~
~~c~~b) Are unprotected from outside signals.
c~~d~~) Are significantly less reliable than wired PHYs.
d~~e~~) 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~~of~~ 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

802.11 is required to appear to higher layers (LLC) as an ~~current~~ 802 style LAN. This requires that the 802.11 network handle station mobility within the MAC layer. To meet reliability an security assumptions (that LLC makes about lower layers), it is necessary for 802.11 to incorporate functionality which is untraditional for other 802 MAC layers.

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.

~~**Basic Service Set (BSS): A set of STAs controlled by a single CF.**~~

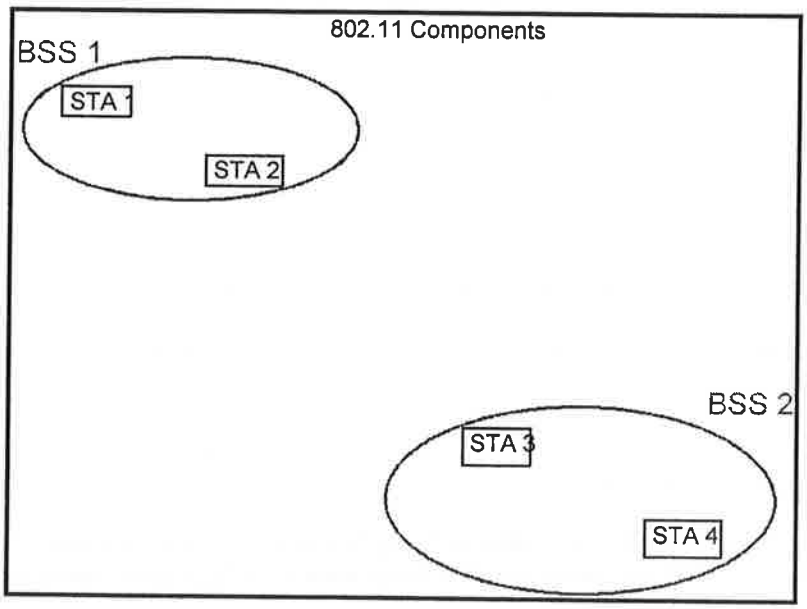

Figure 2-1: Basic Service Sets

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 ~~coverage area~~, 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~~close enough to form a direct connection.~~. 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 association between a STA and a BSS is dynamic (STAs turn on, turn off, come within range and go out of range). To become a member of an `infrastructure` BSS a station must become "Associated". This involves the use of `Distribution` System Services which are described later.

2.2.2 Distribution System Concepts

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

Instead of existing independently, a BSS may also form a component of an extended form of ~~an 802.11~~ 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).

~~**Distribution System** (DS): A system used to interconnect a set of BSSs to create an ESS.~~

~~**Distribution System Medium** (DSM): The medium used by a DS (for BSS 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 ~~architectural~~ 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.

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

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

~~Access Point (AP): Any entity that has STA functionality and provides access to the DS.~~

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

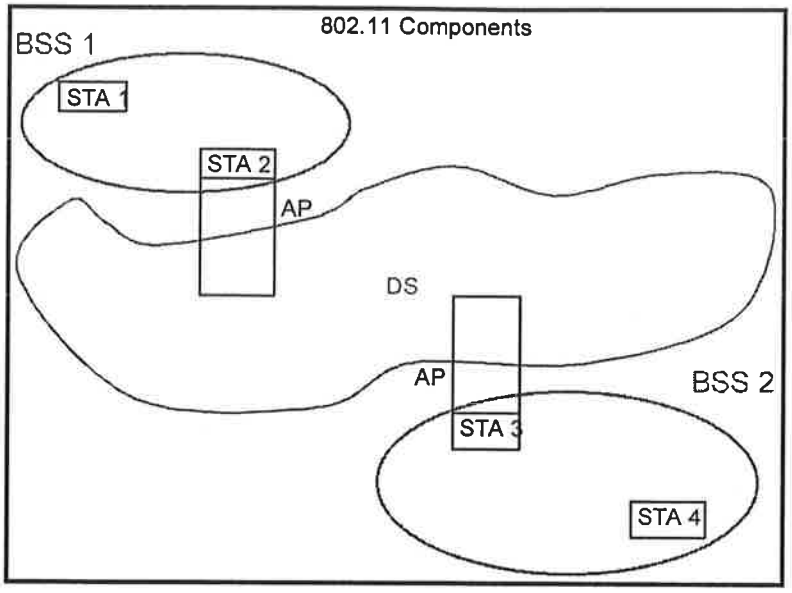

Figure 2-2: Distribution Systems and Access Points

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.

