Subject Name: Mobile Computing and Wireless Communication
Subject Code: 3170710

Faculties: Ms. Alpa Rupala

CHAPTER NO -4:
Wi-Fi and the IEEE 802.11 Wireless LAN Standard:

DESCRIPTIVE QUESTIONS

1. Explain IEEE 802.11 standards in details. **(Winter-2015)[L.J.I.E.T]** 7

The 802.11 standard is defined through several specifications of WLANs. It defines an over-the-air interface between a wireless client and a base station or between two wireless clients.

There are several specifications in the 802.11 family −

- **802.11 −** This pertains to wireless LANs and provides 1 or 2Mbps transmission in the 2.4-GHz band using either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS).
- **802.11a −** This is an extension to 802.11 that pertains to wireless LANs and goes as fast as 54 Mbps in the 5-GHz band. 802.11a employs the orthogonal frequency division multiplexing (OFDM) encoding scheme as opposed to either FHSS or DSSS.
- **802.11b −** The 802.11 high rate WiFi is an extension to 802.11 that pertains to wireless LANs and yields a connection as fast as 11 Mbps transmission (with a fall back to 5.5, 2, and 1 Mbps depending on strength of signal) in the 2.4-GHz band. The 802.11b specification uses only DSSS. Note that 802.11b was actually an amendment to the original 802.11 standard added in 1999 to permit wireless functionality to be analogous to hard-wired Ethernet connections.
- **802.11g −** This pertains to wireless LANs and provides 20+ Mbps in the 2.4-GHz band. Introducing new modulation schemes, forward error correction and OFDM also allows for higher data rates at 2.4 GHz. This approach should be backward compatible to 802.11b and should benefit from the better propagation characteristics at 2.4 GHz compared to 5 GHz. Currently, chips for 54 Mbit/s are available as well as first products. An alternative (or additional) proposal for 802.11g suggests the so called packet binary convolutional coding (PBCC) to reach a data rate of 22 Mbit/s. While the 54 Mbit/s OFDM mode is mandatory, the 22 Mbit/s PBCC mode can be used as an option.
- **802.11e (MAC enhancements):** Currently, the 802.11 standards offer no quality of service in the DCF operation mode. For applications such as audio, video, or media stream, distribution service classes have to be provided. For this reason, the MAC layer must be enhanced compared to the current standard.

- **802.11f (Inter-Access Point Protocol):** The current standard only describes the basic architecture of 802.11 networks and their components. Seamless roaming between access points of different vendors is often impossible. 802.11f standardizes the necessary exchange of information between access points to support the functions of a distribution system.

- **802.11h (Spectrum managed 802.11a):** The 802.11a standard was primarily designed for usage in the US U-NII bands. The standardization did not consider non-US regulations such as the European requirements for power control and dynamic selection of the transmit frequency. To enable the regulatory acceptance of 5 GHz products, dynamic channel selection (DCS) and transmit power control (TPC) mechanisms (as also specified for the European HiperLAN2 standard) have been added. With this extension, 802.11a products can also be operated in Europe. These additional mechanisms try to balance the load in the 5 GHz band.

- **802.11i (Enhanced Security mechanisms):** As the original security mechanisms (WEP) proved to be too weak soon after the deployment of the first products (Borisov, 2001), this working group discusses stronger encryption and authentication mechanisms. IEEE 802.1x will play a major role in this process.

2. List all and explain any five IEEE 802.11 services. **[New] (Nov-2016) [L.J.I.E.T]** 7

- IEEE 802.11 defines nine services that need to be provided by the wireless LAN to provide functionality equivalent to that which is inherent to wired LANs.

IEEE 802.11 Services

Service	Provider	Used to support
Association	Distribution System	MSDU delivery
Authentication	Station/AP	LAN access and security
Deauthentication	Station/AP	LAN access and security
Disassociation	Distribution System	MSDU delivery
Distribution	Distribution System	MSDU delivery
Integration	Distribution System	MSDU delivery
MSDU delivery	Station/AP	MSDU delivery
Privacy	Station/AP	LAN access and security
Reassociation	Distribution System	MSDU delivery

MSDU – MAC Service Data Unit

Association Related Services:

- The primary purpose of the MAC layer is to transfer MSDUs between MAC entities; this purpose is fulfilled by the distribution service.
- For that service to function, it requires information about stations within the ESS, which is provided by the association-related services.
- Before the distribution service can deliver data to or accept data from a station, that station must

be associated. Before looking at the concept of association, we need to describe the concept of mobility.

- The standard defines three transition types based on mobility:
  - **No transition:** A station of this type is either stationary or moves only within the direct communication range of the communicating stations of a single BSS.
  - **BSS transition:** This is defined as a station movement from one BSS to another BSS within the same ESS. In this case, delivery of data to the station requires that the addressing capability be able to recognize the new location of the station.
  - **ESS transition:** This is defined as a station movement from a BSS in one ESS to a BSS within another ESS.
  - This case is supported only in the sense that the station can move. Maintenance of upper-layer connections supported by 802.11 cannot be guaranteed. In fact, disruption of service is likely to occur.
- To deliver a message within a DS, the distribution service needs to know where the destination station is located.
- Specifically, the DS needs to know the identity of the AP to which the message should be delivered in order for that message to reach the destination station.
- To meet this requirement, a station must maintain an association with the AP within its current BSS. Three services relate to this requirement:
  - **Association**: Establishes an initial association between a station and an AP Before a station can transmit or receive frames on a wireless LAN, its identity and address must be known.
  - For this purpose, a station must establish an association with an AP within a particular BSS. The AP can then communicate this information to other APs within the ESS to facilitate routing and delivery of addressed frames.
  - **Reassociation**: Enables an established association to be transferred from one AP to another, allowing a mobile station to move from one BSS to another.
  - **Disassociation**: A notification from either a station or an AP that an existing association is terminated.
  - A station should give this notification before leaving an ESS or shutting down. However, the MAC management facility protects itself against stations that disappear without notification.

