UNIT - II

#) Wireless Network

- Wireless networks are computer networks that are not connected by cables of any kind.
- The use of a wireless network enables enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations.
- The basis of wireless systems are radio waves, an implementation that takes place at the physical level of network structure.
- Wireless networks use radio waves to connect devices such as laptops to the Internet, the business network and applications.
- There are four main types of wireless networks:
    i. Wireless Local Area Network (LAN): Links two or more devices using a wireless distribution method, providing a connection through access points to the wider Internet.
    ii. Wireless Metropolitan Area Networks (MAN): Connects several wireless LANs.
    iii. Wireless Wide Area Network (WAN): Covers large areas such as neighboring towns and cities.
    iv. Wireless Personal Area Network (PAN): Interconnects devices in a short span, generally within a person's reach

#) Wireless LAN

- Wireless LAN stands for **Wireless Local Area Network**. It is also called LAWN (**Local Area Wireless Network**). WLAN is one in which a mobile user can connect to a Local Area Network (LAN) through a wireless connection.
- Wireless LANs provide high speed data communication in small areas such as building or an office. WLANs allow users to move around in a confined area while they are still connected to the network.
- In some instance wireless LAN technology is used to save costs and avoid laying cable, while in other cases, it is the only option for providing high-speed internet access to the public.

Advantages of WLANs

- **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 independent, small devices which can for example be put into a pocket. Cables not only restrict users but also designers of small notepads, PDAs, etc.
- **Cost:** The cost of installing and maintaining a wireless LAN is on average lower than the cost of installing and maintaining a traditional wired LAN
- **Ease of Use**: Wireless LAN is easy to use and the users need very little new information to take advantage of WLANs.

Disadvantages of WLANs

- **Quality of Services:** Quality of wireless LAN is typically lower than wired networks.
- **Restrictions:** Several govt. and non-govt. institutions world-wide regulate the operation and restrict frequencies to minimize interference.
- **Global operation:** Wireless LAN products are sold in all countries so, national and international frequency regulations have to be considered.
- **Low Power:** Devices communicating via a wireless LAN are typically power consuming, also wireless devices running on battery power. Whereas the LAN design should take this into account and implement special power saving modes and power management functions.
- **License free operation:** LAN operators don't want to apply for a special license to be able to use the product.

#) MAC Issues

The three important issues are:

1. Half Duplex operation –> either send or receive but not both at a given time
2. Time varying channel
3. Burst channel errors

1. **Half Duplex Operation** :

In wireless, it's difficult to receive data when the transmitter is sending the data, because: When node is transmitting, a large fraction of the signal energy leaks into the receiver path. The transmitted and received power levels can differ by orders of magnitude. The leakage signal typically has much higher power than the received signal —Impossible to detect a received signal, while transmitting data. Collision detection is not possible, while sending data. As collision cannot be detected by the sender, all proposed protocols attempt to minimize the probability of collision - Focus on collision avoidance.

2. **Time Varying Channel** :

- Three mechanisms for radio signal propagation
- Reflection – occurs when a propagating wave impinges upon an object that has very large dimensions than the wavelength of the radio wave e.g. reflection occurs from the surface of the earth and from buildings and walls · Diffraction – occurs when the radio path between the transmitter and the receiver is obstructed by a surface with sharp edges
- Scattering – occurs when the medium through which the wave travels consists of objects

The time varying signals (time varying channel) phenomenon also known as multipath propagation. The rate of variation of channel is determined by the coherence time of the channel . Coherence time is defined as time within which When a node's received signal strength drops below a certain threshold the node is said to be in fade .

3. **Burst Channel Errors :**

As a consequence of time varying channel and varying signals strengths errors are introduced in the transmission (Very likely) for wire line networks the bit error rate (BER) is the probability of packet error is small .For wire line networks the errors are due to random For wireless networks the BER is as high. For wireless networks the errors are due to node being in fade as a result errors occur in a long burst. Packet loss due to burst errors - mitigation techniques ·

