Electrical Engineering Department,

Fourth Year - Communications & Electronics.

EE484 COMMUNICATION SYSTEMS

Experiment 3: WLAN

PREPARED BY	SECTION	SEAT.NO.
Mahmoud Mohamed Kamal Ismail	7	250
Mahmoud Alaa-Elden Mahmoud	7	249
Mahmoud AbdElHady Mahmoud	7	248
Mahmoud Adel Hassan Mohamed	7	247
Mostafa Khaled Gaber Rahal	7	262

➢ Contents

All Experiments and m files:
https://github.com/MahmoudFierro98/EE484_Communication_Systems_Lab

1. Problem 1: General report about WLAN Standard

1. Describe the history of the WLAN and how this standard started.
   - In 1970, the University of Hawaii developed the first wireless network to wirelessly communicate data among the Hawaiian Islands. However, it wasn't until 1991 that the Institute of Electrical and Electronics Engineers (IEEE) (which I will describe in more detail next week) began to discuss standardizing WLAN technologies. In 1997, the IEEE ratified the original 802.11 standard—the "802.11" technology term simply refers to Wi-Fi.
   - In 1999 wireless was introduced to the general public as a "nice to have" with the 802.11 a and b ratifications. These standards had very low speeds (up to 54 Mbps & 11Mbps respectively) but it was ok, because there were no handheld mobile phones that utilized Wi-Fi and very few laptops.
   - By 2003, however, some mobile devices that utilized Wi-Fi were coming out and portable laptops were becoming more standard for both business and personal use. That is when 802.11g was ratified— delivering up to 54 Mbps in the 2.4 GHz space. As we moved closer to today, in 2007, the birth of the smartphone really came about and along with it came the ratification of 802.11n.
   - The "n" standard brought about faster processing speeds of up to 450 Mbps for Wi-Fi and it supported both 2.4 GHz and 5 GHz devices. Today, smart devices are robust enough to replace specialized, more expensive laptop technologies so wireless has had to catch up.

2. Mention some of WLAN applications.
   - Vehicles
     Many wireless communication systems and mobility aware applications are used for following purpose:

     - Transmission of music, news, road conditions, weather reports, and another broadcast information are received via digital audio broadcasting (DAB) with 1.5Mbit/s.
     - For personal communication, a universal mobile telecommunications system (UMTS) phone might be

available offering voice and data connectivity with 384kbit/s.
    - For remote areas, satellite communication can be used, while the current position of the car is determined via the GPS (Global Positioning System).
    - A local ad-hoc network for the fast exchange of information (information such as distance between two vehicles, traffic information, road conditions) in emergency situations or to help each other keep a safe distance. Local ad-hoc network with vehicles close by to prevent guidance system, accidents, redundancy.
    - Vehicle data from buses, trucks, trains and high speed train can be transmitted in advance for maintenance.
    - In ad-hoc network, car can comprise personal digital assistants (PDA), laptops, or mobile phones connected with each other using the Bluetooth technology.
- Emergency

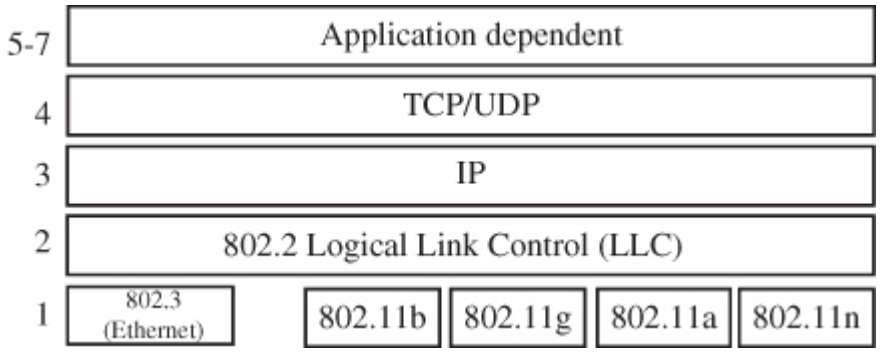
  Following services can be provided during emergencies:
    - Video communication: Responders often need to share vital information. The transmission of real time situations of video could be necessary. A typical scenario includes the transmission of live video footage from a disaster area to the nearest fire department, to the police station or to the near NGOs etc.
    - Push To Talk (PTT): PTT is a technology which allows half duplex communication between two users where switching from voice reception mode to the transmit mode takes place with the use of a dedicated momentary button. It is similar to walkie-talkie.
    - Audio/Voice Communication: This communication service provides full duplex audio channels unlike PTT. Public safety communication requires novel full duplex speech transmission services for emergency response.
    - Real Time Text Messaging (RTT): Text messaging (RTT) is an effective and quick solution for sending alerts in case of emergencies. Types of text messaging can be email, SMS and instant message.

- Business
  Travelling Salesman
  - Directly access to customer files stored in a central location.
  - Consistent databases for all agents
  - Mobile office
  - To enable the company to keep track of all the activities of their travelling employees.

  In Office
  - Wi-Fi wireless technology saves businesses or companies a considerable amount of money on installations costs.
  - There is no need to physically setup wires throughout an office building, warehouse or store.
  - Bluetooth is also a wireless technology especially used for short range that acts as a complement to Wi-Fi. It is used to transfer data between computers or cellphones.

  Transportation Industries
  - In transportation industries, GPS technology is used to find efficient routes and tracking vehicles.
- LAN Extension
  - Save installation of LAN cables.
  - Eases reallocation and modification of network structure.
- Open hotspots in campuses, hotels, restaurants …etc.
- Can be used for indoor positioning system.

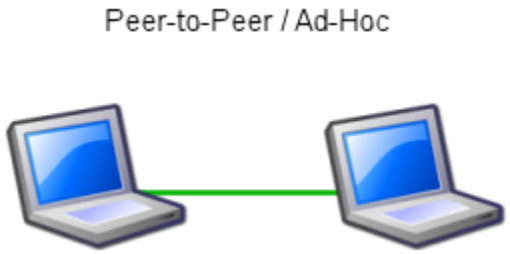
3. Describe the protocol stack of WLAN
   - Wireless LAN received its name from the fact that it is primarily based on existing LAN standards. These standards were initially created by the IEEE for wired interconnection of computers and can be found in the 802.X standards (e.g. 802.3 [2]). In general, these standards are known as 'Ethernet' standards. The wireless variant, which is generally known as Wireless LAN



(WLAN), is specified in the 802.11 standard. As shown in Figure 6.1, its main application today is to transport IP packets over layer 3 of the OSI model. Layer 2, the data link layer, has been adapted from the wired world with relatively few changes. To address the wireless nature of the network, a number of management operations have been defined, which are described in Section 6.2. Only layer 1, the physical layer, is a new development, as WLAN uses airwaves instead of cables to transport data frames.

4. In details describe the WLAN system architecture (configurations), with the difference between the two modes.

- Ad-Hoc /Peer-to-peer mode
    - An ad hoc network (not the same as a Wi-Fi Direct network) is a network where stations communicate only peer to peer (P2P). There is no base and no one gives permission to talk. This is accomplished using the Independent Basic Service Set (IBSS).

