DAY 02 24-12-2024

★ Advantages

1) It is centralised, which means that all data and services are stored and managed in a single place. This makes it easier to maintain, update and secure the system.

2) It is cost-effective, as it requires less hardware and software resources for the client side. The client only needs a network connection and an application or web browser to access the server.

3) It has high performance and low latency, as the server can handle many requests from many clients simultaneously and efficiently.

★ Disadvantages

1) It has limited scalability, as it depends on the capacity and availability of the server. If the server is overloaded or fails, the system may not function properly or at all.

2) It has high network dependency, as it relies on the network connection between the client and the server. If the network is slow or disrupted, the system may experience delays or errors.

3) It has complex architecture, as it involves multiple components and layers that need to be designed, implemented and coordinated. The system may also face challenges such as security, synchronisation and compatibility.

✱ OSI Model

① Physical layer - Transmits raw bit stream over the physical medium.

② Data Link Layer - Defines the format of data on the network.

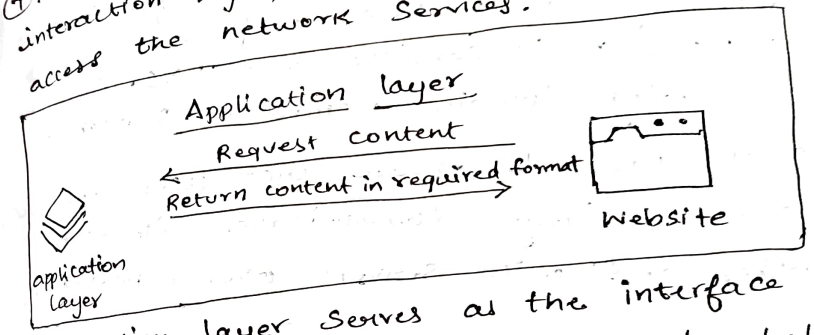
③ Network Layer - Decides which physical path the data will take.

④ Transport layer - Transmits data using transmission protocols including TCP and UDP.

⑤ Session layer - Maintains connection and is responsible for controlling ports and sessions.

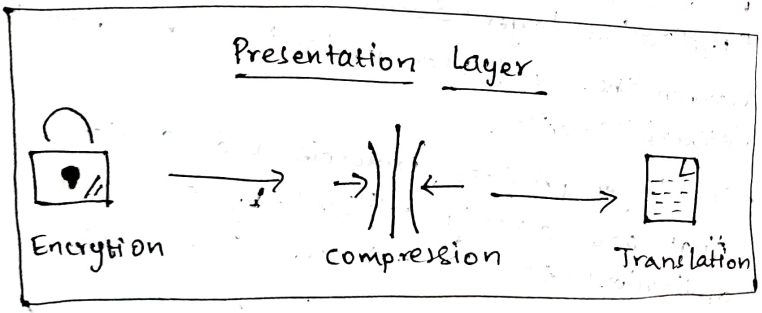
⑥ Presentation layer - Ensures that data is in a suitable and usable format and is where data encryption occurs.

⑦ Application layer - Human - computer interaction layer, where applications can access the network services.

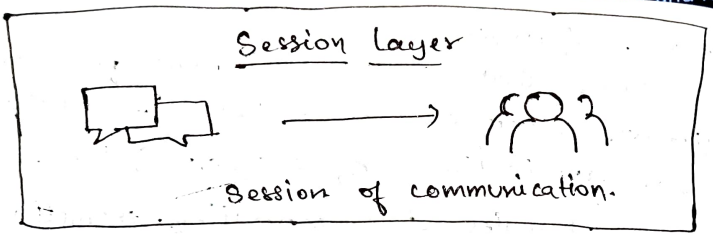


- Application layer serves as the interface between the end user applications and underline network services.
- The layer provides protocols and services that are directly utilized by end user applications to communicate across the network.
- Key functionalities of the application layer includes resource sharing, remote file access and network management.

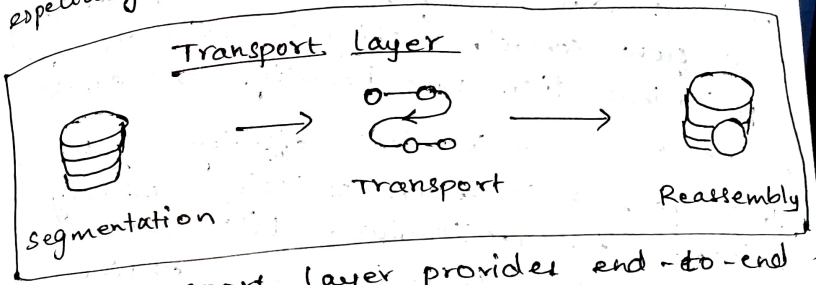
- Examples of protocols operating at the application layer include: HTTP for web browsing, FTP - File Transfer, SMTP - Email services and DNS - for converting domains names to IP addresses.
- These protocols ensure that user application can effectively communicate with each other and with servers over a network.



