# 1. Introduction

### Overview of the Course

This course is designed to introduce you to the principles of computer networking and network security. These are crucial for building, maintaining, and securing modern digital systems.

- **Career Opportunities:** These skills are fundamental for roles in IT support, network administration, cybersecurity analysis, and more.
- **Relevance Across Industries:** Networking knowledge is essential for industries ranging from healthcare to e-commerce and finance.

### Importance of Computer Networks and Network Security

- **Dependence on Networks:** Businesses use networks for data sharing, communication, and operational workflows.
- **Risks:** Networks are prime targets for cyber threats such as hacking, data breaches, and ransomware attacks.
- **Benefits of Security:** Network security prevents unauthorized access, protects sensitive data, and ensures business continuity.

## 2. Fundamentals of Computer Networks

### What is a Network?

A computer network links devices (computers, servers, IoT devices) to share resources like data, printers, and the internet.

- **Types of Networks:**
    - **LAN (Local Area Network):** Limited to a small area, such as a building or office.
    - **WAN (Wide Area Network):** Covers large areas, often connecting multiple LANs (e.g., the internet).
    - **MAN (Metropolitan Area Network):** Larger than LAN, smaller than WAN, typically covers a city.
    - **PAN (Personal Area Network):** Connects personal devices like smartphones, laptops, and wearables.

### Reference Models: OSI Model and Its 7 Layers

The **OSI Model** is a conceptual framework for understanding how data moves through a network:

1. **Physical Layer (L1):**
    - Handles raw data transmission over physical mediums like cables and radio signals.

- Includes hardware like hubs, repeaters, and network interface cards (NICs).

2. **Data Link Layer (L2):**
   - Manages node-to-node data transfer and error detection.
   - Protocols: Ethernet, Wi-Fi.
3. **Network Layer (L3):**
   - Handles routing, IP addressing, and forwarding of data packets.
   - Protocols: IPv4, IPv6.
4. **Transport Layer (L4):**
   - Ensures reliable data delivery through error-checking and retransmission.
   - Protocols: TCP (reliable) and UDP (fast but less reliable).
5. **Session Layer (L5):**
   - Establishes and manages communication sessions between devices.
   - Example: Video conferencing apps.
6. **Presentation Layer (L6):**
   - Formats data for application-level processing (e.g., encryption, compression).
7. **Application Layer (L7):**
   - Interface for end-user applications to access network services (e.g., web browsers using HTTP).

## 3. Core Networking Concepts

### Routing and Switching Basics

- **Routing:**
  - Determines the best path for data packets to travel between devices across different networks.
  - Routers operate at the Network Layer (L3) to connect LANs to WANs.
- **Switching:**
  - Connects devices within the same network, directing data to specific devices.
  - Switches operate at the Data Link Layer (L2).

**IP Addressing: IPv4 and IPv6**

- **IPv4:**
    - 32-bit addressing scheme with 4 billion unique addresses.
    - Example: 192.168.1.1.
- **IPv6:**
    - 128-bit addressing scheme with trillions of unique addresses to accommodate modern devices.
    - Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

**Introduction to TCP and UDP**

- **TCP (Transmission Control Protocol):**
    - Ensures reliable data transmission with error correction and acknowledgment.
    - Used for emails, file transfers, and web browsing.
- **UDP (User Datagram Protocol):**
    - Faster but does not guarantee delivery or order.
    - Ideal for real-time applications like streaming and gaming.

## 4. Application Layer Protocols

**Overview of Common Protocols**

- **HTTP (Hypertext Transfer Protocol):**
    - Used for accessing web pages.
    - Operates over port 80 or 443 (for HTTPS with security).
- **FTP (File Transfer Protocol):**
    - Transfers files between systems.
    - Operates over ports 20 and 21.
- **SMTP (Simple Mail Transfer Protocol):**
    - Sends emails from clients to servers.
    - Operates over port 25.
- **DNS (Domain Name System):**
    - Resolves human-readable domain names into machine-readable IP addresses.

## 5. Overview of Network Security

### Cybersecurity and Its Importance

Cybersecurity protects digital systems and data from attacks, ensuring:

- **Confidentiality:** Only authorized users can access sensitive information.
- **Integrity:** Data is protected from unauthorized modification.
- **Availability:** Systems and data remain accessible when needed.

### What is Network Security?

Network security involves tools and policies to protect data during transmission and storage, preventing unauthorized access.

### Types of Network Security

- **Firewalls:** Block unauthorized traffic.
- **Intrusion Detection Systems (IDS):** Identify potential threats.
- **Encryption:** Converts data into unreadable formats without a key.

## 6. Understanding Network Attacks

### Types of Cyber Attacks

- **Phishing:** Fraudulent attempts to steal sensitive information.
- **Malware:** Harmful software like viruses, worms, and trojans.
- **Denial-of-Service (DoS):** Overloads systems to make them unavailable.
- **Ransomware:** Encrypts files, demanding payment for decryption.

### Network Vulnerabilities

Weaknesses that attackers exploit include:

- Poorly configured systems.
- Lack of security updates.
- Weak passwords.

## 7. Ensuring Network Security

### Tools and Techniques for Network Security

- **Firewalls:** Block malicious traffic.
- **VPNs (Virtual Private Networks):** Provide secure remote access.
- **Antivirus Software:** Detects and removes malware.
- **Encryption:** Protects data integrity and confidentiality.

### Network Security Protocols

- **SSL/TLS:** Secure communications for websites and apps.
- **IPsec:** Secures data during network transmission.

### Best Practices for Businesses

- Regularly update systems and software.
- Educate employees on recognizing cyber threats.
- Use multi-factor authentication for secure access.

## 8. Future Trends in Networking and Security

### Mobile and Wireless Networks

- Growth in 5G and Wi-Fi 6 offers faster speeds and better connectivity but raises security concerns.
- Ensuring secure connections for IoT and mobile devices is a top priority.

### Emerging Technologies in Cybersecurity

- **AI and Machine Learning:** Enhance threat detection by analyzing patterns.
- **Quantum Cryptography:** Provides next-level encryption to counteract quantum computing threats.
- **Zero-Trust Architecture:** Assumes no device or user is inherently trusted.

# Certification of Completion