Networking (The OSI Model)

The Open Systems Interconnection (OSI) Reference Model

- A conceptual framework showing us how data moves throughout a network.
- Developed by the International Organization for Standardization (ISO) in 1977.

Its's Purpose

- Gives us a guide to understand how networks operate.

It's Only a reference model so don't get wrapped up in the details.

- Wasn't implemented in the real world. TCP/IP is

The OSI Model Stack

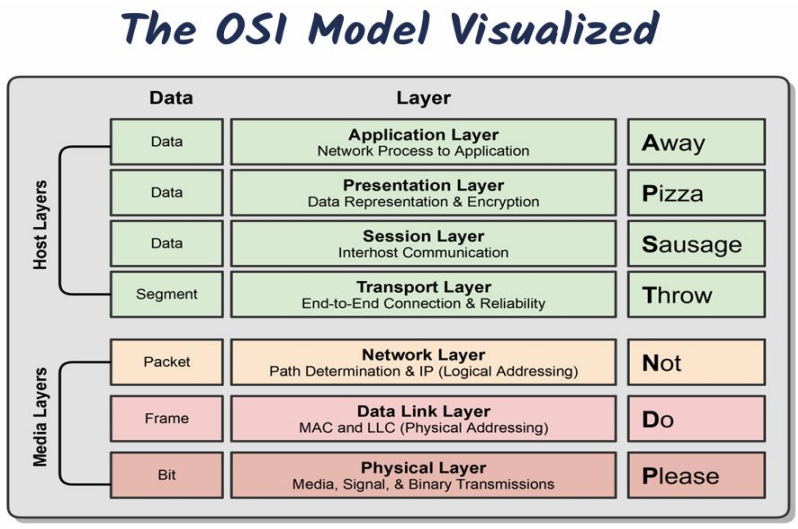
The OSI Model breaks down the complex task of computer-to-computer network communication into seven layers.

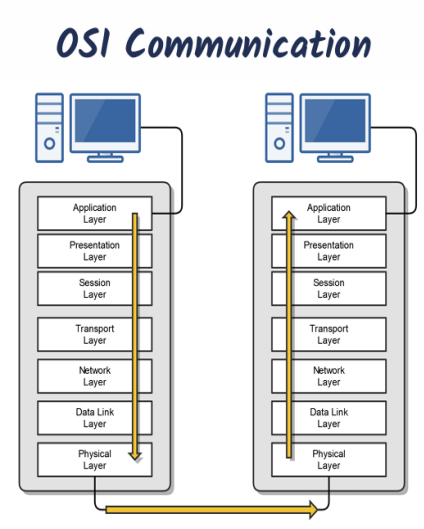
Upper Layers (Host Layers)

- Handled by the host computer and performs application-specific functions, such as data formatting, encryption, and connection management.

Lower Layers (Media Layers)

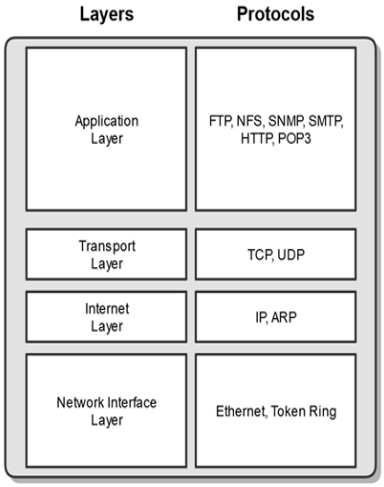
- Provide network-specific functions, such as routing, addressing, and flow control.

