

UNIT-I

Application Layer

Q1] What is DNS ? Explain in brief hierarchical structure of DNS. Explain how name resolution happens in DNS. Enlist all the resource records and its function.

-
- DNS also known as Domain Name System (DNS) is a system that translates human readable domain names (www.google.com) into machine-readable IP addresses (eg. 198.68.10.00)
 - It allows user to access website using domain name instead of ^{numeric} IP address
 - DNS runs on UDP and uses port 53

Services provided by DNS

- 1) Host aliasing
- 2) mail service aliasing
- 3) Load Distribution.

Eg → When user enters www.google.com into web browser. DNS converts it into IP address that connects browser with appropriate web server.

Hierarchical structure of DNS

1] Root level (.)

- Topmost level of DNS represented by (.)
- Managed by root name server.

2] Top Level Domains (TLDs)

- eg → .com, .io, .edu, .gov, .in, .org, .net
- Managed by TLD name server.

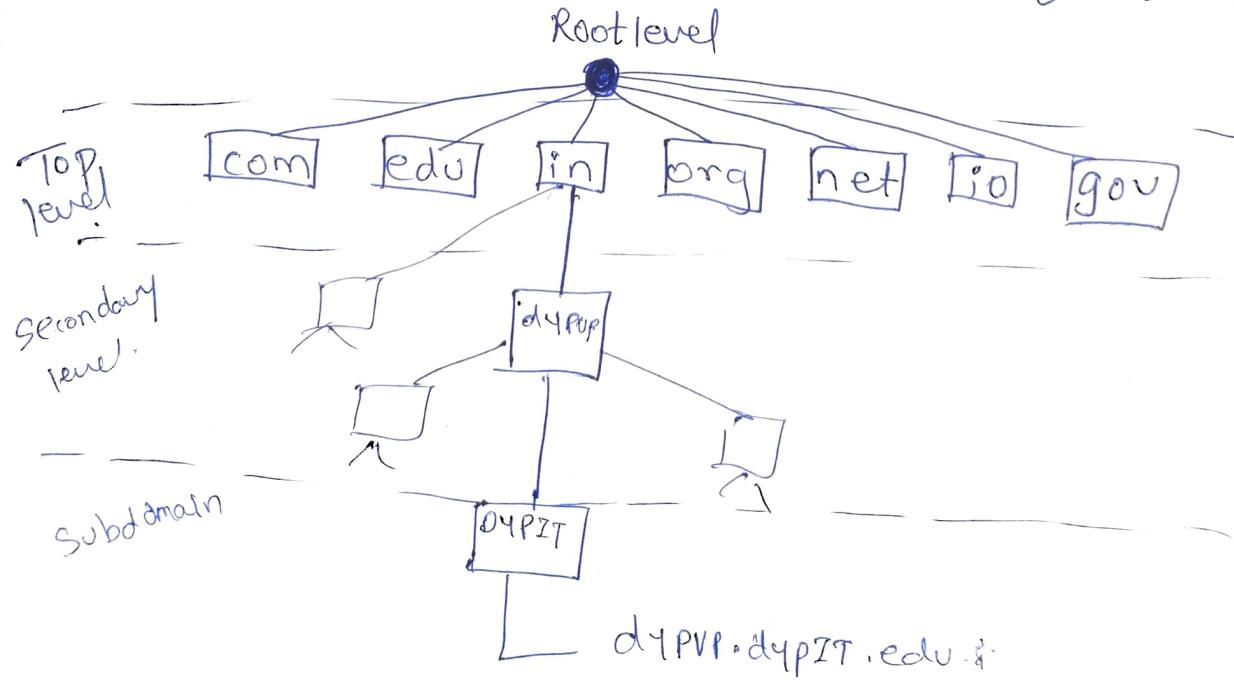
3] Second Level Domains

- Eg → example.com
- Registered by organization or individual
- Managed by Authoritative Name Server

4] Subdomains & Hostnames

eg → www.example.com

- Subdomains are used for organization (eg - blog.example.com)



DNS name resolution process

1] Query Sent to local Resolver

- The User's computer sends the query to local DNS resolver

2] Check Cache

- If IP address found in cache, it is returned immediately

3] Recursive Query to root server

- If not in the cache, resolver queries a root DNS server.

4] Query TLD

- Root level responds for TLD name server e.g. (.com)

5] Query Secondary Level Domain (SLD).

- TLD responds with authoritative name server.
e.g. → Example.com

6] Return IP Address

- Authoritative server provides the IP address, which is returned to the client.

7] Website is loaded

- Browser uses IP to reload the website.

Resources & P^n

A → ~~Address~~ Address record (Maps domain name to IPV4)

AAAA → to IPV6 address

TXT - Text records.

SRV → Service records.

Q] Explain FTP in detail. why FTP requires two TCP ports? Explain commands of FTP

→ FTP(File Transfer protocol) is a standard network ~~for~~ protocol used for transferring files between client & the server over a TCP/IP network. It follows the Client-Server architecture where client requests the files, and the server responds by providing or receiving the files.

Default ports → FTP uses port 21 for control commands and port 20 for data transfer

Modes of operation → FTP can work in Active mode or passive mode. to manage connections between client & server.