- The presentation layer is also known as Syntax layer.
- It is responsible for translating the data between the application layer and the network format.
- It ensures that the data sent from the application layer of one system is readable by the application of another system.
- This layer handles data formatting, encryption, and compression facilitating interoperability between different system.
- One of the key roles of presentation layer is data translation and code conversion.
- It transforms data into a format that the application layer can understand.
- It also includes encryption protocols to ensure data security during transmission and compression protocols to reduce the amount of data, for efficient transmission.

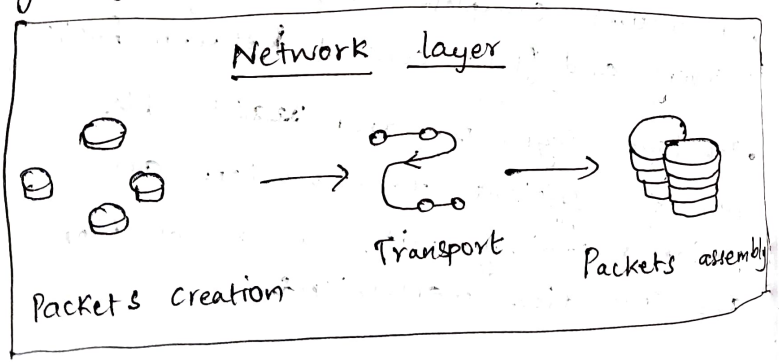


- The session layer manages and controls the connections between computers.
- It establishes, maintains and terminates connections, ensuring that data exchanges occur efficiently in an organized manner.
- The layer is responsible for check pointing and recovering, which allows sessions to resume after operations.
- The protocols operating at the Session layer include RPC - Remote Procedure Call which enables a program to execute a procedure on a remote host as if it were local and the session establishment face in protocols like SQL.
- These services enable reliable communication especially in complex network environments.



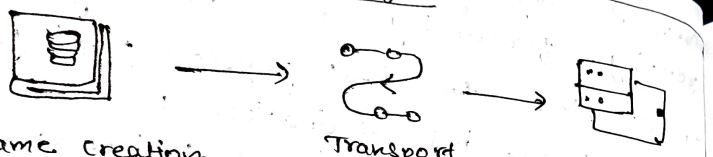
- The transport layer provides end-to-end communication services for applications.
- It ensures complete data transform, error recovery and flow control between hosts.
- This layer segments and reassembles data for efficient transmission and
- provides reliability with error detection and correction mechanisms.

- Protocols at this layer include TCP and UDP.
- TCP is connection oriented and ensures reliable data transfer with error checking and flow control, making it suitable for applications like web browsing and email.
- UDP is connection less offering faster but less reliable transmission usually suitable for applications like video gaming, video streaming and online gaming.



- Network layer is responsible for data routing, forwarding, and addressing.
- It determines the best physical path for data to reach its destination based on network conditions, Priority of service and other factors.
- This layer manages logical addressing through IP addresses and handles packet forwarding.
- Protocols for this layer include IP for routing and addressing ICMP (Internet control Message Protocol) for diagnostic and error reporting purposes and routing protocols like RIP (Routing Information Protocol) that manages routing of data across networks

Data Link layer

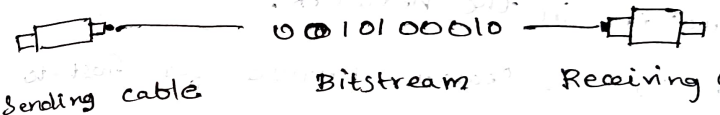


- The data link layer is responsible for node-to-node data transfer, error detection and correction.
- It ensures that data is transmitted to the correct device on local network segment.
- This layer manages MAC addresses and is divided into two sub layers LLC and MAC.

LLC - logical Link Control
MAC - Media Access Control

- Protocols include ethernet which defines the rules for data transmission over local Area Networks and point to point protocol for direct connections between two network nodes.
- It also has mechanisms for detecting errors and correcting those errors that occur in physical layer.

Physical layer



- This physical layer is responsible for physical connection between devices.
- It defines the hardware elements involved in the network including cables, switches, & other physical components.
- This layer specifies electrical, optical and radio characteristics of the network.

- functions of the physical layer include the modulation, bit synchronization, and transmission of raw binary data over the physical medium.

- Technologies such as wifi operate at this layer ensuring that the data physically moves from one device to another, in the network.

(NOTE: You can search, browse for host-to Host communication)

IOT OSI Model

People & Process - Layer 7 - Transformational decision making based on "Thing"

Applications & Data

Applications - Layer 6 - Custom Apps built using "Thing" data

} Business value

Data Analytics - Layer 5 - Reporting, mining, Machine Learning

Data Ingestion - Layer 4 - Big data, Harvest & Storage of "Thing" data

} Big data

Global Infrastructure - Layer 3 - Cloud Infrastructure (Public, Private, hybrid, managed)

} - cloud

Connectivity / Edge Computing - Layer-2 - Communications, Protocols, Networks, Wifi, Telecom

Things - Layer 1 - Devices, sensors, Controllers, etc.