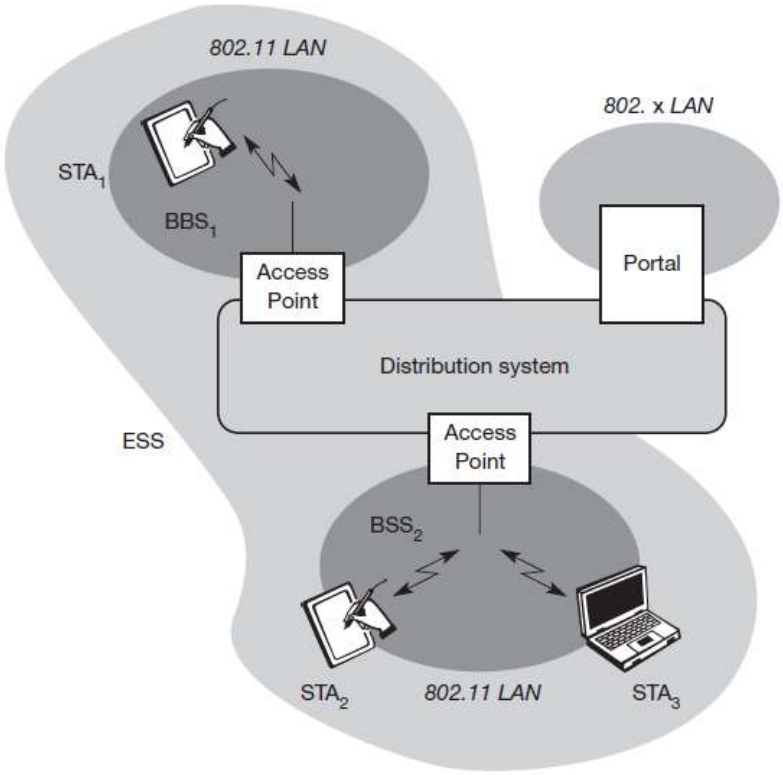
Access and Privacy Services:

- There are two characteristics of a wired LAN that are not inherent in a wireless LAN.

1. In order to transmit over a wired LAN, a station must be physically connected to the LAN. On the other hand, with a wireless LAN, any station within radio range of the other devices on the LAN can transmit. In a sense, there is a form of authentication with a wired LAN, in that it requires some positive and presumably observable action to connect a station to a wired LAN.
2. Similarly, in order to receive a· transmission from a station that is part of a wired LAN, the receiving station must also be attached to the wired LAN. On the other hand, with a wireless LAN, any station within radio range can receive. Thus, a wired LAN provides a degree of privacy, limiting reception of data to stations connected to the LAN.

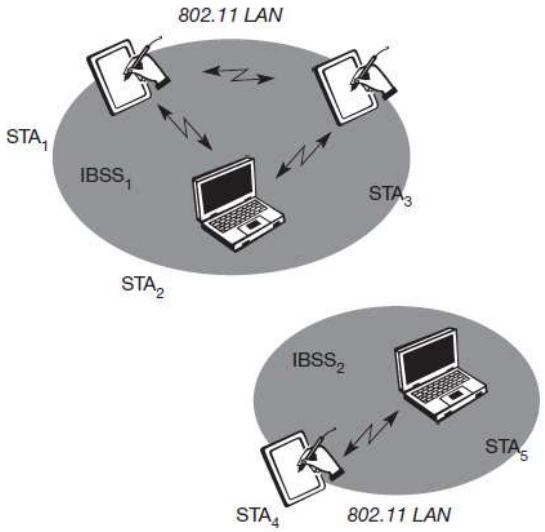
	• IEEE 802.11 defines three services that provide a wireless LAN with these two features: **Authentication**: • Used to establish the identity of stations to each other. In a wired LAN, it is generally assumed that access to a physical connection conveys authority to connect to the LAN. • This is not a valid assumption for a wireless LAN, in which connectivity is achieved simply by having an attached antenna that is properly tuned. • The authentication service is used by stations to establish their identity with stations they wish to communicate with IEEE 802.11 supports several authentication schemes and allows for expansion of the functionality of these schemes. • The standard does not mandate any particular authentication scheme, which could range from relatively unsecure handshaking to public key encryption schemes. • However, IEEE 802.11 requires mutually acceptable, successful authentication before a station can establish an association with an AP. **Deauthentication**: • This service is invoked whenever an existing authentication is to be terminated. **Privacy:** • Used to prevent the contents of messages from being read by other than the intended recipient. The standard provides for the optional use of encryption to assure privacy.	
3.	Draw and Explain the IEEE 802.11 Architecture in Details? **(May-2017)[L.J.I.E.T]** Explain IEEE 802.11 Architecture. **(Nov-2017)[L.J.I.E.T]** Explain the IEEE 802.11 Architecture with the neat diagram. **(May-2018)[L.J.I.E.T]** Explain Wireless LAN standards and Wireless LAN architecture**(Summer-2014) (Summer-2015) [L.J.I.E.T** • Wireless networks can exhibit two different basic system architectures infrastructure-based or ad-hoc. **Infrastructure based:** • Figure 1 shows the components of an infrastructure and a wireless part as specified for IEEE 802.11. Several nodes, called stations (STAi), are connected to access points (AP). • Stations are terminals with access mechanisms to the wireless medium and radio contact to the AP. • The stations and the AP which are within the same radio coverage form a basic service set (BSSi). The example shows two BSSs – BSS1 and BSS2 – which are connected via a distribution system. A distribution system connects several BSSs via the AP to form a single network and thereby extends the wireless coverage area. • This network is now called an extended service set (ESS) and has its own identifier, the ESSID. The ESSID is the 'name' of a network and is used to separate different networks. Without knowing the ESSID (and assuming no hacking) it should not be possible to participate in the WLAN. • The distribution system connects the wireless networks via the APs with a portal, which forms the interworking unit to other LANs. • The architecture of the distribution system is not specified further in IEEE 802.11. It could consist of bridged IEEE LANs, wireless links, or any other networks.	7, 4, 4

- However, distribution system services are defined in the standard (although, many products today cannot interoperate and needs the additional standard IEEE 802.11f to specify an inter access point protocol).
- Stations can select an AP and associate with it. The APs support roaming (i.e., changing access points), the distribution system handles data transfer between the different APs. APs provide synchronization within a BSS, support power management, and can control medium access to support time-bounded service.



Ad-hoc based:

- In addition to infrastructure-based networks, IEEE 802.11 allows the building of ad-hoc networks between stations, thus forming one or more independent BSSs (IBSS) as shown in Figure 2.
- In this case, an IBSS comprises a group of stations using the same radio frequency. Stations STA1, STA2, and STA3 are in IBSS1, STA4 and STA5 in IBSS2.
- This means for example that STA3 can communicate directly with STA2 but not with STA5. Several IBSSs can either be formed via the distance between the IBSSs (see Figure) or by using different carrier frequencies (then the IBSSs could overlap physically).
- IEEE 802.11 does not specify any special nodes that support routing, forwarding of data or exchange of topology information as, e.g., HIPERLAN 1 or Bluetooth.



4. **Explain MAC Layer in WLAN.**

Medium Access Control.

- The 802.11 working group considered two types of proposals for a MAC algorithm:
  1. Distributed access protocols, which, like Ethernet, distribute the decision to transmit over all the nodes using a carrier sense mechanism; and
  2. Centralized access protocols, which involve regulation of transmission by a centralized decision maker.

