Overview of IEEE 802.11 Networks and Standards

Mauri Kangas, Helsinki University of Technology, 17.02.2004

Table Of Contents:

1. INTRODUCTION

Computer systems have been networked already for several decades, but just during the last few years wireless networking has spread into wide use especially in office environment. Furthermore, wireless networking is rapidly spreading also into home environment. There are a number of standards that are used for wireless connectivity: IEEE 802.11 WLAn, Bluetooth, and hiperLAN are the three most widely used wireless technologies. Each of them operates in a slightly different way and they ae used in different areas.

For computer peripheral interconnections, the IEEE 802.11 family of specifications is becoming widely used. The first versions of the IEEE 802.11 standard were developed to support roaming within an office environment or where wired connections are not convenient.

2. IEEE STANDARDS FAMILY

2.1 Overview

The IEEE 802 Local and Metropolitan Atrea Network Standards Committee is a major working group to create, maintain, and courage the use of IEEE and equivalent IEC/ISO standards. IEEE formed the committee already in 1980, and has met at least three times per year as a plenary body. IEEE 802 produces the series of standards known as IEEE 802.xx, and the Joint Technical Comiittee (JTC) 1 series of the equivalent standards are known as ISO 8802-xx.

IEEE 802 includes a family of standards, as depicted in Figure 1. The MAC and physical layers of the IEEE 802 standard were organized into a separate set of standards.

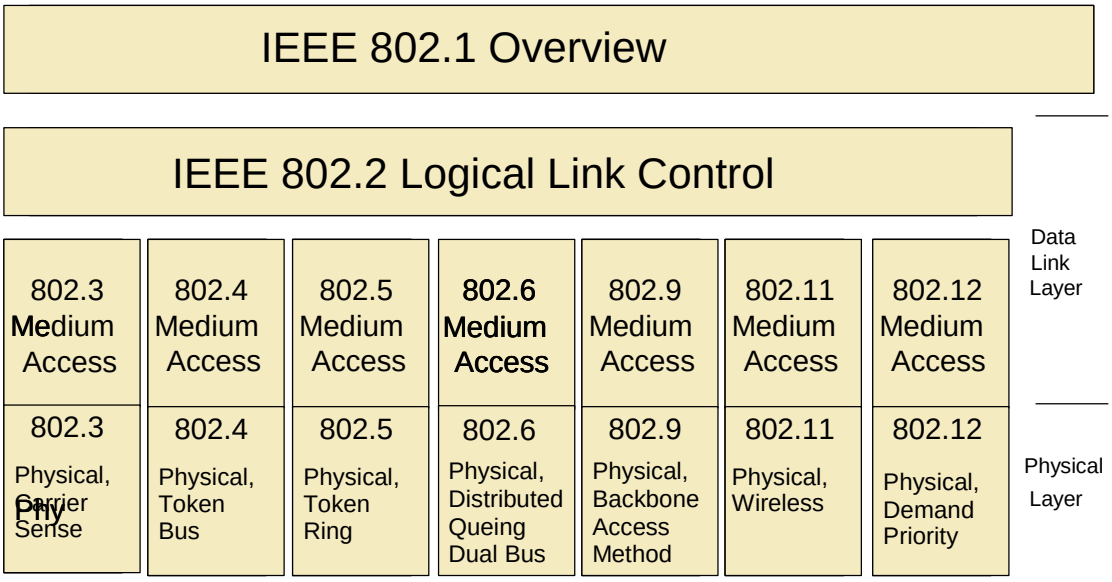


Figure 1. The IEEE 802 Family of standards

The wireless standard IEEE 802.11 has several variants, of which IEEE 802.11a, IEEE 802.11b and IEEE 802.11g are the most popular ones. For example, the performance of IEEE 802.11b standard is comparable with many wired systems, supporting data rates up to 11 Mbps. It uses direct sequence spread spectrum techniques with a total of 52 carrier centre frequencies. IEEE 802.11b uses the 2.4 GHz ISM (Industrial, Scientific and Medical) band allocation, such as Bluetooth.

The IEEE 802.11a specification is a higher performance specification using the 5 GHz ISM band, because it's assumed to be less congested. IEEE 802.11a specification can reach upt o 54 Mbps data rates, and it employs orthogonal frequency division multiplex (OFDM). It is not as popular as IEEE 802.11b, because the transition to the new technology might not be seamless due to different frequency band and transmission technology.

IEEE 802.11g wireless standard can achieve data rate of 54 Mbps with the help of the OFDM technology, and using 2.4 GHz ISM it is backward compatible with IEEE 802.11b, thereby enabling the new standard to work seamlessly with existing 802.11b PC cards.

2.2 IEEE 802.2 LLC Overview

The Logical Link Control (LLC) is the highest layer of the IEEE 802 reference model and it is specified in the IEEE 802.2 standard. The purpose of the LLC is to exchange data between end users across a LAN using a 802-based MAC controlled link. The LLC provides addressing and data link control , and it is independent of the topology, transmission medium, and chosen mediaum access control technology.

Higher layers, such as TCP/IP, pass user data down to the LLC layer expecting error-free transmission across the network. The LLC appends a control header, creating An LLC protocol data unit (PDU). The LLC utilizes control information in the LLC protocol operation (see Figure 2) …

