**1: Networking – Models and protocols**

**1.1: What is Devops & Why:**

It is the combination of Development and Operations. It is used to speed of the cycle without Latency.

**1.2: OSI Model:**

OSI – Open-Source Interconnection having 7 layers:

1. **Physical Layer:** connects Physically (Hub, Modems, Cables)

* Bits

1. **Data Link Layer:** data transfer node to node, by making it error free.

* When the packet came to network it will DLL responsible for delivery to host by MAC Address

1. **Network Layer:** Transfer data from one host to another located in different network

* It also takes care of routing, noting but identifying the shortest path.

1. **Transport Layer:**  In form of segments, like delivering the message completely

* Order of the Data(Sequence)

1. **Session Layer:** Manages the connection and how long it should be last.
2. **Presentation Layer:** Encryption and formatting.
3. **Application Layer:** Create Data

**1.3: Connection Oriented :** Checks whether the messages are delivered and checks aby left overs and recover it.

**1.4: Windowing :**  We can control the flow of date between 2 devices.

* First the data is divided in to chunks.
* By giving window size to chunks we can deliver without the ack of the receiver like we can send 1 , 2, 3 and wait for Ack
* If the receiver is fast then we can speed up vice versa.

**1.4: Client Server Model:** Client will request to the server and server will give the data.

**1.5: TCP/IP: (Connection oriented)**

**TCP:** It is the set of rules that will ensure the data is transfer, received securely via internet.(Handshake)

**IP:** Ensure delivered to correct address. (IP Addresses are unique while in network, like a postal code so that can deliver to the correct destination)

**1.6: UDP: (Connection less)**

Faster then TCP , but not reliable , not error free

**1.7: Protocols (Icmp,Arp)**

**ICMP (Internet control message protocol):** It is network layer protocol used by routes and other devices to send the error messages and status of the network.

**ARP** (Address Resolution protocol): It is used to map a device’s IP address to its physical MAC address in a local network.

**1.8: DNS: Domain name system**

Helps to convert name to the Ip Address.

For exe… we don’t need to remember the port address of the website we have to just know the name.

**1.9: Ports: (Switches works on MAC address, while having multiple devices)**

It’s like door to enter and exit the data from internet.

We are having different ports for diff services.

Mainly:

HTTP: 80

HTTPS: 443  
SMPT: 25

**1.13: NIC: (Network Interface card ):**

It’s a device used to connect the device to the internet.

**1.14: MAC:(Media Access Control):**

It’s a unique identifier having for every device

**1.15: Submarine Cable Maps:**  Mainly for transferring of the internet with high speed by using optical fiber which are under the sea.

**1.17: Nodes:**

A node in a network refers to any physical device or point that is capable of sending, receiving, or forwarding data.

**1.18: Scaling up and down(Vertical) :**

Adding more power to the device. Like when the storage is over we can add more , that is scaling up.

And scaling down is when we don’t want it should reduce.

**1.19: Scaling in and out(Horizontal):**

Adding more devices. Like storage is over we are connecting with another devices, which is scaling out.

And we can reduce the connecting devices which is scaling in.

**1.20: Modem/Routers:**

**Modems:**  It will convert digital to analog to transmit to more distances and also are not using bits anymore.

* Modems will help to connects network to internet.

**Routers:** It will distribute the internet to multiple devices.

**1.21: Topologies:**

**Bus, Ring, Tree, Mesh**

**Bus:** Simple only one network multiple devices are connected. (dis: only 1 net so it fails all will, security ADV: simple , high speed)

**Ring:** 2 devices we can connect to

**Tree:** Central node connect to the subsequent nodes.

**Mesh:** Directly connected to every device.

**1.22: Socket/ port:**

**Socket = IP Address + Port Number**

The combination of an IP address and a port number allows multiple applications on the same device to use different communication channels without interference.

**Example**: If you're using a web browser, your browser and the web server communicate using a socket. The web server might use port 80 (for HTTP) or port 443 (for HTTPS), while the browser uses a dynamically assigned port.

**Port:**

A **port** is a number that identifies a specific service or application on a device. It allows the operating system to differentiate between different types of communication happening on the same device.

**1.23: HTTP Method**

**GET:** The GET method is used to request data from a specified resource.

**POST:** creating a resource. POST requests typically include a request body, which contains the data to be submitted.

**PUT:** The PUT method is used to update a resource on the server.

**DELETE:** The DELETE method is used to delete a specified resource from the server.

**1.24: peer to peer:**

Simply 2 persons are directly talking without need of third person.

And Every device will act both client and server.

**1.25: Service Discovery:**

Its like phone book , it helps services to find and connect with each other even they change location.

you have two services, **A** and **B**. If **A** needs to talk to **B**, it uses service discovery to find out where **B** is, without needing to know its address beforehand.

Service discovery will have to know which is alive or not.

