WNS UNIT-4

Introduction to Wireless Data Networks: Cellular Digital Packet Data (CDPD), CDPD Architecture, CDPD Security, Mobitex- Mobitex Architecture, Mobitex Security Architecture, Security Issues, Gateway, Security Model Wireless Standards and Technologies: Current and Future Technologies-Infrared, Radio, Spread Spectrum, OFDM, Current and Future Standards- IEEE 802 Standards, ETSI, Home RF, Ultra-wide band Radio (UWB)

Introduction:

As we know AMPS (Advanced Mobile Phone System) cellular network has been developed for voice communication in 1980s. Due to long established setup times and modem handshaking requirement packet data communication was not supported by AMPS. In order to support packet data, CDPD has been introduced in 1993.

Cellular Digital Packet Data (CDPD) was developed by IBM (along with a consortium of Regional Bell Operating Companies) and other organizations to leverage the existing installed base of AMPS cellular equipment in the United States to provide low-cost, packet-switched data services. CDPD was first offered in 1994 by Bell Atlantic Mobile.

CDPD stands for Cellular Digital Packet Data. Though it has its own infrastructure it utilizes vacant AMPS assigned channels or gaps between the channels for packet communication. CDPD architecture is explained below. It co-exist with AMPS network architecture. Hence it supports both data and voice communication.

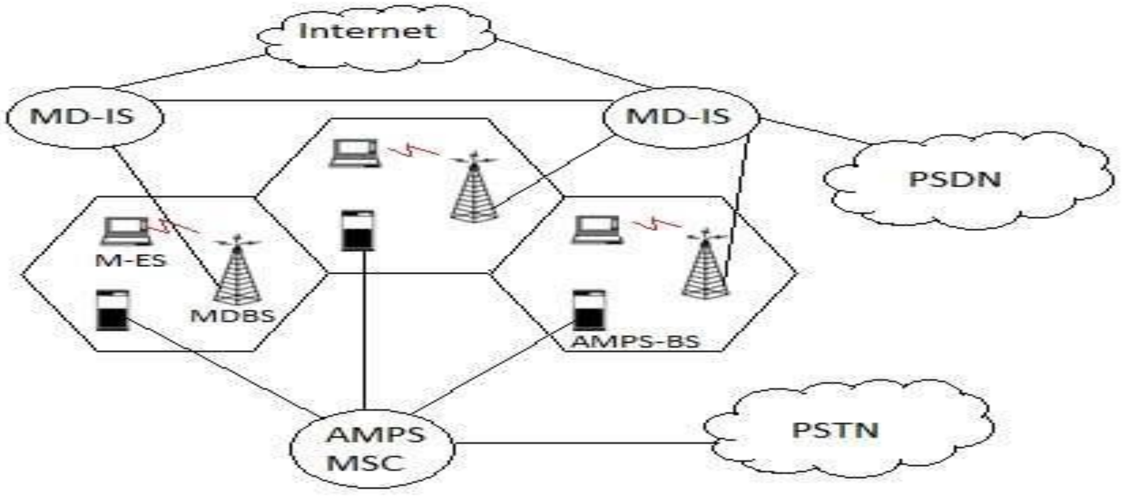
CDPD technology features:-

Following are the features of CDPD (Cellular Digital Packet Data).

- Communication between BS (Base station i.e. MDBS) and MS (i.e. M-ES) is full duplex.

- It utilizes or seizes 30 KHz channel from existing AMPS/GSM networks for transmitting data at 19.2 Kbps. The net data rate is 9.2 Kbps due to large amount of overhead.
- It utilizes same frequency band as used by AMPS i.e. 824 MHz and 894 MHz for uplink and downlink. Both uplink and downlink are separated using FDMA.
- There are two types of handsets or phones available viz. single mode and dual mode. In single mode phone can initiate data call or voice call. In dual mode phone can switch between data call and voice call due to simultaneous registration on both AMPS and CDPD networks.
- It utilizes DSMA (Digital Sense Multiple Access) technique. In this technique CDPD mobile checks for flag bit in downlink channel which informs whether uplink slot is idle or busy. If idle, it utilizes for transmission. If busy, it waits for random period instead of transmitting in the next time slot.
- It supports different types of services and has access to internet backbone.

CDPD network architecture:-



CDPD Network Architecture

The figure depicts CDPD network architecture. As shown it consists three major system elements M-ES, MDBS and MD-IS. Moreover CDPD co-exist with AMPS network and hence will have fall back to AMPS for voice call. Figure shows AMPS-BS and AMPS-MSC which are part of AMPS network connected with PSTN for voice connectivity.

There are three CDPD interfaces viz. E-interface, I-interface and A-interface. E-interface exists between CDPD and fixed network external to CDPD. I-interface exists between two CDPD networks. A-interface exists between BS and MS. It is also known as Air interface.

Let us understand network elements used in CDPD architecture.

M-ES: It functions similar to subscriber or mobile unit used in any cellular system. It requires SIM for operation which can be housed in laptop, mobile or PDA. It interfaces with radio equipment at 19.2 Kbps. Each M-ES has unique NEI (Network Equipment Identifier) which is associated with its home MD-IS.

MDBS: It functions similar to Base Station. It broadcasts available channels for M-ES. It takes care of radio activities such as channel allocation, usage etc. These MDBSs co-exist with AMPS Base Stations and hence share the same antenna and site together.