~~Extended Service Set (ESS): A set of interconnected BSSs which appear as a single BSS.~~

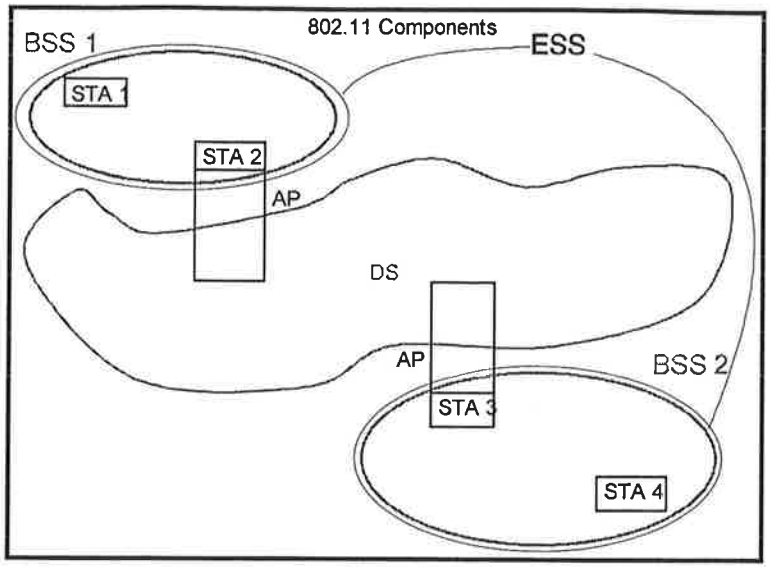

Figure 2-3: Extended Service Set

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.

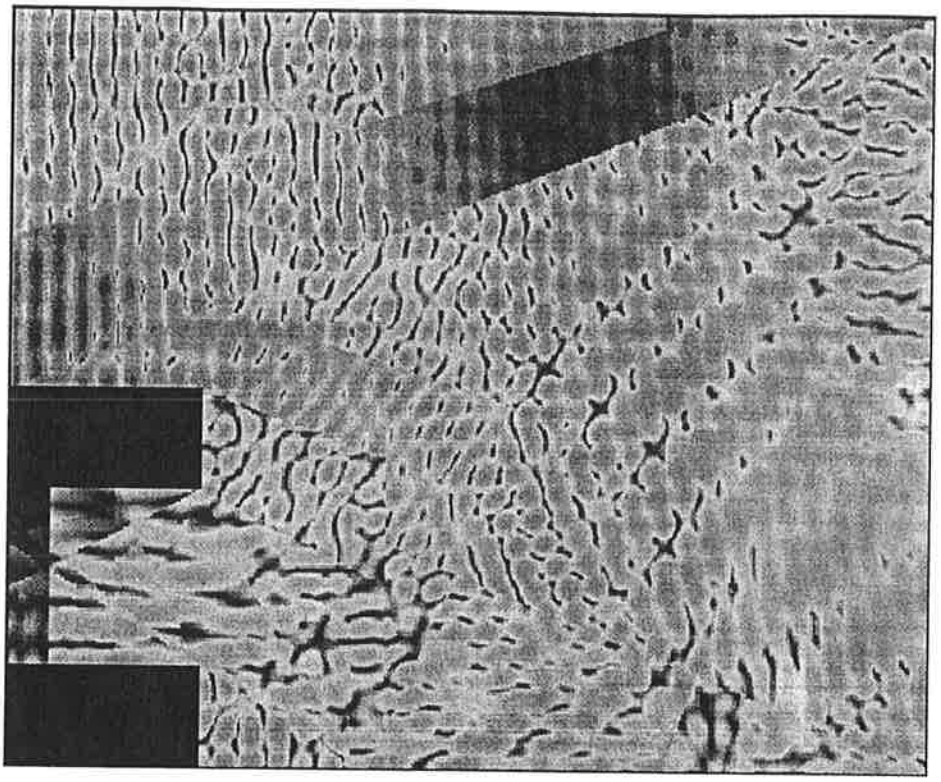

Figure 2-4: A Representative Signal Intensity Map

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?