} - fog

★ Protocols

There are 3 types of protocols in Network

1. Network communication
2. Network Management
3. Network Security

- Network Communication Management:
  - HTTP - HyperText Transformation Protocol
  - TCP - Transmission Control Protocol
  - UDP - User Datagram Protocol
  - BGP - Border Gateway Protocol
  - ARP - Address Resolution Protocol
  - IP - Internet Protocol
  - DHCP - Dynamic Host Configuration Protocol

- Network Management:
  - ICMP - Internet Control Message Protocol
  - SNMP - Simple Network Management Protocol
  - FTP - File Transfer Protocol
  - POP3 - Post Office Protocol
  - TELNET - Telecommunication Network

- Network Security
  - HTTPS - Hyper Text transmission Protol which is secure.
  - SSL - Secure Socket layer
  - TLS - Transport layer Security

- Other Protocols
  - IMAP - Internet Message Access Protocol
  - SIP - Session Initiation Protocol
  - RTP - Real time Transport Protocol
  - RLP - Resource Location Protocol
  - PPTP - Point-to-Point Tunneling Protocol

★ Ports and Networks

- Ports:
  - whenever any application in one computer sends data to another application to offer different computer. Then it sends using IP address and MAC address
  - The System understands that this data is for a Specific application through the port mentioned

• In a computer, data is first received using their IP or MAC address then it is delievered to the application whose port number is with the data packets.

★ Types of Ports

1. Well known Ports
2. Registered Ports
3. Dynamic Ports

1. Well-known Ports :

- It is from the range 0 to 1023
- It is reserved for common and specifically used service.
- It is used by some widely adopted protocol and services like HTTP (Port 80) FTP (Port 21), DNS (Port 53), SSH (Port 22) etc.,

2. Registered Ports :

- It is from range 1024 to 49151
- These are used by applications or services that are not as common.
- But it is used by those applications or services which require its Specific Port.
- organizations can ask IANA (Internet Assigned Number Authority) for any specific port number within this range.

3. Dynamic Port

- It is from range 49152 to 65535
- It is also known as Ephemeral or Private Port.
- It is used for those connections that are temporary or short-lived.
- It is not registered or assigned and can be used by any process.

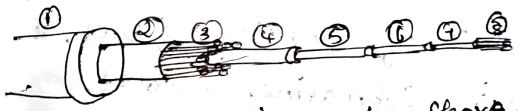
★ Why ports are required?

1. Multiplexing and Demultiplexing
2. End-to-End Communication
3. Protocol Identification
4. Security and firewalls
5. Load Balancing
6. Custom Application Communication

Important Port Numbers

Port Number	Service	used for	Protocol
20	FTP-DATA	file transfer	TCP
21	FTP	File transfer control	TCP
22	SSH	Secure Remote login	TCP
23	Telnet	Unencrypted Remote Access	TCP
25	SMTP	Email Routing	TCP
53	DNS	Domain Name Resolution	UDP/TCP
67	DHCP-S	DHCP Server	UDP
68	DHCP-C	DHCP Client	UDP
69	TFTP	Trivial File Transfer	UDP
80	HTTP	Web Traffic	TCP
110	POP3	Email Retrieval	TCP
123	NTP	Time Synchronization	UDP
143	IMAP	Email Management	TCP
443	HTTPS	Secure Web Traffic	TCP
3306	MySQL	Database Service	TCP
3389	RDP	Remote Desktop Access	TCP
5432	PostgreSQL	Database Service	TCP
5060	SIP	VoIP Communication	UDP/TCP
5900	VNC	Remote Desktop Sharing	TCP
8080	HTTP-ALT	Alternative Web Traffic	TCP
2049	NFS	Network file System	TCP/UDP
161	SNMP	Network Management	UDP
162	SNMP-TRAP	SNMP Trap Messages	UDP
445	SMB	File Sharing	TCP
27017	MongoDB	Database Service	TCP
5000	UPnP	Universal Plug and Play	UDP/TCP

* Submarine Cables - Under water cable



A Cross section of shore-end of a Submarine cable.

1. Polyethylene
2. mylar tapes
3. Stranded steel wire
4. Aluminium water barrier
5. Polycarbonate
6. Copper or aluminium tube
7. Petroleum jelly
8. Optic fibres.

- Submarine cables play a critical role in global interconnected networks.
- It caries around 99% of international communication traffic.
- There has been an exponential increase in the demand for data and bandwidth intensive applications, which includes audio and video streaming and growing demand for cloud based services.
- Submarine cables exist from 1850's and it is used for telegraph and later tele communication use cases and applications
- After emergance of optical fibres, it has been used in Submarine cables.
- The current speed is around 200Terabits per second. and there are appoximately 400 Submarine cables with 1.2 million kilometers criss crossing the earth.
- Multiple global telecom companies and internet providers have come together to finance this global Submarine network cable connectivity.

*Factors contributing to the growth of global submarine cables

i) cloud Services
ii) Data centres
iii) Content Delivery Networks
iv) Enterprise Applications
v) OTT
vi) Mobile applications

★ ~~Network Topologies~~ ★ Network Architectu

LAN - local Area Network
MAN - Metropolitan Area Network
WAN - Wide Area Network

★ LAN - Local Area Network

- Short for local area network
- Connects a group of computers within a limited geographic area.
- High bandwidth for data transfer.
- Owned by private companies or individuals.
- Limited to 100 to 1000 meters.
- Lower setup cost due to inexpensive devices.
- Higher data transfer speeds with 10, 100 and 1000 Mbps high-speed ethernet.

