Computer Networks Notes

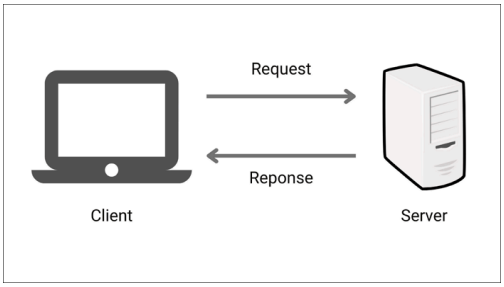
BASICS

1. *What is Computer Networking?*

Computer networking refers to connected computing devices (such as laptops, desktops, servers, smartphones, and tablets) and an ever-expanding array of IoT devices (such as cameras, door locks, doorbells, refrigerators, audio/visual systems, thermostats, and various sensors) that communicate with one another.

2. *Basic terms:*

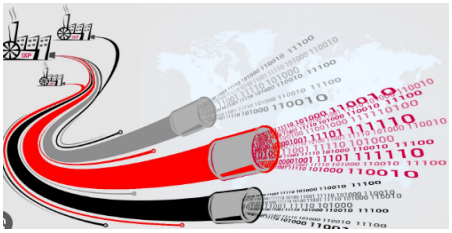
a. **Client**: A client is a computer program or device that requests services or resources from a server. It's usually part of a client-server architecture where the client initiates requests, and the server responds to those requests.



b. **Server**: A server is a computer or system that provides resources, services, or data to other computers, known as clients, over a network. Servers respond to requests from clients and can store and manage data or perform specific tasks.

c. **Peer**: In networking, a peer refers to a computer or device that shares the same level of functionality and responsibility with others. Peers communicate with each other in a peer-to-peer network without a central server.

d. **Host**: A host is any device connected to a network, such as a computer or a server, capable of sending or receiving data. It can be a client, server, or both.



e. **Bandwidth**: Bandwidth refers to the capacity of a communication channel to transmit data. It is often used to describe the data transfer rate of an internet connection and is measured in bits per second (bps) or a similar unit.

f. **Throughput :** Throughput is the term given to the number of packets that are processed within a specific period of time.

g. **Jitter**: Jitter is the variation in the delay of received data packets in a network. It can lead to inconsistent packet delivery times, which may affect the quality of real-time applications like voice or video.

h. **Packet**: Packets are used at the network layer of the OSI model. A packet is a small unit of data transmitted over a network. It contains both the actual data being sent and the necessary control information, such as source and destination addresses.

i. **Frame**: In networking, a frame is a data transmission unit at the data link layer of the OSI model. A frame is a data transmission unit that includes both the data being sent and the necessary control information for reliable transmission within a local network segment.

j. **Local Host**: Local host typically refers to the computer or device you are currently using. It's often identified by the loopback address (127.0.0.1), allowing a device to communicate with itself.

k. **Bit Rate**: Bit rate is the number of bits processed or transmitted in a unit of time, often measured in bits per second (bps). It represents the speed of data transfer in a network.

l. **Noise**: In the context of networking, noise refers to unwanted electrical or electromagnetic interference that can disrupt the transmission of data signals.

m. **Attenuation**: Attenuation is the reduction in signal strength as it travels through a medium, such as a cable or fiber optic. It can affect the quality and integrity of the transmitted data.

n. **Distortion**: Distortion in networking refers to any alteration or corruption of the signal during transmission, leading to errors in the received data.

3. *Difference between Web and Internet?*

Internet:

- Definition: The internet is like a giant network that connects millions of smaller networks worldwide.
- Example: Think of the internet as a massive library. Each book in the library is like a website or online service. The library itself is the internet, connecting all these books (websites) together.

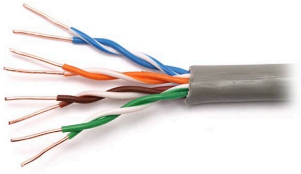
Web:

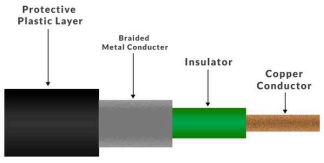
- Definition: The web (or World Wide Web) is a part of the internet where you access information using websites and web browsers.

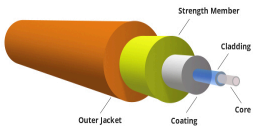
- Example: Imagine a book in the library (internet). When you open the book and read its pages, that's like using a website on the web. The pages of the book are like different web pages you navigate through.

In short, the internet is a vast network, and the web is a way to access information on that network through websites.

4. *Types of Transmission Media*







<u>Physical Transmission Media</u>:

- Twisted Pair Cable: Copper wires twisted for local networks. Eg: Telephone lines and LANs
- Coaxial Cable: Central conductor for cable connecting TV and broadband.
- Fiber Optic Cable: Glass fibers transmit data using light for high-speed internet and long-distance communication.

