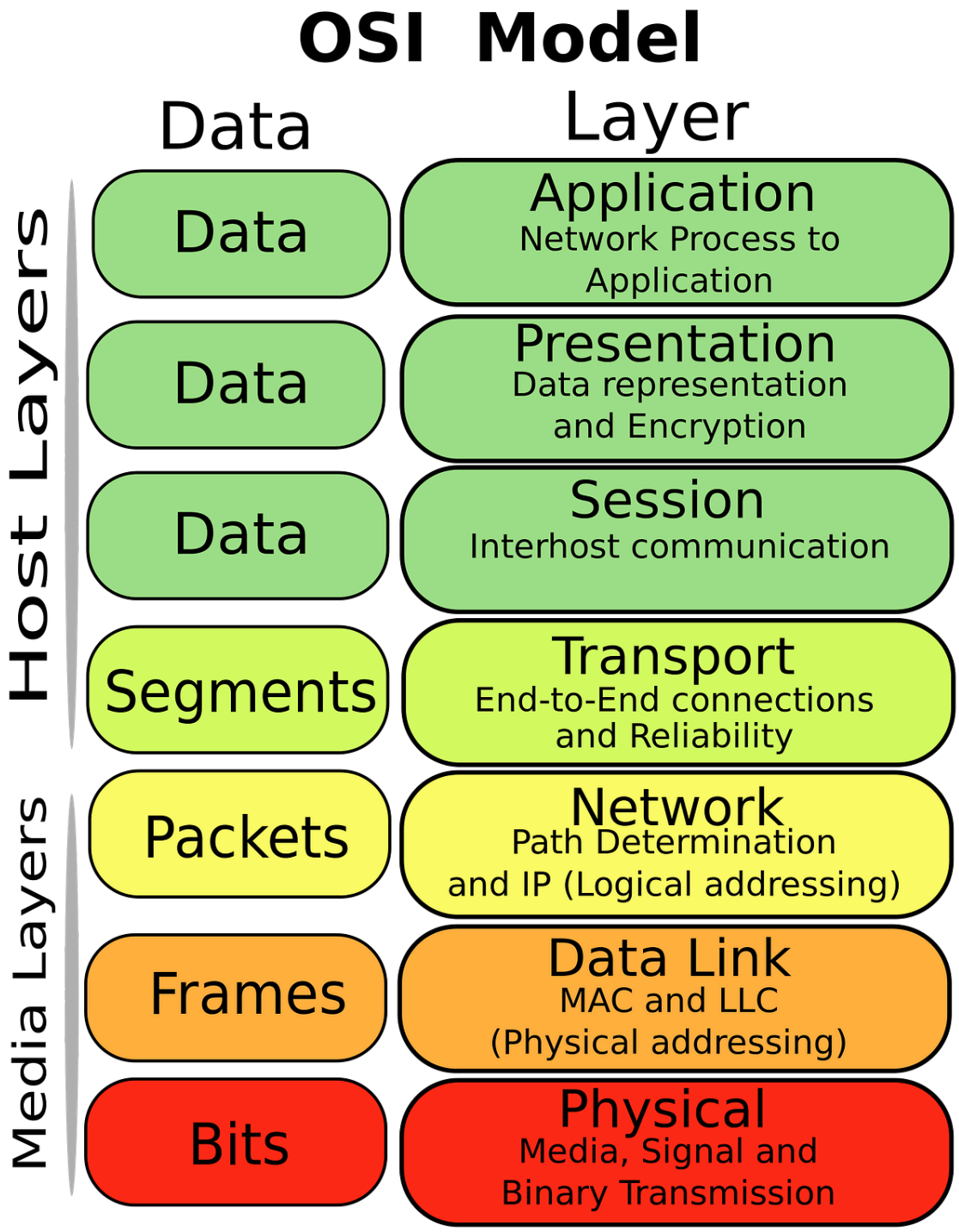
Day 2

OSI Model



1. **Physical Layer:**
   - It is the lowest layer of OSI model.
   - Actual physical connection between devices.
   - It transmits data or information in the form of Bits.

- Functions of Physical layer are:
  - **Data rate:**
    Defines the Rate of Transmission(Number of bits transmitted per second)
  - **Interface:**
    Defines the interface between devices and transmission media.
  - **Representation of Bits:**
    Defines the type of encoding, how 0s and 1s are changed to signals.
  - **Line configuration**:
    Defines how devices connect to a communication link.
  - **Transmission Modes:**
    Defines direction of transmission, i.e. Simplex, Half-Duplex & Full-Duplex.
  - **Topology:**
    Physical structure of network, i.e. Bus, Ring, Star, Mesh.
- **Some Attacks on Physical Layer:**
  - **USB Attacks:**
    Plugging infected USB devices into the target. The USB contains a malware. E.g. Rubber Ducky attacks.
  - **Sniffing/Eavesdropping:**
    Capturing raw data transmitted over the wires. Example: Physically tapping a cable to copy data over a wire.
  - **Skimming:**
    The physical installation of a malicious electronic device (a "skimmer") onto a legitimate card reader (like an ATM, gas pump, or POS terminal) to illegally capture card data from the magnetic stripe or chip during a transaction.