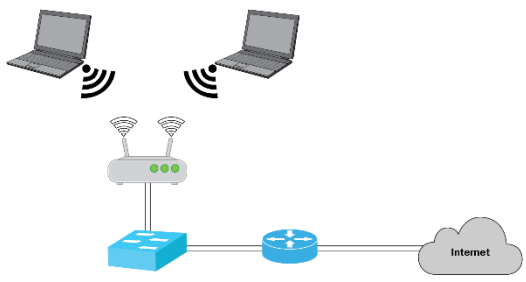


    - A Wi-Fi Direct network is another type of network where stations communicate peer to peer.
    - In a Wi-Fi P2P group, the group owner operates as an access point and all other devices are clients. There are two main methods to establish a group owner in the Wi-Fi Direct group. In one approach, the user sets up a P2P group owner manually. This method is also known as Autonomous Group Owner (autonomous GO). In the second method, also called negotiation-based group creation, two devices compete based on the group owner intent value. The device with higher intent value becomes a group owner and the second device becomes a client. Group owner intent value can depend on whether the wireless device performs a cross-connection between an infrastructure WLAN service and a P2P group, remaining power in the wireless device, whether the wireless device is already a group owner in

another group or a received signal strength of the first wireless device.

  - A peer-to-peer network allows wireless devices to directly communicate with each other. Wireless devices within range of each other can discover and communicate directly without involving central access points. This method is typically used by two computers so that they can connect to each other to form a network. This can basically occur in devices within a closed range.
  - If a signal strength meter is used in this situation, it may not read the strength accurately and can be misleading, because it registers the strength of the strongest signal, which may be the closest computer.
  - IEEE 802.11 defines the physical layer (PHY) and MAC (Media Access Control) layers based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). This is in contrast to Ethernet which uses CSMA-CD (Carrier Sense Multiple Access with Collision Detection). The 802.11 specification includes provisions designed to minimize collisions, because two mobile units may both be in range of a common access point, but out of range of each other.

- Infrastructure mode
  - Most Wi-Fi networks are deployed in infrastructure mode. In infrastructure mode, wireless clients, such as laptops and smartphones, connect to the WAP to join the network. The WAP usually has a wired network connection and may have permanent wireless connections to other WAPs.
  - WAPs are usually fixed and provide service to their client nodes within range. Some networks will have multiple WAPs, using the same SSID and security arrangement. In that case connecting to any WAP on that network joins the client to the network and



the client software will try to choose the WAP that gives the best service, such as the WAP with the strongest signal.

5. what are the advantages and disadvantages of Infrastructure mode?

Advantages	Disadvantages
Two wireless devices can communicate with each other over larger distance with AP in middle.	Packet that is transmitted between two wireless devices has to be transmitted twice over air.

6. How to configure Ad-Hoc network?

- Network must have name (Service set identity SSID).
- All users select the same Frequency channel number.
- All users use same ciphering key.
- Individual IP address has to be configured in every device.
- Referred to as independent basic service set(IBSS).

7. Show in detail how the WLAN standard changed through the versions 802.11b/g/a/n/ac/ad.

Standard	Frequency band	Theoretical max data rate
802.11b	2.4 GHz	1 to 11 Mbps
802.11g	2.4 GHz	6 to 54 Mbps
802.11a	5 GHz	6 to 54 Mbps
802.11n	2.4 GHz/5 GHz	6 to 600 Mbps
802.11ac	5 GHz	Up to 6.39 Gbps
802.11ad	60 GHz	Up to 6.76 Gbps

Standard	Frequency Band	Bandwidth	Modulation Scheme	Channel Arch.	Maximum Data Rate	Range
802.11	2.4 GHz	20 MHz	BPSK to 256-QAM	DSSS, FHSS	2 Mbps	20 m
b	2.4 GHz	21 MHz	BPSK to 256-QAM	CCK, DSSS	11 Mbps	35 m
a	5 GHz	22 MHz	BPSK to 256-QAM	OFDM	54 Mbps	35 m
g	2.4 GHz	23 MHz	BPSK to 256-QAM	DSSS, OFDM	54 Mbps	70 m
n	2.4 GHz, 5 GHz	24 MHz and 40 MHz	BPSK to 256-QAM	OFDM	600 Mbps	70 m
ah	900 MHz	1, 2, 4, 8, and 16 MHz	BPSK to 256-QAM	SC, OFDM	40 Mbps	1 km

- 802.11a (OFDM waveform)
  - 802.11a, published in 1999, uses the same data link layer protocol and frame format as the original standard, but an OFDM based air interface (physical layer) was added. It was later relabeled Wi-Fi 2, by the Wi-Fi Alliance, relative to Wi-Fi 1 (802.11b).
  - It operates in the 5 GHz band with a maximum net data rate of 54 Mbit/s, plus error correction code, which yields realistic net achievable throughput in the mid-20 Mbit/s. It has seen widespread worldwide implementation, particularly within the corporate workspace.
  - Since the 2.4 GHz band is heavily used to the point of being crowded, using the relatively unused 5 GHz band gives 802.11a a significant advantage. However, this high carrier frequency also brings a disadvantage: the effective overall range of 802.11a is less than that of 802.11b/g. In theory, 802.11a signals are absorbed more readily by walls and other solid objects in their path due to their smaller wavelength, and, as a result, cannot penetrate as far as those of 802.11b. In practice, 802.11b typically has a higher range at low speeds (802.11b will reduce speed to 5.5 Mbit/s or even 1 Mbit/s at low signal strengths). 802.11a also suffers from interference, but locally there may be fewer signals to interfere with, resulting in less interference and better throughput.
- 802.11b
  - The 802.11b standard has a maximum raw data rate of 11 Mbit/s (Megabits per second) and uses the same media access method defined in the original standard. 802.11b products appeared on the market in early 2000, since 802.11b is a direct extension of the modulation technique defined in the original standard. The dramatic increase in throughput of 802.11b (compared to the original standard) along with simultaneous substantial price reductions led to the rapid acceptance of 802.11b as the definitive wireless LAN technology.
  - Devices using 802.11b experience interference from other products operating in the 2.4 GHz band. Devices operating in the 2.4 GHz range include microwave ovens, Bluetooth

devices, baby monitors, cordless telephones, and some amateur radio equipment. As unlicensed intentional radiators in this ISM band, they must not interfere with and must tolerate interference from primary or secondary allocations (users) of this band, such as amateur radio.

