**Networking**

Network: Logical grouping of hosts which require similar connectivity. Hosts in a network share the same IP address space and differentiated only by Host id.

**Rules for networking are divided into 7-layered OSI ARCHITECTURE: PDNTSPA**

* **Physical Layer:** 
  + **Goal:** Transporting bits
  + **Components:** Cables: Fibre, coaxial, twisted pair, etc WiFi, repeater, Hubs
* **Data Link Layer:**
  + **Goal**: Hop to Hop Delivery, interacting with the wire (Physical Layer), puts and retrieves bits from the wire.
  + **Components:** NIC, Ethernet Card, WiFi Access cards, Switches
  + **Addressing Scheme:** MAC addresses: 48 bits represented as 12 Hexadecimal digits
  + Packet plus MAC address 🡪 Frame
* **Network Layer:**
  + **Goal:** End to end Delivery
  + **Addressing scheme:** IP Addressing: 32 bits represented as 4 octets, each 0-255
  + **Components:** Routers, Hosts
  + **ARP:** Address Resolution Protocol links Layer 3 IP address to Layer 2 MAC address by passing an ARP Request to know the MAC address of the receiver. It gets and ARP response.
  + **IP protocol** is used in this layer
  + Segment plus IP address header and Footer 🡪 Packet
* **Transport Layer:**
  + **Goal:** Service to service delivery, distinguish data streams to decide which application needs it.
  + **Addressing scheme:** Ports
  + **Protocols:** TCP (Favours reliability) AND UDP (Favours efficiency) (0-65535)
  + Will pass the data plus TCP/UDP header comprising of port number 🡪 Segment
* **Session Layer:** Maintains the user specific information in the form of cookies.
* **Presentation Layer:** Converts data into machine readable bit stream. Determines **how to interpret** the 0’s and 1’s. In what groups the bits should be interpreted. Eg. HTTP ASCII encoding takes groups of 8 bits as different ASCII character.
* **Application Layer:** Top layers for user interaction, **tells what to do with the interpreted characters. Eg.** 01000111 (G) 01000101 (E) 01010100 (T) 🡪 GET request in HTTP. Different protocols use different interpreting techniques and have different methods to accomplish their goals in different layers of the OSI model.

Since every application and protocol is going to implement Session, Presentation and Application in their own way, the TCP/IP model combines them into a single Application layer.

**Data moves through the network based upon three tables:**

* MAC Address table: Mapping of Switchport to MAC address
* ARP table/cache: Mapping of IP address to MAC address
* Routing table: Mapping of IP network to Interface or Next Router

**Basically, Encapsulation on Sender and Decapsulation on Receiver happens in the complete delivery of the data between client and server.**

**Subnet mask:** Identifies the size of the IP address.

**Default Gateway**: is the IP Address of the first router which the packet flows through.

**NETWORKING DEVICES:**

* Repeater: Repeats/regenerates, the strength of the signal but does not amplify it. Now, if hosts increase it is difficult to connect each with the remaining one's. So we have the following devices.
* Hub: It is a multiport repeater. But, in a hub everybody receives the sent data which should not be the case. Bridge soves this problem. It sits between hub connected host networks. Types of hubs:
  + Active Hub: Amplifies the data signals thus helps in extending the distance over which data can flow. Requires external power supply. Useful for maintaining data integrity.
  + Passive Hub: No amplification, simply a conduit a data.
* Bridge: It only has two ports. Operates at the data-link layer. Helps in containing packets to the relative netwrok. A bridge simply segments a complex network to reduce traffic and limit where it reaches in the network by limiting the number of devices in each segment. It also has a MAC address table using which it makes intelligent decisions to direct the flow of traffic.
* Switch: is a multiport bridge that can perform error checking. The are like a combination of hubs and bridges but which can selectively send the packets and repeat the signals. Communication flow can be controlled by a switch. Basically, a switch facilitates communication within a network. But, what if a host in one network wants to facilitate communication with a host in a different network. It performs 3 basic operations:
  + Learn: Update MAC address table with mapping of Switch port to Source MAC
  + Flood: Duplicate and send frame out all switch ports except the sending port. After flooding only the destined host will revert back and learning happens again. Now the switch will remember the Mac and port map, for the future.
  + Forward: Uses updated Mac address table to deliver frame to appropriate switch port.
* Router: is a switch that routes the data based on the IP addresses between different networks. Thus, it provides a traffic control point (security, filtering, redirecting). It has the knowledge of different routes which is stored in a routing table. Gateway: is a interface/passage in a router to connect to different networks. They create a hierarchy in the network and thus the entire internet. Any node that forwards packets not explicitly addressed to itself (RFC:2460 ). When routers receive a packet with unknown Destination IP, packet is dropped.