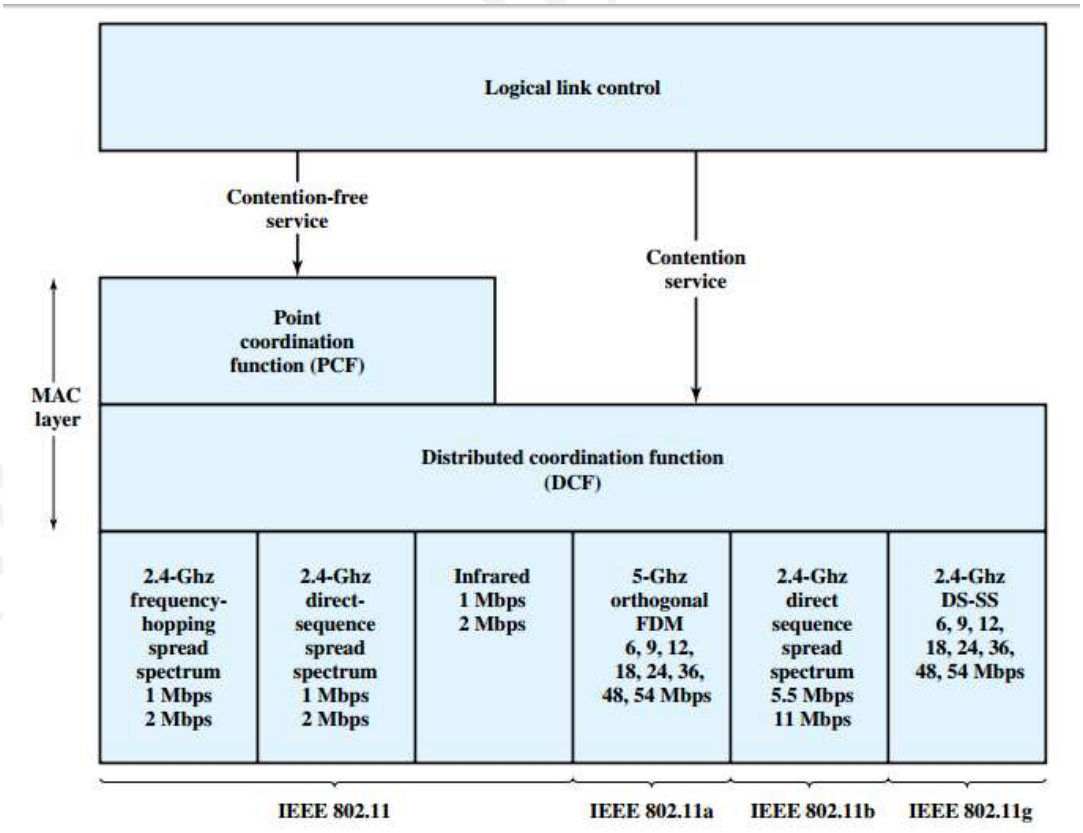


Figure 17.5 IEEE 802.11 Protocol Architecture

	• A distributed access protocol makes sense for an ad hoc network of peer workstations (typically an IBSS) and may also be attractive in other wireless LAN configurations that consist primarily of bursty traffic. • A centralized access protocol is natural for configurations in which a number of wireless stations are interconnected with each other and some sort of base station that attaches to a backbone wired LAN; it is especially useful if some of the data is time sensitive or high priority. • The end result for 802.11 is a MAC algorithm called DFWMAC (distributed foundation wireless MAC) that provides a distributed access control mechanism with an optional centralized control built on top of that. • Figure 17.5 illustrates the architecture. The lower sublayer of the MAC layer is the distributed coordination function (DCF). • DCF uses a contention algorithm to provide access to all traffic. Ordinary asynchronous traffic directly uses DCF. • The point coordination function (PCF) is a centralized MAC algorithm used to provide contention-free service. PCF is built on top of DCF and exploits features of DCF to assure access for its users.	
5.	Discuss with suitable diagram distributed coordination function with IEEE 802.11 medium access control logic. **[New] (Nov-2016) [L.J.I.E.T]** • Distributed Coordination Function the DCF sublayer makes use of a simple CSMA (carrier sense multiple access) algorithm. • If a station has a MAC frame to transmit, it listens to the medium. If the medium is idle, the station may transmit; otherwise the station must wait until the current transmission is complete before transmitting. • The DCF does not include a collision detection function (i.e., CSMA/CD) because collision detection is not practical on a wireless network. • The dynamic range of the signals on the medium is very large, so that a transmitting station cannot effectively distinguish incoming weak signals from noise and the effects of its own transmission. • To ensure the smooth and fair functioning of this algorithm, DCF includes a set of delays that amounts to a priority scheme. • Let us start by considering a single delay known as an Inter frame space (IFS). • In fact, there are three different IFS values, but the algorithm is best explained by initially ignoring this detail. • Using an IFS, the rules for CSMA access are as follows (Figure 17.6): • A station with a frame to transmit senses the medium. If the medium is idle, it waits to see if the medium remains idle for a time equal to IFS. If so, the station may transmit immediately. • If the medium is busy (either because the station initially finds the medium busy or because the medium becomes busy during the IFS idle time), the station defers transmission and continues to monitor the medium until the current transmission is over. • Once the current transmission is over, the station delays another IFS. If the medium remains idle for this period, then the station backs off a random amount of time and again senses the medium. If the medium is still idle, the station may transmit. During the backoff time, if the medium becomes busy, the backoff timer is halted and resumes when the medium becomes idle. • If the transmission is unsuccessful, which is determined by the absence of an acknowledgement, and then it is assumed that a collision has occurred. • To ensure that backoff maintains stability, binary exponential backoff. • Binary exponential backoff provides a means of handling a heavy load. Repeated failed attempts to transmit result in longer and longer backoff times, which helps to smooth out the load.	7

- Without such a backoff, the following situation could occur: Two or more stations attempt to transmit at the same time, causing a collision. These stations then immediately attempt to retransmit, causing a new collision.
- The preceding scheme is refined for DCF to provide priority-based access by the simple expedient of using three values for IFS:
  - SIFS (short IFS): The shortest IFS, used for all immediate response actions, as explained in the following discussion
  - PIFS (point coordination function IFS): A mid length IFS, used by the centralized controller in the PCF scheme when issuing polls
  - DIFS (distributed coordination function IFS): The longest IFS, used as a minimum delay for asynchronous frames contending for access.
- Figure 17.7a illustrates the use of these time values. Consider first the SIFS. Any station using SIFS to determine transmission opportunity has, in effect, the highest priority, because it will always gain access in preference to a station waiting an amount of time equal to PIFS or DIFS.