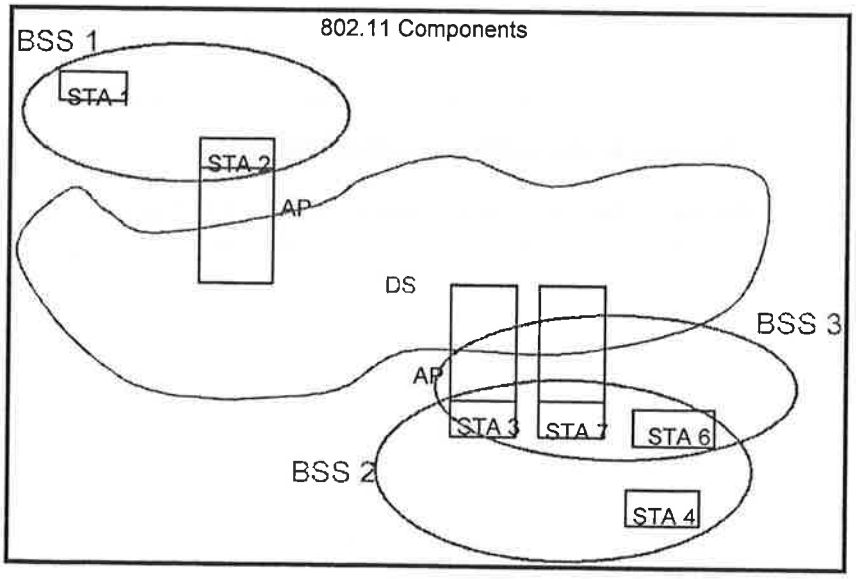

Figure 2-5: Collocated Coverage Areas

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 ~~traditional~~ 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.

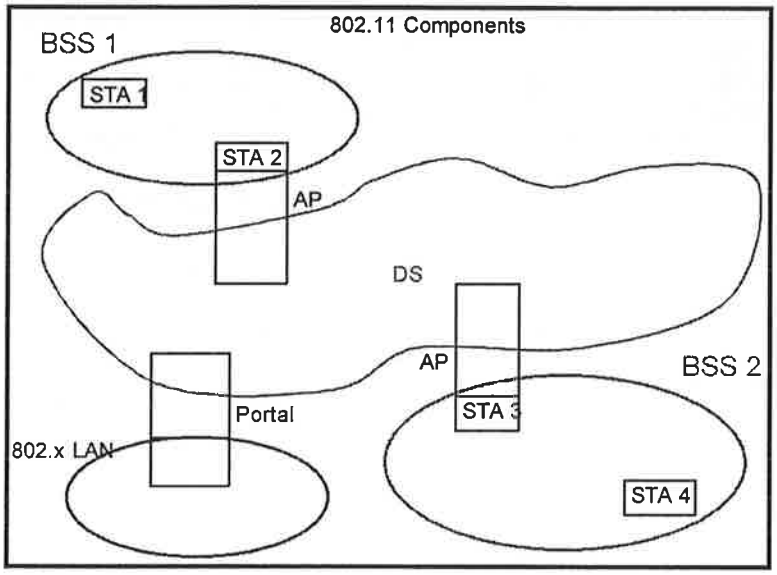

Figure 2-6: Connecting to Other 802 LANs

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) Disassociation
d) Distribution
e) Integration
f) Privacy
g) Reassociation

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. ~~In the figures, dots will represent Station Services.~~

The Station Services subset is:

a) Authentication
b) Deauthentication
~~c~~b) 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.