MD-IS: It provides connectivity with internet and PSDN. It has functionalities of both frame relay switch and packet router. It does buffering of packets routed for M-ES. It also supports roaming management as it contains registration directory.

How CDPD Works:-

Cellular Digital Packet Data makes use of idle times between calls in cellular phone network channels for interleaving packets of digital data. In other words, CDPD makes use of the «bursty» nature of typical voice transmission on the AMPS cellular system. Voice communication has gaps or pauses where packet data can be inserted and transmitted without interfering with the communication taking place between customers.

Although CDPD supports data transmission rates of 19.2 Kbps and higher, actual data throughput is usually around 9.6 Kbps. This is because of the large overhead added by CDPD to each data block transmitted. This overhead is designed to ensure that communications are reliable and to maintain synchronization between the modems at each end of the transmission. In addition, a color code is added to every data block to detect interference resulting from transmissions on the same channel from neighboring cell sites.

CDPD uses the Reed-Solomon forward-error-correcting code to encode each block or burst of data sent, and includes built-in RC4 encryption to ensure security and privacy of the transmitted data. CDPD is also based on the industry standard Internet Protocol (IP), allowing data to be transmitted to and from the Internet.

A typical implementation of CDPD consists of three components:

- **Mobile-End System (M-ES):** A user device such as a laptop equipped with a cellular modem. This system communicates in full-duplex mode with a Mobile Data Base Station (MDBS) using the Digital Sense Multiple Access protocol, which prevents collisions of data streams from multiple Mobile-End Systems.
- **Mobile Data Base Station (MDBS):** A telco device for receiving and transmitting CDPD data.
- **Mobile Data Intermediate System (MDIS):** Provides the central control for a CDPD network.

CDPD is typically used to provide wireless access to public packet-switched networks such as the Internet so that mobile users can access their e-mail and other services. Multiple users can share the same channel; the user’s modem determines which packets are destined for the user’s machine. CDPD also supports IP multicasting and is an open standard based on the Open Systems Interconnection (OSI) reference model for networking.

CDPD advantages and disadvantages:-

Following are the advantages of CDPD:

• Utilizes existing channels of the AMPS network and hence easy to install and start using the existing channels if not in use.

• It has cellular like architecture and hence can support larger capacity due to ease in upgrading the network.

• There is no delay in establishing data call as CDPD phone is already registered with the CDPD network.

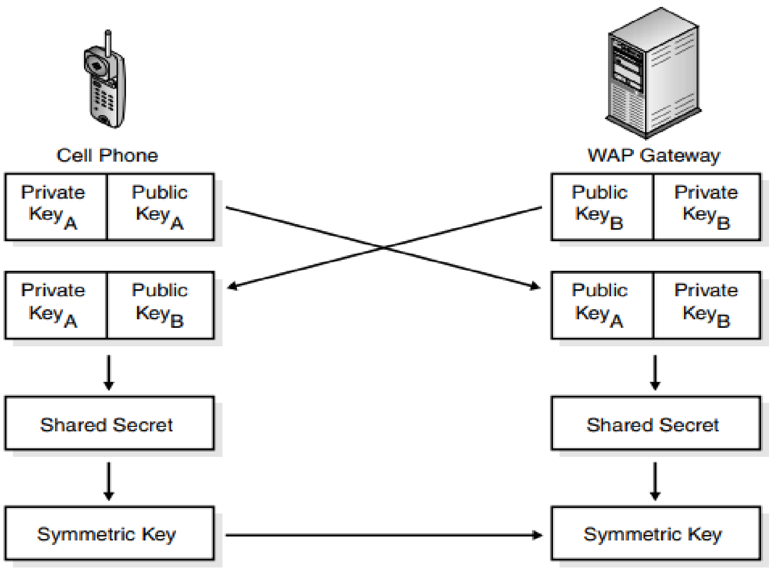
Following are the disadvantages of CDPD:

- There is no mesh connectivity in CDPD. Hence M-ES and M-ES can not communicate directly. Communication between them occurs via MDBS.
- CDPD cell size is limited to less than 10 miles.

CDPD Security:-

- The security requirements of CDPD are similar to those of a wireless voice network.
- CDPD devices are programmed at the time of manufacture with a unique numeric value called the Network Entity Identifier (NEI)
- The value is stored in the memory of the CDPD device and is used to authenticate the device on the CDPD network.
- The CDPD security architecture differs from a voice network in one significant manner. Whereas as a voice network utilizes a challenge response protocol over an unencrypted channel, CDPD establishes an encrypted channel first before progressing with authentication.
- This authentication is based on a widely used security protocol called the Diffie-Hellman key exchange. Diffie Hellman is not a mechanism that encrypts data, but is a mechanism that enables two unknown parties to exchange private keys that can be used to encrypt data.
- This makes Diffie-Hellman ideally suited for the CDPD architecture. Because the Diffie-Hellman protocol is used in some WAP implementations.
- In an asymmetric system, each party has a private and public key. In the protocol, the device sends its public key to the network, and vice versa. Because the keys are public, they can be transmitted over an insecure link. Each party now combines its private key with the received public key.
- Through this mechanism, each party can generate a secret session key that can be utilized for establishing an encrypted session.