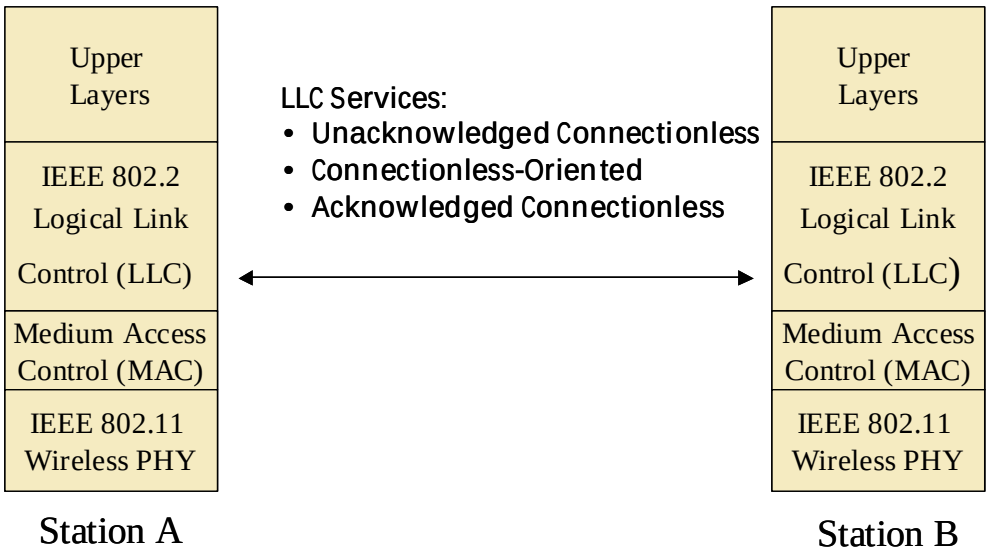


Figure 2. The LLC provides end-to-end link control over an 802.11-based wireless LAN.

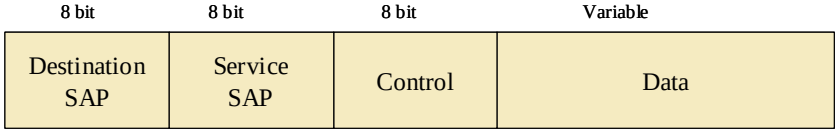
2.3 IEEE 802.2 LLC Services

The LLC provides the following three services for a Network Layer protocols:

- Unacknowledged connectionless service
- Connection-oriented service
- Acknowledged connectionless ervice

These three services are operational as a peer-to-peer communication service between the LLC layers of the source and target stations.

All these three LLC protocols employ the same PDU format that consists of four fields as shown in Figure 3.



Control field indicates the type of the frame:

- *Information*: used to carry user data
- *Supervisory*: used for flow control and error control
- *Unnumbered*: various protocol control PDUs

Figure 3. The LLC PDU Structure

The Destination Service Access Point (DSAP) and Source Service access Point (SSAP)field each contain 7-bit addresses that specify the destination and source stations of the peer LLCs.

2.3.1 Unacknowledged Connectionless Service

The *unacknowledged connectionless service* is a datagram-tyle service that doesn't involve any error-control or flow-control mechanisms. This service doesn't involve the establishment of a Data Link Layer connection between peer-LLCs. This service supports indiidual, multicast and broadcast addressing. This service just sends and receives LLC P>Dus, with no aknowledgement of delivery so that higher layers must take care of reliability issues.

2.3.2 Connection-Oriented Service

The *connection-oriented service* establishes a logical connection that provides flow and error control between communicayting stations. In this service type connection between peer LLCs must be established. Connection can be made only between two stations and thus multicats and broadcast modes are not supported. The connection-oriented service I

sadvantageous if higher layers of the protocol stack do not provide the necessary reliability and flow-control mechanisms, which is generally the case with terminal controllers.

The connection-oriented and acknowledged-connectionless LLCs use error-control mechanisms that detect and correct transmission errors. The LLC Automatic Repeat-Request (ARQ) mechanism recognizes the possibility of the following two types of errors:

- *Lost PDU:* A PDU faisl to arrive at the other end or is damaged beyong recognition
- *Damaged PDU:* A P>DU has arrived, but some bits are altered.

In the ARQ mode the receiving station will answer with a positive or negative aknowledgent depending on the outcome of the error detection process. In the case of lost aknowledgement the sending station will retransmit the frame after a certain period of time. There are two approaches for the retransmission scheme, which are explained in the following subparagraphs.

Continuous ARQ

Continuous ARQ, which is often called *sliding window nprotocol*, the sending station transmits frames continuously until the receiving station detects an error. When negative acknowledgement is received, the transmitting station could use the *go-back-n technique*, in which the transmitter stations searches the erroneous frame from its transmitter buffer and it will send that one and all the following frames once again. This is not very efficient retransmission scheme, but the receiver doesn't need to have reordering capability for the received frames. More effective is the *selective repeat*, where the transmitting station retransmits only the erred frame, but th ereceiver must be capable of reordering the received frames.

Stop-and-Wait ARQ

In the stop-and-wait ARQ mode the tramnsmitter will send the next frame only after it receives a positive aknowledgement from the receiver. Stop-and-wait ARQ doesn't require large buffer space, but wpropagation delay between source and destination becomes large.

2.3.3 Aknowledged Conectionless Service

The *acknowledged connectionless service* doesn't establish logical connection with the target station, but all the datagram delivery uses aknowledgement mechanism. Flow and error control is handled thorugh us of the stop-and-wait ARQ method. The acknowledged connectionless sservice is useful in application requiring communication a number of receivers, but the messages are very short in nature. In this case connection-oriented service would require upkeeping of a number of tables and handling very complicated retransmission and acknowledgement scheme between numerous receivers, and that would be impractical in straightforward applications.

2.4 LLC/MAC Layer Service Primitives

Layers within the 802 architecture communicate with each other via service primitives having the following forms:

- *Request*: A layer uses this type of primitive to request that another layer perform a specific service.

- *Confirm*: A layer uses this type of primitive to convey the results of a previous service request primitive.

- *Indication*: A layer uses this type of primitive to indicate to anbother layer that a significant event has occurred. This primitive could result from a service request or from some internally generated event.

- *Response*: A layer uses this type of primitive to complete a procedure initiated by an indication primitive.

3. INTRODUCTION TO IEEE 802.11 STANDARD

The IEEE 802.11 standard provides MAC and PHY functionality for wireless connectivity of fixed, portable, and moving stations moving at pedestrian and vehicular speeds within a local area. The standard IEEE 802.11 includes the following:

- Describes the functions, services and mobility aspects required by an IEEE 802.11 device to operate within ad hoc and infrastructure networks.

- Defines the MAC procedures to support the asynchronous MAC service data unit (MSDU) delivery services.

- Defines several PHY signaling techniques and interface functions that are controlled by th eIEEE 802.11 MAC.