<u>Wireless Transmission Media:</u>

- Microwave Transmission: High-frequency radio waves for long-distance.
- Satellite Communication: Orbits relay signals globally. Satellite TV broadcasting signals from a satellite to a home dish.
- Infrared Transmission: Short-range, like TV remote controls.

5. *Unicast, BroadCast and Multicast*

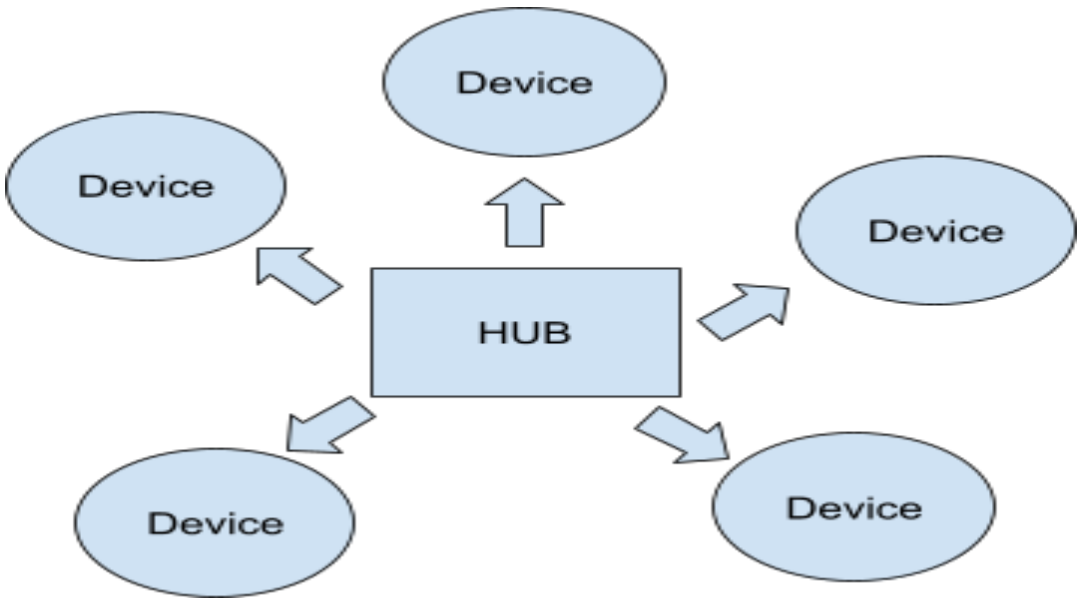
a. **Unicast**: One-to-one communication (e.g., sending an email to a friend).

b. **Broadcast**: One-to-all communication (e.g., TV broadcasting to all TVs in range).
c. **Multicast**: One-to-many communication to specific receivers (e.g., video conference call to a specific group).

6. Computer Network Devices

a. **Repeater:** (Physical Layer)
Signals lose strength as they travel through cables or airwaves. A repeater steps in, amplifies those weakened signals, and sends them on their way with renewed energy.
Eg: Use a Wi-Fi repeater to strengthen the signal in areas where the Wi-Fi from the router is weak or has to travel a long distance.

b. **Hub:** (Physical layer)
Connects multiple devices in a network. It broadcasts data to all connected devices, making it less efficient than a switch.



c. **Switch**: (DataLink Layer)
Connects devices within the same network. It intelligently forwards data only to the intended recipient, improving network efficiency.

d. **Bridge**: (DataLink Layer)
   Connects and filters traffic between two different LANs.

e. **Routers**: (Network Layer)
   Connects different networks at the network layer, directing data between them based on IP addresses. It makes decisions based on logical addressing.
   Example: Home router connecting devices to the internet.

7. Network Topology

a. **Bus Topology:**
   All devices share a common communication line (the bus). Data is sent to all devices, but only the intended recipient processes it.

b. **Ring Topology:**
   Devices are connected circularly. Data travels in one direction, passing through each device until it reaches the intended recipient.

c. **Star Topology:**
   All devices are connected to a central hub or switch. Data communication occurs through this central point.

d. **Mesh Topology:**
   Devices are interconnected, and there are multiple paths for data to travel from one device to another. Offers high redundancy and fault tolerance.

e. **Tree Topology:**
   A combination of bus and star topologies, forming a hierarchical structure. Groups of star-configured networks are connected to a central bus backbone.

Example: Large organizational networks, where individual departments have their own star topology, connected to a central bus serving the entire organization.

8. Different types of networks

a. **LAN (Local Area Network)**: It is used for a small geographical location like an office, hospital, school, etc.

b. **MAN (Metropolitan Area Network)**: It is used to connect the devices that span over large cities like metropolitan cities over a wide geographical area.

