Proposal for Frame Processing Simplification by applying WEP to MPDU payload rather than MSDU payload.

David Bagby
Advanced Micro Devices
7 July 1995

This paper is very short. It simply proposes that WEP be applied to the MPDU body instead of the MSDU body.

This has the advantage of allowing a simpler interaction between Fragmentation and WEP (by applying WEP after fragmentation rather than before). With this change, it will not be necessary to receive an entire MSDU before decrypting the contents, resulting in implementation simplification.

Essentially, this change would logically move WEP processing from the top of the MAC layer to the bottom. Since WEP is invisible outside of the MAC layer, this change has no noticeable impact external to the MAC.

The included printed pages from D1.2 are the actual text alterations that would be required to implement this change to D1.2 text.

Moved:
That WEP processing be changed from an MSDU basis to and MPDU basis by adopting the changes shown to D1.2, said changes to be reflected in the next draft standard revision.

(Section 2) 1. General Description

1.1. 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.

1.1.1. How Wireless LAN Systems are Different

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

1.1.1.1. 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.

1.1.1.2. 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.

1.1.1.3. 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.

1.1.1.4. 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.

1.2. 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.

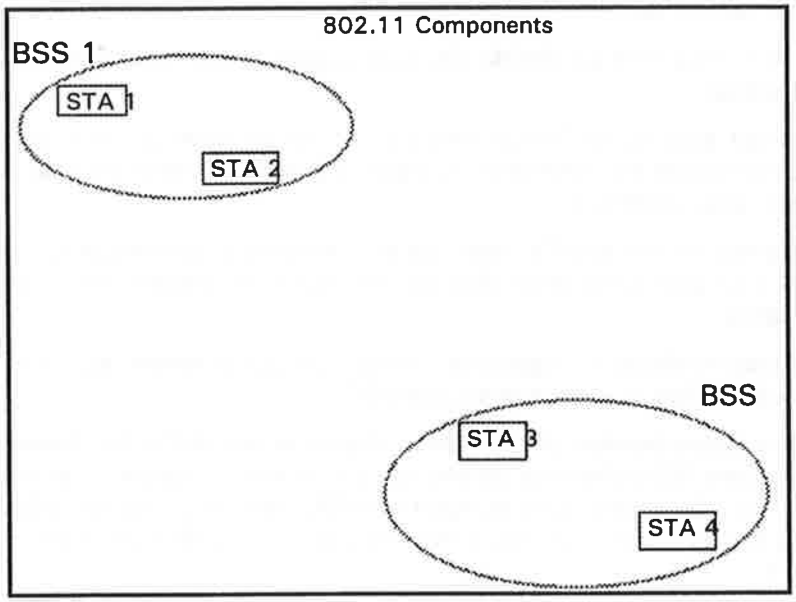


Figure 2-1: Basic Service Sets

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.

1.2.1. 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.

1.2.1.1. 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.

1.2.2. 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.

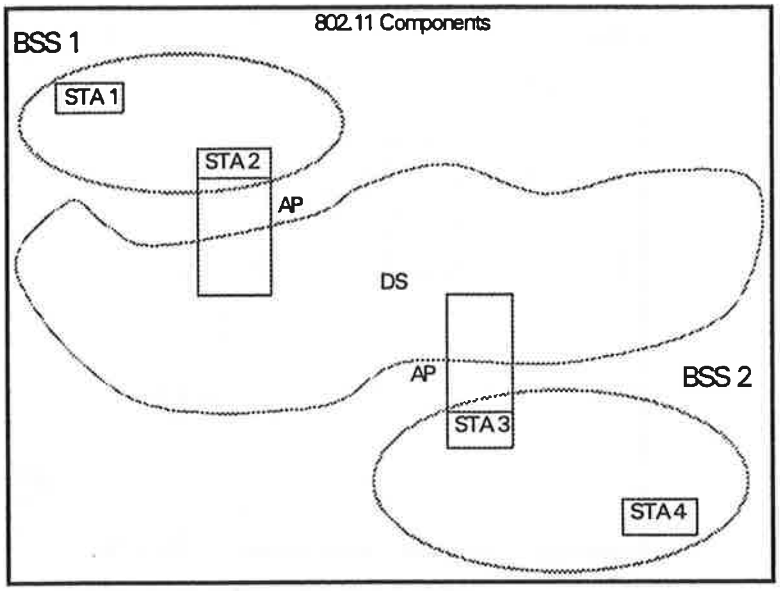


Figure 2-2: Distribution Systems and Access Points

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.

1.2.2.1. 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.

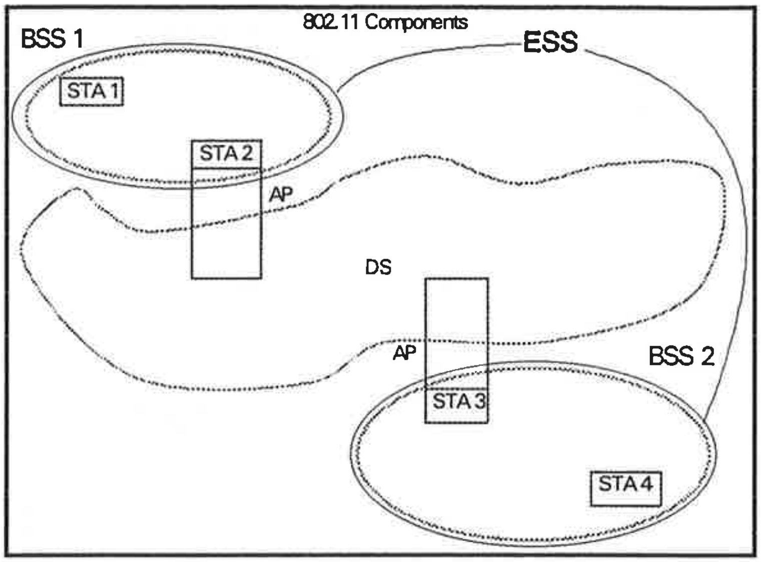


Figure 2-3: Extended Service Set

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.

1.2.3. 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.

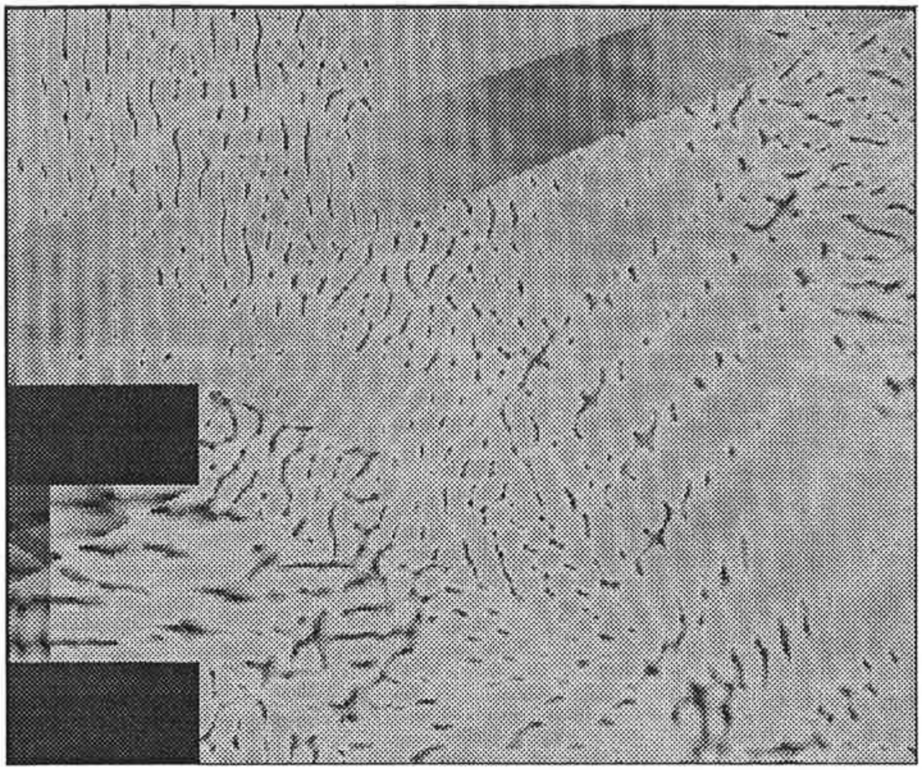


Figure 2-4: A Representative Signal Intensity Map

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?

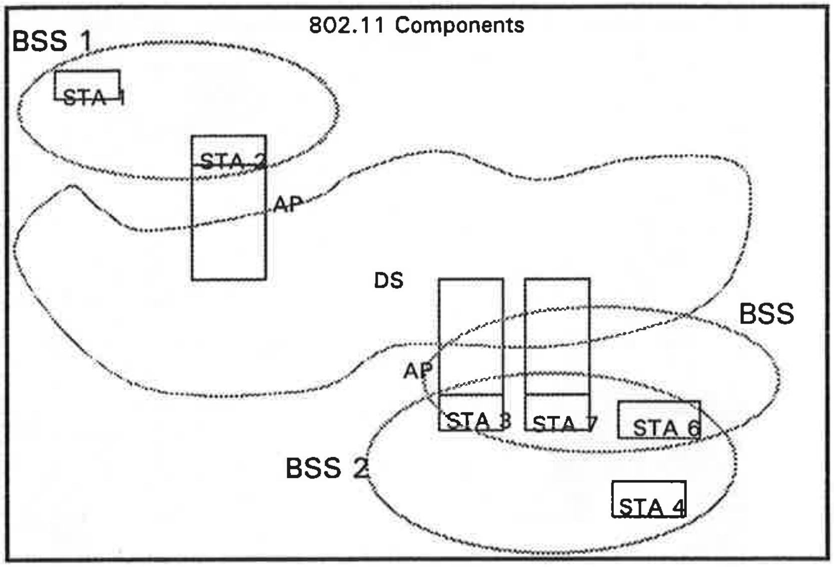


Figure 2-5: Collocated Coverage Areas

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

1.2.4. 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.

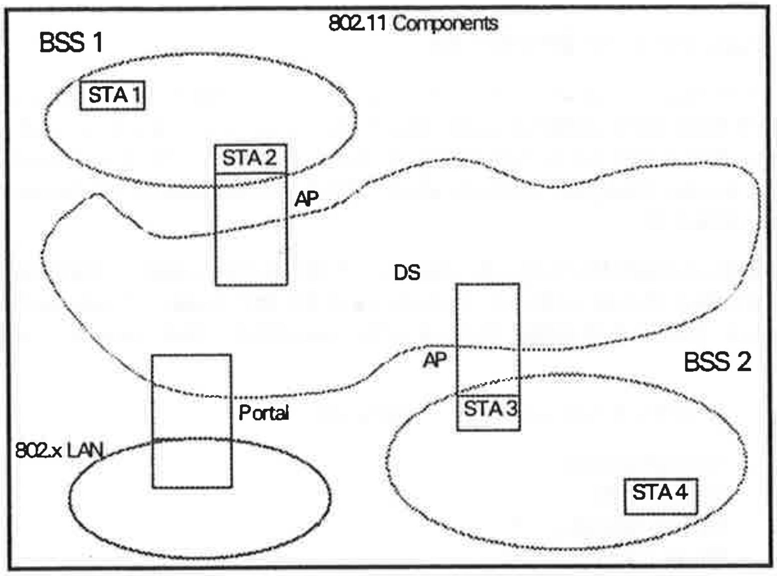


Figure 2-6: Connecting to Other 802 LANs

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.

1.2.4.1. 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.

1.3. 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) Disassociation
e) Distribution
f) Integration
g) Privacy
h) Reassociation

i) 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.

1.3.1. 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

1.3.2. 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.

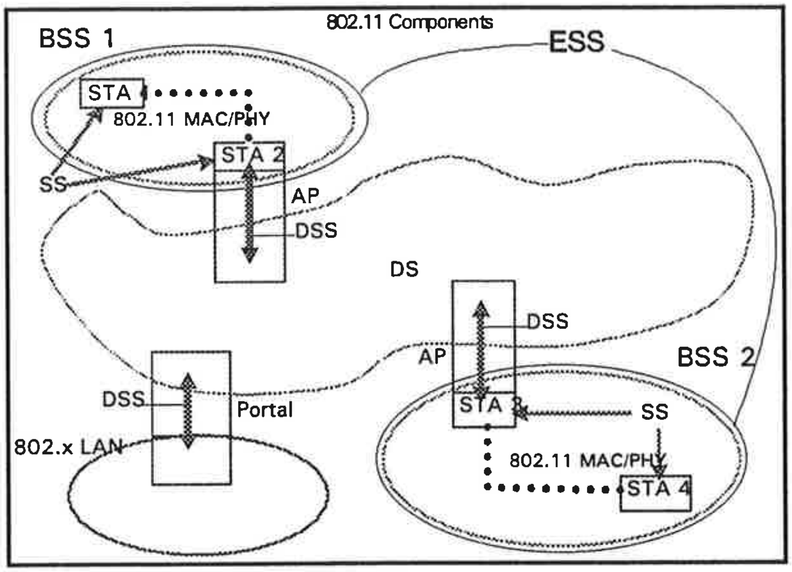


Figure 2-7: Complete 802.11 Architecture

1.3.3. 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).

1.4. 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.

1.4.1. Distribution of Messages Within a DS

1.4.1.1. 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).

1.4.1.2. 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.

1.4.2. 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.

1.4.2.1. 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.

1.4.2.2. 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.

1.4.2.3. 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.

1.4.2.4. 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).

1.4.3. 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-s_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.

1.4.3.1. 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 authentication processes. The 802.11 authentication mechanism also allows expansion of the supported 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 "sharedkey 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 shared, secret, ~~shared~~ WEP encryption key.

Management Information Base (MIB) function sare provided to support the standardized authentication schemes.

802.11 requires mutually acceptable, successful, authentication.

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

1.4.3.1.1. 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.

1.4.3.2. 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~~-causes an~~d~~ 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.

1.4.3.3. 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 perform the actual encryption of messages. MIB function-s are provided to support WEP.

Note that privacy may only be invoked for Data frames and some Authentication Management frames. All stations initially start "in the clear" in order to set up the Authentication and Privacy services.

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

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 X.X~~5.4~~ for more details.

1.5. 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.

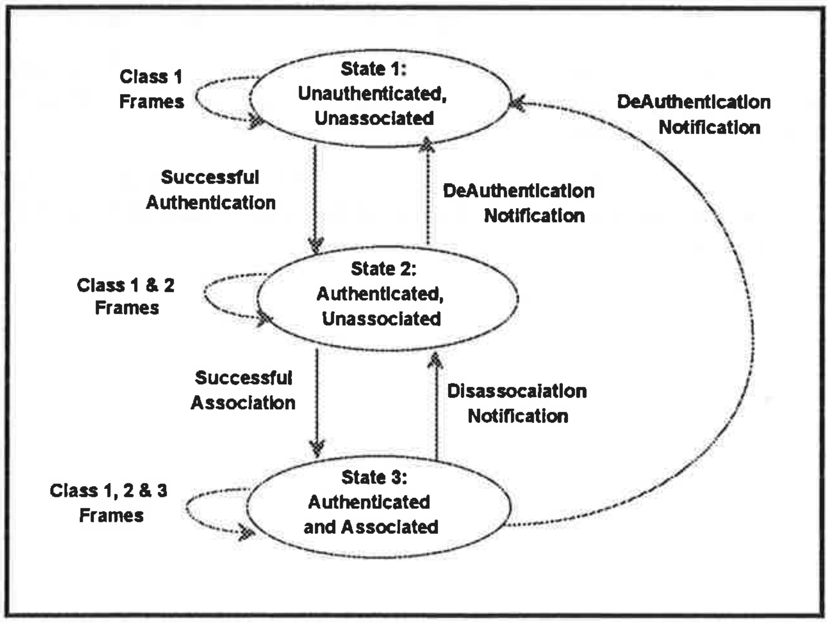

Class 1 Frames
State 1: Unauthenticated, Unassociated
DeAuthentication Notification
Successful Authentication
DeAuthentication Notification
Class 1 & 2 Frames
State 2: Authenticated, Unassociated
Successful Association
Disassocaiation Notification
Class 1, 2 & 3 Frames
State 3: Authenticated and Associated

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) ATIM
2) Association R/R
Successful Association enables Class 3 frames.
Unsuccessful Association leaves STA in state 2.
3) 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

1.6. 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.

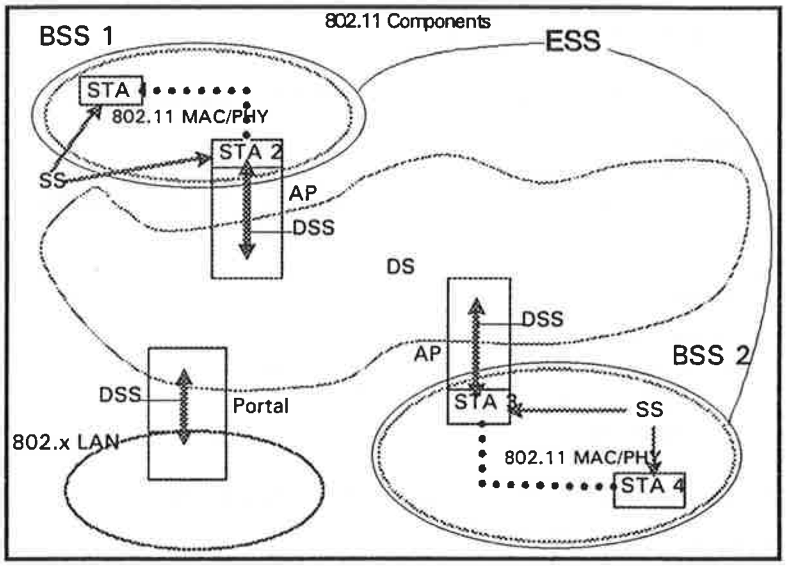


Figure 2-9: 802.11 Architecture (again)

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.

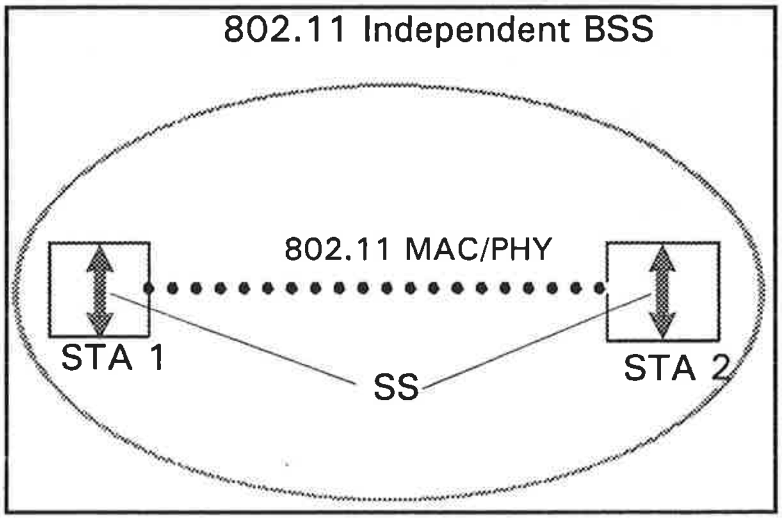


Figure 2-10: Logical Architecture of an Independent BSS

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.

1.7. 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.

1.7.1. 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

1.7.2. 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.
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.

1.7.3. 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.
    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.

1.7.4. 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).

1.7.5. Privacy

When two STAs wish to invoke the WEP privacy algorithm (as controlled by the related MIB variables, see section 7), the privacy service causes MSDU encryption and sets the WEP frame header bit appropriately (see section 4).

1.7.6. Authentication

When a STA wishes to authenticate with another STA, the authentication service causes one or more Authentication Management frames to be exchanged. The exact sequwnce of frames and their content is dependent on the authentication scheme invoked. For all authentication schemes, the authentication algorithm is identified within the Management frame body.

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.

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

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

Authentication (intermediate sequence frames)

Message type:
    Management
Message sub-type:
    Authentication
Information Items:
    Authentication Algorithm Identification.
    Authentication transaction sequence number.
    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

Authentication (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".
Direction of message:
    STA 2 to STA 1.

1.7.7. 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).

1.8. 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]).

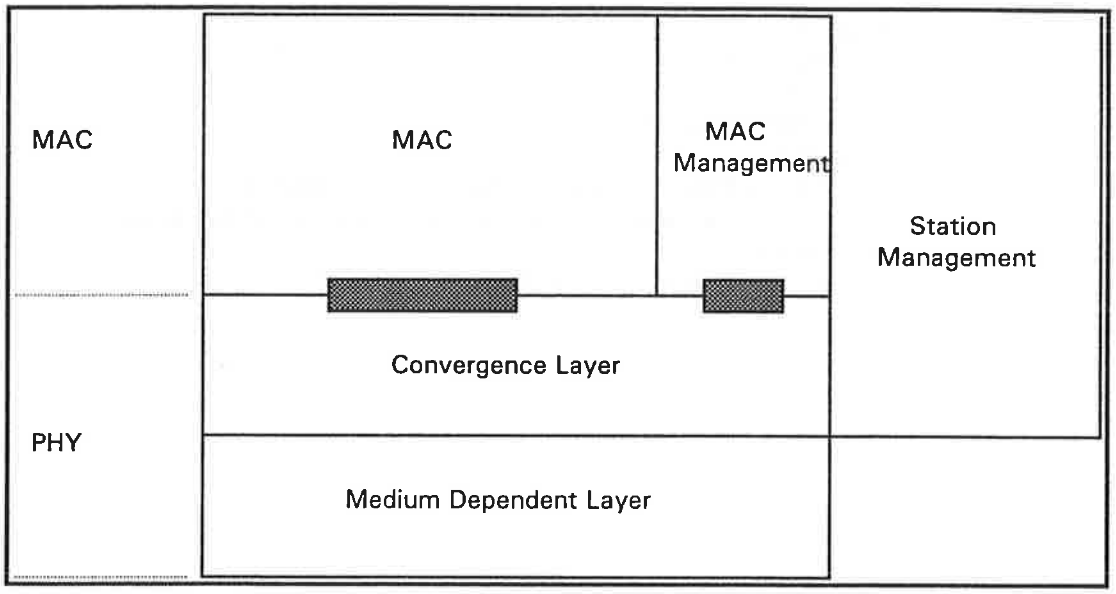


Figure 2-11, Portion of the ISO Basic Reference Model Covered in this Standard

1.9. Service Primitives

Proposal for Frame Processing Simplification by applying WEP to MPDU payload rather than MSDU payload.

David Bagby
Advanced Micro Devices
7 July 1995

This paper is very short. It simply proposes that WEP be applied to the MPDU body instead of the MSDU body.

This has the advantage of allowing a simpler interaction between Fragmentation and WEP (by applying WEP after fragmentation rather than before). With this change, it will not be necessary to receive an entire MSDU before decrypting the contents, resulting in implementation simplification.

Essentially, this change would logically move WEP processing from the top of the MAC layer to the bottom. Since WEP is invisible outside of the MAC layer, this change has no noticeable impact external to the MAC.

The included printed pages from D1.2 are the actual text alterations that would be required to implement this change to D1.2 text.

Moved:
That WEP processing be changed from an MSDU basis to and MPDU basis by adopting the changes shown to D1.2, said changes to be reflected in the next draft standard revision.

(Section 3) 1. MAC Service Definition

1.1. Overview of MAC Services

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 Asynchronous Data Service.

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.

1.1.3. Security Services

Security services in 802.11 shall be provided by the Authentication service and the Wired Equivalency Privacy mechanism], hereafter referred to as WEP. The scope of the security services provided is limited to Station-to-Station~~Data Exchange~~data exchange. The ~~confidentiality~~privacy service offered by an 802.11 ~~WEP~~ WEP implementation shall be the encipherment of the MSDU payload. For the purposes of this standard, ~~the~~ WEP is viewed as a logical sub-layer located within~~at the top of~~ the MAC sub-layer as shown in the reference model - section 2.4. Actual implementations of the WEP sub-layer are~~is~~ considered transparent to the LLC or other layers above the MAC sub-layer.

The security services provided by the WEP in 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.

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

The Layer 2 security services provided by ~~the~~ WEP rely on information from non-Layer 2 management or system entities. Management entities communicate ~~the~~ information to ~~the~~ WEP ~~entity~~ through a set of MIB variables.

1.1.4. Reordering of MPDUs

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

1.2. Detailed Service Specification

1.2.1. MAC Data Services

1.2.1.1. MA_UNITDATA.request

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.

Semantics of the Service Primitive

The semantics of the primitive are as follows:

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

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

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.

Effect of Receipt

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

1.2.1.2. MA_UNITDATA.indication

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.

