

Domain 4

Communication & Network Security

OSI Layers

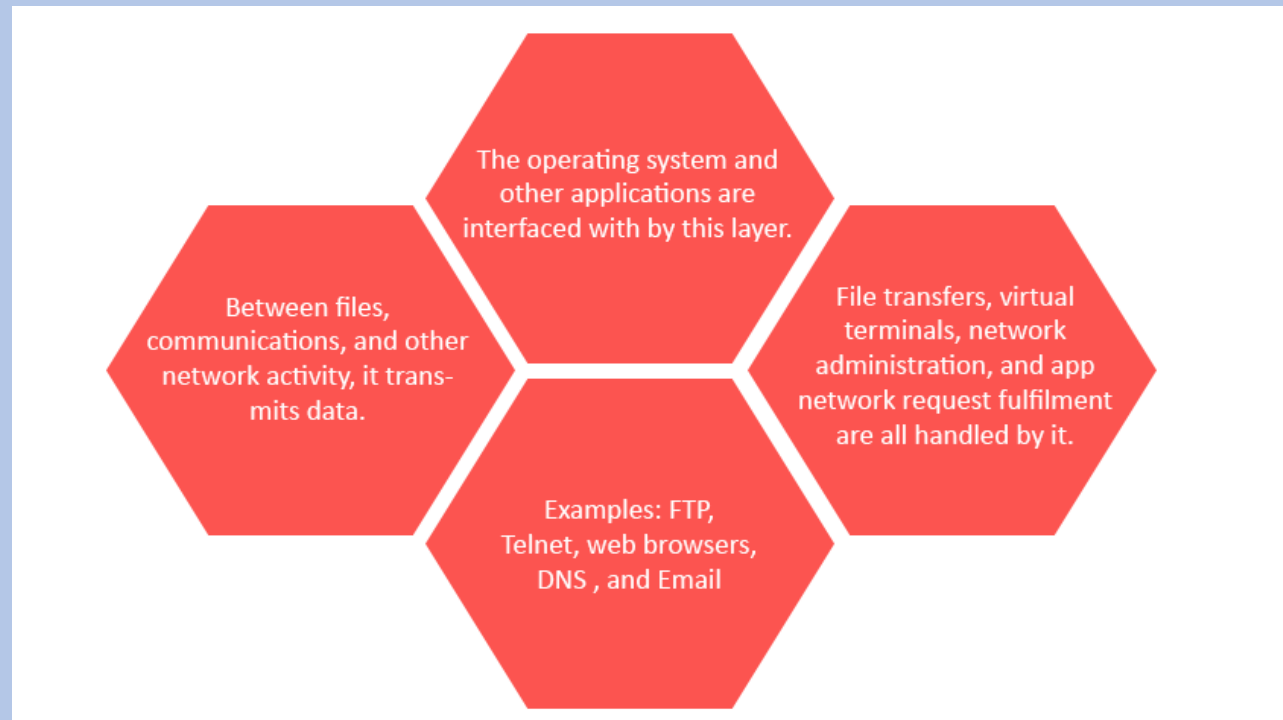
- In early days of computer, only same vendor machines can communicate
- TCP/IP – OS can communicate to different OS

Communication b/w host & remote device

- Application – Data – HTTP, Telnet, FTP, DNS
- Presentation – Data – SSL, TLS
- Session – Data – NetBios, PPTP, PAP
- Transport – Segments – TCP, UDP
- Network – Packets – IP, ARP, ICMP, IPSec
- Data link – Frames – PPP, ATM, Ethernet
- Physical – Bits – Ethernet, USB
- ISO – OSI Model
- Encapsulation
 - Add header in each layer

Application Layer

Message created & originated



Presentation Layer

- Compression
- Encryption

Translate the info to understand both parties

Data is presented and services are provided to the application layer by the presentation layer.

It is responsible of specifying how data is displayed to the user in the interface (application layer) they are using.

A common method of representing data is offered by this layer.

No protocols are functional in this layer; it serves as a translator.

It is more concerned with the syntax and presentation of the data than its meaning.

