

Information Security

Prepared by Dr. Ahmed Omar

IT373
Information Security

Lecture 8



Network Security & Protocols

Lecture 8

IT373
Information Security

Prepared by
Dr. Ahmed Omar



Agenda

- ☐ **Understanding Network Communication: The OSI Model**
- ☐ **Network Security Protocols**
- ☐ **Network Security Protections**

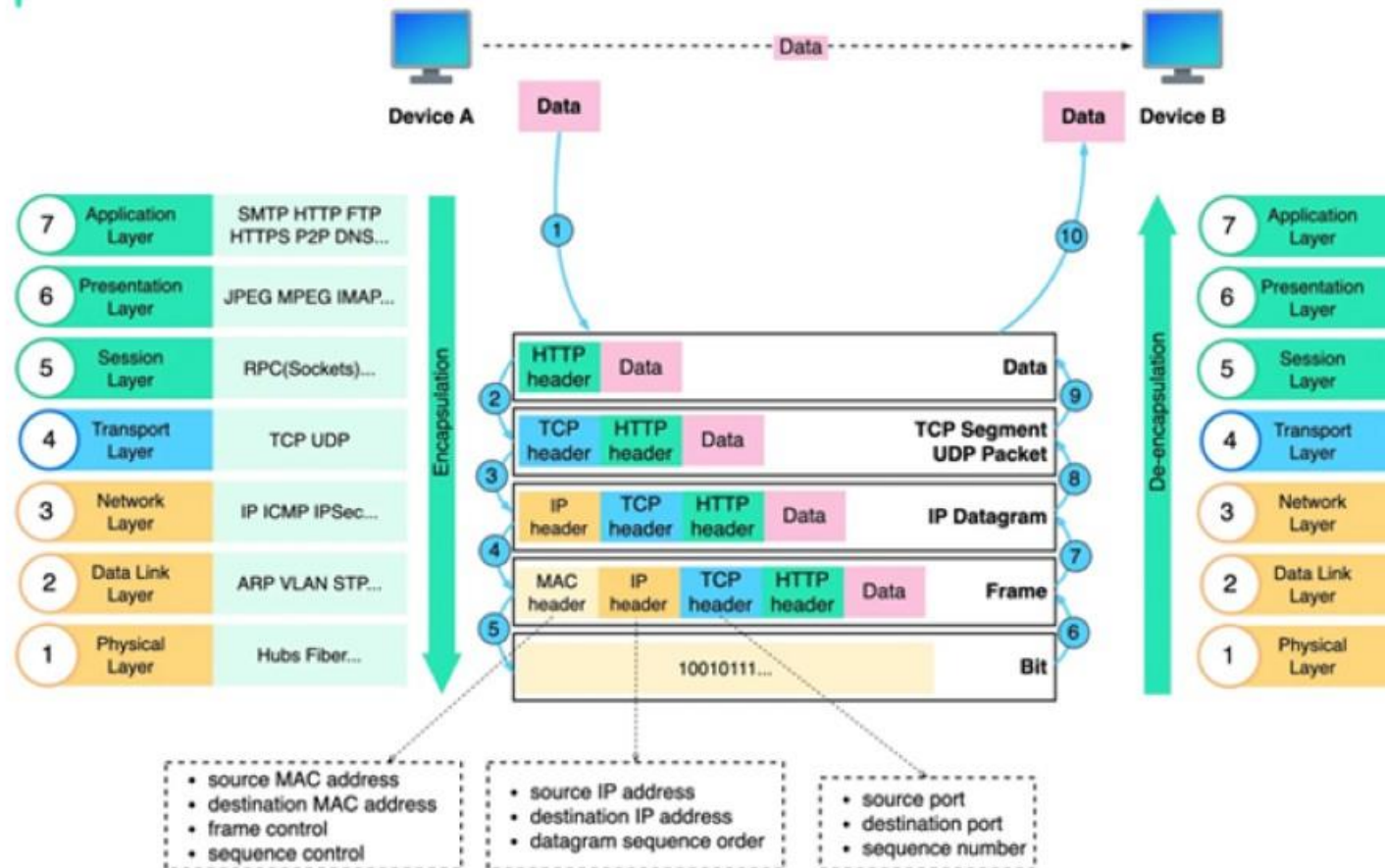
Introduction to Network Security

❑ Network security is the broad discipline dedicated to the **protection** of digital networks, both *private* and *public*, against unauthorized access, misuse, malfunction, modification, or destruction. In today's interconnected world, attackers increasingly target networks for sensitive data theft, service disruption, and financial gain.