★ WAN - Wide Area Network

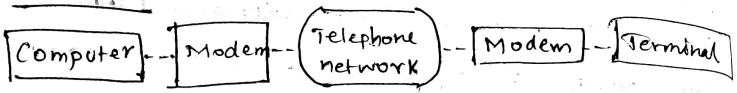
- Short for wide area network.
- Covers a large geographical area such as a state, country or a continent.
- Low bandwidth for data transfer.
- Established under distributed ownership.
- spans a huge area of 100,000 kilometers.
- Higher setup cost than LAN and MAN
- Low data transfer rates between 10 to 60 Mbps.

★ MAN - Metropolitan Area Network

- Short for metropolitan Area Network
- confined to a city or town. Distance coverage is larger than LAN and smaller than WAN.
- Bandwidth is moderate for data transfer.
- Ownership can be private or public.
- Distance Coverage is up to 100 kilometers
- Moderate installation costs.
- Speed Can go up to 100 Mbps

★ Modem vs Router

★ Modem



• A modem is a short form of Modulator/Demodulator. The modem is a hardware component / device that can connect computers and other devices such as routers and switches to the internet. Modems convert or modulate the analog signals coming from telephone wire into a digital form that is in the form of 0's and 1's.

• It acts as a bridge between the telephone line and the computer.

• It converts the input analog signal to a digital signal and directs it to the computer and vice versa.

★ Router

• The Router is supposed to connect totally different networks along.

• The essential distinction between electronic equipment and a modem router is that electronic equipment is necessary for connecting your electronic network to the web whereas, a router is crucial to direct the trial to the traffic of information packets on the network.

Modem	Router
• The modem is crucial to access the net because it connects your laptop to ISP.	• While in which you can access the net while not employing a router.
• In modem, the information packet is not examined; thus the security threat is often there	• While in the router, the information packet is always examined before forwarding it, to work out the threat.
• It is placed straight to the computer or It is also placed between a telephone line and a router.	• While a router is placed between electronic equipment and a network.
• The modem performs Signal decoding by decoding the ISP Signal.	• While a router does not perform Signal decoding.
• Modem brings the requested info from the net to your network.	• While the router distributes that requested data to your PC.
• Modem is not secure.	• Router is secure

⊙ Types of Modem

i) Dial-up ii) Digital Subscriber Line
iii) Satellite Modem iv) Cable v) internal modem
vi) External modem vii) Two-wire modem
viii) four-wire modem

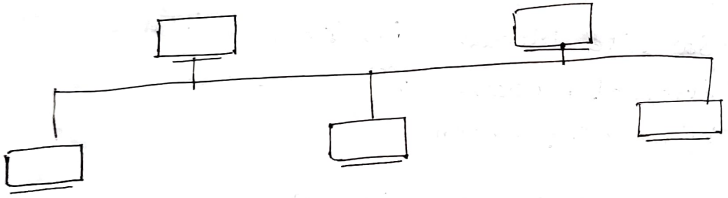
★ Types of Network Topology

i) Point-to-Point Topology

• Point-to-Point is a simple topology that directly links two nodes and reserves the entire bandwidth of the connection for them to communicate with one another.

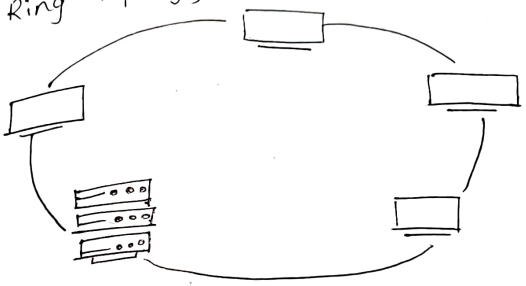
- Physically, point-to-point connections rely on a cable or wire that connects the two endpoints.
- However, logical topological connections using satellite links and microwaves are more common nowadays.

ii) Bus Topology

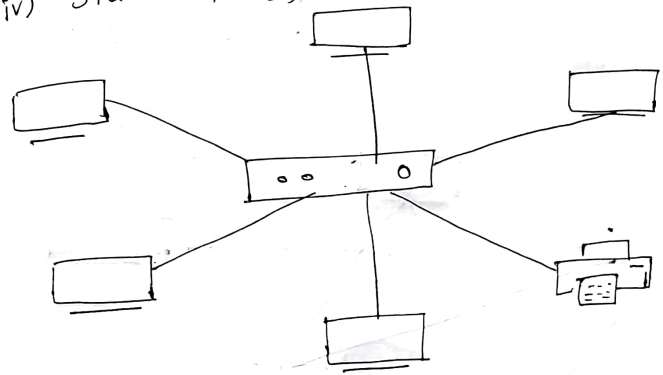


- In a bus topology, all nodes or devices are connected to a single central cable known as bus or backbone.
- The configuration is often used in local area networks (LANs) due to its simplicity and ease of installation.