Exp: GIF, JPEG, ASCII, BMP, WAV, MPEG, and AVI

Session Layer

User1 connect to webSite

Every users have different sessions

s/w to s/w communication – Session Layer

h/w to h/w communication – Transport Layer

Establish & terminate the session on network

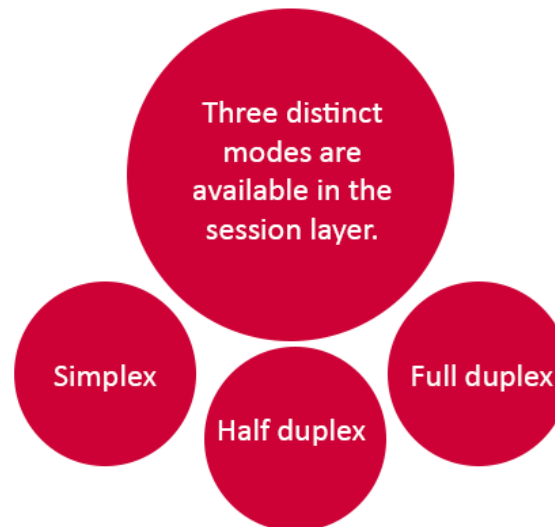
Three types of communication

Simplex – A to B, B not to A (one way)

Half Duplex – A to B, then B to A (one at a time)

Full Duplex – A to B & B to A (both at a time)

The session layer establishes the first contact and lines of communication with other computers.



Transport

TCP – Connection oriented

UDP – (User Datagram Protocol) Connectionless communication

TCP – Reliable, slow, flow control

Transmit packets over the network by using TCP or UDP

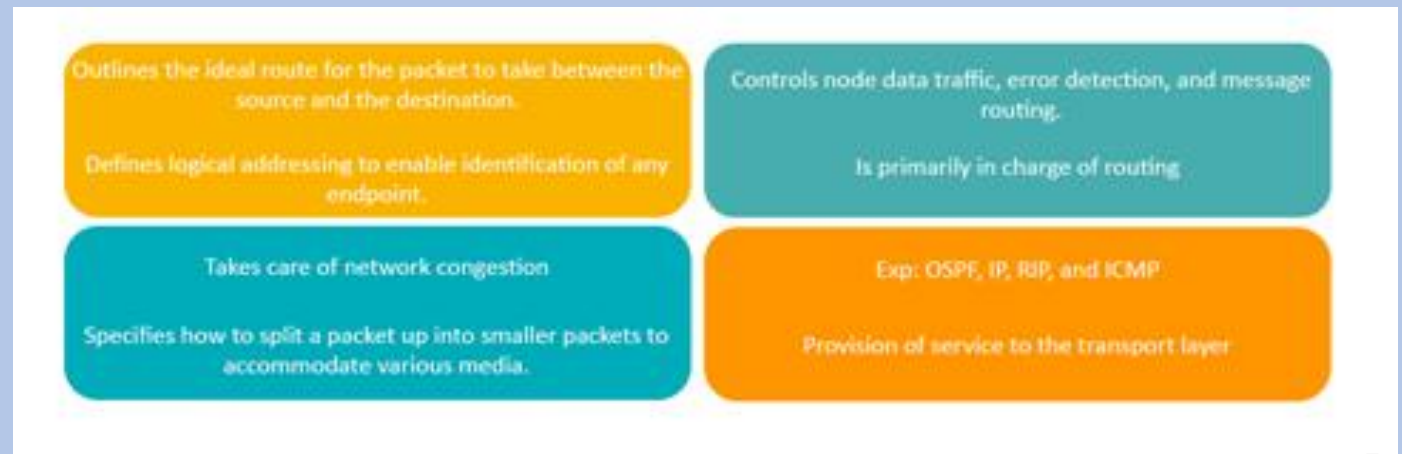
THE TRANSPORT LAYER SPECIFIES HOW TO CONNECT NODES, HOW TO ADDRESS PHYSICAL LOCATIONS AND DEVICES ON THE NETWORK, AND HOW TO CONDUCT MESSAGE NETWORKING.