Understanding Network Communication

What is OSI model

blog.bytebytego.com

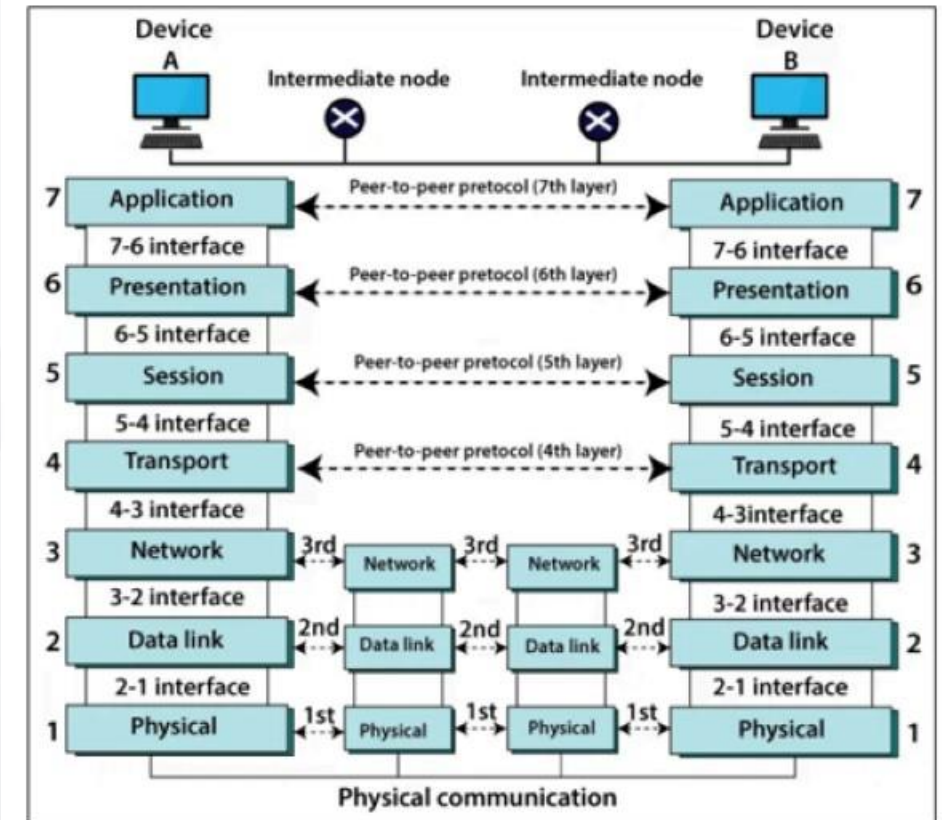


What is the OSI Model?

- ❑ The **Open Systems Interconnection** (OSI) model is a conceptual framework that **standardizes** the functions of a telecommunication or computing system without regard to its underlying internal structure and technology.
- ❑ **Purpose:** To provide a common basis for the coordination of standards development for systems interconnection while allowing existing standards to be placed into perspective.