- There are two issues worth knowing about the Diffie-Hellman protocol. First, Diffie-Hellman does not authenticate the participants; it merely establishes a session key between two parties. For this reason, Diffie Hellman is susceptible to a so-called man-in-the-middle attack.
- In this attack, an intermediate party intercepts the device's public key during transmission, replaces it with a different public key, and sends that value to the intended recipient. The intermediary conducts the same process with the recipient's public key.
- Through this process, the intermediary can then decrypt and read all traffic. There is protection against man in-the-middle attacks in the Diffie-Hellman key exchange; however, this protection typically requires the use of a more elaborate public key infrastructure (PKI) architecture.
- Getting back to the topic of CDPD, once the Diffie-Hellman protocol has been completed, the M-ES and MD-IS create two ciphering keys. Because Diffie-Hellman has provided each party with the same shared secret, that secret can be utilized to generate a symmetric key.
- All CDPD encryption utilizes a variable key size stream cipher called RC4. To authenticate itself to the CDPD network, the mobile device transmits its NEI along with some additional unique identifiers to the MD-IS. The MD-IS forwards this information to an authentication server that compares the results, if the results match, the device is authenticated and allowed onto the network. As an additional level of security, the CDPD devices utilize something called a shared history record (SHR).



Mobitex:-

- Mobitex is a wireless data technology developed by Ericsson in the mid 1980.
- All Mobitex networks operate in one of four frequency families: 80 MHz, 400 MHz, 800 MHz, or 900 MHz.
- Mobitex is a packet-based switching technology and is capable of throughput rates of up to 8 Kbps. Mobitex data is transmitted in 512-byte blocks.

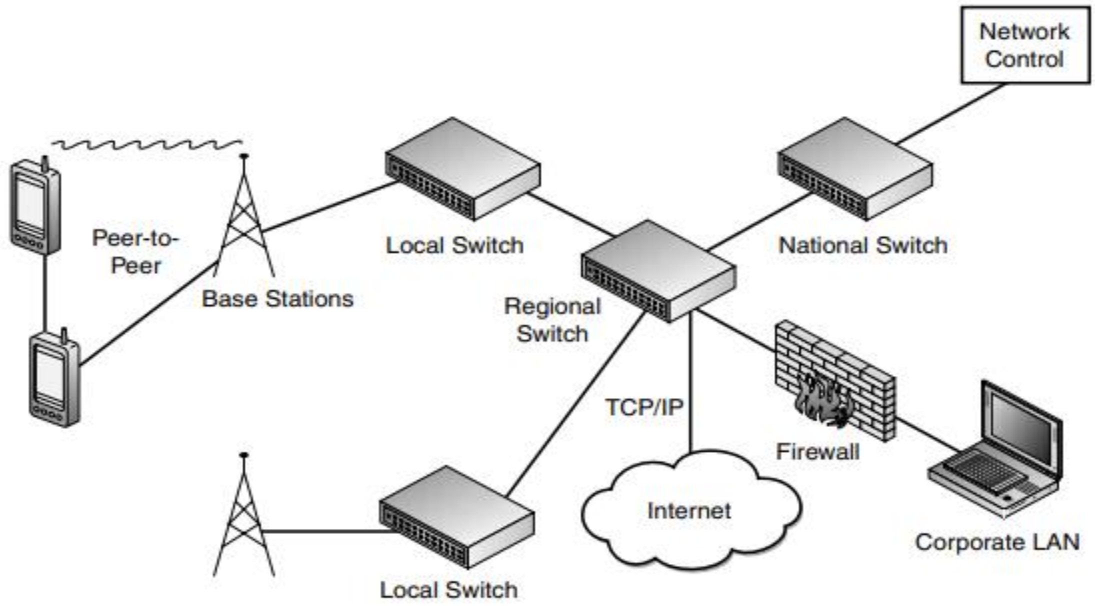
Mobitex Architecture:-

- The design of Mobitex networks is similar to traditional cellular voice networks. Each Mobitex hand-held device connects to a base station, which in turn connects to a local switch.
- The local switch connects to the Mobitex operator's network backbone, but it can also connect to external networks (such as a corporate local area network [LAN] or gateway).
- In addition to the local switches, Mobitex networks utilize regional switches (which control a set of local switches) as well as a Network Control Center (NCC), which handles billing, monitors usage, and oversees network performance.

- One unique feature of Mobitex is its capability to offer peer-to-peer communication between two Mobitex devices. With peer-to-peer communication, two devices communicate without engaging the entire Mobitex network infrastructure.
- the base station coordinates all the communication and then ultimately forwards the activity back to the NCC.
- The main advantage of this approach is that it minimizes the back-haul network traffic.

Mobitex Security Architecture:-

- The Mobitex security architecture is quite similar to other wireless data networks. The main difference is that the Mobitex security specifications are not widely published and have not been subjected to the same level of scrutiny as other standards.
- The same general authentication principles that are used in cellular networks are used in Mobitex. Each Mobitex device contains a unique serial number and another value called the Mobitex Access Number
- These values are stored locally in the Mobitex hand-held device and are transmitted over the air to the base station where they are forwarded onto the NCC for authentication.
- Mobitex is a packet-based network, it is possible to utilize some of the security features available in wired networks to encrypt data at the application layer.
- This exchange is then used to create a pair of DES-X keys (a variant of the Data Encryption Standard [DES]) that can be used to establish an encrypted session between the device and the network.
- GPRS is based on the same fundamental GSM security architecture, GPRS introduces several new security threats that have to be considered and for which appropriate countermeasures must be created.