**2. Day-2**

* **HTTP Error**
* **Cookies**
* **More about Switch and Ip address**
* **VPN & Types**
* **Checksum**
* **Ip Packet Structure //**
* **ICMP**
* **ARP**
* **Ping**
* **TCP/IP Layer //**
* **Subnetting**
* **VPC**
* **NAT**
* **Symmetric & Asymmetric**
* **Microservices //**

**HTTP Errors:**

200: ok

404: Not Found

500: Internal Server Error

**Cookies:**

Cookies are the text files storing some required data for a point of time. So that we can connect faster. For example, google the login credentials will store for a particular point of time.

**Switch and Ip address:**

**Switch:**

Here we can connect to multiple devices.

**Example Workflow:**

Device A (MAC: A1) sends a packet to Device B (MAC: B1).

The switch:

Sees the source MAC (A1): Updates its table (A1 → Port 1).

Checks for destination MAC (B1) in the table: Not found.

Broadcasts the packet to all ports except the one Device A is connected to.

Device B (MAC: B1) receives the broadcasted packet and responds.

The switch:

Sees the response and learns B1 → Port 2.

Updates its MAC address table.

Future packets from A1 to B1 are sent directly to Port 2, with no broadcast.

**VPN & Types:**

Simply we are encrypting the data using vpn.

For Example there are 2 devices and in one device when we entered the credentials and vpn will encrypt the data then it will send to another device, in another device also there is vpn , vpn knows how to decrypt it so it will do.

**types of VPN**:

        1. Remote access VPN

* **Purpose**: Enables individual users to securely connect to a private network remotely.
* **Use Case**: Employees working from home accessing company resources.
* **Example**: Using a VPN app to connect to a corporate network.

2.site to site VPN:

* **Purpose:** Connects two or more networks in different locations.
* **Use Case:** Linking branch offices to the main office network.

3. SSL VPN:

* **Purpose**: Provides secure remote access through a web browser without needing special software.
* **Use Case**: Securely accessing resources via HTTPS.

4. Cloud VPN:

* **Purpose**: Connects users to cloud services securely.
* **Use Case**: Organizations moving resources to cloud platforms like AWS or Azure.

        5.double VPN - two VPN instead of one

**Checksum:**

Simply checksum is used to check whether there is any manipulation of data or changing of data is done while reaching the destination.

For Example, 1011 is the data to send and in the adding the parity we mentioned it has odd no.of 1’s but after the receiving the data by the destination it is showing that 1001 which is even 1’s . so we can easily find it is not the same data.

**ICMP:**

ICMP will used for the error detection noting but.

Icmp first send the ICMP Eco request to the device 2 and waits to ack for the ICMP Eco Reply . Then it will understand that packets to going the correct destination without any manipulation.

**Ping:**

Ping is the diagnostic tool which used to test the connection between 2 devices using  **ICMP**

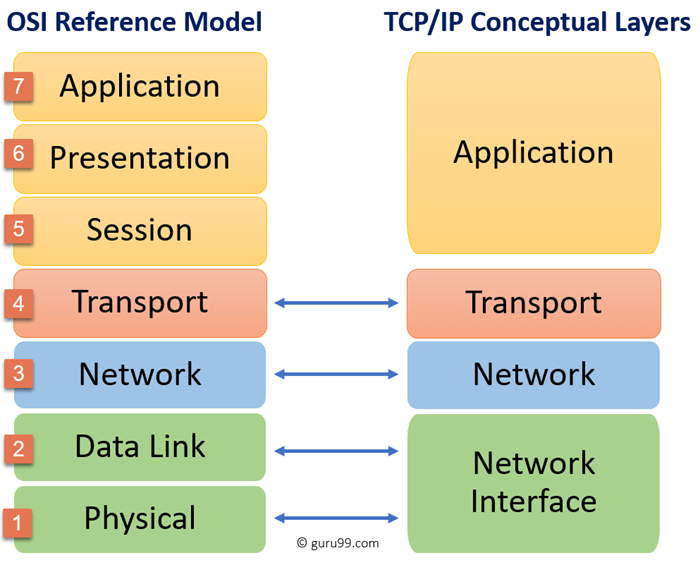
**ARP:**

It is used to Map the ip address to the Mac address.

**YY because:**

Just to connect to another machine we want ip address but **to transmit** the data we want **mac address.**

**TCP/IP Model:**



**Subnetting**:

Subnetting is the process of dividing a larger network into smaller, more manageable sub-networks, known as subnets. This is done by borrowing bits from the host portion of an IP address to create additional network bits. Subnetting helps improve network performance, security, and address management.

**NAT (Network Address Translation)**:

Network Address Translation (NAT) is a technique used in networking to modify the source or destination IP addresses in the header of IP packets as they pass through a router or firewall. NAT enables multiple devices on a local network to share a single public IP address for accessing external networks like the internet.

**Symmetric and Asymmetric Encryption Symmetric:**

**symmetric** encryption, the same key is used for both encryption and decryption.

**Asymmetric:** In asymmetric encryption, two different keys are used: a public key and a private key. The public key is used to encrypt data, while the private key is used to decrypt it.

**Monolithic Architecture**:

Monolithic architecture refers to a traditional model of software design where an entire application is built as a single, unified unit.