Bridging the Gap Between Concepts and Reality: 802.11 Standard Uncovered

A. Verhoeven akverhoe@mtu.edu

Abstract

The ability to communicate within any destination, at any given moment both effectively and efficiently tends to define our success (existence) within not only the world of technology but also the world’s social and economical standpoint. The 802.11 standard had helped emerge the Wireless Local Area Network (WLAN) industry as one of the fastest-growing segments of the communications industry. WLAN equipment shipments grew to almost 12 million units in 2001 and the market research firm, Cahners In-Stat expect sales of wireless network cards and WLAN base stations to grow from $1.9 billion in 2001 to $5.2 billion in 2005. Using a wireless protocol, allows for tremendous world advancements in the realm of communications. Third world countries are able to afford communication networks and participate in the future advancements and technology breakthroughs for the first time since their initial existence. Countries around the world are able to use the 802.11 standard to communicate with the world while at the same time decrease the country’s financial costs by excluding the hard wire communication lines and capitalize on the standard’s flexibility and functionality revolving around the concept of cellular architecture. The 802.11 standard has been redefined several times in order to accommodate technological advancement needs. Within the next few years, the standard’s success will be based off interoperability between WLAN products between different equipment manufacturers. In addition, new industries such as education, healthcare, manufacturing and warehouse, production, retail and financial will begin to integrate the 802.11 standard to increase their overall efficiency and decrease their financial overhead.
I Introduction

In 1989 the Federal Communications Committee (FCC) approved and allocated frequency spectrums for commercial use such as the 900 MHz, 2.4GHz, and 5GHz. In 1990, the Institute of Electrical and Electronic Engineers (IEEE) began developing what would eventually be approved as the 802.11 Standard in 1997 [1]. The IEEE is a non-profit, technical professional association of more than 377,000 individual members in 150 countries [13]. The full name is the Institute of Electrical and Electronics Engineers, Inc. Through its members, the IEEE is a leading authority in technical areas ranging from computer engineering, biomedical technology and telecommunications, to electric power, aerospace and consumer electronics, among others [13]. IEEE’s mission is to promote the engineering process of creating, developing, integrating, sharing, and applying knowledge about electro and information technologies and sciences for the benefit of humanity and the profession [13]. The 802.11 Standard was established to create compatibly standards for the newly emerging local area network (LAN) technology [2]. 802.11 was first published in 1997 and initially contained three variants. The first specified an infrared technology that was never really adopted in a meaningful way. The other two used different implementations of spread spectrum radio technology operating in the 2.400 - 2.483 GHz unlicensed spectrum.