- Permits the operation of an IEEE 802.11 conformant device within a wireless local area network (LAN) that may coexist with multiple overlapping IEEE 802.11 wireless LANs.

- Describes the requirements and procedures to provide privacy of user information being transferred over the wireless medium (WM) and authentication of IEEE 802.11 conformant devices.

The IEEE 802.11 standard takes into account the following significant differencies between wireless and wired LANs:

- *Power management*: portable devices should have low power consumption, and that's why 802.11 Working Goup has found a technique to enable wireless 802.11 devices to switch to lower-power standby modes periodically when not transmitting. Because sleeping stations can miss critical data transmissions, but 802.11 solves the problem by incorporating buffers to queue messages.

- *Bandwidth*: The ISM spread spectrum bands do not offer a great deal of bandwidth, keeping data rates lower than desired for some applications. The 802.11 Working Group has dealt with methods to compress data, making the best use fo the bandwidth. Efforts are also underway to increase 802.11 data rate to accommodate the growing need for exchanging larger and larger files.

- *Security:* The 802.11 Working Group has coordinated their work with the 802.10 Standards Committee responsible for developing security mechanisms for all 802 series LANs.

- *Addressing*: Destination address doesn't correspond to the destinations location, because wireless network topology is dynamic. This raises a problem, when routing packets through the network to the intended destination. Therefore, there may become a need to utilize a TCP/IP-based protocol, such as MobileIP, to accommodate mobile stations.

4. IEEE 802.11 ARCHITECTURE

4.1 Overview

Wireless network have fundamental characteristics that make them significantly different from traditional wired LANs. IEEE 802.11 is required to appear to higher layers, actually to the Logical Link Control (LLC) layer, as a current style IEEE 802 LAN. This requirement assumes that the mobility issues are handled within the MAC sub-layer.

The following physical layer specific features in the wireless IEEE 802.11 standard compared to the respective wired media:

1. Used media doesn't have absolute or observable boundaries ouside of which conformant stations are unable to receive network frames.

2. Are unprotected from outside signals.

3. Communicate over a medium, which is significantly less reliable than wired PHYs.

4. Have dynamic topologies.

5. Lack full connectivity, and therefore the assumption normally made that every station (STA) can hear every other station is invalid.

6. Have time-varying and asymmetric propagation properties.

One of the requirements of 802.11 is to handle *portable* as well as *mobile* stations. Station is said to be portable when it potentially is moved from one location to another, while mobile stations can access the LAN while in motion.

4.2 Components of the IEEE 802.11 Architecture

The IEEE 802.11 topology consists of components, interacting to provide a wireless LAN that enables station mobility transparent to higher protocol layers, such as the LLC. The 802.11 supports two topologies:

- Independent Basic Service Set (IBSS) networks

- Extended Service Set (ESS) networks

These networks utilize a basic building block the 802.11 refers to a Basic Service Set (BSS), providing a coverage area whereby stations of the BSS remain fully connected. A

station is free to move within the BSS, but it can no longer communicate directly with other stations if it leaves BSS.

4.3 Independent Basic Service Set (IBSS) Networks

An IBSS is a stand-alone BSS, or more precisely a BSS without Access Point (AP), having no backbone infrastructure and consists of at least two wireless stations (see Figure 4). This kind of a network is often referred to as an *ad hoc network* because it can be constructed quickly without much planning.

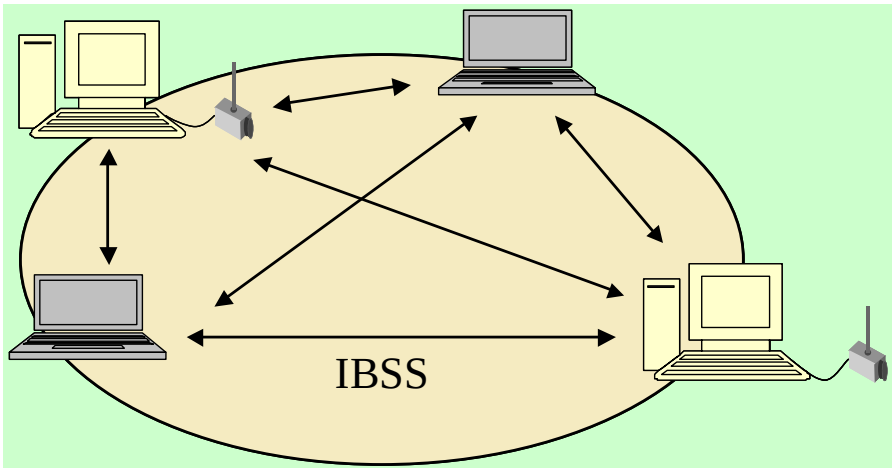


Figure 4. Independent Basic Service Set (IBSS)

4.4 Infrastructure BSS Networks

All mobile stations must be accessible by the access point in the infrastructure BSS, but no restrictions are palced on the distance between stations. The infrastructure BSS is illustrated in IFigure 5. All the traffic must flow through the access point, there are no direct links between stations in this scenario. Of course, there can be scenarios, where the same stations may belong to an infrastructure BSS and ad-hoc network.