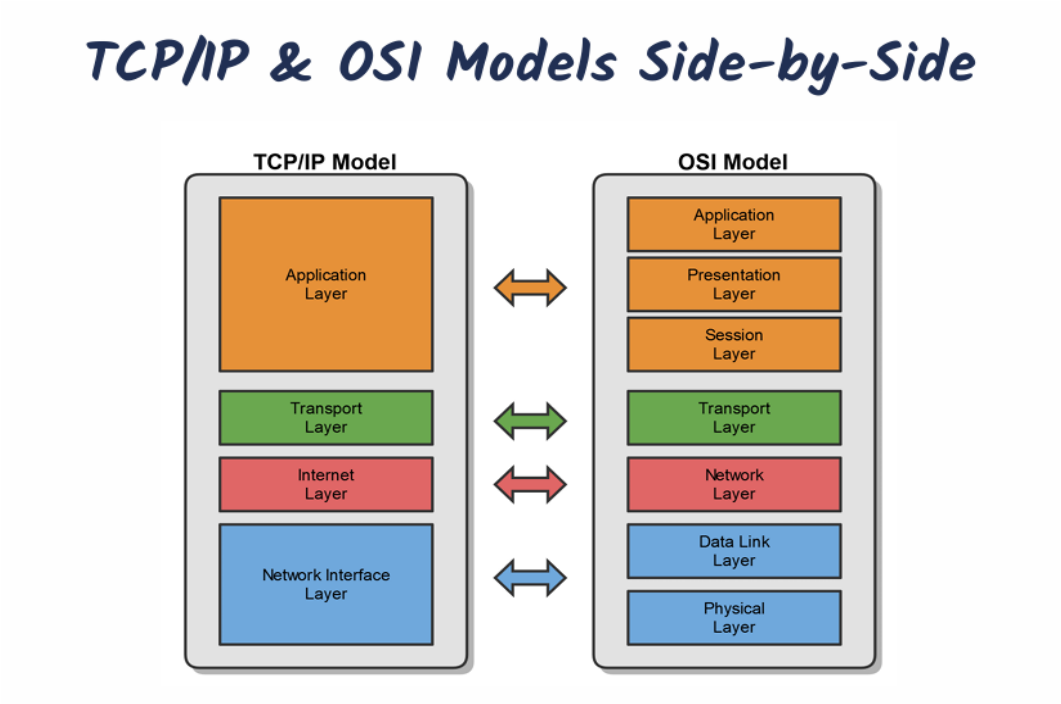




The TCP/IP Model:

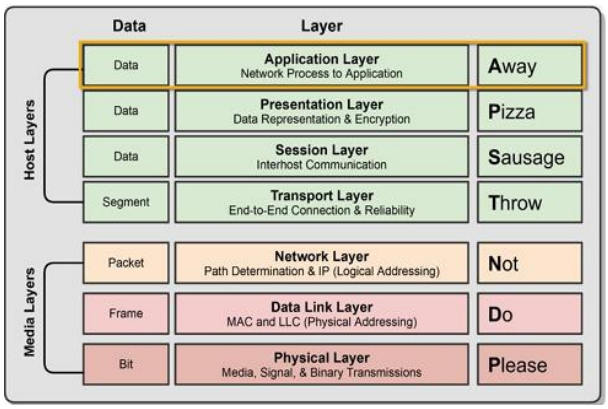
- The TCP/IP suite is the most commonly used protocol suite in the networking world.
- It's essentially the protocol suite in which the Internet was built.
- It's the standard for computer networking.
- It is based on a 4-layer model that is similar to the OSI model.
- History of TCP/IP:
    - Developed by the United States Department of Defense (DoD) in the early 1970s.
    - In 1982, the DOD declared TCP/IP as the standard for all military computer networking.
    - In 1984, broad adoption of TCP/IP began (IBM, AT&T, etc.).