Security Issues:-

- GPRS is based on the same fundamental GSM security architecture, GPRS introduces several new security threats that have to be considered and for which appropriate counter measures must be created.
- The single biggest security threat to GPRS is the network's connection to public networks (such as the Internet) means that wireless networks are susceptible to attack from the back end. Previous wireless voice-only networks were closed networks, making access to them considerably harder. This means that operators must take added measures to protect the connection between the GPRS gateway (GGSN) and the Internet.
- Another significant development is that GPRS is packet and IP based. This means that GPRS is now susceptible to some of the same security threats facing the wired Internet, including the following:
  i. **Denial of service (DoS):-** This attack consists of sending thousands or millions of simultaneous requests to an individual web server. These requests overwhelm the web server and it crashes, making it unable to provide service to valid users (hence, DoS). In GPRS, it is

theoretically possible to launch a DoS attack against the GGSN (thereby stopping all GPRSs for all subscribers) or even against an individual mobile phone to prevent it from operating.

ii. **IP address spoofing:-** In this attack, a hacker successfully determines the valid numeric IP address for a given web site. The hacker can then create data packets that appear genuine and send them to unsuspecting users. Because the subscriber cannot tell if the content has been hijacked, hackers can use this attack to retrieve passwords, credit-card numbers, and other sensitive data from users.

WAP Gateway:-

- WAP(Wireless Application Protocol) is not a wireless standard like GPRS or CDPD (in fact, it can operate over most network interfaces), WAP is another important component to wireless data services.
- The WAP primary goal was to develop a common architecture for accessing the wireless Internet and collectively promote the benefits of WAP. Although the WAP worked on developing a series of technical specifications starting with WAP v1.0 in early 1998.
- The WAP gateway serves as the central interface to the Internet. All requests and data from the wireless devices must pass through the WAP gateway before proceeding onto the Internet.
- The WAP gateway was always managed and maintained by the network operator. Depending on the subscriber base, an operator might utilize multiple WAP gateways for load balancing.
- The WAP gateway serves several key functions:-
  i. **Protocol converter:-**Converts WAP protocols (such as the Wireless Data Protocol [WDP] and Wireless Transport Layer Security [WTLS]) to wired protocols (like TCP and TLS).

ii. **Content converter:-** Translates HTML web pages into WML compatible content.

iii. **Performance optimization and overhead reduction :-** Given the low bandwidth and throughput of the phone, the WAP gateway's routines are designed to compress data as much as possible and minimize the number of roundtrips that must take place between the client and the gateway.

- When a WAP gateway receives a request for content from a WAP device, the WAP gateway will translate that request into HTTP and retrieve the content from the original web server. Although the WAP gateway is capable of converting HTML to WML dynamically, in most WAP implementations, the content provider creates a subset of data in the WML format.
- Given WML's interoperability with HTML, this is not an enormous task, but it does point out that some effort must be expended to enable existing web content for wireless device.

WAP Security Model:-

- The WAP security layer is different from the wired world. Rather than relying on the Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocol, the WAP specification adopted WTLS.
- This protocol was designed to provide authentication, data encryption, and privacy for WAP users. WTLS was included in the WAP 1.1 specification.
- Traditional SSL is not suitable for wireless networks primarily for performance reasons. SSL works fine in a PC world where the client PC has significant processing power, ample battery supply, and a relatively fast connection to the web server. A WAP device has none of these features, which explains the reason for developing WTLS.
- The WAP specification also created a WMLScript function called SignText that provides capabilities for providing digital signatures on WAP devices.

- SignText-compliant products are just being introduced into the market, the SignText capability will add significant value to existing WAP environments by providing a level of nonrepudiation that can be used for security-sensitive transactions.
- The WAP specification introduces three different classes of authentication:-
    i. Class 1 authentication is anonymous. Neither client nor gateway can authenticate each other.
    ii. Class 2 authentication is server authentication only. This is equivalent to shopping over a SSL link from a wired browser. The SSL protocol authenticates the server (so that the user knows it really is the corporation's web site).
    iii. Class 3 authentication is both client and server authentication. This requires the use of a PKI(Public Key Infrastructure)
- Although Class 3-capable devices introduce the possibility of a true wireless public key infrastructure (WPKI), they also introduce a whole host of unresolved business issues.
- Specifically, in Class 3 devices, the critical issue is how the user's public/private key is going to be managed, installed, supported, and so on.
- Again, the WTLS protocol specified a process to minimize the amount of communication required between the client and server. The Class 2 authentication process completes itself in four steps:
    1. The WAP device sends a request to the WAP gateway.
    2. The gateway responds and sends a copy of its certificate (containing the gateway's public key) to the WAP device.
    3. The WAP device retrieves the certificate and public key, generates a unique random value, and encrypts it with the gateway's public key.
    4. The WAP gateway receives the encrypted value and decrypts it with its corresponding private key.

- Unfortunately, the WTLS protocol only encrypts data from the WAP device to the WAP gateway. From the WAP gateway to the content web server, information is transmitted over standard SSL. Because the data must be converted from WTLS to SSL, there is a brief millisecond in time when data is unencrypted on the gateway.
- This brief millisecond soon became known as the WAP Gap. Even though the practical risks of this gap were extremely minor, the press and analysts used the gap to proclaim that WAP was insecure.