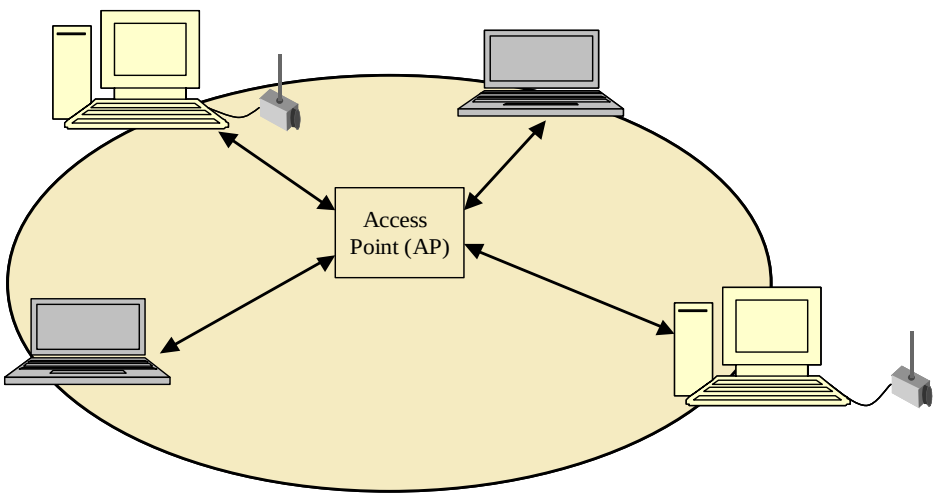


Figure 5. Infrastructure BSS

4.5 Extended Service Set (ESS)

For requirements exceeding the range limitations of an independent BSS, IEEE 802.11 defines an Extended Service Set (ESS) LAN, as illustrated in Figure 6. Physical link limitations determine the direct station-to-station distance and that may be supported. 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). An access point (AP) is a station (STA) that provides access to the DS by providing DS services in addition to acting as a STA. Addresses used by an AP on the WM and on the DSM are not necessarily the same.

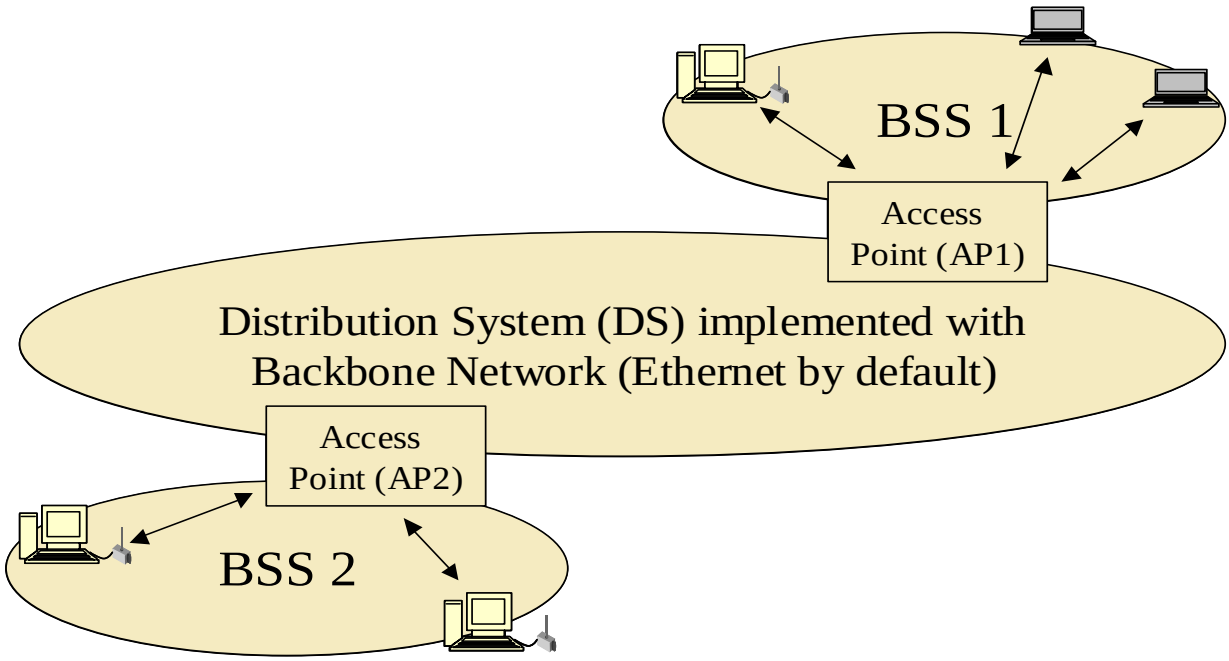


Figure 6. An Extended service Set (ESS) 802.11 Wireless LAN

In order to integrate the IEEE 802.11 architecture with a traditional wired LAN, a final *logical* architectureal component is introduced - a *portal*. A portal is the logical point in which MSDUs from the integrated non-IEEE 802.11 LAN enter the IEEE 802.11 DS. The complete IEEE 802.11 architetcure is illustrated in Figure 7.