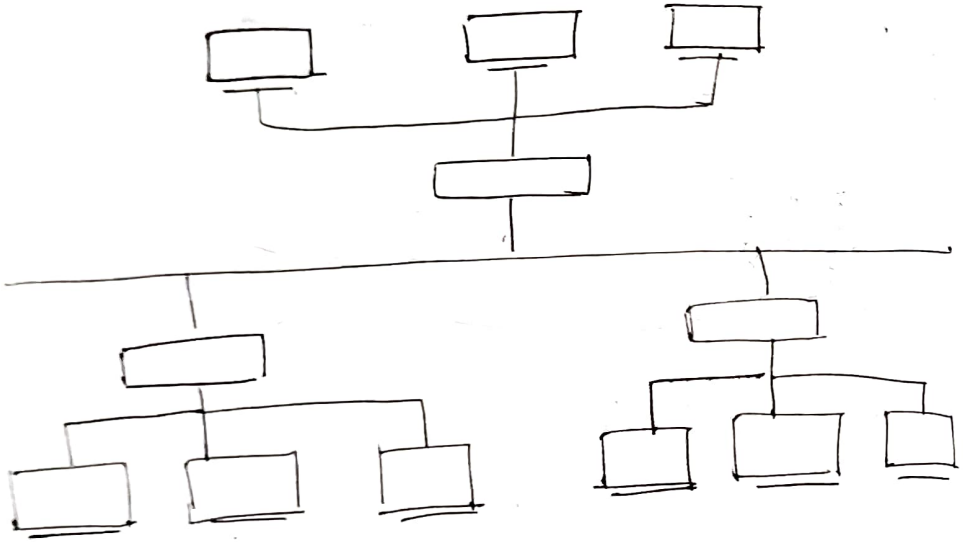
iii) Ring Topology



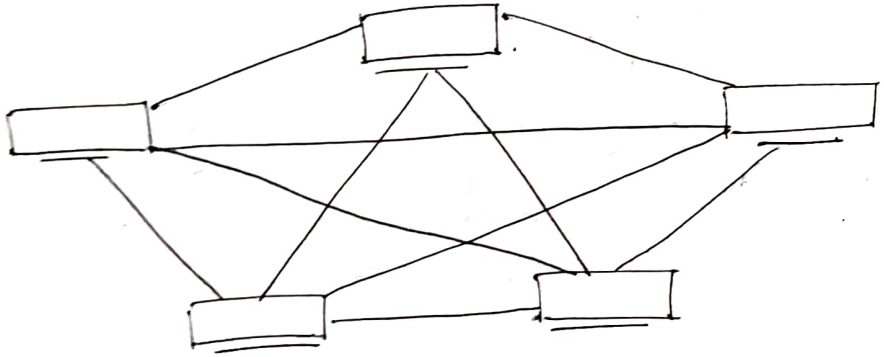
iv) Star Topology



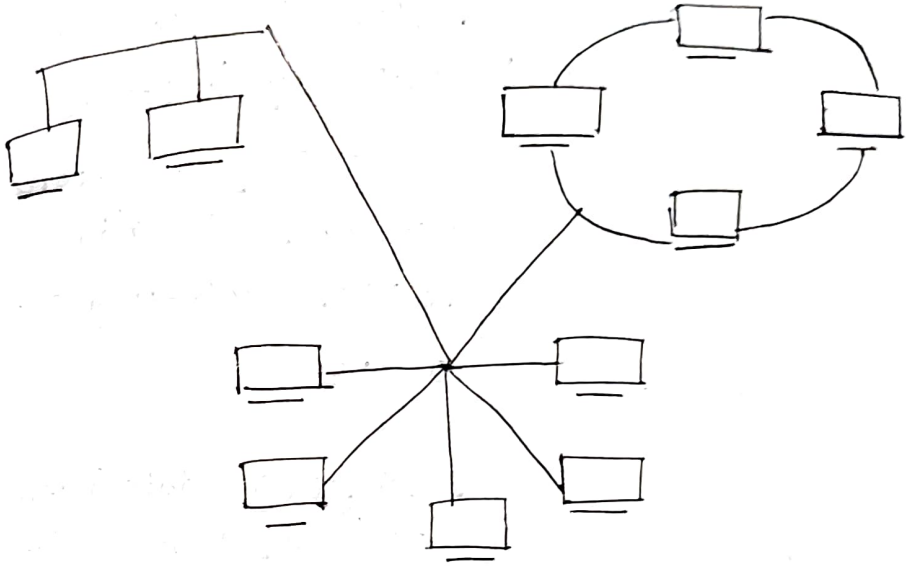
v) Tree Topology



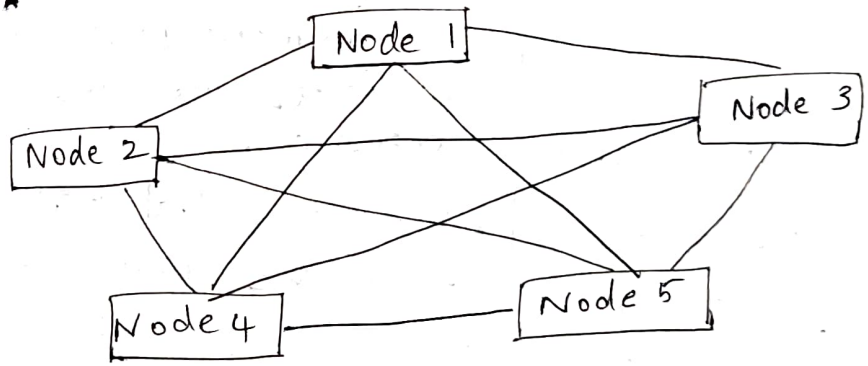
vi) Mesh Topology



vii) Hybrid Topolgy



★ Peer to Peer Architecture



• Peer to Peer architecture customized protocols to ensure decentralized networks can support specific usecases.