- 802.11g
  - In June 2003, a third modulation standard was ratified: 802.11g. This works in the 2.4 GHz band (like 802.11b), but uses the same OFDM based transmission scheme as 802.11a. It operates at a maximum physical layer bit rate of 54 Mbit/s exclusive of forward error correction codes, or about 22 Mbit/s average throughput.[34] 802.11g hardware is fully backward compatible with 802.11b hardware, and therefore is encumbered with legacy issues that reduce throughput by ~21% when compared to 802.11a.
  - The then-proposed 802.11g standard was rapidly adopted in the market starting in January 2003, well before ratification, due to the desire for higher data rates as well as reductions in manufacturing costs.[citation needed] By summer 2003, most dual-band 802.11a/b products became dual-band/tri-mode, supporting a and b/g in a single mobile adapter card or access point. Details of making b and g work well together occupied much of the lingering technical process; in an 802.11g network, however, the activity of an 802.11b participant will reduce the data rate of the overall 802.11g network.
  - Like 802.11b, 802.11g devices also suffer interference from other products operating in the 2.4 GHz band, for example, wireless keyboards.
- 802.11n
  - 802.11n is an amendment that improves upon the previous 802.11 standards; its first draft of certification was published in 2006. The 802.11n standard was retroactively labelled as Wi-Fi 4 by the Wi-Fi Alliance.[37][38] The standard added support for multiple-input multiple-output antennas (MIMO). 802.11n operates on both the 2.4 GHz and the 5 GHz bands. Support for 5 GHz bands is optional. Its net data rate ranges from 54 Mbit/s to 600 Mbit/s. The IEEE has approved the amendment,

and it was published in October 2009.[39][40] Prior to the final ratification, enterprises were already migrating to 802.11n networks based on the Wi-Fi Alliance's certification of products conforming to a 2007 draft of the 802.11n proposal.

8. Discuss how the WLAN system improved through the versions 802.11e/f/h/i/w

- 802.11e
  - 802.11e is a proposed enhancement to the 802.11a and 802.11b wireless LAN (WLAN) specifications. It offers quality of service (QoS) features, including the prioritization of data, voice, and video transmissions. The 802.11a, 802.11b, and 802.11e standards are elements of the 802.11 family of specifications for wireless local area networks (wireless LANs or WLANs). Business and consumer products using 802.11e are expected to become widely available in late 2004 or in 2005.
  - 802.11e enhances the 802.11 Media Access Control layer (MAC layer) with a coordinated time division multiple access (TDMA) construct, and adds error-correcting mechanisms for delay-sensitive applications such as voice and video. The 802.11e specification provides seamless interoperability between business, home, and public environments such as airports and hotels, and is especially well suited for use in networks that include multimedia capability. It offers all subscribers high-speed Internet access with full-motion video, high-fidelity audio, and voice over IP.
  - Networks employing 802.11e operate at radio frequencies between either of two ranges: 2.400 GHz to 2.4835 GHz (the same as 802.11b networks), or 5.725 GHz to 5.850 GHz (the same as 802.11a networks). There are certain advantages to the higher frequency range, including faster data transfer speed, more channels, and reduced susceptibility to interference.
- 802.11f
  - The IEEE approved 802.11f on June 12, 2003. 802.11f is not a specification, per se. Instead, it's a "recommended practice" document, meaning that vendor compliance is

completely voluntary. The document was drafted with the goal of improving the handover mechanism in Wi-Fi networks, so that end-users can maintain a connection while roaming between two different switched segments (radio channels), or between access points attached to two different networks. This is vital if Wi-Fi networks are to offer the same mobility that cell phone users take for granted.

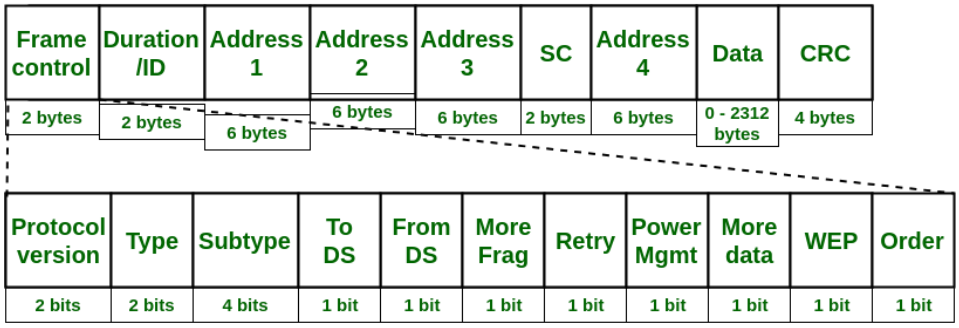
- 802.11h-2003
    - 802.11h-2003, or just 802.11h, refers to the amendment added to the IEEE 802.11 standard for Spectrum and Transmit Power Management Extensions. It solves problems like interference with satellites and radar using the same 5 GHz frequency band. It was originally designed to address European regulations but is now applicable in many other countries. The standard provides Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) to the 802.11a PHY. It has been integrated into the full IEEE 802.11-2007 standard.
- 802.11i-2004
    - IEEE 802.11i-2004, or 802.11i for short, is an amendment to the original IEEE 802.11, implemented as Wi-Fi Protected Access II (WPA2). The draft standard was ratified on 24 June 2004. This standard specifies security mechanisms for wireless networks, replacing the short Authentication and privacy clause of the original standard with a detailed Security clause. In the process, the amendment deprecated broken Wired Equivalent Privacy (WEP), while it was later incorporated into the published IEEE 802.11-2007 standard.
- 802.11w-2009
    - 802.11w-2009 is an approved amendment to the IEEE 802.11 standard to increase the security of its management frames.

9. How to limit/decrease the interference between Access Points (AP) within the Extended service set (ESS)

- To extend the range of the network several Aps can be cooperate with each other and extended service set (ESS) is formed.
- All APs of ESS located in the same IP subnet.
- All Aps use the same SSID.
- APs have to send on different frequency.
- The coverage area of different APs should overlap so that client doesn't lose coverage ID border areas.

10. Discuss the MAC frame format for WLAN and mention the function of each group of bits in it.

- The MAC layer frame consist of 9 fields. The following figure shows the basic structure of an IEEE 802.11 MAC data frame along with the content of the frame control field.



IEEE 802.11 MAC Frame Structure

- Frame Control (FC):

  It is 2 bytes long field which defines type of frame and some control information. Various fields present in FC are:

  - Version:

    It is a 2-bit long field which indicates the current protocol version which is fixed to be 0 for now.
  - Type:

    It is a 2 bit long field which determines the function of frame i.e. management (00), control (01) or data(10). The value 11 is reserved.
  - Subtype:

    It is a 4-bit long field which indicates sub-type of the frame like 0000 for association request, 1000 for beacon.

- To DS:
  It is a 1-bit long field which when set indicates that destination frame is for DS (distribution system).
- From DS:
  It is a 1-bit long field which when set indicates frame coming from DS.
- More frag (More fragments):
  It is 1-bit long field which when set to 1 means frame is followed by other fragments.
- Retry:
  It is 1-bit long field, if the current frame is a retransmission of an earlier frame, this bit is set to 1.
- Power Mgmt. (Power management):
  It is 1-bit long field which indicates the mode of a station after successful transmission of a frame. Set to 1 the field indicates that the station goes into power-save mode. If the field is set to 0, the station stays active.
- More data:
  It is 1-bit long field which is used to indicates a receiver that a sender has more data to send than the current frame. This can be used by an access point to indicate to a station in power-save mode that more packets are buffered or it can be used by a station to indicate to an access point after being polled that more polling is necessary as the station has more data ready to transmit.
- WEP:
  It is 1-bit long field which indicates that the standard security mechanism of 802.11 is applied.
- Order:
  It is 1-bit long field, if this bit is set to 1 the received frames must be processed in strict order.