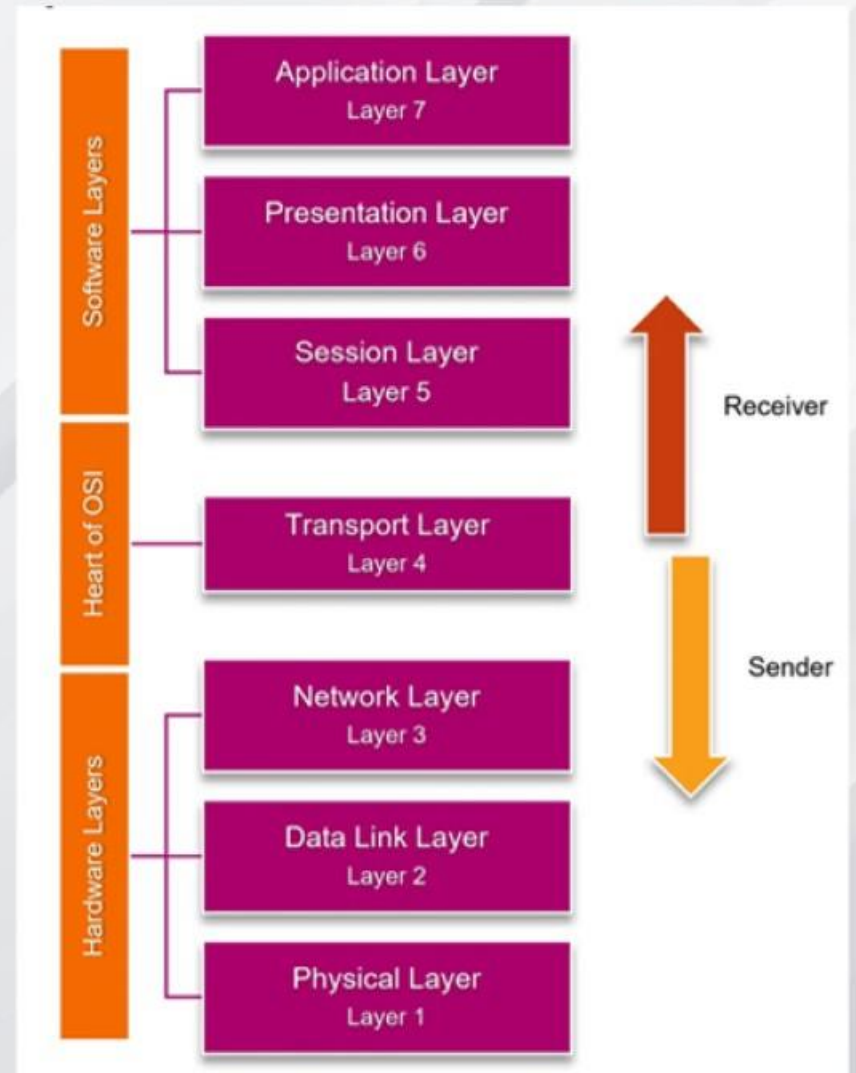
What is the OSI Model?

- ❑ **History:** Developed by the International Organization for Standardization (ISO) in 1984 to facilitate communication between different systems.
- ❑ **Importance:** Provides a systematic way to discuss network operations, troubleshoot networking problems, and develop new networking technologies.



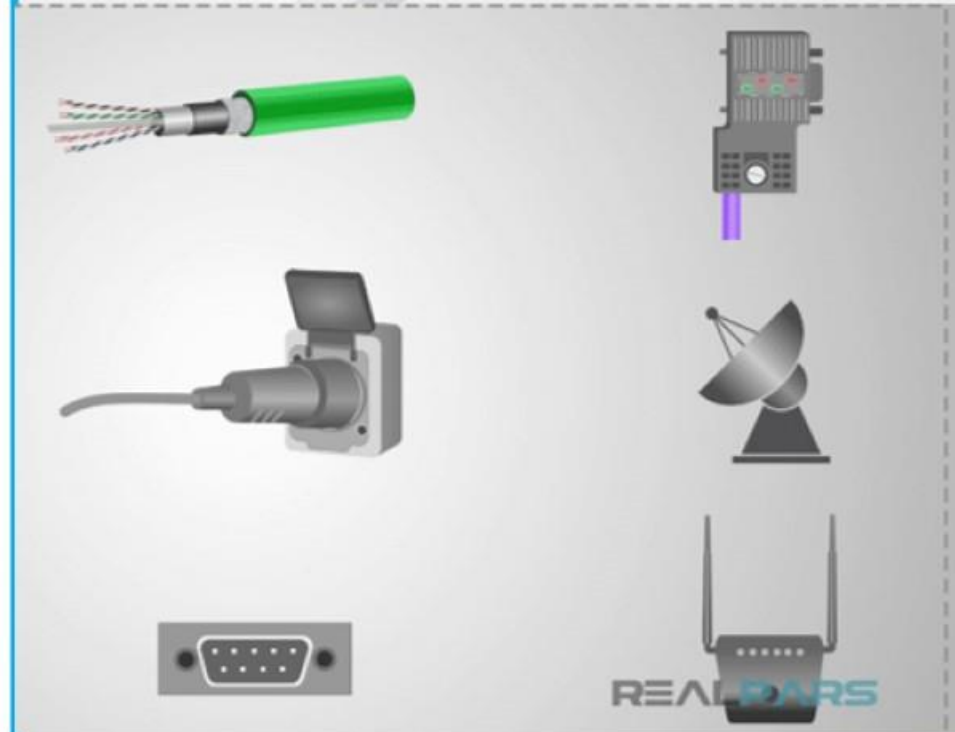
The 7 Layers Overview

- ❑ The **OSI** model divides network communication into seven distinct layers, each with specific functions and responsibilities



Layer 1: Physical Layer

- ❑ **Definition:** The lowest layer of the OSI model that transmits **raw bit** streams over a physical medium. focuses on the physical connection between devices and the transmission of raw data bits.
- ❑ **Key Functions:** Defines electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating physical links.