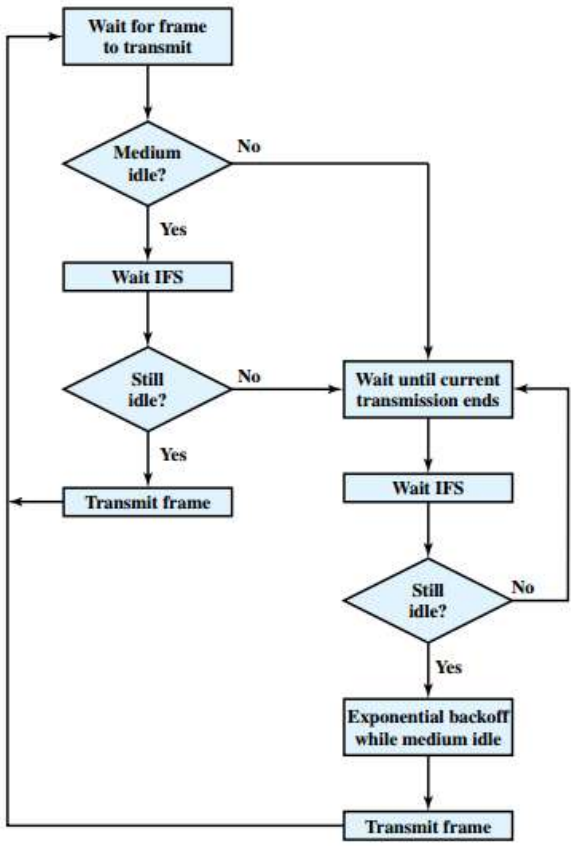


Figure 17.6 IEEE 802.11 Medium Access Control Logic

- The SIFS is used in the following circumstances:
  - **Acknowledgment (ACK):** When a station receives a frame addressed only to itself (not multicast or broadcast), it responds with an ACK frame after waiting only for an SIFS gap. This has two desirable effects. First, because collision detection is not used, the likelihood of collisions is greater than with CSMA/CD, and the MAC-level ACK provides for efficient collision recovery. Second, the SIFS can be used to provide efficient delivery of an LLC protocol data unit (PDU) that requires multiple MAC frames. In this case, the following scenario occurs. A station with a multi frame LLC PDU to transmit sends out the MAC frames one at a time. Each frame is acknowledged by the recipient after SIFS. When the source receives an ACK, it immediately (after SIFS) sends the next frame in

the sequence. The result is that once a station has contended for the channel, it will maintain control of the channel until it has sent all of the fragments of an LLC PDU.

- **Clear to Send (CTS):** A station can ensure that its data frame will get through by first issuing a small Request to Send (RTS) frame. The station to which this frame is addressed should immediately respond with a CTS frame if it is ready to receive. All other stations receive the RTS and defer using the medium.
- **Poll response:** This is explained in the following discussion of PCF. The next longest IFS interval is the PIFS. This is used by the centralized controller in issuing polls and takes precedence over normal contention traffic. However, those frames transmitted using SIFS have precedence over a PCF poll.

Finally, the DIFS interval is used for all ordinary asynchronous traffic.

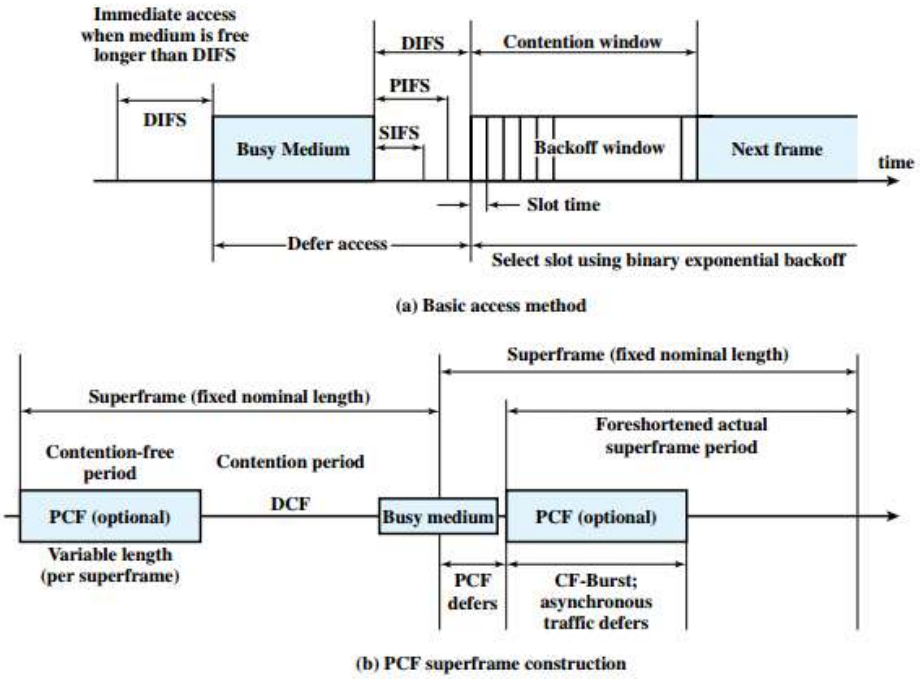


Figure 17.7 IEEE 802.11 MAC Timing

6. List and explain different types of wireless LAN. **[New](Dec-2013) [L.J.I.E.T]** 7
List types of wireless LAN. **[New] (May-2015)[L.J.I.E.T]** ,
There are different types of WLAN. 4

1. **IEEE 802.11:** In June 1997, the IEEE finalized the initial specification for wireless LANs: IEEE 802.11. This standard specifies a 2.4 GHz frequency band with data rate of 1 Mbps and 2 Mbps. This standard evolved into many variations of the specification like 802.11b, 802.11a, and 802.11g etc. using different encoding technologies. Local area network of bandwidths doing up to a maximum of 54Mbps.

2. **HyperLAN:** HyperLAN began in Europe as a specification ratified in 1996 by the ETSI Broadband Ratio Access Network Group. HyperLAN/1, the current version works at the 5GHz band and offers up to 24 MBps bandwidth. Next version HyperLAN/2 will support a bandwidth of 54 Mbps with QoS support. This will be able to carry Ethernet frames, ATM cells, IP packet and support data, voice, voice and image.

3. **HomeRF:** In 1998, the HomeRF Working Group offered to provide an industry specification to offer Shared Wireless Access Protocol (SWAP). This standard will offer interoperability between PC and consumer electronic devices within the home. SWAP uses frequency hopping spread spectrum modulation and offer 1 Mbps and 2 Mbps at 2.4GHz frequency band.