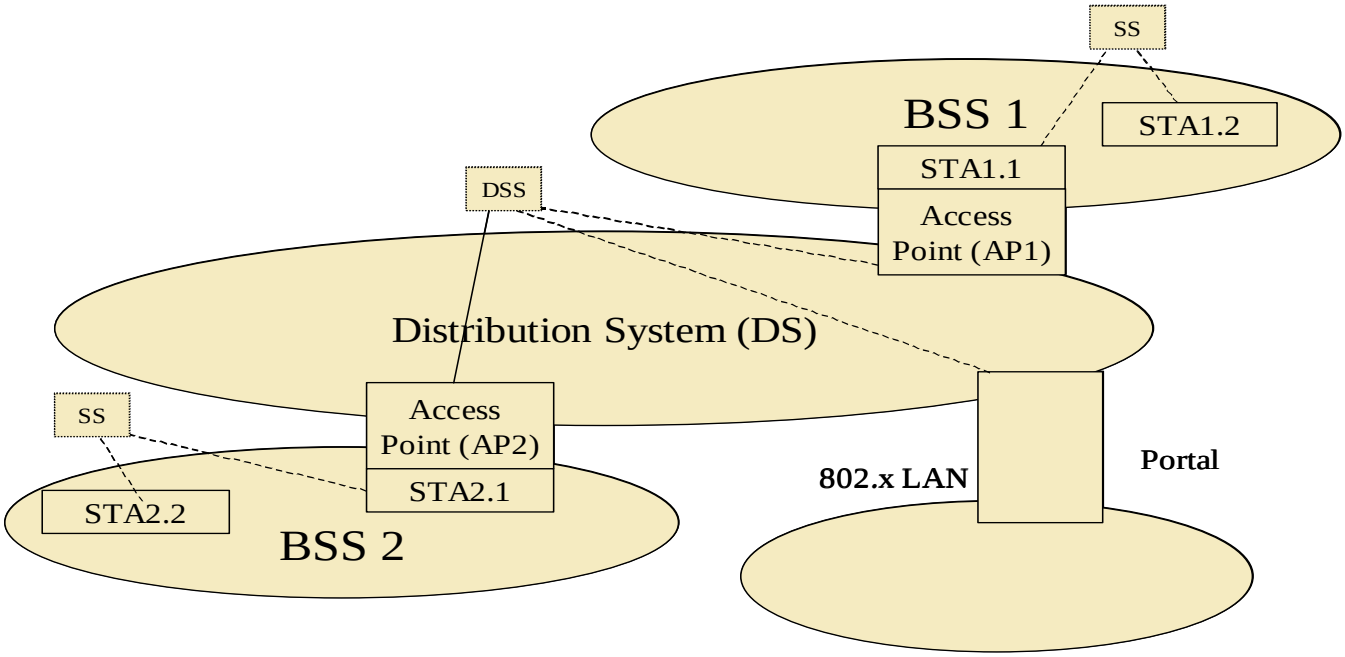


Figure 7. Complete IEEE 802.11 Architecture

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 either as the station service (SS) or the distribution system service (DSS). Both categories of service are used by the IEEE 802.11 MAC sublayer.

Station Service

Station service (SS) class contains the following services:

- Authentication
- Deauthentication
- Privacy
- MSDU delivery

Authentication service is used to ensure that only authenticated user can access the network.

Deauthentication service is used to deauthenticate user, when (s)he wants to leave the network. Deauthentication also terminates any current association.

Privacy in IEEE 802.11 is implemented by using Wired Equivalent Privace (WEP). The original target of the WEP security has been that the encrypted air interface in IEEE 802.11 would have the same security level as the wired network.

MSDU delivery service is responsible for getting the data to the actual endpoint.

Distribution System Service

Distribution system service (DSS) class contains the following servcies:

- Association
- Diassociation
- Distribution
- Integration
- Reassociation

Association service enables the stations to register, or associate, with access points.

Disassociation service is the complementary service for association. It is used to terminate an existing association.

Distribution service is used by the access points to deliver data to its destination. Communication between stations within some access point's area will not go through the distribution system.

Integration service allows connectivity between IEEE 802.11 distribuiton system and non-IEEE 802.11 network.

R-eassociation service is needed, when a mobile station is moving within an ESS area from one access point's area to another access point's area. Mobile stations initiate re-associations, when signal conditions indicate that a different association would be beneficial.

5. MOBILITY SUPPORT

IEEE 802.11 wireless networking has been deployed because of mobility reasons. IEEE 802.11 can move aroud and transmit frames while in motion, when they connected to the network. Mobility can cause three types of transition:

- No transition
- BSS transition
- ESS transition

5.1 No transition

When stations do not move outside from their current access point's service area, no transition is necessary. Thia state occurs because the station is moving within th ebasic service area of its current access point.

5.2 BSS Transition

IEEE 802.11 provides MAC layer mobility within an ESS. Distribution system need not to know the exact location within the same extended service area (i.e., within what BBS area the station is located).

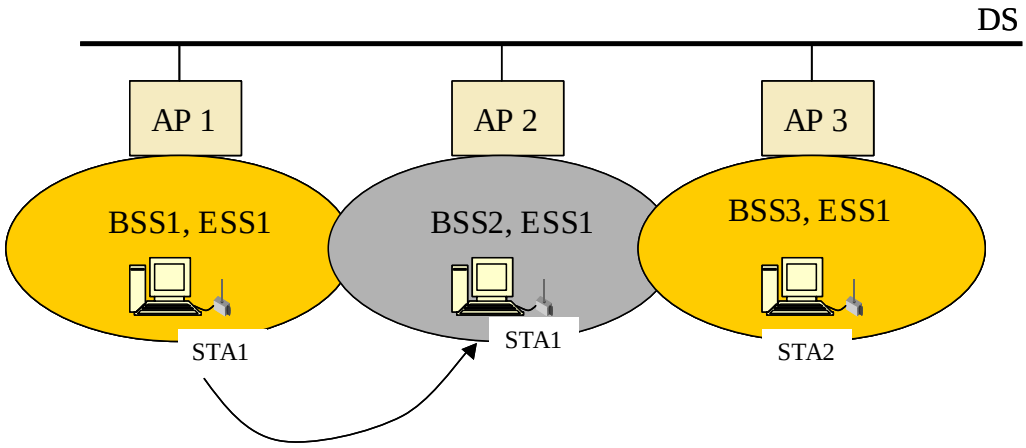


Figure 8. Station STA1 carrying out a BSS transition

In Figure 8 is illustrated a situation, where station (STA1) is moving from one basic service set (BSS1) area BSS1 to another basic service set (BSS2) area.

5.3 ESS Transition

An ESS transition ocuurs, when a staion is moving from one ESS to a second distinct ESS. IEEE 802.11 doesn't support this type of transition, except to allow the station to associate with an access point in th esecond ESS once it leaves the first one.

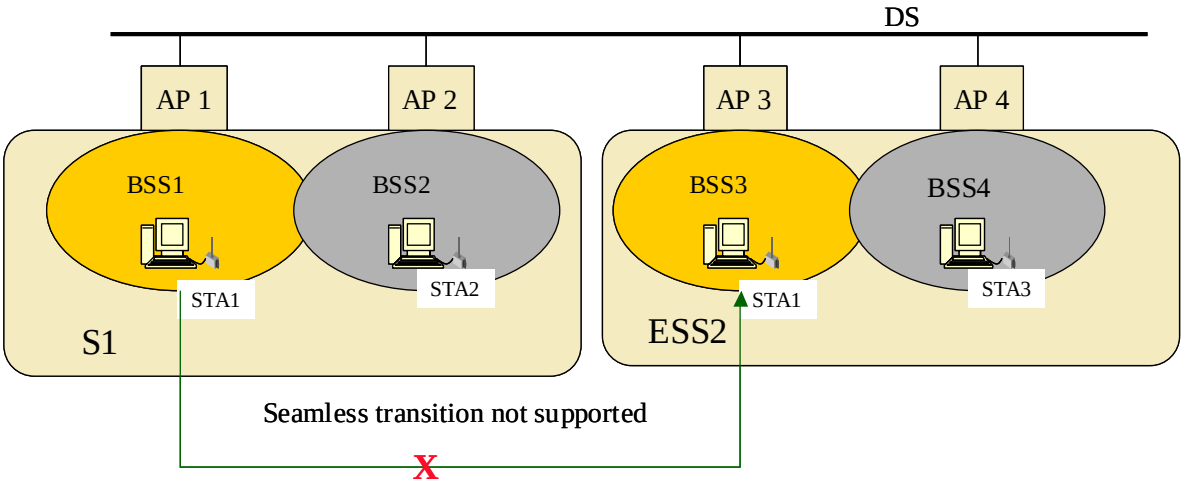


Figure 9. ESS transition illustrated

In Figure 9 is depicted an ESS transition, where station STA1 is moving from the extended service set (ESS1) area to another extended service set (ESS2) area. Seamless transition cannot be carried out.