Some concepts which are important to obtain a clear understanding about the 802.11 are discussed in the following paragraph. The 802.11 Local Area Network (LAN) is designed around the same architecture as cellular. The entire system is subdivided into individual areas labeled as cells. According to the IEEE nomenclature, each cell is referred to as a Base Service
Station (BSS). The BSS is controlled by a Base Station also referred to as an Access point (AP). The 802.11 Standard allows for a minimum of one cell along with or without a single AP to create a wireless LAN. Typically most applications will be formed using several Access Point and cells. The backbone of the system, where the Access Points are connected is known as the Distribution System (DS) [3]. The most common example of a DS is the Ethernet, including wireless Ethernet connections. The whole interconnected wireless LAN, including the different cells, their respective Access Points and Distribution Systems, is seen in the upper layers of the OSI model as a single network. This single network is known as the Extended Service Set (ESS) [3]. 802.11 addresses two separate layers of the wireless spectrum. The Media Access layer, or MAC, is mostly made up of software-based protocols that enable devices to talk to each other. The other is the Physical layer, or PHY, which defines the physical characteristics of the radio signal such as the frequency, power levels, and type of modulation. The Physical layer is divided into three separate layers, Infra-Red layer, Direct Sequence layer and the Frequency Hoping layer. The MAC layer’s primary goal is to manage and maintain communication between 802.11 stations (radio network cards and access points) by coordinating access to a shared radio channel and utilizing protocols that enhance communication over a wireless medium [7]. The MAC layer is often viewed as the “brains” of the entire network. Before transmitting frames, a station must first gain access to the medium, which is the radio channel that stations share. The 802.11 standard defines two forms of medium access, Distributed Coordination Function (DCF) and Point Coordination Function (PCF). DCF is mandatory and based on the Carrier Sense Multiple Access with Collision Avoidance protocol (CSMA/CA) [7]. CSMA is a contention-based protocol making certain that all stations first sense the medium before transmitting. The main goal is to avoid having stations transmit at the same time, which results in collisions and
corresponding re-transmissions [7]. A collision occurs when two or more devices attempt to send a signal along the same channel at the same time. The result of a collision is generally a garbled message. All computer networks require some sort of mechanism to either prevent collisions altogether or to recover from collisions when they do occur. The coordination to accessing the medium is carried out by the MAC layer checking the value of its Network Allocation Vector (NAV), which is a counter resident at each station which represents the amount of time that the previous frame needs to send its frame [7]. The NAV must equal zero before the station attempts to send a frame. The Point Coordination Function (PCF) supports the time-bounded delivery of data frames. The Access Point (AP) grants access to an individual station to the medium by polling the station during the contention free period [7]. The station is unable to transmit frames unless the AP polls them first. The Infra Red physical layer deals primarily with Radio Frequency (RF) technology. RF is defined as any frequency within the electromagnetic spectrum associated with radio wave propagation. The other two layers are two types of spread spectrum technology, frequency hopping (FH) and direct sequence (DS). Both involve spreading a radio signal to improve performance, but FH and DS are not compatible and each has its own industry proponents to t-out its. The Frequency Hoping layer (FH) deals primarily with the Frequency Hopping Spread Spectrum (FHSS) technique. FHSSS allows the data to be split up across the time domain. The Direct Sequence layer uses a Direst Sequence Spread Spectrum (DSSS) technique. DSSS allows the data to be chopped up into small pieces and spread across the frequency domain. The DSSS physical layer uses an 11-bit Barker Sequence to spread the data before it is transmitted. In essence, when a bite is transmitted it is then modulated by the 11- bit sequence. The modulation of the 11-bit sequence is achieved by
spreading the Radio Frequency (RF) energy across a wider bandwidth than required to transmit
the raw data [5]. Various frame types are used by stations, such as the radio Network Interface
Card (NIC) and the AP, for not only communication but also managing and controlling the
wireless link.[6] The radio Each frame contains a control field that depict the 802.11 protocol
version frame type. The control field also contains various indicators such as whether the WEP
is on, power management is active, and other additional add on functions discussed previously.
All frames also contain MAC addresses of the source and destination station known as the AP, a
frame sequence number, frame body, and frame check sequence [6]. Task groups were formed
by the IEEE 802.11 WG (working group) to make revisions [9]. Each task group refers to a
different version of the original 802.11. The following are a list of current task groups for
example the task groups range from the letter A to the letter I, (802.11a, 802.11b 802.11c ect).
The letter represents the different task groups [12].

Section two will discuss the two different architectures used in the 802.11 standard, Ad-
Hoc and Infrastructure. Section three will discuss the different types of frames used to
communicate by the 802.11 standard. Section four will elaborate on the 802.11 MAC layer and
the Physical Layers, Infra-Red, FH and DS. Section five will describe how a station joins
another station. Section six will discuss the different generations and revisions of the initial
802.11 standard. Section seven will comment on where the 802.11 standard is headed in the
future. Section eight will be a brief conclusion of the 802.11 standard.
IEEE’s proposed standard for wireless LANs (IEEE 802.11) consists of two individual ways to configure a network. The first being an ad-hoc network in which computers are integrated to form a network “on the fly”. Figure 2 represents an ad-hoc network. The advantages of an ad-hoc network are there is not set structure, no fixed points and in most cases every node possesses the ability to communicate directly with all other nodes on the network. An example of this is people joining their laptop computers together to communicate and share information. In order to maintain this type of network, algorithms such as the Spokesman Election Algorithm (SEA) [10] have been designed to elect a machine as the base station (master) [4] of the network with the
others being the slaves. A second algorithm used in an ad-hoc architectures is the use of a broadcast and flooding method to all other nodes to establish who is who [4]

**Figure 2: Ad-Hoc Architecture**

The second type of network architecture used in the 802.11 wireless LAN standard is known as the Infrastructure. This type of network uses fixed network access points for mobile units to communicate. The network access points can be connected to landlines in order to widen the LAN’s capability by bridging wireless nodes to other wired nodes. Therefore, if service areas overlap, hand-offs can occur. An example of this structure is the present day cellular networks around the world [4]. This structure is represented in Figure 3.
III Frames

Various frame types are used by stations, such as the radio Network Interface Card (NIC) and the AP, for not only communication but also managing and controlling the wireless link [6]. Each frame contains a control field that depict the 802.11 protocol version frame type. The control field also contains various indicators such as whether the WEP is on, power management is active, and other additional add on functions discussed previously. All frames also contain MAC addresses of the source and destination station known as the AP, a frame sequence number, frame body, and frame check sequence [6].