Layer 1: Physical Layer

Security Concerns:

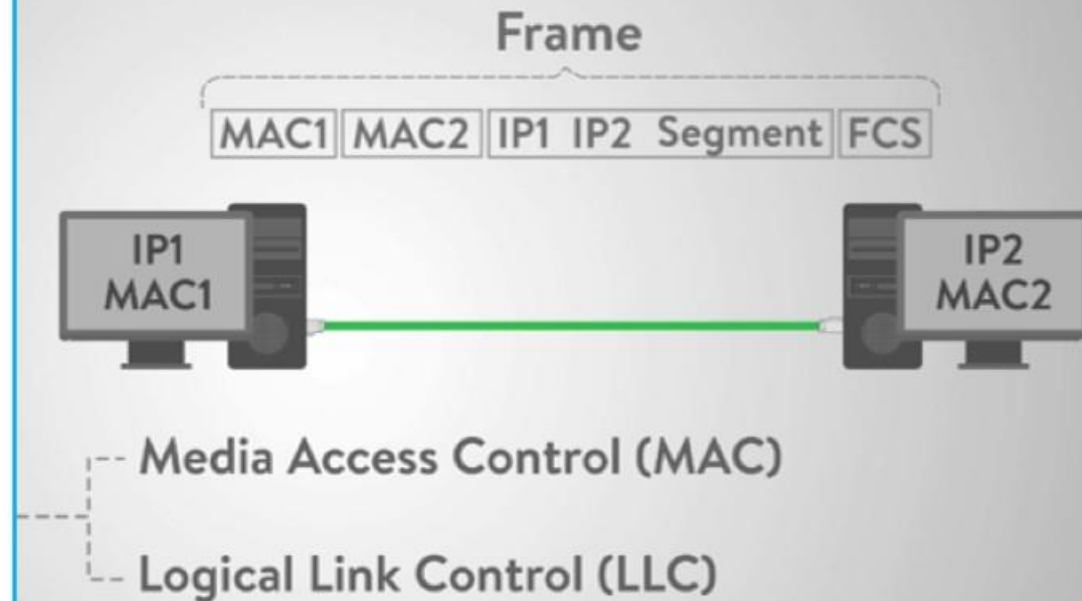
- Physical access to network infrastructure (cables, switches, routers)
- Electromagnetic interference and eavesdropping
- Cable tapping and wiretapping
- Environmental attacks (power, cooling, natural disasters)

Vulnerabilities:

- Unsecured network closets and data centers
- Unencrypted data transmission over physical media
- Lack of physical access controls

Layer 2: Data Link Layer

- ❑ **Definition:** The Data Link Layer provides reliable data transfer across the physical link, handling error detection and correction, flow control, and **medium access control**.
- ❑ This layer is responsible for organizing bits from the Physical Layer into **frames** and ensuring reliable delivery between directly connected nodes.



Layer 2: Data Link Layer

❑ Key Functions

- ❑ **Frame Formation:** The layer organizes raw bits into structured frames that include **headers**, **data payload**, and **trailers**. Frame formats vary by technology but typically include addressing information, control fields, and error detection codes.
- ❑ **Error Detection and Correction:** Implementing mechanisms to detect and potentially correct transmission errors. Common techniques include **Cyclic Redundancy Check (CRC)**, checksums, and **Forward Error Correction (FEC)** codes. The layer can request retransmission of corrupted frames.

Layer 2: Data Link Layer

❑ Key Functions

- ❑ **Flow Control:** Managing the rate of data transmission between devices to prevent overwhelming the receiver. This includes *stop-and-wait* protocols, *sliding window* protocols, and buffer management to ensure smooth data flow.
- ❑ **Medium Access Control (MAC):** In shared media environments, this sublayer coordinates access to the transmission medium to prevent collisions and ensure fair access among multiple devices. This includes CSMA/CD for Ethernet and CSMA/CA for Wi-Fi.