6. MODULATION SCHEME AND DATA STRUCTURE

IEEE 802.11. contains three different physical layer implementations: frequency hopping spread spectrum (FHSS), direct sequence spread spectrum (DSSS), and IR. The FHSS system contains in U.S. a maximum of 79 channels starting from 2.4020 GHz center frequency (frequency range: 2.4000-2.4835 GHz). The channel spacing requirement is U.S. is 1 MHz with 1 Mbps data rate. There are three hopping sets with 26 hopping sequences in each set. Different hopping sets enable multiple BSSs to coexist in the same geographical are. The basic access rate of 1 Mbps uses two-level Gaussian frequency shift keying (GFSK). And the enhanced access rate of 2 Mbps uses four-level GFSK.

IEEE 802.11b uses a technique known as direct sequence spread spectrum (DSSS). It spreads the signal out over a wide bandwidth and as a result it enables the system to operate in an environment where there are other users and levels of interference may be high. A variety of modulation types can be used and they are chosen dependent upon the rate at which data is to be transmitted. Systems running at 1 Mbps use BPSK (Binary Phase Shift Keying) modulation, and those running at 2 Mbps QPSK (Quaternary Phase Shift Keying) modulation. The spreading is done by dividing the available bandwidth into 11 sub-channels. Overlapping and adjacent BSSs can be accommodated by ensuring that the center frequencies of each BSS are separated by at least 30 MHz. This rigid requirement requirement will enable only two overlapping or adjacent BSSs to operate without interference.

For higher data rates, systems running at 5.5 Mbps and 11 Mbps use CCK (Complementary Code Keying) and QPSK modulation. CCK involves 64 unique code sequences, each of which supports 6 bits per code word. The CCK code word is then modulated onto the RF carrier using QPSK, and this allows another two bits to be encoded for each 6-bit symbol resulting into a 8 bits.

The wavelength in the IR specification is between 850 and 950 nm. The basic rate of 1 Mbps is performed using 16-pulse position modulation (PPM), where 4 data bits are encoded into 16 coded bits, and the enhanced access rate of 2 Mbps is performed by using 4-PPM modulation, where 2 data bits are mapped to 4 coded bits for transmission.

7. PROTOCOLS

When a station wants tocommunicate with other stations in a cell, it must first synchronize with them. This may happen in two ways. The first method is called passive scanning. The station waits to reveive what a beacon frame from the access point or another station in an ad-hoc network. This frame is a periodic frame of data that is sent out with syncronisation information on it. This enables new stations to synchronise, and also ensures existing stations maintain their synchonisation.

The alternative method is for the station entering a network to send out a ‘probe’ transmission and then wait for a response.

Once the new station has the synchronization information it can then request access to the cell. It does this by going through an authentication process. Only when this has been completed can the station enter the cell and exhange data. The process includes exchanging passwords to ensure that the new station should be in the cell.

8. MEDIUM ACCESS CONTROL (MAC) SUBLAYER

8.1 General

The MAC sublayer is responsible for the channel allocation procedures, protocol data unit (PDU) addressing, frame formatting, error checking, and fragmentation and reassembly. There are two operation modes in the wireless communication: 1) the transmission media operates in fully contention mode, 2) operation mode can alternate between contention and contention-free modes.

When the transmission medium operates in the contention mode exclusively, all stations need to contend for access for each transmitted packet.

When the transmission medium can also alternate between the contention mode, known as the *contention period* (CP), and a *contention-free period* (CFP). During the CFP period access point (AP) is controlling the media usage, and stations do not need to contend for channel access.

IEEE 802.11 MAC frame is illustrated in Figure 10.

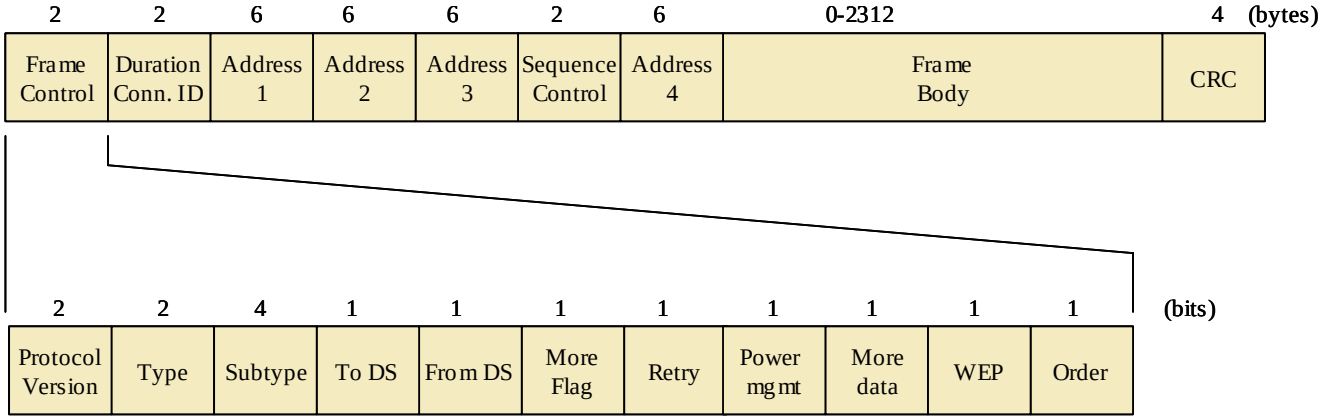


Figure 10. MAC Frame Format

The address in the MAC frame structure can be BSS-ID, Destination Address (DA), Source Address (SA), Receiver Address (RA) or Transmitter Address (TA). Each of the address fields contain a 48-bit MAC address. MAC sublayer address is either individual address or group address (multicast group address or broadcast address)

The two duration bytes indicate the time (in microseconds) the channel will be allocated for successful transmission of a MAC protocol data unit (MPDU)

8.2 Distributed Coordination Function (DCF)

8.2.1 General

The DCF is the fundamental access method to support asynchronous data transfer on a best effort basis. All stations must support this fully contention-based access method. The

DCF operates solely in ad-hoc network, and either operates solely or coexist with the PCF in a infrastructure network.