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

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.

Effect of Receipt

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

1.2.2. MAC Management Services

To facilitate the three distribution system services:

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

1.2.3. Contention Free Connection Services

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

1.2.3.1. Function

Semantics of the Service Primitive

When Generated

Effect of Receipt

1.2.3.2. MA_CONNECTION_END.request

Function

Semantics of the Service Primitive

```
MA_CONNECTION_END.request          (
                                    connection_id
                                    )
```

When Generated

Effect of Receipt

1.2.3.3. MA_CONNECTION_END.indication

Function

Semantics of the Service Primitive

```
MA_CONNECTION_END.indication       (
                                    connection_id
                                    )
```

When Generated

Effect of Receipt

1.2.3.4. MA_CONNECTION_GRANT.indication

Function

Semantics of the Service Primitive

```
MA_CONNECTION_GRANT.indication     (
                                    connection_id
                                    )
```

When Generated

Effect of Receipt

1.2.3.5. MA_CONNECTION_NOT_GRANTED.indication

Function

Semantics of the Service Primitive

```
MA_CONNECTION_NOT_GRANTED.indication()
```

When Generated

Effect of Receipt

1.2.3.6. Access Point Initiates Connection Set-up Illustration

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

1. AP MAC user makes Start Connection Request. If the AP MAC believes that it can support this connection then the AP MAC generates Start Connection Request frame (otherwise the AP MAC asserts a Connection Not Granted Indication).
2. If the STA MAC can support this connection then it generates a Grant Connection frame and a Grant Connection Indication. On receipt of the Grant Connection Frame a Grant Connection Indication is generated.

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

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

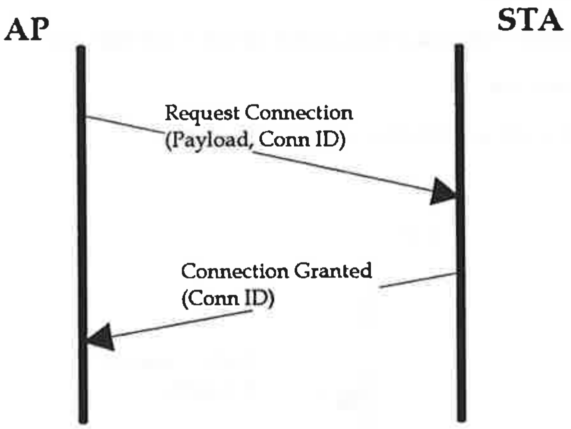


Figure 3-1: Connection Initiated by AP

1.2.3.7. Station Initiates Connection Set-up Illustration

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

1. STA MAC user makes a Start Connection Request. If the STA MAC can support this connection then it generates a Start Connection Request frame (otherwise it will assert the Connection Not Granted Indication).
2. If the AP MAC believes that it can support this connection request then it will generate a Grant Connection frame and a Grant Connection Indication.

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

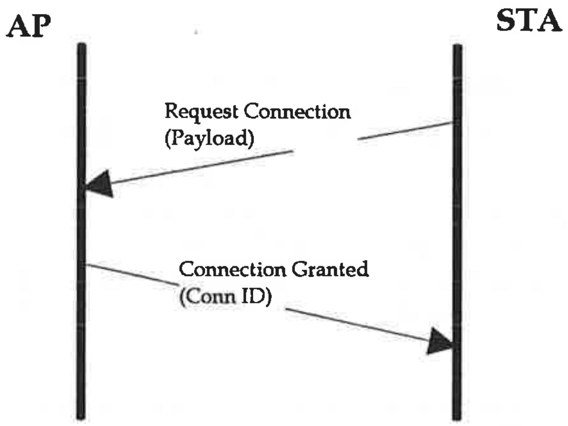


Figure 3-2: Connection Initiated by STA

1.2.3.8. End Connection

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

1. End Connection.

No MAC layer negotiation is needed to end a connection.

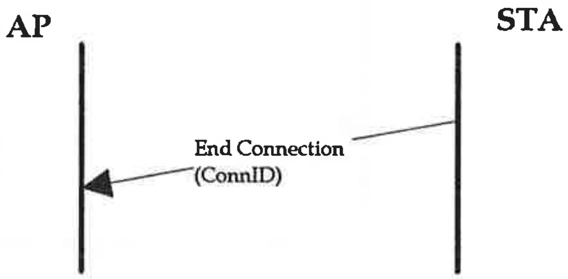


Figure 3-3: End Connection

Proposal for Frame Processing Simplification by applying WEP to MPDU payload rather than MSDU payload.

David Bagby
Advanced Micro Devices

7 July 1995

This paper is very short. It simply proposes that WEP be applied to the MPDU body instead of the MSDU body.

This has the advantage of allowing a simpler interaction between Fragmentation and WEP (by applying WEP after fragmentation rather than before). With this change, it will not be necessary to receive an entire MSDU before decrypting the contents, resulting in implementation simplification.

Essentially, this change would logically move WEP processing from the top of the MAC layer to the bottom. Since WEP is invisible outside of the MAC layer, this change has no noticeable impact external to the MAC.

The included printed pages from D1.2 are the actual text alterations that would be required to implement this change to D1.2 text.

Moved:
That WEP processing be changed from an MSDU basis to and MPDU basis by adopting the changes shown to D1.2, said changes to be reflected in the next draft standard revision.

(Section 4) 1. Frame and MPDU Formats

1.1. MAC Frame Formats

Each frame shall consist of the following basic components:

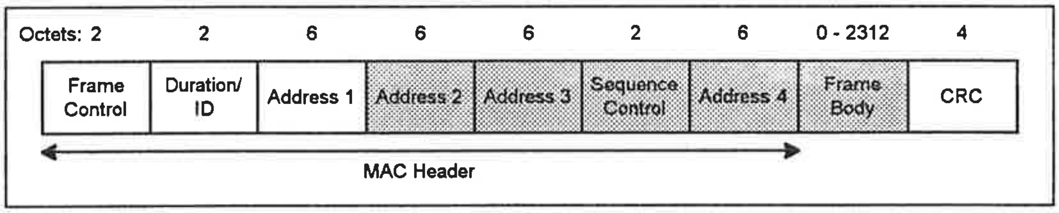
a) A *MAC Header*, which comprises frame control, duration, address and sequence control information.
b) A variable length *Frame Body*, that contains information specific to the frame *type*.
c) An IEEE 32-bit CRC.

1.1.1. General Frame Format

The MAC frame format comprises a set of fields that shall occur in a fixed order in all frames.

Figure 4-1 depicts the general MAC frame format. The fields that appear shaded are only present in certain frame types. Each field is defined in section 4.1.2. The format of the each of the individual frame types is defined in section 4.2.

A frame is an ordered octet string. The order of transmission of the octets of a frame shall be from left to right.



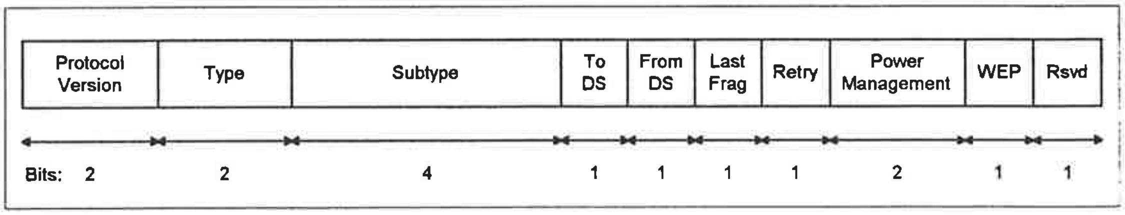
Octets: 2	2	6	6	6	2	6	0 - 2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	CRC

Figure 4-1: MAC Frame Format

1.1.2. Frame Fields

1.1.2.1. Frame Control Field

The Frame Control field shall consist of the following sub-fields: Protocol Version, Type, Subtype, To DS, From DS, Last Fragment, Retry, Power Management and WEP. The remaining subfields in the Frame Control field are reserved. All reserved bits and fields shall be set to '0'. Reserved bits and fields shall be ignored on reception.



Protocol Version	Type	Subtype	To DS	From DS	Last Frag	Retry	Power Management	WEP	Rsvd
Bits: 2	2	4	1	1	1	1	2	1	1

Figure 4-2: Frame Control Field

1.1.2.1.1. Protocol Version

The protocol version field shall be two bits in length and shall be invariant in size and placement across all revisions of the 802.11 standard. For this revision of the standard the value of the protocol version shall be 0. All other values are reserved. The revision level shall be incremented only when a fundamental incompatibility exists between a new revision and this revision of the standard. A device that receives a frame with a higher revision level than it can understand shall discard the frame without indication to LLC.

1.1.2.1.2. Type and Subtype

The Type field shall be two bits and the Subtype field four bits in length. The Type and Subtype fields shall together identify the function of the frame. There are three frame types: control, data and management. Each of the frame types have several defined subtypes. The table below defines the valid combinations 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	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101	Connection Request
00	Management	1110	Grant Connection
00	Management	1111	End Connection
01	Control	0000-1001	Reserved
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF End
01	Control	1111	CF End + CF-ACK
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null Function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000-1111	Reserved
11	Reserved	0000-1111	Reserved

Table 4-1: Valid Type/Subtype Combinations

1.1.2.1.3. To DS

The To DS field shall be one bit in length and shall be set to '1' in Data Type frames destined for the Distribution System. It shall be set to '0' in all other frames.

1.1.2.1.4. From DS

The From DS field shall be one bit in length and shall be set to '1' in Data Type frames exiting the Distribution System. It shall be set to '0' in all other frames.

The permitted To/From DS bit combinations and their meaning are given in table 4.2.

To/From DS Values	Meaning
To DS = '0' From DS = '0'	A Data Frame direct from one STA to another STA within the same BSS.
To DS = '1' From DS = '0'	Data Frame entering the DS.
To DS = '0' From DS = '1'	Data Frame exiting the DS.
To DS = '1' From DS = '1'	WDS frame being distributed from one AP to another AP.

Table 4-2: To / From DS Combinations

1.1.2.1.5. Last Fragment

The Last Fragment field shall be one bit in length and shall be set to '1' in a frame containing the last fragment of a fragmented MSDU, or the sole fragment of an unfragmented MSDU.

1.1.2.1.6. Retry

The Retry field shall be one bit in length and shall be set to '1' in a Data Type frame that is a retransmission of an earlier frame. A station shall use this indication to aid in the process of eliminating duplicate frames.

1.1.2.1.7. Power Management

The Power Management field shall be two bits in length and shall be used to indicate the power management state and buffered traffic state of the station. The value of this field shall remain constant in each frame within a frame sequence defined in section 4.3. The value shall indicate the state in which the station will be after the completion of the frame sequence. The permitted values for this field and their meaning are given in table 4–3.

Value	Description
00	Active Mode, with More buffered frames
01	PSP - Power Save, Polling
11	Active Mode, without More buffered frames

Table 4-3: Power Management Values

1.1.2.2. WEP

The WEP field shall be one bit in length. It shall be set to '1' if the Frame Body field contains information that has been processed by the WEP algorithm. The WEP bit may only be set to '1' within frames of Type Data and frames of Type Management, Subtype Authentication. The WEP bit shall be set to '0' in all other frames.

1.1.2.3. Duration/ID

The Duration/ID field shall be 16 bits in length. The contents of the this field shall be as follows:

a) In Data Type frames transmitted during the contention free period that have frame body information associated with a time-bounded connection, the Duration/ID field shall carry the connection identity of the time-bound connection.
b) In Control Type frames of SubType PS-Poll, the Duration/ID field shall carry the station identity (SID) of the station that transmitted the frame.
c) In all other frames the Duration/ID field shall contain a duration value. For frames transmitted during the contention period the duration value shall be set to the time in microseconds from the end of the current frame to the end of the next anticipated frame of Type Control and Subtype ACK. For frames transmitted during the contention free period the duration value shall be set to 0. The duration value shall be used to update the Net Allocation Vector according to the procedures defined in section 5.

1.1.2.4. Address Fields

There are four address fields in the MAC frame format. These fields are used to indicate the BSSID, source address, destination address, transmitting station address and receiving station address. The usage of the four address fields in each frame type will be indicated by the abbreviations BSSID, DA, SA, RA, TA indicating BSS Identifier, Destination Address, Source Address, Receiver Address and Transmitter Address, respectively. Some frames may omit some of the address fields.

1.1.2.4.1. Address Representation

Each Address field shall contain a 48-bit address as defined in section 5.2 of IEEE Std 802-1990.

1.1.2.4.2. Address Designation

A MAC Sublayer address is of one of two types:

a) Individual Address. The address associated with a particular station on the network.
b) Group Address. A Multidestination address, associated with one or more stations on a given network. There are two kinds of Group Addresses:
    1) Multicast-Group Address. An address associated by higher-level convention with a group of logically related stations.
    2) Broadcast Address. A distinguished, predefined multicast address that always denotes the set of all stations on a given local area network. All 1's in the Destination Address field shall be predefined to be the Broadcast address. This group shall be predefined for each communication medium to consist of all stations actively connected to that medium; it shall be used to broadcast to all the active stations on that medium. All stations shall be able to recognize the Broadcast Address. It is not necessary that a station be capable of generating the broadcast address.

The address space shall also be partitioned into locally administered and globally administered addresses. The nature of a body and the procedures by which it administers these global (U) addresses is beyond the scope of this standard. (Please refer to the IEEE Standard Overview and Architecture, IEEE Std 802-1990, ISBN 1-55937-052-1)

1.1.2.4.3. BSS Identifier

The BSS Identifier (BSSID) shall be a 48-bit field of the same format as an IEEE 802 MAC address. This field shall uniquely identify each BSS in an infrastructure LAN. The value of this field, in an infrastructure LAN, shall be the MAC address of the STA in the AP of the BSS. The mechanisms used to ensure the uniqueness of MAC addresses also create unique BSS Identifiers. The Individual/Group bit of the address shall be transmitted as zero.

In an ad hoc LAN, this field shall be transmitted with the BSS ID of the ad hoc network. The value of this field, in an ad-hoc LAN, shall be the MAC address of the STA that initiated the ad-hoc network.

1.1.2.4.4. Destination Address

The destination address (DA) field shall contain an IEEE MAC individual or group address that identifies the MAC entity or entities intended as the final recipient(s) of the MSDU (or fragment thereof) contained in the frame body field.

1.1.2.4.5. Source Address

The source address (SA) field shall contain an IEEE MAC individual address that identifies the MAC entity from which the transfer of the MSDU (or fragment thereof) contained in the frame body field was initiated. The Individual/Group bit shall always be transmitted as a zero in the source address

1.1.2.4.6. Receiver Address

The receiver address (RA) field shall contain an IEEE MAC individual or group address address that identifies the intended immediate recipient STA(s), on the wireless medium, for the MPDU contained in the frame body field.

1.1.2.4.7. Transmitter Address

The transmitter address (TA) field shall contain an IEEE MAC individual address that identifies the STA which transmitted, onto the wireless medium, the MPDU contained in the frame body field. The Individual/Group bit shall always be transmitted as a zero.

1.1.2.5. Sequence Control

The Sequence Control field shall be 16 bits in length and shall consist of two subfields, the Sequence Number and the Fragment number. The format of the Sequence Control field is illustrated in figure 4-3.

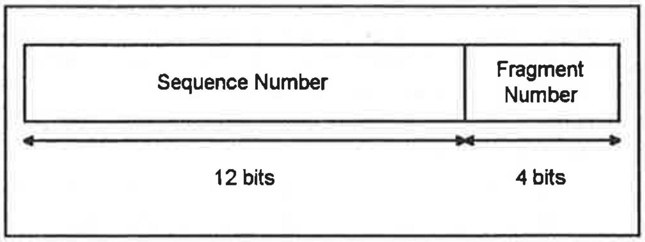


Figure 4-3: Sequence Control Field

1.1.2.5.1. Sequence Number

The Sequence Number shall be a 12 bit field indicating the sequence number of the MSDU. MSDUs shall be numbered sequentially starting at zero. Each transmission of an MSDU or fragment thereof shall contain the sequence number of that MSDU. The sequence number shall remain constant in all retransmissions of an MSDU or fragment.

1.1.2.5.2. Fragment Number

The Fragment Number shall be a 4 bit field indicating the number of each fragment of an MSDU. The fragment shall be set to zero in the first or only fragment of an MSDU and shall be incremented by one for each successive fragment of that MSDU.

1.1.2.6. Frame Body

The Frame Body shall be a variable length field and shall contain information specific to individual frame types and subtypes.. The minimum frame body shall be zero octets~~ and the maximum 2312 octets~~. The maximum length frame body is defined by the maximum length (MSDU + ICV + IV); where ICV and IV are the WEP fields defined in section X.X~~n.n~~.

1.1.2.7. CRC

The CRC field shall be a 32 bit field containing a 32-bit Cyclic Redundancy Check (CRC). The CRC shall be calculated over all the fields of the MAC header and the frame body field. These are referred to as the calculation fields.

The CRC shall be calculated using the following standard generator polynomial of degree 32:

$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1$

The CRC shall be the one's complement of the sum (modulo 2) of the following:

1) The remainder of $x^{k}*(x^{31} + x^{30} + x^{29} + ... + x^{2} + x + 1)$ divided (modulo 2) by G(x), where k is the number of bits in the calculation fields, and

2) The remainder after multiplication of the contents (treated as a polynomial) of the calculation fields by x^{32} and then division by G(x).

The CRC field shall be transmitted commencing with the coefficient of the highest order term.

As a typical implementation, at the transmitter, the initial remainder of the division is preset to all ones and is then modified by division of the calculation fields by the generator polynomial G(x). The ones complement of this remainder is transmitted, with the most significant bit first, as the CRC field.

At the receiver, the initial remainder is preset to all ones and the serial incoming bits of the calculation fields and CRC, when divided by G(x) results in the absence of transmission errors, in a unique non-zero remainder value. The unique remainder value is the polynomial:

$x^{31} + x^{30} + x^{26} + x^{25} + x^{24} + x^{18} + x^{15} + x^{14} + x^{12} + x^{11} + x^{10} + x^{8} + x^{6} + x^{5} + x^{4} + x^{3} + x + 1$

1.2. Format of Individual Frame Types

1.2.1. Control Frames

In the following descriptions, "immediately previous" frame means a frame, the reception of which concluded within the prior SIFS interval.

The subfields within the Frame Control field of Control frames shall be set as illustrated in figure 4-4 below.

Protocol Version	Type	Subtype	To DS	From DS	Last Frag	Retry	Power Management	WEP	Rsvd
Protocol Version	Control	Subtype	0	0	0	0	Power Management	0	0
Bits: 2	2	4	1	1	1	1	2	1	1

Figure 4-4: Frame Control field subfield values within Control Frames

1.2.1.1. RTS Frame Format

The frame format for the RTS frame shall be as defined in Figure 4-5.

octets: 2	2	6	6	4
Frame Control	Duration	RA	TA	CRC

MAC Header

Figure 4-5: RTS Frame

The RA of the RTS frame shall be the address of the STA, on the wireless medium, that is the intended immediate recipient of the pending directed Data or Management frame.

In an infrastructure BSS, the RA shall always designate the AP with which the STA transmitting the RTS frame is associated.

The TA shall be the address of the STA transmitting the RTS frame.

1.2.1.2. CTS Frame Format

The frame format for the CTS frame shall be as defined in Figure 4-6.

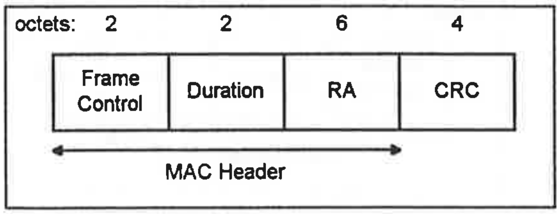


Figure 4-6: CTS Frame

The Receiver Address (RA) of the CTS frame shall be copied from the Transmitter Address (TA) field of the immediately previous RTS frame to which the CTS is a response.

1.2.1.3. ACK Frame Format

The frame format for the ACK frame shall be as defined in Figure 4-7.

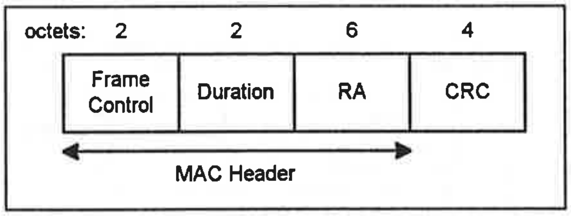


Figure 4-7: ACK Frame

The Receiver Address of the ACK frame shall be copied from the Address 2 field of the immediately previous directed Data or Management frame.

1.2.1.4. PS-Poll Frame Format

The frame format for the Power Save Poll (PS-Poll) frame shall be as defined in Figure 4-8.

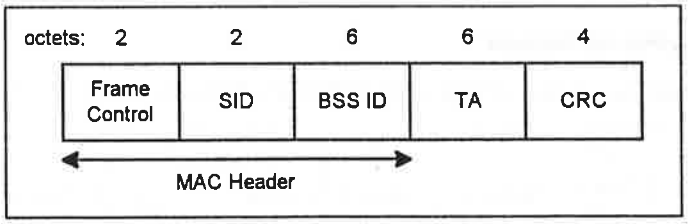
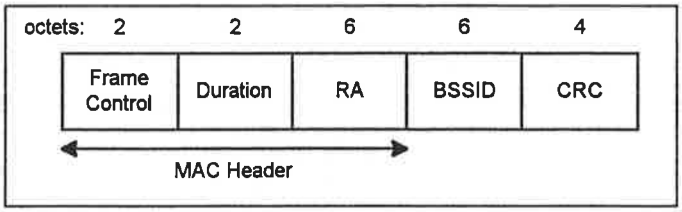


Figure 4-8: PS-Poll Frame

The BSS Identifier shall be the address of the STA contained in the AP. The Transmitter Address (TA) shall be the address of the STA transmitting the frame. The SID shall be the value assigned by the AP in the Associate Response frame.

1.2.1.5. CF-End Frame Format

The frame format for the Contention Free-End (CF-END) frame shall be as defined in Figure 4-9.



octets:	2	2	6	6	4
	Frame Control	Duration	RA	BSSID	CRC

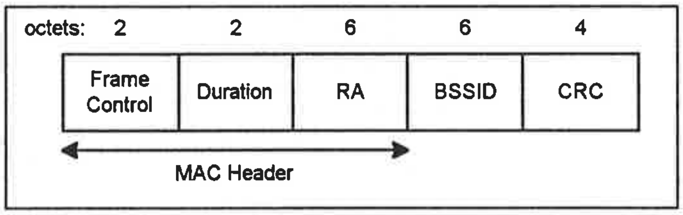
Figure 4-9: CF-End Frame

The BSS Identifier shall be the address of the STA contained in the AP. The Receiver Address (RA) shall be the broadcast group address.

The Duration field shall be set to 0.

1.2.1.6. CF-End+CF-ACK Frame Format

The frame format for the Contention Free-End Acknowledge (CF-END + CF-ACK) frame shall be as defined in Figure 4-10.



octets:	2	2	6	6	4
	Frame Control	Duration	RA	BSSID	CRC

Figure 4-10: CF-End + CF-ACK Frame

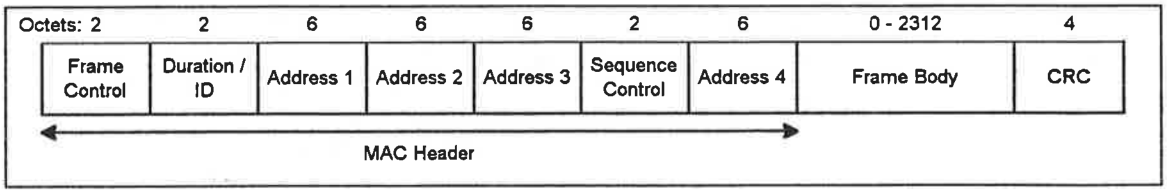
The BSS Identifier shall be the address of the STA contained in the AP. The Receiver Address (RA) shall be the broadcast group address.

The Duration field shall be set to 0.

1.2.2. Data Frames

1.2.2.1. DATA Frame Format

The frame format for a Data frame is independent of subtype and shall be as defined in Figure 4-11.



Octets: 2	2	6	6	6	2	6	0 - 2312	4
Frame Control	Duration / ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	CRC

Figure 4-11: DATA Frame

The contents of the Address fields of the Data frame shall be dependent upon the values of the To DS and From DS bits and are defined in table 4-4, below. Where the content of a field is shown as N/A, the field shall be omitted.