A. Control Frames

The 802.11 control frames assist in the delivery of data frames between stations. The subtypes of control frames are Request to Send frame (RTS), Clear to Send frame (CTS), and Acknowledgment frame (ACK). The RTS frame’s main function is optional and reduces frame
collisions present when hidden stations have associations with the same AP. A station sends a RTS frame to another station as the first phase of a two-way handshake necessary before sending a data frame. [6] The CTS frame is used to respond to an RTS by a station. After this step is completed the requesting station is able to transmit data frames. The CTS includes a time value that causes all other stations (including hidden stations) to hold off transmission of frames for a time period in order for the requesting station to properly send its frame. Collisions are therefore minimized by the hidden stations and the overall effect is a high throughput [11][12]. The ACK frame is used after the data frame is received. If the receiving station will perform an error check on the received frame and if there are no errors the station will send out an ACK frame to the sending station. After a period of time has passed, if the sending station does not receive an ACK from the receiving station, the sending station will assume there was an error in the frame or the receiving station did not receive it and therefore retransmit the frame.

**B. Data Frames**

A data frame is responsible for carrying the information stored in packets such as protocols and data from higher layers within the body of the frame. Such examples include, data frames carrying HTML code from a Web page (complete with TCP/IP) headers that the user is viewing.

**C. Management frames**

Common management frame types include Authentication frame, De-authentication frame, Association request frame, Association response frame, Re-association request frame, Re-
association Response frame, Disassociation frame, Beacon frame, Probe request frame, and Probe Response frame. The Authentication frame is exercised in the Authentication process where the AP either accepts or denies the identity of the radio NIC. Only one authentication frame is sent by the radio NIC to the AP for acceptance or rejection. If the AP station rejects the request then a De-authentication frame is sent to the radio NIC. The procedure was discussed in the Section 3 Functionality labeled Authentication. The Association request and response frames are sent in order to enable or deny the AP the ability to allocate resources for and synchronize with the radio NIC. The Re-association request and response frames handle the condition when a radio NIC roams away from currently associated AP and finds another AP having a stronger beacon signal, the radio NIC will send a re-association frame to the new access point [6]. The forwarding of data frames are stored in the buffer from the precious AP. The new AP then coordinates the buffered frames until it is able to transmit to the radio NIC. The Re-association Response is sent by the second AP indicating either an acceptance or rejection of the radio NIC’s re-association request. The Disassociation frame is used for a station to terminate its association with its current station. For example, a radio NIC that is shut down gracefully can send a disassociation frame to alert the AP that the NIC is powering off. Therefore, memory allocation can be removed and the radio NIC is removed from the allocation table. Beacon frames are periodically sent by the AP to announce its presence and relay information. This is used as a timestamp, SSID, and other parameters regarding the access point to the radio NIC’s that are within range [6]. The main advantage of a beacon is it gives the radio NIC the ability to choose the best AP to associate with. The Probe Request and Response frames are used to obtain information from another station. An example of this is the radio NIC sending a probe request in
order to determine which Access Points are within its range. The response frame contains information such as the supported data rates, and other capability information.

**IV Layers**

The 802.11 Standard consists of two major layers known as the MAC (Medium Access Control) Layer and the Physical Layer. The MAC layer interacted interacts directly with the Physical Layer. Figure 4 represents the 802.11 layers.

![Figure 4: 802.11 Layers](image)

**A Mac Layer**

In stead of detecting when a collision, this protocol attempts to avoid collisions which is based off the fact that detecting a collision in a Radio Frequency (RF) transmission network is extremely difficult to detect [4]. DCF 802.11 stations contend for access and attempt to transmit frames when there is no other station transmitting. However, if another station is transmitting a frame, the other stations are “polite” and refrain from transmission until the channel is free [7]. The MAC layer coordinates the mediums’ access. The layer checks the values of the Network Allocation Vector (NAV), a counter resident at each station. The counter represents the amount of time needed by the previous frame to transmit its frames. The NAV must equal zero before
the station attempts to send a frame. Prior to transmission of a frame, the station calculates the amount of time necessary to send the frame based on the frame’s length and data rate. The station places a value representing this time in the duration field in the header of the frame. [7].