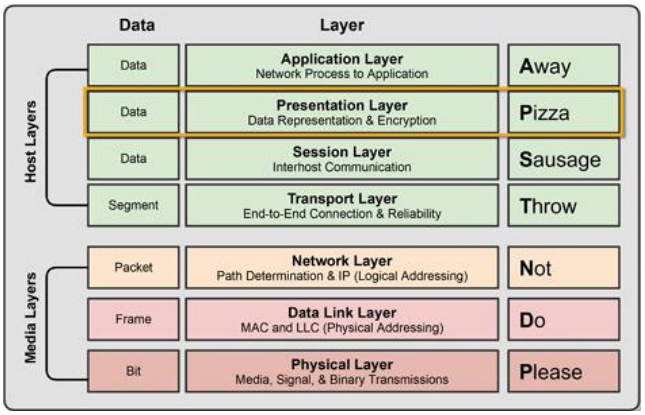
All 7 Layers of OSI Model Details Explanaton :

Layer 7 – Application Layer



- Where users interact with the computer.
- Acts as an interface between an application and end-user protocols.
- Provides an interface to communicate with the network (Outlook, Chrome, etc.).
- Applications don't reside in the application layer but instead interfaces with application layer protocols.
- Example Application Layer Protocols:
    - **E-Mail:** IMAP4, POP3, SMTP
    - **Web Browsers:** HTTP, HTTPS
    - **Remote Access:** SSH, Telnet

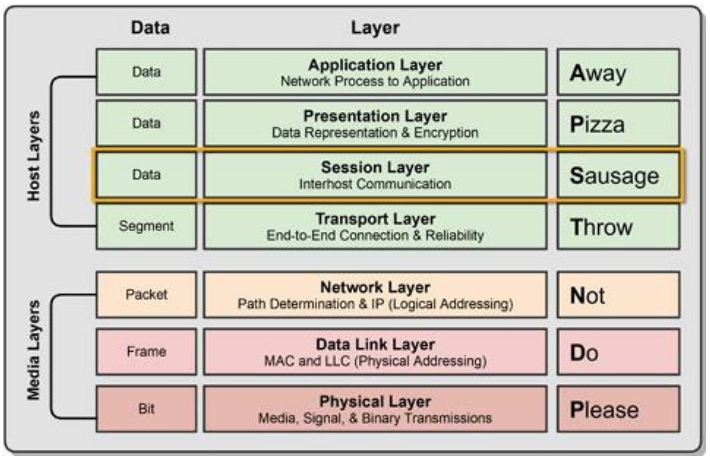
Layer 6 – Presentation Layer

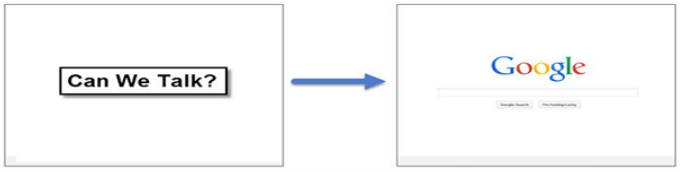


- Ensures that data transferred from one system's Application Layer can be read by the Application Layer on another one.
- Provides character code conversion, data compression, and data encryption/decryption.
- Example: Google Chrome HTML converted to ASCII Format.
- Example Layer 6 File Formats:
    - Web Browser: HTML, XML, JavaScript
    - Graphics Files: JPEG, GIF, PNG
    - Audio/Video: MPEG, MP3
    - Encryption: TLS, SSL
    - Text/Data: ASCII, EBCDIC

Layer 5 – Session Layer

- Responsible for setting up, managing, and then tearing down sessions between network devices.
- Ensures data from different application sessions are kept separate.
- Utilizes Application Program Interfaces (APIs) to communicate with TCP/IP protocols.
- Coordinates communication between systems.
- Start, Stop, Restart.



