Chapter III

THE IEEE 802.11 ARCHITECTURE

3.1 Components of the IEEE 802.11 Architecture

The IEEE 802.11 architecture consists of several components. These components interact to provide a wireless LAN that supports station mobility transparently to upper layers. The basic service set (BSS) is the basic building block of an IEEE 802.11 LAN. Figure 3.1 shows two BSSs, each of which has two stations that are members of the BSS. In the figure, ovals are used to depict a BSS as the coverage area within which the member stations of the BSS may remain in communication. If a station moves out of its coverage area, i.e., its BSS, it can no longer directly communicate with other members of the BSS [1-2].

3.1.1 Wireless LAN Topologies

The WLAN station (STA) is one of the components of the wireless network. A station may be a laptop PC, handheld device, or an Access Point (AP) that contains the functionality of the 802.11 protocol. The BSS consists of a logical group of wireless stations, which may be a collection of a number of stations. There are basically two types of BSS that correspond to two transmission methods supported by WLANs. They are namely,

- *Peer-to-Peer or Ad Hoc*
- *Infrastructure.*

Estelar

Peer-to-peer or ad hoc networking consists of a group of computing devices equipped with wireless Network Interface Cards (NICs) directly communicating with one another [2-3]. This setup does not use a wireless AP and is called an Independent Basic Service Set (IBSS).

Infrastructure networking requires all wireless nodes to communicate via an AP. The AP is connected to the main wired networking infrastructure and acts as a relay between the wireless and wired LANs. This structure is referred to as an Infrastructure Basic Service Set [4].

3.1.2 The Independent Basic Service Set as an Ad hoc Network

The Independent Basic Service Set (IBSS) is the most basic type of IEEE 802.11 LAN. A minimum IEEE 802.11 LAN may consist of only two stations. Figure 3.1 shows two IBSSs. This mode of operation is possible when IEEE 802.11 stations are able to communicate directly. Because this type of IEEE 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.

Estelar

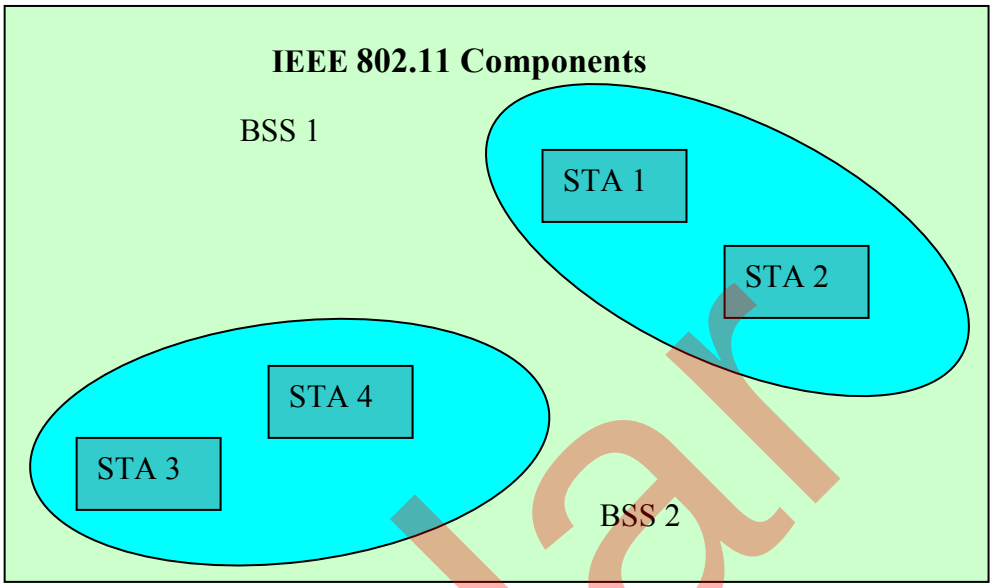

Figure 3.1: Basic Service Sets

3.1.3 STA and BSS association

The association between an STA and a BSS is dynamic i.e., STAs turn on, turn off, come within range, and go out of range. To become a member of an infrastructure BSS, a station shall become "associated." These associations are dynamic and involve the use of the distribution system service (DSS) [2].

3.1.3.1 Distribution System Service Concepts

For some networks the physical distance is sufficient; for other networks, increased coverage is required. In that case, instead of existing independently, a BSS may also form a component of an extended form of network that is built with multiple BSSs. The architectural component used to interconnect BSSs is the distribution system (DS). IEEE 802.11 logically separates the wireless medium (WM) from the distribution system medium (DSM). Each logical medium is used

Estela

for different purposes, by a different component of the architecture. The IEEE 802.11 definitions neither preclude, nor demand, that the multiple media be either the same or different. Recognizing that the multiple media are *logically* different is a key to understanding the flexibility of the architecture [1],[3].

The IEEE 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. An access point (AP) is a STA that provides access to the DS by providing DS services in addition to acting as a STA [1-5]. Figure 3.2 adds the DS and AP components to the IEEE 802.11 architecture picture.

