Chapter 3: Computer Networks

Introduction to Networks

1. Basics of Computer Networks

Definition:

A computer network is a set of interconnected devices that can communicate with each other. Networks can be local, connecting devices within a limited area, or wide, connecting devices across larger geographical distances.

Types of Networks:

LAN (Local Area Network), WAN (Wide Area Network), and MAN (Metropolitan Area Network) are types of networks that differ in terms of their geographical scope and the number of interconnected devices. Here's a brief overview of the differences:

a. LAN (Local Area Network):

Geographical Scope: LANs cover a relatively small geographic area, such as a single building, a campus, or a group of nearby buildings.

Typical Size: LANs typically serve a limited number of users and devices, often within the range of a few kilometers.

Connection Medium: LANs are commonly connected using Ethernet cables or wireless technologies like Wi-Fi.

Examples: Home networks, office networks, and school networks are common examples of LANs.

b. WAN (Wide Area Network):

Geographical Scope: WANs cover a broader geographic area, often spanning cities, countries, or even continents.

Typical Size: WANs can connect LANs over long distances, allowing communication between devices that are far apart.

Connection Medium: WANs use a variety of technologies, including dedicated leased lines, satellite links, and the internet.

Examples: The internet itself is a massive WAN. Private corporate networks connecting offices across different cities or countries are also WANs.

c. MAN (Metropolitan Area Network):

Geographical Scope: MANs fall between LANs and WANs in terms of geographic coverage. They cover a larger area than a single LAN but are smaller than a WAN.

Typical Size: MANs are designed to connect networks within a specific metropolitan area, such as a city or a large campus.

Connection Medium: MANs may use technologies like fiber optics, Ethernet, or wireless connections.

Examples: MANs are often deployed in urban environments to connect multiple buildings within a city, facilitating high-speed data transfer over shorter distances.

2. Network Components

Nodes and Links:

Nodes are individual devices in a network, and links are the connections between them. Together, they form the basic building blocks of a network.

Switches and Routers:

Switches facilitate communication within a local network, while routers manage data transfer between different networks.

Protocols:

Network protocols define the rules and conventions for communication between devices. Common protocols include TCP/IP (Transmission Control Protocol/Internet Protocol).

Internet Technologies

1. Evolution of the Internet

Origins and Development:

The internet originated from ARPANET in the 1960s and has since evolved into a global network connecting billions of devices.

Key Milestones:

Significant milestones in internet development include the creation of the World Wide Web (WWW) and the introduction of web browsers.

2. Internet Services and Applications

Email and Communication:

Email services and instant messaging platforms are integral parts of internet communication.

Web Services:

Websites, search engines, and online applications provide various services on the internet.

Social Media:

Social media platforms enable users to connect, share content, and engage with others globally.

Network Security:

1. Importance of Network Security

Definition and Scope:

Network security involves implementing measures to protect a network from unauthorized access, data breaches, and cyber threats.

Goals of Network Security:

The primary goals include confidentiality, integrity, and availability of data within the network.

2. Common Threats and Vulnerabilities

Malware and Viruses:

Malicious software (malware) and viruses pose threats to network security by compromising data and system functionality.

Phishing and Social Engineering:

Techniques like phishing and social engineering exploit human vulnerabilities to gain unauthorized access.

Denial of Service (DoS) Attacks:

DoS attacks aim to disrupt network services by overwhelming the system with excessive traffic.

3. Security Measures and Best Practices

Firewalls and Encryption:

Firewalls monitor and control network traffic, while encryption secures data during transmission.

User Authentication:

Strong authentication methods, such as two-factor authentication, enhance network security.

Regular Updates and Patch Management:

Keeping software and systems updated protects against known vulnerabilities.