2. **Data Link Layer (DLL):**
   - It is responsible for node-to-node transmission of data.
   - It's main functionality is to oversee data transmitted over the physical layer and ensure they are error-free.
   - Major Functions of Data Link Layer:
     - **Framing**:
       a point-to-point connection between two computers or devices consisting of a wire in which data is transmitted as a stream of bits.
     - **Physical addressing:**
       DLL adds physical addresses (MAC Addresses) of the sender and receiver so that they can communicate.
     - **Error Control**:
       It detects and re-transmits lost or corrupted frames.
     - **Access Control:**
       the MAC-sub layer helps to determine which device has control over the channel at a given time.
   - **Some Attacks on Data Link Layer:**

- **ARP Poisoning/Spoofing:**
  An attacker sends fake ARP messages to associate their MAC address with another device's IP address, redirecting traffic (MitM).
- **MAC Spoofing:**
  An attacker changes their device's MAC address to impersonate a legitimate device, bypassing access controls or gaining unauthorized entry.
- **DHCP Spoofing:**
  A fake DHCP server provides malicious IP configurations, or an attacker consumes all available IP addresses, denying service to legitimate users.

3. **Network Layer:**
   - Responsible for connecting different devices.
   - Transmits data through packet routing, i.e finding the shortest path from source to destination from the number of routes available.
   - Sends data as packets
   - Functions of Network Layer:
     - **Routing:**
       Determines the suitable route for data transfer from source to destination.
     - **Logical Addressing:**
       Identifies each device through a unique address i.e. IP addresses (Class A to D).
     - **Host-to-Host Delivery:**
       Ensures the data is transmitted properly from sender to receiver.
   - **Some Attacks on Network Layer:**
     - **DDoS (Distributed Denial of Service):**
       Overwhelming a network or server with traffic, which takes up resources.
     - **IP Spoofing:**
       Faking an IP to evade firewalls.
4. **Transport Layer:**
   - Provides services from application layer and takes services from network layer.
   - Data is represented as Segments
   - Major protocols: TCP(Transmission Control Protocol), UDP (User Datagram Protocol), NetBIOS, PPTP(Point-to-Point Tunneling protocol)
   - Functions:
     - **Segmentation and Reassembly:**
       Accepts the message from session layer and breaks it down into smaller units.
     - **Congestion Control:**
       It uses techniques like Open Bucket and Leaky Bucket Congestion Control.
     - **Service Point Addressing:**
       Using this address Transport Layer ensures the packer is delivered in the correct destination.
   - **Some attacks on Transport Layer:**

- **SYN flood**
- **UDP flood**
- **Smurf Attack**

5. **Session Layer:**
   - Responsible for creation, managing, maintaining and terminating the sessions between two devices.
   - Protocols: NetBIOS and PPTP(Point-to-Point Tunneling Protocol)
   - Functions:
     - Session Establishment, Maintenance and Termination
     - Synchronization (allows a process to add checkpoints that are considered synchronization points in the data.)
     - Dialog Controller (allows two start communications in half-duplex or duplex mode.)
   - Some Attacks on Session Layer:
     - **Session Hijacking:** An Attacker can steal the user's cookie to hijack their session and impersonate them.
6. **Presentation Layer:**
   - Responsible for translating data from one format to another.
   - Also known as Translation layer.
   - Functions:
     - **Translation** from one format to another, e.g. JPG TO PNG
     - **Encryption/Decryption** of data
     - **Compression**
   - **Some Attacks on Presentation Layer:**
     - **XSS/CSRF:** Injecting malicious JavaScript Code or requests into un-sanitized inputs.
     - **Encryption Vulnerabilities:** Exploiting weak ciphers (like older DES/RC4) or implementation flaws (POODLE, BEAST) to decrypt data.
7. **Application Layer:**
   - The top Layer of OSI model
   - It acts as an interface between User and Application.
   - Functions:
     - **Data Representation:**
       Ensures data is in readable format for both receiver and sender.
     - **Network Service Access:**
       Provides applications with access to network services, enabling communication over network.
     - **Application Protocols:**
       Supports protocols like HTTP, FTP, SMTP, and DNS that enable communication between applications.