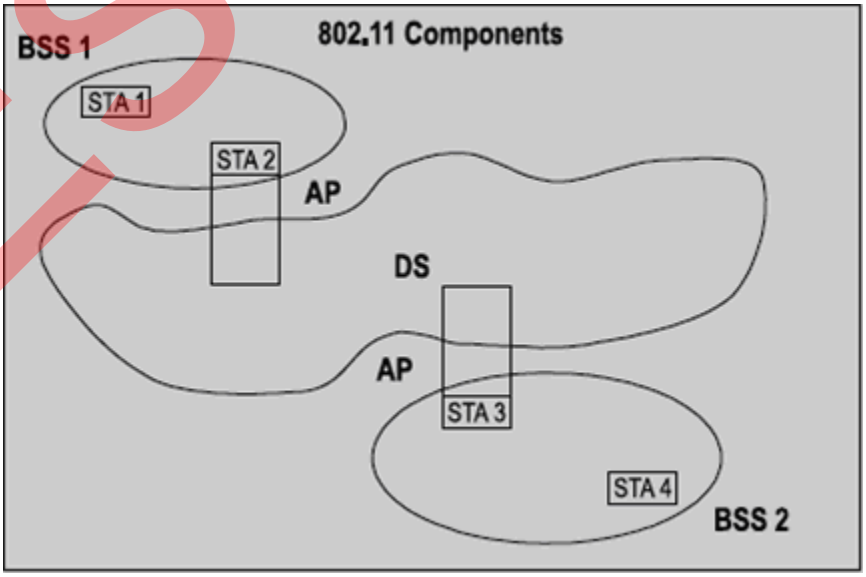

Figure3.2: Distribution systems and access points [1]

Estelar

Data move between a BSS and the DS via an AP. All APs are also STAs thus they are addressable entities. The addresses used by an AP for communication on the WM and on the DSM are not necessarily the same.

3.1.3.2 Extended Service Set (ESS): The large coverage network

The DS and BSSs are responsible for allowing IEEE 802.11 to create a wireless network of arbitrary size and complexity. IEEE 802.11 refers to this type of network as the extended service set network. The key concept is that the ESS network appears the same to an LLC layer as an IBSS network. Stations within an ESS may communicate and mobile stations may move from one BSS to another within the same ESS transparently to LLC as seen in Figure 3.3.

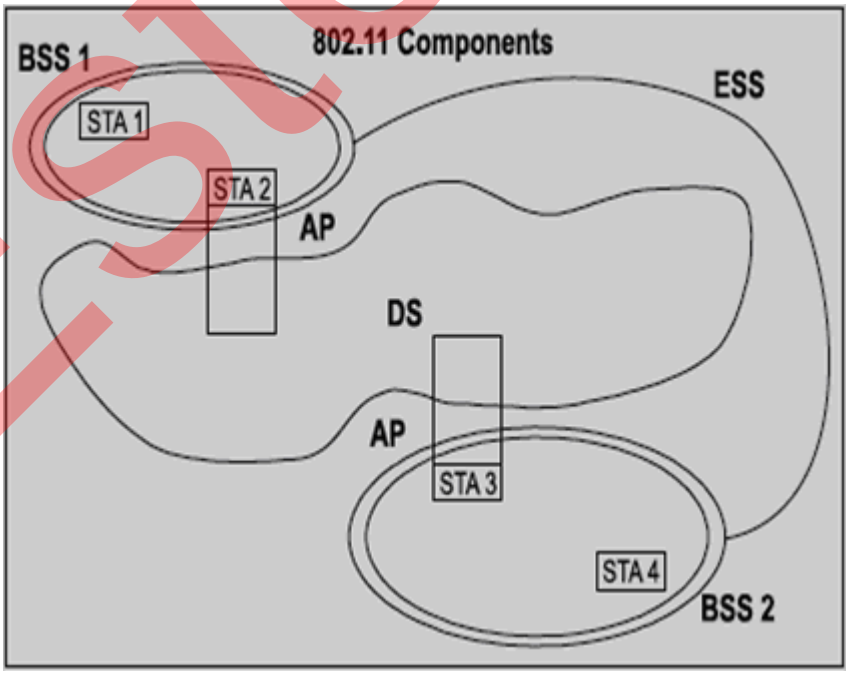

Figure 3.3: Extended Service Set [1]

Estelar

All of the following are possible:

a) *The overlapping of BSSs is allowed. This is commonly used to arrange contiguous coverage within a physical volume.*

b) The BSSs could be physically all over the place and disjointed. Logically there is no limit to the distance between BSSs.

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

d) One or more IBSS or ESS networks may be physically present in the same space as one or more ESS networks. This is possible for a number of reasons. For example, an ad hoc network is operating in a location that also has an ESS network or physically overlapping IEEE 802.11 networks have been set up by different organizations.

3.1.4 Coverage Area

For wireless PHYs, well-defined coverage areas simply do not exist. Propagation characteristics are dynamic and erratic. Small changes in position or direction may result in dramatic differences in signal strength [6-9][11-12]. Similar effects occur whether a STA is stationary or mobile (as moving objects may impact station-to-station propagation).

Figure 3.4 shows a signal strength map for a simple square room with a standard metal desk and an open doorway [1]. Figure 3.4 is a static snapshot; the propagation patterns change dynamically as stations and objects in the

Estelar

environment move. In Figure 3.4 the dark (solid) blocks in the lower left are a metal desk and there is a doorway at the top right of the figure. The figure indicates relative differences in field strength with different intensities and indicates the variability of field strength even in a static environment.

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 IEEE 802.11 architectural diagrams to represent the coverage of a BSS.