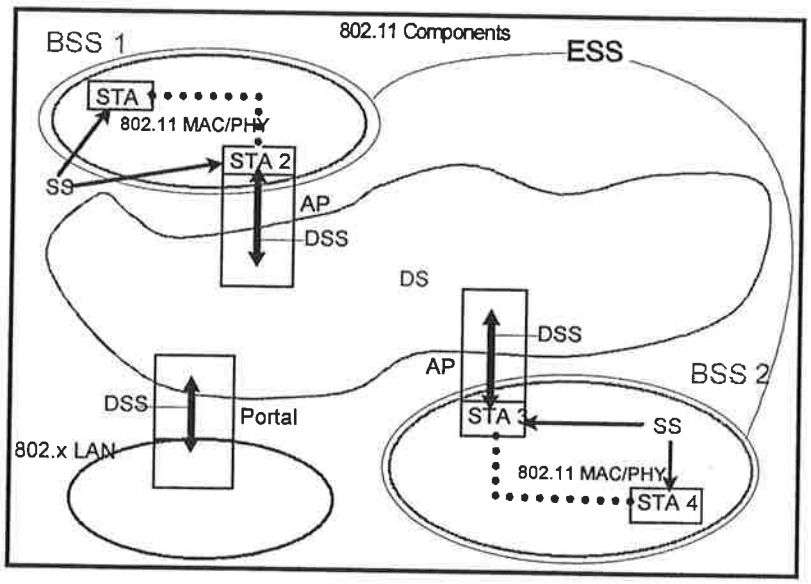

Figure 2-7: Complete 802.11 Architecture

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).

How 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. ~~e.g.~~ 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 ~~support by 802.11~~ 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 ~~mobile~~ 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 ~~mobile~~ 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 ~~mobile~~ 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 (~~mobile~~ STA or AP). Disassociation is a notification, ~~is n~~not a request~~, it is a notification~~. 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 assume 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 a general authentication 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.

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.

~~C/R exchanges are sufficient to support authentication from password based systems up through cryptographic authentication schemes.~~ Details of the usage of cryptographic authentication schemes are outside the scope of this standard.

~~802.11 uses 802.10 services to perform the actual challenge and response calculations.~~ A Management Information Base (MIB) function is provided to support inquiries into the 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.

in 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~~would~~ 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 IEEE 802.10 SDE clause 2 to perform the actual encryption of messages. A MIB function is provided to 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 is not invoked until the frame following the Privacy Response frame. All stations start "in the clear" in order to set up the Authentication and Privacy services.

The default privacy 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 the default is not acceptable to one party or the other, 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 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.