Layer 2: Data Link Layer

Security Concerns:

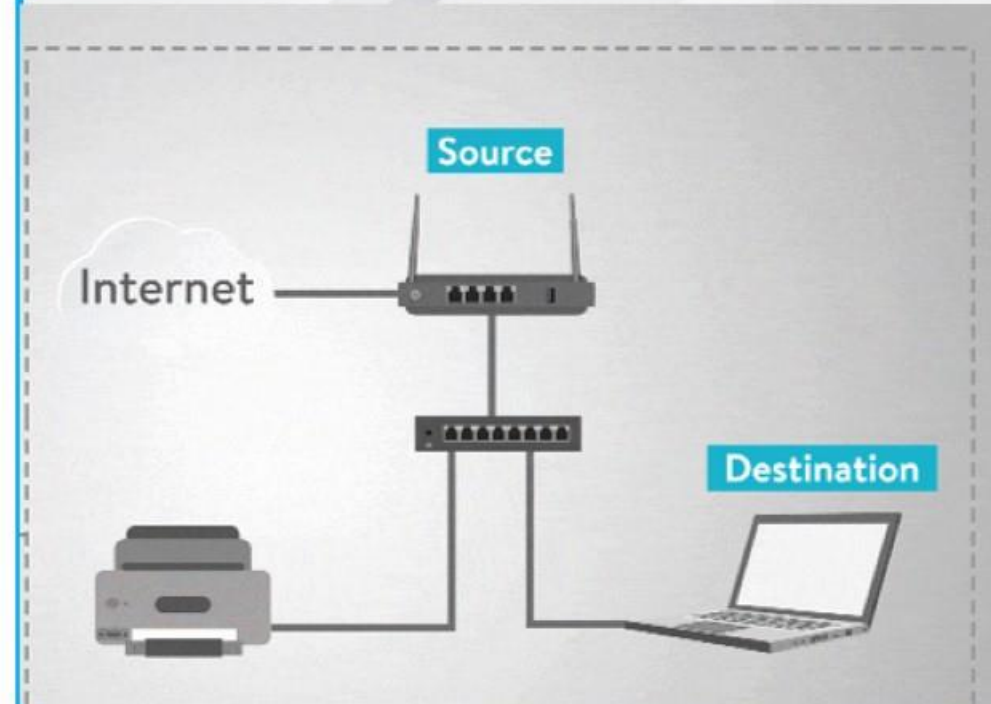
- **MAC** address spoofing and **Address Resolution Protocol(ARP)** poisoning
- **VLAN** hopping attacks
- Wireless security (WEP/WPA vulnerabilities)
- Switch flooding and CAM table overflow

Vulnerabilities:

- Weak wireless encryption protocols
- Unmanaged switch configurations
- Broadcast domain security weaknesses

Layer 3: Network Layer

- ❑ The Network Layer is responsible for routing data between different networks, providing logical addressing, path determination, and packet forwarding. This layer enables communication between devices across multiple network segments and provides the foundation for internetworking.
- ❑ **Key Responsibilities:** Logical addressing, path determination, packet switching, and traffic control.



Layer 3: Network Layer

Key Functions

- ❑ **Logical Addressing:** Implementing hierarchical addressing schemes that enable routing across multiple networks. The most common addressing scheme is Internet Protocol (IP) addressing, which provides globally unique addresses for network devices.
- ❑ **Routing:** Determining the best path for data packets to travel from source to destination across multiple networks. Routing involves path selection based on metrics such as hop count, bandwidth, delay, and network congestion.
- ❑ **Packet Forwarding:** Making forwarding decisions for each packet based on destination addresses and routing table information. Routers examine destination addresses and forward packets toward their destinations.
- ❑ **Fragmentation and Reassembly:** Handling packets that are too large for the underlying network technology by fragmenting them into smaller pieces and reassembling them at the destination.