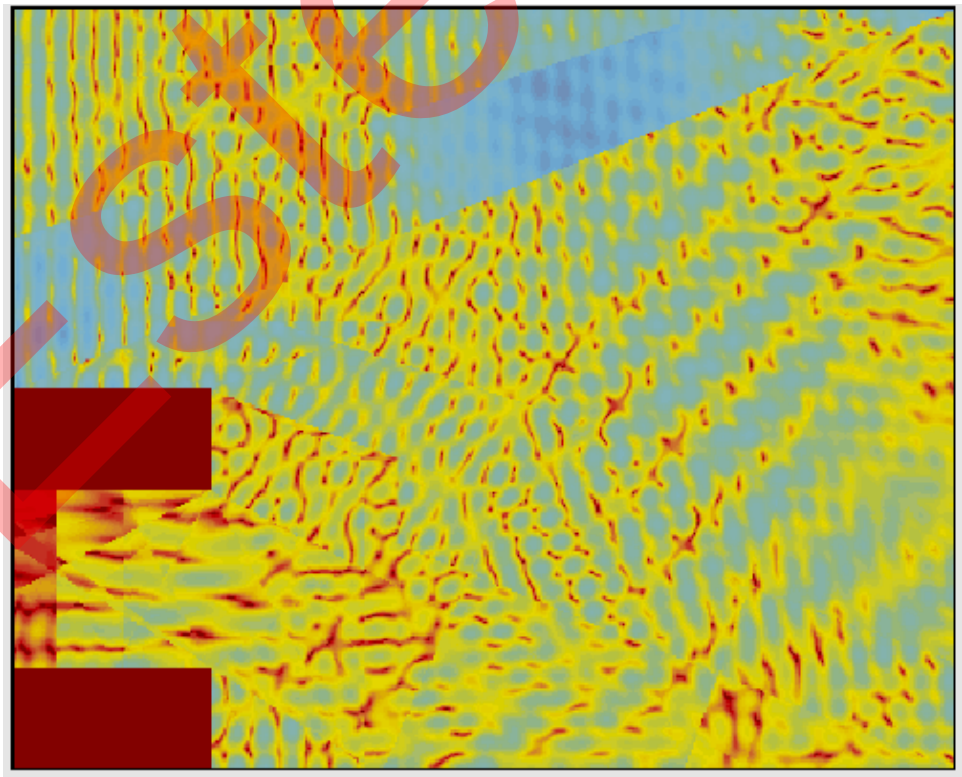

Figure 3.4: A Signal Intensity Map [1]

Fetelar

3.1.5 Integration with wired LANs

WLANs are generally augmented with the wired LANs. To integrate the IEEE 802.11 architecture with a traditional wired LAN, a logical architectural component is introduced called a portal. A portal is the logical point at which MSDUs from an integrated non-IEEE 802.11 LAN enter the IEEE 802.11 DS [1].

For example, a portal is shown in Figure 3.5 connecting to a wired IEEE 802 LAN. All data from non-IEEE 802.11 LANs enter the IEEE 802.11 architecture via a portal. The portal provides logical integration between the IEEE 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 IEEE 802 LAN components.

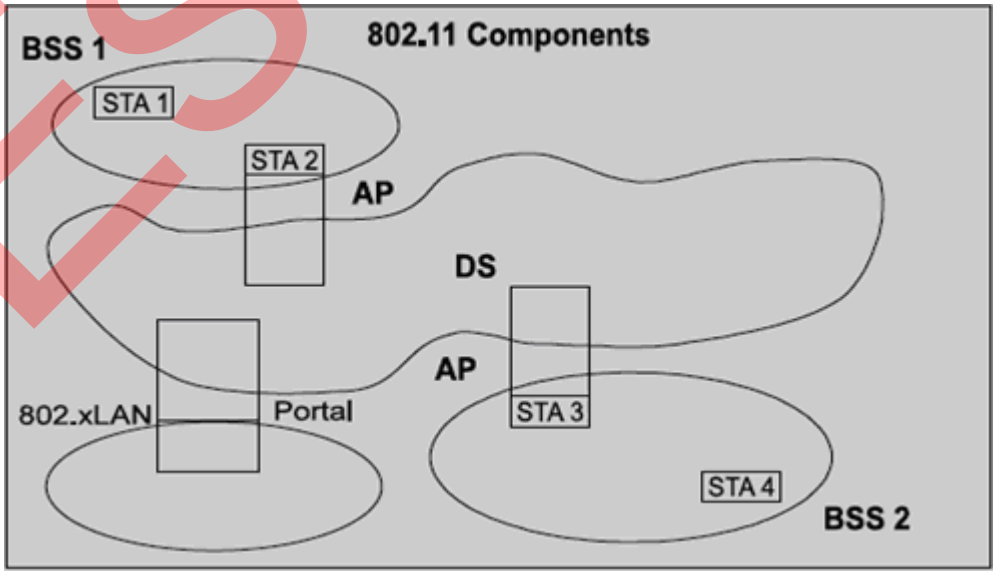

Figure 3.5: WLAN with other IEEE 802 LANs [1]

Estelar

In IEEE 802.11, the ESS architecture, consist of Access Points and the Distribution System, provides traffic segmentation and range extension. Logical connections between IEEE 802.11 and other LANs are through the portal. Portals connect between the DSM and the LAN medium that is to be integrated.