Wireless Standards and Technologies:-

Current and Future Technologies:-

- Currently, wireless technologies use either radio or light waves to move information from one point to another. Most of us have been wireless users for years with our mobile/cordless phones and television remote controls.
- However, wireless technologies continue to evolve. For example, mobile phones, the veterans of the wireless world, are beginning to delve into the world of data transmission. Let's look at the basics of how these technologies work.
- **Infrared:-**
  - **i.** Infrared radiation (IR) involves electromagnetic waves in the spectrum just below visible light. Being close to visible light lends infrared a number of the same properties that visible light has.
  - **ii.** For example, like light waves, infrared travels in straight lines and bounces off objects, but it cannot penetrate physical or opaque objects. Data can be transmitted over infrared in much the same way that light is used to transmit data in fiber optics—by pulsing it (turning it on or off)
  - **iii.** This is the same type of technology used in many remote control units for TVs, VCRs, and so on.

- **Radio:-**

  i. Radio is the use of electromagnetic waves that are emitted when an alternating current is input to an antenna. This can be used to transmit data invisibly through the air to devices such as radios, televisions, and mobile phones

  ii. Radio is the most widely used technology for wireless communications. As with anything good, only a limited amount of usable radio frequencies is available, and radio is used in an almost endless number of ways in today's world.

  iii. Many of the frequencies in the radio spectrum require a license. Some frequencies allocated in the radio spectrum have been made available for use without a license.

  iv. One of these groups of unlicensed frequencies is known as the industrial, scientific, and medical (ISM) band because it is allocated for use by the industrial, scientific, and medical fields.

  v. Specific allocation of radio frequencies for wireless LAN use, radio frequency availability is still limited. Therefore, a number of interesting ways to fit more data into the existing available frequencies have come into use.

  vi. Some of these include the use of spread spectrum techniques and Orthogonal Frequency Division Multiplexing (OFDM).

- **Spread Spectrum:-**

  i. Spread spectrum refers to the method of dividing data and sending it over a "spread" or wideband of different frequencies.

  ii. Spread spectrum signals use multiple frequencies (wideband) and appear to be radio noise to narrowband devices

  iii. This kind of noise can be easily filtered out, which is what enables the coexistence of narrowband devices.

iv. Some common spread spectrum methods are frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS).

v. In FHSS systems, the transmitter and the receiver hop from one frequency to another in prearranged synchronized patterns. The hops occur frequently with very little time being spent on any one frequency. This reduces the possibility of interference with other devices and enables several overlapping FHSS systems to be operational at the same time.

vi. DSSS pushes data through a binary encoding process that spreads the data by combining it with a multibit pattern or pseudo-noise code. The resulting data is now somewhat hidden and inflated. For example, if the bit pattern is 11 bits long (which is typical for most DSSS wireless applications), then 1 bit of data would now be 11 bits long. This data is modulated and then sent out over multiple frequencies (which typically consist of about 22 MHz of bandwidth) at the same time. Since the original data bit was encoded into 11 bits, the data is more resilient to air loss because the data has a tremendous amount of redundancy.

- **OFDM:-**

i. OFDM is a multicarrier modulation method that divides a communications channel into a number of equally spaced frequency bands. Each band is then used to transmit a portion of the user information.

ii. Each band is independent of, or orthogonal, to every other band. This multicarrier approach also reduces multipath problems where the reflected radio signals bounce back from different sources with slightly different timing.