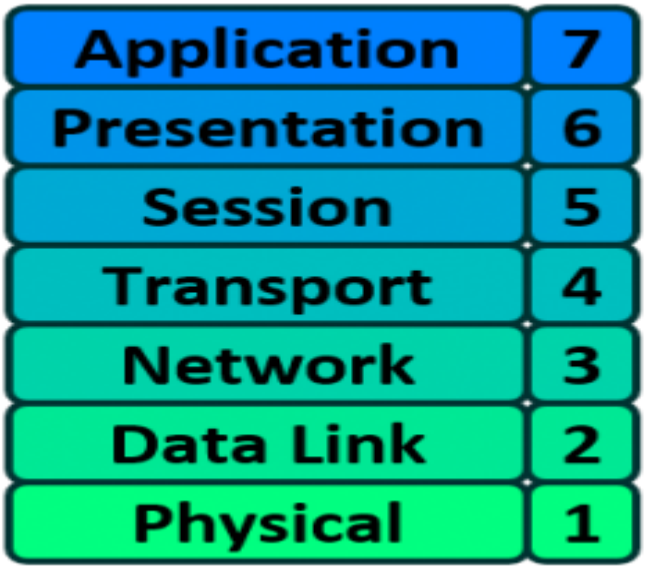
c. **WAN (Wide Area Network)**: It is used over a wide geographical location that may range to connect cities and countries.

d. **PAN (Personal Area Network)**: Its range limit is 10 meters. It is created for personal use. Generally, personal devices are connected to this network—for example computers, telephones, fax, printers, etc.

OSI Model

The Open Systems Interconnect model (OSI Model) explains all the functions necessary for the Internet to work.

The OSI model is divided into **seven different layers**, each of which fulfills a very specific function. When combined, each function contributes to enabling full computer-to-computer data communication.



1. Physical Layer:

The Physical layer of the OSI model is responsible for the transfer of bits — the 1's and 0's which make up all computer code.
It encompasses the physical medium, like Ethernet cables or Serial Cables. Despite its name, it includes wireless technologies like WiFi.
Simply put, **Layer 1 is anything that carries 1's and 0's between two nodes**.
Ethernet uses electric pulses, WiFi uses radio waves, and Fiber uses light pulses.
Repeaters and Hubs also function at this layer.

2. Data Link Layer

Layer 2 is responsible for putting 1's and 0's on the wire, and pulling 1's and 0's from the wire.

The Network Interface Card (NIC) that you plug your Ethernet wire into handles the Layer 2 functionality. It receives signals from the wire, and transmits signals on to the wire.

Layer 2 will then group together those 1's and 0's into chunks known as Frames.

There is an addressing system that exists at Layer 2 known as the Media Access Control address, or MAC address. **The MAC address uniquely identifies each individual NIC**.

A **Switch** also operates at this layer. **The role of Layer 2 is to deliver packets from *hop to hop***.

3. Network Layer

The **Network layer of the OSI model is responsible for packet delivery from end to end**.

The Internet achieves this by employing another addressing scheme— the Internet Protocol address, commonly known as the IP Address. This system provides a logical identification for each node connected to the Internet.

Routers operate at this layer.

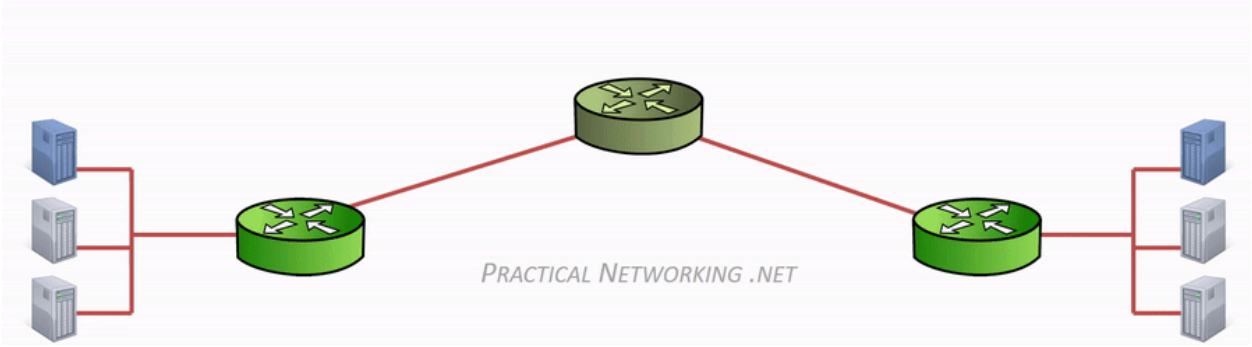
Q. If we already have a unique L2 addressing scheme on every NIC (like MAC addresses), why do we need yet another addressing scheme at L3 (like IP addresses)? Or vice versa?

- **Layer 2** uses **MAC addresses** and is responsible for packet delivery from **hop to hop**.
- **Layer 3** uses **IP addresses** and is responsible for packet delivery from **end to end**.

When a computer has data to send, it encapsulates it in an IP header which will include information like the Source and Destination IP addresses of the two “ends” of the communication.

The IP Header and Data are then further encapsulated in a MAC address header, which will include information like the Source and Destination MAC address of the current “hop” in the path towards the final destination.