3.1.5.1 Logical Service Interfaces

IEEE 802.11 does not restrain the DS to be either data link or network layer based, nor does IEEE 802.11 limit a DS to be either centralized or distributed in nature. IEEE 802.11 explicitly does not specify the details of DS implementations. Instead, IEEE 802.11 specifies services. The services are associated with different components of the architecture. There are two categories of IEEE 802.11 service:

1. *The station service (SS) and*
2. *The distribution system service (DSS).*

Both categories of service are used by the IEEE 802.11 MAC sublayer [1-4]. The complete set of IEEE 802.11 architectural services is as follows:

a) *Authentication*

b) Association

c) Deauthentication

d) Disassociation

Estelar

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 STA, and those that are part of a DS [1-4].

3.1.5.2 Station Service (SS)

The station service is provided by stations. The SS is present in every IEEE 802.11 station (including APs, as APs include station functionality). The SS is specified for use by MAC sublayer entities. All conformant stations provide SS. The SS is as follows:

a) Authentication

b) Deauthentication

c) Privacy

d) MSDU delivery

3.1.5.3 Distribution System Service (DSS)

The distribution system service is provided by the DS. These services are represented in the IEEE 802.11 architecture by arrows within the APs, indicating

Estelar

that the services are used to cross media and address space logical boundaries. The physical embodiment of various services may or may not be within a physical AP [1],[3]. The DSSs are provided by the DS. They are accessed through a STA that also provides DSSs. A STA that is providing access to DSS is an AP.

The DSSs are as follows:

a) Association

b) Disassociation

c) Distribution

d) Integration

e) Reassociation

DSSs are specified for use by MAC sublayer entities.

Figure 3.6 combines the components from previous figures with both types of services to show the complete IEEE 802.11 architecture.

Estelar

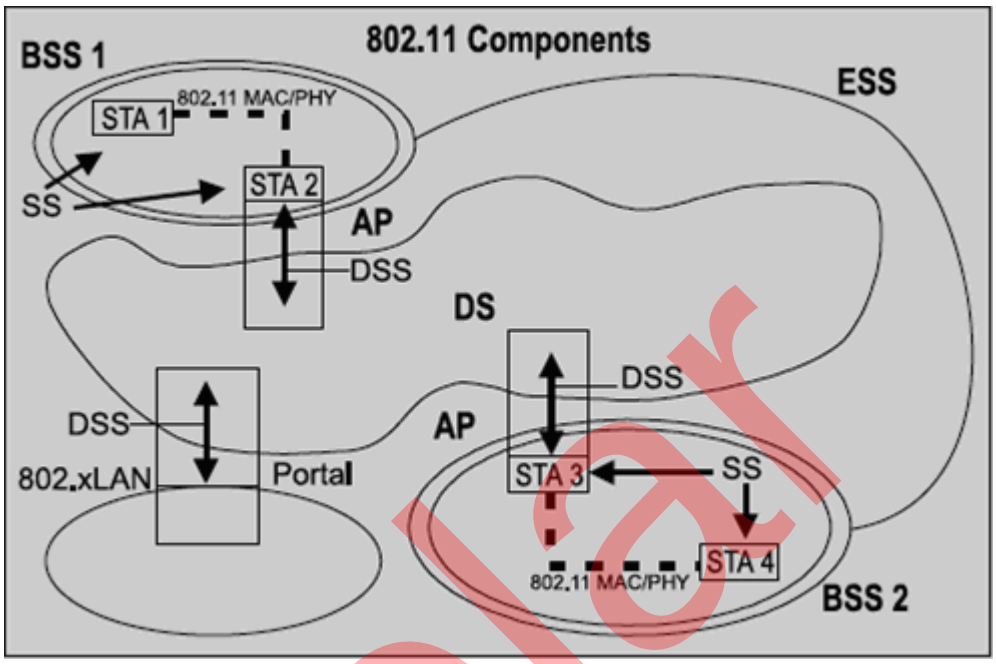

Figure 3.6: Complete Architecture [1]

Estelar

3.1.5.4 Multiple logical address spaces

The IEEE 802.11 architecture permits that the WM, DSM, and an integrated wired LAN may all be different physical media; it also allows that each of these components may be operating within different address spaces. IEEE 802.11 only uses and specifies the use of the WM address space. Each IEEE 802.11 PHY operates in a single medium, i.e., the WM.

The IEEE 802.11 MAC operates in a single address space. MAC addresses are used on the WM in the IEEE 802.11 architecture. Therefore, it is unnecessary for the standard to explicitly specify that its addresses are “WM addresses”. IEEE 802.11 has chosen to use the IEEE 802 48-bit address space [1],[3]. Thus IEEE 802.11 addresses are compatible with the address space used by the IEEE 802

LAN family. The IEEE 802.11 choice of address space implies that for many instantiations of the IEEE 802.11 architecture, the wired LAN MAC address space and the IEEE 802.11 MAC address space may be the same. In those situations where a DS that uses MAC level IEEE 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 IEEE 802.11 architecture allows for all three logical address spaces to be distinct. A multiple address space example is one in which the DS implementation uses 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 a key to the ability of IEEE 802.11 to be independent of the DS implementation and to interface cleanly with network layer mobility approaches [1] [10-12].

Estelar

3.2 Overview of the Services

There are nine services specified by IEEE 802.11. Six of the services are used to support MSDU delivery between STAs. Three of the services are used to control IEEE 802.11 LAN access and confidentiality. Here presented the services, an overview of how each service is used, and a description of how each service relates to other services and the IEEE 802.11 architecture. 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 IEEE 802.11 MAC sublayer medium access method.

The IEEE 802.11 MAC sublayer uses three types of messages:

1. *data*,
2. *management*, and
3. *control*.