Pros	Cons
• There is no Single Point of failure (SPOF) Since the network is not dependent on a central server. If one node fails, the network can still function.	• Without a central authority, it can be challenging to enforce network security policies uniformly across all nodes.
• P2P scales up naturally.	• Difficult data integrity if nodes join and leave.
• Lower cost of maintainence.	• Performance degrade if too many peers need to access the same resources.
• P2P network offers anonymous and Privacy network.	• Without central control, it can be difficult to prevent the distribution of harmful or unethical content.

• The purpose of the protocols is to ensure that the data is distributed accross the network and that nodes can locate and exchange data with each other.

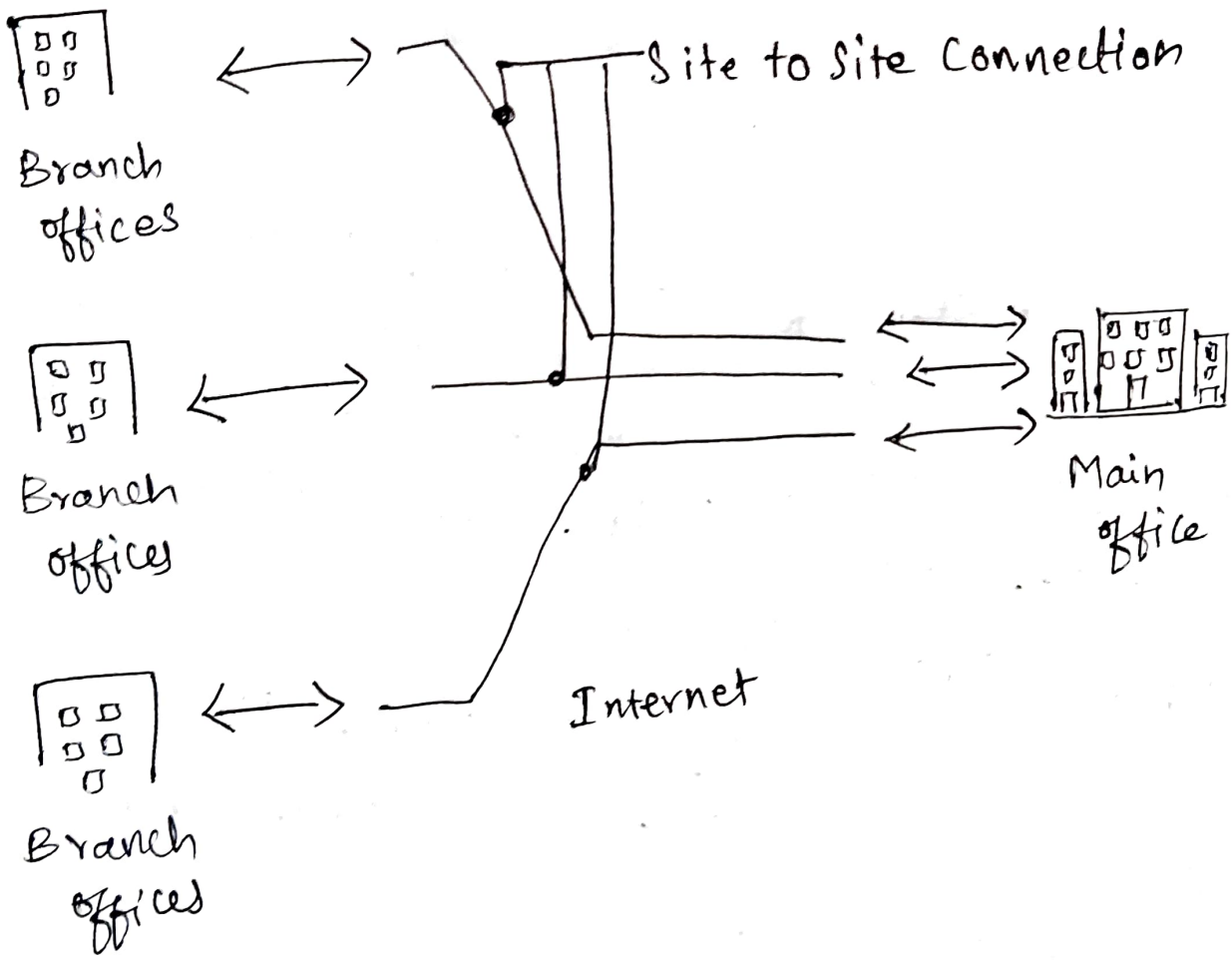
★ VPN (Virtual Private Cloud)

• It is a technology that allows to create a secure and private connection over a less secure network.