	4. **Bluetooth:** Bluetooth was promoted by big industry leaders like IBM, Ericsson, Intel, Lucent, 3Com, Microsoft, Nokia, Motorola, and Toshiba. It was named after Harold Bluetooth, King of Denmark during 952 to 995 A.D., who had a vision of a world with cooperation and interoperability. Bluetooth is more of a wireless Personal Area Network (PAN) operating at 2.4 GHz band and offers 1Mbps data rate. Bluetooth uses frequency hopping spread-spectrum modulation with relatively low power and smaller range (about 10 meters). 5. **MANET:** MANET is a working group within the IETF to investigate and develop the standard for Mobile ad-hoc NETworks.	
7.	Mention some of the advantages and dis advantages of WLANS? Mention the design goals of WLANS? **(Nov-2011)[L.J.I.E.T]** Explain Wireless LAN standards and Wireless LAN architecture**(Summer-2014) (Summer-2015) [L.J.I.E.T]** What re the advantages and disadvantages of wireless LAN? Under what situation is a wireless LAN desirable over wired LAN? **(Dec-2012)[L.J.I.E.T]** Describe Wireless LAN advantages. Also explain mobility in wireless LAN. **(Winter-2014) [L.J.I.E.T]** • Wireless is a local area data network without any physical connectivity like without wires. • WLAN is implemented as an extension to a wired LAN within a building or campus. • Wireless LAN is referred as Wireless Fidelity(Wi-Fi) • Typically restricted in their diameter: buildings, campus, single room etc... • The global goal is to replace office cabling and to introduce high flexibility for ad hoc communication (e.g. Group meetings). **Wireless LAN advantages:** • **Mobility:** WLAN offers wire-free access within operating range. • **Flexibility:** Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.). • **Design:** Wireless networks allow for the design of small, independent devices which can for example be put into a pocket. Cables not only restrict users but also designers of small PDAs, notepads etc. Wireless senders and receivers can be hidden in historic buildings, i.e., current networking technology can be introduced without being visible. • **Low Implementation Costs:** WLAN is easy to setup, relocate, change and low cost. • **Quicker deployment:** It is easier to add or move subscribers or workstations. • **Installation Speed and Simplicity:** Fast and simple installation of WLAN. It reduces the need of LAN wiring through ceiling and walls. • **Network Expansion:** Easy expansion of WLAN possible. • **Higher Flexibility**: within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls. • **Planning**: Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans. • **Robustness**: wireless networks can survive disasters; if the wireless devices survive people can still communicate. • **Increased Productivity**: They have a direct impact on increase in productivity because of minimum set up requirement and centralised access to the system databases.	7

Wireless LAN disadvantages

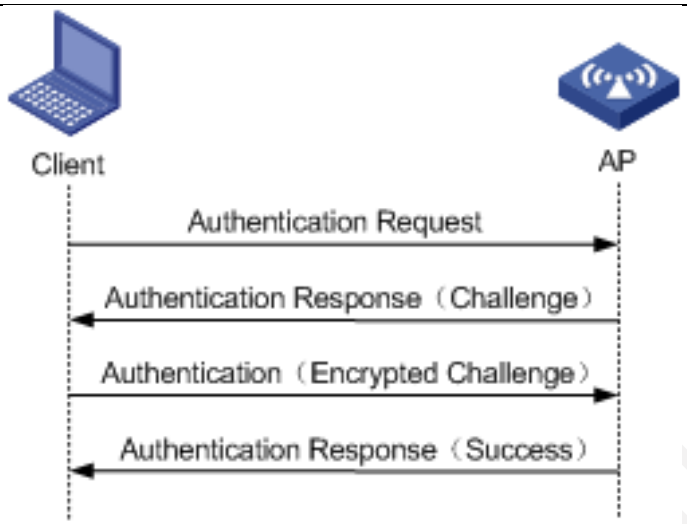
- **QoS**: WLANs typically offer lower quality than their wired counterparts. The main reasons for this are the lower bandwidth due to limitations in radio transmission (e.g., only 1–10 Mbit/s user data rate instead of 100–1,000 Mbit/s), higher error rates due to interference (e.g., 10–4 instead of 10–12 for fiber optics), and higher delay/delay variation due to extensive error correction and detection mechanisms.
- **Cost**: Ethernet adapter vs. wireless LAN adapters.
- **Proprietary solutions**: Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardized functionality plus many enhanced features (typically a higher bit rate using a patented coding technology or special inter-access point protocols).
- **Restrictions:** All wireless products have to comply with national regulations. Several government and non-government institutions worldwide regulate the operation and restrict frequencies to minimize interference. Consequently, it takes a very long time to establish global solutions like, e.g., IMT-2000, which comprises many individual standards. WLANs are limited to low-power senders and certain license-free frequency bands, which are not the same worldwide.
- **Safety and security**: using radio waves for data transmission might interfere with other high-tech equipment.

Wireless LAN: Main Design Goals

- **Global operation**: LAN equipment may be carried from one country to another and this operation should be legal (frequency regulations national and international).
- **Low power**: take into account that devices communicating via WLAN is typically running on battery power. Special power saving modes and power management functions.
- **Simplified spontaneous co-operation**: no complicated setup routines but operate spontaneously after power.
- **Robust transmission technology:** Compared to their wired counterparts, WLANs operate under difficult conditions. If they use radio transmission, many other electrical devices can interfere with them (vacuum cleaners, hairdryers, train engines etc.). WLAN transceivers cannot be adjusted for perfect transmission in a standard office or production environment. Antennas are typically omnidirectional, not directed. Senders and receivers may move.
- **License-free operation:** LAN operators do not want to apply for a special license to be able to use the product. The equipment must operate in a license-free band, such as the 2.4 GHz ISM band.
- **Easy to use**: WLANs are made for simple users; they should not require complex management but rather work on a plug-and-play basis.
- **Protection of investment**: a lot of money has been invested for wired LANs; WLANs should be able to interoperate with existing network (same data type and services).
- **Safety and security**: safe to operate. Encryption mechanism, do not allow roaming profiles for tracking people (privacy)
- **Transparency for applications**: existing applications should continue to work.

8.	How are mobility and handoff managed in wireless LAN? **(Dec-2012)[L.J.I.E.T]**	7

9.	How authentication is possible in wireless LAN? List and discuss the possible attacks on such networks. **[New] (June-2014)[L.J.I.E.T]** Many access point support MAC address filtering. This is similar to IPFiltering. The AP manages a list of MAC addresses that are allowed or disallowed in the wireless network. The idea is that the MAC address of the network card is unique and static. By controlling the access from known addresses, the administrator can allow or restrict the access of network only to known client. **Authentication Mode:** Two types of client authentication are defined in 802.11: 1. Open system authentication: It is no authentication at all. 2. Shared Key Authentication: It is based on the fact that both stations taking part in the authentication have the same "Shared" Key. • It is assumed that this key has been transmitted to both stations through some secure channel other than the wireless media itself. In typical implementation, this is set manually on the client station and the AP. The Authenticating station receives a challenge text packet (Created using the WEP Pseudo Random Number Generator (PRNG)) from the AP. The station encrypts this PRNG using shared key, and sends it back to the AP. • If, after decryption, the challenge text matches, then one-way authentication is successful. To obtain mutual authentication, the process is repeated in the opposite direction. **WEP (Wired Equivalent Privacy):** • WEP was designed to protect users of a WLAN from casual eavesdropping and was intended to offer following facilities: • **Reasonably strong encryption:** It relies on the difficulty of recovering the secret key through a brute force attack. The difficulty grows with the key length. • **Self-synchronizing:** Each packet contains the information required to decrypt it. There is no need to deal with lost packets. • **Efficient:** It can be implemented in software with reasonable efficiency. • **Exportable:** Limiting the key length leads to a greater possibility of export beyond US. • The WEP algorithm is the RC4 cryptographic algorithm from RSA Data Security. RC4 uses stream cipher technique. It is a symmetric algorithm and uses the same key for both enciphering and deciphering the data. For each transmission, the plaintext is bitwise XORed with a pseudorandom keystream to produce cipher text. For decryption the process is reversed. • The algorithm operates as follows: 1. It is assumed that the secret key has been distributed to both the transmitting and receiving stations by some secure means. 2. On the transmitting station, the 40 bit secret key is concatenated with a 24 bit Initialization Vector (IV) to produce a seed for input into the WEP PRNG. 3. The seed is passed into the PRNG to produce a stream (Keystream) of pseudo random octets. 4. The plaintext PDU is then XORed with the pseudo random keystream to produce the cipher text PDU. 5. This cipher text PDU is then concatenated with the 24-bit IV and transmitted on the wireless media. 6. The receiving station reads the IV and concatenates it with the secret key, producing the seed that is passes to the PRNG. 7. The receiver's PRNG produces identical keystream used by the transmitting stations. When this PRNG is XORed with the cipher text, the original plain text PDU is produced.	7