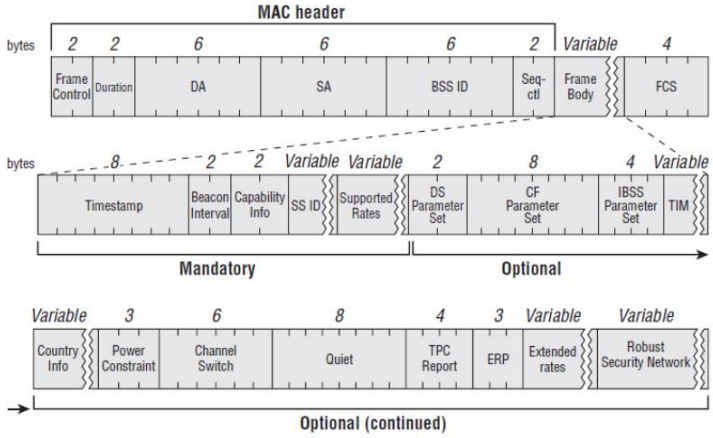
- Duration/ID:
  It is 4 bytes long field which contains the value indicating the period of time in which the medium is occupied (in μs).
- Address 1 to 4:

These are 6 bytes long fields which contain standard IEEE 802 MAC addresses (48 bit each). The meaning of each address depends on the DS bits in the frame control field.

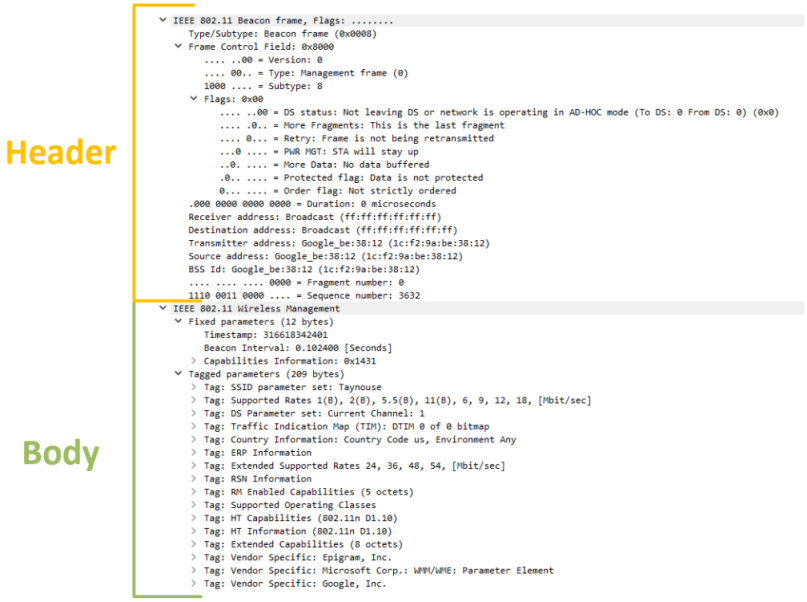
- SC (Sequence control):
  It is 16 bits long field which consists of 2 sub-fields, i.e., Sequence number (12 bits) and Fragment number (4 bits). Since acknowledgement mechanism frames may be duplicated hence, a sequence number is used to filter duplicate frames.
- Data:
  It is a variable length field which contain information specific to individual frames which is transferred transparently from a sender to the receiver(s).
- CRC (Cyclic redundancy check):
  It is 4 bytes long field which contains a 32-bit CRC error detection sequence to ensure error free frame.

11. what are beacon frames, and what are their frame body contents and functionalities.

- APs send beacons at a regular interval called the target beacon transmit time (TBTT) to advertise the SSIDs they service. Beacons contain the configuration of the WLAN including whether it supports standards such as 802.11k, 802.11r, the required cipher suites and authentication key management (AKM) methods, whether protection mechanisms are required, etc. The presence of certain information elements (IE) indicates whether the related configuration is present. The figure below shows which fields are mandatory in a beacon frame. Note that this information is in the body of the management frame.

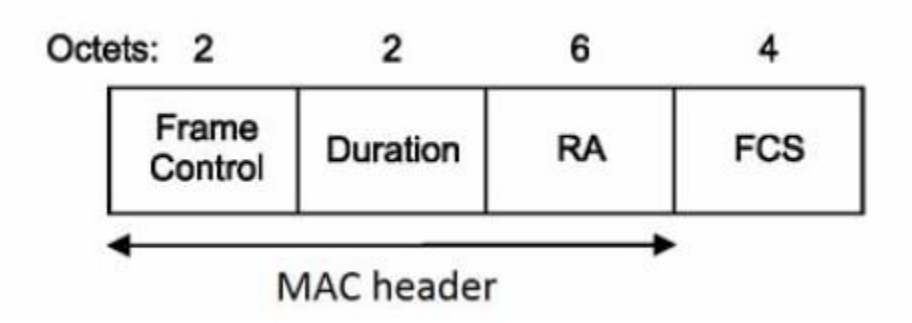


- Below shows a beacon frame in Wireshark. We can see a timestamp of 316618342401 which is used to keep time synchronized among stations in a BSS. Our beacon interval, also known as target beacon transmit time (TBTT) is the default of 102.4ms. The required “Capability Info” field is expanded below. The SSID being advertised by the beacon is “Taynouse” and supported data rates are listed following. It is important to capture your own beacons and start poking around; the number of optional fields is much longer than the required fields. It is important to know the names and purpose of all the beacon fields for the CWAP exam. I highly recommend downloading a copy of the 802.11-2016 standard for free here and searching for each of these fields yourself.

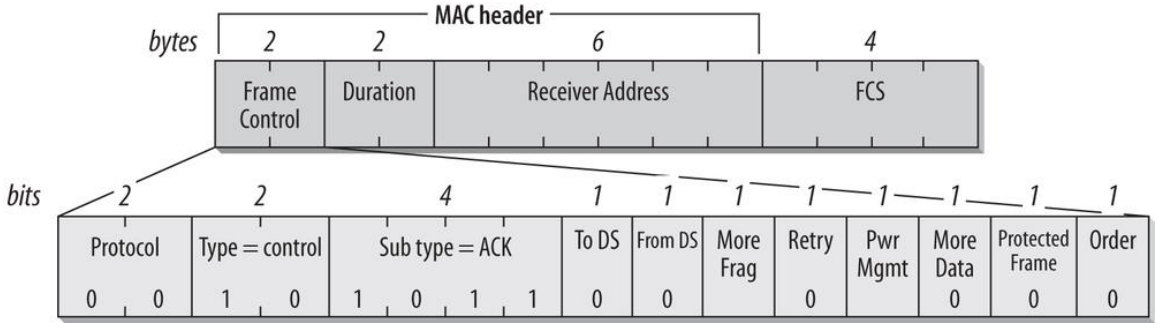


12. Describe the ACK frame format and what is the functionality of the ACK frame.

- ACK frames create a delivery verification method; they are expected after the transmission of data frames to confirm receipt of the frame. If the CRC check fails, the receiver will not send an ACK. If the sender does not receive an ACK, it will retransmit the frame.