Why Two Ports ?

- FTP requires two ports i.e port 21 & port 20 because it ~~for~~ separates ^{command} control and data transfer.

1) Port 21 (control connection)

- Used for sending commands and responses b/w the FTP client & server
- Maintain Session control & authentication.

2] Port 20 (Data connection).

- Used for actual file transfer (upload/download)
- It ensures that connection is uninterrupted during data transfer.

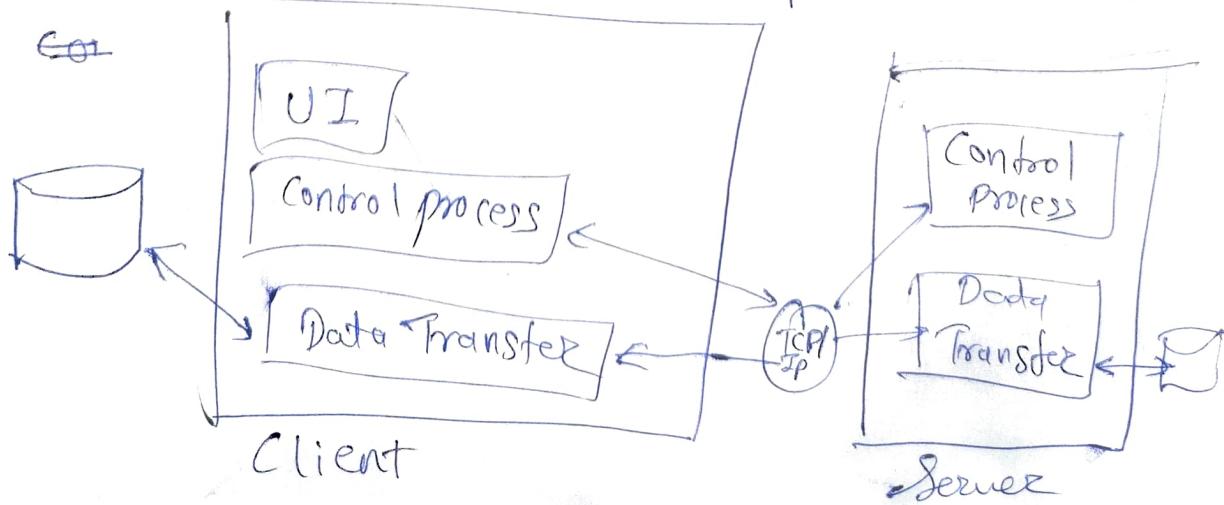
FTP connection modes

1) Active :

- The Client connects to server on port 21 & send the port command
- The server opens a connection from port 20 to client's specified port.
- Client must allow incoming connection which may be blocked by firewall

2] Passive

- When user is behind firewall & cannot accept incoming connections.
- Client request data connection using PASV command
- The server responds with a random port number and client connects to that port for data transfer



Commands

open → connect to computer

get → Retrieve file from the computer

cd → Change directory

close → close FTP connection.

quit → quit FTP

pwd → Display current Directory

Q] Diff between FTP & TFTP

FTP	TFTP
1] FTP uses two connections	1] TFTP uses one connection.
2] Provide many commands	2] Provides only five commands
3] Use TCP	3] Uses UDP
4] Client must login to server	4] No login procedure
5] Allow for user authentication	5] TFTP does not allow for user authentication.
6] FTP provides reliable service	6] TFTP must handle its own retransmissions.
7] file transfer Protocol	7] Trivial FTP

Commands

FTP → close → close FTP connection

quit → quit FTP connection

cd → command or current directory

pwd → Display

open → Connect to computer

get → Retrieve file from computer.

list → get lists.

TFTP → ACK → Acknowledgement.

Error → indicates error.

RRQ → Read request

WRQ → write request.

Data → Transfer file betⁿ client and server

Q] Explain role of SMTP & POP protocols in E-mail message transfer

→ SMTP

- SMTP is application layer protocol for TCP/IP model.
- SMTP stands for Simple Mail Transfer Protocol.
- SMTP transfers message from sender's mail server to the recipient's mail server.
- SMTP interacts with local mail system & not the user.
- SMTP uses TCP socket on port 25, 465 & 587 to transfer email from client to server.

Working of SMTP

- 1) User composes an email in a client (Gmail, Outlook)
- 2) The client sends email to SMTP server over Port 25, 465 (SSL), or 587 (TLS).
- 3) Mail Exchange by DNS MX record.
- 4) Recipient's mail server stores the email until it is retrieved by the recipient using POP or IMAP.

SMTP commands

- 1) Hello → Initiating transaction.
- 2) MAIL FROM → Client to ~~Recipient~~
- 3) RCPT TO → Receiver.
- 4) QUIT → Terminate.

POP

- POP stands for post office protocol
- Post office Protocol 3 is used to transfer emails message from a mail server to mail client software.
- It is responsible for retrieving emails from the mail server and delivering them to the recipient's local device. It ensures that user can access their emails offline.