Here is an illustration to drive this point home:



Notice between each Router, the MAC address header is stripped and regenerated to get it to the next hop. The IP header generated by the first computer is only stripped off by the final computer, hence the IP header handled the “end to end” delivery, and each of the four *different* MAC headers involved in this animation handled the “hop to hop” delivery.

Think of your home network as a neighborhood, and each device in your home (like your computer, phone, or smart TV) as a house in that neighborhood. In this analogy, MAC addresses are like unique house numbers. They help devices on the same street communicate with each other efficiently. For instance, if your computer wants to send a message to your printer, it can use the MAC address to find it quickly within the local network (neighborhood).

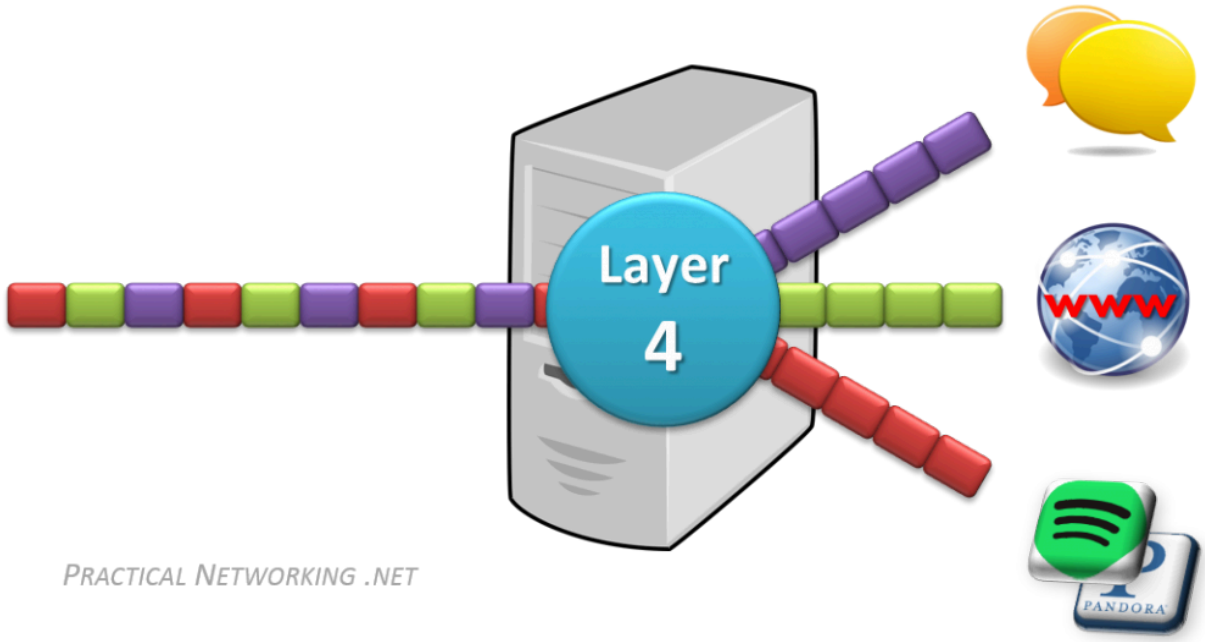
Now, let's extend the analogy to the broader internet. Imagine your neighborhood is just one of many in a city, and each city is a part of a vast country. If you want to send a letter to a friend in a different city or

country, you wouldn't just use your house number; you'd need a more comprehensive address, including the city, state, and country. This is where IP addresses come in.

4. Transport Layer: (Segments)

At any given time on a user's computer there might be an Internet browser open, while music is being streamed, while a messenger or chat app is running. Each of these applications are sending and receiving data from the Internet, and all that data is arriving in the form of 1's and 0's on to that computer's NIC.

Something has to exist in order to distinguish which 1's and 0's belong to the messenger or the browser or the streaming music. That "something" is Layer 4:



Layer 4 accomplishes this by using an addressing scheme known as Port Numbers.

Specifically, two methods of distinguishing network streams exist. They are known as the Transmission Control Protocol (TCP), or the User Datagram Protocol (UDP).

5. Session Layer

The main responsibility of the session layer is beginning, maintaining and ending the communication between the devices.

Session layer establishes and maintains the session between the two users.

6. Presentation Layer

The presentation layer is also known as a Translation layer as it translates the data from one format to another format.

At the sender side, this layer translates the data format used by the application layer to the common format and at the receiver side, this layer translates the common format into a format used by the application layer.

Functions of presentation layer:

a. Character code translation
b. Data conversion
c. Data compression
d. Data encryption

7. Application Layer

The application layer serves as the interface between software applications and the network.

It includes protocols for tasks like email(SMTP), file transfer(FTP), and web browsing(Https).

Example: Facebook, Youtube, Gmail etc.