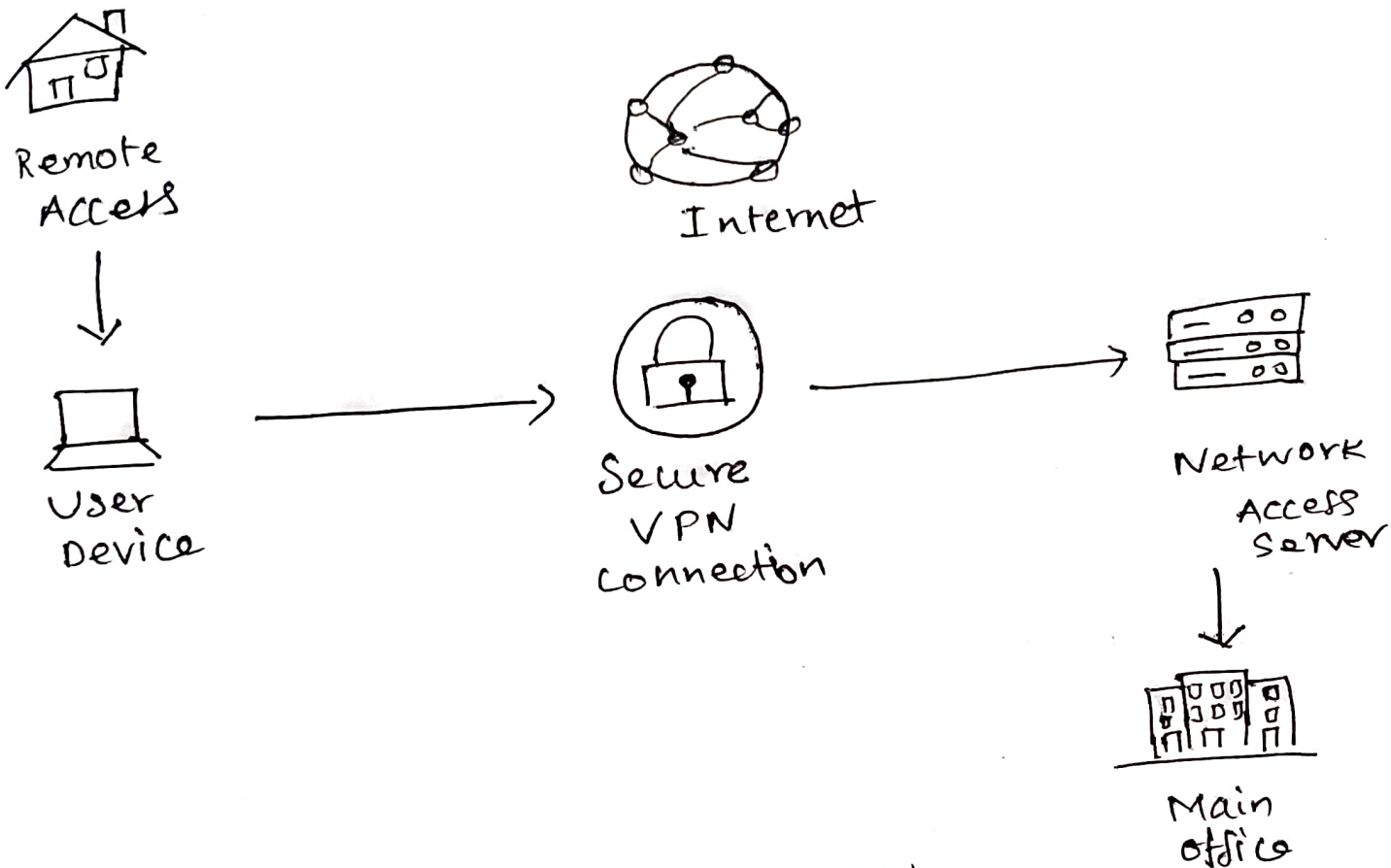
- Types of VPN

1. Site-to-Site VPN
2. Remote access VPN
3. Cloud VPN
4. SSL VPN
5. Double VPN

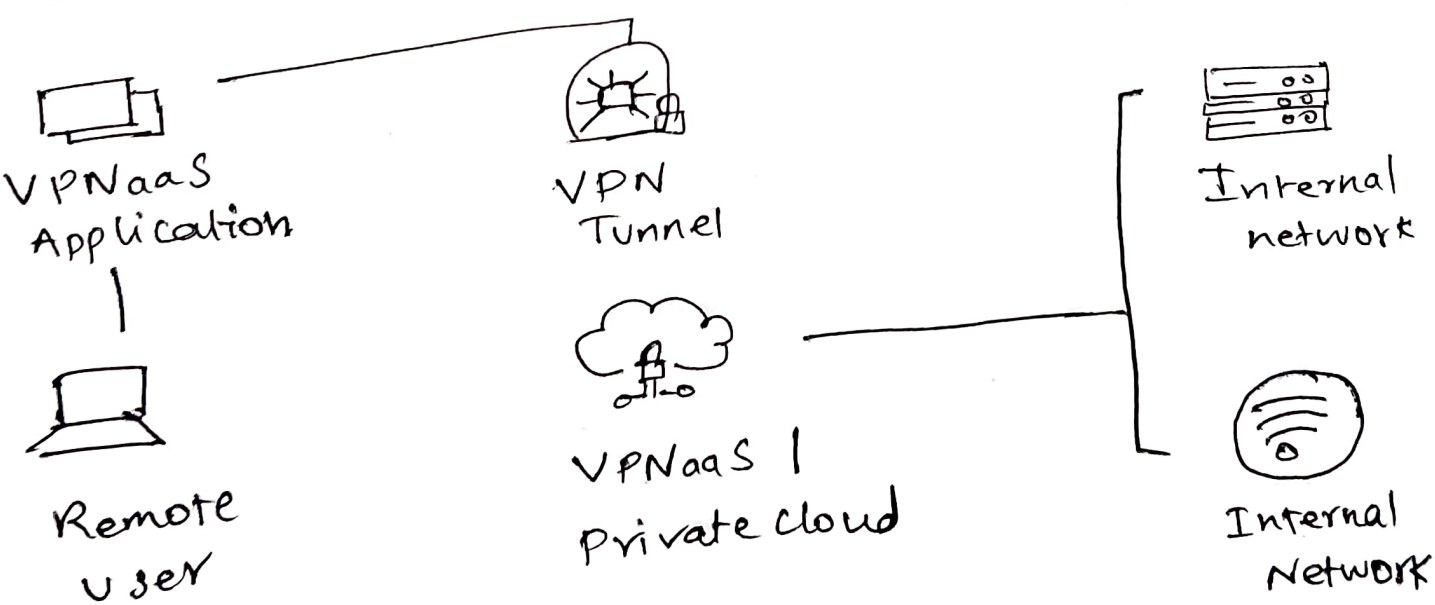