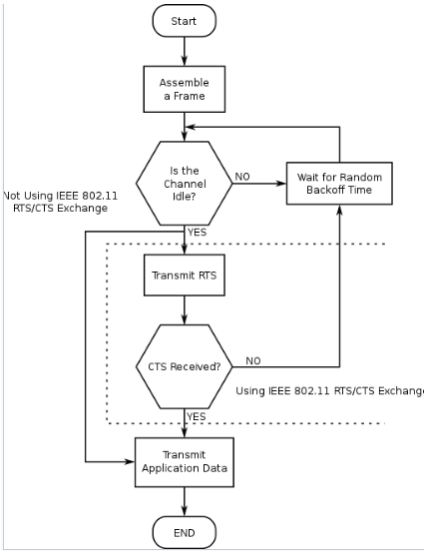



```
IEEE 802.11 Acknowledgement, Flags: ........
   Type/Subtype: Acknowledgement (0x001d)
   Frame Control Field: 0xd400
      .... ..00 = Version: 0
      .... 01.. = Type: Control frame (1)
      1101 .... = Subtype: 13
    > Flags: 0x00
   .000 0000 0000 0000 = Duration: 0 microseconds
   Receiver address: ZebraTec_b3:04:f0 (40:83:de:b3:04:f0)
```



13. Describe the CSMA/CA Protocol and RTS/CTS messages

- CSMA/CA Protocol
  - Collision avoidance is used to improve the performance of the CSMA method by attempting to divide the channel somewhat equally among all transmitting nodes within the collision domain.
  - Carrier Sense: prior to transmitting, a node first listens to the shared medium (such as listening for wireless signals in a wireless network) to determine whether another node is transmitting or not. Note that the hidden node problem means another node may be transmitting which goes undetected at this stage.



- Collision Avoidance: if another node was heard, we wait for a period of time (usually random) for the node to stop transmitting before listening again for a free communications channel.
- Request to Send/Clear to Send (RTS/CTS) may optionally be used at this point to mediate access to the shared medium. This goes some way to alleviating the problem of hidden nodes because, for instance, in a wireless network, the Access Point only issues a Clear to Send to one node at a time. However, wireless 802.11 implementations do not typically implement RTS/CTS for all transmissions; they may turn it off completely, or at least not use it for small packets (the overhead of RTS, CTS and transmission is too great for small data transfers).
- Transmission: if the medium was identified as being clear or the node received a CTS to explicitly indicate it can send, it sends the frame in its entirety. Unlike CSMA/CD, it is very challenging for a wireless node to listen at the same time as it transmits (its transmission will dwarf any attempt to listen). Continuing the wireless example, the node awaits receipt of an acknowledgement packet from the Access Point to indicate the packet was received and check summed correctly. If such acknowledgement does not arrive in a timely manner, it assumes the packet collided with some other transmission, causing the node to enter a period of binary exponential backoff prior to attempting to re-transmit.
- Although CSMA/CA has been used in a variety of wired communication systems, it is particularly beneficial in a wireless LAN due to a common problem of multiple stations being able to see the Access Point, but not each other. This is due to differences in transmit power, and receive sensitivity, as well as distance, and location with respect to the AP. This will cause a station to not be able to 'hear' another station's broadcast. This is the so-called 'hidden node', or 'hidden station' problem. Devices utilizing 802.11 based standards can enjoy the benefits of collision avoidance (RTS / CTS handshake, also Point coordination function), although they do not do so by default. By default, they use a Carrier sensing mechanism

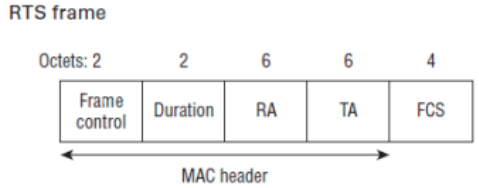
called 'exponential backoff', or (Distributed coordination function) that relies upon a station attempting to 'listen' for another station's broadcast before sending. CA, or PCF relies upon the AP (or the 'receiver' for Ad hoc networks) granting a station the exclusive right to transmit for a given period of time after requesting it (Request to Send / Clear to Send).

- CSMA-CA requires a determination of whether a channel is 'idle', even when incompatible standards and overlapping transmission frequencies are used. Per the standards, for 802.11/Wi-Fi transmitters on the same channel, transmitters must take turns to transmit if they can detect each other even 3 dB above the noise floor (the thermal noise floor is around -101 dBm for 20 MHz channels). On the other hand, transmitters will ignore transmitters with incompatible standards or on overlapping channels if the received signal strength from them is below a threshold Pth which, for non-Wi-Fi 6 systems, is between -76 and -80 dBm.

- RTS/CTS messages
  - CSMA/CA can optionally be supplemented by the exchange of a Request to Send (RTS) packet sent by the sender S, and a Clear to Send (CTS) packet sent by the intended receiver R. Thus, alerting all nodes within range of the sender, receiver or both, to not transmit for the duration of the main transmission. This is known as the IEEE 802.11 RTS/CTS exchange. Implementation of RTS/CTS helps to partially solve the hidden node problem that is often found in wireless networking.
  - To avoid hidden terminal problem we use RTS/CTS signals.

14. Describe both the RTS and CTS frame format.

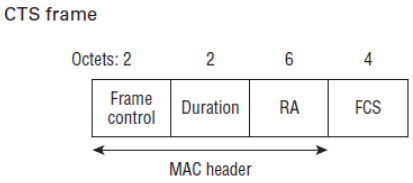
- RTS frame
  - Here is the frame format of a RTS farme. It is 20 byte in length. Frame type is “Control or value 1” & subtype is “RTS or value 11“. Duration value



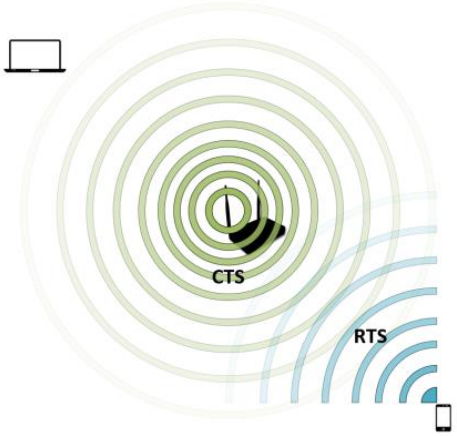
of RTS frame include the time needed for the subsequent frames in the transmit operation to be transmitted.

```
IEEE 802.11 Request-to-send, Flags: ........
    Type/Subtype: Request-to-send (0x001b)
  Frame Control Field: 0xb400
      .... ..00 = Version: 0
      .... 01.. = Type: Control frame (1)
      1011 .... = Subtype: 11
    > Flags: 0x00
    .000 0000 1001 1010 = Duration: 154 microseconds
    Receiver address: Cisco_30:95:0b (0c:85:25:30:95:0b)
    Transmitter address: MurataMa_1a:e5:e4 (b8:d7:af:1a:e5:e4)
```

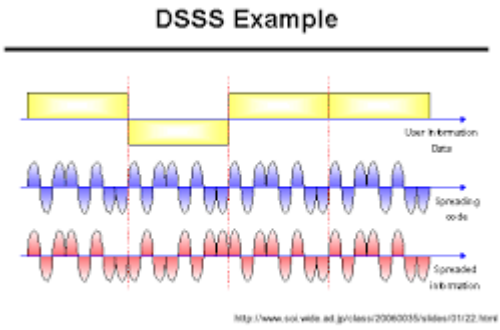
- CTS frame
  - CTS is a 14 byte long control frame. Subtype is 12 in this case. It simply get the TA of the RTS frame & set it to RA. Duration of the CTS frame is the duration field of RTS, adjusted by subtraction of aSIFS & time required to transmit the CTS frame.




```
IEEE 802.11 Clear-to-send, Flags: ........
    Type/Subtype: Clear-to-send (0x001c)
  Frame Control Field: 0xc400
      .... ..00 = Version: 0
      .... 01.. = Type: Control frame (1)
      1100 .... = Subtype: 12
    > Flags: 0x00
    .000 0000 1000 1010 = Duration: 138 microseconds
    Receiver address: Apple_1d:99:c5 (d4:61:da:1d:99:c5)
```



