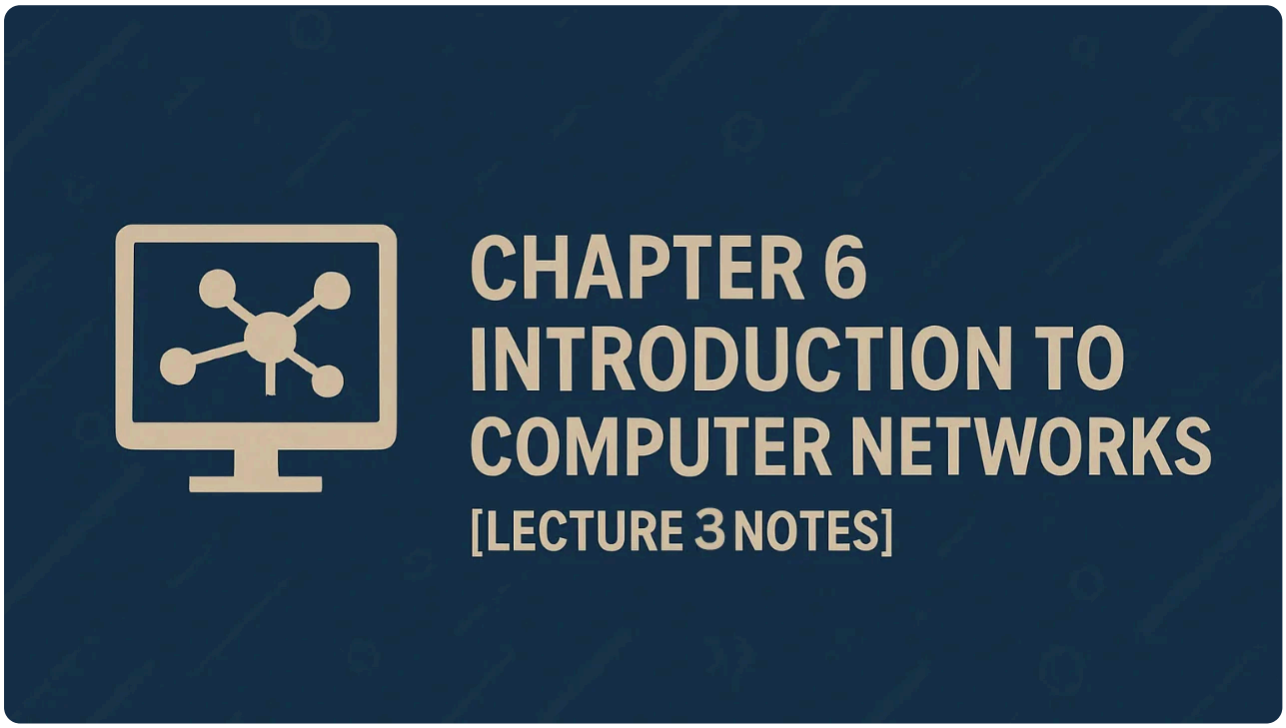
IP Addresses, Network Services, Security, Threats, Types, Applications, Standard Protocols

Posted in **9 Computer Science**



These lecture notes are prepared by **Salman Ahmad**, who is both a **teacher** and a **web developer**. The purpose of this material is to make the topic clear and useful for students of Class 9 Computer Science.

Table of Contents

> TCP/IP Communication

IPv4 and IPv6

Internet Protocol (IP) addresses are unique numbers assigned to devices connected to the Internet. They help identify devices and allow them to communicate with each other. There are two main versions of IP addresses:

- IPv4
- IPv6

Internet Protocol Version 4 (IPv4)

IPv4 is the fourth version of the Internet Protocol and is widely used on the Internet.
It uses a **32-bit address system**, which allows about **4.3 billion unique addresses**. It is represented in the decimal number system.