Layer 3: Network Layer

Security Concerns:

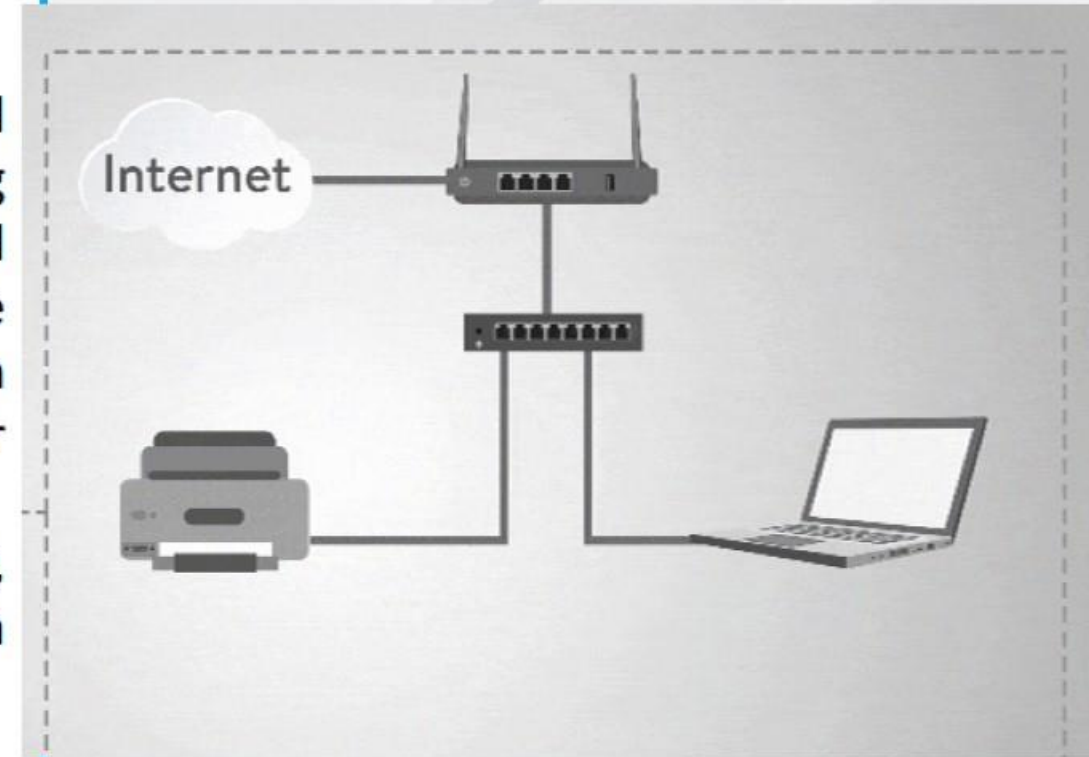
- IP spoofing and routing attacks
- ICMP-based attacks (ping of death, smurf attacks)
- Routing protocol manipulation (BGP hijacking)
- Network reconnaissance and scanning

Vulnerabilities:

- Inadequate router access controls
- Unfiltered ICMP traffic
- Routing protocol authentication weaknesses
- IP fragmentation attacks

Layer 4: Transport Layer

- ❑ The Transport Layer provides reliable end-to-end communication services for applications, handling **segmentation, flow control, error recovery, and connection management**. This layer abstracts the complexities of network communication from applications and provides standardized interfaces for data transfer.
- ❑ **Responsibilities:** Ensures complete data transfer, provides reliability, establishes connection between hosts.



Layer 4: Transport Layer

Key Functions

- ❑ **Segmentation and Reassembly:** Breaking large application data into smaller segments that can be transmitted over the network and reassembling them at the destination.
- ❑ **Connection Management:** Establishing, maintaining, and terminating connections between applications. Connection-oriented protocols provide reliable, ordered delivery while connectionless protocols provide faster, low-overhead communication.
- ❑ **Flow Control:** Managing the rate of data transmission to prevent overwhelming the receiver.
- ❑ **Error Recovery:** Detecting and recovering from lost, corrupted, or duplicate segments. Error recovery typically involves acknowledgment mechanisms, timeout and retransmission, and duplicate detection.
- ❑ **Multiplexing:** Enabling multiple applications to share network resources simultaneously through port-based addressing.