Another important aspect of the DCF is known as the random “back-off” timer, which is implemented is the channel is busy. The back-off timer determines the amount of time the node must wait until it is allowed to transmit its packet. During periods in which the channel is clear, the transmitting node decrements its back-off counter, except when the channel is busy it does not decrement its back-off counter. When the back-off counter reaches zero, the node transmits the packet. Since the probability that two nodes will choose the same back-off factor is small, collisions between packets are minimized. Collision detection, as is employed in Ethernet, cannot be used for the radio frequency transmissions of IEEE 802.11. The reason for this is that when a node is transmitting it cannot hear any other node in the system which may be transmitting, since its own signal will drown out any others arriving at the node [4]. After the channel free and a frame is sent, the receiving station examines duration field value and use it as the basis for settling their corresponding NAVs. This process reserves the medium for the sending station to complete its transmission of data [7].

B. MAC Layer Functions

Functions of the MAC layer includes, Scanning, Authentication, Association, WEP, RTS/CTS, Power Save Mode, and Fragmentation. Scanning is used when a radio Network Interface Card (NIC) searches for access points. Scanning includes two types, active and passive.
Passive scanning is mandatory when the NIC channel scans individual channels in order to find the best possible access point signal [7]. For example, access points broadcast a signal periodically, the radio NIC receives this signal known as beacons. Beacons contain important information about the access point such as, the data rates supported and the Service Set Identifier (SSID). The radio NIC is then able to use this data to compare access points and determine which one to use. Active scanning requires the radio NIC to initiate the process by broadcasting a probe frame, and all access points within range respond with a probe response [7]. Active scanning allows the NIC to receive an immediate response from the access points instead of waiting for a beacon transmission [7]. The disadvantage of active scanning when compared to passive scanning is active scanning requires additional overhead on the network which is due to the transmission of probe and its corresponding response frames [7].

Authentication is the process of proving identity and the 802.11 standard specifies two forms: Open System authentication and Shared Key authentication. Open system authentication is mandatory and is a two step process [7]. First the radio NIC sends an authentication request frame to the AP. The AP replies with its own authentication response frame. The response frame contains approval or disapproval of the authentication indicated in the Status Code field in the frame body [7]. Shared Key authentication is not mandatory. It is a four step process and is based on whether the authentication device has the correct Wired Equivalent Privacy Key (WEP). The radio NIC transmits an authentication request frame to the AP. The AP adds additional ‘challenge text’ into the frame body of its response frame and sends it back to the original radio NIC. The radio NIC uses its WEP key to encrypt the challenge text and then retransmits it back to the AP in a separate authentication frame. The AP decrypts the challenge text and compares it to the initial challenge text. If the two
texts are exactly the same, the AP sends an approval authentication frame to the radio NIC. However, if the two texts are not exactly the same, the AP sends a disapproval authentication response frame to the radio NIC [7].

Association is the process executed after the radio NIC has passed authentication. In order to send data frames, the radio NIC must associate with the AP. Association is necessary to synchronize the radio NIC and AP with important information, such as supported data rates [7]. The radio NIC sends an association request frame to the AP which contains information such as the SSID and supported data rates. The AP sends an association response frame back to the radio NIC which contains information such as and association ID along with other AP pertinent information for the radio NIC. After this is complete the radio NIC is able to send data frames to the AP.

WEP, as stated before, is an optional feature in the 802.11 standard to be exercised when needed. Because the body, not the header of the frame is encrypted, and the 802.11 standard specifies a 40-bit key and no key distribution, wireless 802.11 LANs are vulnerable to eavesdroppers [7].