15. Discuss Direct sequence spread spectrum (DSSS) and how it is useful in WLAN.



- n telecommunications, direct-sequence spread spectrum (DSSS) is a spread-spectrum modulation technique primarily used to reduce overall signal interference. The direct-sequence modulation makes the transmitted signal wider in bandwidth than the information bandwidth. After the dispreading or removal of the direct-sequence modulation in the receiver, the information bandwidth is restored, while the unintentional and intentional interference is substantially reduced.
- DSSS phase-shifts a sine wave pseudo randomly with a continuous string of chips, each of which has a much shorter duration than an information bit. That is, each information bit is modulated by a sequence of much faster chips. Therefore, the chip rate is much higher than the information bit rate.
- DSSS uses a signal structure in which the spreading sequence produced by the transmitter is already known by the receiver. The receiver can then use the same spreading sequence to counteract its effect on the received signal in order to reconstruct the information signal.
- The IEEE 802.11b WLAN is an example of a wireless network that uses DSSS transmission. FHSS uses more powerful signals that are transmitted in a pseudo-random sequence on several different frequencies. The receiver has to ensure that it is on the same frequency as the transmitter at exactly the same time.
- To block interference with Bluetooth.

16-Compare between the DSSS methods (Chipping codes) used in 1Mbit/s and 11Mbit/s Transmissions.

- Direct-sequence spread-spectrum transmissions multiply the data being transmitted by a pseudorandom spreading sequence that has a much higher bit rate than the original data rate. The resulting transmitted signal resembles bandlimited white noise,

like an audio recording of "static". However, this noise-like signal is used to exactly reconstruct the original data at the receiving end, by multiplying it by the same spreading sequence (because 1 × 1 = 1, and −1 × −1 = 1). This process, known as dispreading, is mathematically a correlation of the transmitted spreading sequence with the spreading sequence that the receiver already knows the transmitter is using. After the dispreading, the signal-to-noise ratio is approximately increased by the spreading factor, which is the ratio of the spreading-sequence rate to the data rate.

- While a transmitted DSSS signal occupies a much wider bandwidth than a simple modulation of the original signal would require, its frequency spectrum can be somewhat restricted for spectrum economy by a conventional analog bandpass filter to give a roughly bell-shaped envelope centered on the carrier frequency. In contrast, frequency-hopping spread spectrum pseudo randomly retunes the carrier and requires a uniform frequency response since any bandwidth shaping would cause amplitude modulation of the signal by the hopping code.
- If an undesired transmitter transmits on the same channel but with a different spreading sequence (or no sequence at all), the dispreading process reduces the power of that signal. This effect is the basis for the code division multiple access (CDMA) property of DSSS, which allows multiple transmitters to share the same channel within the limits of the cross-correlation properties of their spreading sequences.
- Due to its wide deployment and maturity, it seems proper to start with 802.11b. 802.11b uses direct-sequence spread spectrum (DSSS) radio transmission for data delivery. DSSS works by transmitting the signal across several frequencies simultaneously, with the idea that one of the transmissions will make it to the receiver. The 802.11b DSSS model uses fourteen carrier signal channels. These carrier channels are the starting point for the transmission, which spreads into the frequency ranges above and below carrier frequency. Four data rates are supported: 1 Mbps, 2 Mbps, 5.5 Mbps and 11 Mbps. To ensure data integrity, 802.11b uses chipping schemes to encapsulate the actual data. The use of the chipping code scheme adds to the size of the data message

(utilizing bandwidth for delivering the data, instead of moving actual data). This is because sending the data as chips increases the resilience of the data transmission, making it possible to reconstruct the data in the event of transmission interference. Once the data has been encoded, the chip is modulated and transmitted over the carrier signal channel.

- The chipping and modulation schemes used with 802.11b differ as the transmission rate increases. Mbps 802.11b uses the Barker code chipping sequence (10110111000 using 11 bits to encode 1 bit, coupled with Binary Phase Shift Keying (BPSK) modulation. BPSK works by shifting the phase of the carrier signal 180 degrees in accordance with the digital data stream. Differences in the signal are detected by comparing the phase of each incoming bit to the phase of the preceding bit. When the bit takes a value "1"or "0," the carrier phase changes between 180 degrees and 0 degrees. The Barker code and Quaternary Phase Shift Keying (QPSK) modulation is used for Mbps. QPSK sends 2-bit symbols using four carrier phase shifts. 802.11b transmission rates of 5.5 and 11 Mbps use a combination of QPSK modulation and Complementary Code Keying (CCK) or the chipping sequencing. Actually, CCK is used for 5.5 Mbps and CCK2 is used for 11 Mbps transmissions. CCK uses 64 unique code words and works by using complementary code sequences in combination with turning bits to transmit 4 and 8-bit data chips. So, at the operational rate of 5.5 Mbps, QPSK/CCK moves 4 data bits and at 11 Mbps, 8 data bits are moved. At each operation speed, a consistent chip transmission rate of 11 Mchip/s is maintained, with changes in encoding and modulation increasing the throughput over the same amount of bandwidth.
- 802.11b utilizes the 83 MHz Industrial, Scientific & Medical (ISM) band, which is crowded and prone to attenuation. This band is utilized by everything from wireless phones and microwaves to garage door openers. And just about everything (walls, posts, power lines, windows, people, etc.) can absorb, reflect and scatter the signal. When deploying an 802.11b wireless network, one of the most common mistakes made is working from the assumption that all of the channels are usable. This is not the case. The carrier

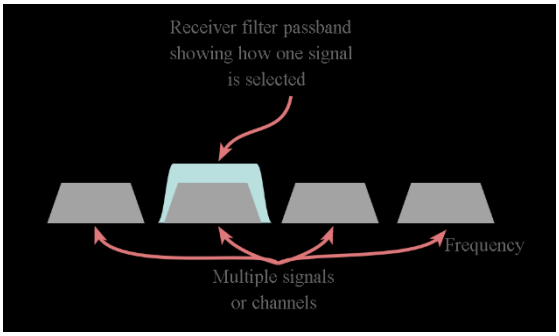
frequency channels, by design, bleed into one another. Each 802.11b transmission occupies between 22 MHz of bandwidth, with only 5 MHz of passband bandwidth separating each of the 802.11b carrier channels. The DSSS transmission results in a 10Mhz bleed-through on either side of the CF. That limits 802.11B to three non-overlapping channels (1,6, and 11) spaced 25 MHz apart, limiting infrastructure AP deployments to three discrete access points within range to one another.