- The plain text PDU is also protected with a CRC to prevent random tampering with the cipher text in transit.

Possible Attacks:

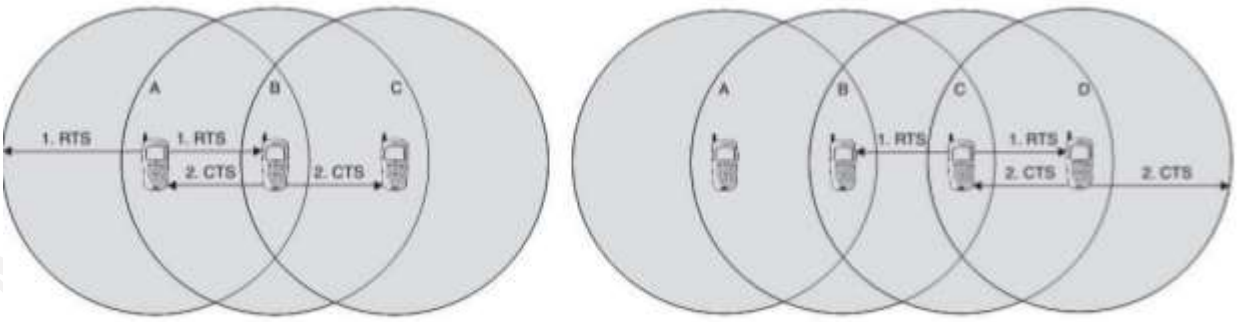
- **Passive attack:** To decrypt traffic based on statistical analysis.
- **Active attack:** To inject new traffic from unauthorized mobile stations, based on known plaintext
- **Active attacks:** To decrypt traffic, based on tricking the access point.
- **Dictionary-Building attack:** That, after analysis of about a day's worth of traffic, allows real time automated decryption of all traffic.
- **Hijacking a session:** Following successful authentication, it is possible to hijack the session.
- **Traffic Analysis:** In this type of attacks the attacker uses the statistics of network connectivity and activity to find information about the attacked network. Information includes: AP location, AP SSID and the type of protocol used by the analysis of size and types of packets
- **Unauthorized Access:** This type of attack is also known by many other names, such as war driving, war walking, and war flying. This is the most common attack type where the attacker tries to get access to a network that she is not authorized to access. Mainly the reason behind such attacks is just to get Internet access for free.
- **Man-in-the-middle Attacks:** In this attack, the attacker gets the packets before the intended receiver does. This allows her to change the content of the message. One of the most known subset of this attack is called ARP (Address Resolution Protocol) attacks, where the attacker redirects network traffic to pass through her device.
- **Replay Attacks:** In this type of attack the attacker uses the information from previous authenticated sessions to gain access to the network.
- **Rouge AP:** Some of the devices allow the user to declare itself as an AP. This will make people confused and sometimes they may connect to this false AP exposing their information to it. This can be solved by imposing mutual authentication between AP and network devices.
- **DoS Attacks:** DoS (Denial of Service) attacks are the hardest type of attacks to overcome. Attackers use frequency devices to send continuous noise on a specific channel to ruin network connectivity. It is known in the wireless world as RF Jamming

10	Explain Wireless LAN security issues and also explain hidden & exposed terminal problem in wireless LAN. **[New] (Winter-2012) [New](May-2016) [New](May-2018)[L.J.I.E.T]** List Wireless LAN security issues and What do you understand by hidden & exposed terminal problem in wireless LAN. **[New] (Dec-2014)[L.J.I.E.T]** Discuss security issues with wireless networks. **[New] (Dec-2015)[L.J.I.E.T]** Explain wireless LAN security. **[New](May-2018)[L.J.I.E.T]**	7, 7, 7

- Despite the productivity, convenience and cost advantage that WLAN offers, the radio waves used in wireless networks create a risk where the network can be hacked. This section explains three examples of important threats: Denial of Service, Spoofing, and Eavesdropping. , 7
  1. **Denial of Service:** In this kind of attack, the intruder floods the network with either valid or invalid messages affecting the availability of the network resources. Due to the nature of the radio transmission, the WLAN are very vulnerable against denial of service attacks. The relatively low bit rates of WLAN can easily be overwhelmed and leave them open to denial of service attacks. By using a powerful enough transceiver, radio interference can easily be generated that would unable WLAN to communicate using radio path. , 7 , 7
  2. **Spoofing and Session Hijacking:** This is where the attacker could gain access to privileged data and resources in the network by assuming the identity of a valid user. This happens because 802.11 networks do not authenticate the source address, which is Medium Access Control (MAC) address of the frames. Attackers may therefore spoof MAC addresses and hijack sessions. Moreover, 802.11 does not require an Access Point to prove it is actually an AP. This facilitates attackers who may masquerade as AP's. In eliminating spoofing, proper authentication and access control mechanisms need to be placed in the WLAN.
  3. **Eavesdropping**: This involves attack against the confidentiality of the data that is being transmitted across the network. By their nature, wireless LANs intentionally radiates network traffic into space. This makes it impossible to control who can receive the signals in any wireless LAN installation. In the wireless network, eavesdropping by the third parties is the most significant threat because the attacker can intercept the transmission over the air from a distance, away from the premise of the company.

Hidden Terminal and Exposed Terminal:

- The basic access mechanism, called Distributed Coordination Function in carrier sense Multiple Access with Collision Avoidance mechanism (CSMA/CA).
- CSMA protocols are well known, the most popular being the Ethernet, which is CSMA/CD protocol.
- In a Wired environment every station connected to the wire can sense the signal in the wire. In a wired LAN, if there is no activity or a collision of messages, every station connected to the LAN will be able to sense collection almost instantly. This is not true in the case of wireless media.



