Network Protocols, TCP/IP & OSI Models, and Security Analysis

Name: Shruti Malik

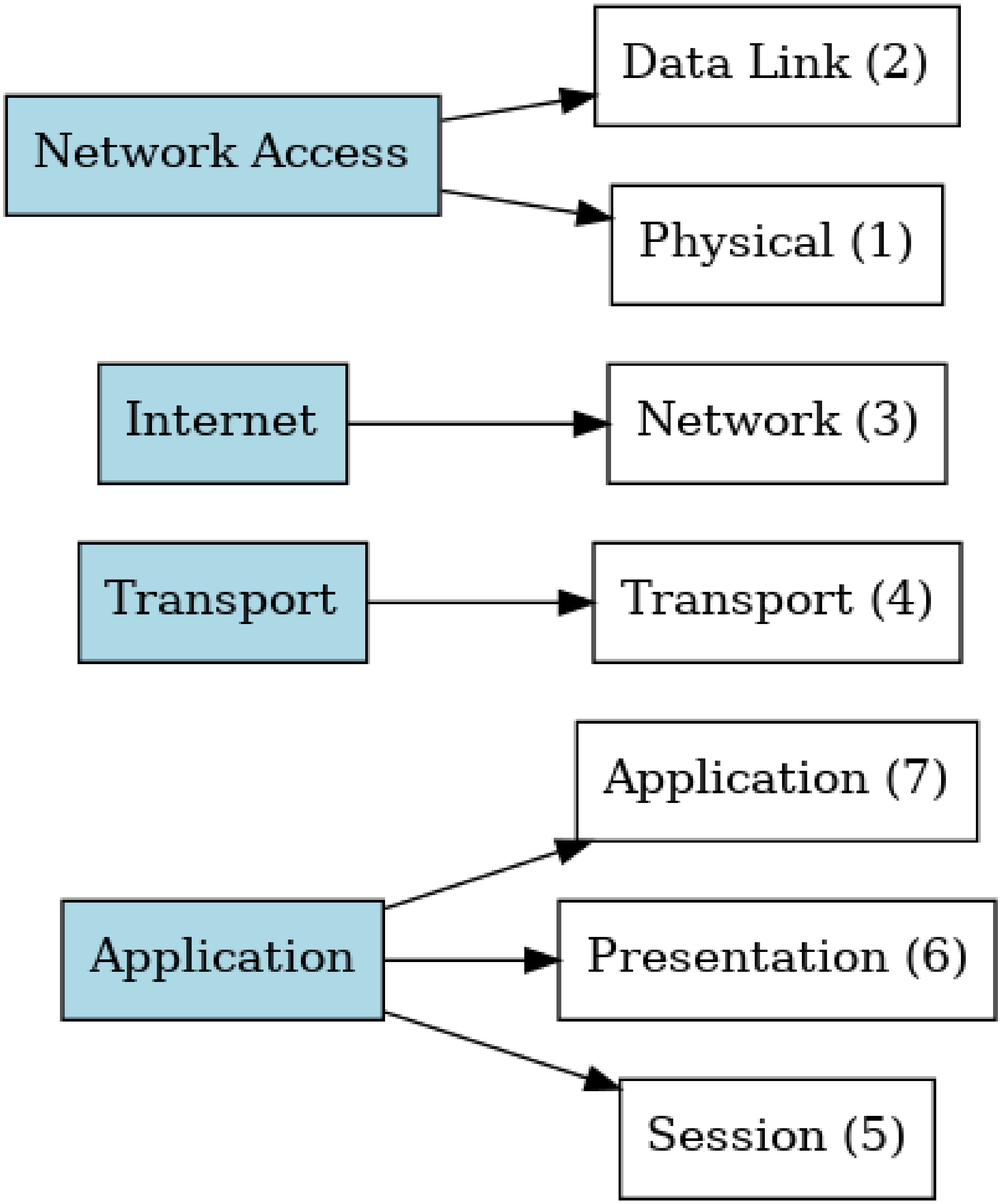
Course: IT Fundamentals and Network Security

Capella University

Date: July 10, 2025

Part 1 – Mapping TCP/IP to OSI Layers

TCP/IP to OSI Layer Mapping Diagram



Encapsulation Process

Data flows from the application layer in the OSI model downwards. As it goes down each layer, the header (sometimes a trailer) of that layer is added, forming a wrapped protocol data unit (PDU):

1. Application/Presentation/Session: data is created/formatted.

2. Transport Layer: TCP or UDP header is added, creating a segment.

3. Network Layer: IP header is added, creating a packet.

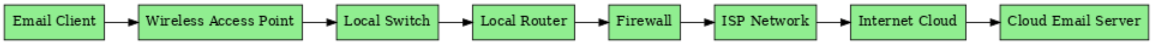
4. Data Link Layer: MAC addresses added in (frame header/trailer), creating a frame.

5. Physical Layer: The frame is converted into bits that can be transmitted on the medium (electrical, fiber or radio).

At the destination host the above process is reversed (decapsulation).

Part 2 – Email Client and Cloud-Based Email Path Diagram

Email Transmission Path Diagram



Data Transmission Process

Steps involved when sending an email with a cloud-based email client:

1. Client to wireless access point, then to local switch

2. To router, firewall, ISP infrastructure, then to the Internet

3. To cloud provider (Microsoft 365, Gmail, etc.)

4. Replies return in the reverse direction back to client

The packets passed between devices on each step carry multiple protocol layers, for example Ethernet frames at the data link layer and IP packets at the network layer.

Part 3 – The OSI Layer and Security

Functions of OSI Layers in Cloud Email Transmission

OSI Layer	Primary Function	Role in Email Transmission
Application	End-user app protocols (HTTP, SMTP)	Email client interface
Presentation	Data format (encryption, compression)	TLS encryption for secure email
Session	Session management	Maintains active email session
Transport	Reliable delivery (TCP)	Ensures message is delivered fully
Network	Logical addressing, routing (IP)	Routes data across networks
Data Link	MAC addressing, framing	Ensures error-free delivery to next hop
Physical	Bit transmission	Wi-Fi or Ethernet signal transmission

TCP/IP Security Vulnerabilities

1. IP Spoofing: The source IP address can be faked to make it appear to be from another host.

2. Man-in-the-Middle (MitM) Attacks: Lack of encryption or validation in communications allow them to be intercepted.

3. Lack of Native Encryption: No built-in encryption to ensure the security of a payload. TLS/SSL must be manually implemented.

4. DoS/DDoS Attacks: Attacks that take advantage of TCP connection-handling to overwhelm networks with traffic.

References

Forouzan, B. A. (2021). Data Communications and Networking (6th ed.). McGraw-Hill Education.

Smith, R. (2023). Understanding TCP/IP Security Vulnerabilities. Cybersecurity Today Journal, 9(2), 33–42.

Polinati, A. K. (2025). Hybrid Cloud Security: Balancing Performance, Cost, and Compliance in Multi-Cloud Deployments. arXiv. https://arxiv.org/abs/2506.00426

ChatGPT 2025