Working of POP:

- 1] The email client connects to the POP server using Port 110
 - 2] The client downloads all messages to the local device
 - 3] After downloading it gets deleted.
-
- It has two mode Keep mode , delete mode
 - In keep mode, mails are not deleted after downloading
 - In delete mode, mails are deleted after downloading.

Q] What is MIME? Explain MIME header in detail. Discuss its role in SMTP.

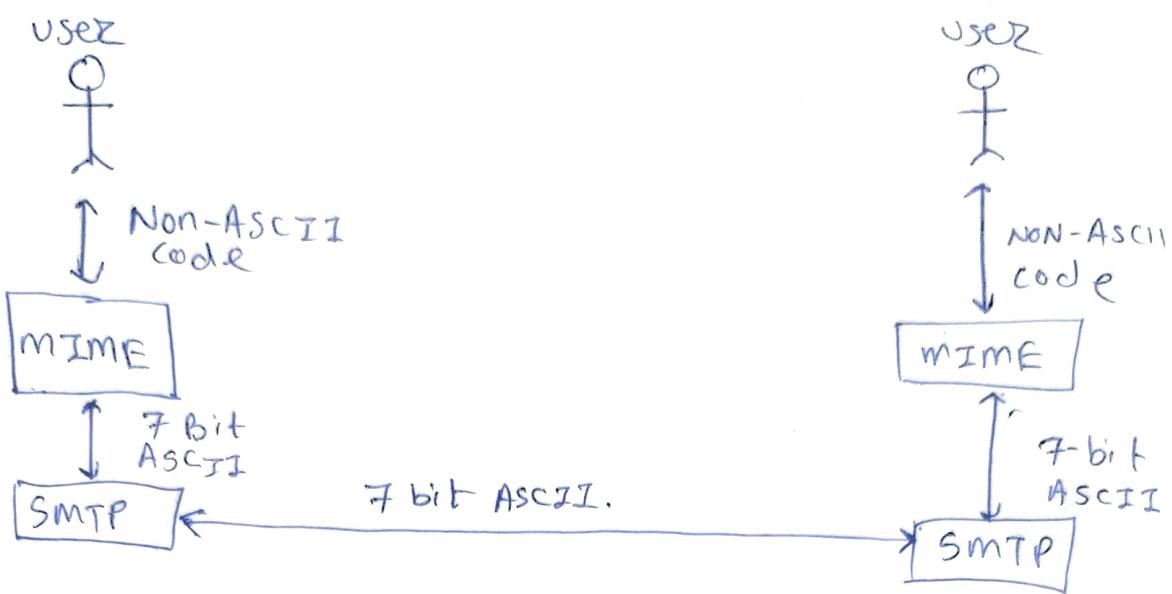
-
- All media types that are sent or received over the world wide web are encoded using different MIME types.
 - MIME - Multipurpose Internet Mail Extensions is an extension of the SMTP that allows email messages to include non-content such as image, audio, video, PDFs, and attachments.

Why is MIME Needed?

- SMTP only supports text
- Enables attachment like images, documents.
 - Allows formatted text.

Header name.	Description
1) MIME-version	specifies the mime version.
2) content-description	what the message is.
3) Content-ID	unique id assigned.
4) Content-Type	Type of Content.

MIME define five headers



SMTP - simple mail Transfer protocol was originally designed to send only plain text messages. However modern email communication requires support for attachments, images, HTML formatting. This is where MIME plays a crucial role by extending SMTP capabilities. Without MIME emails would be limited to simple plain text messages.

Q] Difference between POP3 & IMAP

→ Parameter

	POP3	IMAP
1] Protocol is defined at	RFC 1939	RFC 2060
2] TCP port used	110	143
3] email is stored at	User's PC	Server
4] e-mail is read	offline	online.
5] Time required to connect	Small	long
6] Use of resources	minimal	extensive
7] multiple mail box	Not Possible	Possible
8] for mobile users	Not Good	Good.
9] simple Implementation	Yes	No
10] use case	personal	Business

Q] Explain stepwise the procedure carried out by DHCP client & DHCP server.

1] INIT (initial) State

- The DHCP client starts with no IP address.
- It starts searching for any DHCP server available.
- Message sent to 255.255.255.255.
- This helps in detecting any available DHCP server on the network.

Client: "I have no IP - Is there any DHCP server available?"

2] Selecting State

- After sending DHCPDISCOVER, the client waits for responses from multiple DHCP servers.
- Each DHCP server that receives req. sends DHCPoffer message with an available IP address.
- Client selects one offer from many.

Server 1: "I can offer you 192.168.1.100"

Server 2: " = " "192.168.1.101"

Client: I'll take 192.168.1.100

3] Requesting State

- Client sent DHCPREQUEST message for confirmation of IP address.
- This makes other offers rejected.

Client: I ~~can't~~ accept the IP 192.168.1.100, please accept.

4] Bound State

- DHCP server acknowledges the client's request by sending a DHCPACK message.
- Client starts using IP.
Server : "confirmed! you have 24 hrs"

5] Renewing State

- When so ^{9.} time has passed the client attempts to renew its IP.
- It sends a DHCPREQUEST directly to original DHCP server
- If the DHCP server is available, it responds with DHCPACK,
- If the renewal fails, client moves to the Rebinding state.

client: Can I continue using?