- Layer 4 will add a TCP header which would include a Source and Destination port
- Layer 3 will add an IP header which would include a Source and Destination IP address
- Layer 2 would add an Ethernet header which would include a Source and Destination MAC address

Q. How a packet travels(V.V.V Important)

1. Key Players
2. Host to Host Communication
3. Host to Host through a Switch
4. Host to Host through a Router
5. Final Video

Misc and System Design

1. **Difference between HTTP and HTTPS**

    a. **HTTP (Hypertext Transfer Protocol)**:

        i. **Definition**: HTTP is the foundation of data communication on the World Wide Web. It is an application layer protocol that enables the transfer of hypertext, which are text-based documents containing hyperlinks and multimedia content. Get, post, put and delete are some types of requests.

        ii. **Example**: When you enter a URL in your browser, it typically uses HTTP to request the web page from the server. However, data transferred using HTTP is not encrypted,

making it susceptible to interception and tampering.

b. **HTTPS (Hypertext Transfer Protocol Secure)**:
    i. **Definition**: HTTPS is the secure version of HTTP. It adds a layer of security by using encryption protocols such as TLS (Transport Layer Security) or SSL (Secure Sockets Layer) to ensure that the data exchanged between the client and server is encrypted and secure.
    ii. **Example**: When you visit a website with an "https://" URL, such as "https://www.example.com," the communication between your browser and the server is encrypted, making it more difficult for third parties to intercept or manipulate the data.

2. Common Networking commands

a. **ping**: Tests the reachability of a host on a network using Internet Control Message Protocol (ICMP) echo requests.

b. **netstat**: Displays information about network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.

c. **tracert (traceroute on Unix-like systems)**: Traces the route that packets take to reach a destination, showing the IP addresses of routers in the path.

d. **ipconfig (Windows) / ifconfig (Unix-like systems)**: Displays the configuration of network interfaces on a system, including IP addresses, subnet masks, and gateway addresses.

e. **nslookup**: Allows you to query Domain Name System (DNS) servers to obtain domain name or IP address information.

f. **route**: Displays and manipulates the IP routing table, showing the routing information used by the system.

g. **pathping**: Combines features of ping and tracert, providing information on packet loss at each hop along the route.

h. **netDiag (Windows)**: A network diagnostic tool that can be used to troubleshoot various network issues.

i. **hostname**: Displays the name of the current host or sets the host name.

j. **arp**: Displays and modifies the ARP (Address Resolution Protocol) cache, which maps IP addresses to MAC addresses on a local network.

3. What is an API?

An API, or Application Programming Interface, is a set of rules and protocols that allows one piece of software or application to interact with another. It defines the methods and data formats that applications can use to request and exchange information.

In a hotel setting, envision a scenario where you place an order with a servant, who then communicates the order to the kitchen. Subsequently, the servant returns with the prepared food to serve the customer. Here the servant acts like an API.

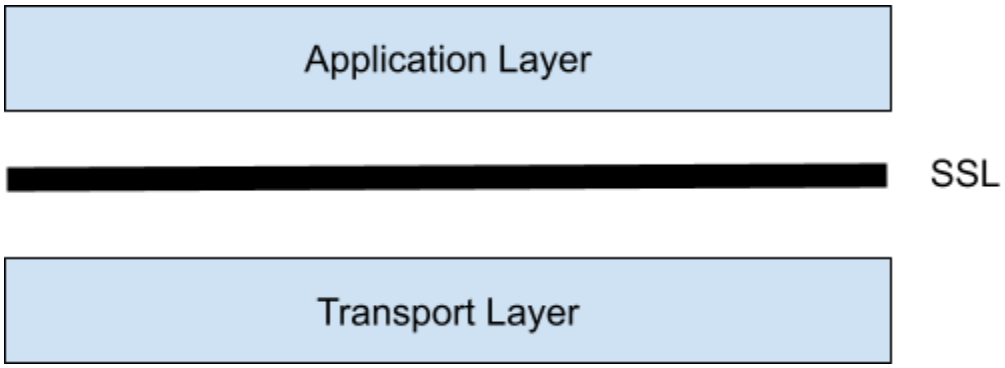
Eg. Google maps API, Weather API, News API.

4. What is SSL(Secure Socket Layer)/TLS(Transport Layer Security)?

To provide security between client and server while transferring data we use SSL.