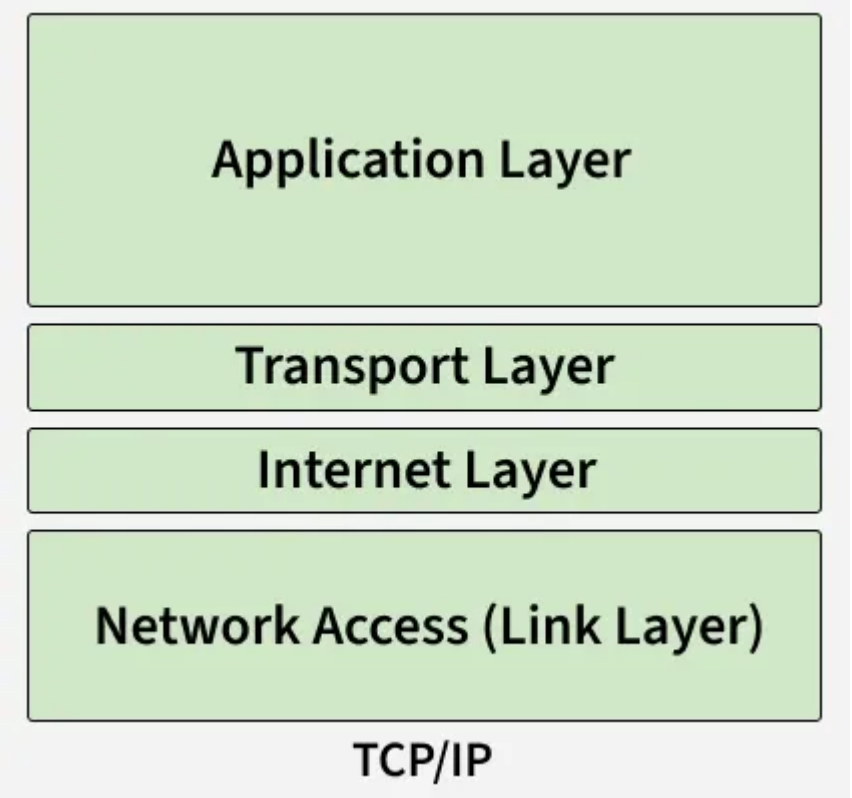
    - **Session Management:**
      Manages establishment, maintenance, and termination of sessions between applications.
- **Some Attacks on Application Layer:**
- **SQLi (SQL Injection):** Injecting malicious payload (SQL code) in unsanitized input connected to SQL databases.

Glossary:

- **Bit Stuffing:**
  a technique implemented in data communication and networking to restrict specific bit patterns in the data to stop from being confused with control signals.
- Byte Stuffing:
  a technique that adds an extra byte when a byte matching the flag or escape byte appears in data.

TCP/IP Basics

A simpler version of OSI model that contains 4 layers instead of 7.



OSI Model	TCP/IP Model
OSI stands for Open Systems Interconnection	TCP/IP stands for Transmission Control Protocol/Internet Protocol
OSI model has 7 layers	OSI model has 4 layers
Packages delivery is guaranteed.	Package delivery is not guaranteed.

OSI Model	TCP/IP Model
Each layer is independent of the other.	Some layers are required by others.
A conceptual model, not used in the practical world.	Widely used in actual networks like Internet and Communication systems.

Common Ports and Protocols in Networking

The most common ports and protocols are:

1. **FTP (File Transfer Protocol):**
   - **Description:**
     File Transfer Protocol is a protocol used to transfer files from one device to another.
   - **Port:** 21
2. **SSH (Secure Shell):**
   - **Description**:
     Secure Remote Connection protocol secured by cryptography.
   - **Port:** 22
3. **TELNET (Teletype Network):**
   - **Description:**
     A legacy protocol used for remote logins and connection.
   - **Port:** 23
4. **SMTP (Simple Mail Transfer Protocol):**
   - Description:
     A standard internet protocol for sending emails.
   - **Port:** 25
5. **DNS (Domain Name System):**
   - **Description:**
     A hierarchical and distributed naming system that translates domain names into IP addresses.
   - **Port:** 53
6. **DHCP (Dynamic Host Configuration Protocol):**
   - **Description:**
     Dynamically assigns IP addresses to the hosts on the network.
   - **Port:** 67 (Server), 68 (Client)
7. **HTTP (Hyper-text Transfer Protocol):**
   - **Description:**
     A Standard client-server protocol that allows web browsers to request and servers to send web contents like images, videos , files, etc.
   - **Port:** 80
8. **Kerberos:**

- **Description:**
  A network authentication system. It works on the basis of tickets.
- **Port:** 88

9. **POP3 (Post Office Protocol Version 3):**
   - **Description:**
     An Old mail service protocol.
   - **Port:** 110
10. **NetBIOS (Network Basic Input/Output System):**
    - **Description:**
      A legacy API and session layer service allowing apps on different computers to talk on a LAN, providing name resolution, datagrams, and sessions, but it's an interface, not a protocol itself.
    - **Port:** 137 (Name Service Registration and Resolution), 138 (Datagram Service), 139 (Session Service).
11. **IMAP (Internet Message Access Protocol):**
    - **Description:**
      Management of electronic mail messages on a server.
    - **Port:** 143
12. **HTTPS (Hyper-text Transfer Protocol over SSL):**
    - **Description:**
      A Secure version of HTTP(Hyper-text Transfer protocol). It uses TLS/SSL (Transport Layer Security/Secure Socker Layer) encryption to protect the data between the browser and website.
    - **Port:** 443
13. **LDAP (Lightweight Directory Access Protocol):**
    - **Description:**
      A central location for accessing and managing directory services.
    - **Port:** 389
14. **syslog:**
    - **Description:**
      A protocol used for collecting and organizing logs sent from various devices on a network.
    - **Port:** 514
15. **MySQL (Structured Query Language):**
    - **Description:**
      A database server that uses relational database using SQL.
    - **Port:** 3306