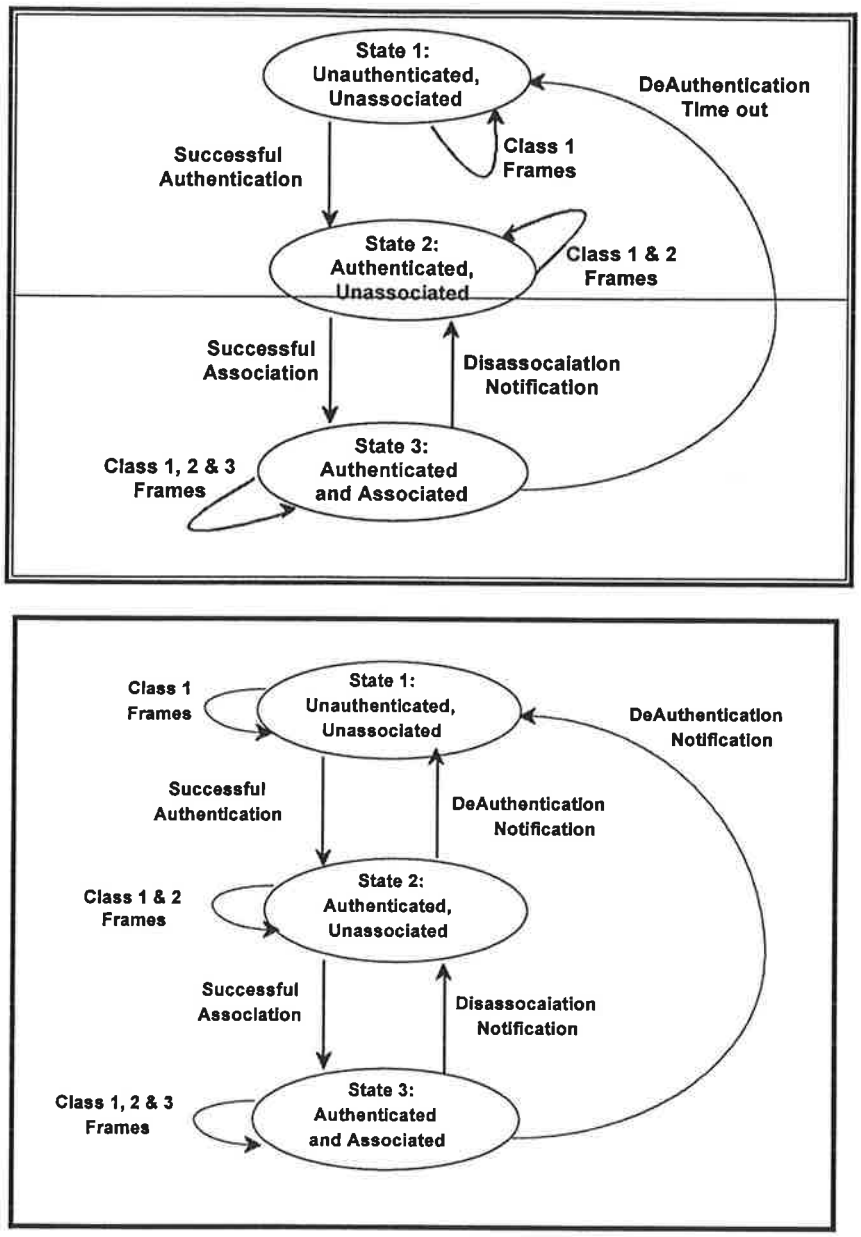

Figure 2-8: Relationship Between State Variables and Services

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
~~4) Poll~~

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
2) ATIM
3) Association R/R
Successful Association enables Class 3 frames.
Unsuccessful Association leaves STA in state 2.
4) 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) CF Data frames:~~
~~1) CF DATA~~
~~2) CF DATA + ACK~~

c~~d~~) ~~CF~~ 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.

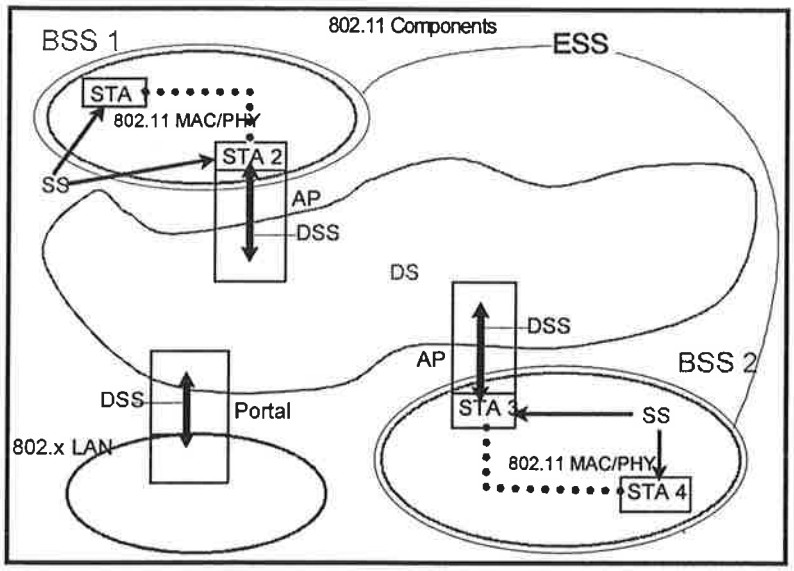

Figure 2-9: 802.11 Architecture (again)

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.

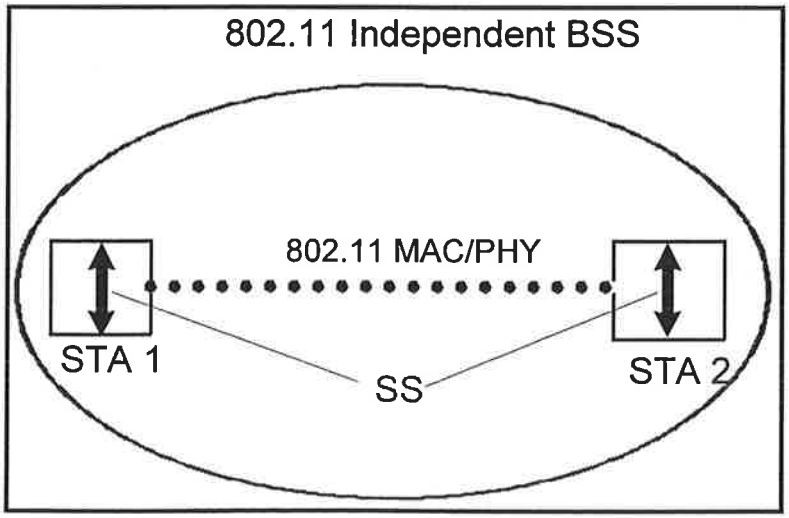

Figure 2-10: Logical Architecture of an Independent BSS

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~~, if the message is to be delivered via an AP.~~
Direction of message:
From STA to STA~~ (e.g. STA to AP or AP 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~~enables~~ 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 privacy algorithm for use, the privacy service causes 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 two STAs wish to mutually authenticate each other, the authentication service causes the following message sequence to occur. 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)