- In the case of wireless LANs, a Carrier Sense Multiple Access/ Collision Avoidance (CSMA/CA) protocol is used, as it is not possible to detect a collision of data packets in mid-air.
- Consider the scenario with three mobile nodes shown in figure (a). The transmission of A reaches B, but not C. The transmission of C reaches B, but not A.
- However, the radio signal of B reaches both A and C making both in the range of B. The net effect is A cannot detect C and vice versa.

- A start sending to B, C does not receive this transmission. C also wants to send to B and sense the medium. To C the medium appears to be free. Thus C starts sending causing collision at B. But now A cannot detect the collision and continues with its transmission. A is 'Hidden' for C and vice versa.
- In another case as shown in figure (b). The radio transmission signal of A reaches C and B.
- The radio signal of C reaches both A and D. A wants to communicate to B, A starts sending signal to B. C wants to communicate to D, C sense the carrier and finds that A is talking to B.
- C has to wait till the time A finishes with B. However, D is outside the range of A, therefore waiting is not necessary.
- In fact A, B and C, D can communicate to each other in parallel without any collision, but according to the protocol that is not possible.
- A and C are 'Exposed' terminals.

While Collision Detection mechanisms are a good idea on a wired LAN, they cannot be used on a wireless LAN environment for two main reasons:

1. Implementing a Collision Detection Mechanism requires the implementation of a Full Duplex radio capable of transmitting and receiving at the same time. This increases the cost significantly.
2. In a wireless environment we cannot assume that all stations will be able to receive radio signal from each other (which is the basic assumption of the Collision Detection scheme). The fact that a station wants to transmit and sense the medium as free (not able to sense signal from another station) does not necessarily mean that the medium is free (like the case of the hidden terminal) around the receiver area.

The mechanism behind CSMA/CA is as follows:

- Let us start by considering a single delay known as an Inter frame space (IFS).
- In fact, there are three different IFS values, but the algorithm is best explained by initially ignoring this detail.
- Using an IFS, the rules for CSMA access are as follows (Figure 17.6):
- A station with a frame to transmit senses the medium. If the medium is idle, it waits to see if the medium remains idle for a time equal to IFS. If so, the station may transmit immediately.
- If the medium is busy (either because the station initially finds the medium busy or because the medium becomes busy during the IFS idle time), the station defers transmission and continues to monitor the medium until the current transmission is over.
- Once the current transmission is over, the station delays another IFS. If the medium remains idle for this period, then the station backs off a random amount of time and again senses the medium. If the medium is still idle, the station may transmit. During the backoff time, if the medium becomes busy, the backoff timer is halted and resumes when the medium becomes idle.
- If the transmission is unsuccessful, which is determined by the absence of an acknowledgement, and then it is assumed that a collision has occurred.
- To ensure that backoff maintains stability, binary exponential backoff.
- Binary exponential backoff provides a means of handling a heavy load. Repeated failed attempts to transmit result in longer and longer backoff times, which helps to smooth out the load.
- Without such a backoff, the following situation could occur: Two or more stations attempt to transmit at the same time, causing a collision. These stations then immediately attempt to retransmit, causing a new collision.

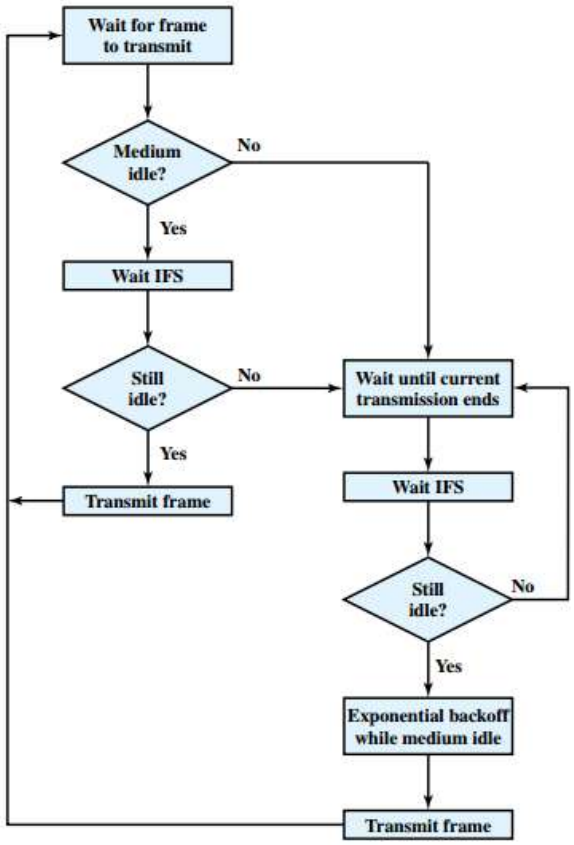


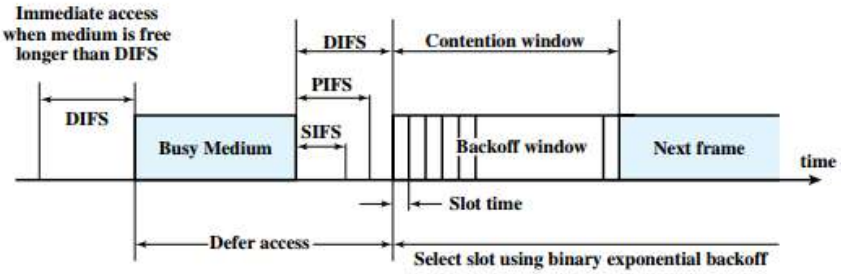
Figure 17.6 IEEE 802.11 Medium Access Control Logic

- The preceding scheme is refined for DCF to provide priority-based access by the simple expedient of using three values for IFS:
  - SIFS (short IFS): The shortest IFS, used for all immediate response actions, as explained in the following discussion
  - PIFS (point coordination function IFS): A mid length IFS, used by the centralized controller in the PCF scheme when issuing polls
  - DIFS (distributed coordination function IFS): The longest IFS, used as a minimum delay for asynchronous frames contending for access.
- Figure 17.7a illustrates the use of these time values. Consider first the SIFS. Any station using SIFS to determine transmission opportunity has, in effect, the highest priority, because it will always gain access in preference to a station waiting an amount of time equal to PIFS or DIFS.
- The SIFS is used in the following circumstances:
  - **Acknowledgment (ACK):** When a station receives a frame addressed only to itself (not multicast or broadcast), it responds with an ACK frame after waiting only for an SIFS gap. This has two desirable effects. First, because collision detection is not used, the likelihood of collisions is greater than with CSMA/CD, and the MAC-level ACK provides for efficient collision recovery. Second, the SIFS can be used to provide efficient delivery of an LLC protocol data unit (PDU) that requires multiple MAC frames. In this case, the following scenario occurs. A station with a multi frame LLC PDU to transmit sends out the MAC frames one at a time. Each frame is acknowledged by the recipient after SIFS. When the source receives an ACK, it immediately (after SIFS) sends the next frame in the sequence. The result is that once a station has contended for the channel, it will maintain control of the channel until it has sent all of the fragments of an LLC PDU.
  - **Clear to Send (CTS):** A station can ensure that its data frame will get through by first issuing a small Request to Send (RTS) frame. The station to which this frame is addressed