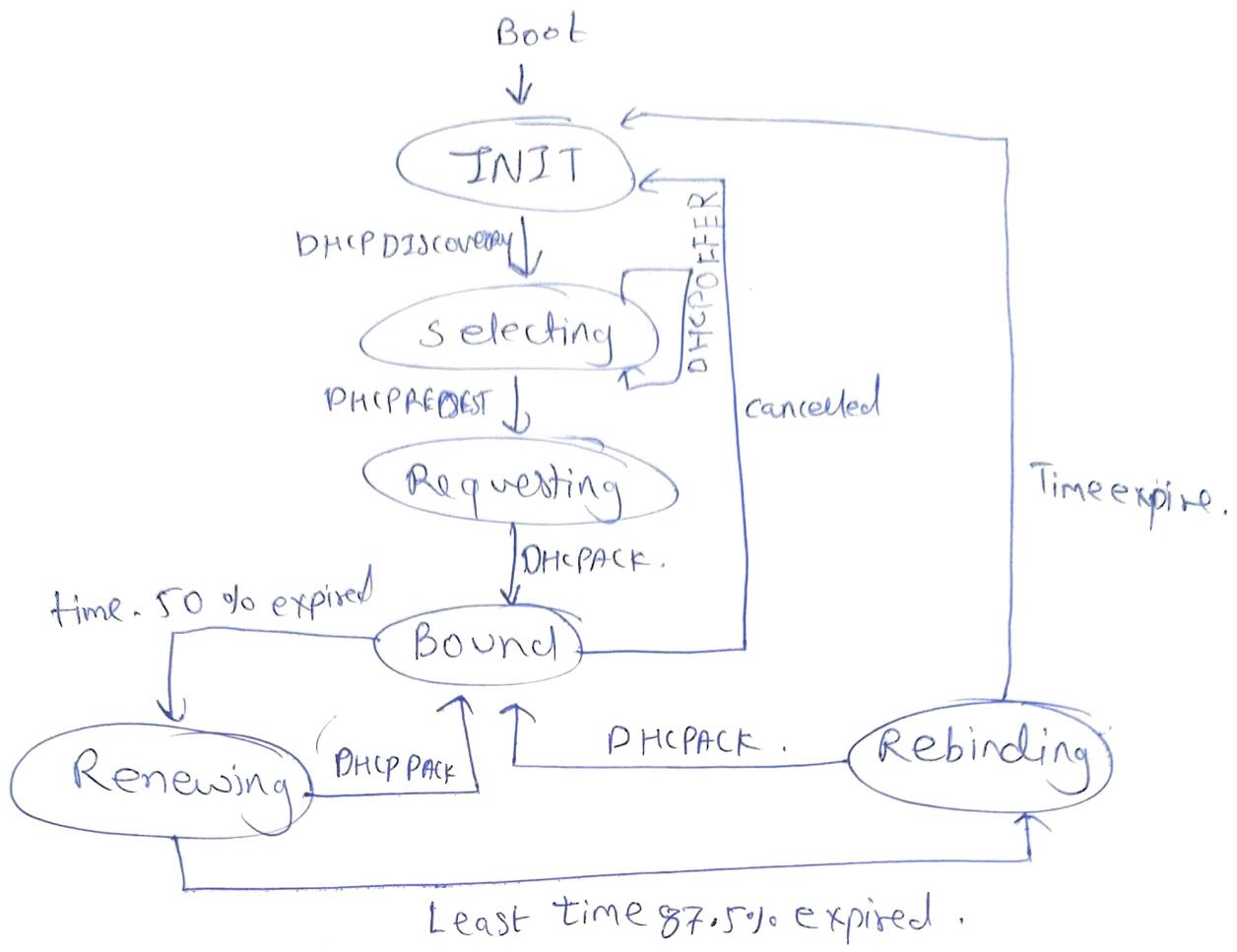
server: "Yes, you can"

6] Rebinding State

- If original server doesn't respond . 87.5% time is over . client start searching other server
- If no response is received , the client moves to INIT state .

client: "my lease is expiring soon! An DHCP server can help?"

server : "I can renew with new IP"