Message type:
Management
Message sub-type:
Authentication

Information Items:
Authentication transaction sequence number.
List of acceptable authentication algorithms supported. This is a variable length list of fixed length items.
Direction of message:
From STA 1 to STA 2.

Authentication (message 2)

Message type:
Management
Message sub-type:
Authentication
Information Items:
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".
Direction of message:
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)

Message type:

Management

Message sub-type:

Authentication

Information Items:

Authentication transaction sequence number.

The 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.

2.8

2.8.1 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).

2.9 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.

2.10 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]).

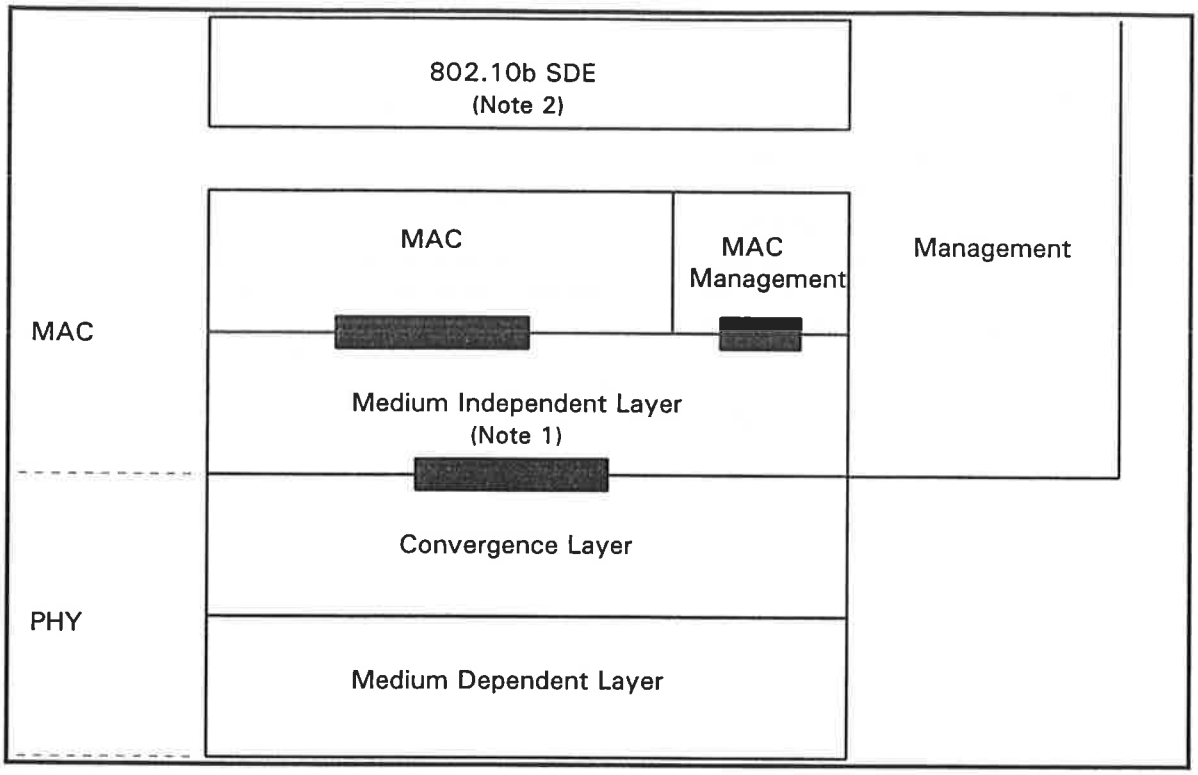

Figure 2-11, Portion of the ISO Basic Reference Model Covered in this Standard

~~Note 1 - Optional exposed DTE/DCE interface~~
Note 2 - 802.10 SDE: IEEE 802.10 - Secure Data Exchange [2]

2.11 Service Primitives

A service primitive is an abstract, implementation independent interaction between a service-user and the service-provider. Each service primitive may have zero or more parameters that convey the information required to provide the service.