- 802.11a uses Orthogonal Frequency Division Multiplexing (OFDM). OFDM works by dividing the data transmission into multiple bit streams. The bit streams are then transmitted over parallel narrowband carriers or sub-carriers, carved out of the available channel bandwidth. The receiver reconstructs the sub-carrier into the original transmission signal. The 802.11a IEEE specification for OFDM defines 52 sub-carriers, 48 of which carry data, the remaining four carriers carry pilot data.
- The IEEE protocol defines eight data transmission rates for 802.11a. Transmission rates of 6, 12 and 20 Mbps are mandatory. Support for 9, 18, 36, 48 and 54 Mbps transmission rates are optional, but are supported on most vendor's products. To accommodate the different transmission rates, 802.11a utilizes different modulation schemes. 802.11a does not utilize a chipping code, like 802.11b. OFDM is far more resistant to interference then DSSS. The lower 802.11a transmission rates use modulation schemes we covered in the 802.11b overview. BPSK modulation is used to transmit data at 6 and 9 Mbps transmission rates. QPSK modulation is used for transmission rates running at 12 and 18 Mbps. For the higher speed transmission rates, 24 thru 54 Mbps Quadrature Amplitude Modulation (QAM) is used. QAM is a digital frequency modulation technique that represents data as phase and amplitude symbols, each representing 4 data bits. 16-QAM, which supports 16 symbols is used for the 24 through 48 Mbps transmission rates. 64-QAM is used for 54 Mbps (and on some vender implementations 48 Mbps) transmissions.
- 802.11a operates using 300MHz of bandwidth in the 5Ghz Unlicensed National Information Infrastructure (U-NII) RF spectrum. The 300 MHz of bandwidth is sub-divided in three 100

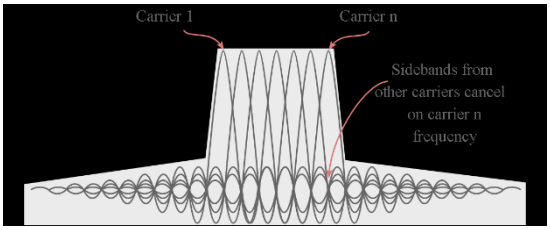
Mhz domains, each with different maximum operating power. The first 200 MHz is contiguous, operating between 5.200 GHz to 5.320. The 5.200 to 5.240 supports 50 mW max output, and 5.260 to 5.320 runs up to 250 mW. The last 100 MHz operates between 5.745 and 5.805 GHz, with a maximum output power of 1W. Each domain has four non-overlapping 20 MHz bandwidth channels, each of which can be utilized for transmission (unlike 802.11b, where the available channels bleed over one another).

17. Discuss orthogonal frequency division multiplexing (OFDM) and how it is useful in WLAN

- OFDM is a form of multicarrier modulation. An OFDM signal consists of a number of closely spaced modulated carriers. When modulation of any form - voice, data, etc. is applied to a carrier, then sidebands spread out either side. It is necessary for a receiver to be able to receive the whole signal to be able to successfully demodulate the data. As a result when signals are transmitted close to one another they must be spaced so that the receiver can separate them using a filter and there must be a guard band between them. This is not the case with OFDM. Although the sidebands from each carrier overlap, they can still be received without the interference that might be expected because they are orthogonal to each another. This is achieved by having the carrier spacing equal to the reciprocal of the symbol period.

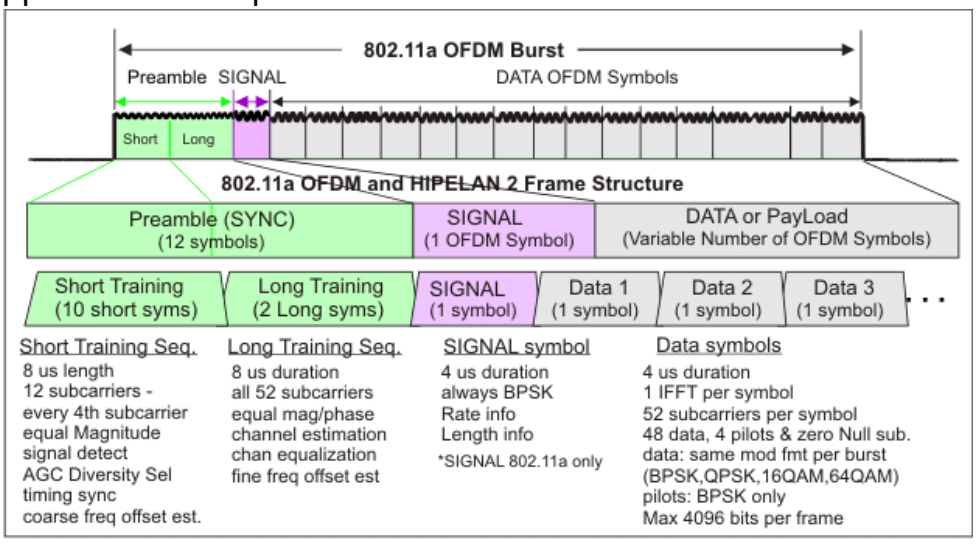


- To see how OFDM works, it is necessary to look at the receiver. This acts as a bank of demodulators, translating each carrier down to DC. The resulting signal is integrated over the symbol period to regenerate the data from that carrier. The same demodulator also demodulates the other carriers. As the carrier spacing equal to the reciprocal of the symbol period means that they will have a whole number of



cycles in the symbol period and their contribution will sum to zero in other words there is no interference contribution.

- One requirement of the OFDM transmitting and receiving systems is that they must be linear. Any non-linearity will cause interference between the carriers as a result of inter-modulation distortion. This will introduce unwanted signals that would cause interference and impair the orthogonality of the transmission.
- In terms of the equipment to be used the high peak to average ratio of multi-carrier systems such as OFDM requires the RF final amplifier on the output of the transmitter to be able to handle the peaks whilst the average power is much lower, and this leads to inefficiency. In some systems the peaks are limited. Although this introduces distortion that results in a higher level of data errors, the system can rely on the error correction to remove them.
- The basic frame structure of an 802.11a burst contains a preamble field followed by a SIGNAL field and multiple data fields. At the start of the burst, a preamble is transmitted at a well-known magnitude and phase. The preamble is used for synchronization and channel equalization. The SIGNAL field (not used in HIPERLAN 2 signals) is transmitted using BPSK, and contains the length, modulation type, and data rate information. Then multiple OFDM symbols containing the input data bits are appended to complete the burst.

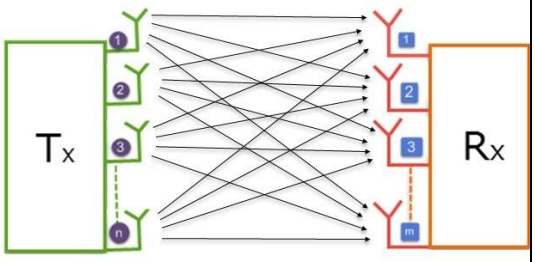


802.11a and HIPERLAN/2 Frame Structure

- It is used to solve problem of multi path fading in WLAN.

18. what is (MIMO) and how can we make use of it.

- MIMO: Multiple Input Multiple Output.
- Use of multiple antennas in both TX and RX.
    - Spatial Multiplexing: Split data across antenna (each antenna sends different data) increase rate.
    - Diversity: Send multiple copies of same data (each antenna same data) to ensure correct reception lower BER.