Network Layer

Router connected – forward traffic based on IP address & ports

Data transmit over the network by using logical address

- Header is added during encapsulation
- IP address
 - IPv4 – 32 bits
 - Uni cast (user 1 connects to user 1)
 - Multi cast (user 1 connects to many users)
 - Broad cast (user 1 connects to all users)
 - IPv6 – 128 bits
 - Doesn't support broadcast because they consume lot of bandwidth
 - Uni case
 - Multi cast
 - Any cast

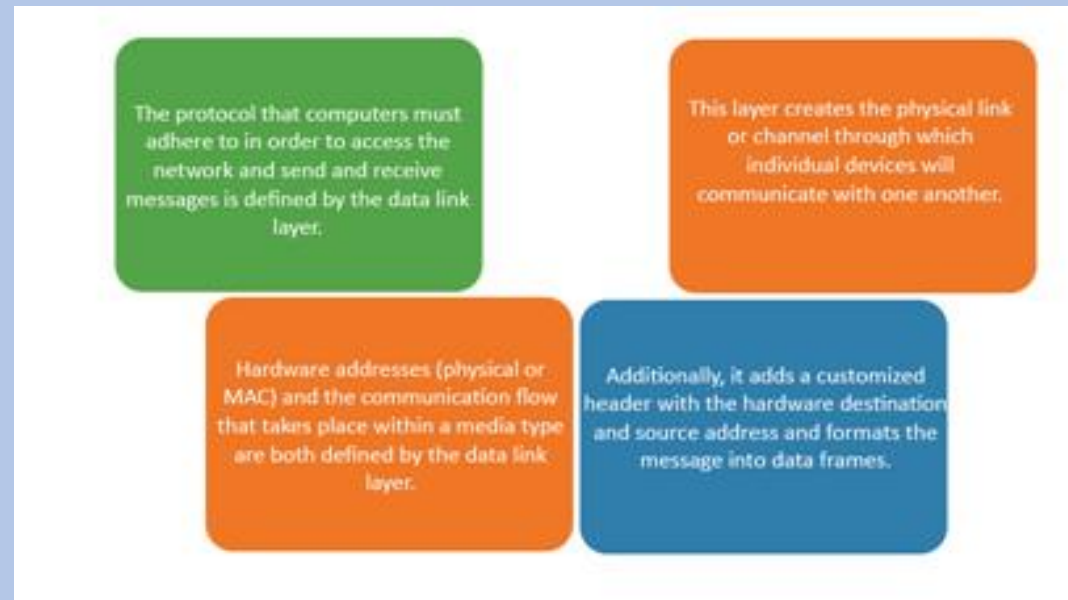


Data Link

Bridges connected

How connections established over physical layer using MAC

- Add header and trailer in the packet
- Trailer – Check error in the message
- Header – Source MAC/Destination MAC
- FQDN – Fully Qualified Domain Name
- If comp1 wants to connect to comp2, add source/destination MAC
- ARP table – Comp 1 has ARP table



Physical Layer

- Wired or wireless connectivity

Repeaters – Receive signals and retransmit

Hubs – Same like repeaters but have two ports

Show actual network cables carry Data on network

- The physical link between a computer and a network is defined by the physical layer.

- For transmission, it transforms the bits into voltages or light impulses.

- It outlines the procedures by which bits are transferred between systems using a physical communication media.

- It outlines many signalling kinds, including analogue and digital, electrical and optical, asynchronous and synchronous, simplex, full, and half-duplex.

- IP Address
- Class A -----
- Class B
- Class C
- Class D

IPv4

There are currently two types of IP in use: IP version 4 (IPv4) and IP version 6 (IPv6).

Best effort packet delivery is available with IPv4 version.

In IPv4, network addresses are expressed as 32-bit dot-decimal numbers.

IPv6 Address Terminology

In an IPv6 address the prefix contains the network portion of the address

The network portion of the address is also known as the network prefix in IPv4.

The prefix is defined by the left-most bits which are the most important.

This is the same as the subnet mask used in IPv4.

Since IPv6 addresses are 128 bit the prefix length can be /0 or /128.

Loopback Address

Some network addresses are for specific use and are not available for general use.

A private address is used by private networks to grant access to a guest machine.

Organizations are advised to assign private IP addresses to nodes in their internal networks.

The following address blocks are assigned to private networks.

A loopback address is an a specific address used to identify a certain node.

Loopback addresses 127.0.0.1 are designed to revert back to the issuing computer.

Software Defined Network (SDN)

Router connect two networks

When communication transmit through router or switch they decide where packets have to go

Decision comes from central point
SDN used in cloud and IT environment

Software connects through API
Software defined Wide Area Network (SD-WAN)

* Software defined networking enables network administrators to programmatically configure control and manage network behavior dynamically through open interfaces and abstracted lower level functionality.