RTS/CTS allows the AP to control the use of the medium for stations activating RTS/CTS. The standard allows for most radio NIC’s to set a threshold of maximum frame length for the RTS/CTS to be activated. RTS/CTS as previously explained allows for the handshake process to continue for each frame, as long as the frame size does not exceed the set threshold. Power Save Mode is an optional feature when using the 802.11 standard. It enables the radio NIC to conserve its battery power when there is not need to send data. In addition, when the power save mode is on the radio NIC also has the ability to go to sleep. Sleep mode is achieved by the radio NIC sending the AP a specific status bit. The status bit is located in the header of each frame. Once the radio NIC is in sleep mode, in order for it to still receive data frames, the sleeping NIC must wake up periodically (at
the right time) to receive regular beacon transmissions coming from the AP. Beacons identify whether or not the NIC has data frames buffered at the AP ready for delivery or not. The NIC can go back to sleep after receiving the frames [7]. Fragmentation is an optional function of the 802.11 standard which enables a station to divide data packets into smaller packets. As with RTC/CTS, users are able to set a requirement for the maximum bit length threshold. Therefore, if the frame length is larger than the threshold, the radio NIC will break the packet into multiple frames no larger than the threshold packet size. [7]

Typical LAN protocols use packets of several hundred of bytes (i.e, Ethernet packet could be up 1518 bytes long). On a WLAN there are some reasons why fragmentation would be desirable to implement. First, the radio link tends to have a higher bit rate error therefore the probability that a packet will become corrupted increases with packet size. Second, in case of packet corruption, (either because of corruption or noise) the smaller the packet, the less overhead it causes to retransmit the packet. Lastly, on a frequency hopping system, the medium is interpreted periodically for hopping (every 20 milliseconds) therefore the smaller the packet the smaller the chance the transmission of the packet will be postponed to after the dwell time [2].

However, introducing a protocol that cannot deal with the standard Ethernet length of 1518 bytes would have caused a major dilemma. Therefore, in order to alleviate future problems a simple fragmentation/reassembly mechanism was introduced. The mechanism is a simple send-and-wait algorithm, where the transmitting station is not allowed to transmit a new fragment until one of the following conditions is met. One, an ACK is received for the transmitted fragment. Two, the fragment was re-transmitted too many times and therefore the frame was dropped. However, the
station is not allowed to transmit to different addresses between retransmission of a given fragment [2]. Figure 5 represents an example of packet fragmentation.

**Figure 5: Fragmentation**

Interframe Spaces consist of four separate types within the standard which are used to define priority. First, Short Inter-Frame Space (SIFS) is the minimum inter frame space and is used to separate transmissions belonging to a single dialog. At any given time, there is always one single station to transmit therefore having priority over all other stations. This value is fixed at 28 microseconds and is calculated in such a way that the transmitting station will have ability to switch back into receive mode and decode the incoming packet [2]. Second, the Point Coordination IFS (PIFS) is used by the AP to gain access to the medium before other stations. Third, the Distributed IFS (DIFS) is used by a station willing to start a new transmission, which is calculated as PIFS plus one time slot [2]. Lastly, the Extended IFS (EIFS) which is a longer IFS is used by a station which has received a packet in which it could not understand. This is needed to prevent the station from colliding with a future packet belonging to the current dialog [2].
C. Physical Layers:

The 802.11 Physical Layer consists of three separate layers known the Infra-Red layer, the Direct Sequencing Spread Spectrum (DSSS) layer, and the Frequency Hopping Spread Spectrum (FHSS) layer. The Infra-Red physical layer operated in the 850 to 950nM band with a peak power of 2 Watts. This physical layer supports two data rates; 1 and 2 Mbps. The modulation is accomplished through either a 4 or 16 level pulse positioning modulation [5]. The DSSS physical layer uses an 11-bit Barker Sequence to spread the data before it is transmitted. In essence, when a bit is transmitted it is them modulated by the 11-bit sequence. The modulation of the 11-bit sequence is achieved by spreading the RF energy across a wider bandwidth than required to transmit the raw data [5]. The receiver is responsible for de-spreading the RF input in order to recover the original data. An advantage of DSSS is, it reduces the effect of narrowband sources of interference [5]. The FHSS physical layer has 22 individual hop patterns to choose from. The frequency hop physical layer is required to hop across the 2.4GHz ISM band covering 79 channels. Each channel occupies 1MHz of bandwidth and must hop at the minimum rate of 2.5 hops per second, which is the specification for the United Sates [5]. Each of the three physical layers has their own unique header. The header is used for synchronizing the receiver and to determine the signal modulation format and data packet length. The headers are always transmitted at 1Mbps. In order to increase the data rate to 2 Mbps for the actual data packet, the headers contain a pre-defined field which allows adjustments to be made [5].
**V Joining a Radio NIC to an AP**

In the case of a radio-based LAN, the transmitting station is unable to listen for collisions while sending data. This is due to the station not being able to have its receiver on while transmitting the frame. As a result, the receiving station needs to send an acknowledgment (ACK) if it detects no errors in the received frame [7]. However, if the receiving station does not receive an ACK after a allocated period of time, the transmitting station will assume there was a collision (or RF interference) and retransmit the frame [7]. Figure 6 represents a Handshake between the radio NIC and the AP.