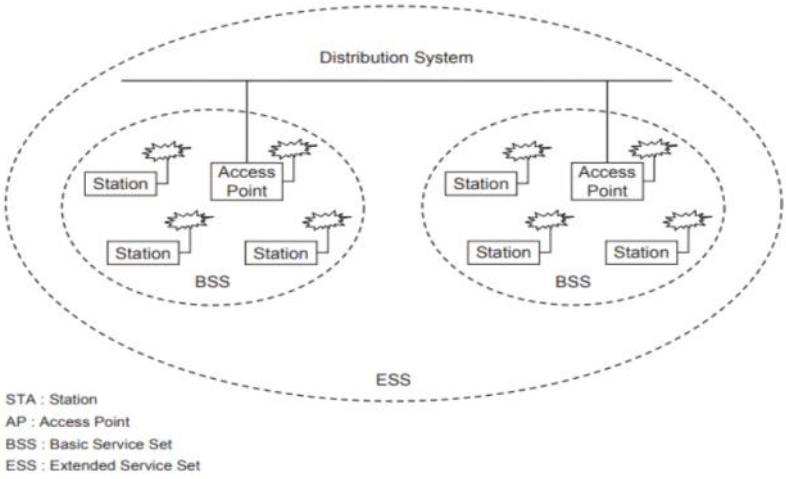
- □ Smaller packets
- □ Forward Error Correcting Codes
- □ Retransmissions (Acks)

#) IEEE 802.11

IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network(WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands The IEEE developed an international standard for WLANs. The 802.11 standard focuses on the bottom two layers of the OSI model, the physical layer (PHY) and data link layer (DLL). The objective of the IEEE 802.11 standard was to define a medium access control (MAC) sublayer, MAC management protocols and services, and three PHYs for wireless connectivity of fixed, portable, and moving devices within a local area. The three physical layers are an IR base band PHY, an FHSS radio in the 2.4 GHz band, and a DSSS radio in the 2.4 GHz.

IEEE 802.11 Architecture:

The architecture of the IEEE 802.11 WLAN is designed to support a network where most decision making is distributed to mobile stations. This type of architecture has several advantages. It is tolerant of faults in all of the WLAN equipment and eliminates possible bottlenecks a centralized architecture would introduce. The architecture is flexible and can easily support both small, transient networks and large, semipermanent or permanent networks. In addition, the architecture and protocols offer significant power saving and prolong the battery life of mobile equipment without losing network connectivity Two network architectures are defined in the IEEE 802.11 standard:



- **Infrastructure network**: An infrastructure network is the network architecture for providing communication between wireless clients and wired network resources. The transition of data from the wireless to wired medium occurs via an AP. An AP and its associated wireless clients define the coverage area. Together all the devices form a basic service set

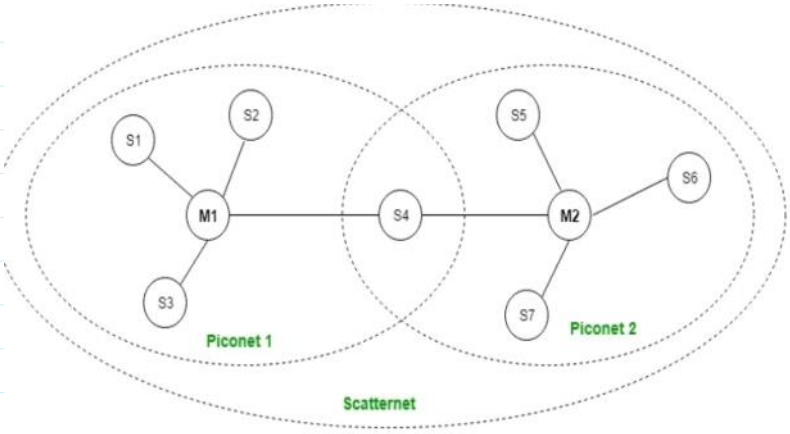
- **Point-to-point (ad-hoc) network**: An ad-hoc network is the architecture that is used to support mutual communication between wireless clients. Typically, an ad-hoc network is created spontaneously and does not support access to wired networks. An ad-hoc network does not require an AP. IEEE 802.11 supports three basic topologies for WLANs, the independent basic service set (IBSS), the basic service set, and the extended service set (ESS). The MAC layer supports implementations of IBSS, basic service set, and ESS configurations.