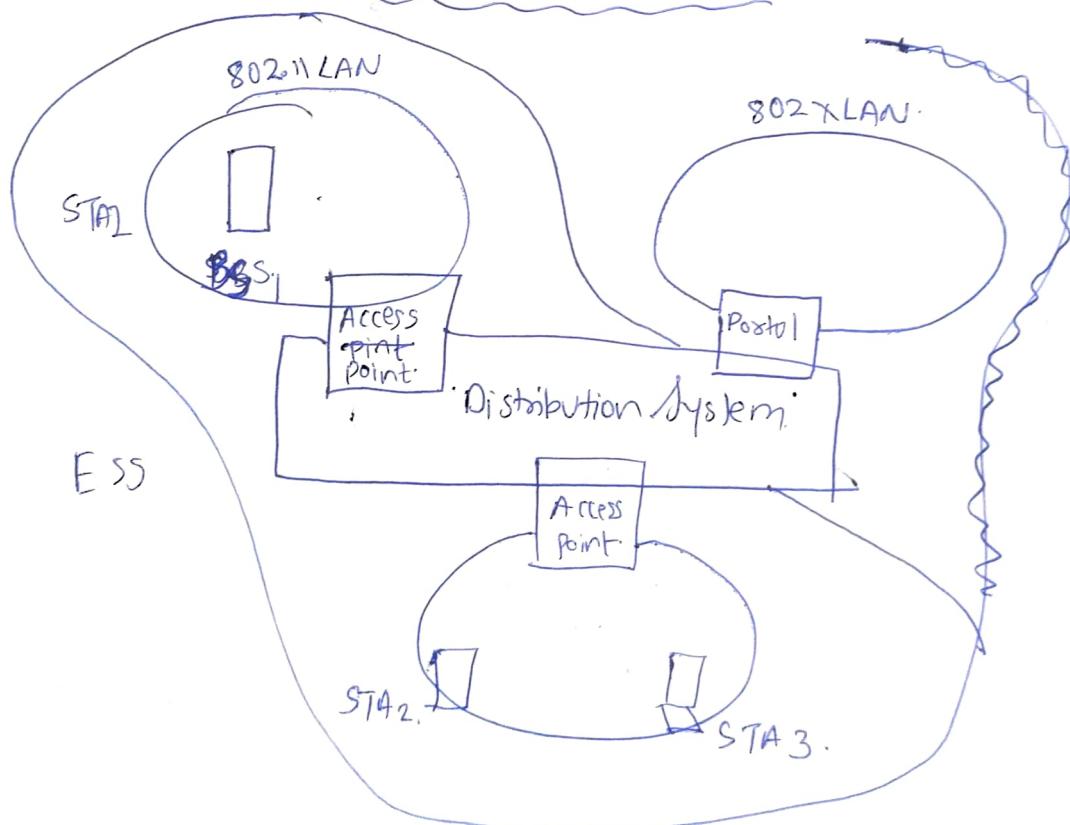


UNIT-II-Wireless Standards

Q] Explain the basic architecture of WLAN and discuss various components in it.

- • Wireless Local area network (WLAN) is a network that allows devices to communicate & connect wirelessly using radio waves instead of wired connections. It is widely used in homes, offices, public places to provide seamless internet access.
- WLAN basically have this architecture
- 1) Infrastructure based WLAN
 - 2) Ad hoc WLAN.

1) Infrastructure based WLAN



1) STA (station)

- Nothing but mobile station

2) Access point (AP)

- They control power management & synchronization function.

- It supports roaming that is changing access point.

3) Port (Po).

- It connects the wired LAN & wireless LAN.

- It is logical interconnection between the two network.

4) Distribution System (DS)

- It is the backbone network that is responsible for MAC layer transport of MAC service data

- The DS connects several BSS via AP to form a single network.

- It handles data transfer betⁿ different AP.

5) BSS (Basic Service Set)

- It is smallest building block of WLAN Network system

- It consists of some number of stations & access point in the network.

6) ESS (Extended Service Set).

- Two or more BSS forming single sub-network.

2] AD-hoc Network.

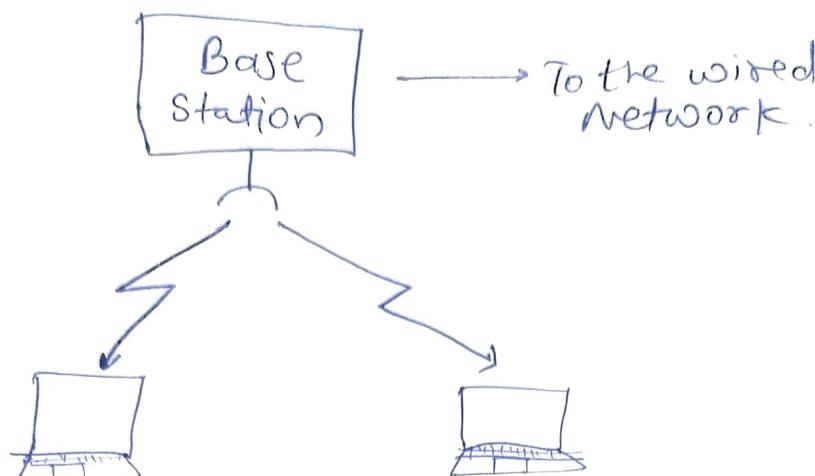
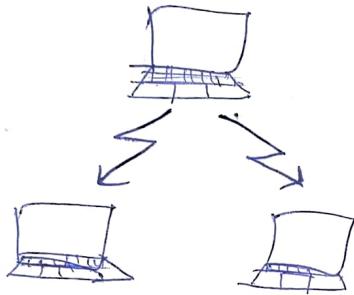