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Table 4-4: Address Field Contents

A station shall use the contents of Address 1 field to perform address matching for receive decisions. In cases where the Address 1 field contains a group address, the BSSID must also be validated to ensure that the broadcast, or multicast originated in the same BSS.

A station shall use the contents of the Address 2 field to direct the acknowledgement if an acknowledgement is necessary.

The DA shall be the destination of the MSDU (or fragment thereof) in the frame body field.

The SA shall be the address of the MAC entity initiating the transmission of the MSDU (or fragment thereof) in the frame body field.

The RA shall be the address of the STA contained in the AP in the wireless distribution system that is the next immediate intended recipient of the frame.

The TA shall be the address of the STA contained in the AP in the wireless distribution system that is transmitting the frame.

The BSSID of the Data frame shall be determined as follows:

a) If the station is an AP or is associated with an AP, the BSS Identifier shall be the address of the STA contained in the AP.

b) If the station is a member of an ad hoc LAN, the BSS Identifier shall be the BSS ID of the ad hoc LAN.

The Frame Body shall consist of~~be~~ the MSDU or a fragment thereof, and a~~plus the~~ WEP IV and ICV (IFF~~if~~ the WEP subfield in the frame control field is set to '1'). The frame body is null (zero octets length) in Data frames of Subtype 01xx.

Data frames sent during the contention period shall use the Data Subtypes 0000, or 0100. Data frames sent by the PCF during the contention free period shall use the appropriate ones of the Data Subtypes 0000–0111 based upon the usage rules:

Data Subtypes 0010, 0011, 0110, and 0111 shall only be sent by a PCF.

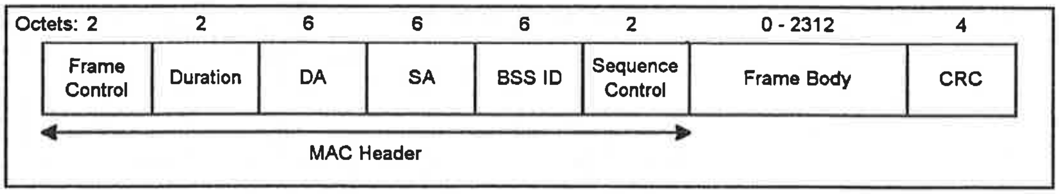
Data Subtypes 0000, 0001, 0100, and 0101 may be sent by any CF-aware station.

Stations receiving Data frames shall only process the Data frame body, and shall only consider the frame body as the basis of a possible indication to LLC, if the Data Subtype is of the form 00xx. Stations capable of transmitting in response to polling by a PCF shall interpret all Subtype bits of received Data frames for CF purposes, but shall only inspect the frame body if the Subtype is of the form 00xx.

All stations shall process the duration field contents of valid data frames to update their NAV settings as appropriate under the coordination function rules.

1.2.3. Management Frames

The frame format for a Management frame is independent of subtype and shall be as defined in Figure 4-12.



Octets: 2	2	6	6	6	2	0 - 2312	4
Frame Control	Duration	DA	SA	BSS ID	Sequence Control	Frame Body	CRC

Figure 4-12: Management Frame Format

The address fields for Management frames shall not vary by frame subtype.

The BSS Identifier of the Management frame shall be determined as follows:

a) If the station is an AP or is associated with an AP, the BSS Identifier shall be the address of the STA contained in the AP.

b) If the station is a member of an ad hoc LAN, the BSS Identifier shall be the BSS ID of the ad hoc LAN.

c) In Management frames of Subtype Probe, the BSSID shall either be a specific BSSID, or the broadcast BSSID as defined in the procedures specified in section 7.

The DA shall be the destination of the frame.

The SA shall be the address of the station transmitting the frame.

The Frame Body shall consist of the fixed fields and information elements defined for each management frame subtype. All fixed fields and information elements are mandatory unless stated otherwise and shall only appear in the specified order. Stations encountering an element type they do not understand shall ignore that element. Element type codes not explicitly defined in the standard are reserved, and shall not appear in any frames.

1.2.3.1. BEACON Frame Format

The Frame Body of a Management frame of Subtype Beacon shall contain the following information:

Order	Information	Note
1	Timestamp	
2	Beacon Interval	
3	Regulatory Domain	
4	Capability Information	
5	ESS ID	
6	Supported Rates	
7	FH Parameter Set	1
8	CF Parameter Set	2
9	DTIM	
10	TIM	

Notes:

1 The FH Parameter Set information shall be mandatory only within Beacon Frames generated by STAs using Frequency Hopping Physical Layers

2 The CF Parameter Set information shall be mandatory only within Beacon Frames generated by APs supporting a PCF

1.2.3.2. Disassociation Frame Format

The Frame Body of a Management frame of Subtype Disassociation shall contain the following information:

Order	Information	Note
1	Status Code	

1.2.3.3. Association Request Frame Format

The Frame Body of a Management frame of Subtype Association Request shall contain the following information:

Order	Information	Note
1	Capability Information	
2	ESSID	
3	Supported Rates	

1.2.3.4. Association Response Frame Format

The Frame Body of a Management frame of Subtype Association Response shall contain the following information:

Order	Information	Note
1	Capability Information	
2	Status Code	
3	Station ID (SID)	
4	Supported Rates	

1.2.3.5. Reassociation Request Frame Format

The Frame Body of a Management frame of Subtype Reassociation Request shall contain the following information:

Order	Information	Note
1	Capability Information	
2	Current AP Address	
3	ESSID	
4	Supported Rates	

1.2.3.6. Reassociation Response Frame Format

The Frame Body of a Management frame of Subtype Reassociation Response shall contain the following information:

Order	Information	Note
1	Capability Information	
2	Status Code	
3	Station ID (SID)	
4	Supported Rates	

1.2.3.7. Probe Request Frame Format

The Frame Body of a Management frame of Subtype Probe Response shall contain the following information:

Order	Information	Note
1	Capability Information	
2	ESSID	
3	Supported Rates	

1.2.3.8. Probe Response Frame Format

The Frame Body of a Management frame of Subtype Probe Response shall contain the following information:

Order	Information	Note
1	Timestamp	
2	Beacon Interval	
3	Regulatory Domain	
4	Capability Information	
5	ESS ID	
6	Supported Rates	
7	FH Parameter Set	1
8	CF Parameter Set	2

Notes:

1 The FH Parameter Set information shall be mandatory only within Probe Response Frames generated by STAs using Frequency Hopping Physical Layers

2 The CF Parameter Set information shall be mandatory only within Probe Response Frames generated by APs supporting a PCF

1.2.3.9. Authentication Frame Format

The Frame Body of a Management frame of Subtype Authentication shall contain the following information:

Order	Information	Note
1	Authentication Algorithm Number	
2	Authentication Transaction Sequence Number	
3	Status Code	1
4	Challenge Text	2

Notes:

1 The Status Code information shall be reserved and set to 0 in the Authentication frames defined in the table below.

2 The Challenge Text Information shall only be present in the Authentication frames defined in the table below.

Authentication Algorithm Number	Authentication Trans. Sequence Number	Status Code	Challenge Text
Open System	1	reserved	not present
Open System	2	status	not present
Shared Key	1	reserved	not present
Shared Key	2	reserved	present
Shared Key	3	reserved	present
Shared Key	4	status	not present

1.2.3.10. Deauthentication

The Frame Body of a Management frame of Subtype Deauthentication shall contain the following information:

Order	Information	Note
1	Status Code	

1.2.3.11. Connection Request

The Frame Body of a Management frame of Subtype Connection Request shall contain the following information:

Order	Information	Note
TBD		

1.2.3.12. Grant Connection

The Frame Body of a Management frame of Subtype Grant Connection shall contain the following information:

Order	Information	Note
TBD		

1.2.3.13. End Connection

The Frame Body of a Management frame of Subtype End Connection shall contain the following information:

Order	Information	Note
TBD		

1.3. Management Frame Body Components

Within Management frames, fixed length mandatory frame body components are defined as fixed fields, variable length mandatory and all optional frame body components are defined as information elements.

1.3.1. Fixed Fields

1.3.1.1. Timestamp

This field shall represent the value of the TSFTIMER of a frame's source. The element specific field length is eight octets.

1.3.1.2. Beacon Interval

The Beacon Interval field shall represent the number of milliseconds between Beacon generations. The length of the Beacon Interval field is one octet.

1.3.1.3. Regulatory Domain

The Regulatory Domain field shall identify a regulatory domain. The following values are defined:

1	USA
2	Europe
3	Japan

All other values are reserved

The length of the Regulatory Domain field is one octet.

1.3.1.4. Capability Information

The Capability Information field contains a number of subfields that are used to indicate requested or advertised capabilties. The length of the Capability Information octet is one octet. The following subfields are defined:

Bit 0:	Infrastructure BSS
Bit 1:	Ad-hoc BSS
Bit 2:	CF-aware
Bit 3:	CF Polling Request
Bits 4 - 7:	Reserved

1.3.1.5. Station ID (SID)

The Station ID (SID) field shall be a value assigned by an AP during association and shall represent the 16-bit ID of a station. The length of the SID field is two octets.

1.3.1.6. Current AP Address

The Current AP Address field shall be the MAC address of the access point with which the station is currently associated. The length of the Current AP Address field is six octets.

1.3.1.7. Authentication Algorithm Number

The Authentication Algorithm Number field shall indicate a single authentication algorithm. The length of the Authentication Algorithm Number field is two octets. The following values are defined:

Authentication Algorithm Number = 0: Open System
Authentication Algorithm Number = 1: Shared Key
All other values of Authentication Number shall be reserved.

1.3.1.8. Authentication Transaction Sequence Number

The Authentication Transaction Sequence Number field shall indicate the current state of progress through a multi-step transaction. The length of the Authentication Transaction Sequence Number is one octet.

1.3.1.9. Status Code

This Status Code shall be used to indicate the success of failure of an operation. The length of the status code field is one octet. If an operation is successful then the Status Code shall be set to 0. If an operation results in failure the Status Code shall indicate a failure cause. The following failure cause codes are defined: *TBD*

1.3.2. Information Elements

Elements are defined to have a common general format consisting of a one-octet Element ID field, a one octet length field and a variable-length element-specific information field. Each element is assigned a unique Element ID as defined in this specification. The length field shall specify the number of octets in the information field.

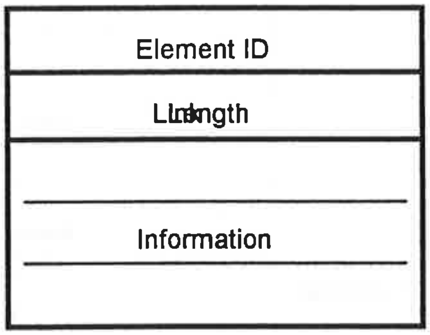


Figure 4-13, Element Format

The set of valid elements is defined below.

Information Element	Element ID
ESSID	0
Supported Rates	1
FH Parameter Set	2
CF Parameter Set	3
DTIM	4
TIM	5
Challenge Text	6

1.3.2.1. DTIM

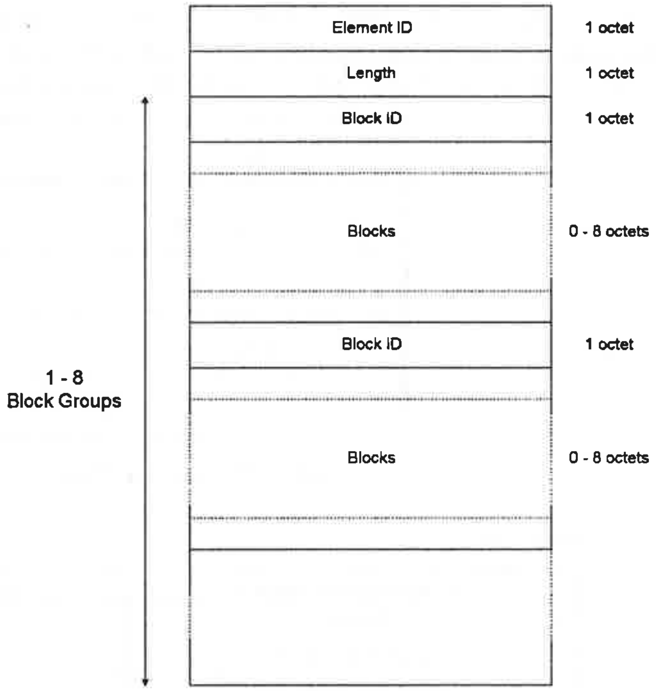
The DTIM element shall contain two fields DTIM Count and DTIM Period.

Element ID	1 octet
Length	1 octet
DTIM Period	1 octet
DTIM Count	1 octet

The DTIM count field shall indicate how many Beacons (including the current frame) will appear before the next DTIM. A DTIM Count of 0 shall indicate that the current TIM is a DTIM. The DTIM count field shall be a single octet.

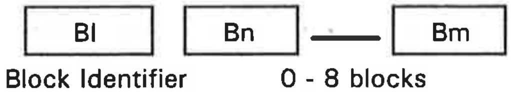
The DTIM period field shall indicate the number of Beacon intervals between successive DTIMs. If all TIMs are DTIMs, the DTIM Period field shall have value 1. The DTIM period field shall be a single octet.

1.3.2.2. Traffic Indication Map (TIM)



The TIM Element information field shall contain between one and eight *block groups*, with each block group consisting of a *block identifier* followed by 0 to 8 one-octet *blocks*. Each bit within a block shall indicate whether a frame is currently buffered for a station with a particular Station ID. There is a one-to-one mapping between the bits in a *virtual bit map* and the station IDs. The virtual bit map is maintained within the access point; the actual transmitted TIM is a compressed representation of the virtual bit map. .

Block Group: Consists of a Block Identifier followed by from 0 to 8 Blocks.



BI: Block Identifier (1 octet)

b0							b7
B1	B2	B3	B4	B5	B6	B7	B8

Bit N (N = 1..8) 0 = Nth block in this group is absent
1 = Nth block in this group is present

Block (8 bits) Each bit corresponds to a specific station within the block. If this block represents the Nth block within the virtual bit map, then Bit M within the block shall correspond to the station with Station ID equal to 8*(N-1) + M.
Bit = 1: There is a frame pending for this station
Bit = 0: There is no frame pending for this station.

1.3.2.3. ESS ID

The ESSID element shall indicate the identity of the Extended Service Set.

Element ID	1 octet
Length	1 octet
ESS ID	0 - 32 octets

The ESSID Information field shall be between 0 and 32 octets. A zero octet information field shall indicate the broadcast ESSID.

1.3.2.4. FH Parameter Set

The FH Parameter Set element shall contain the set of parameters necessary to allow synchronisation for STAs using a Frequency Hopping (FH) Physical Layer. The information field shall contain Dwell Time, Hop Set, Hop Pattern and Hop Index parameters. The total length of the information field shall be 5 octets.

Element ID	1 octet
Length	1 octet
Dwell Time (ms)	2 octets
Hop Set	1 octet
Hop Pattern	1 octet
Hop Index	1 octet

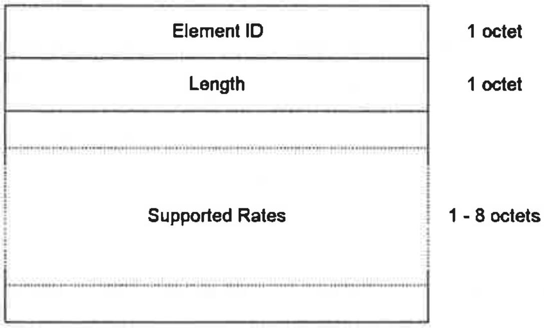
The Dwell Time field shall be two octets in length and contain the Dwell Time in ms.

The Hop Set field shall identify the particular set of hop patterns and shall be a single octet. The Hop Pettern field shall identify the individual pattern within a set of hop patterns and shall be a single octet.

The Hop Index field shall select the channel index within a pattern and shall be a single octet.

1.3.2.5. Supported Rates

The Supported Rates element shall specify all the rates in which this station is capable to receive. The information field is encoded as 1 to 8 octets where each octet describes a single supported rate in units of 100 kbit/s (e.g. a 1 Mbps rate will be encoded as 0x0A).



1.3.2.6. Connection ID

The Connection ID element shall be used to specify a unique identifier for a time bounded connection to transfer data between an access point and a station. Each connection ID shall be unique for a given station. The element specific field length is two octets.

[needs work - SAB]

1.3.2.7. CF Parameter Set

The CF Parameter Set element shall contain the set of parameters necessary to support the PCF. The information field shall contain CF Maximum Duration and ?? parameters. The total length of the information field shall be n octets.

[needs work - SAB]

1.3.2.8. Challenge Text

The Challenge Text element shall contain the challenge text within Authentication exchanges. The element information field length shall be dependent upon the authentication algorithm and the transaction sequence number as specified in the Authentication and Secuity section. ~~128 octets in length~~.

~~[needs work - SAB]~~

1.4. Frame Exchange Sequences

The following frame sequences are valid:

a) DATA
b) DATA-DATA (fragmented broadcast MSDU)
c) DATA - ACK
d) RTS - CTS - DATA - ACK
e) DATA - ACK - DATA - ACK (fragmented MSDU)
f) RTS - CTS - DATA - ACK - DATA - ACK (fragmented MSDU)
g) POLL - DATA - ACK
h) POLL - DATA - ACK - DATA - ACK (fragmented MSDU)
i) POLL - ACK (no data)
j) REQUEST - ACK
k) RESPONSE - ACK

Proposal for Frame Processing Simplification by applying WEP to MPDU payload rather than MSDU payload.

David Bagby
Advanced Micro Devices
7 July 1995

This paper is very short. It simply proposes that WEP be applied to the MPDU body instead of the MSDU body.

This has the advantage of allowing a simpler interaction between Fragmentation and WEP (by applying WEP after fragmentation rather than before). With this change, it will not be necessary to receive an entire MSDU before decrypting the contents, resulting in implementation simplification.

Essentially, this change would logically move WEP processing from the top of the MAC layer to the bottom. Since WEP is invisible outside of the MAC layer, this change has no noticeable impact external to the MAC.

The included printed pages from D1.2 are the actual text alterations that would be required to implement this change to D1.2 text.

Moved:
That WEP processing be changed from an MSDU basis to and MPDU basis by adopting the changes shown to D1.2, said changes to be reflected in the next draft standard revision.

(Section 5) 1. Authentication and Privacy

Note to Editors: This section was inserted into D1.2 after section 4. It was supposed to be inserted immediately after section 3. It is written to follow section 2 and 3 as it contains the description of the logical information needed for the authentication management messages and thus should precede the details of fame formats in section 4. Please move this section as part of the next draft revision (at which time this editor's note should be deleted from the draft). - Dave Bagby

0.1. Authentication Services

802.11 defines two subtypes of authentication service; “Open System” and “Shared Key”. The subtype invoked is indicated in the body of authentication management frames. Thus authentication frames are self identifying~~idenfitfying~~ with re~~r~~spect to authentication algorithm.

0.1.1. Open System Authentication

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

Open system~~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.

0.1.1.1. 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 algorithm~~algortithm~~ dependent information~~infromation~~ (none)
Direction of message:
From authentication initiating STA

This frame shall be sent with WEP OFF.

0.1.1.2. 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 algorithm~~algortithm~~ dependent information~~infromation~~. (none)
The result of the requested authentication. This is a fixed length item with values "successful" and "unsuccessful".
Direction of message:
From authenticating~~authenticatiing~~ station to initiating station.

This frame shall be sent with WEP OFF.

0.1.2. 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.

The~~refore, this~~ Shared Key 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 which~~wich~~ is independent~~independnt~~ of 802.11. This shared key is stored in a write~~read-~~only MIB variable via the MAC management path.

0.1.2.1. 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 algorithm~~algortithm~~ dependent information~~infromation~~ (none)
- Direction of message:
    - From authentication initiating STA

This frame shall be sent with WEP OFF.

0.1.2.2. 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 algorithm~~algortithm~~ dependent information~~infromation~~ = Challenge~~Challlenge~~ text.
        - This fieled shall be of fixed length of 128 octets. The field shall be filled with octets generated by the WEP mechanism using a random initial seed.~~.~~
- Direction of message:
    - To authentication initiating STA

This frame shall be sent with WEP OFF.

0.1.2.3. Shared Key Authentication (Third frame)

The station which received~~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 algorithm~~algortithm~~ dependent information~~infromation~~ = challenge text from sequence two frame.
Direction of message:
From authentication initiating STA

This frame shall be sent with WEP ON.

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

The stations which receives~~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 sufficient~~suffeient~~ ~~proof that the~~ authentication for the two ~~requesting~~ stations involved in the authentication sequence. Upon successful completion of the authentication sequence, both stations shall change their state with respect to each other to "Authenticated ~~shall become succesfully authenticated.~~

Message type:
Management
Message sub-type:
Authentication
Information Items:
Authentication Algorithm Identification = " shared key~~open system~~"
Authentication transaction sequence number = 4
Authentication algorithm~~algortithm~~ dependent information~~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.

0.2. The Wired Equivalent Privacy (WEP) Algorithm~~ (WEP)~~

0.2.1. 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 privacy 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.

0.2.2. 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 encrypts each message independentlyis ~~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 for~~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:

The implementation and use of WEP is an 802.11 option.

0.2.3. 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,

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

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:*

$$E_k(P) = C$$

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

$$D_k(C) = P$$

As illustrated in Figure 5-1, note that if the same key is used for encryption and decryption then

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

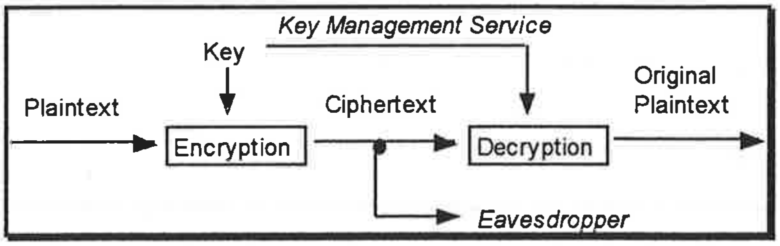


Figure 5-1: A Confidential Data Channel

The WEP algorithm is a form of stream cipher~~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.

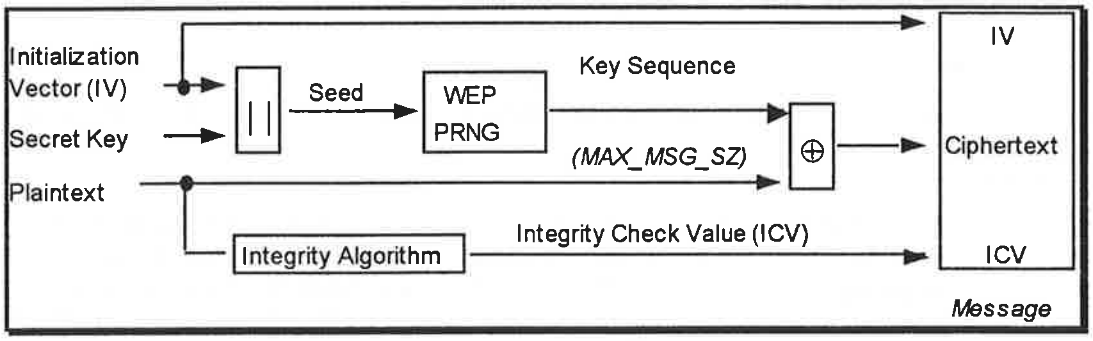


Figure 5-2: WEP Encipherment Block Diagram

Referring to Figure 5-2 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 MP~~S~~DU. Two processes are applied to the plaintext MP~~S~~DU. 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 strength of the WEP algorithm increases as the IV change frequency increases. -The IV may be changed as frequently as every MP~~S~~DU and, since it travels with the message, the receiver will always be able to decipher any message. The IV shall~~may~~ be transmitted in the clear (since it does not provide an attacker with any information about the secret key).

The WEP algorithm is applied after any fragmentation of the MSDU, i.e. WEP is applied to an MPDU payload. ~~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, encrypted MP~~S~~DU, 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. The~~This~~ IV field shall contain two sub-fields: :A 3-octet field that contains the initialization vector itself, followed by -a~~A~~ 1-octet alignment field that shall be all zero.~~contains the confidentiality algorithm ID, followed by a 3-octet field that contains the initialization vector~~ The WEP IV is 24~~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 field is followed by the encrypterd MP~~S~~DU body, which is followed by the ICV. The WEP ICV is 32 bits and shall be transmitted in the clear. 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.