- **Independent basic service set:** The IBSS configuration is referred to as an independent configuration or an ad-hoc network. An IBSS configuration is analogous to a peer-to-peer office network in which no single node is required to act as a server. IBSS WLANs include a number of nodes or wireless stations that communicate directly with one another on an ad-hoc, peer-to-peer basis. Generally, IBSS implementations cover a limited area and are not connected to any large network. An IBSS is typically a short-lived network, with a small number of stations, that is created for a particular purpose.
- **Basic service set:** The basic service set configuration relies on an AP that acts as the logical server for a single WLAN cell or channel. Communications between station 1 and station 4 actually flow from station 1 to AP1 and then from AP1 to AP2 and then from AP2 to AP4 and finally AP4 to station 4 (refer to Figure 2). An AP performs a bridging function and connects multiple WLAN cells or channels, and connects WLAN cells to a wired enterprise LAN.

#) Bluetooth

It is a Wireless Personal Area Network (WPAN) technology and is used for exchanging data over smaller distances. This technology was invented by Ericson in 1994. It operates in the unlicensed, industrial, scientific and medical (ISM) band at 2.4 GHz to 2.485 GHz. Maximum devices that can be connected at the same time are 7 Bluetooth ranges upto 10 meters. It provides data rates upto 1 Mbps or 3 Mbps depending upon the version. The spreading technique which it uses is FHSS (Frequency hopping spread spectrum). A bluetooth network is called piconet and a collection of interconnected piconets is call scatternet.

Bluetooth Architecture:



Bluetooth protocol stack:
1. Radio (RF) layer: It performs modulation/demodulation of the data into RF signals. It defines the physical characteristics of bluetooth transceiver. It defines two types of physical link: connection-less and connection-oriented.
2. Baseband Link layer: It performs the connection establishment within a piconet.
3. Link Manager protocol layer: It performs the management of the already established links. It also includes authentication and encryption processes.
4. Logical Link Control and Adaption protocol layer: It is also known as the heart of the bluetooth protocol stack. It allows the communication between upper and lower layers of the bluetooth protocol stack. It packages the data packets received from upper layers into the form expected by lower layers. It also performs the segmentation and multiplexing.
5. SDP layer: It is short for Service Discovery Protocol. It allows to discover the services available on another bluetooth enabled device.
6. RF comm layer: It is short for Radio Frontend Component. It provides serial interface with WAP and OBEX. 7. OBEX: It is short for Object Exchange. It is a communication protocol to exchange objects between 2 devices. 8. WAP: It is short for Wireless Access Protocol. It is used for internet access.
9. TCS: It is short for Telephony Control Protocol. It provides telephony service.
10. Application layer: It enables the user to interact with the application.

Advantages:
- Low cost.
- Easy to use.
- It can also penetrate through walls.
- It creates an adhoc connection immediately without any wires.
- It is used for voice and data transfer.

Disadvantages:
- It can be hacked and hence, less secure.
- It has slow data transfer rate: 3 Mbps.
- It has small range: 10 meters.

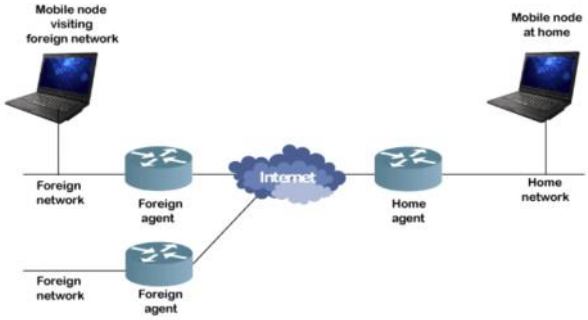
#) Mobile Internet Protocol

Mobile Internet Protocol (or Mobile IP) Mobile IP is a communication protocol (created by extending Internet Protocol, IP) that allows the users to move from one network to another with the same IP address. It ensures that the communication will continue without user's sessions or connections being dropped.