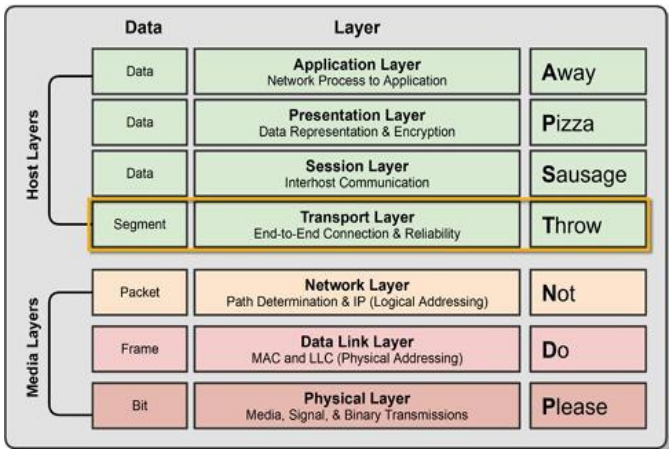


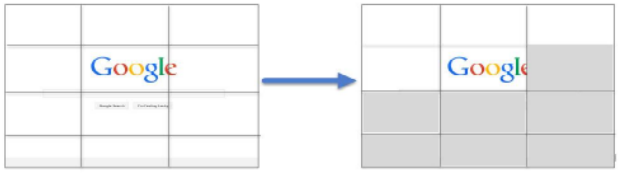
Can provide three different methods of communication between devices:

- **Simplex:** One-way communication between two devices, like listening to a radio station.
- **Half Duplex:** Two-way communication between two devices, but only one device can communicate at a time.
- **Full Duplex:** Two-way communication between two devices, where both sides can communicate at the same time.

Layer 4 – Transport Layer

- Ensures data is delivered error-free and in sequence.
- Segments data and reassembles correctly.
- Can be connection-oriented or connectionless.
- Considered the "Post Office" Layer
    - TCP (Transmission Control Protocol)
    - UDP (User Datagram Protocol)
    - Covered in detail in the next section.



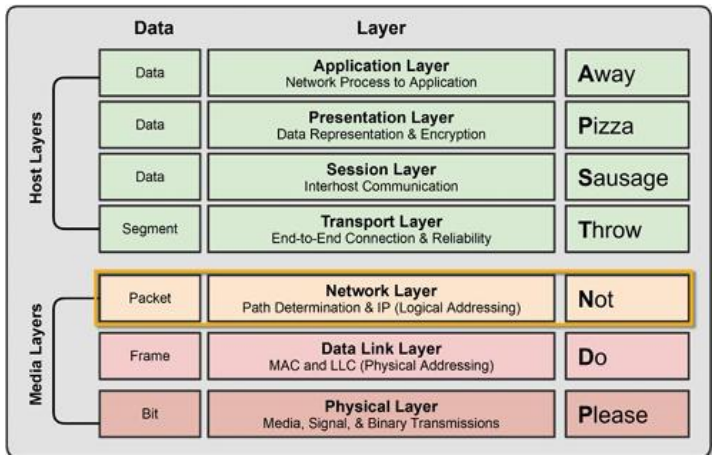


- Responsible for two data flow control measures:
    - Buffering: Stores data in memory buffers until destination device is available.
    - Windowing: Allows devices in session to determine the "window" size of data segments sent.

Layer 3 – Network Layer

- The "Routing" Layer
- Provides logical addressing (IP Addressing) and routing services.
- Places two IP addresses into a packet:
    - Source Address & Destination IP Address

- Internet Protocol (IP)
    - The Primary network protocol used on the internet, IPv4, IPv6 Logical Addresses.



Types of Packets at Network Layer:

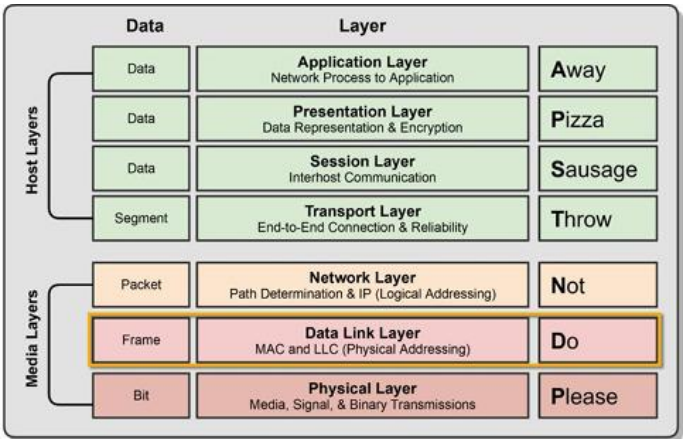
- **Data Packets**
    - Routed Internet Protocol (IP) data packet.
      (IPv4 & IPv6)
- **Route-Update Packets**
    - Routing protocol designed to update neighboring routers with router information for path determination.
      (RIP, OSPF, EIGRP, etc.)