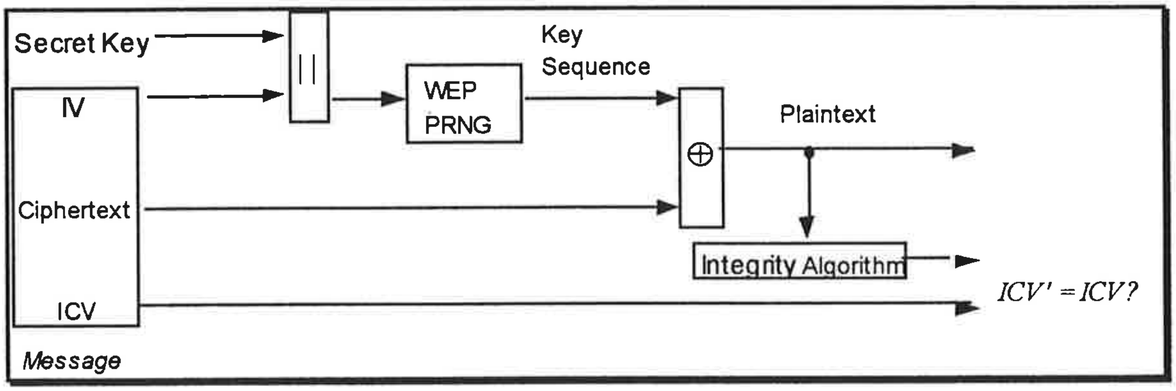


Figure 5-3: WEP Decipherment Block Diagram

Referring to Figure 5-3 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 computed~~output~~ ICV' to the ICV transmitted with the message. If ICV' is not equal to ICV, the received MSDU (of which the unsuccesfully decrypted MPDU is a part) is not passed to LLC and-an~~and~~ error indication is sent to MAC management.

0.2.4. WEP Algorithm Specification

WEP uses the RC4 PRNG algorithm from RSA Data Security, Inc..

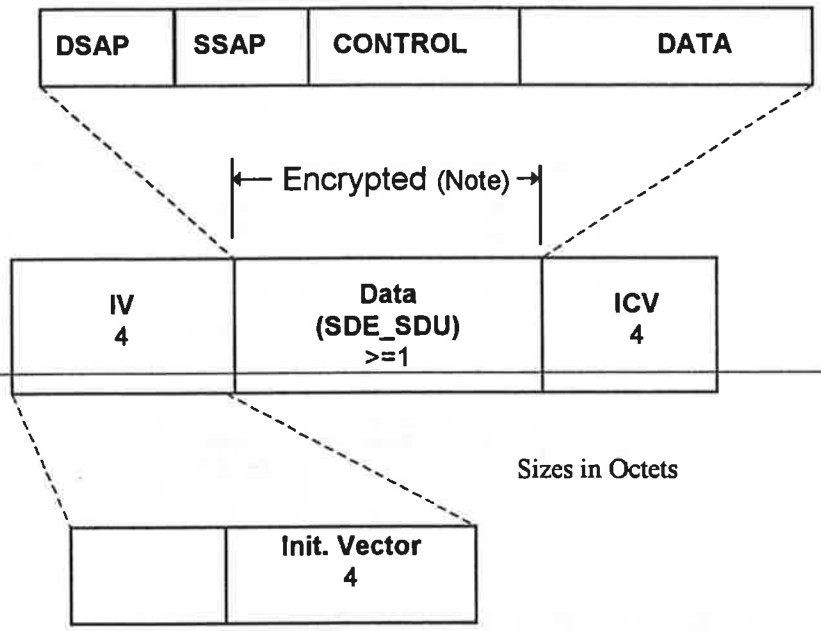
Details of the RC4 algorithm are ~~specified in <insert document reference here>~~ available from RSA. Please contact RSA for algorithm details and the uniform RC4 licensee~~liscense~~ terms which RSA offers to anyone wishing to use RC4 for the purpose of implementing the 802.11 WEP option.

0.2.5. WEP MP~~S~~DU Expansion~~Expanison~~:

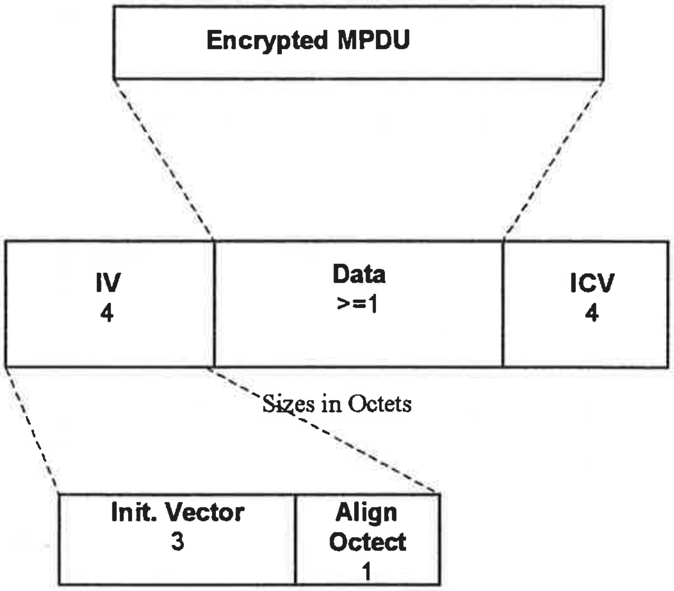
Figure 5-4 shows the encrypted MP~~S~~DU as constructed by the WEP.

The WEP ICV = 32 bits. The expanded MP~~S~~DU shall include the~~a~~ ~~32 bit~~ IV field immediately preceding the encrypted MP~~S~~DU. ~~This field shall contain one sub-field: A 4-octet field that contains the initialization vector.~~

The WEP mechanism is invisible to entities outside the 802.11 MAC.



Note: The encipherment process has expanded the original MSDU by 8 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 encipherment process has expanded the original MPDU Payload.
The ICV is calculated on the Data field only.

Figure 5-4: Construction of expanded WEP MSDU

0.3. 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 8~~7~~.X.

0.3.1. 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.

0.3.2. Privacy related MIB variables.

The default value for all shared, secret WEP keys shall be Null. This indicates an invalid WEP key. An

All MIB variables which store WEP keys shall be write-only variables. The use of write-only MIB variables prevents entities from learning secret WEP keys via MAC management facilities.

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 default~~deafault~~ key to be used with WEP.

An additional variable called "WEP_Default" is a Boolean~~boolean~~. If set True then on transmit, Data frames shall be encrypted~~encypted~~ using Default_WEP_Key and on receive they shall be decrypted using Default_WEP_Key. The MIB shall not allow WEP_Default~~WEP_DEfault~~ to be set to TRUE if Default_WEP_Key~~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 supports~~suppprts~~ the ability to have a separate WEP key for each station with~~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 implementation~~implmementation~~ dependent~~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) = True~~Ture~~ then use WEP_KEY_Mapping(RA,
            WEP_Key) for encryption,
        if WEP_Default = True~~Ture~~ then Use WEP_Default for encryption,
        otherwise do no encrypt~~encypt~~ the frame.

Receive case:
```

if WEP_Key_Mapping(TA, WEP_On) = True~~Ture~~ then use WEP_KEY_Mapping(TA,
    WEP_Key) for decryption,
if WEP_Default = True~~Ture~~ then Use WEP_Default for decryption,
otherwise do no attempt to decrypt~~decypt~~ the frame.

Proposal for Frame Processing Simplification by applying WEP to MPDU payload rather than MSDU payload.

David Bagby
Advanced Micro Devices
7 July 1995

This paper is very short. It simply proposes that WEP be applied to the MPDU body instead of the MSDU body.

This has the advantage of allowing a simpler interaction between Fragmentation and WEP (by applying WEP after fragmentation rather than before). With this change, it will not be necessary to receive an entire MSDU before decrypting the contents, resulting in implementation simplification.

Essentially, this change would logically move WEP processing from the top of the MAC layer to the bottom. Since WEP is invisible outside of the MAC layer, this change has no noticeable impact external to the MAC.

The included printed pages from D1.2 are the actual text alterations that would be required to implement this change to D1.2 text.

Moved:
That WEP processing be changed from an MSDU basis to and MPDU basis by adopting the changes shown to D1.2, said changes to be reflected in the next draft standard revision.

(Section 6) 1. MAC Sub-layer Functional Description

In the following sections, the MAC functional description is presented. Section 6.1 introduces the architecture of the MAC sublayer, including the distributed coordination function, the point coordination function and their coexistence in an 802.11 LAN. Sections 6.2 and 6.3 expand on this introduction and provide a complete functional description of each. Section 6.4 describes the security mechanisms within the MAC layer. Section 6.5 and 6.6 cover fragmentation and reassembly. Multirate support is addressed in Section 6.7. Section 6.8 reiterates the functional descriptions in the form of state machines.

1.1. MAC Architecture

The MAC is composed of several functional blocks: the MAC-LLC Service Interface, the MAC State Machines, the MAC Management State Machines and the MAC Management Information Base (MIB). The MAC-LLC Service Interface comprises the MAC Data Service and the MAC Management Service. These blocks perform the functions required to provide contention and contention-free access control on a variety of physical layers. The functions are provided without reliance upon particular data rates or physical layer characteristics. The MAC provides both distributed and point coordination functions and is able to support both asynchronous and time bounded service clases. Figure 6-1 illustrates the MAC architecture.

The MAC-LLC Service Interface shall accept MAC service requests from higher layer entities and shall distribute those requests to either the MAC Data Service or the MAC Management Service as appropriate. The MAC Data and MAC Management Services shall interpret the service requests and shall cause the appropriate signals to be generated to initiate actions in the state machines. The MAC-LLC Service Interface shall also accept indications from the state machines and provide those indications to higher layer entities. The particular service requests and indications are described in Section 3.2.

The MAC State Machine shall provide the sequencing required to provide the distributed coordination function. The MAC State Machine shall provide the protocol sequencing necessary to provide asynchronous communication service. The MAC State Machine shall provide the sequencing required to provide the point coordination function and the associated time-bounded and contention-free communication services. The implementation of the PCF portions of the MAC State Machine (and the associated Time-bounded and contention-free services) are optional . The MAC State Machine shall not interfere with time-bounded nor contention-free communications even if the optional point coordination function is not implemented.

The MAC Management State Machine shall provide the protocol sequencing required to provide the following services:

a) Association and re-association
b) Access to the MAC MIB
c) Timing synchronization
d) Power management
e) Authentication

The MAC MIB shall provide storage of and access to all of the information required to properly manage the MAC.

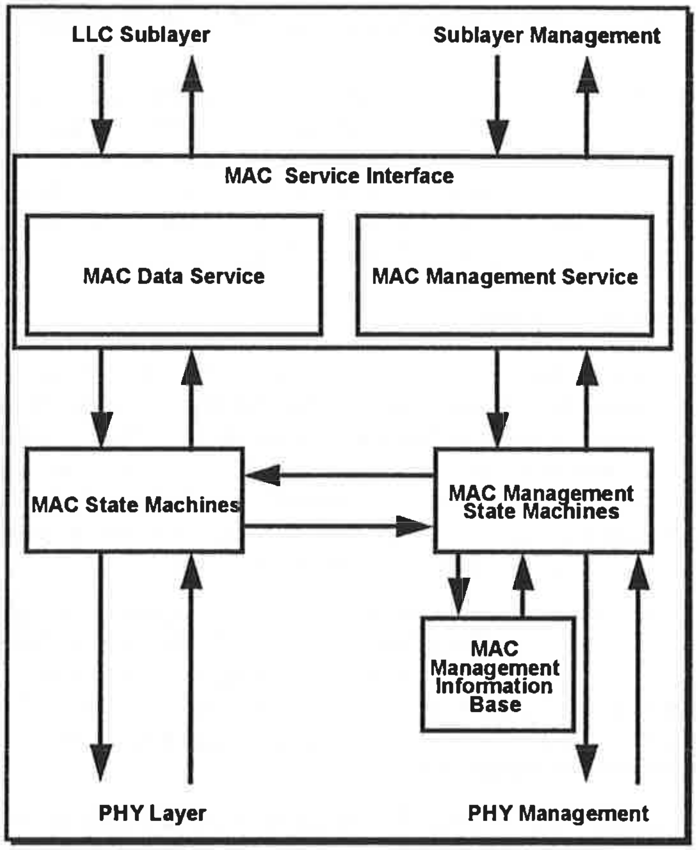


Figure 6-1: MAC Architecture Block Diagram

Viewed along a different axis, the MAC architecture can be described as shown in Figure 6-2 below as providing the point coordination function through the services of the distributed coordination function.

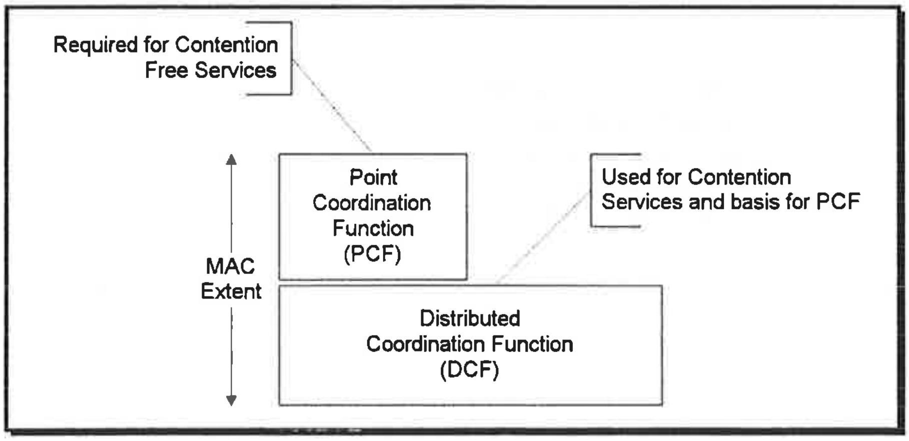

Required for Contention Free Services
Point Coordination Function (PCF)
Used for Contention Services and basis for PCF
MAC Extent
Distributed Coordination Function (DCF)

Figure 6-2: Alternative view of MAC architecture.

1.1.1. Distributed Coordination Function

The fundamental access method of the 802.11 MAC is a distributed coordination function known as carrier sense multiple access with collision avoidance, or CSMA/CA. The distributed coordination function shall be implemented in all stations. It is used within both ad hoc and infrastructure configurations.

A station wishing to transmit shall sense the medium to determine if another station is transmitting. If the medium is not busy, the transmission may proceed. The CSMA/CA distributed algorithm mandates that a gap of a minimum specified duration exist between contiguous frames. A transmitting station shall ensure that the medium is idle for the required duration before attempting to transmit. If the medium is sensed busy the station shall defer until the end of the current transmission. After deferral, the station shall select a random backoff interval and shall decrement the interval counter while the medium is free. A refinement of the method may be used under various circumstances to further minimize collisions - here the transmitting and receiving station exchange short control frames (**RTS** and **CTS** frames) prior to the data transmission. The details of CSMA/CA are described in Section 6.2. RTS/CTS exchanges are also presented in Section 6.2.

1.1.2. Point Coordination Function

The 802.11 MAC may also incorporate an optional access method described as a point coordination function. This optional access method shall be implemented on top of the distributed coordination function. This access method uses a point coordinator to determine which station currently has the right to transmit. The operation is essentially that of polling with the point coordinator playing the role of the polling master. The operation of the Point Coordination Function may require additional coordination, not sepcified in this standard, to permit effiecent operation in cases where multiple Point-Coordinated BSSs are operating on the same channel in overlapping physical space.

The point-coordination function shall be built up from the distributed coordination function through the use of an access priority mechanism. Different classes of traffic can be defined through the use of different values for IFS, thereby creating prioritized access to the medium for those classes with a shorter IFS. The point coordination function shall use an IFS that is smaller than the IFSfor data frames transmitted via the distributed coordination function. The use of a smaller IFS implies that point-coordinated traffic shall have priority access to the medium.

The access priority provided by point-coordinated traffic may be utilized to create a **contention-free** access method. The priority access of the PIFS allows the point coordinator to "seize control" of the medium, at a time whenthe medium is free, by starting its transmission before the other stationsare allowed to begin their transmissions under the DCF access method. The point coordinator can then control the frame transmissions of the stations so as to eliminate contentionfor a limited period of time.

1.1.3. Coexistence of DCF and PCF

The distributed coordination function and the point coordination function shall coexist in a manner that permits both to operate concurrently in the same BSS. When a point coordinator is operating in a BSS, the two access methods alternate, with a contention-free period followed by a contention period. This is described in greater detail in Section 6.3.

1.1.4. Fragmentation/Reassembly Overview

The process of partitioning a MAC Service Data Unit (MSDU) into smaller MAC level frames, MAC Protocol Data Units (MPDUs), is defined as fragmentation. Fragmentation creates MPDUs smaller than the MSDU size to increase reliablity of successful transmission of the MSDU over a given PHY. Fragmentation is accomplished at each immediate transmitter. The process of recombining MPDUs into a single MSDU is defined as reassembly. Reassembly is accomplished at each immediate recipient.

When a frame is received from the LLC with a MSDU size greater than aFragment_Threshold, the frame must be fragmented. The MSDU is divided into MPDUs. Each MPDU is a fragment with a frame body no larger than aFragment_Threshold. It is possible than any fragment may contain a frame body smaller than aFragment_Payload. An illustration of fragmentation is shown in Figure 6-3.

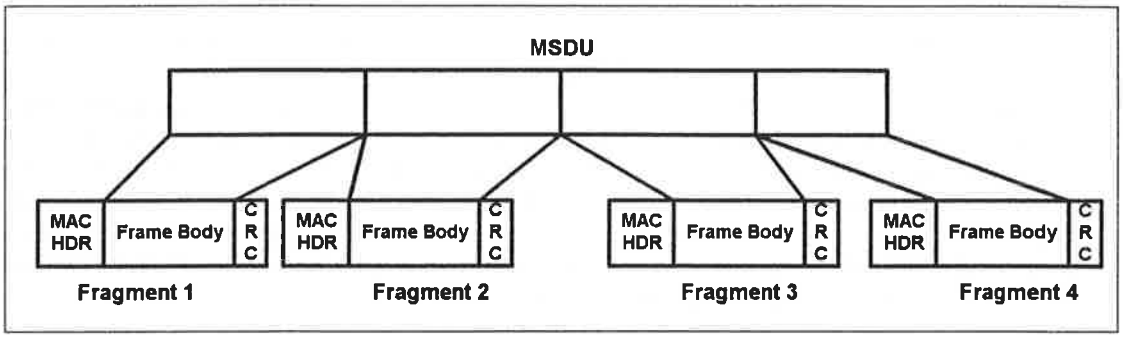


Figure 6-3: Fragmentation

1.1.5. MAC Data Service

The MAC Data Service shall translate MAC service requests from LLC into input signals utilized by the MAC State Machines. It shall also translate output signals from the MAC State Machines into service indications to LLC. The translations are given below.

The MA_DATA.request from LLC shall initiate one of the transmit cycles in the MAC State Machine. The psuedo-code below shall be used to translate this request into inputs to the MAC State Machine.

```
Tx_data_req = { requested_service_class = async & length(MSDU) > RTS_threshold
                & destination_address <> (broadcast | multicast) }
Tx_multicast_req = { requested_service_class = async & destination_address = multicast }
Tx_unitdata_req = { requested_service_class = async & length(MSDU) < RTS_threshold}
DA = { destination_address }
Length = { Rate_factor * ( length(MSDU) + Overhead ) }
Connection ID = integer. Note a value of zero is reserved for all asynchronous data requests
```

The MAC Data Service shall translate outputs from the MAC State Machine to MA_DATA.indication as shown in the following pseudo-code.