1. Site-to-Site VPN



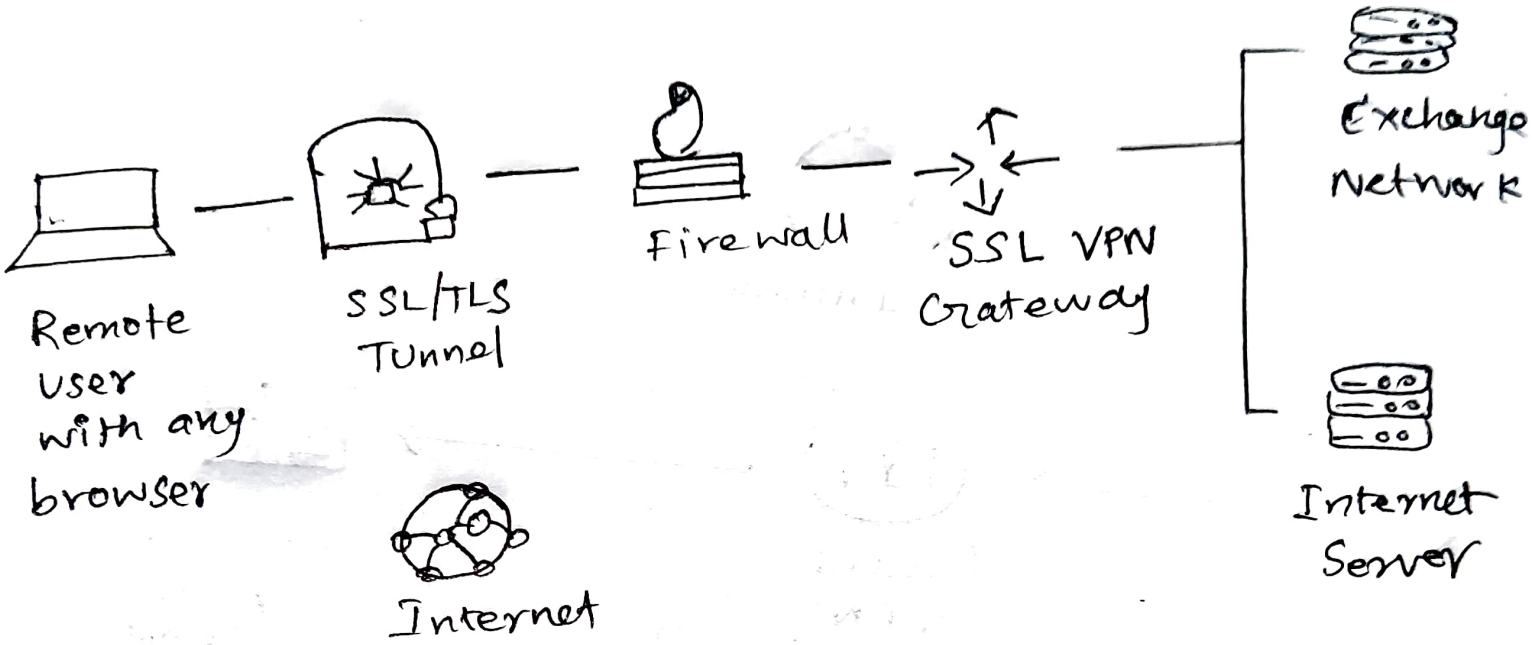
2. Remote Access VPN



3. Cloud Remote Access VPN



4. SSL VPN



5. Double VPN