The data messages are handled via the MAC data service path. MAC management messages are used to support the IEEE 802.11 services and are handled via the MAC management service data path. MAC control messages are used to support the delivery of IEEE 802.11 data and management messages [1].

3.2.1 Distribution of messages within a DS

3.2.1.1 Distribution

This is the primary service used by IEEE 802.11 STAs. It is conceptually invoked by every data message to or from an IEEE 802.11 STA operating in an ESS when the frame is sent through the DS. Distribution is via a DSS. Refer to the ESS network in Figure 3.6 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

Estelar

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 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 DS is not specified by IEEE 802.11. All IEEE 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 that corresponds to the desired recipient. The necessary information is provided to the DS by the three association related services (association, reassociation, and disassociation).

The previous example was a case in which the AP that invoked the distribution service was different from the AP that received the distributed message. If the message had been intended for a station that 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 [1].

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 is not specified by this standard. While IEEE 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 IEEE 802.11 frame formats.

Estelar

3.2.1.2 Integration

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 that are distributed to a portal cause the DS to invoke the Integration function. The Integration function 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 DSS.

Messages received from an integrated LAN (via a portal) by the DS for an IEEE 802.11 STA will invoke the Integration function before the message is distributed by the distribution service. The details of an Integration function are dependent on a specific DS implementation and are outside the scope of this standard.

3.2.2 Services Supporting the Distribution Service

The primary purpose of a MAC sublayer is to transfer MSDUs between MAC sublayer 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 shall be "associated". To understand the concept of association, it is necessary first to understand the concept of mobility.

Estelar

3.2.2.1 Mobility types

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

a) ***No-transition:***

In this type, two subclasses that are usually indistinguishable are identified:

1) Static i.e., no motion.

2) Local movement i.e., movement within a basic service area (BSA).

b) ***BSS-transition:***

This type is defined as a station movement from one BSS in one ESS to another BSS within the same ESS.

c) ***ESS-transition:***

This type is defined as station movement from a BSS in one ESS to a BSS in a different ESS. This case is supported only in the sense that the STA may move. Maintenance of upper layer connections cannot be guaranteed by IEEE 802.11; in fact, disruption of service is likely to occur. The different association services support the different categories of mobility.

3.2.2.2 Association

To deliver a message within a DS, the distribution service needs to know which AP to access for the given IEEE 802.11 STA. This information is provided to the

Estelar

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 DSS. Before a STA is allowed to send a data message via an AP, it shall 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 its message distribution service. How the information provided by the association service is stored and managed within the DS is not specified by this standard.

At any given instant, a STA may be associated with no more than one AP. This ensures that the DS may 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. Association is always initiated by the STA, not the AP.

An AP may be associated with many STAs at one time. A STA learns what APs are present and then requests to establish an association by invoking the association service.

3.2.2.3 Reassociation

Association is sufficient for no-transition message delivery between IEEE 802.11 stations. Additional functionality is needed to support BSS-transition mobility. The additional required functionality is provided by the reassociation service.

Estelar

Reassociation is a DSS. 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 [1],[3]. Reassociation also enables changing association attributes of an established association while the STA remains associated with the same AP. Reassociation is always initiated by the mobile STA.

3.2.2.4 Disassociation

This service is invoked whenever an existing association is to be terminated. Disassociation is a DSS. In an ESS, this tells the DS to void existing association information. Attempts to send messages via the DS to a disassociated STA will be unsuccessful. The disassociation service may be invoked by either party to an association (non-AP STA or AP). Disassociation is a notification, not a request. Disassociation cannot be refused by either party to the association. APs may need to disassociate STAs to enable the AP to be removed from a network for service or for other reasons. STAs shall attempt to disassociate whenever they leave a network. However, the MAC protocol does not depend on STAs invoking the disassociation service.

3.2.3 Access and Confidentiality Control Services

The design of wired LANs assumes the physical attributes of wire. In particular, wired LAN design assumes the physically closed and controlled nature of wired media. The physically open medium nature of an IEEE 802.11 LAN violates

Estelar

those assumptions. Two services are provided to bring the IEEE 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 [1-3][13-14].

3.2.3.1 Authentication

Authentication is an SS. In wired LANs, physical security can be used to prevent unauthorized access. This is impractical in wireless LANs since they have a medium without precise bounds. IEEE 802.11 provides the ability to control LAN access via the authentication service. This service is used by all stations to establish their identity to stations with which they will communicate. This is true for both ESS and IBSS networks. If a mutually acceptable level of authentication has not been established between two stations, an association shall not be established.

IEEE 802.11 supports several authentication processes. The IEEE 802.11 authentication mechanism also allows expansion of the supported authentication schemes. IEEE 802.11 does not mandate the use of any particular authentication scheme. IEEE 802.11 provides link-level authentication between IEEE 802.11 STAs [1-2]. IEEE 802.11 does not provide either end-to-end (message origin to message destination) or user-to-user authentication. IEEE 802.11 authentication is used simply to bring the wireless link up to the assumed physical standards of a wired link.

Estelar

If desired, an IEEE 802.11 network may be operated using Open System authentication. This may violate implicit assumptions made by higher network layers. In an Open System, any station may become authenticated. IEEE 802.11 also supports Shared Key authentication. Use of this authentication mechanism requires implementation of the wired equivalent privacy (WEP) option.

In a Shared Key authentication system, identity is demonstrated by knowledge of a shared, secret, WEP encryption key [14]. Management information base (MIB) functions are provided to support the standardized authentication schemes. IEEE 802.11 requires mutually acceptable, successful, authentication. A STA may be authenticated with many other STAs at any given instant.