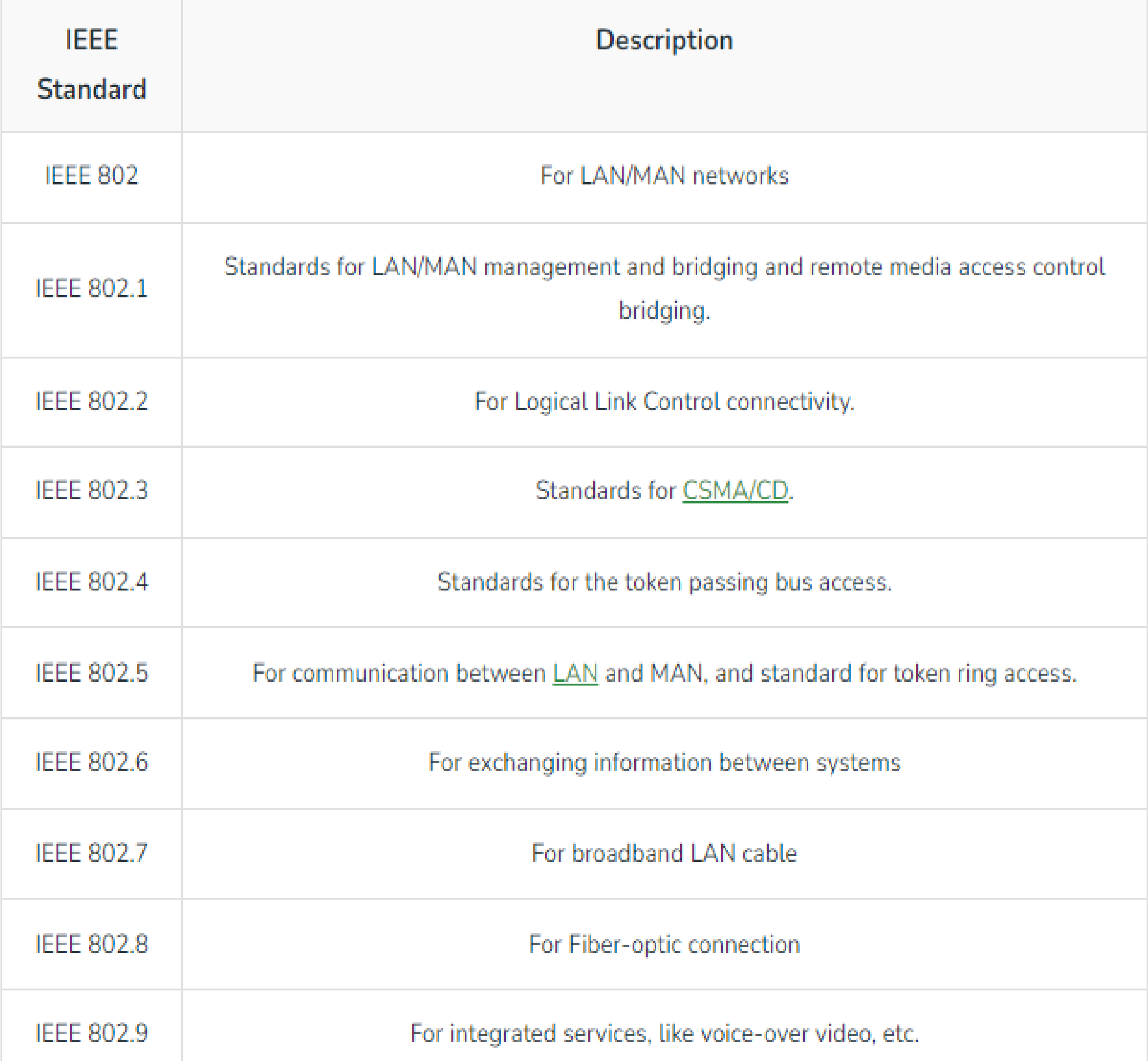
iii. At the same time, it increases the performance and data throughput.

Current and Future Standards:-

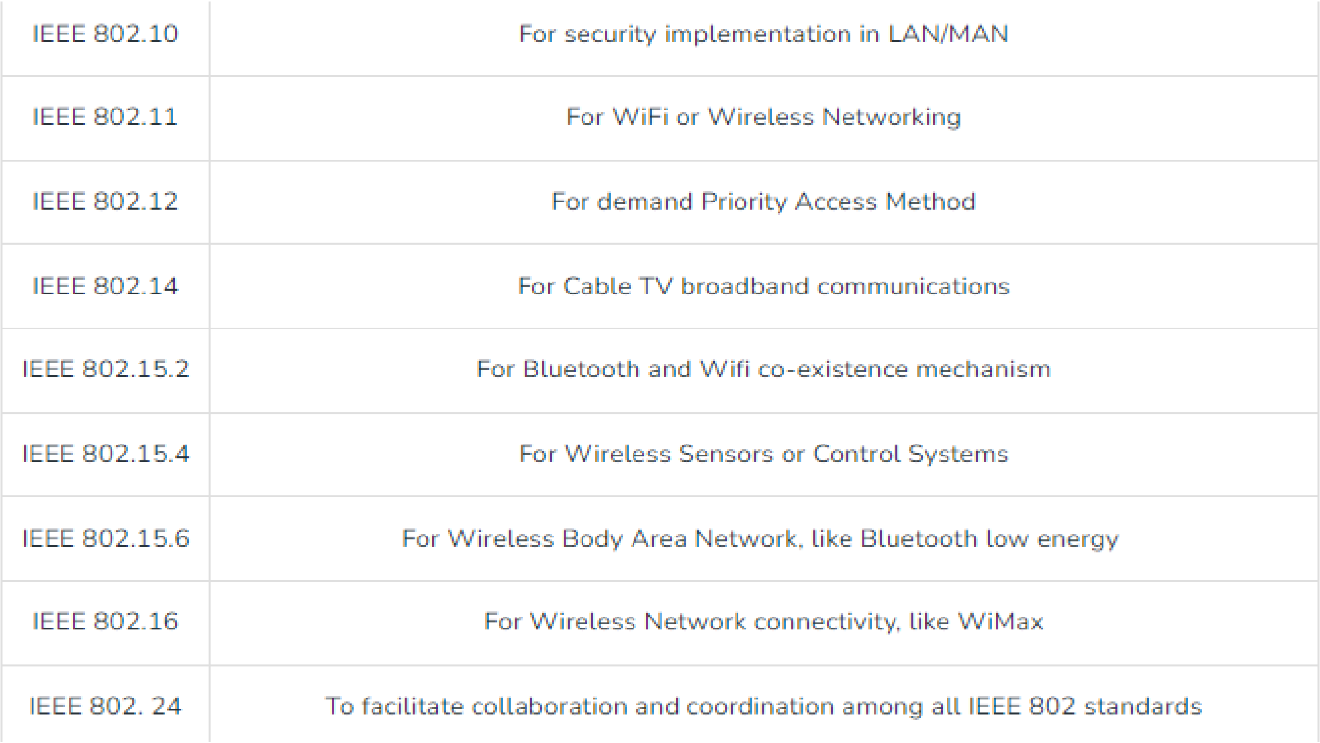
- A number of standard-setting organizations exist, but the two that are having the most impact on wireless technologies are the Institute of Electrical and Electronics Engineers (IEEE) and the European Telecommunications Standards Institute (ETSI).