```
control = { type,control }
destination_address = { DA }
source_address = { SA }
MSDU = { info_field }
reception_status = { !(CRC_error | Format_error) }
Connection ID = integer. Note a value of zero is used when there is no connection.
```

1.2. Distributed Coordination Function

The basic medium access protocol is a Distributed Coordination Function (DCF) that allows for automatic medium sharing between compatible PHYs through the use of CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) and a random backoff time following a busy medium condition. In addition, all directed traffic uses immediate positive acknowledgements (ACK frame) where retransmission is scheduled by the sender if no ACK is received.

The CSMA/CA protocol is designed to reduce the collision probability between multiple stations accessing a medium, at the point where they would most likely occur. Just after the medium becomes free following a busy medium (as indicated by the CS function) is when the highest probability of a collision occurs. This is because multiple stations could have been waiting for the medium to become available again. This is the situation where a random backoff arrangement is needed to resolve medium contention conflicts.

Carrier Sense shall be performed both through physical and virtual mechanisms.

The virtual Carrier Sense mechanism is achieved by distributing medium busy reservation information through an exchange of special RTS and CTS (medium reservation) frames prior to the actual data frame. For stations & all AP's that do not initiate an RTS/CTS sequence, the duration information is also available in all data frames. The RTS and CTS frames contain a duration field that defines the period of time that the medium is to be reserved to transmit the actual data frame and the returning ACK. This information is distributed to all stations within detection range of both the transmitter and the receiver, so also to stations that are possibly "hidden" from the transmitter but not from the receiver. This scheme can only be used for directed frames. When multiple destiniations are addressed by broadcast/multicast frames, then this mechanism is not used.

It can also be viewed as a Collision Detection mechanism. Because the actual data frame is only transmitted when a proper CTS frame is received in response to the RTS frame, this results in a fast detection of a collision if it occurs on the RTS.

However the addition of these frames will result in extra overhead, which impacts short data frames. Also since all stations will likely be able to hear traffic from the AP but may not hear the traffic from all stations within a BSA.

However in situations where multiple BSS's utilizing the same channel do overlap, then the medium reservation mechanism will work accross the BSS boundaries, when RTS/CTS is also used for all traffic.

The use of the RTS/CTS mechanism is under control of RTS_Threshold attribute. However in situations where multiple BSS's utilizing the same channel do overlap, then the medium reservation mechanism will work accross the BSS boundaries, when RTS/CTS is also used for all traffic.

This parameter is a manageable object and can be set on a per station basis. This mechanism allows stations to be configured to use RTS/CTS either always, never or only on frames longer then a specified payload length.

Although a station can be configured not to initiate RTS/CTS to transmit its frames, every station shall respond to the duration information in the RTS/CTS frames to update its virtual Carrier Sense mechanism, and respond with a proper CTS frame in response to an addressed RTS frame.

The basic medium access protocol allows for stations supporting different set of rates to coexist, this is achieved by the fact that all stations are required to be able to receive any frame transmitted on a given Basic Rate Set, and must be able to transmit at (at least) one of these rates. All Multicast, Broadcast and Control frames (RTS, CTS and ACK) are always transmitted at one of this mandatory rates. This set of restrictions will assure that the Virtual Carrier Sense Mechanism described above will still work on multiple rate environments.

1.2.1. Physical Carrier Sense Mechanism

A physical carrier sense mechanism shall be provided by the PHY. See Section 8, Physical Service Specification for how this information is conveyed to the MAC. The details of carrier sense are provided in the individual PHY specification sections.

1.2.2. Virtual Carrier Sense Mechanism

A virtual carrier sense mechanism shall be provided by the MAC. This mechanism is referred to as the Net Allocation Vector(NAV). The NAV maintains a prediction of future traffic on the media based on duration information that is announced in RTS/CTS frames prior to the actual exchange of data. The duration information is also available in all data and Ack frames. The mechanism for setting the NAV is described in 6.2.6.4

1.2.3. MAC-Level Acknowledgments

To allow detection of a lost or errored frame an ACK frame shall be returned to the source STA by the destination STA immediately following a successfully received frame. Success shall be determined by an identical CRC generated from the received frame and the FC field of the same frame. The gap between the received frame and the ACK frame shall be the SIFS. This technique is known as positive acknowledgement.

The following frame types shall be acknowledged with an ACK frame:

a) Data
b) Poll
c) Request
d) Response

The lack of an ACK frame from a destination STA on any of the listed frame types shall indicate to the source STA that an error has occurred. Note however, that the destination STA may have received the frame correctly and the error has occurred in the ACK frame. This condition shall be indistinguishable from an error occurring in the initial frame.

1.2.4. Inter-Frame Space (IFS)

The time interval between frames is called the inter-frame space. A STA shall determine that the medium is free through the use of the carrier sense function for the interval specified. Three different IFS's are defined so as to provide a corresponding number of priority levels for access to the wireless media. The following three different IFSs are defined:

a) SIFS	Short Interframe Space
b) PIFS	PCF Interframe Space
c) DIFS	DCF Interframe Space

It should be noticed that the different IFSs are independent of the station bitrate, and are fixed per each PHY (even in multi-rate capable PHYs),

The IFS timings are defined as time gaps on the medium. The standard shall specify the relation of the relative PHY MIB parameters to achieve the specified timegaps as further specified in section 6.2.13.

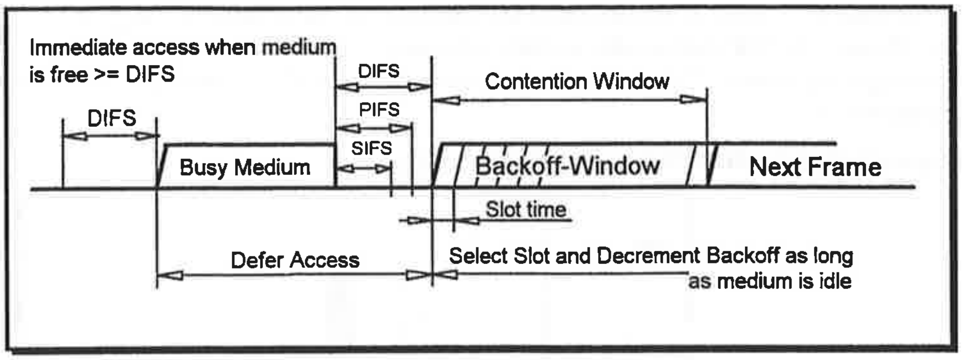

Immediate access when medium is free >= DIFS
DIFS
DIFS
PIFS
SIFS
Busy Medium
Contention Window
Backoff-Window
Next Frame
Slot time
Defer Access
Select Slot and Decrement Backoff as long as medium is idle

Figure 6-4: IFS Relations

1.2.4.1. Short-IFS (SIFS)

This inter-frame space shall be used for an ACK frame, a CTS frame, a Data frame of a fragmented MSDU, and, by a STA responding to any polling as is used by the Point Coordination Function (PCF) (See Section 6.3, Point Coordination Function). The SIFS is the time from the end of the last symbol of the previous frame to the begining of the first symbol of the pre-amble of the listed frame as seen at the air interface. The valid cases where the SIFS interval is used are listed in Frame Exchange Sequences found in section 4.3.

The SIFS timing will be achieved when the transmission of the subsequent frame is started at the TX_SIFS Slot boundary as specified in section 6.2.13.

1.2.4.2. PCF-IFS (PIFS)

This PCF priority level shall be used only by the PCF to send any of the Contention Free Period (CFP) frames. The PCF shall be allowed to transmit after it detects the medium free at the Tx-PIFS slot boundary as defined in section 6.2.13. This can occur at the start of and during a CF-Burst .

1.2.4.3. DCF-IFS (DIFS)

The DCF priority level shall be used by the DCF to transmit asynchronous MPDUs. A STA using the DCF shall be allowed to transmit if it detects the medium to be free at the Tx_DIFS slot boundary as defined in section 6.2.13, and its backoff time has expired.

1.2.5. Random Backoff Time

STA desiring to initiate transfer of asynchronous MPDUs shall utilize the carrier sense function to determine the state of the media. If the media is busy, the STA shall defer until after a DIFS gap is detected, and then generate a random backoff period for an additional deferral time before transmitting. This process resolves contention between multiple STA that have been deferring to the same MPDU occupying the medium.

Backoff Time = INT(CW * Random()) * Slot time

where:

CW = An integer between CW_{min} and CW_{max}
Random() = Pseudo random number between 0 and 1
Slot Time = Transmitter turn-on delay + medium propagation delay + medium busy detect response time (including MAC delay) and is PHY dependent.

The Contention Window (CW) parameter shall contain an initial value of CW_{min} for every MPDU queued for transmission. The CW shall double at every retry until it reaches Cwmax. The CW will remain at CWmax for the remaining of the retries. This is done to improve the stability of the access protocol under high load conditions. See Figure 6-5.

Suggested values are for: CWmin=31, Cwmax = 255.

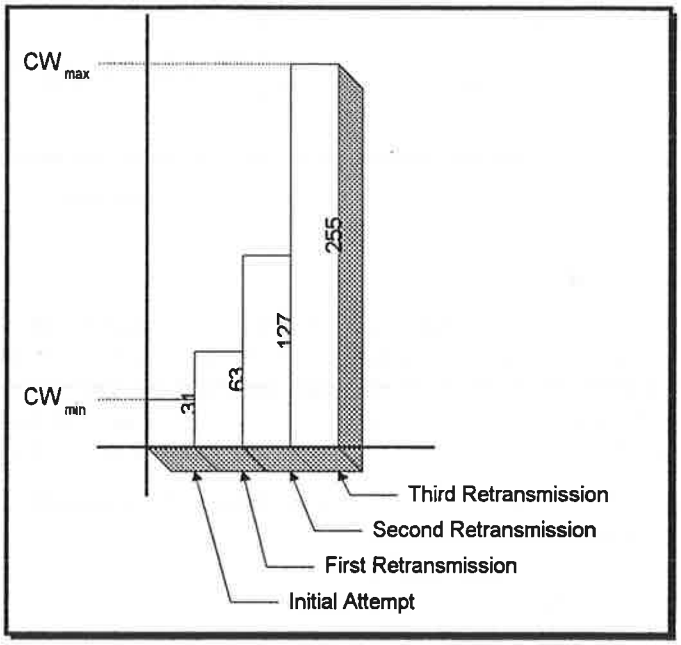


Figure 6-5: Exponential Increase of CW

CWmin and CWmax are MAC constants that should be fixed for all MAC implementations, because they effect the access fairness between stations.

1.2.6. DCF Access Procedure

The CSMA/CA access method is the foundation of the Distributed Coordination Function. The operational rules vary sligthly between Distributed Coordination Function and Point Coordination function.

1.2.6.1. Basic Access

Basic access refers to the core mechanism a STA uses to determine whether it has permission to transmit.

Both the Physical and Virtual Carrier Sense functions are used to determine the busy state of the medium. When either of them indicate a busy medium, the medium shall be considered busy. The opposite of a busy medium shall be known as a free medium.

A STA with a pending MPDU may transmit when it detects a free medium for greater than or equal to a DIFS time. This rule applies both when using the DCF access method exclusively and when using the PCF access method in the Contention Area.

If the medium is busy when a STA desires to initiate an RTS, Data, Poll, and Management MPDU transfer, and only a DCF is being used to control access, the Random Backoff Time algorithm shall be followed.

Likewise, if the medium is busy when a STA desires to initiate an RTS, Data, Poll, and Management MPDU transfer, and a Contention Period portion of a Superframe is active (See 6.3 PCF), the Random Backoff Time algorithm shall be followed.

The basic access mechanism is illustrated in the following diagram.

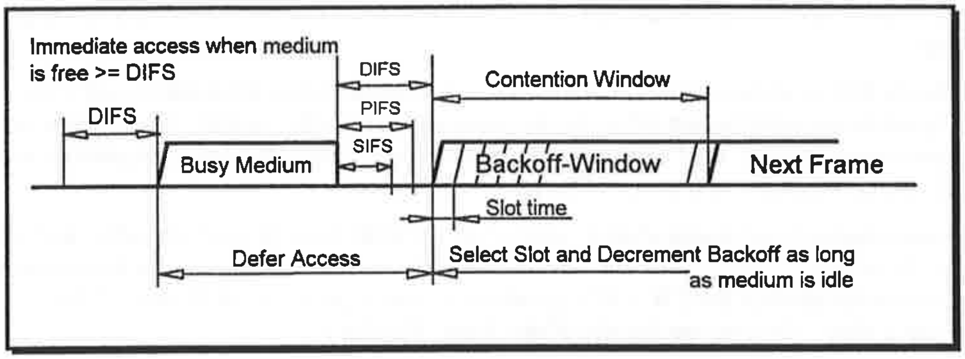

Immediate access when medium is free >= DIFS
DIFS
DIFS
PIFS
SIFS
Contention Window
Busy Medium
Backoff-Window
Next Frame
Slot time
Defer Access
Select Slot and Decrement Backoff as long as medium is idle

Figure 6-6: Basic Access Method

1.2.6.2. Backoff Procedure

The backoff procedure shall be followed whenever a STA desires to transfer an MPDU and finds the medium busy.

The backoff procedure consists of selecting a backoff time from the equation in Section 6.2.5 Random Backoff Time. The Backoff Timer shall decrement by slottime amount after every slottime, while the medium is free. The Backoff Timer shall be frozen while the medium is sensed busy. Decrementing the Backoff Timer shall resume whenever the medium is detected to be free at the Tx_DIFS slot boundary as defined in section 6.2.13. Transmission shall commence whenever the Backoff Timer reaches zero.

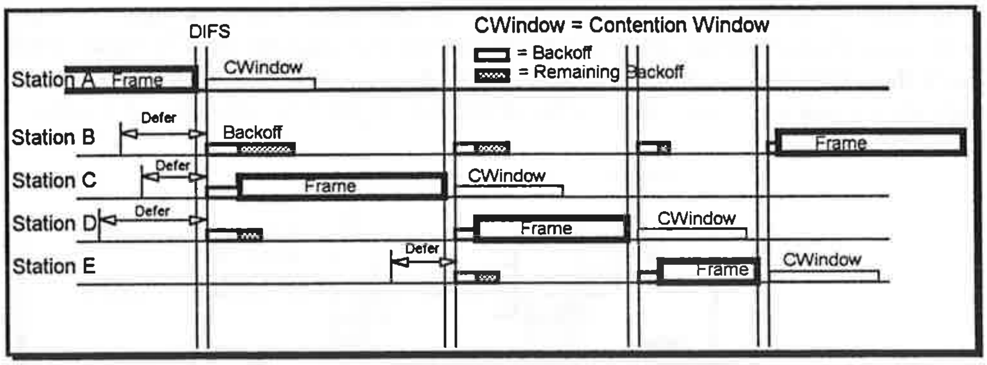


Figure 6-7: Backoff Procedure

A station that has just transmitted an MSDU and has another MSDU ready to transmit (queued), shall perform the backoff procedure. This requirement is intended to produce a level of fairness of access amongst STA to the medium.

The effect of this procedure is that when multiple stations are deferring and go into random backoff, then the station selecting the lowest delay through the random function will win the contention. The advantage of this approach is that stations that lost contention will defer again until after the next, and will then likely have a shorter backoff delay than new stations entering the backoff procedure for the first time. This method tends toward fair access on a first come, first served basis.

1.2.6.3. RTS/CTS Recovery Procedure and Retransmit Limits

Many circumstances may cause an error to occur in a RTS/CTS exchange.

For instance, CTS may not be returned after the RTS transmission. This can happen due to a collision with another RTS or a DATA frame, or due to interference during the RTS or CTS frame. It can however also be that CTS fails to be returned because the remote station has an active carrier sense condition, indicating a busy medium time period.

If after an RTS is transmitted, the CTS fails in any manner within a predetermined CTS_Timeout (T1), then a new RTS shall be generated while following the basic access rules for backoff. Since this pending transmission is a retransmission attempt, the CW shall be doubled as per the backoff rules. This process shall continue until the aRTS_Retry_Counter reaches an aRTS_Retry_Max limit.

The same backoff mechanism shall be used when no ACK frame is received within a predetermined ACK_Window (T3) after a directed DATA frame has been transmitted. Since this pending transmission is a retransmission attempt the CW will be greater than one as per the backoff rules. This process shall continue until the aData_Retry_Counter reaches the aData_Retry_Max limit .

1.2.6.4. Setting the NAV Through Use of RTS/CTS Frames

In the absence of a PCF, reception of RTS and CTS, Data and ACK frames are the events that shall set the NAV to a non-zero duration. Various conditions may reset the NAV.

RTS and CTS frames contain a Duration field based on the medium occupancy time of the MPDU from the end of the RTS or CTS frame until the end of the ACK frame. (See Section 4: RTS and CTS Frame Structure.) All STA receiving these frame types with a valid FCS field but with the exception of the station that is addressed shall interpret the duration field in these frames, and maintain the Net Allocation Vector (NAV). Stations receiving a valid frame should update their NAV with the information received in the Duration field, but only when the new NAV value is greater then the current NAV value.

Maintenance of the NAV shall consist of an internal state accurate to 1 microsecond of the busy/free condition of the medium. Figure 6-8 indicates the NAV for stations that can hear the RTS frame, while other stations may only receive the CTS frame, resulting in the lower NAV bar as shown. Although the NAV effectively will "count-down" from a non-zero value, only the fact of whether the NAV is non-zero or not is necessary for correct protocol operation.

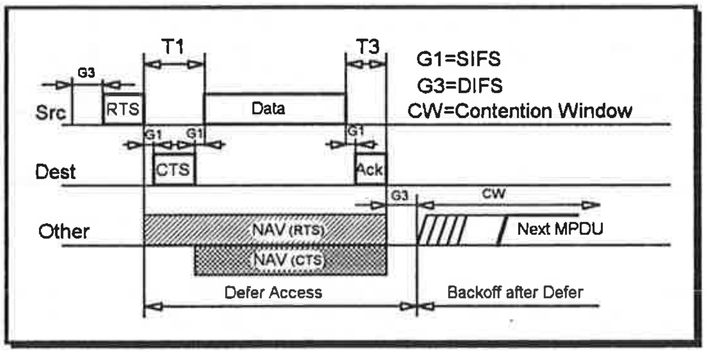


Figure 6-8: RTS/CTS/DATA/ACK MPDU

1.2.6.5. Control of the Channel

The Short Interframe Space (IFS) is used to provide an efficient MSDU delivery mechanism. Once a station has contended for the channel, it will maintain control of the channel until it has sent all the fragments of a MSDU, and received their corresponding Acks, or until it failed to receive an Ack for a specific fragment. After all fragments have been transmitted, the station will relinquish control of the channel.

Once the station has contended for the channel, it will continue to send fragments until either all fragments of a MSDU have been sent, an acknowledgment is not received, or the station can not send any additional fragments due to a dwell time boundary.

Figure 6-9 illustrates the transmission of a multiple fragment MSDU using the IFS.

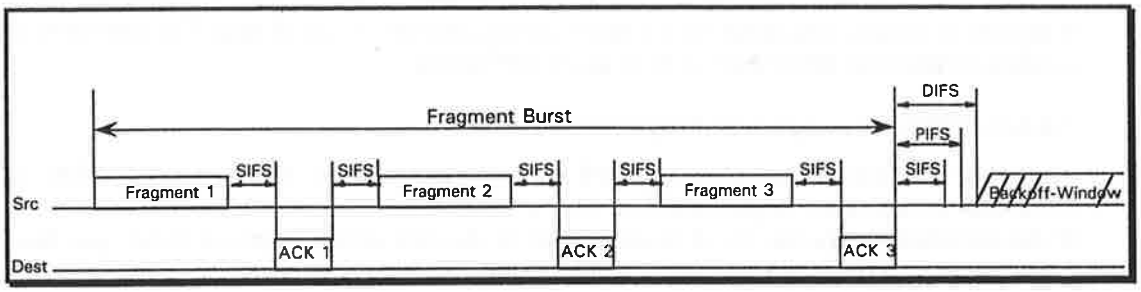


Figure 6-9: Transmission of a Multiple Fragment MSDU using IFS

The source station transmits a fragment then releases the channel and waits for an acknowledgment. When the source station releases the channel following its fragment, it will immediately monitor the channel for an acknowledgment frame from the destination station.

When the destination station has finished sending the acknowledgment, the SIFS following the acknowledgment is then reserved for the source station to continue (if necessary) with another fragment. The station sending the acknowledgment does not have permission to transmit on the channel immediately following the acknowledgment.

The process of sending multiple fragments after contending for the channel is defined as a fragment burst.

If the source station receives an acknowledgment but there is not enough time to transmit the next fragment and receive an acknowledgment due to an impending dwell boundary, it will contend for the channel at the beginning of the next dwell time.

If the source station does not receive an acknowledgment frame, it will attempt to retransmitaccording to the backoff algorithm. When the time arrives to retransmit the fragment, the source station will contend for access in the contention window.

After a station contends for the channel to retransmit a fragment of a MSDU, it will start with the last fragment that was not acknowledged. The destination station will receive the fragments in order since the source sends them one at a time, in order. It is possible however, that the destination station may receive duplicate fragments. This will occur if the destination station sends an acknowledgment and the source does not receive it. The source will resend the same fragment after executing the backoff algorithm and contending for the channel.

A station will transmit after the SIFS only under the following conditions during a fragment burst:

> The station has just received a fragment that requires acknowledging.
>
> The source station has received an acknowledgment to a previous fragment, has more fragment(s) for the same MSDU to transmit, and there is enough time left in the dwell time to send the next fragment & receive an acknowledgment.

The following rules also apply.

> When a station has transmitted a frame other than a fragment, it shall not transmit on the channel following the acknowledgment for that frame, without going through a backoff.

When a MSDU has been succesfully delivered, and want to transmit a subsequent MSDU, then it should go through a backoff.

Only unacknowledged fragments are retransmitted.

If a multiple fragment MSDU does not require an acknowledgment (for example, a broadcast/multicast packet transmitted by the Access Point), the source station will transmit all fragments of the MSDU without releasing the channel as long as there is enough time left in the dwell time. If there is not, the station will transmit as many fragments as possible and recontend for the channel during the next dwell time. The spacing between fragments of a broadcast/multicast frame shall be equal to the SIFS period.

1.2.6.6. RTS/CTS Usage with Fragmentation

The following is a description of using RTS/CTS for the first fragment of a fragmented MSDU. RTS/CTS will also be used for retransmitted fragments if their size warrents it. The RTS/CTS frames define the duration of the first frame and acknowledgment. The duration field in the data and acknowledgment frames specifies the total duration of the next fragment and acknowledgment. This is illustrated in Figure 6-10.

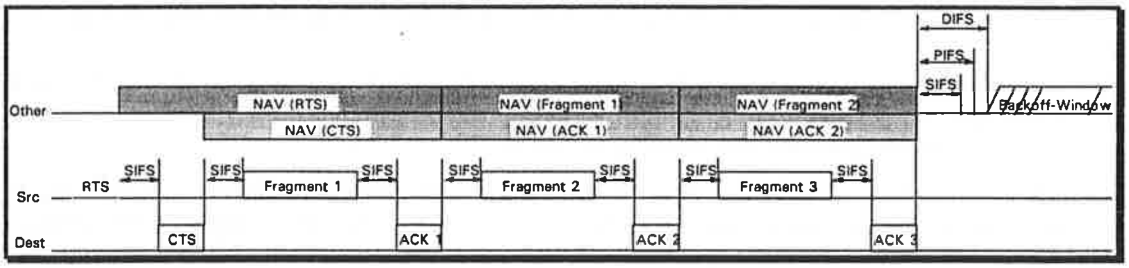


Figure 6-10: RTS/CTS with Fragmented MSDU

Each frame contains information that defines the duration of the next transmission. The RTS will update the NAV to indicate busy until the end of ACK 1. The CTS will also update the NAV to indicate busy until the end of ACK 1. Both Fragment 1 and ACK 1 will update the NAV to indicate busy until the end of ACK 2. This is done by using the duration field in the DATA and ACK frames. This will continue until the last Fragment and ACK which will have the duration set to zero. Each Fragment and ACK acts as a virtual RTS and CTS, therefore no RTS/CTS frame needs to be generated even though subsequent fragments are larger the aRTS_Threshold.

In the case where an acknowledgment is not received by the source station, the NAV will be marked busy for next frame exchange. This is the worst case situation. This is shown in Figure 6-11. If the acknowledgment is not sent by the destination station, stations that can only hear the destination station will not update their NAV and be free to access the channel. All stations that hear the source will be free to access the channel after the NAV from Frame 1 has expired.