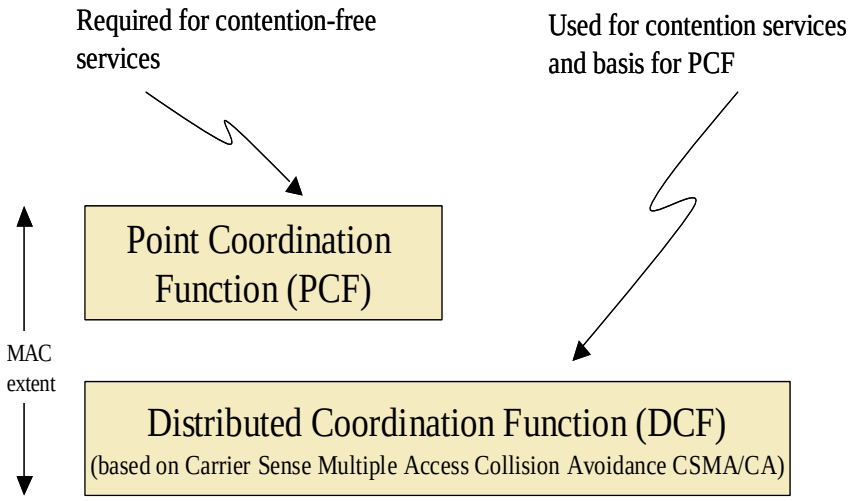


Figure 11. MAC Architecture

The MAC architecture is depicted in Figure 11.

8.2.2 Collision Avoidance

Collision in wireless networks happen, whne two station transmit at the same time. This situation is handled by the Colision Sense Mulitple Access with Collision Avoidance (CSMA/CA) in the Media Access Controller (MAC) of the software protocol stack. This is very similar to the Collision Sense Multiple Access Collision Detection (CSMA/CD), which is used IN IEEE 802.3 for Ethernet. A different system is required for wireless system, because on a wired network all will be able to hear each other, whereas on a wireless networks it's possible that one station may not be able to hear all the others. When a station wants to transmit, it first checks the frequency to ensure no other stations are transmitting. If the channel is occupied the station delays sending its message fro a random amount of time.

The first message that is sent is so called Request-To-Send (RTS) message defining also the length of the actual message to be sent. After a Interframe Space (IFS) time the receiver will transmit a Clear-To-Send (CTS) message back. After receiving this message the transmitter will send the actual data message (MPDU). This method is called *virtual carrier sensing*, but the MPDU transmission can be carried out withot this method also. In this scenario all stations in the BSS listen to the channel and they are aware, how long time does the transmission in question take.

8.3 Point Coordination Function (PCF)

The PCF is an optional capability, which is connection-oriented, and provides contention-free (CF) frame transfer. The PCF relies on the point coordinator (PC) to perform polling, enabling polled stations to transmit without contending for the channel.

The PCF is required to coexist with the DCF and logically sits on top of the DCF (see Figure 11).

9. IEEE 802.11 FAMILY OF SPECIFICATIONS

9.1 IEEE 802.11a WLAN Specification

IEEE 802.11a specifies a physical layer for an orthogonal frequency division multiplexing (OFDM) system. The radio frequency LAN system is initially aimed for the 5.15–5.25, 5.25–5.35 and 5.725–5.825 GHz unlicensed national bands.

The OFDM system provides a wireless LAN with data payload communication capabilities of 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s. The support of transmitting and receiving at data rates of 6, 12, and 24 Mbit/s is mandatory. The system uses 52 subcarriers that are modulated using binary or quadrature phase shift keying (BPSK/QPSK), 16-quadrature amplitude modulation (QAM), or 64-QAM. Forward error correction coding (convolutional coding) is used with a coding rate of 1/2, 2/3, or 3/4.

9.2 IEEE 802.11b WLAN Specification

IEEE 802.11b is based on the original standard text for IEEE 802.11, which defines max. 2 Mbps data rates. IEEE 802.11b adds higher data rate specification for up to 11 Mbps data rates. Also two different modulation code types: CCK = complementary code keying, and PBCC = packet binary convolutional coding. The IEEE 802.11b is currently the most widespread and popular WLAN standard in use (2004).

9.3 IEEE 802.11d WLAN Specification

This amendment specifies the extensions to IEEE Std 802.11 or Wireless Local Area Networks providing specifications for conformant operation beyond the original six regulatory domains of that standard. These extensions provide a mechanism for an IEEE Std 802.11 access point to deliver the required radio transmitter parameters to an IEEE Std 802.11 mobile station, which allows that station to configure its radio to operate within the applicable regulations of a geographic or political subdivision. This mechanism is applicable to all IEEE Std 802.11 PHY types. A secondary benefit of the mechanism described in this amendment is the ability for an IEEE Std 802.11 moble station to roam between regulatory domains.

More detailed list of the modification, which have been added to the IEEE 802.11d specification.