Terminologies:

• Mobile Node (MN): It is the hand-held communication device that the user caries e.g. Cell phone.
• Home Network: It is a network to which the mobile node originally belongs to as per its assigned IP address (home address).
• Home Agent (HA): It is a router in home network to which the mobile node was originally connected
• Home Address: It is the permanent IP address assigned to the mobile node (within its home network).
• Foreign Network: It is the current network to which the mobile node is visiting (away from its home network).
• Foreign Agent (FA): It is a router in foreign network to which mobile node is currently connected. The packets from the home agent are sent to the foreign agent which delivers it to the mobile node.
• Correspondent Node (CN): It is a device on the internet communicating to the mobile node.
• Care of Address (COA): It is the temporary address used by a mobile node while it is moving away from its home network.

Working:



The working of Mobile IP can be described in 3 phases:

Agent Discovery

In the Agent Discovery phase, the mobile nodes discover their Foreign and Home Agents. The Home Agent and Foreign Agent advertise their services on the network using the ICMP Router Discovery Protocol (IRDP).

Registration

The registration phase is responsible for informing the current location of the home agent and foreign agent for the correct forwarding of packets.

Tunnelling

This phase is used to establish a virtual connection as a pipe for moving the data packets between a tunnel entry and a tunnel endpoint.

Applications of Mobile IP

- The mobile IP technology is used in many applications where the sudden changes in network connectivity and IP address can cause problems. It was designed to support seamless and continuous Internet connectivity.
- It is used in many wired and wireless environments where users have to carry their mobile devices across multiple LAN subnets.
- Although Mobile IP is not required within cellular systems such as 3G, it is often used in 3G systems to provide seamless IP mobility between different packet data serving node (PDSN) domains.

Wireless Applications Protocol

Wireless Application Protocol or WAP is a programming model or an application environment and set of communication protocols based on the concept of the World Wide Web (WWW), and its hierarchical design is very much similar to TCP/IP protocol stack design. See the most prominent features of Wireless Application Protocol or WAP in Mobile Computing:

WAP is a De-Facto standard or a protocol designed for micro-browsers, and it enables the mobile devices to interact, exchange and transmit information over the Internet.
WAP protocol was resulted by the joint efforts of the various members of WAP Forum. In 2002, WAP forum was merged with various other forums of the industry resulting in the formation of Open Mobile Alliance (OMA).
WAP was opted as a De-Facto standard because of its ability to create web applications for mobile devices.

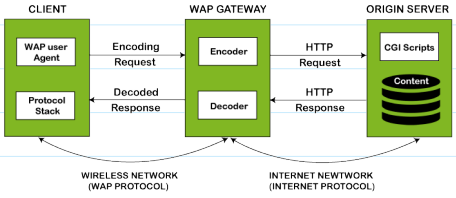
WAP Protocol Stack

It specifies the different communications and data transmission layers used in the WAP model:
Application Layer: This layer consists of the Wireless Application Environment (WAE), mobile device specifications, and content development programming languages, i.e., WML.
Competitive questions on Structures in HindiKeep Watching
Session Layer: The session layer consists of the Wireless Session Protocol (WSP). It is responsible for fast connection suspension and reconnection.
Transaction Layer: The transaction layer consists of Wireless Transaction Protocol (WTP) and runs on top of UDP (User Datagram Protocol). This layer is a part of TCP/IP and offers transaction support.
Security Layer: It contains Wireless Transaction Layer Security (WTLS) and responsible for data integrity, privacy and authentication during data transmission.
Transport Layer: This layer consists of Wireless Datagram Protocol (WDP). It provides a consistent data format to higher layers of the WAP protocol stack.

Working of Wireless Application Protocol or WAP Model

The following steps define the working of Wireless Application Protocol or WAP Model:

- The WAP model consists of 3 levels known as Client, Gateway and Origin Server.
- When a user opens the browser in his/her mobile device and selects a website that he/she wants to view, the mobile device sends the URL encoded request via a network to a WAP gateway using WAP protocol.
- The request he/she sends via mobile to WAP gateway is called as encoding request.
- The sent encoding request is translated through WAP gateway and then forwarded in the form of a conventional HTTP URL request over the Internet.
- When the request reaches a specified Web server, the server processes the request just as it would handle any other request and sends the response back to the mobile device through WAP gateway.



Advantages of Wireless Application Protocol (WAP)

- WAP is a very fast-paced technology.
- It is an open-source technology and completely free of cost.
- It can be implemented on multiple platforms.
- It is independent of network standards.
- It provides higher controlling options.
- It is implemented near to Internet model.
- By using WAP, you can send/receive real-time data.
- Nowadays, most modern mobile phones and devices support WAP.