* The objective SDN is to separate the control layer which are the network of services data transmission management from the infrastructure layer which includes hardware and hardware based settings.

Content Delivery Network (CDN)

An extensive, geographically dispersed network of specialised servers known as a content delivery network (CDN) is used to speed up the distribution of web content and rich media to internet-connected devices.

- When users far from server, the communication will be delayed
- To minimize communication time delays, deploy content in each country
- The users can directly connect nearby content and can increase the process speed
- If content not available, they can forward to nearest content

Advantages:

- Good performance
- Availability
- Security

Benefits

PERFORMANCE:

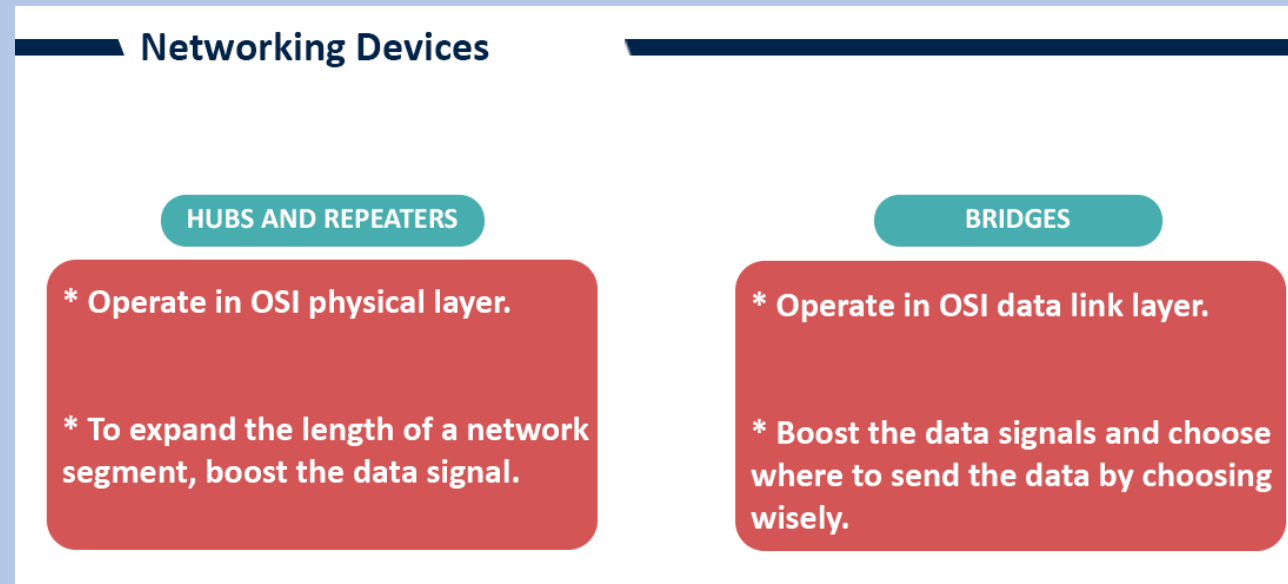
A closer distance to users will improve performance by lowering latency and decreasing packet loss.

AVAILABILITY:

- * Requests are always sent to the closest location that is available.
- * Requests are immediately sent to the next available server if one is unavailable.