**Figure 6: Handshake**

The CSMA/CA protocol allows for options that can minimize collisions by using request to send (RTS), clear-to-send (CTS) and data and acknowledge (ACK) transmission frames, in a sequential fashion. Communication is established when one of the wireless nodes sends a short message RTS frame. The RTS frame includes the destination and the length of the message.
The NAV alerts all others in the medium, to back off for the duration of the transmission, the receiving stations issues a CTS frame which echoes the senders address and the NAV. If the CTS frame is not received, it is assumed that a collision occurred and the RTS process starts over. After the data frame is received, an ACK frame is sent back verifying a successful data transmission [5]. Figure 7 represents a schematic of the access mechanism.

The Collision Detection mechanism is an excellent idea for wireless LANs however it is not a good idea for wired LANS. First, a Full-Duplex radio, capable of transmitting and receiving at once, would need to be implemented. This approach would increase the price significantly. Second, the basic assumption of the Collision Detection mechanism, that every station is able to hear each other, cannot be made when dealing with a wired LAN. In a wired LAN, the station is only able to attempt to sense when the channel is free to transmit information not actually verify the channel is free [2]. To avoid these problems, Collision Detection is therefore coupled with a Positive Acknowledgment scheme previously introduced.
A dilemma associated with the 802.11 packet transmission is known as the “hidden node” problem. Figure 5 represents this problem. As shown, node A can communicate to node B and node B can communicate to node C. However, node A and node C cannot communicate. Thus, for instance although node A may sense the channel to be clear, node C may in fact be transmitting to node B. The CSMA/MA protocol described above alerts node A that node B is busy, and hence it must wait before re-transmitting its packet [4]. Figure 8 represents an example of the Hidden Node problem.

The Point Coordination Function (PCF) supports the time-bounded delivery of data frames. The AP grants access to an individual station to the medium by polling the station during the contention free period [7]. The station is unable to transmit frames unless the AP polls them first. The period of time for the PCF -based data traffic occurs alternately between contentions (DCF) periods. The access points polls stations according to a polling list, then
switches to a contention period when stations use DCF. This process enables support for both synchronous (i.e., video applications) and asynchronous (i.e., e-mail and Web browsing applications) modes of operation. However, no known wireless NICs or access points on the market today implement the PCF scheme. [7].

**VI 802.11 Generations**

Table 1 defines the 802.11 task groups and their function in continually developing the existing standard.

**Table 1: 802.11 Task Groups and Functionality**

<table>
<thead>
<tr>
<th>Task Group</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Take advantage of a newly allocated unlicensed radio band to create a new physical layer definition in order to support higher data rates 802.11a.</td>
</tr>
<tr>
<td>B</td>
<td>Upgrade 802.11 using DSSS technique.</td>
</tr>
<tr>
<td>C</td>
<td>Improve MAC layer and bridging.</td>
</tr>
<tr>
<td>D</td>
<td>Modify the Physical layer to meet global regulations.</td>
</tr>
<tr>
<td>E</td>
<td>Enhance the MAC layer to improve quality of service (QoS) for time-sensitive applications</td>
</tr>
<tr>
<td>F</td>
<td>Security improvements</td>
</tr>
<tr>
<td>G</td>
<td>Improve interoperability of access points</td>
</tr>
<tr>
<td>H</td>
<td>Develop a higher speed physical layer extension to 802.11b</td>
</tr>
<tr>
<td>I</td>
<td>Improve security and authentication</td>
</tr>
</tbody>
</table>