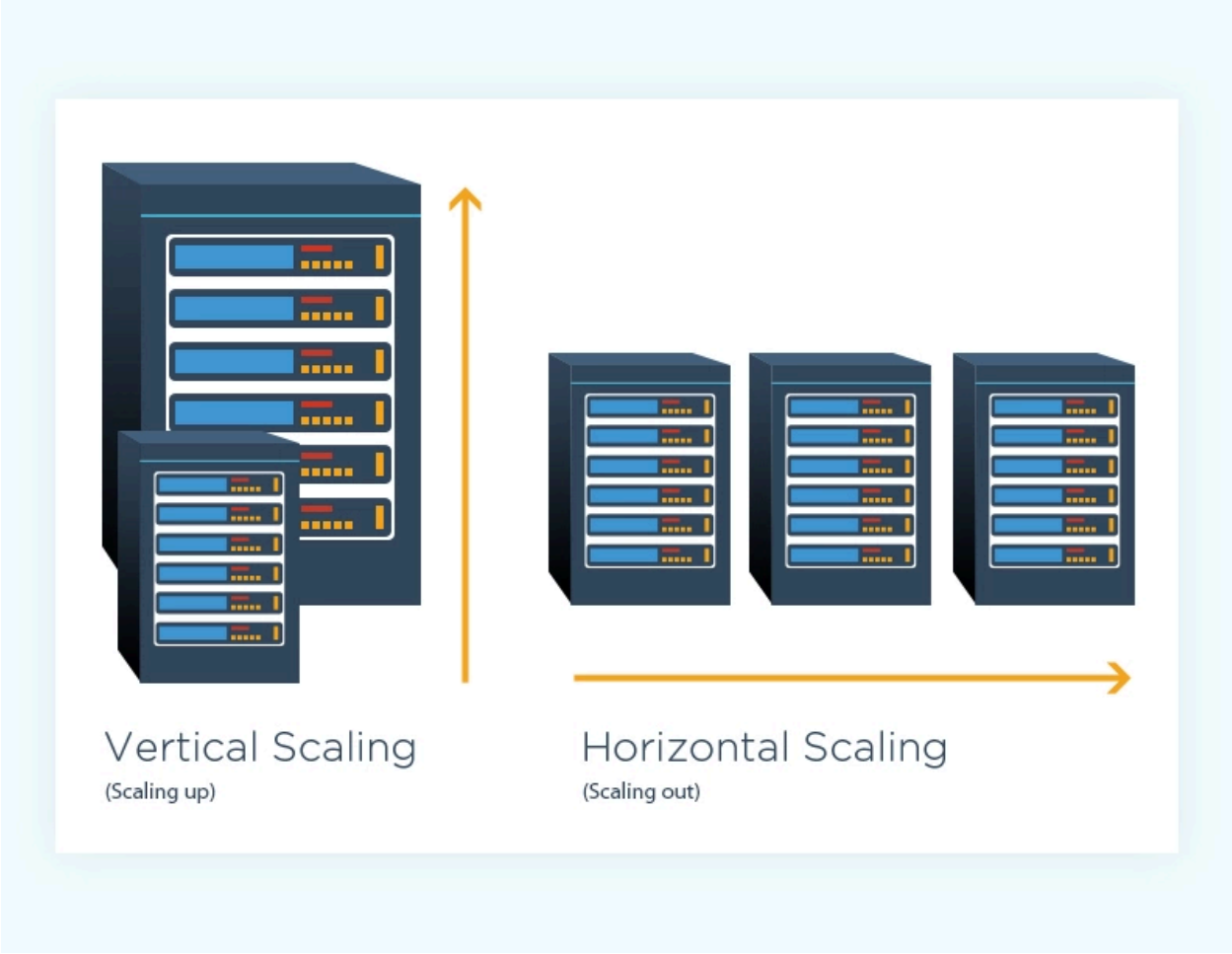
It mainly has 3 important features:

a. **Integrity**: The message should be sent without tampering to the client.
b. **Authentication/Authorization**
c. **Confidentiality**: Encrypting the data before transferring.



5. Horizontal Vs Vertical Scaling

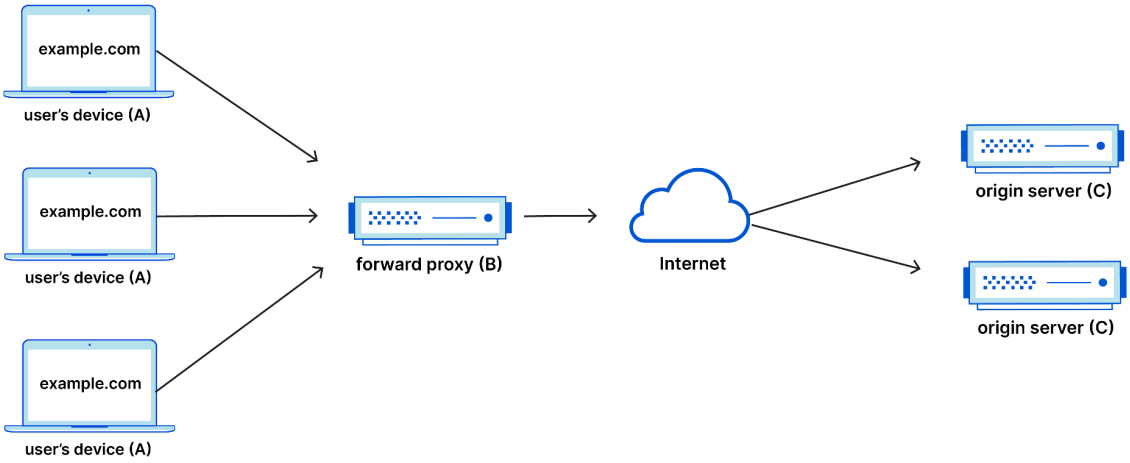
Horizontal scaling, also known as scaling out, involves adding more machines or nodes to your system. This approach distributes the workload across multiple machines.
Vertical scaling, on the other hand, also called scaling up, means increasing the power of a single machine by adding more resources like CPU, RAM, or storage.
Horizontal scaling is typically more cost-effective and provides better fault tolerance, while vertical scaling may have limitations and can be more expensive as you reach the upper bounds of a single machine's capacity.