Routing Tables can be populated via 3 methods:

* Directly Connected: Routes for networks which are directly connected.
* Static Routes: Routes manually provided by an administrator.
* Dynamic Routes: Routers learn automatically from other routers. Protocols used : RIP, OSPF, BGP, EIGRP, IS-IS

Routers also have ARP tables. Router hierarchy allows for route summarization, reducing congestion, consistent connectivity, decreasing path traversal, increasing speed and scaling and reducing network failures.

There can be two types of Frames:

Unicast Frame: Destination MAC is another host. Sometimes flooded when mac table is not populated.

Broadcast Frame: Destination MAC address of FFFF.FFFF.FFFF. Always flooded uses ARP

**Remember: Switches facilitate communication within a network whereas Routers facilitate communication between networks.**

There are many other network devices as well. Access-points, firewalls, Layer 3 switches, IDS/IPS, Load Balancers, Proxies, Virtual switches and Virtual Routers. All of these either do routing or switching or both.

**Socket**: A socket is a fundamental concept in computer networking that allows communication between devices. It serves as an endpoint for sending and receiving data across a network.

Practical Applications

Web Browsing: When you access a website, your browser creates a socket to connect to the web server’s IP address and port 80 (HTTP) or 443 (HTTPS).

Email: Email clients use sockets to communicate with email servers over ports like 25 (SMTP), 143 (IMAP), or 993 (IMAPS).

Instant Messaging: Instant messaging apps use sockets to send and receive messages in real time.

HTTP: Application layer protocol used in Client-Server model. It is a stateless protocol. Uses TCP in the transport layer.

**HTTP Methods:**

* Get: Requesting the server. Purpose: To retrieve data from a server. Example: Accessing a webpage or retrieving a specific piece of data from an API.
* Post: Submit data to a server to create or update a resource. Client giving something to the server eg. password. Example: Submitting a form or uploading a file. Not idempotent (repeated requests may result in multiple resources being created or different outcomes). Used when you want to submit data to a server, which then determines the resulting action and the resource URL.
* Put: Puts the data on a specific location. Updates an existing resource or creates a new resource at a specific URL. Idempotent (repeated requests yield the same result). Used when you know the exact URL of the resource to be created or updated.
* Delete: Removes a resource from a server.

**Status Codes:**

* 100+ Informational category codes
* 200+ Success codes
* 300+ Redirecting purposes
* 400+ Client Error
* 500+ Server errors

**VLANS:** Allows one to divide switch ports into isolated groups. Thus, switches start acting as multiple mini-switches.

**PROTOCOLS:**

* **Address Resolution Protocol:** RFC-826, Resolves IP address to 48-bit MAC mappings.
* **File Transfer Protocol:** Uses RETR command (retrieve)
* **SMTP**
* **HTTP:** Uses get, post, etc
* **SSL**
* **TLS:** Transport Layer Security
* **HTTPS**
* **Domain Name System:** Converts URL to IP address and also email id to IP address.

**Every host needs 4 items for internet connectivity:**

* IP address
* Subnet Mask ( /24 or 255.255.255.0): Decides network and host portions of an IP address. This in turn allows segmentation of larger network into more manageable subnets. This also facilitates IP routing and efficient use of IP addresses.
* Default Gateway: The IP address of default router.
* Domain Name Server Ips

To configure these 4 things in a new connection another protocol runs in the background, It is known as DHCP.