Primitives are four generic types:

Request. A primitive issued by a service user to invoke some procedure.

Indication. A primitive issued by a service-provider either:

1) to invoke some procedure; or
2) to indicate that a procedure has been invoked by the service-user at the peer Service Access Point (SAP).

Response. A primitive issued by a service-user to complete, at a particular SAP, some procedure previously invoked by an indication at the SAP. Responses can be positive or negative as appropriate to the Circumstances.

Confirm. A primitive issued by a service-provider to complete, at a particular SAP, some procedure previously invoked by a request at that SAP. Confirms can be positive or negative as appropriate to the circumstances.

3. Dummy section 3

4. 3.Frame and MPDU Formats

4.1 MAC Frame Formats

4.1.1 General Frame Format

4.1.2 Frame Fields

4.1.2.1 Frame Control Field

4.1.2.1.1 Protocol Version

4.1.2.1.2 Type and Subtype

The Type and Subtype fields shall identify the function and interpretation of a frame. There are three frame types: control, data and management. Each of the frame types may have several subtypes. The table below lists the valid combination of Type and Subtype.

Type Value	Type Description	Subtype Value	Subtype Description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Reassociation Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0110	Privacy Request
00	Management	0111	Privacy Response
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	~~Connection Request~~Deauthentication
00	Management	1101	~~Grant Connection~~ Connection Request
00	Management	1110	~~End Connection~~ Grant Connection
00	Management	1111	~~Reserved~~ End Connection
01	Control	0000-1010	Reserved
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF End
01	Control	1111	Poll
10	Asynchronous Data	0000	Data
10	Asynchronous Data	0001	Data + CF-Ack
10	Asynchronous Data	0010	Data + CF-Poll
10	Asynchronous Data	0011	Data + CF-Ack + CF-Poll
10	Asynchronous Data	0100	Null Function (no data)

10	Asynchronous Data	0101	CF-Ack (no data)
10	Asynchronous Data	0110	CF-Poll (no data)
10	Asynchronous Data	0111	CF-Ack + CF-Poll (no data)
10	Asynchronous Data	1000-1111	Reserved
11	Reserved	0000-1111	Reserved

Table 4-1: Valid Type/Subtype Combinations

4.1.2.1.3 **To DS**

4.1.2.1.4 **From DS**

4.1.2.1.5 **Last Fragment**

4.1.2.1.6 **Retry**

4.1.2.1.7 **Power Management**

4.1.2.1.8 **Elements Present**

4.1.2.2 **Duration or Connection ID**

4.1.2.3 **Address Fields**

4.1.2.3.1 **Address Representation**

4.1.2.3.2 **Address Designation**

4.1.2.3.3 **BSS Identifier**

4.1.2.3.4 **Destination Address**

4.1.2.3.5 **Source Address**

4.1.2.3.6 **Receiver Address**

4.1.2.3.7 **Transmitter Address**

4.1.2.4 **Sequence Control**

Figure 4-3: Sequence Control Field

4.1.2.4.1 **Dialog Token**

4.1.2.4.2 **Fragment Number**

4.1.2.5 **Frame Body**

4.1.2.6 **CRC**

4.2 Format of Individual Frame Types

4.2.1 Control Frames

4.2.1.1 RTS Frame Format

4.2.1.2 CTS Frame Format

4.2.1.3 ACK Frame Format

4.2.1.4 Poll Frame Format

4.2.2 Data Frames

4.2.2.1 DATA Frame Format

4.2.3 Management Frames

4.2.3.1 BEACON Frame Format

4.2.3.2 ATIM Frame Format

4.2.3.3 Disassociation Frame Format

4.2.3.4 Association Request Frame Format

4.2.3.5 Association Response Frame Format

4.2.3.6 Reassociation Request Frame Format

4.2.3.7 Reassociation Response Frame Format

4.2.3.8 Probe Request Frame Format

4.2.3.9 Probe Response Frame Format

4.2.3.10 Privacy Request Frame Format

4.2.3.11 Privacy Response Frame Format

4.2.3.12 Authentication Frame Format

4.2.3.13 Deauthentication Frame Format

The Frame body of this frame is null.

4.3 Frame Exchange Sequences