6. **Forward Proxy and Reverse Proxy**

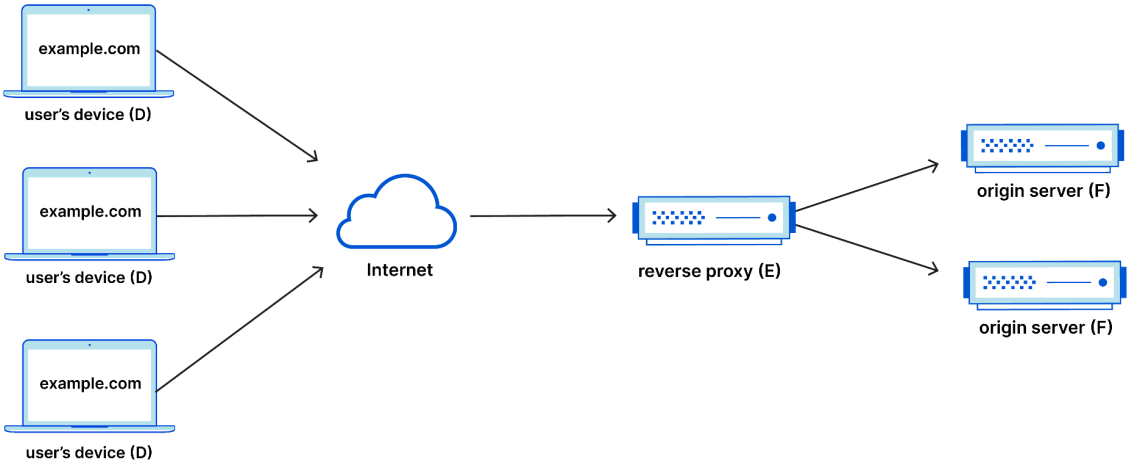
    a. **Forward Proxy**: (On Client Side)
        - Protects the client's online identity
        - To avoid state or institutional browsing restrictions
        - To block access to certain content (School network might be configured to connect to the web through a proxy with certain rules)

Forward Proxy Flow



b. **Reverse Proxy**: (On Server side)
   - Load Balancing
   - Protection from attacks to a server
   - Caching

Reverse Proxy Flow



For clear understanding watch this video :

Proxy vs Reverse Proxy (Real-world Examples)

7. CDN (Content Delivery Network)

A content delivery network (CDN) is a geographically distributed group of servers that caches content close to end users. A CDN allows for the quick transfer of assets needed for loading Internet content, including HTML pages, JavaScript files, stylesheets, images, and videos.

8. Modem vs Router vs Gateway

a. **Modem:**
   i. A modem is short for modulator-demodulator. In simpler terms, it connects your home network to the internet service provider (ISP) by converting digital data from your devices into a form that can be transmitted over the ISP's network and vice versa.

b. **Router:**
   i. A router is a device that directs data traffic between different networks. In a home network, it typically manages the flow of data between your local devices and the internet.
   ii. Routers use a system called Network Address Translation (NAT) to assign local IP addresses to devices within your home network, allowing them to share a single public IP address when accessing the internet.

c. **Gateway:**
   i. A gateway is a device that connects two different networks and facilitates communication between them. It acts as a bridge between your local network and the internet.
   ii. In the context of home networking, a gateway often combines the functionality of a modem and a router in a single device. It serves as the entry point to the internet and manages both the connection to the ISP and the local network.

9. Private and Public IP addresses.

a. Public IP addresses are distinct and registered on the internet, assigned by your Internet Service Provider (ISP) for a fee. Routers typically receive public IP addresses.
b. In contrast, private IP addresses are not unique, and due to the limited availability of IP addresses, we use private ones for devices within a local network. Routers assign private IP addresses to connected devices.

   Network Address Translation (NAT) comes into play by converting private IP addresses to public ones and vice versa, enabling communication between devices within a private network and the broader internet.

10. Difference Between TCP (Transmission Control Protocol) and UDP (User Datagram Protocol):

a. **TCP** is a connection-oriented protocol, whereas **UDP** is a connectionless protocol. A key **difference between TCP and UDP** is speed, as **TCP** is comparatively slower than **UDP**. Overall, **UDP** is a much faster, simpler, and efficient protocol, however, retransmission of lost data packets is only possible with **TCP**
b. TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data. UDP has only the basic error checking mechanism using checksums.