Fig → With base station

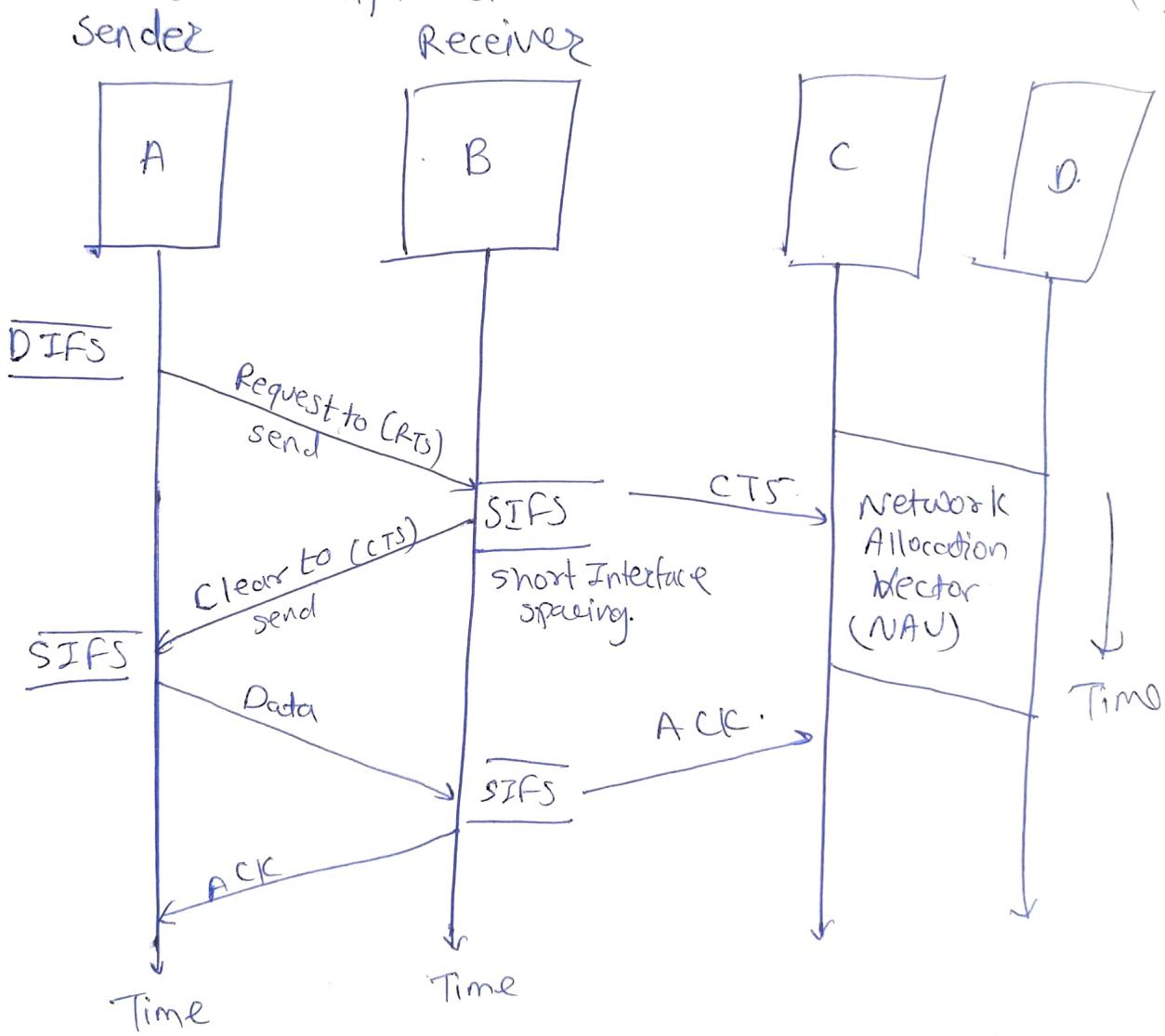


without base station.

- Device communicate directly with each other without AP.
- forms P2P (peer-to-Peer) network for temporary connection
- Generally used for file sharing, Gaming etc..

Q] Explain DCF & PCF in 802.11

- DCF → Distributed co-ordination function
is basic method used to support asynchronous data transfer.
• All station must support the DCF.
• DCF is based on CSMA/CA ⇒ i.e Carrier Sense multiple access with collision avoidance.



- 1) Station A sends signal the Request to send to station B to check whether the station is IDLE or not
- 2) After receiving the RTS, the channel B will send clear to send acknowledgement to station A stating that station B is ready to receive data.
- 3) Station A will send the data after short inter spacing Time.
- 4) After receiving the data, station B will send acknowledgement to station A after SIFS.

PCF (Point Co-ordination Function)

- PCF is an optional MAC protocol used in Infrastructure-based WLAN.
- It is way to avoid collision when multiple device try to send data at the same time.
- It uses AP to decide which device will send data first.

Q2] Compare 802.11 & 802.15. What are the limitations of Bluetooth.

Parameter	802.15	802.11	802.16
1) Protocol	802.15	802.11	802.16
2) Standards	wifi Bluetooth	wifi	wimax
3) Coverage	Person	Within Building or Campus	Within City
4) Performance	Moderate	High	High
5) Frequency	2.4 - 2.483 GHz	5.15 - 5.35 GHz	10 - 66 GHz
6) Cell radius	10 m	1-500 m	1 Km - 50 Km
7) Security	Weaker	Strong	Strongest
8) Power used	Low	High	Highest
9) Speed	Up to 3 mbps	Up to 9.6 Gbps	Up to 1 Gbps
10) Usage	Person to Person	Home, Cafe	Cities, rural areas

Q] Explain frame format of IEEE 802.11

Frame control											
F	Version	Type	Subtype	To DS	From DS	More flag	Retry	Pwr mgmt	More Data	WEP	RSVD
FC	D	Add 1	Add 2	Add 3	SC	Add 4	frame body 0-2312 b			FS	

1] FC → Frame Control → It is 2 bytes long & define the type of frame.