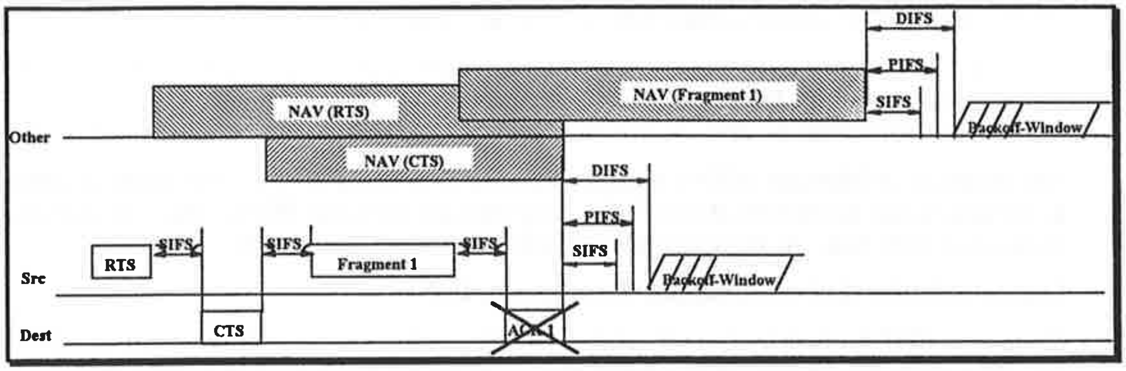


Figure 6-11: RTS / CTS with Transmitter Priority with Missed Acknowledgment

The source station must wait until the ACK timeout before attempting to contend for the channel after not receiving the acknowledgment.

1.2.7. Directed MPDU Transfer Procedure Using RTS/CTS

Figure 6-11 shows the Directed MPDU transfer procedure with the use of RTS/CTS. In certain circumstances the DATA frames will be preceded with an RTS and CTS frame exchange that include duration information.

STA shall use an RTS/CTS exchange for directed frames only when the length of the MPDU is greater than the length threshold indicated by the RTS_Threshold attribute. The RTS_Threshold attribute shall be set to a MPDU length threshold in each STA.

The RTS_Threshold attribute shall be a managed object within the MAC MIB, and its value can be set and retrieved by the MAC LME. The RTS_Threshold attribute shall be constrained to range (0 ... Maximum MPDU Length). The value 0 shall be used to indicate that no MPDU shall be delivered without the use of RTS/CTS. Values of RTS_Threshold ≥ MDPU_Maximum shall indicate that all MPDU shall be delivered with RTS/CTS.

The asynchronous payload frame (e.g. DATA) shall be transmitted after the end of the CTS frame and an SIFS gap period. No regard shall be give to the busy or free status of the medium.

1.2.7.1. Directed MPDU Transfer Procedure without RTS/CTS

Following the basic access mechanism, the source STA shall transmit the asynchronous payload frame (e.g. DATA). The destination STA shall follow the ACK Procedure.

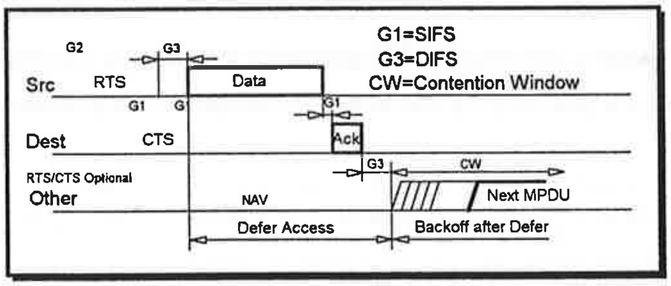


Figure 6-12: Directed Data/ACK MPDU

1.2.8. Broadcast and Multicast MPDU Transfer Procedure

In the absense of a PCF, when Broadcast or Multicast MPDUs are transferred from an AP to a STA, or from one STA to other STA's, only the basic access mechanism shall be used. Regardless of the length of the frame, no RTS/CTS exchange shall be used. In addition, no ACK shall be transmitted by any of the receipients of the frame.

Any Broadcast or Multicast MPDUs transferred from a STA with a To_DS bit set shall, in addition to conforming to the basic access mechanism of CSMA/CA, obey the rules for RTS/CTS exchange. In addition, the AP shall transmit an ACK frame in response just as if the MPDU were directed traffic.

Multicast MSDUs shall be propagated throughout the ESS.

There is no MAC level recovery on Broadcast or Multicast frames except for those frames sent with the To_DS bit set. As a result the reliability of this traffic is reduced due to the increased probability of lost frames from interference or collisions.

1.2.9. ACK Procedure

Upon successful reception of a data or management frame with the ToAP bit set, an AP shall always generate an ACK frame. An ACK frame shall be transmitted by the destination STA which is not an AP whenever it successfully receives a unicast data frame or management frame, but not if it receives a broadcast or multicast data frame. The transmission of the ACK frame shall commence after an SIFS period without regard to the busy/free state of the medium.

The Source STA shall wait an Ack_timeout amount of time without receiving an Ack frame before concluding that the MPDU failed.

This policy induces some probability that a pending frame in a neighboring BSA (using the same channel) could be corrupted by the generated ACK. However if no ACK is returned because a busy medium was detected, then it is guaranteed that the frame would be interpreted as in error due to the ACK timeout, resulting in a retransmission.

1.2.10. Duplicate Detection and Recovery

Since MAC-level acknowledgments and retransmissions are incorporated into the protocol, there is the possibility that a frame may be received more than once. Such duplicate frames shall be filtered out within the destination MAC.

Duplicate frame filtering is facilitated through the inclusion of a dialog token (consisting of a sequence number and fragment number) field within DATA and MANAGEMENT frames. MPDUs which are part of the same MSDU shall have the same sequence number, and different MSDUs will (with a very high probability) have a different sequence number.

The sequence number is generated by the transmitting station as an incrementing sequence of numbers.

The receiving station shall keep a cache of recently-received <source-address, sequence-number, fragment-number> tuples.

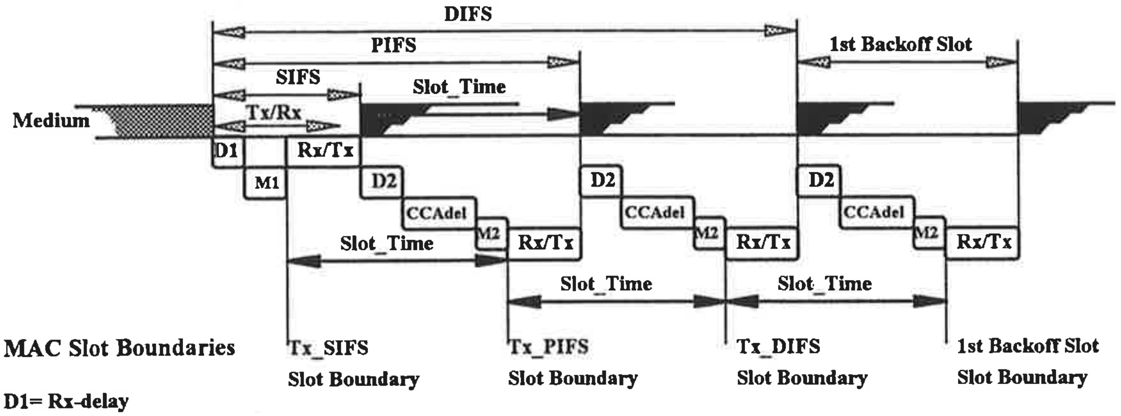
A destination STA shall reject a frame which has the RETRY bit set in the CONTROL field as a duplicate if it receives one which matches both source-address, sequence-number and fragment-number in the cache .

There is the small possibility that a frame will be improperly rejected due to such a match; however, this occurrence would be rare and would simply result in a lost frame similar to an FCS error in ethernet.

The Destination STA shall perform the ACK procedure even if the frame is subsequently rejected due to duplicate filtering.

1.2.11. DCF Timing Relations

This section formulates the relation between the IFS specifications as have been defined as time gaps on the medium, and the associated MIB variables that are provided per PHY.



D1= Rx-delay
D2= Medium + Rx-delay
Rx/Tx=Full Tx delay including rampup
M1 / M2= MAC decision delay
CCAdel= CCA evaluation time
Assumption:
SIFS= minimum (components listed OR Tx/Rx_Turnaround time)

Figure 6-13

All timings are referenced to the end of the last symbol of a frame on the medium.

The SIFS, and Slot_Time are defined in the MIB, and are fixed per PHY.

SIFS is based on: Rx_Delay + MAC_Delay-1 + Rx/Tx_Delay.

Slot_Time is based on: Rx/Tx_Delay + Medium_Delay + Rx_Delay + CCA_Delay + MAC_Delay-2

The PIFS and DIFS are derived by the following equations, as illustrated in figure 6-13.

PIFS = SIFS + Slot_Time

DIFS = SIFS + 2 * Slot_Time

The Medium_Delay component is fixed at 1 usec.

Figure 6-13 illustrates the relation between the SIFS, PIFS and DIFS as they are measured on the medium and the different MAC Slot Boundaries Tx_SIFS, Tx_PIFS and Tx_DIFS. These Slot Boundaries define when the transmitter can be turned on by the MAC to meet the different IFS timings on the medium, after subsequent detection of the CCA result of the previous Slot_Time.

The following equations define the MAC Slot Boundaries, using parameters defined in the MIB, which are such that they compensate for implementation timing variations. The reference of these slot boundaries is again the end of the last symbol of the previous frame on the medium.

Tx_SIFS = SIFS - a Rx/Tx_Turnaround_Time (MIB variable)

Tx_PIFS = Tx_SIFS + Slot_Time

Tx_DIFS = Tx_SIFS + 2 * Slot_Time.

The tolerances are specified in the MIB, and will only apply to the SIFS specification, so that tolerances will not accumulate.

1.3. Point Coordination Function

The Point Coordination Function (PCF) provides Contention Free frame transfer. It is an option for a STA to be able to become the Point Coordinator(PC). All STA inherently obey the medium access rules of the PCF, because these rules are based on the DCF, with the Point Coordinator gaining priority access to the medium using a PCF IFS (PIFS) which is smaller than the DCF IFS (DIFS) usedby the DCF to access the medium. The operating characteristics of the PCF are such that all stations are able to operate properly in the presence of a BSS in which a Point Coordinator is operating, and, if associated with a point-coordinated BSS, are able to receive data frames sent under PCF control.. It is also an option for a station to be able to respond to a contention-free poll (CF-poll) received from a Point Coordinator. A station which is able to respond to CF-polls is referred to as being CF-Aware, and may request to be polled by an active Point Coordinator. When polled by the Point Coordinator, a CF-Aware station may transmit one frame to any destination (not just to the Point Coordinator), and may ÒpiggypackÓ the acknowledgement of a frame received from the Point Coordinator using particular data frame subtypes for this transmission. If the addressed recipient of a CF transmission is not CF-Aware, that station acknowledges the transmission using the DCF acknowledgement rules, and the Point Coordinator retains control of the medium by waiting the PIFS duration before resuming CF transfers.

When more than one point-coordinated BSS is operating on the same PHY channel in overlapping space, the potential exists for collisions between PCF transfer activities by the independent point coordinators. The rules under which multiple, overlapping point-coordinated BSSs can coexist are presented in section 6.3.3.3.As shown in Figure 6-2, the PCF is built on top of the CSMA/CA based DCF, by utilizing the access priority provisions provided by this scheme.An active Point Coordinator must be located at an AP, which restricts PCF operation to infrastructure networks. However, there is no requirement that a distribution system be attached to this AP, which permits a station capable of AP and PC functionality to be designated as the ÒAPÓ in an isolated BSS. PCF is activated at a PC---capable AP by setting the aCFP_Max_Duration managed object to a non--zero value.

1.3.1. Contention Free Period Structureand Timing

The PCF controls frame transfers during a Contention Free Period (CFP) . The CFP alternates with a Contention Period (CP), when the DCF controls frame transfers,as shown in Figure 6-14. Each CFP begins with a Beacon frame that contains a DTIM Element (hereafter referred to as a ÒDTIMÓ). The CFPs occur at a defined repetition rate, which is synchronized with the beacon interval as specified below.

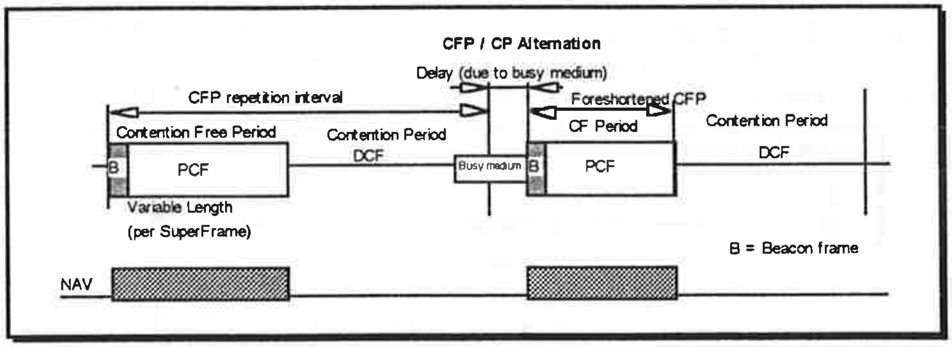


Figure 6-14: CFP / CP Alternation

The PC generates CFPs at the **Contention-Free Repetition Rate** (CFP-Rate), which shall be an integral number of DTIM intervals. The PC determines the CFP-Rate (depicted as a repetition interval in the illustrations below) to use from the aCFP_Rate managed object. This value, in units of beacon intervals, is communicated to other stations in the BSS in a field of the PCF Element of Beacon frames. The PCF Element is only present in Beacon frames transmitted by stations containing an active Point Coordinator.

The length of the CFP is controlled by the PC, with maximum duration specified by the value of the aCFP_Max_Duration managed object at the PC. Neither the maximum duration nor the actual duration (signalled by transmission of a CF-End or CF-End+Ack frame by the PC) are constrained to be a multiple of the beacon interval. If the CFP-Rate is greater than the beacon interval, the PC shall transmit beacons at the appropriate times during the CFP (subject to delay due to traffic at the nominal times, as with all beacons). The PCF Element in all beacons at the start of, or within, a CFP contain a non-zero value in the CFP_Dur_Remaining field. This value, in units of milliseconds, specifies the maximum time from the transmission of this beacon to the end of this CFP. The value of the CFP_Dur_Remaining field is zero in beacons sent during the contention period. An example of these relationships is illustrated in figure 6-15, which shows a case where the CFP-Rate is 2 DTIM intervals, the DTIM interval is 3 beacon intervals, and the CFP_Max_Duration is approximately 2.5 beacon intervals.

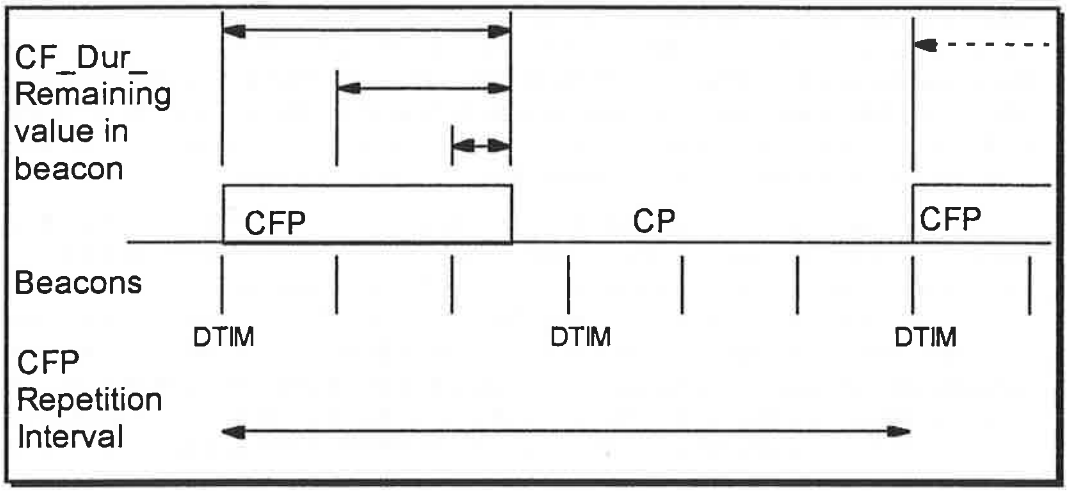


Figure 6-15: Beacons & Contention Free Periods

The PC may terminate any CFP at or before the CFP_Max_Duration, based on available traffic and size of the polling list. Because the transmission of any beacon may be delayed due to a medium busy condition at the nominal beacon transmission time, a CFP may be foreshortened by the amount of the delay. In the case of a busy medium due to DCF traffic, the upper bound on this delay is the maximum RTS + CTS + max_MPDU + Ack duration. In cases where the beacon transmission is delayed, the CFP_Dur_Remaining value in the beacon at the beginning of the CFP shall specify a time that causes the CFP to end no later than the nominal beacon transmission time plus the value of aCFP_Max_Duration. This is illustrated in figure 6-16.

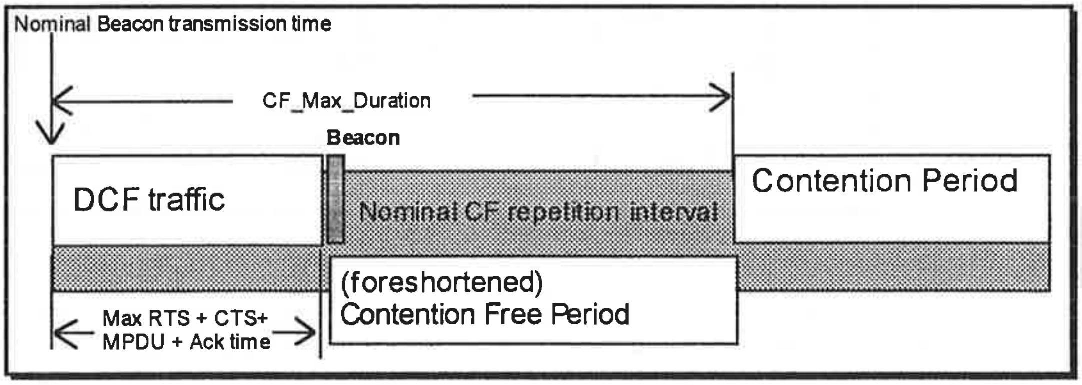


Figure 6-16: Example of Delayed Beacon and Foreshortened CFP

1.3.2. PCF Access Procedure

The contention free transfer protocol is based on a polling scheme controlled by a Point Coordinator operating at the AP of the BSS. The PC gains control of the medium at the beginning of the CFP and attempts to maintain control for the entire CFP by waiting a shorter time between transmissions than the stations using the DCF access procedure. Acknowledgement of frames sent during the Contention Free Period may be accomplished using Data+CF-Ack, CF-Ack, Data+CF-Poll+CF-Ack (only on frames transmitted by the PC), or CF-Ack+CF-Poll (only on frames transmitted by the PC) frames in cases where a data (or null) frame immediately follows the frame being acknowledged, thereby avoiding the overhead of separate Ack frames.

1.3.2.1. Fundamental Access

At the nominal beginning of each CFP, the PC shall sense the medium. When the medium is free (both CCA and NAV) for one PIFS interval, the PC shall transmit a beacon frame containing a PCF Element with CFP-Rate and CFP_Dur_Remaining fields set as specified above. A DTIM element is also required in this beacon frame.

After the initial beacon frame, the PC waits for the medium to be free (CCA only, not NAV) for one SIFS interval then transmits either a Data frame, a CF-Poll frame, a Data+CF-Poll frame, or a CF–End frame. If a null CFP is desired, a CF–End frame shall be transmitted immediately after the initial beacon.

Stations receiving error-free frames from the PC are expected to respond after an SIFS interval, in accordance with the transfer procedures defined in Section 6.3.3. If the recipient station is not CF-Aware, the response to receipt of an error-free Data frame is always an Ack frame.

1.3.2.2. NAV Operation During the Contention Free Period

Each station, except the station with the PC, shall preset it's NAV to the CF_Dur_Remaining value in the PCF Element of the beacon frame at the beginning of every CFP. This prevents stations from taking control of the medium during the CFP, which is especially important in cases where the CFP spans multiple medium-occupancy intervals, such as dwell periods of an FH PHY. This setting of the NAV also minimizes eliminates the risk of hidden stations sensing a DIFS gap during the CFP and possibly corrupting a transmission in progress.

The PC shall transmit a CF–End or CF-End+Ack frame at the end of each CF-Period. Receipt of either of these frames shall reset the NAV of all stations in the BSS.

1.3.3. PCF Transfer Procedure

Frame transfer under the PCF typically consists of alternating between frames sent from the AP/PC and frames sent to the AP/PC. During the CFP, the ordering of these transmissions, and the station allowed to transmit frames to the PC at any given point in time, is controlled by the PC. Figure 6-17 depicts a frame transfer during a typical CFP. The rules under which this frame transfer takes place are detailed in the following paragraphs.

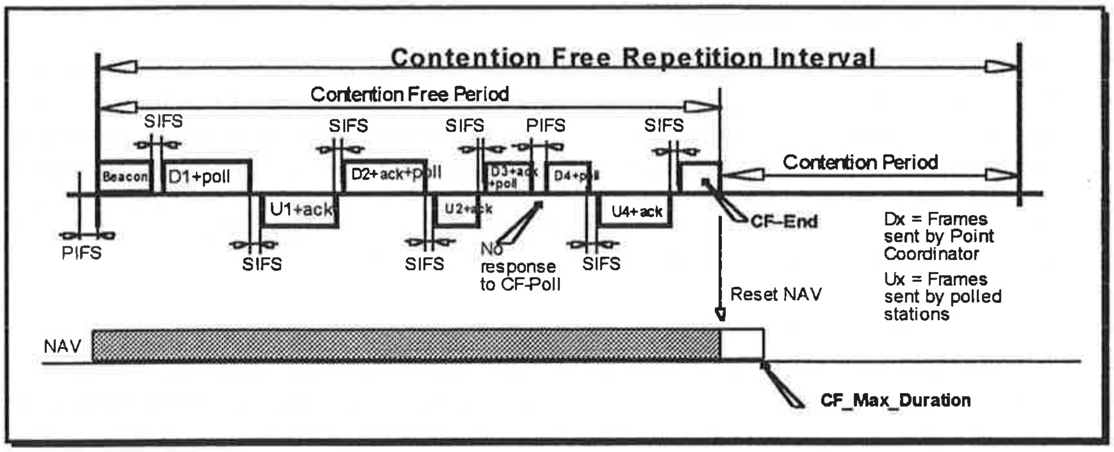


Figure 6-17: Example of PCF Frame Tranfser

1.3.3.1. PCF Transfers When the PCF Station is Transmitter or Recipient

The PC shall transmit frames between the beacon which starts of the CFP and the CF–End using the SIFS gap (CCA only, not NAV) except in cases where a transmission by another station is expected by the PC and an SIFS gap elapses without the receipt of the expected transmission. In such cases the PC shall send its next pending transmission a PIFS gap after the end of its last transmission. This permits the PC to retain control of the medium in cases where an expected response or acknowledgement does not occur. The PC may transmit any of the following frame types to CF-Aware stations:

Data, used when the addressed recipient is not being polled and there is nothing to acknowledge;

Data+CF-Ack, used when the addressed recipient is not being polled and the PC needs to acknowledge the receipt of a frame received from a CF-Aware station an SIFS interval before starting this transmission;

Data+CF-Poll, used when the addressed recipient is the next station to be permitted to transmit during this CFP and there is nothing to acknowledge;

Data+CF-Ack+CF-Poll, used when the addressed recipient is the next station to be permitted to transmit during this CFP and the PC needs to acknowledge the receipt of a frame received from a CF-Aware station an SIFS interval before starting this transmission;

CF-Poll (no data), used when the addressed recipient has no pending frames buffered at the AP, but is the next station to be permitted to transmit during this CFP and there is nothing to acknowledge;

CF-Ack+CF-Poll (no data), used when the addressed recipient has no pending frames buffered at the AP but is the next station to be permitted to transmit during this CFP and the PC needs to acknowledge the receipt of a frame from a CF-Aware station an SIFS interval before starting this transmission;

CF-Ack (no data), used when the addressed recipient has no pending frames buffered at the AP or insufficient time remains in the CFP to send the next pending frame, but the PC needs to acknowledge receipt of a frame from a CF-Aware station an SIFS interval before starting this transmission (useful when the next transmission by the PC is a management frame, such as a beacon); or

any management frame that is appropriate for the AP to send under the rules for that frame type.

The PC may transmit Data or management frames to non-CF-Aware, non-Power Save stations during the CFP. These stations acknowledge receipt with Ack frames after and SIFS gap, as with the DCF. The PC may also transmit broadcast or multicast frames during the CFP. Because the Beacon frame that initiates the CFP contains a

DTIM Element, if there are associated stations using Power Save Mode, the broadcasts and multicasts buffered for such stations shall be sent immediately after the initial Beacon.

A CF-Poll bit in the Subtype field of these frames will allow the stations to send their (CF-Up) data if any. Stations shall respond to the CF-Poll immediately when a frame is queued, by sending this frame after an SIFS gap. This results in a burst of Contention Free traffic; the CF-Burst.

A CF-Aware station that receives a directed frame with any of data subtypes that include CF-Poll may transmit one data frame when the medium is free (CCA only) an SIFS gap after receiving the CF-Poll. CF-Aware stations ignore, but do not reset, their NAV when performing transmissions in response to a CF-Poll.

For frames that require MAC level acknowledgment, CF-Aware stations that received a CF-Poll (of any type) may perform this acknowledgment using the Data+CF-Ack subtype in the response to the CF-Poll. For example, the U1 frame in Figure 6-18 contains the acknowledgement to the preceding D1 frame. Also the D2 frame contains the acknowledgement to the preceding U1 frame. The PC may use the CF-Ack subtypes to acknowledge a received frame even if the Data frame sent with the CF-Ack subtype is addressed to a different station than the one being acknowledged. CF-Aware stations that are expecting an acknowledgement shall interpret the subtype of the frame (if any) sent by the PC an SIFS gap after that stationÕs transmission to the PC. If a frame that requires MAC level acknowledgement is received by a non-CF-Aware station, that station does not interpret the CF-Poll indication (if any), and acknowledges the frame by sending an Ack frame after an SIFS gap.

If a frame, transmitted during the CFP, requires MAC level acknowledgement and is not acknowledged, that frame is *not* retransmitted during the same CFP. The frame may be retried once, during a subsequent CFP, at the discretion of the PC or CF-Aware station.

The sizes of the frames may be variable, only bounded by the frame and/or fragment size limitations that apply for the BSS. If a CF-Aware station does not respond to a CF-Poll (of any type) within the SIFS gap following a transmission from the PC, or a non-CF-Aware station does not return the Ack frame within an SIFS gap following a transmission from the PC that requires acknowledgment, then the PC shall resume control and transmit its next frame after a PIFS gap from the end of the PCF's last transmission. or a non-CF-Aware station does not return the Ack frame within an SIFS gap following a transmission from the PC that requires acknowledgment,