Layer 4: Transport Layer

Security Concerns:

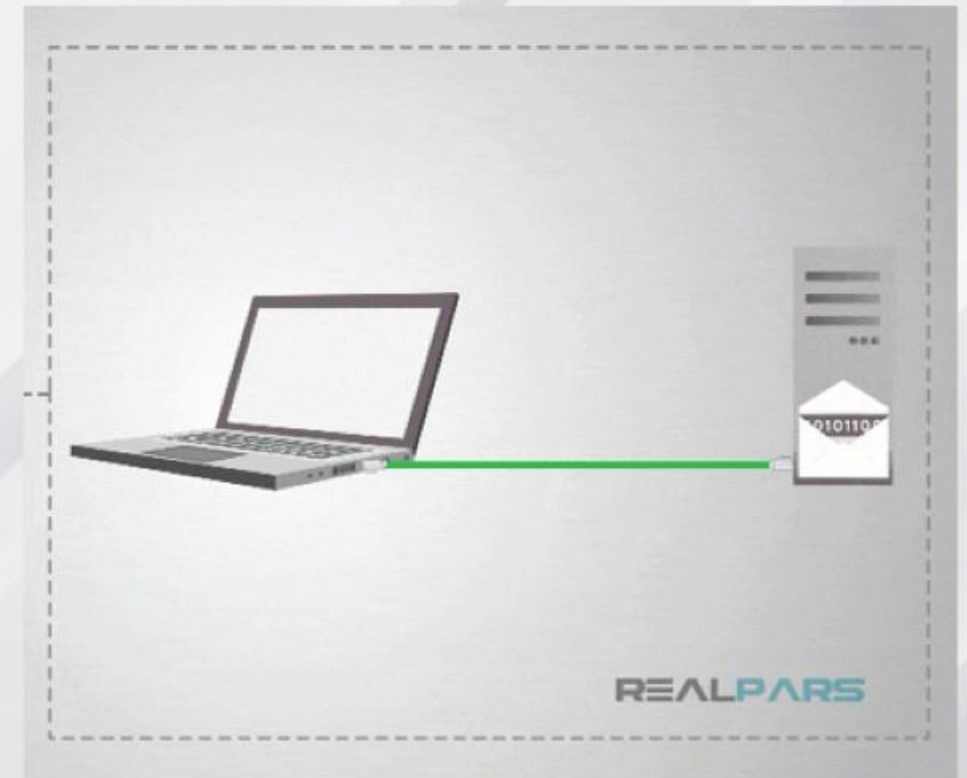
- TCP sequence number attacks and session hijacking
- SYN flooding and other DoS attacks
- Port scanning and service enumeration
- UDP-based amplification attacks

Vulnerabilities:

- Weak session management
- Unencrypted data transmission
- Inadequate port filtering and access controls

Layer 5: Session Layer

- ❑ The **Session Layer** manages sessions between applications, providing services for establishing, managing, and terminating communication sessions. This layer handles session establishment, coordination, and **synchronization** between applications running on different hosts.
- ❑ Verifying the **identity** of users or applications attempting to establish sessions. This may involve **password authentication**, certificate-based authentication, or integration with directory services.



Layer 5: Session Layer

Key Functions

- ❑ **Session Establishment:** Creating communication sessions between applications, including authentication, and authorization. Session establishment may involve multiple round-trips to agree on communication parameters.
- ❑ **Session Management:** Maintaining active sessions including session state information, checkpointing, and recovery mechanisms. The layer tracks session status and handles session interruptions or failures.
- ❑ **Dialog Control:** Managing the communication flow between applications, including half-duplex (alternating) and full-duplex (simultaneous) communication modes. Dialog control determines which party can transmit at any given time.

Layer 5: Session Layer

Security Concerns:

- Session hijacking and fixation attacks
- Authentication bypass vulnerabilities
- Session timeout and management issues
- NetBIOS and SMB-related attacks

Vulnerabilities:

- Weak session token generation
- Inadequate session validation
- Persistent session vulnerabilities

Layer 6: Presentation Layer

- ❑ The Presentation Layer is responsible for data **translation**, **encryption**, **compression**, and **formatting** services that ensure data sent by applications can be properly interpreted by receiving applications. This layer handles syntax and semantics of information exchange between systems.



Layer 6: Presentation Layer

Key Functions

- ❑ **Data Translation:** Converting data between different formats, character encodings, and representations.
- ❑ **Encryption and Decryption:** Providing cryptographic services to protect data confidentiality and integrity.
- ❑ **Data Compression:** Reducing the size of data for more efficient transmission and storage.
- ❑ **Data Formatting:** Ensuring data is presented in formats that applications can properly interpret

Layer 6: Presentation Layer

Security Concerns:

- Encryption and decryption vulnerabilities
- Data format manipulation attacks
- SSL/TLS implementation flaws
- Compression-based attacks (CRIME, BREACH)

Vulnerabilities:

- Weak cryptographic implementations
- Certificate validation issues
- Data encoding/decoding exploits

Layer 7: Application Layer

- ❑ The Application Layer is the topmost layer of the OSI model and provides network services directly to **end-user applications**. This layer serves as the **interface** between network services and application software, handling high-level protocols, data formatting, and user interface issues.