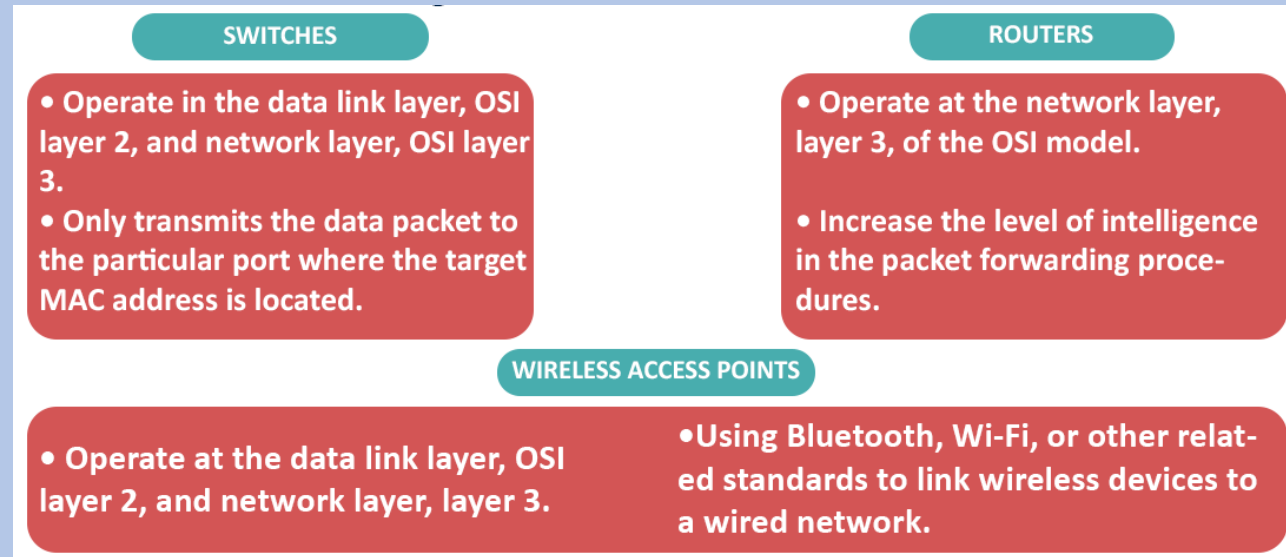
Hub

- Layer 2 – communicate to multiple machines
- Layer 3 – enable routing (IP address)



Bridge

- Connect two different networks through MAC



Router

- Connect two different networks

Transmission Media

Transmission media is used for transmitting data from a source to destination.

Following are the classes and types of transmission media:

- Unshielded twisted pair
- Shielded twisted pair
- Coaxial cable
- Fiber-optic cable

Category 1: Used for telephone communications and not suitable for transmitting data.

Category 2: Specified in the EIA or TIA-586 standard to be capable of handling data rates of up to 4 million bits per second (Mbps).

Category 3: Used in 10Base-T networks and specified to be capable of handling data rates of up to 10 Mbps.

Category 4: Used in Token Ring networks and able to transmit data at speeds of up to 16 Mbps.

Coaxial Cable Box

Coaxial cable box consists of a hollow outer cylindrical conductor.

It is expensive and resistant to Electromagnetic Interference (EMI).

Two types of coaxial cables are currently used in LAN: 50-ohm cable and 75-ohm cable.

Coax can come in two types for LANS: thinnet and thicknet.

There are two common types of coaxial cable transmission methods: baseband and broadband.

Fiber-Optic Cable Box

Fiber-optic cable box is a physical medium that can conduct modulated light transmission.

There are two types of light sources:

- Light-Emitting Diodes (LEDs)
- Diode lasers

There are two types of optical fibers:

- Multimode fiber
- Single-mode fiber

Fiber Optic Cable

Data transmitted in the form of light waves

LED – 10-20km

Laser – 100km

Coaxial cable

10Base2 (200m)

10Base5 (500m)

Endpoint Security

The technique of protecting user endpoints, such as desktops, laptops, and mobile devices, from cyberattacks is known as endpoint security.

- * Platform for centralized endpoint management.
- * Advanced antivirus and anti-malware security.
- * Proactive web security to guarantee secure Internet browsing.
- * To stop data exfiltration, use data classification and data loss prevention.
- * A built-in firewall to block hostile network attacks.
- * phishing and social engineering email gateway protection.
- * Administrators can immediately isolate affected devices with the help of insightful and practical threat forensics.
- * Protection against unintended or malicious activities by insiders.

Unified Endpoint Management (UEM) is a method for connecting and coordinating the security and control of mobile devices, such as laptops, tablets, and smartphones, from a single interface.

Virtual Private Network (VPN)

Any traffic keep confidential over the internet

Virtual Private Network

It is a private network that links users or remote locations via a public network, typically the Internet.

VPN Tunnel

- * It refers to the link that connects the user and the VPN server.
- * Each data packet is contained in an outer packet that is encrypted to keep it safe, a procedure known as encapsulation.
- * The data is protected during the transmission by this outer packet.
- * To obtain the data of the inner packet, the outer packet is removed at the VPN server.