A CF-Aware station must respond to a CF-Poll. If the station has no frame to send when polled, the response shall be a Null frame. If the station has no frame to send when polled, but an acknowledgment is required for the frame that conveyed the CF-Poll, the response shall be either a CF-Ack (no data) or an Ack frame. The null response is required to permit a 'no-traffic' situation to be distinguished from a collision between overlapping PCFs.

The the CFP ends when the CF_Max_Duration time has elapsed since the last Beacon or when the PC has no further frames to transmit nor stations to poll. In either case, the end of the CFP is signalled by the transmission of a CF-End by the PC. If there is a received frame which requires acknowledgement at the time the CF-End is to be transmitted, the PC transmits a CF-End+Ack frame instead. All stations of the BSS receiving a CF-End or CF-End+Ack reset their NAVs so they may attempt to transmit during the contention period.

1.3.3.2. PCF Transfers When the PCF Station is Neither Transmitter nor Recipient

A CF-Aware station, when transmitting in response to a CF-Poll (any type), may send a Data frame to any station in the BSS an SIFS gap after receiving the CF-Poll. If the addressed recipient of this transmission is not the AP, the Data frame is received and acknowledged according to the DCF rules for Data frames. This is illustrated in Figure 6-18. The PC resumes transmitting an SIFS gap after the Ack frame, if the PC hears the Ack, or a PIFS gap after the expected time for the Ack frame if the PC does not hear the Ack.

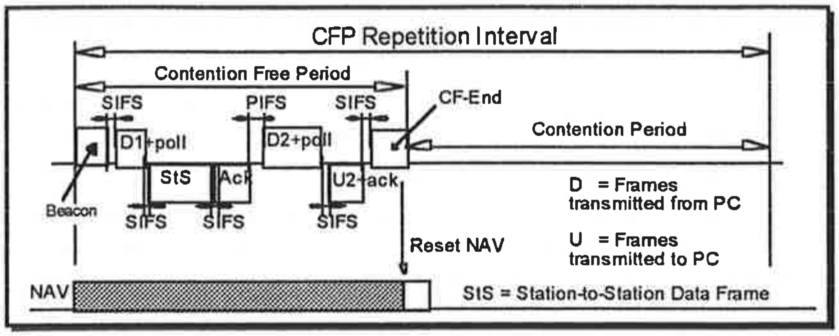


Figure 6-18: Station-to-Station Contention Free Transfer

1.3.3.3. Operation with Overlapping Point-Coordinated BSSs

Because the PCF operates without the CSMA/CA contention window randomization and backoff of the DCF, there is a risk of repeated collisions if multiple, overlapping BSSs are operating with PCF on the same PHY channel, and their CFP-Rates and beacon intervals are approximately equal. To minimize the risk of significant frame loss due to undetected collisions during contention free operation, transmissions of data an management frames during the CFP are only initiated when the medium is free (CCA only, NAV ignored) for the SIFS interval. This is in contrast to Ack frames, which are transmitted (under DCF or PCF) after the SIFS interval without regard to the state of the medium. In addition, whenever the PC has a Data and/or CF-Poll transmission go unacknowledged, the PC shall sense medium free (CCA only) for the PIFS interval, rather than the SIFS interval prior to its next transmission.

To further reduce the susceptibility to inter-PCF collisions, the PC shall require the medium be free for a random (over range of 1 to CW_min) number of slot times once every aMedium_Occupancy_Limit milliseconds during the CFP. This can only result in loss of control of the medium to overlapping BSS or hidden station traffic, because the stations in this BSS are prevented from transmitting by their NAVs. For operation of the PCF in conjunction with an FH PHY, aMedium_Occupancy_Limit shall be set equal to the dwell time. For operation in conjunction with other PHY types, when using a short CFP_Max_Duration that does not require this extra protection against inter-PCF collisions, aMedium_Occupancy_Limit can be set equal to aCFP_Max_Duration. (The Medium_Occupancy_Limit is also useful for compliance in regulatory domains that impose limits on continuous transmission time as part of a spectrum etiquette.)

1.3.3.4. CFP_Max_Duration Limit

The value of aCFP_Max_Duration shall be limited to allow coexistence between Contention and Contention Free traffic.

> The minimum value for aCFP_Max_Duration, if the PCF is going to be used, is two times aMax_MPDU plus the time required to send the initial Beacon frame and the CF-End frame of the CFP. This allows sufficient time for the AP to send one Data frame to a station, while polling that station, and for the polled station to respond with one Data frame.
>
> The maximum value for aCFP_Max_Duration is the duration of aCFP_Rate minus aMax_MPDU plus the time required for the RTS/CTS and Ack frames associated with this MSDU when operating with default size contention window. This allows sufficient time to send at least one contention-based Data frame.

1.3.3.5. Contention Free Usage Rules

A PC may send broadcast or multicast frames, and directed Data or management frames to any active station, as well as to CF-Aware Power Save stations. During the CFP, CF-aware stations shall acknowledge receipt of each

Data+CF-Poll frame , Data+CF-Ack+CF-Poll frame, CF-Poll (no data) frame, or CF-Ack+CF-Poll frame using Data+CF-Ack or CF-Ack (no data) frames, sent after an SIFS–interval (CCA only, NAV ignored); and shall acknowledge the receipt of all other Data and management frames using ACK Control frames sent after an SIFS–interval (CCA and NAV ignored, as with all ACK frames). Non-CF-aware stations shall acknowledge receipt of (all) Data and management frames using ACK Control frames sent after an SIFS–interval (CCA and NAV ignored, as will all ACK frames). This non-CF-Aware operation is the same as these stations already do for DCF operation.

When polled by the PCF (Data+CF-Poll, Data+CF-Ack+CF-Poll, CF-Poll, or CF-Ack+CF-Poll) a CF-aware station may send one Data or managment frame to any destination. Such a frame directed to or through the PC station shall be acknowledged by the PC, using the CF-Ack indication (Data+CF-Ack, Data+CF-Ack+CF-Poll, CF-Ack, CF-Ack+CF-Poll, or CF-End+Ack) sent after an SIFS–interval. Such a frame directed to non–PCF stations shall be acknowledged using an ACK Control frame sent after an SIFS–interval. (This is the same as these stations already do.) A polled CF-aware station with neither a Data frame nor acknowledgement to send shall respond by transmitting a Null frame after an SIFS-interval.

The PC shall not issue CF-Polls if insufficient time remains in the current CFP to permit the polled station to transmit a Data frame containing a maximum–length MPDU.

1.3.4. Contention Free Service Types

The PCF provides a frame transfer mechanism, not a service class. This transfer mechanism may be used for delivery of asynchronous traffic (data and management frames) that would otherwise be sent in the contention period,and connection-oriented traffic, which may include Time-Bounded Services (TBS) as defined elsewhere in this standard.

1.3.5. Contention Free Polling List

The PC maintains a "polling list" for use in selecting stations that are eligible to recive CF-Polls during contention free periods. The polling list is used to force the polling of CF-Aware stations, whether or not the PC has no pending traffic to transmit to those stations. The polling list may be used to control the use of Data+CF-Poll and Data+CF-Ack+CF-Poll types for transmission of Data frames being sent to CF-Aware stations by the PC. The polling list is a *logical* construct, which is not exposed outside of the PCF. A minimum set of polling list maintenance techniques are required to ensure interoperability of arbitrary CF-Aware stations in BSSs controlled by arbitrary CF-Capable access points. APs may also implement additional polling list maintenance techniques which are outside the scope of this standard.

1.3.5.1. Polling List Processing

The PC shall send a CF-Poll to at least one station during each station begins when there are entries in the polling list. The PCF shall issue polls to stations whose entries on the polling list are for reasons other than time-bounded service connections in order by ascending SID value. If there is insufficient time to send CF-Polls to all such entries on the polling list during a particular CFP, the polling commences with the next such entry during the next CFP. The issuance of polls to stations whose entries on the polling list are for time-bounded service connections shall follow the rules applicable to the service class.

While time remains in the CFP, the PC may generate one or more CF-Polls to *any* stations on the polling list. While time remains in the CFP, the PC *may* send Data or Management frames to *any* stations.

In order to gain maximum efficiency from the contention free period, and the ability to piggyback acknowledgements on successor Data frames in the opposite direction, the PC should generally use Data+CF-Poll and Data+CF-Ack+CF-Poll types for each data frame transmitted while sufficient time for the potential response to the CF-Poll remains in the CFP. The PC may send multiple frames (with or without CF-Polls) to the same station during a single CFP, and may send multiple CF-Polls to a station in cases where time is available and the station indicates that More frames are available in the frame control field of a transmission in response to a CF-Poll.

1.3.5.2. ACFS Procedure

A station indicates its CF-Awareness during the Association process. If a station desires to change the PCF's record of CF-Awareness, that station must perform a Reassociation. During Association, a CF-Aware station may also request to be placed on the polling list for the duration of its association, or to never be placed on the polling list. The later is useful for CF-Aware stations that normally use Power Save Mode, permitting them to receive buffered traffic during the CFP (since they have to be awake to receive the DTIM that initiated the CFP), but not requiring them to stay awake to receive CF-Polls when they have no traffic to send.

Stations that establish connections are automatically placed on the polling list for the duration of each connection. Note that ony CF-Aware stations may establish connections, and that connection-based services are only available when a PC is operating in the BSS.

CF-Aware stations that are not on the polling list due to a static request during Association, and are not excluded from the polling list due to a static request during Association, may be dynamically placed on the polling list by the PC to handle bursts of frame transfer activity by that station. The PC monitors CF-aware station activity during both the Contention Free period and the contention period. When a CF-aware station placed on the polling list dynamically has not transmitted a Data frame in response to the number of successive CF-Polls indicated in aPoll_Inactivity, then the PCF may delete that station from the polling list. When a CF-aware station not on the polling list, but not excluded from the polling list, has transmitted any Data frames during the previous contention period, then the PC may add that station to the polling list. This is illustrated in Figure 6-19.

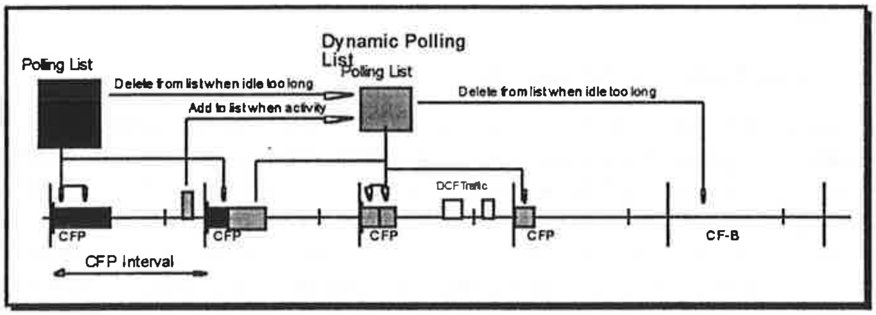

Dynamic Polling List
Polling List
Polling List
Delete from list when idle too long
Add to list when activity
Delete from list when idle too long
DCF Traffic
CFP
CFP
CFP
CFP
CF-B
CFP Interval

Figure 6-19: Dynamic Polling List Update Technique

1.3.6. Connection Management Frame Usage

Note: The incomplete definition of the connection service specification and the incomplete specification of the connection management frames prevents this section from being complete. These updates reflect letter ballot comments, and do not constitute an attempt to complete definition of the connection management frames nor their usage.

The contention free management frames are used in the following way.

1.3.6.1. STA Start Connection Request

Generated if the MAC user (of a station) makes a "Start Connection Request" when there is no outstanding request.

A station initiates a request for a connection to be established. The Payload must be included in this frame.

Receipt of this management frame will generate a "Start Connection Indication".

1.3.6.2. AP Start Connection Request

Generated if the MAC user (of an AP) makes a "Start Connection Request" when there is no outstanding request

An AP initiates a request for a connection to be established within the contention free period. The Payload and Connection ID must be included in this frame. The connection ID is the proposed connection ID that of the connection that will be established if this request is granted.

1.3.6.3. Grant Connection

After a Start Connection Request frame has been received the MAC shall reply with a "Grant Connection" frame which indicates the success or failure of the connection request.

If the requested connection is granted, the PC places an entry corresponding to that connection onto the polling list. If a station has multiple connections active, that station appears on the polling list multiple times. Only an access point may assign MAC connection numbers; so if a station is to grant a connection it must return the connection ID that was proposed by the access point. The MAC Connection ID must be included in this frame.

Transmitting or receiving this frame causes a Connection Granted Indication or a Connection Denied Indication..

1.3.6.4. End Connection

Either a station or an access point may initiate the end of a connection. When a node receives an End Connection frame it should stop using that connection, since the sending node will no longer maintain it. The MAC Connection ID must be included in this frame. When the connection is ended, the PC removes the entry corrresponding to that station from the polling list.

1.4. Fragmentation

The MAC may fragment and reassemble MSDUs, directed and multicast/broadcast. The primary reason for fragmenting an MSDU is that it is larger than the PHY is capable of sending in one MPDU. The fragmentation and reassembly mechanisms allows for fragments to be retransmitted.

All stations shall support the simultaneous reception of a minimum of 6 MSDUs.

The fragmentation design also allows for the characteristics of FH PHYs. For the purposes of this description a 'dwell time' will refer to the duration of time spent on a single frequency in a FH system. Therefore in a FH PHY the PHY will hop to the next frequency in the hop sequence at the end of the current dwell time.

The payload of a fragment shall be an even number of octets for all fragments except the last. The payload of a fragment shall never be larger than aFragment_Payload (including IV and ICV if WEP is invoked for the MPDU). However, it may be less than aFragment_Payload.

When data is to be transmitted, the number of octets in the payload of the fragment shall be determined based on the time at which the fragment is to be transmitted for the first time. Once a fragment is transmitted for the first time, its contents shall be fixed until it is successfully delivered to the immediate receiving station.

The number of data octets in the payload of a fragment shall depend on the values of the following three variables at the instant the fragment is assembled to be transmitted for the first time:

a) aFragment_Payload
b) The time remaining in the current dwell time.
c) The number of octets in the MSDU that have not yet been transmitted for the first time.

Since the control of the channel will be lost at a dwell time boundary and the station will have to contend for the channel after the dwell boundary, it is required that the acknowledgment of a fragment be transmitted before the stations cross the dwell time boundary. Hence, if there is not enough time remaining in the dwell time to transmit a fragment with an aFragment_Payload payload, the number of octets in the payload may be reduced to the maximum number of octets that will allow the fragment plus the MAC acknowledgment to fit within the time remaining in the dwell time. This is shown in Figure 6-21 for an MSDU of 1500 octets.

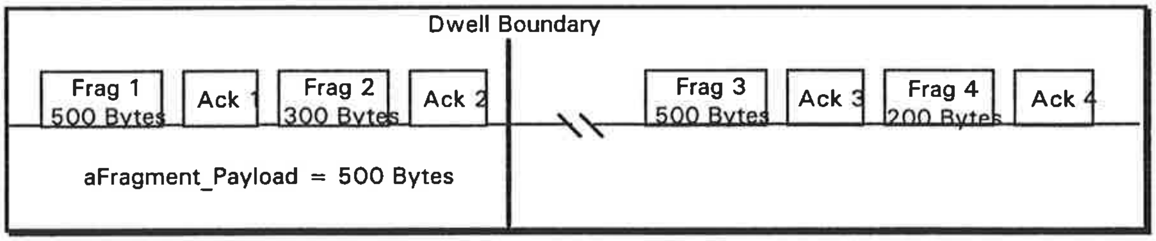


Figure 6-21: Fragmentation Near a Dwell Boundary

Referring to Figure 6-21, a 1500 octet MSDU is fragmented into four fragments with aFragment_Payload set at 500 octets. There is enough time left in the dwell to send two fragments, one of 500 octets and a second of 300 octets. After the dwell boundary, the rest of the MSDU is sent, one 500 octet fragment and one 200 octet fragment.

A station may elect not to adjust the size of the payload when approaching a dwell boundary. In this case, the station must wait until after the next dwell boundary to create and transmit a fragment with a aFragment_Payload octet payload (provided there are at least aFragment_Payload more octets remaining in the MSDU). A station must be capable of receiving fragments of varying size for a single MSDU.

If a fragment requires retransmission, its contents and length shall remain fixed for the lifetime of the MSDU at that station. In other words, after a fragment is transmitted once, contents or length of that fragment are not allowed to fluctuate to accommodate the dwell time boundaries. Let the fragmentation set refer to the contents and length of each of the fragments that make up the MSDU. The fragmentation set is created at a station as soon as the fragments are attempted for the first time. The fragmentation set remains fixed for the lifetime of the packet at the transmitting station. This is shown in Figure 6-22.

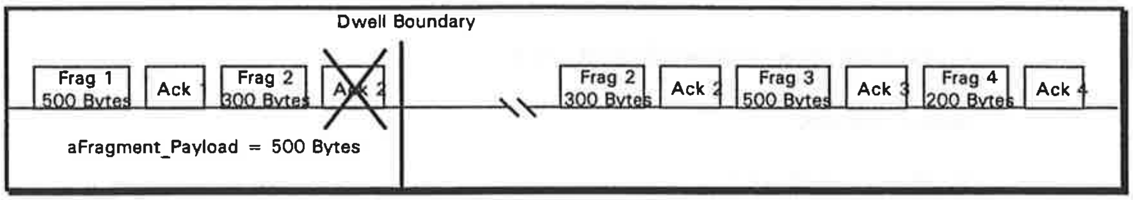


Figure 6-22: Fragmented MSDU with missed ACK Near a Dwell Boundary

In the example shown in Figure 6-22, the same 1500 octet MSDU is fragmented at the same point in the dwell time as in Figure 6-21 but the ACK for the second fragment is missed. After the dwell boundary, the fragment is retransmitted and the fragment size remains 300 octets.

Each fragment will contain a Sequence Control Field, which is comprised of a Sequence Number and Fragment Number. When a station is transmitting a MSDU, the Sequence Numberwill remain the same for all fragments of that MSDU. The fragments will be sent in order of lowest Fragment Numberto highest Fragment Number, where the fragment number increases by one for each fragment. The Frame Control Field also contains a bit, the Last Fragment bit, that indicates the last (or only) fragment of the MSDU.

If, when retransmitting a fragment, there is not enough time remaining in the dwell time to allow transmission of the fragment plus the acknowledgment, the station shall wait until after the next dwell boundary before retransmitting that fragment.

The source station will maintain a aTransmit_MSDU_Timer attribute for each MSDU being transmitted. There is also an attribute, aMax_Transmit_MSDU_Lifetime, that specifies the maximum amount of time allowed to transmit a MSDU. The aTransmit_MSDU_Timer starts on the attempt to transmit the first fragment of the MSDU. If aTransmit_MSDU_Timer exceeds aMax_Transmit_MSDU_Lifetime than all remaining fragments are discarded by the source station and no attempt is made to complete transmission of the MSDU.

1.5. Reassembly

Each data fragment contains information to allow the complete MSDU to be reassembled from its constituent fragments. The header of each fragment contains the following information that is used by the destination station to reassemble the MSDU:

Frame Type (data, acknowledgment, etc.).

Source Address

Destination Address

Sequence Control Field: This field allows the destination station to check that all incoming fragments belong to the same MSDU, and the sequence in which the fragments should be reassembled. The Sequence Number within the Sequence Control Field remains the same for all fragments of an MSDU, while the Fragment Number within the Sequence Control Field increments for each fragment.

Last Fragment Indicator: Indicates to the destination station that this is the last fragment of the MSDU. Only the last fragment of the MSDU will have this bit set to one. All other fragments of the MSDU will have this bit set to zero.

The destination station can reconstruct the MSDU by combining the fragments in order of Fragment Number portion of the Sequence Control Field. If the fragment with the last fragment bit set to one has not yet been received, then the destination station knows that the MSDU is not yet complete. As soon as the station receives the fragment with the last fragment bit set to one, the station knows that no more fragments will be received for the MSDU.

The destination station will maintain a aReceive_MSDU_Timer attribute for each MSDU being received. There is also an attribute, aMax_Receive_MSDU_Lifetime, that specifies the maximum amount of time allowed to receive a MSDU. The aReceive_MSDU_Timer starts on the reception of the first fragment of the MSDU. If aReceive_MSDU_Timer exceeds aMax_Receive_MSDU_Lifetime than all received fragments are discarded by the destination station.