IEEE 802 Standards:-

The IEEE (www.ieee.org) develops standards in a wide range of electrical/electronic fields. The 802 Local and Metropolitan Area Networks Standards Committee (LMSC) of the IEEE Computer Society defines specifications related to LANs.



IEEE Standard	Description
IEEE 802	For LAN/MAN networks
IEEE 802.1	Standards for LAN/MAN management and bridging and remote media access control bridging.
IEEE 802.2	For Logical Link Control connectivity.
IEEE 802.3	Standards for CSMA/CD.
IEEE 802.4	Standards for the token passing bus access.
IEEE 802.5	For communication between LAN and MAN, and standard for token ring access.
IEEE 802.6	For exchanging information between systems
IEEE 802.7	For broadband LAN cable
IEEE 802.8	For Fiber-optic connection
IEEE 802.9	For integrated services, like voice-over video, etc.



IEEE 802.10	For security implementation in LAN/MAN
IEEE 802.11	For WiFi or Wireless Networking
IEEE 802.12	For demand Priority Access Method
IEEE 802.14	For Cable TV broadband communications
IEEE 802.15.2	For Bluetooth and Wifi co-existence mechanism
IEEE 802.15.4	For Wireless Sensors or Control Systems
IEEE 802.15.6	For Wireless Body Area Network, like Bluetooth low energy
IEEE 802.16	For Wireless Network connectivity, like WiMax
IEEE 802. 24	To facilitate collaboration and coordination among all IEEE 802 standards

802.11:-

- IEEE 802.11 standard, popularly known as **WiFi**, lays down the architecture and specifications of wireless **LANs** (**WLANs**). WiFi or WLAN uses high frequency radio waves for connecting the nodes.
- There are several standards of IEEE 802.11 WLANs. The prominent among them are 802.11, 802.11a, 802.11b, 802.11g, 802.11n and 802.11p. All the standards use carrier-sense multiple access with collision avoidance (CSMA/CA).
- IEEE 802.11 was the original version released in 1997. It provided 1 Mbps or 2 Mbps data rate in the 2.4 GHz band and used either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS). It is obsolete now.

a) IEEE 802.11a:-

- 802.11a was published in 1999 as a modification to 802.11, with orthogonal frequency division multiplexing (OFDM) based air interface in physical layer instead of FHSS or DSSS of 802.11.

- It provides a maximum data rate of 54 Mbps operating in the 5 GHz band. Besides it provides error correcting code.
- As 2.4 GHz band is crowded, relatively sparsely used 5 GHz imparts additional advantage to 802.11a.

b) <u>IEEE 802.11b:-</u>

- 802.11b is a direct extension of the original 802.11 standard that appeared in early 2000. It uses the same modulation technique as 802.11, i.e. DSSS and operates in the 2.4 GHz band.
- It has a higher data rate of 11 Mbps as compared to 2 Mbps of 802.11, due to which it was rapidly adopted in wireless LANs.
- However, since 2.4 GHz band is pretty crowded, 802.11b devices faces interference from other devices.

c) <u>IEEE 802.11g:-</u>

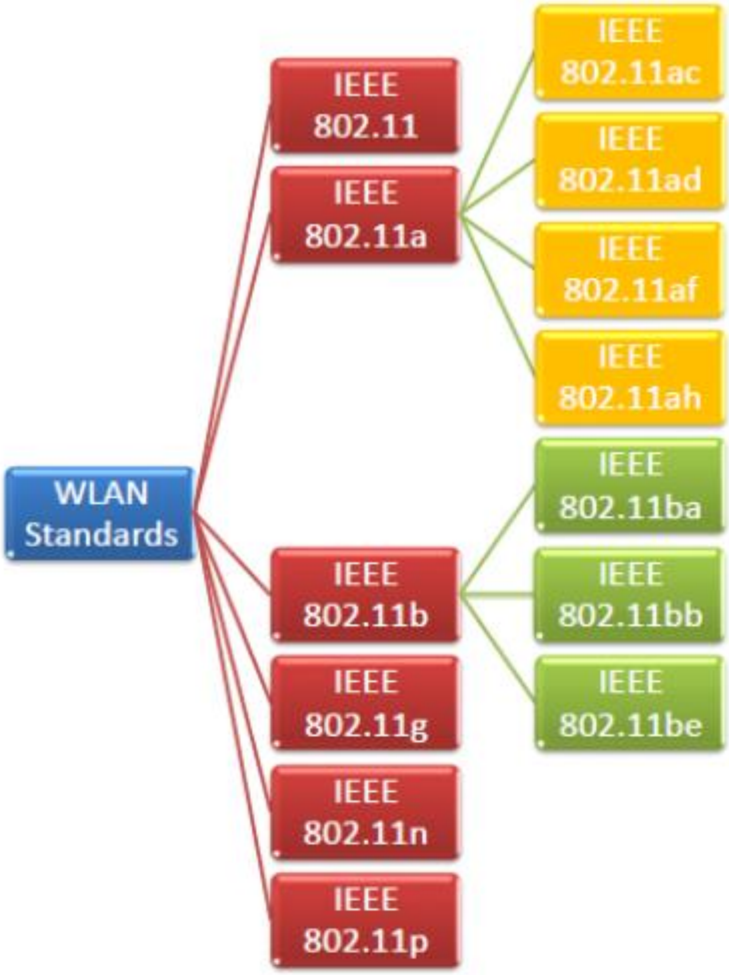
- 802.11g was indorsed in 2003. It operates in the 2.4 GHz band (as in 802.11b) and provides a average throughput of 22 Mbps. It uses OFDM technique (as in 802.11a).
- It is fully backward compatible with 802.11b. 802.11g devices also faces interference from other devices operating in 2.4 GHz band.