- 1] Version → Current 0
- 2] Type → Info type
- 3] Subtype → Subtype of each type
- 4] To DS → Defined later
- 5] From DS → Defined later
- 6] More flag → 1 → more flag fragment
- 7] ~~Retry~~ → 1 → again
- 8] Pwr mgmt → 1 → pwr mgmt mode
- 9] More data → 1 → more to send
- 10] WEP → 1 → encryption
- 11] RSVD → Reserved
- 12] D → It defines duration of transmission used to set value of NAV.
- 13] Address : There are 4 address each of 6 bytes long, depends on To DS From DS

4] Sequence Control → ⑧. Defines the sequence no. of the frame to be used in flow control.

5] frame Body → It is between 0 & 2312 bytes.

6] FCS: It is 4 byte long & contain CRC-32 error detection.

frame types

1] management frame → Communication betⁿ station & access points.

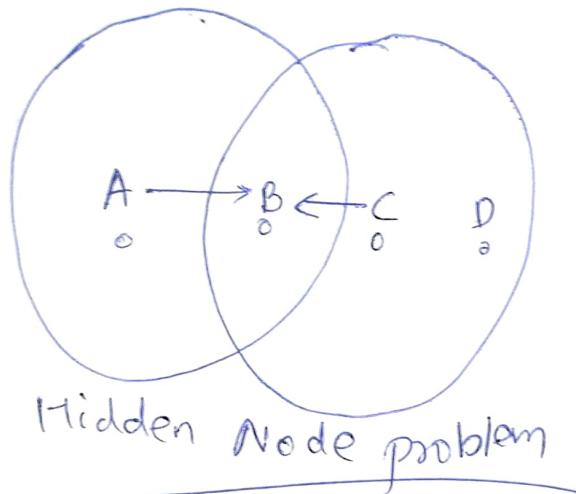
2] control frame → Used for accessing the channel & acknowledgement.

3] Data frames → used for carrying data & control info.

(8) What are hidden station & exposed station problem in WLAN

→ 1] Hidden Station Problem

- Occurs when two stations are out of each other's range but both can communicate with a common access point.
- This leads to collision, as the stations are unaware of each other.



e.g. →

- A is transmitting to station B
- C is also
- Station A ~~can't~~ station C cannot hear each other but both are within range of station B
- Since A is hidden from C, A & C gets collide.

Solⁿ

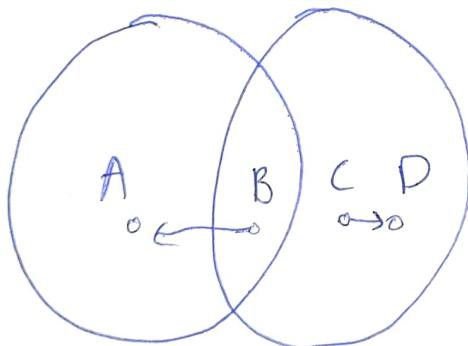
1] Request to send (RTS)

2] Clear to send. (CTS)

This mechanisms are used.

2] Exposed Station Problem

- Occurs when station senses the transmitting and unnecessarily stop transmitting, even though they do not cause interference.
- This leads to wastage of network capacity.



Exposed Node problem.

- B is transmitting to A
 - C hears B's signal assume channel is busy
- C stops transmitting even though there is no connection b/w them

Sol¹

1] RTS 2] CTS

Q] Explain Bluetooth architecture with diagram

- • Bluetooth is short-range wireless technology used for communication betⁿ devices.

Bluetooth have two main architectures -

1] Protocol stack (Software Architecture)

2] Topological Architecture (Hardware Architecture)

1) Topological Architecture .

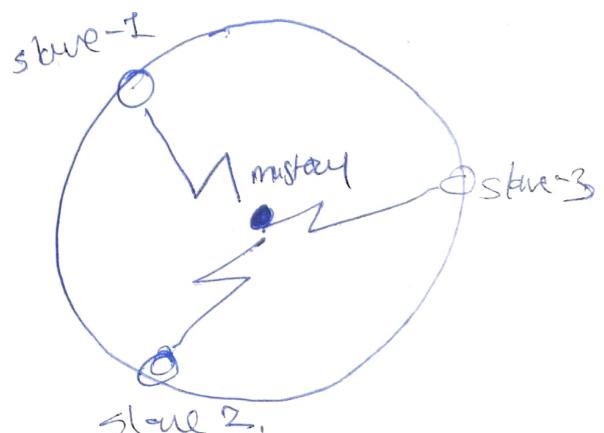
- It is based on master-Slave communication consist of .

A) Piconets.

- Basic unit of Bluetooth communication
- consists of one Master ~~Slave~~ & upto 7 master slaves.
- Master control communication & slave responds
- Slave ~~s~~ cannot communicate with each other directly they connect with Master.



a) Single-Slave piconet.