Layer 3 Device & Protocols:

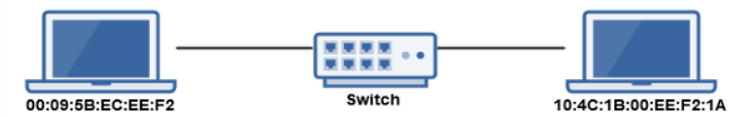
- Routers & Multi-Layer Switches
- IPv4 & IPv6
- Internet Control Message Protocol (ICMP), i.e., Ping

Layer 2 – Data Link Layer

- The “Switching” Layer
- Ensures that messages are delivered to the proper device on a LAN using hardware addresses.
    - MAC (Media Access Control) Address
    - Only concerned with the local delivery of frames on the same network.



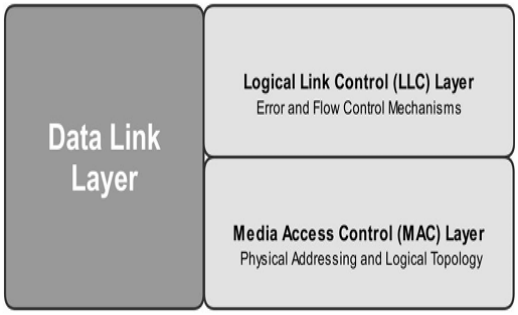
- Responsible for packaging the data into frames for the physical layer.
- Translates messages from the Network layer into bits for the Physical layer.



Has two Sub-Layers

Logical Link Control (LLC) Layer :

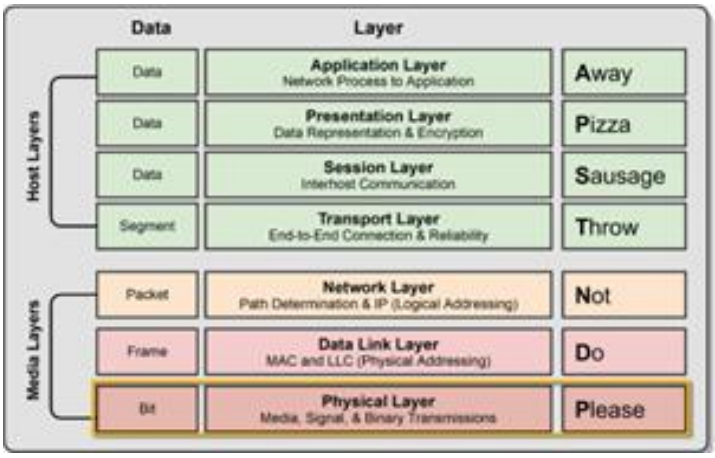
- Error Control and Flow Control
    - Detect and correct corrupted data frames.
    - Limits amount of data sent so devices aren’t overwhelmed.
- Media Access Control (MAC) Layer
    - Physical Addressing (MAC Address)
      48-Bit MAC Address burned on NIC.
    - Logical Topology and Media Access
      Ethernet, Token Ring, etc.
      CSMA/CD & CSMA/CA



Layer 1 – Physical Layer

Defines the physical and electrical medium for network communication:

- Sending and receiving bits (1 or 0)
- Encoding Signal Types
    - Electricity, radio waves, light
- Network Cabling, Jacks, Patch Panels, etc.
    - Copper or Fiber
- Physical Network Topology.
    - Star, Mesh, Ring, etc.
- Ethernet IEEE 802.3 Standard
- Layer 1 Equipment
    - Hubs, Media Converters, Modems



It's responsible for the network hardware and physical topology.

OSI Encapsulation & De-Encapsulation