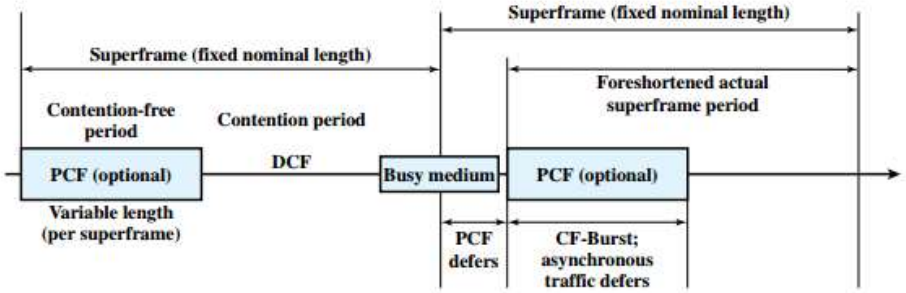
should immediately respond with a CTS frame if it is ready to receive. All other stations receive the RTS and defer using the medium.

- **Poll response:** This is explained in the following discussion of PCF. The next longest IFS interval is the PIFS. This is used by the centralized controller in issuing polls and takes precedence over normal contention traffic. However, those frames transmitted using SIFS have precedence over a PCF poll.

Finally, the DIFS interval is used for all ordinary asynchronous traffic.



(a) Basic access method



(b) PCF superframe construction

Figure 17.7 IEEE 802.11 MAC Timing

11 Compare Wifi Vs. 3G and also discuss wireless LAN security issues. **(Nov-2011)[L.J.I.E.T]** 7,
Describe the contrast between 3G and Wi-Fi technologies. **(Summer-2013) (Winter-2014) (Summer-2015) [L.J.I.E.T]**
Compare the WiFi and 3G Technologies. **[New] (May-2013)[L.J.I.E.T]** 7,
Discuss 3G versus Wifi **[New] (May-2015)[L.J.I.E.T]** 7,

Functions	3G	Wi-Fi
Genesis	Evolved from voice network (real time traffic) where QoS is a critical success factor	Evolved from data network (store and forward) where QoS is not a critical factor
Radio Interface	Use spread spectrum as the modulation technique	Use spread spectrum as the modulation technique
Access Technologies	Access or Edge-network facility. Offer alternatives to the last-mile wireline network. The wireless link is from the end-user device to the cell base station, which may be at a distance of up to a few kilometres.	Access or edge-network facility. Offers alternatives to the last-mile wireline network. The wireless link Is a few hundred feet from the end-user device to the base station.

7,
6,
7,

Bandwidth	3G supports broadband data service of up to 2Mbps, 3G will support 'always on' connectivity	Wifi offers broadband data service of up to 54Mbps, wifi will support 'always on' connectivity
Business models/ deployment are different	Service providers own and manage the infrastructure (including the spectrum). End customers typically have a monthly service contract with the 3G service provider to use the network.	User's organization owns the infrastructure. Following the initial investment, the usage of the network does not involve an access fee.
Spectrum policy and management	3G uses licensed spectrum. This has important implications for: 1. Cost of service 2. QoS 3. Congestion management 4. Industry structure	WiFi uses unlicensed free shared spectrum. Therefore, it does not involve any additional costs to acquire the spectrum.
Status of standard	The formal standards picture of 3G is perhaps clearer than for WiFi. For 3G, there is a relatively small family of internationally sanctioned standard, collectively referred to as IMT-2000.	WiFi Protocol is one of the family of continuously evolving 802.11x wireless Ethernet standards, which itself is one of many wireless LAN technologies that are under development.
Roaming	3G will offer well-coordinated continuous and ubiquitous coverage. This offers a seamless roaming.	WiFi network growth is unorganized. Therefore seamless ubiquitous roaming over WiFi cannot be guaranteed.
Applications	Virtual home environment, Personal communication network, download music, Multimedia, News etc, Voice over IP (VoIP) Downloading software and Content etc.	Office/Campus Environment, homes, factor shop floor, public places like airport, railway station, war or defence sites etc.

12 Differentiate the WiMAX and WiFi Technologies. **(June-2012) (May-2018) [L.J.I.E.T]** 6,
What is WiMax? How is it different from WiFi? (**Dec-2012)[L.J.I.E.T]**
Compare and contrast WiMAX and WiFi technologies. [**New] (Dec-2013)[L.J.I.E.T]**
Explain Term : WiFi v/s WiMax. **[New] (June-2014)[L.J.I.E.T]** 3,
Explain Wi-Fi and Wi-Max technology in detail. Also discuss the differences.. **[New] (Dec-2015) [L.J.I.E.T]**
Explain WiFi and WiMax technology in detail. **[New] (May-2016)[L.J.I.E.T]** 7,
What is WiMax?How is it different from WiFi? **[New](May-2017) [New](May-2018) [L.J.I.E.T]**

Feature	**WiMax (802.16a)**	**Wi-Fi (802.11b)**	**Wi-Fi (802.11a/g)**
Primary Application	Broadband Wireless Access	Wireless LAN	Wireless LAN
Frequency Band	Licensed/Unlicensed 2 G to 11 GHz	2.4 GHz ISM	2.4 GHz ISM (g) 5 GHz U-NII (a)

3, 7, 7,

		Channel Bandwidth	Adjustable 1.25 M to 20 MHz	25 MHz	20 MHz		7, 7, 7
		Half/Full Duplex	Full	Half	Half		
		Radio Technology	OFDM (256-channels)	Direct Sequence Spread Spectrum	OFDM (64-channels)		
		Bandwidth Efficiency	<=5 bps/Hz	<=0.44 bps/Hz	<=2.7 bps/Hz		
		Modulation	BPSK, QPSK, 16-, 64-, 256-QAM	QPSK	BPSK, QPSK, 16-, 64-QAM		
		FEC	Convolutional Code Reed-Solomon	None	Convolutional Code		
		Encryption	Mandatory- 3DES Optional- AES	Optional- RC4 (AES in 802.11i)	Optional- RC4 (AES in 802.11i)		
		Mobility	Mobile WiMax (802.16e)	In development	In development		
		Mesh	Yes	Vendor Proprietary	Vendor Proprietary		
		Access Protocol	Request/Grant	CSMA/CA	CSMA/CA		