- Beacon Frame Body, Probe Message Body
    - Structures specified to contain: Country information and Frequency Hopping (FH) information
    - Contents of the Country Information Elements (CIE)
- MAC sub-layer specification:
    - Operation upon entering a regulatory domain
    - Suport for frequency hopping PHYs

- Determining hopping patterns

- MAC sub-layer management
  - Initializing a BSS and synchronizing with a BSS

- Frequency Hopping Spread Spectrum (small editorial)
  - Frequency hopping pattern may be received as the frequency hopping table information from beacon or Probe Response frame

9.4 IEEE 802.11f WLAN Specification

Recommended practices for implementation of an Inter-Access Point Protocol (IAPP)on a Distribution System (DS) supporting ISO/IEC 8802-11:1999 and IEEE 802.11™ wireless local access network (WLAN) links are described. The recommended DS utilizes an IAPP that provides the necessary capabilities to achieve multi-vendor Access Point (AP) interoperability within the DS. This IAPP is described for a DS consisting of IEEE 802 LAN components utilizing an Internet Engineering Task Force (IETF) Internet Protocol (IP) environment. Throughout this recommended practice, the terms ISO/IEC 8802-11:1999, IEEE 802.11, 802.11™, and IEEE Std 802.11™-1999 are used interchangeably to refer to the same document, ISO/IEC 8802-11:1999, and its amendments and supplements published at the time this recommended practice was adopted.

This recommended practice describes a service access point (SAP), service primitives, a set of functions and a protocol that will allow APs to interoperate on a common DS, using the Transmission Control Protocol over IP (TCP/IP) or User Datagram Protocol over IP (UDP/IP) to carry IAPP packets between APs, as well as describing the use of the Remote Authentication Dial-in User Service (RADIUS) Protocol, so APs may obtain information about one another. A proactive caching mechanism is also described that provides faster roaming times by sending STA context to neighboring APs. The devices in a network that might use the IAPP are 802.11 APs. Other devices in a network that are affected by the operation of the IAPP are layer 2 networking devices, such as bridges and switches.

Throughout the 80.11F recommended practice, reference is made to an “AP management entity (APME).” These are references to a function that is external to the IAPP, though likely still a function of the AP device.

Typically, this management entity is the main operational program of the AP, implementing an AP manufacturer’s proprietary features and algorithms, and incorporating the station management entity (SME) of 802.11. Figure 12 depicts an architecture of a typical AP in which the IAPP operates. The grey areas indicate areas where there is an absence of connection between blocks. The IAPP services are accessed by the APME through the IAPP SAP. The IAPP SAP is shown in Figure 12, as the small block between the APME and the IAPP blocks. IAPP service primitives are de.ned that allow the AP management entity to cause the IAPP to perform some function or to communicate with other APs in the DS or with a RADIUS server. Other service primitives indicate to the AP management entity that operations have taken place at other APs in the DS that can have an effect on information local to the AP.

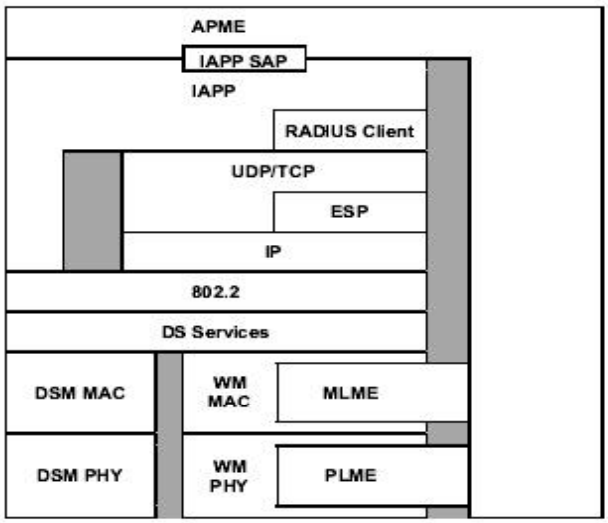


Figure 12. AP Architecture with IAPP.

9.5 IEEE 802.11i WLAN Specification

Anyone developing wireless LAN (WLAN) systems knows the security problem created by the wired equivalency protocol (WEP). The bigger issue designers must wrestle with is how to solve the problems caused by WEP.

Fortunately, the IEEE 802.11 committee is helping out. Through the work in its "i" working group, the 802.11 committee is producing a detailed specification that will dramatically enhance the security features provided in a WLAN system.

After more than two years of work, the 802.11i committee is coming closer to having a unified spec in the market. The 802.11i specification can be viewed as consisting of three main pieces organized into two layers. On the lower level are improved encryption algorithms in the form of the temporal key integrity protocol (TKIP) and the counter mode with CBC-MAC protocol (CCMP). Both of these encryption protocols provide enhanced data integrity over WEP, with TKIP being targeted at legacy equipment and CCMP being targeted at future WLAN equipment.

Above TKIP and CCMP sits 802.1x, a standard for port based access control developed by a different body within the IEEE 802 organization. As used in 802.11i, 802.1x provides a framework for robust user authentication and encryption key distribution, both features originally missing from the original 802.11 standard.

When looking at 802.11i, it's important to understand that the three pieces discussed above work together to form an overall security system. But to understand how each of

these pieces fit together, we must first understand how they operate individually. So, let's take a look at each piece in more detail, starting with 802.1x.

10. REFERENCES

[1] Brian B. Crow, Indra Widjaja, Jeong Geun, Prescott T. Sakai, “IEEE 802.11 Wireless Local Area Networks”, IEEE Communications Magazine, September 1997, pp. 116-126

[2] Ian Poole, “Fundamentals of 802.11”, Electronics World, August 2003, pp. 12-14

[3] Matthew S. Gast, “802.11 Wireless Networks, The Definitive Guide”, O’Reilly, April 2002, 444 pages.

[4] Jim Geier, “Wireless LANs, Implementing High Performance IEEE 802.11 Networks”, 2nd edition, 2002, Sams Publishing, 345 pages

[5] IEEE Std. 802.11, “Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specifications”, ISO/IEC, 1999 edition

[6] IEEE Std. 802.11b-1999/Cor 1-2001, “Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specifications, Amendment 2: Higher-speed Physical Layer (PHY) extension in the 2.4 GHz band, IEEE, 1999 edition

[7] IEEE Std. 802.11d-2001Amendment, “Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specifications, Amendment 3: Specification for operation in additional regulatory domains, IEEE, 2001 edition