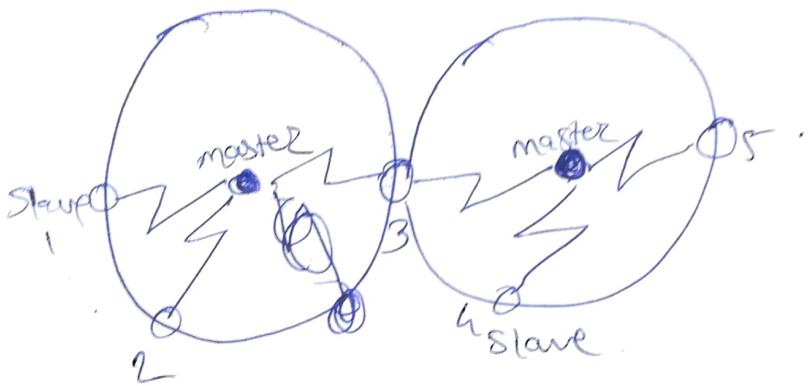


b) Scatternet

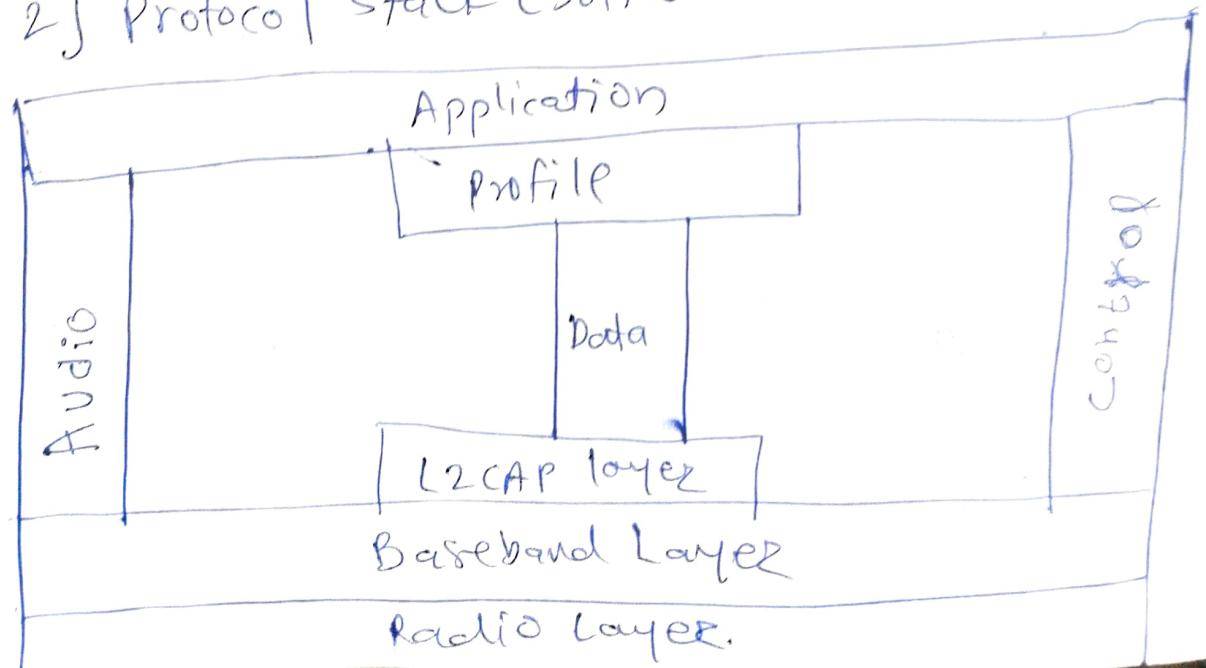
• formed when two or more piconet are interconnected

- A device can be a slave in one piconet & master in another.
- Increase range & connectivity.

e.g. → headphone connected to Laptop & Laptop connected with smartphone.



2] Protocol stack (Software Architecture).



1) Radio Layer

- Handles wireless transmission over the 2.4 GHz band

2) BaseBand Layer

- Controls master slave communication
- Manages device addressing, packet formation, & timing

3] Logig

3) Logical Link Control & Adaptation Protocol (L2CAP)

- Manages data Segmentation & reassembly.
- Provides quality of service.

4] HCI

- Acts as a bridge betⁿ hardware & software layers.

5] Application layer

- Defines specific application-level services

Limitations

- 1) Limited Range
- 2) Low Data Range
- 3) Interface Issue
- 4) Limited Scalability.

QJ What is WiMax? List the advantages of WiMax?

-
- WiMax stands for Worldwide interoperability for microwave Access
 - WiMax is based on IEEE 802.16 standards.
 - Provides high speed Internet access over long distance
 - Supports both fixed & mobile broadband services.
 - WiMax consists of
 - 1) WiMax tower
 - 2) WiMAX receiver

Advantages

- 1] Wide coverage Area
- 2] High Data speed
- 3] Cost - Effective
- 4] Scalability
- 5] Supports Mobility
- 6] Secure .