802.11a is a physical layer standard that was established in 1999 to operate in the 5Ghz UNII band. The 802.11a revision is based off of the orthogonal frequency division multiplexing (OFDM) technology which allows for the standard to support data ranges ranging from 6 to 54Mbps. OFDM breaks the ceiling of the date bit rate by sending data in massively parallel fashion and solving the symbol rate down so each symbol transmission is much longer than the
typical delay spread [10]. The advantage of the standard operating in the 5GHz band is it allows for a decrease in radio frequency (RF) interference other than the 802.11b and 802.11g standards which utilize the 2.4 GHz frequencies. With high data rates and relatively little interference, 802.11a does a great job of supporting multimedia applications and densely populated user environments. 802.11b was designed to enhance the initial 802.11 DSSS physical layer and include 5.5Mbps and 11Mbps rates compared to the 1Mbps and 2Mbps data rates of the initial 802.11 standard. The 802.11b IEEE Standard was established in 1999. The ability to provide higher data rates is due to the fact the standard takes advantage of the CCK (Complementary Code Keying) technique. The CCK is a modulation technique which uses the radio spectrum as efficiently as possible. 802.11b is most compliant with most wireless LANs in today’s market. The standard is Wi-Fi certification from the Wireless Ethernet Compatibility Alliance (WECA). [1] 802.11c was developed to ensure proper bridge operations and to improve the existing MAC layer. This standard is most commonly used by product developers interested in developing access points. Unfortunately, this standard is not very useful in wireless LAN applications and therefore is not used often.[1] 802.11d was developed to ensure the 802.11 standard would meet global standards and become harmonized. The 802.11d task group has an ongoing charter to define the Physical Layer requirements and satisfy global regulations.[1] 802.11e was developed to ensure a Quality of Service (QoS) would be met with the initial 802.11 standard and to refine the 802.11 MAC layer. Based on the fact the 802.11 does not optimize the transmission of voice and video therefore no effective mechanism is used to prioritize its traffic. The 802.11e task group will refine the MAC layer in order to accommodate this new technological need and therefore enhance the standard’s QoS.[1] 803.11f
was developed to improve the security requirements of the 802.11 standard. The 802.11 standard did not specify the communication between the access points in order to support users roaming from one AP to another AP.[1] Because access points differ slightly when made by different vendors, the AP may not interpolate when the roaming feature is supported. 802.11 G was designed to improve the interoperability of access points and as a higher bandwidth of 54Mbps.

VII 802.11 Future

The flexible nature of 802.11 allows for its continued survival due to adaptation. As new technologies emerge and new developments are made the 802.11 standard can be edited and amended. This makes it functionality limited only by the ability of those running it to continue to make the necessary discoveries, which at present they are very capable of doing. Currently there are projects in the works to both revise past parts of the standard and create new standards within it. These include things from allowing higher speed data rates, improved energy efficiency, increased security and enhancing the standard to allow for other country’s rules of radio operation. With the ability for such adaptation the lifetime of the 802.11 standard can only be determined by the innovations of the developing engineers and the demand in the market for the products of the field.

The 802.11 only has one real competitor which is HiperLAN2. HiperLAN2 is another wireless communication system working within the 5GHz range. From a technological standpoint the two different standard’s clear dividing point is in their QoS methods. While 802.11 is adapting there QoS in 802.11e, HiperLAN2 has been using a time-division duplexing
(TDD). TDD packets information into smaller sections and transmits them in the time domain, and with these small packets allotting time for base station to mobile station and mobile to base station, it is possible to give the appearance of a full duplex (a continuous signal in both directions). However, HiperLAN2 does not make any contributions to the 2.4GHz range, making it unlikely for it to completely overtake 802.11. The 802.11 standard’s constant revamping and advancement will make it a long lasting standard as long as there is a market for items to use their functions.

**VIII Conclusion**

In this paper, we described the basic functionality, working groups associated and future generations of the 802.11 IEEE Standard. We described the two different architectures, Ad-hoc and Infrastructure, along with the two important layers known as the MAC and Physical layers. We described in more detail the underlying functionality of each layer and whether or not it depended on any other techniques to complete transmission successfully. We also presented the basic steps a radio NIC takes to join a station, AP, and how they communicate.

The ongoing development of the 802.11, specifically with 802.11g will continue studying new methods to increase performance and make better use of the radio spectrum. Hopefully within the next few years, everyone in the world will be able to reap the benefits of the 802.11 technology to decrease communication financial spending with wired LANs and therefore provide an opportunity for developing countries to enhance their communication with the world.
References:


  =about&file=index.xml&amp;xsl=generic.xsl.