3.2.3.2 Preauthentication

Since, 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. Preauthentication is done by a STA while it is already associated with an AP (with which it previously authenticated). IEEE 802.11 does not require that STAs preauthenticate 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 [1-3]. The use of preauthentication takes the authentication service overhead out of the time-critical reassociation process.

Estelar

3.2.3.3 Deauthentication

The deauthentication service is invoked whenever an existing authentication is to be terminated. Deauthentication is an SS. In an ESS, since authentication is a prerequisite for association, the act of deauthentication shall cause the station to be disassociated. The deauthentication service may be invoked by either authenticated party (non-AP STA or AP). Deauthentication is not a request; it is a notification. Deauthentication shall not be refused by either party. When an AP sends a deauthentication notice to an associated STA, the association shall also be terminated [1-3].

3.2.3.4 Privacy

In a wired LAN, only those stations physically connected to the wire may hear LAN traffic. With a wireless shared medium, this is not the case. Any IEEE 802.11-compliant STA may hear all like-PHY IEEE 802.11 traffic that is within range. 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 implicit in wired LAN design, IEEE 802.11 provides the ability to encrypt the contents of messages. This functionality is provided by the privacy service. Privacy is an SS. In its first document, IEEE 802.11 specifies an optional privacy algorithm, WEP [14-15], 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

Estelar

secure as a wire". IEEE 802.11 uses the WEP mechanism to perform the actual encryption of messages.

It is noticeable 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 IEEE 802.11 STAs is "in the clear." If the privacy service is not invoked, all messages shall be sent unencrypted. If this default is not acceptable to one party or the other, data frames shall not be successfully communicated between the LLC entities.

Unencrypted data frames received at a station configured for mandatory privacy, as well as encrypted data frames using a key not available at the receiving station, are discarded without an indication to LLC (or without indication to distribution services in the case of "To DS" frames received at an AP). These frames are acknowledged on the WM, if received without frame check sequence (FCS) error, to avoid wasting WM bandwidth on retries [1],[13],[15].

Estelar

3.2.4 Relationships between services

An STA keeps two state variables for each STA with which direct communication via the WM is needed as follows:

1. Authentication state: The values are unauthenticated and authenticated.

2. Association state: The values are unassociated and associated.

These two variables create three local states for each remote STA:

State 1: Initial start state, unauthenticated, unassociated.

State 2: Authenticated, not associated.

State 3: Authenticated and associated.

The relationships between these station state variables and the services are given in Figure 3.7.

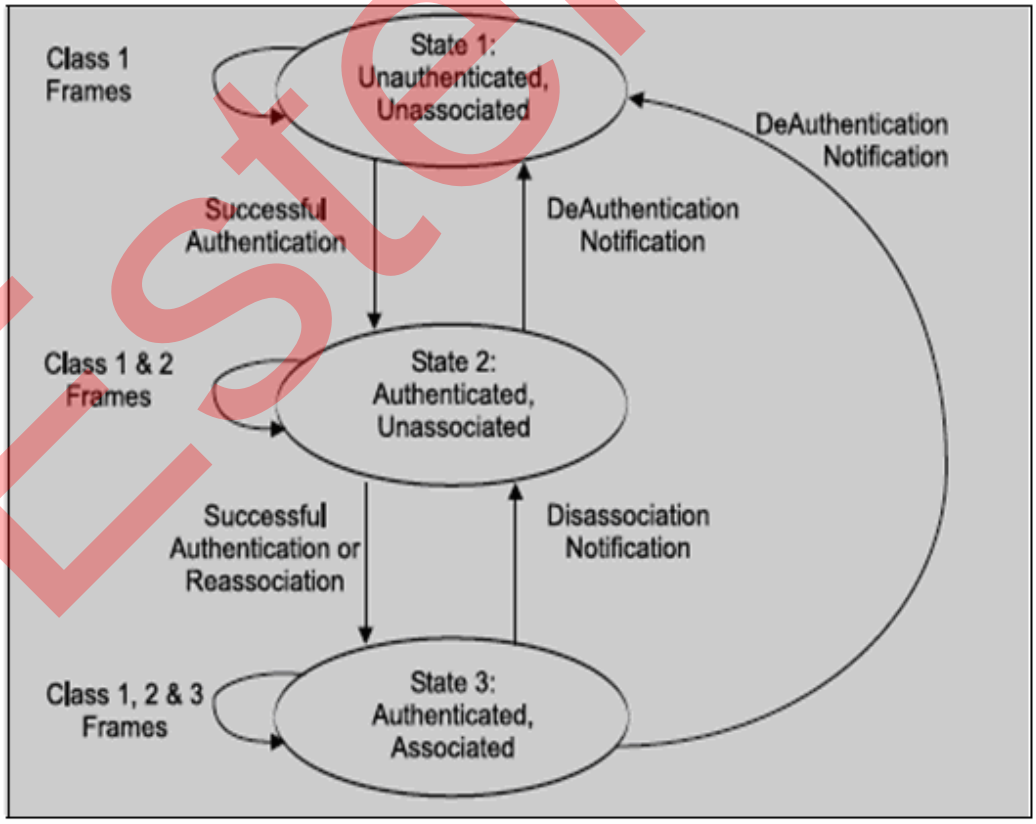

Figure 3.7: Relationship between state variables and services [1] [2]

Estelar

The current state existing between the source and destination station determines the IEEE 802.11 frame types that may be exchanged between that pair of STAs. 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 frame classes 1, 2, and 3 are allowed. The frame classes are defined as follows:

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

1) Control frames

i) Request to send (RTS)

ii) Clear to send (CTS)

iii) Acknowledgment (ACK)

iv) Contention-Free (CF)-End+ACK

v) CF-End

2) Management frames

i) Probe request/response

ii) Beacon

iii) Authentication: Successful authentication enables a station to exchange Class 2 frames. Unsuccessful authentication leaves the STA in State 1.