Disadvantages of Wireless Application Protocol (WAP)

- The connection speed in WAP is slow, and there is limited availability also.
- In some areas, the ability to connect to the Internet is very sparse, and in some other areas, Internet access is entirely unavailable.
- It is less secured.
- WAP provides a small User interface (UI).

Applications of Wireless Application Protocol (WAP)

- WAP facilitates you to access the Internet from your mobile devices.
- You can play games on mobile devices over wireless devices.
- It facilitates you to access E-mails over the mobile Internet.
- Mobile hand-sets can be used to access timesheets and fill expenses claims.
- Online mobile banking is very popular nowadays.

Traditional TCP

Transmission Control Protocol (TCP) is the transport layer protocol that serves as an interface between client and server. The TCP/IP protocol is used to transfer the data packets between transport layer and network layer. Transport protocol is mainly designed for fixed end systems and fixed, wired networks. In simple terms, the traditional TCP is defined as a wired network while classical TCP uses wireless approach. Mainly TCP is designed for fixed networks and fixed, wired networks.

The main research activities in TCP are as listed below.

1. **Congestion control**: During data transmission from sender to receiver, sometimes the data packet may be lost. It is not because of hardware or software problem. Whenever the packet loss is confirmed, the probable reason might be the temporary overload at some point in the transmission path. This temporary overload is otherwise called as Congestion. Congestion is caused often even when the network is designed perfectly. The transmission speed of receiver may not be equal to the transmission speed of the sender. if the capacity of the sender is more than the capacity of output link, then the packet buffer of a router is filled and the router cannot forward the packets fast enough. The only thing the router can do in this situation is to drop some packets. The receiver sense the packet loss but does not send message regarding packet loss to the sender. Instead, the receiver starts to send acknowledgement for all the received packets and the sender soon identifies the missing acknowledgement. The sender now notices that a packet is lost and slows down the transmission process. By this, the congestion is reduced. This feature of TCP is one of the reason for its demand even today.

2. **Slow start**: The behaviour TCP shows after the detection of congestion is called as slow start. The sender always calculates a congestion window for a receiver. At first the sender sends a packet and waits for the acknowledgement. Once the acknowledgement is back it doubles the packet size and sends two packets. After receiving two acknowledgements, one for each packet, the sender again doubles the packet size and this process continues. This is called Exponential growth. It is dangerous to double the congestion window each time because the steps might become too large. The exponential growth stops at congestion threshold. As it reaches congestion threshold, the increase in transmission rate becomes linear (i.e., the increase is only by 1). Linear increase continues until the sender notices gap between the acknowledgments. In this case, the sender sets the size of congestion window to half of its congestion threshold and the process continues.

3. **Fast re-transmission**: In TCP, two things lead to a reduction of the congestion threshold. One of those is sender receiving continuous acknowledgements for the single packet. By this it can convey either of two things. One such thing is that the receiver received all the packets up to the acknowledged one and the other thing is the gap is due to packet loss. Now the sender immediately re-transmit the missing packet before the given time expires. This is called as Fast re-transmission.

Problems with Traditional TCP in wireless environments

- Slow Start mechanism in fixed networks decreases the efficiency of TCP if used with mobile receivers or senders.
- Error rates on wireless links are orders of magnitude higher compared to fixed fibre or copper links. This makes compensation for packet loss by TCP quite difficult.
- Mobility itself can cause packet loss. There are many situations where a soft handover from one access point to another is not possible for a mobile end-system.
- Standard TCP reacts with slow start if acknowledgements are missing, which does not help in the case of transmission errors over wireless links and which does not really help during handover. This behaviour results in a severe performance degradation of an unchanged TCP if used together with wireless links or mobile nodes

#) Data Broadcasting

Datacasting (data broadcasting) is the broadcasting of data over a wide area via radio waves. It most often refers to supplemental information sent by television stations along with digital terrestrial television, but may also be applied to digital signals on analog TV or radio. It generally does not apply to data which is inherent to the medium, such as PSIP data which defines virtual channels for DTT or direct broadcast satellite systems; or to things like cable modem or satellite modem, which use a completely separate channel for data.