Layer 7: Application Layer

Key Functions

- ❑ **Application Services:** Providing network services that applications can directly use, such as file transfer, email, web browsing, and database access. These services abstract network complexities from application developers.
- ❑ **User Interface:** Managing the interaction between users and network applications, including command-line interfaces, graphical user interfaces, and web-based interfaces.
- ❑ **Network Process Management:** Coordinating application processes across networks, including distributed computing, remote procedure calls, and client-server interactions.

Layer 7: Application Layer

Security Concerns:

- Web application vulnerabilities (SQL injection, XSS)
- Email-based attacks (phishing, malware)
- Authentication and authorization flaws
- API security issues
- Social engineering attacks

Vulnerabilities:

- Input validation failures
- Broken access controls
- Insecure direct object references
- Security misconfigurations

Core Security Protocols

❑ Transport Layer Security (TLS/SSL)

TLS is the foundation of secure web communications, encrypting data between clients and servers. It provides authentication, encryption, and data integrity. TLS has evolved through several versions, with TLS 1.3 being the current standard offering improved security and performance.

❑ Internet Protocol Security (IPSec)

IPSec operates at the network layer, providing end-to-end security for IP communications. It includes two main protocols: Authentication Header (AH) for data integrity and authentication, and Encapsulating Security Payload (ESP) for encryption and authentication.

Core Security Protocols

❑ **Secure Shell (SSH)**

SSH enables secure remote access and command execution over unsecured networks. It uses public-key cryptography for authentication and symmetric encryption for data transfer, replacing insecure protocols like Telnet.

Authentication Protocols

- ❑ **Kerberos** This network authentication protocol uses symmetric key cryptography and a trusted third party (Key Distribution Center) to authenticate users and services in a network environment.
- ❑ **LDAP over SSL/TLS** Lightweight Directory Access Protocol secured with encryption for accessing and maintaining distributed directory information services.

Email Security Protocols

- ☐ **S/MIME** (Secure/Multipurpose Internet Mail Extensions) Provides encryption and digital signatures for email messages.
- ☐ **PGP/GPG (Pretty Good Privacy/GNU Privacy Guard)** End-to-end encryption for email and file security using public-key cryptography.

Hyper Text Transfer Protocol Secure

- ☐ **HTTPS (Hyper Text Transfer Protocol Secure)**
- ☐ **HTTPS** is definitely among the key network security protocols, is actually HTTP combined with TLS/SSL encryption.
- ☐ **HTTPS** uses **TLS** (Transport Layer Security) to encrypt the communication between web browsers and web servers. When you see the padlock icon in your browser's address bar, that indicates the website is using HTTPS.

Network security protections

- **Firewalls** serve as the first line of defense, controlling traffic flow between networks based on predetermined security rules. They can be hardware-based, software-based, or cloud-delivered, filtering packets at various network layers.
- **Network Access Control (NAC)** systems authenticate and authorize devices before allowing network access, ensuring only compliant and trusted devices can connect to network resources.

Network security protections

❑ Traffic Analysis and Monitoring

- **Intrusion Detection Systems (IDS)** monitor network traffic for suspicious activities and known attack patterns, alerting administrators to potential threats.
- **Intrusion Prevention Systems (IPS)** go further by actively blocking detected threats in real-time.
- **Network segmentation** divides networks into smaller, isolated segments to limit the spread of attacks and control access to sensitive resources.

Network security protections

☐ Data Protection

- **Virtual Private Networks (VPNs)** create encrypted tunnels for secure remote access and site-to-site connections, protecting data in transit over untrusted networks.
- **Data Loss Prevention (DLP)** systems monitor and control data movement, preventing unauthorized transmission of sensitive information outside the organization.

Network security protections

❑ Advanced Threat Protection

- **Network sandboxing** isolates suspicious files and programs in controlled environments to analyze their behavior without risking the production network.
- **Behavioral analytics** use machine learning to establish baseline network behavior and identify anomalies that might indicate advanced persistent threats or insider attacks.

Summary

- ❑ Network Security Fundamentals
- ❑ The OSI Model
- ❑ Key Security Protocols
- ❑ Network Security Protections



Thank You