To properly reassemble packets, a destination station must discard any duplicated fragments received. If a station receives a fragment with the same Source, Destination, and Sequence Control Field as a previous fragment, then the station must discard the duplicate fragment. However an acknowledge must be sent in response to a duplicate fragment of a directed MSDU.

1.6. Multirate Support

The following set of rules must be followed by all the stations to ensure coexistence and interoperability on MultiRate Capable PHYs.

All Control Frames (RTS, CTS and ACK) are transmitted on the STATION_BASIC_RATE (which as specified before belongs to the ESS_BASIC_RATE) so they will be understood by all the stations in the ESS.

All Multicast and Broadcast Frames are transmitted on the STATION_BASIC_RATE, regardless of their type.

Unicast Data and/or Management Frames are sent on any available transmit rate. The algorithm for selecting this rate is implementation dependent and is beyond the scope of this standard.

1.7. MAC State Machines

There are two distinct sets of state machines in the 802.11 MAC, the media access control state machines and the MAC management state machines. The media access control state machines implement the distributed, time-bounded and contention-free media access control protocols providing a frame-based communication channel. The MAC management state machines make use of this channel inoder to provide some if the required MAC management services.

1.7.1. General Notes to the State Machine Diagrams

The state machine diagrams on the following pages use the following conventions:

> 1. States are indicated by vertical bars that are labeled above the bar. The state labels are a descriptive title and a state number that includes a letter to indicate the identity of the state machine. For example, state C0 is in the control state machine, R0 is in the receive state machine and T0 is in the transmit state machine.
>
> 2. Transitions are indicated by horizontal bars that terminate in an arrowhead. A transition that is a loop that returns to the same state it leaves may include a short vertical bar as part of the transition. Any conditions that must be met in order to take a transition a listed above the transition. Actions that are taken only on particular transitions are listed below the transition. Transitions are labelled with a descriptive title and a letter indicating the state machine followed by two numbers that indicate the originating state and the terminating state. For example, C01 is the transition from state C0 to state C1 in the control state machine. If there is more than one transition between two states that would result in the same label for the transition, a letter is appended to each of the transition labels such that the new labels are unique. For example, R20a and R20b indicate two unique transitions from state R2 to state R0.
>
> 3. In addition to actions taken on transitions, actions may also be taken as part of a state. If this is the case, the actions to be taken in the state will be noted in the notes on a particular state machine that follow the state machine diagram.

1.7.2. Media Access Control State Machines

There are three state machines used to describe the asynchronous communication portion of the 802.11 MAC. The transmit state machine is a simple "data pump" that will forward data to the PHY after including the required MAC header and parameters and calculating the frame CRC. The receive state machine is a simple "data acceptor" that receives data from the PHY, checks this data for valid format and errors and indicates the type of frame received. The control state machine performs the major MAC protocol sequencing and error handling. In addition to the three state machines, there are resources supporting the operation of the state machines. These resources include the timer block and the NAV. The block diagram shows how these state machines communicate.

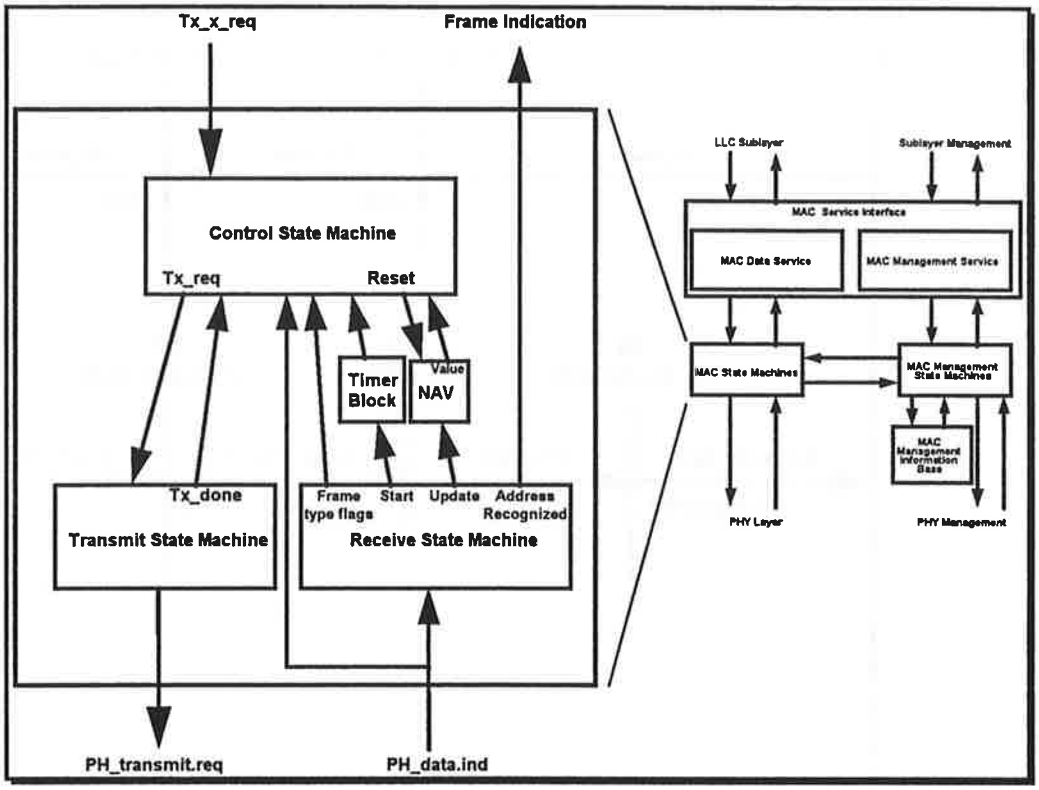


Figure 6-23: Media Access Control State Machines

1.7.2.1. Transmit State Machine

As can be seen in the transmit state machine diagram, this state machine is a simple, unconditional loop. The control state machine uses the service of the transmit state machine to form a valid frame and send it to the PHY. Upon leaving the idle state, the transmit state machine is guaranteed that the media is available and that there is a frame to be sent. The transmit state machine forms a complete, valid frame by prepending any PHY required preamble, a start delimiter, and a MAC header to the data (SDU) to be transmitted. It also appends a CRC and any PHY required end delimiter or postamble to complete the frame (MPDU). After sending the MPDU to the PHY via PH_data.indicate operations, the transmit state machine signals that it has completed its task.

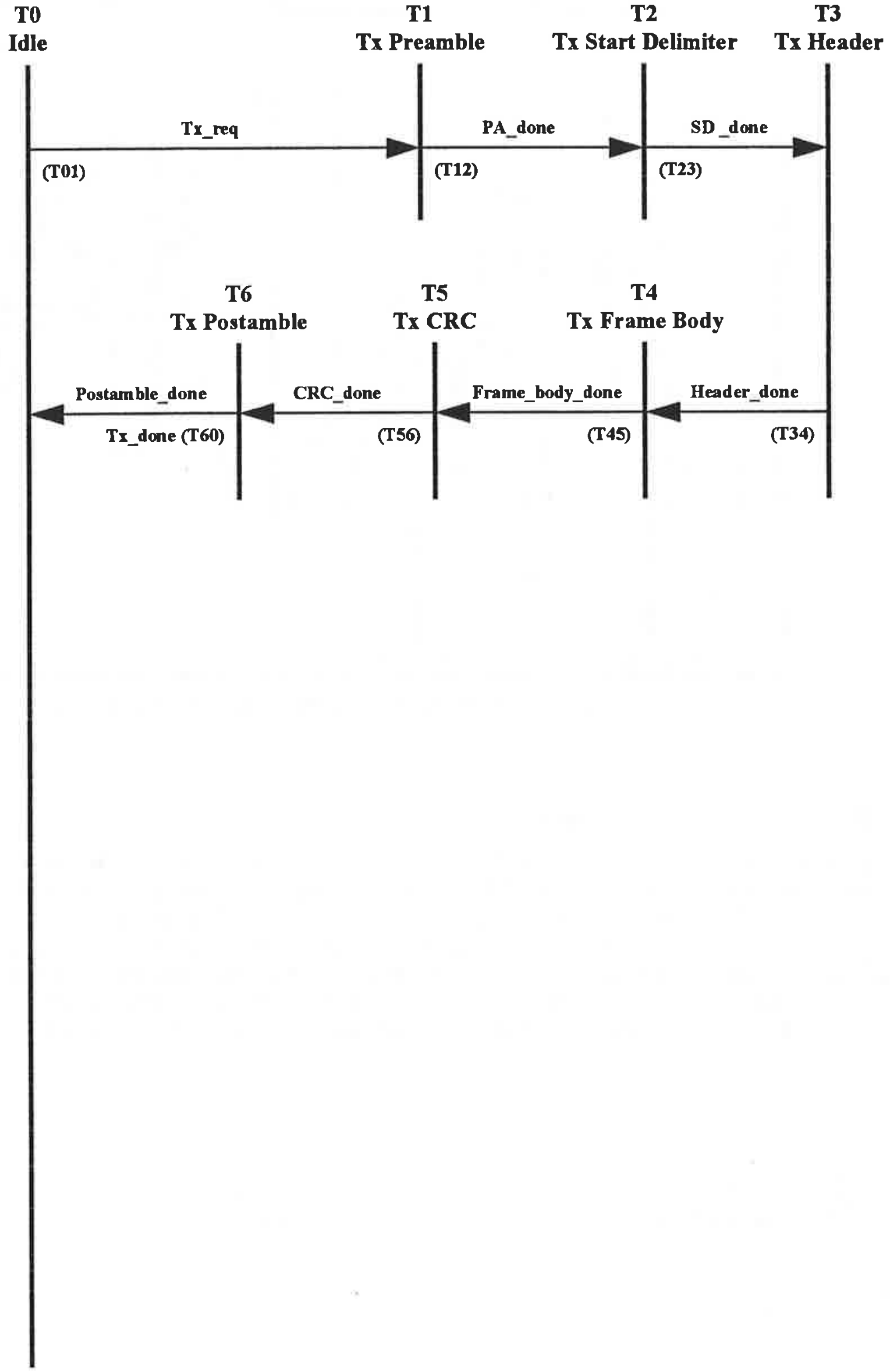


Figure 6-24: Transmit State Machine

Notes to the transmit state machine

State T0, Idle: The MAC transmitter shall enter this state upon initialization or after a transmission is concluded.
T01, Start_transmit: When a transmit request is received this transition shall be taken to begin a transmission.

State T1, Tx Preamble: In this state the transmit state machine shall cause the PHY-specific preamble to be transmitted. PA_done shall be set when the preamble has been transmitted.
T12, Send_start_delimiter: This transition shall be taken when the transmission of the preamble is complete.

State T2, Tx Start Delimiter: The state machine shall enter this state at the conclusion of the transmission of the preamble. In this state, the unique word that delimits the start of a frame shall be transmitted. At the conclusion of the transmission of the start delimiter, SD_done shall be set.
T23, Send_MAC_header: This transition shall be taken when the transmission of the start delimiter is complete.

State T3, Tx Header: In this state , the MAC header shall be assembled and transmitted. Bits in the Type, Control and MPDUID/ConnID fields shall be updated immediately before transmission. At the conclusion of the header transmission, Header_done shall be set.
T34, Send_frame_body: This transition shall be taken when the transmission of the MAC header is complete.

[T3 needs better definition of the fields to be updated immediately before transmission -Bob]
State T4, Tx Frame Body: In this state, the body of the MAC frame, if any, shall be transmitted. At the conclusion of the transmission of the frame body, or unconditionally if there is no frame body, Frame_body_done shall be set.
T45, Send_CRC: This transition shall be taken when the transmission of the frame body is complete.

State T5, Tx CRC: In this state the CRC shall be transmitted. At the conclusion of the transmission of the CRC, CRC_done shall be set.
T56, Send_postamble: This transition shall be taken when the transmission of the CRC is complete.

State T6, Tx Postamble: In this state, any required ending delimiter and PHY-specific trailer shall be transmitted. At the conclusion of the transmission of the postamble, Postamble_done shall be set.
T60, Transmit_complete: This transition shall be taken when the transmission of the postamble is complete. Tx_done shall be set.

1.7.2.2. Receive State Machine

The receive state machine is almost as simple as the transmit state machine. The receive state machine remains idle until the PHY indicates that a frame is being received. When the PHY signals that a start delimiter has been received, the receive state machine takes the transition to the state that processes the frame body. If no errors are detected and a valid frame type is received, the exit from this state is solely dependent on the frame type received. Based on the frame type, the next state is chosen such that the proper actions required by each frame type are accomplished. Most of the states chosen based on the frame type have two exit paths. One path is chosen to indicate to the control state machine that additional protocol actions are required. The other path is chosen if there is no protocol action required by the control state machine.

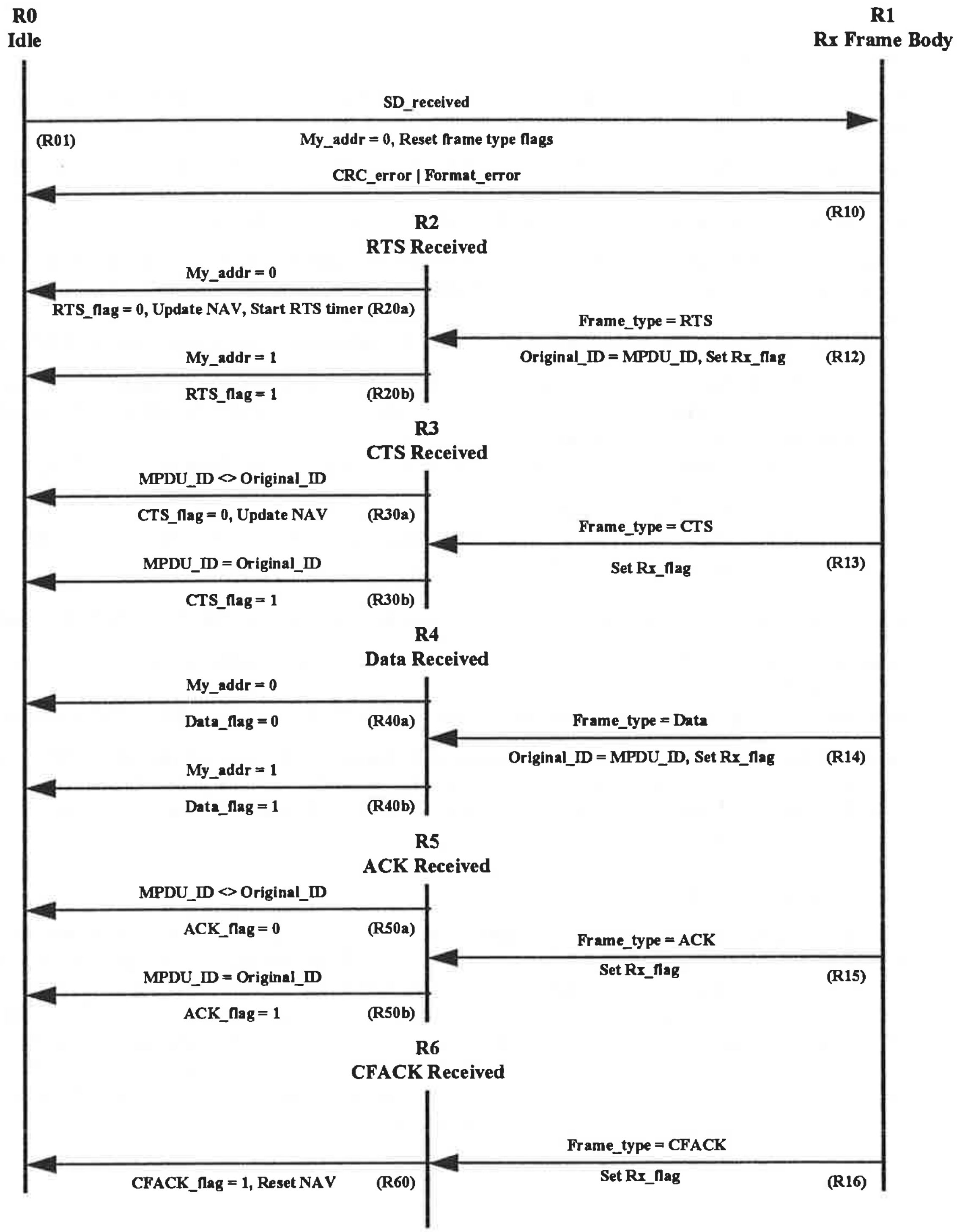


Figure 6-25: Receive State Machine

Notes to the receive state machine

State R0, Idle: This state shall be entered whenever the MAC receiver is initialized. In this state the receiver awaits the receipt of the start delimiter.
R01, Start_Receive: If a start delimiter is received from the PHY, a transition to state R1 shall occur. The address recognized flag and error detected flag shall be cleared. The CRC accumulator shall be cleared in preparation for receiving a frame. My_addr and the frame type flags shall be cleared.

State R1, Rx Frame Body: This state shall be entered when a valid start delimiter is detected. In this state the incoming frame shall be checked for valid format, correct CRC, valid network identifier and correct MPDU_ID as appropriate for the frame type. Based upon the frame type received, the appropriate exit shall be chosen. If the frame is uniquely addressed to this station, My_addr shall be set.
R10, Frame_error: If there is an error in the frame format or the frame contains a CRC error, this transition shall be taken to return the receiver to the Idle state. The error flag shall be set.
R12, Received_RTS: When the frame is valid and the frame type is RTS, this transition shall be taken. Original_ID shall be set to MPDU_ID. Rx_flag shall be set.
R13, Received_CTS: When the frame is valid and the frame type is CTS, this transition shall be taken.. Rx_flag shall be set.
R14a, Received_Data: When the frame is valid and the frame type is Data, this transition shall be taken.. Rx_flag shall be set.
R14b, Received_Unitdata: When the frame is valid and the frame type is Unitdata, this transition shall be taken. Original_ID shall be set to MPDU_ID.. Rx_flag shall be set.
R15, Received_ACK: When the frame is valid and the frame type is ACK, this transition shall be taken.. Rx_flag shall be set.

State R2, RTS Received: This state shall be entered when a valid RTS frame is received. In this state the actions appropriate to receipt of an RTS frame shall be taken.
R20a, Other_RTS: This transition shall be taken when the RTS receipt actions are complete and My_addr is not set. The NAV shall be updated with the value in the Length field of the frame plus the value of RTS_time_offset. The RTS_flag shall be reset. The RTS timer shall be initialized and started.
R20b, RTS_complete: This transition shall be taken when the RTS receipt actions are complete and My_addr is set. The RTS_flag shall be set.

State R3, CTS Received: This state shall be entered when a valid CTS frame is received. In this state the actions appropriate to receipt of a CTS frame shall be taken. The CTS timer shall be stopped.
R30a, Other_CTS: This transition shall be taken when the CTS receipt actions are complete and the MPDU_ID is not equal to the Original_ID. The NAV shall be updated with the value in the Length field of the frame plus the value of CTS_time_offset. The CTS_flag shall be reset.
R30b, CTS_complete: This transition shall be taken when the CTS receipt actions are complete and the MPDU_ID is equal to the Original_ID. The CTS_flag shall be set.

State R4, Data Received: This state shall be entered when a valid Data or Unitdata frame is received. In this state the actions appropriate to receipt of a Data or Unitdata frame shall be taken. If the destination address received is contained in the set of this station's destination addresses and the To_AP bit is not set in the control field, the address recognized flag shall be set and the frame shall be passed to the LLC entity.
R40a, Other_Data: This transition shall be taken when the data receipt actions are complete and My_addr is not set. The data_flag shall be reset.
R40b, Data_complete: This transition shall be taken when the data receipt actions are complete and My_addr is set. The data_flag shall be set.

State R5, ACK Received: This state shall be entered when a valid ACK frame is received. In this state, the actions appropriate to the receipt of an ACK frame shall be taken.
R50a, Other_ACK: This transition shall be taken when the ACK receipt actions are complete and the MPDU_ID

is not equal to the Original_ID. The ACK_flag shall be reset. The NAV shall be updated to indicate that the network is now free.
R50b, ACK_complete: This transition shall be taken when the ACK receipt actions are complete and the MDPU_ID is equal to the Original_ID. The ACK_flag shall be set.

State R6, CFACK Received: This state shall be entered when a valid CFACK frame is received.
R60, CFACK_complete: This transition shall be taken when the CFACK receipt actions are complete. The NAV shall be reset. The CFACK_flag shall be set.

1.7.2.3. Control State Machine

The control state machine is a combination of several simple loops. The largest loop consists of states C0, C1, C2 C3 and C4. This is the loop used to transmit a frame with the RTS/CTS handshake. There are two conditional exits from this loop; one exit is used when CTS is not received in response to RTS, the other is used when an ACK is not received after transmitting the data frame. This loop may also be entered in the middle, at state C3, in order to transmit a Unitdata frame, i.e., a data frame without the RTS/CTS handshake. When either of the conditional exits from this loop is taken or if a transmission is attempted while the media is not free, a path is entered that calculates a backoff interval and initiates the backoff period. The remainder of the state machine is a set of four short loops that handle the responses to receipt of RTS frames, data frames, expiration of the backoff period and the lack of CTS response to an RTS addressed to another station.

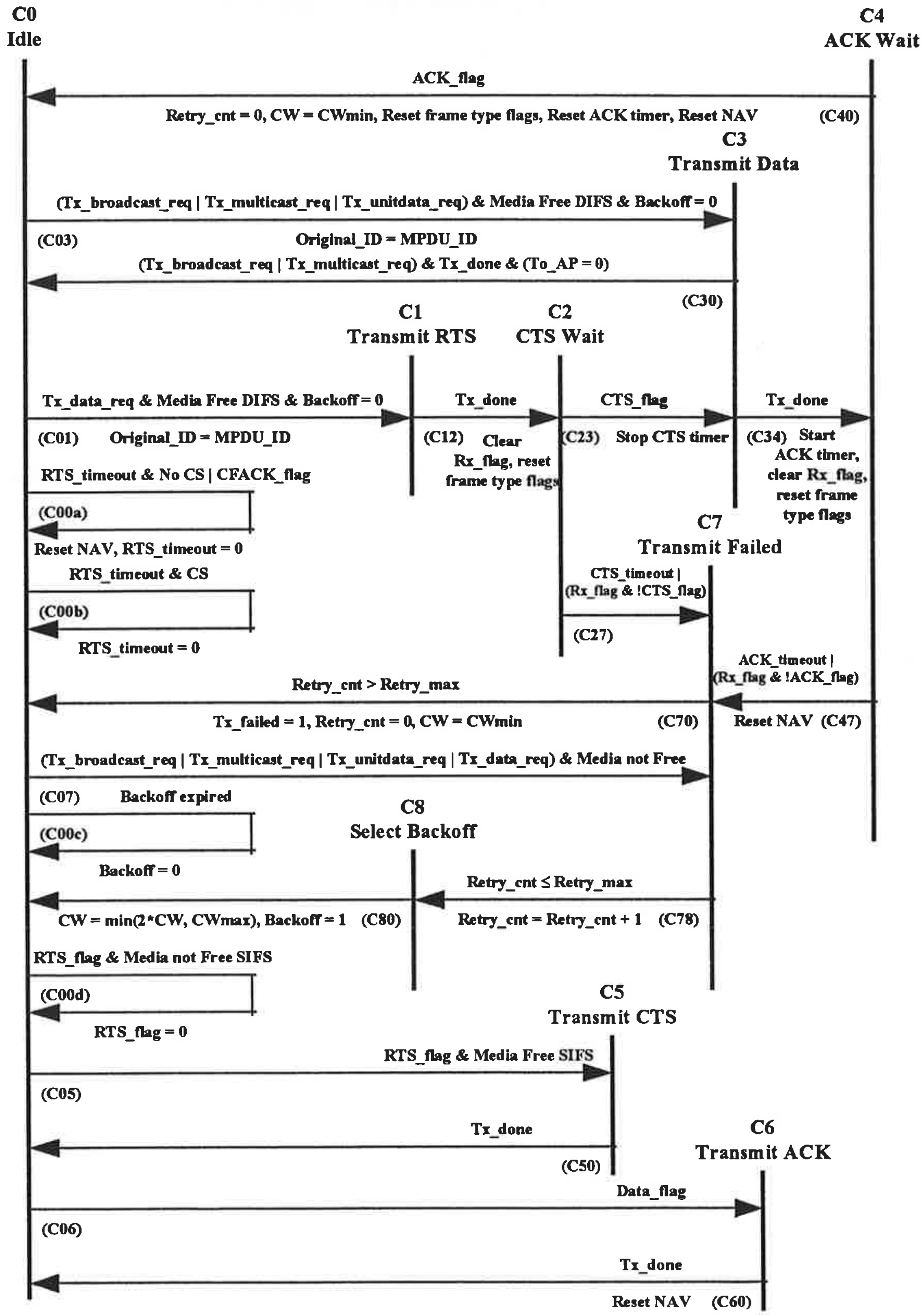

C0
Idle
C4
ACK Wait
ACK_flag
Retry_cnt = 0, CW = CWmin, Reset frame type flags, Reset ACK timer, Reset NAV
(C40)
C3
Transmit Data
(Tx_broadcast_req | Tx_multicast_req | Tx_unitdata_req) & Media Free DIFS & Backoff = 0
(C03)
Original_ID = MPDU_ID
(Tx_broadcast_req | Tx_multicast_req) & Tx_done & (To_AP = 0)
(C30)
C1
Transmit RTS
C2
CTS Wait
Tx_data_req & Media Free DIFS & Backoff = 0
(C01)
Original_ID = MPDU_ID
Tx_done
(C12)
Clear Rx_flag, reset frame type flags
CTS_flag
(C23)
Stop CTS timer
Tx_done
(C34)
Start ACK timer, clear Rx_flag, reset frame type flags
RTS_timeout & No CS | CFACK_flag
(C00a)
Reset NAV, RTS_timeout = 0
RTS_timeout & CS
(C00b)
RTS_timeout = 0
C7
Transmit Failed
CTS_timeout | (Rx_flag & !CTS_flag)
(C27)
ACK_timeout | (Rx_flag & !ACK_flag)
Retry_cnt > Retry_max
Tx_failed = 1, Retry_cnt = 0, CW = CWmin
(C70)
Reset NAV
(C47)
(Tx_broadcast_req | Tx_multicast_req | Tx_unitdata_req | Tx_data_req) & Media not Free
(C07)
Backoff expired
(C00c)
Backoff = 0
C8
Select Backoff
Retry_cnt ≤ Retry_max
CW = min(2*CW, CWmax), Backoff = 1
(C80)
Retry_cnt = Retry_cnt + 1
(C78)
RTS_flag & Media not Free SIFS
(C00d)
RTS_flag = 0
C5
Transmit CTS
RTS_flag & Media Free SIFS
(C05)
Tx_done
(C50)
C6
Transmit ACK
Data_flag
(C06)
Tx_done
Reset NAV
(C60)

Figure 6-26: Control State Machine

Notes to the control state machine

State C0, Idle: The control state machine shall enter this state upon initialization and after any of the following conditions: receipt of ACK after a successful transmission, exceeding the maximum retry count during transmission, after a backoff interval has been computed, after transmitting a CTS and after transmitting an ACK. In this state, the backoff interval shall be counted down while the media is free. While in a backoff interval, transmit requests shall be postponed.
C00a, No_Data: This transition shall be taken when the RTS timer expires due to not receiving a data frame that corresponds to the RTS frame or due to the receipt of a CFACK frame signalling the end of a contention-free period. The NAV shall be reset and the RTS_timeout shall be reset.
C00b, RTS_timeout_and_busy: This transition shall be taken when the RTS timer expires and the PHY indicates activity on the medium. The RTS timeout condition shall be reset.
C00c, Backoff_done: This transition shall be taken when the backoff interval expires. The Backoff flag shall be reset.
C00d, Can't_respond_to_RTS: This transition shall be taken when a valid RTS frame addressed to this station has been received and a response is not possible because the media is not free.
C01, Start_transmit_handshake: This transition shall be taken when the MAC is requested to transmit with the full RTS, CTS handshake, the MAC is not in a backoff interval and the media is free for longer than DIFS.
C03, Start_transmit_unitdata: This transition shall be taken when the MAC is requested to transmit a unitdata frame, a multicast frame or a broadcast frame, the media is free longer than DIFS and the MAC is not in a backoff interval.
C05, Send_CTS: This transition shall be taken when a valid RTS frame addressed to this station is received and the media is free longer than SIFS.
C06, Send_ACK: This transition shall be taken when a valid data frame addressed to this station is received.
C07, Media_busy: This transition shall be taken when a transmit data request is received and the media is busy.

State C1, Transmit RTS: In this state , a valid RTS frame addressed to the destination shall be formed and passed to the Transmit state machine. The Tx_req shall be set.
C12, Wait_for_CTS: This transition shall be taken when the transmission of the RTS frame is complete. The Rx_flag and frame type flags shall be reset.

State C2, CTS Wait: This state shall be entered after an RTS frame has been transmitted. The CTS timeout timer shall be initialized and started.
C23, Send_data: This transition shall be taken when a valid CTS frame that matched the MPDUID of the previously transmitted RTS has been received. The CTS timer and CTS_timeout shall be reset.
C27, No_CTS: This transition shall be taken when the CTS timer expires or the Rx_flag is set and the frame type is not CTS_frame.

State C3, Transmit Data: In this state, the MAC data frame shall be formed and the Tx_request shall be set.
C30, Multicast_sent: This transition shall be taken when the transmission of a broadcast or multicast frame is complete and the frame is not to be forwarded by an access point.
C34, Wait_for_ACK: This transition shall be taken when the transmission of the data frame is complete and the frame was not a multicast or broadcast frame sent to an AP. The ACK timer shall be initialized and started. The Rx_flag and frame type flags shall be reset.

State C4, ACK Wait: This state shall be entered while waiting for an ACK response to a transmitted data frame.
C40, End_transmit_handshake: This transition shall be taken when a valid ACK frame that matches the MPDUID of the previously transmitted RTS has been received. Retry_cnt and the frame type flags shall be reset and CW set to CWmin. The ACK timer shall be reset. The NAV shall be reset.
C47, No_ACK: This transition shall be taken when the ACK timer expires or the Rx_flag is set and the frame type is not ACK_frame. The NAV shall be reset.

State C5, Transmit CTS: In this state, the control state machine shall respond to an RTS frame directed to this station. A CTS frame shall be formed and passed to the Transmit state machine. The Tx_req shall be set.
C50, CTS_complete: This transition shall be taken when the CTS frame has been transmitted.

State C6, Transmit ACK: In this state, the control state machine shall respond to the successful receipt of a data frame. An ACK frame shall be formed and passed to the Transmit state machine. The Tx_req shall be set.
C60, ACK_complete: This transition shall be taken when the transmission of the ACK frame is complete. The NAV shall be reset.

State C7, Transmit Failed: In this state, the control state machine shall react to a failure in the handshake required for data transmission or to a request to transmit while the medium is not free.
C70, Transmission_failure: This transition shall be taken when the maximum number of retry attempts has been exhausted. Tx_failed shall be set. Retry_cnt shall be reset. CW shall be set to CWmin.
C78, Try_again: This transition shall be taken when the maximum number of retry attempts has not been exhausted. The Retry_cnt shall be incremented.

State C8, Select Backoff: In this state a backoff interval shall be calculated by multiplying a random number uniformly distributed between zero and one by the product of the contention window parameter (CW) and the slot time.
C80, Wait_for_Backoff: This transition shall be taken when the backoff interval is computed. The CW shall be doubled and limited by CWmax. The backoff flag shall be set.

1.7.3. MAC Management State Machines