11. Important Protocols:

a. **DHCP**: DHCP is the **Dynamic Host Configuration Protocol**. It is an application layer protocol used to auto-configure devices on IP

networks enabling them to use the TCP and UDP-based protocols. The DHCP servers auto-assign the IPs and other network configurations to the devices individually which enables them to communicate over the IP network. It helps to get the subnet mask, IP address and helps to resolve the DNS. It uses port 67 by default.

b. **FTP** : FTP is a **File Transfer Protocol.** It is an application layer protocol used to transfer files and data reliably and efficiently between hosts. It can also be used to download files from remote servers to your computer. It uses port 27 by default.

c. **ICMP** : ICMP is the **Internet Control Message Protocol.** It is a network layer protocol used for error handling. It is mainly used by network devices like routers for diagnosing the network connection issues and crucial for error reporting and testing if the data is reaching the preferred destination in time. It uses port 7 by default.

d. **ARP** : ARP is **Address Resolution Protocol**. It is a network-level protocol used to convert the logical address i.e. IP address to the device's physical address i.e. MAC address. It can also be used to get the MAC address of devices when they are trying to communicate over the local network.

e. **RIP** :RIP stands for Routing Information Protocol. It is accessed by the routers to send data from one network to another. RIP is a dynamic protocol which is used to find the best route from source to the destination over a network by using the hop count algorithm. Routers use this protocol to exchange the network topology information. This protocol can be used by small or medium-sized networks.

f. **SMTP Protocol** : SMTP is the **Simple Mail Transfer Protocol**. SMTP sets the rule for communication between servers. This set of rules helps the software to transmit emails over the internet. It supports

both End-to-End and Store-and-Forward methods. It is in always-listening mode on port 25.

Security

1. What is Firewall? Types of Firewall.

A firewall is like the security guard of your computer network, determining what can enter or exit. It acts as a barrier between your internal network and external networks (like the internet), filtering and controlling traffic based on predetermined security rules.

a. **Packet Filtering Firewall**:
   As the data is sent in packets, this firewall checks the header of each packet. As it doesn't check the payload data it is not that secure.
b. **Proxy Firewall:**
   It hides the IP address of the computer and acts as a proxy. It also checks the payload of the data that's why it is very secure. It is slower compared to Packet Filtering Firewalls.
c. **Hybrid Firewall:**
   Combination of both Packet Filtering Firewall and Proxy Firewall. It offers highest security

2. Basic Network Attacks in Computer

a. **Man-in-the-Middle (MitM) Attack:**
   The attacker intercepts communication between two parties, gaining unauthorized access to sensitive information.

b. **Denial of Service (DoS) Attack:**
   Overwhelms a system or network with a flood of traffic, rendering it unauthorized to legitimate users.

c. **Spoofing Attacks:**
   Attackers manipulate their identity or IP address to appear as a trusted entity.

d. **Phishing Attacks:**
   Deceptive attempts to trick individuals into revealing sensitive information through emails, messages, or websites.

e. **SQL Injection:**
   Exploiting vulnerabilities in web applications to manipulate or gain unauthorized access to a database.

3. Various terms in cryptography.

a. **Hash function:**
   It is a function which converts a plain text into a cipher text. It is really difficult to convert the cipher text back to plain text.
   Eg: MD5 and SHA256.

b. **Encryption:**
   It's like putting a message into a secret language that only those with the right "key" can understand.
   - **Symmetric Encryption:**
     In this type, the same key is used for both the encryption and decryption of the data.
   - **Asymmetric Encryption:**
     Also known as public-key cryptography, it involves a pair of keys – a public key and a private key. The public key is used for encryption, while the private key is used for decryption.

4. **Process of end-to-end encryption using asymmetric encryption**

    a. **Key Generation:**
        i. Both the sender and receiver generate a pair of cryptographic keys: a public key and a private key.
        ii. The public key is shared openly, while the private key is kept secret.

    b. **Sender Encrypts Message:**
        i. The sender obtains the recipient's public key.
        ii. Using the recipient's public key, the sender encrypts the message. Only the recipient's private key can decrypt this message.

    c. **Transmission of Encrypted Message:**
        i. The sender transmits the encrypted message to the recipient.

    d. **Receiver Decrypts Message:**
        i. The recipient uses their private key to decrypt the received message.
        ii. Since the private key is known only to the recipient, it's assumed that only the intended recipient can successfully decrypt the message.

5. Digital Signatures

- A digital signature is a cryptographic technique used to verify the authenticity and integrity of a digital message, document, or transaction.

- It involves the use of asymmetric cryptography, where the sender uses their private key to encrypt a hash of the message, creating a digital signature.
- The recipient, using the sender's public key, can decrypt the signature to obtain the original hash.
- By hashing the received message and comparing it with the decrypted hash, the recipient can verify both the sender's identity and that the message has not been altered during transmission.