d) <u>IEEE 802.11n:-</u>

- 802.11n was approved and published in 2009 that operates on both the 2.4 GHz and the 5 GHz bands. It has variable data rate ranging from 54 Mbps to 600 Mbps.
- It provides a marked improvement over previous standards 802.11 by incorporating multiple-input multiple-output antennas (MIMO antennas).

e) <u>IEEE 802.11p:-</u>

- 802.11 is an amendment for including wireless access in vehicular environments (WAVE) to support Intelligent Transportation Systems (ITS).
- They include network communications between vehicles moving at high speed and the environment. They have a data rate of 27 Mbps and operate in 5.9 GHz band.



Advantages:-

1. The data communication system is faster than the speed of transportation.
2. Multi-path propagation increases the transmission rate and reduces error incidence.
3. Manually fix the modulation used by the transmission.
4. Developing standards for the computer and electronic industry.
5. It is a non-profit professional association and works for the benefit of Humanity.

Disadvantages:-

1. It requires periodic maintenance.
2. Network security needs to stay secure.
3. It has unauthorized use.

ETSI:-

- ETSI stands for European Telecommunications Standards Institute.
- ETSI (www.etsi.org) is the European counterpart to IEEE.
- **HiperLAN/1:-**
    i. In 1991, ETSI formed the Subtechnical Committee RES10 to develop a HiperLAN. The resulting standard was the HiperLAN/1 standard (approved in 1996) and defines the PHY and MAC specifications for wireless high-speed communications

    ii. HiperLAN/1 uses gaussian minimum shift keying (GMSK) and specifies data rates of up to 20 Mbps between portable devices.

    iii. One advantage of HiperLAN/1 is that it works in a dedicated bandwidth (5.1 to 5.3 GHz, which is allocated only in Europe) so it doesn't have to use spread spectrum technologies in order to coexist with other radio usage as is the case in the 2.4 GHz ISM range.

    iv. Also, the protocol uses a variant of CSMA/CA and includes optional encryption and power savings.

    v. Another nice feature of HiperLAN/1 is ad-hoc routing. For example, if your destination is out of reach, intermediate nodes will automatically forward it through the best route within the HiperLAN/1 network (the routes are automatically recalculated regularly).

- **HiperLAN/2:-**
    i. In 1997, ETSI formed the Broadband Radio Area Network (BRAN) group to work on HiperLAN/2.HiperLAN/2 is a redesign of HiperLAN/1 and was the first standard to use OFDM.

    ii. HiperLAN/2 and IEEE 802.11a are similar in their use of the 5 GHz band and OFDM to attain data rates as high as 54 Mbps. However, a key difference between the two standards is in the MAC portion of the systems.

iii. HiperLAN/2 uses Time Division Multiplexing (TDM),whereas 802.11a/g use CSMA/CD. Because of this, HiperLAN/2 can provide QoS, while IEEE 802.11a does not currently include it.

iv. HiperLAN/2 is regarded as wireless Asynchronous Transfer Mode (ATM).

v. It is possible that a joint standard may exist between ETSI and IEEE because a joint project, referred to as the 5 GHz Unified Protocol (5-UP) project, is currently being worked on.

vi. The objective of the project is to provide a single universal standard in the 5 GHz range for wireless LANs

HomeRF:-

- HomeRF (www.homerf.org) is a label for a group of manufacturers that came together in 1998 to develop a standard for wireless connectivity between personal computers and electronic devices.
- The standard that resulted is the Shared Wireless Access Protocol (SWAP), which allows for voice and data transmission with data rates of up to 1.6 Mbps.
- Targeting the home market, the premise behind HomeRF was that 802.11 devices would be too costly and complicated for home/consumer markets.
- HomeRF is working on SWAP 2.0, which will use wideband frequency hopping (WBFH) to increase the data rate of the standard.
- It is also trying to differentiate HomeRF from the other wireless standards by promoting it as a standard for wireless communication between not just data but also voice and multimedia devices.

Ultrawideband Radio (UWB):-

- The FCC approved the use of ultrawideband (UWB) radio in the 3.1 through 10.6 GHz band, opening the way for the use of radio impulse technology in wireless LANs.
- Instead of traditional sine waves, UWB radio broadcasts digital pulses that are timed very precisely on a signal across a very wide spectrum at the same time.
- The transmitter and receiver must be coordinated to send and receive pulses with an accuracy of trillionths of a second. This actually sidesteps the multipath issues typically associated with radio signals.
- With the current power restrictions mandated by the FCC, UWB signals appear as radio noise to other frequency users. This is why UWB has been approved for use in the 3.1 to 10.6 GHz range.
- UWB also has a low power consumption, making this a very desirable technology for many portable wireless applications.