2. Problem 2: Questions Related to the Experiment

1. for WLAN module in our experiment what is the type of antenna in it?
    - The MRF24WB0MA has an integrated PCB antenna.
    - The antenna is tuned to have FR4 PCB material underneath the module.

2. How can we set the network name?
    -
```
char strSSID[13] = "Ahmed50";
```
    - Change to “MaKamal”
    -
```
char strSSID[13] = "MaKamal";
char channels[11]  = {1, 2, 3,
```

3. How can we change the channel number we use to transmit?
    -
```
char channels[11]  = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11};
```
    - Change to channel 5
    -
```
char channels[11]  = {5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5};
```

4. How can we change the mode of WLAN in our Experiment from Infrastructure to Ad-hoc?
    - Open CMD
    - Write this command: >> netsh wlan set profileparameter strSSID connectiontype=ibss
    -
```
>netsh wlan set profileparameter MaKamal connectiontype=ibss
```

3. Problem 3: Mini-Simulations

3.1. Code

```
clc; clear all; close all;
%% Initialization
Frames = 1000; %Number of Frames
fft_size = 128; %FFT Size (Number of subcarriers)
M = 16; K = log2(M); %16-QAM Modulation
delta = 312.5*10^(3); %Carrier Separation
delay_spread = 0.2*10^(-6); %Delay Spread
SNRdb = 0:3:30; %SNR Range in dB
delay_spread_max = delay_spread*fft_size*delta; %Number of paths
msg_size_bits = K*fft_size;
msg_size_symbols = msg_size_bits/K;
BER = zeros(length(SNRdb),Frames);
BER_avg = zeros(length(SNRdb),1);
%%
for i = 1:length(SNRdb)
for k = 1:Frames
%% Message Generation
msg_bits=randi([0,1],msg_size_symbols,K);
msg = bi2de(msg_bits,'left-msb')';
%% QAM Modulation
X = qammod(msg,M,'UnitAveragePower',true);
%% IFFT
x = sqrt(fft_size).*ifft(X);
%% ADD Cyclic Prefix
CP = x(128-31:128);
msg_CP = [CP x];
%% Channel (fading + noise)
[fadedSamples, gain] =ApplyFading(msg_CP,1,delay_spread_max);
msg_rx=awgn(fadedSamples,SNRdb(i),'measured');
%% Cyclic prefix removal
Y = msg_rx(33:160);
%% Freq domain equalization
Y_ = fft(Y)./sqrt(fft_size);
Z = Y_./fft(gain,128);
%% QAM Demodulation
msg_demod = qamdemod(Z,M,'UnitAveragePower',true);
msg_demod_bits  = de2bi(msg_demod,4,'left-msb');
%% BER calculation
[~,BER(i,k)] = biterr(msg_demod_bits,msg_bits);
BER_avg(i) = sum(BER(i,:))./Frames;
end
end
%% Plotting BER vs. SNR
figure
semilogy(SNRdb',BER_avg)
title('BER vs. SNR for 16-QAM with fading');
xlabel('SNR(dB)')
ylabel('BER')


```

3.2. Plots

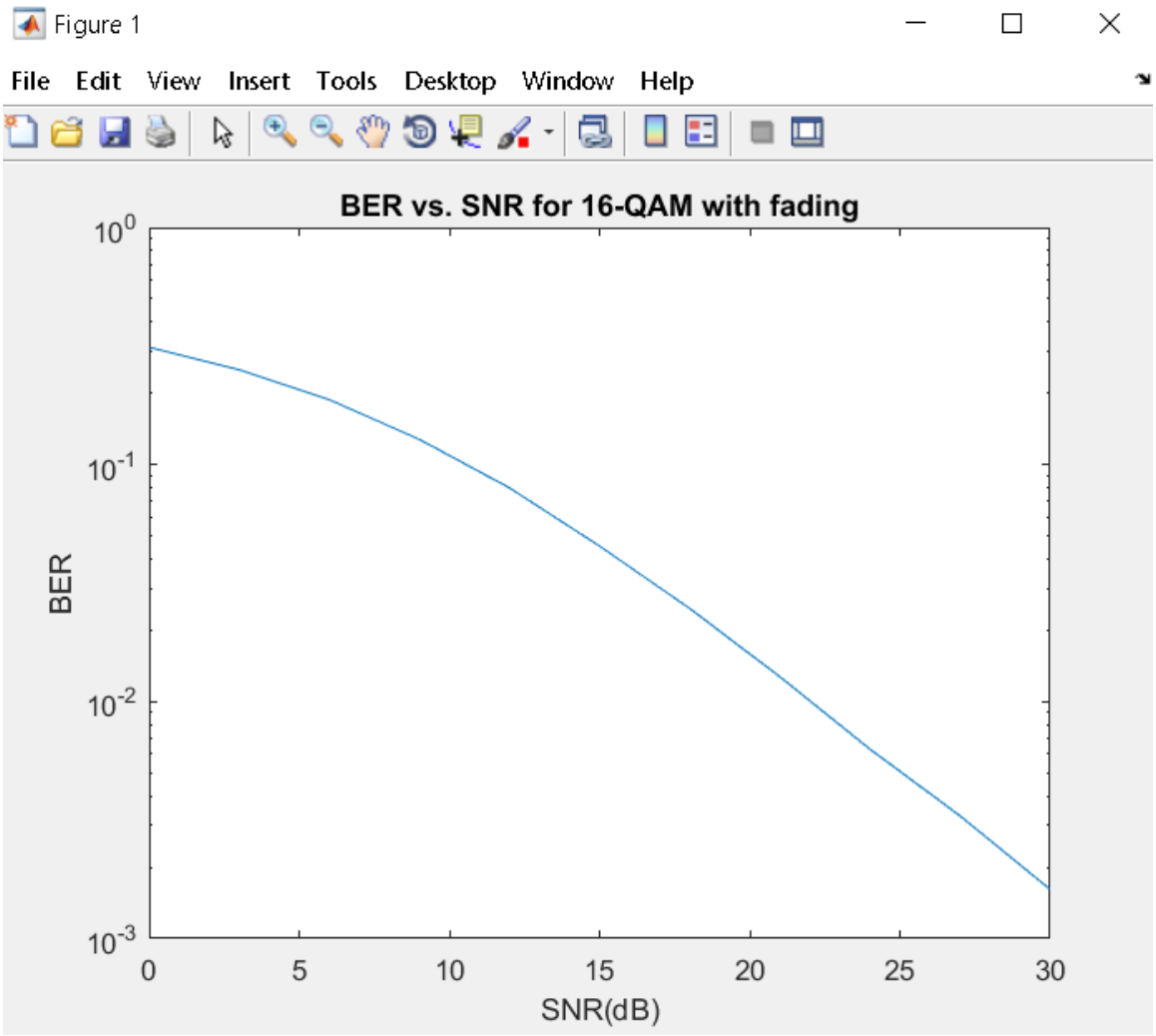


Figure 1
File Edit View Insert Tools Desktop Window Help
BER vs. SNR for 16-QAM with fading
BER
SNR(dB)
10^0
10^-1
10^-2
10^-3
0
5
10
15
20
25
30