Estelar

iv) Deauthentication: Deauthentication notification when in State 2 or State 3 changes the STA's state to State 1. The STA shall become authenticated again prior to sending Class 2 frames.

v) Announcement traffic indication message (ATIM).

3) Data frames

Data: Data frames with frame control (FC) bits "To DS" and "From DS" both false.

b) Class 2 frames (if and only if authenticated; allowed from within States 2 and 3 only):

1) Management frames:

i) Association request/response

- *Successful association enables Class 3 frames.*
- *Unsuccessful association leaves STA in State 2.*

ii) Reassociation request/response

- *Successful reassociation enables Class 3 frames.*
- *Unsuccessful reassociation leaves the STA in State 2 (with respect to the STA that was sent the reassociation message). Reassociation frames shall only be sent if the sending STA is already associated in the same ESS.*

iii) Disassociation

Estelar

- *Disassociation notification when in State 3 changes a Station's state to State 2. This station shall become associated again if it wishes to utilize the DS. If STA A receives a Class 2 frame with a unicast address in the Address 1 field from STA B that is not authenticated with STA A, STA A shall send a deauthentication frame to STA B.*

c) Class 3 frames (if and only if associated; allowed only from within State 3):

1) Data frames

- *Data subtypes: Data frames allowed. That is, either the "To DS" or "From DS" FC bits may be set to true to utilize DSSs.*

2) Management frames

- *Deauthentication: Deauthentication notification when in State 3 implies disassociation as well, changing the STA's state from 3 to 1. The station shall become authenticated again prior to another association.*

3) Control frames

- *PS-Poll: If STA A receives a Class 3 frame with a unicast address in the Address 1 field from STA B that is authenticated but not associated with STA A, STA A shall send a disassociation frame to STA B. If STA A receives a Class 3 frame with a unicast address in*

Estelar

the Address 1 field from STA B that is not authenticated with STA A, STA A shall send a deauthentication frame to STA B.

3.2.5 Differences between ESS and IBSS LANs

It should be noted that an IBSS is often used to support an ad hoc network. In an IBSS network, an STA communicates directly with one or more other STAs. An IBSS consists of STAs that are directly connected. Thus there is only one BSS. Further, since there is no physical DS, there cannot be a portal, an integrated wired LAN, or the DSSs. The logical picture reduces to Figure 3.8.

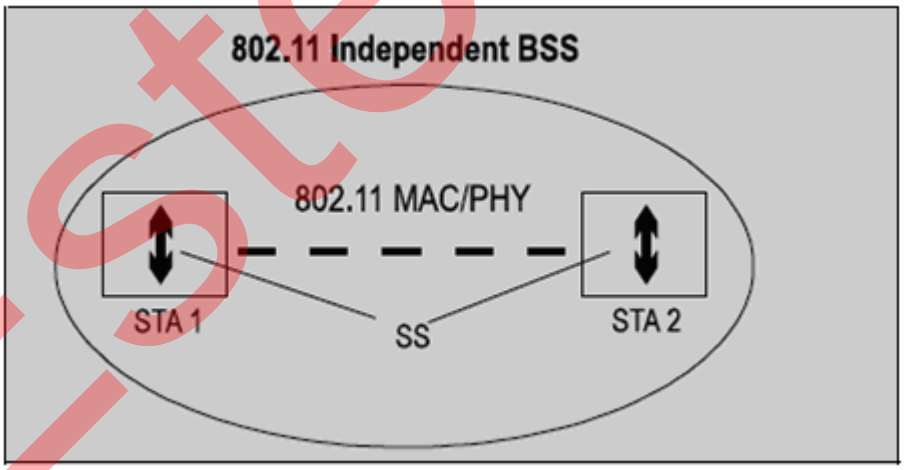

Figure 3.8: Logical architecture of an IBSS [1]

Only the minimum two stations are shown in Figure 3.8. An IBSS may 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 that apply to an IBSS are the SSs [1].

Estelar

3.2.6 Message information contents that support the services

Each service is supported by one or more IEEE 802.11 messages.

3.2.6.1 Data

For a STA to send data to another STA, it sends a data message, as shown below:

Data messages

i Message type: Data

ii Message subtype: Data

iii Information items:

- *IEEE source address of message*
- *IEEE destination address of message*
- *BSS ID*

iv Direction of message: From STA to STA

3.2.6.2 Association

For a STA to associate, the association service causes the following messages to occur:

Association request

i Message type: Management

ii Message subtype: Association request

iii Information items:

- *IEEE address of the STA initiating the association*
- *IEEE address of the AP with which the initiating station will associate*

Estelar

- *ESS ID*

iv Direction of message: From STA to AP

Association response

i Message type: Management

ii Message subtype: Association response

iii Information items:

- *Result of the requested association. This is an item with values "successful" and "unsuccessful."*
- *If the association is successful, the response shall include the association identifier (AID).*

iv Direction of message: From AP to STA

3.2.6.3 Reassociation

For a STA to reassociate, the reassociation service causes the following message to occur:

Reassociation request

i Message type: Management

ii Message subtype: Reassociation request

iii Information items:

- *IEEE address of the STA initiating the reassociation*
- *IEEE address of the AP with which the initiating station will reassociate*
- *IEEE address of the AP with which the initiating station is currently associated*

Estelar

• *ESS ID*

iv 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 [1].*

Reassociation response

i Message type: Management

ii Message subtype: Reassociation response

iii Information items:

- *Result of the requested reassociation. This is an item with values "successful" and "unsuccessful."*
- *If the reassociation is successful, the response shall include the AID.*

iv Direction of message: From AP to STA

3.2.6.4 Disassociation

For a STA to terminate an active association, the disassociation service causes the following message to occur:

Disassociation

i Message type: Management

ii Message subtype: Disassociation

iii Information items:

Estelar

• *IEEE address of the station that is being disassociated. This shall be the broadcast address in the case of an AP disassociating with all associated stations [1],[2].*

• *IEEE address of the AP with which the station is currently associated.*

iv Direction of message: From STA to STA (e.g., STA to AP or AP to STA)

3.2.6.5 Privacy

For a STA to invoke the WEP privacy algorithm, the privacy service causes MPDU encryption and sets the WEP frame header bit appropriately.

3.2.6.6 Authentication

For a STA to authenticate with another STA, the authentication service causes one or more authentication management frames to be exchanged. The exact sequence 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 IBSS environment, either station may be the initiating STA (STA 1). In an ESS environment, STA 1 is the mobile STA, and STA 2 is the AP.

Authentication (first frame of sequence)

i Message type: Management

ii Message subtype: Authentication

Estelar

iii Information items:

- *Authentication algorithm identification*
- *Station identity assertion*
- *Authentication transaction sequence number*
- *Authentication algorithm dependent information*

iv Direction of message: First frame in the transaction sequence is always from STA 1 to STA 2.

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

Authentication (intermediate sequence frames)

i Message type: Management

ii Message subtype: Authentication

iii Information items:

- *Authentication algorithm identification*
- *Authentication transaction sequence number*
- *Authentication algorithm dependent information*

iv 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)

i Message type: Management

ii Message subtype: Authentication

Estelar

iii Information items:

• *Authentication algorithm identification*

• *Authentication transaction sequence number*

• *Authentication algorithm dependent information*

• *The result of the requested authentication. This is an item with values "successful" and "unsuccessful."*

iv Direction of message: From STA 2 to STA 1

3.2.6.7 Deauthentication

For a STA to invalidate an active authentication, the following message is sent:

Deauthentication

i Message type: Management

ii Message subtype: Deauthentication

iii Information items:

• *IEEE address of the STA that is being deauthenticated*

• *IEEE address of the STA with which the STA is currently authenticated*

• *This shall be the broadcast address in the case of a STA deauthenticating all STAs currently authenticated.*

iv Direction of message: From STA to STA

Estelar

References:

[1] International Standard ISO/IEC 8802-11: 1999(E) ANSI/IEEE Std. 802.11, 1999 Edition

[2] An introduction to Ultra Wideband (UWB) wireless.htm: Rafael Kolic, Feb. 24, 2004

[3] Evaluation of the RC4 Algorithm for Data Encryption: Allam Mousa and Ahmad Hamad, International Journal of Computer Science and Applications, Vol 3, No. 2, June, 2006

[4] Network Security Fundamentals: Peter Nortan, Techmedia, SAMS Publications, II Edition, 2003

[5] Computer Networks: UYLESS BLACK, Prentice-Hall of IndiaPvt. Ltd., New Delhi, Ninth Edition, September, 2002

[6] Computer Networks: Andrew S. Tanenbaum, Pearson Education, IV Edition, 2003

[7] LAN Security Handbook: Ellen Dutton, BPB Publications, I Indian Edition, 1995

Estelar

[8] Introduction to Local Area Networks: Robert M. Thomas, Bpb publications, II Edition, 1998

[9] The ABC's of LANs: Michael Dortch, Bpb publications, I Edition, 1990

[10] Mastering Local Area Networks: Christa Anderson with Mark Minasi, I Indian Edition, 1991

[11] Towards an WLAN Infrastructure: Amit Jardosh, Gianluca Iannaccone, Dina Papagiannaki, and Bapi Vinnakota, UC Santa Barbara, Intel Research, Intel Corporation, pdf document accessed on 18th April, 2009

[12] Introduction to Wireless LANs: Wireless Local Area Network Association (1999) http://www.wlana.com

[13] Why the Future Is Bright for WLAN? Paul Dibeasi, Research Analyst at the Burton Group, talks to Motorola's Kevin Goulet, Cisco's Ben Gibson and Luc Roy at Siemens' Chantry Networks about why wireless is the way forward. February 05, 2009

Estelar

[14] Encapsulating WLAN standards 802.11b, 802.11a, 802.11g and 802.11n: A comparative study: Pant Durgesh and Lohani Manoj Chandra, Acta Ciencia Indica (Society for the Progress of Science), ACTA-140/M08/08-09

[15] Security Problems in Wireless Local Area Networks with the Suggested Possible Solutions: Pant Durgesh and Lohani Manoj Chandra, Acta Ciencia Indica (Society for the Progress of Science), ACTA-71/M08/08-09

Estelar