Example IPv4 Address:

192.168.1.1

192.168.1.2

192.168.1.3

Internet Protocol Version 6 (IPv6)

IPv6 is the newer version of the Internet Protocol designed to replace IPv4.
It uses a **128-bit address system**, which provides an extremely large number of unique addresses.
IPv6 addresses are written in eight groups of hexadecimal numbers separated by colons.

Example IPv6 Address:

2001:0db8:0000:130F:0000:0900:876A:130B

DNS (Domain Name System)

DNS (Domain Name System) converts domain names into IP addresses so users can easily access websites without typing long numbers.

Example:

When a user types **www.google.com**, DNS finds its IP address so the browser can connect to the website.

Dynamic Host Configuration Protocol (DHCP)

DHCP automatically assigns IP addresses to devices connected to a network.

Example:

- When a phone connects to Wi-Fi, it receives an IP address automatically.

Network Security

Network security includes methods used to protect networks and data from unauthorized access or attacks.

Importance of Network Security

Network security is important because it helps:

- **Data Protection:** Keeps sensitive information safe from unauthorized access, loss, or damage.
- **Preventing Attacks:** Helps defend the network against hackers, viruses, and other malicious software.
- **Maintaining Privacy:** Protects personal and confidential information from being exposed or misused.
- **Ensuring Availability:** Ensures that network services and resources remain accessible to authorized users whenever they are needed.

Key Concepts in Network Security

Firewalls

A firewall is a security system that monitors and controls incoming and outgoing network traffic based on security rules. It helps prevent unauthorized users from accessing a network.

Encryption

Encryption is the process of converting plain text into an unreadable format so that unauthorized users cannot read it. The encrypted text is called **ciphertext**.

Example:

hello → encrypted → 123ab → decrypted → hello

Decryption

Decryption is the process of converting encrypted data back into plain text using the correct key.

Example:

hello → encrypted → 123ab → decrypted → hello

Password

A password is a secret combination of characters (letters, numbers, or symbols) used to verify a user's identity and protect access to a system or account.

Authentication

Authentication is the process of verifying the identity of a user before allowing access to a system or network.

Common Threats to Network Security

- **Malware:** Bad software like viruses or ransomware that can damage or steal data.
  Example: Ransomware locks your files and asks for money.
- **Phishing:** Tricks people into giving passwords or personal information using fake emails or websites.
  Example: A fake bank email asking for login details.
- **Denial of Service (DoS) Attacks:** Sends too much traffic to a network to make it stop working.
  Example: A website crashes due to fake traffic.
- **Man-in-the-Middle (MitM) Attacks:** Someone secretly intercepts communication between two users.
  Example: A hacker sitting on a public Wi-Fi network intercepts messages between your phone and a bank website, capturing your username and password.

Types of Networks

Networks are grouped based on size, range, and purpose.

1. Personal Area Network (PAN)

A small network for personal devices within a short range.

Example:

Connecting a smartphone to wireless headphones via Bluetooth.

2. Local Area Network (LAN)

Connects computers and devices in a small area like a home, school, or office.

Example:

All computers in a school lab connected to the same network.

3. Metropolitan Area Network (MAN)

Covers a city or large campus and connects multiple LANs.

Example:

A network connecting all branches of a university within a city.

4. Wide Area Network (WAN)

Covers large geographical areas and connects multiple networks.

Example:

The Internet or company networks connecting offices worldwide.

5. Campus Area Network (CAN)

Connects multiple LANs within a limited area such as a university campus.

Example:

A network linking all departments and buildings in a university.

Uses of Networks

1. Business

Helps employees communicate, share resources, and manage data.

Example:

Companies using intranets to share files internally.

2. Education

Supports online classes and access to learning resources.

Example:

Universities using platforms like Moodle or Blackboard.

3. Healthcare

Healthcare networks help share patient information and provide online medical services.

Example:

Hospitals using Electronic Health Record (EHR) systems.

Standard Protocols in TCP/IP Communication

Introduction to TCP/IP

TCP/IP (Transmission Control Protocol / Internet Protocol) is a set of communication rules used on the Internet.

It allows computers and devices to send and receive data over networks.

Key Protocols

Transmission Control Protocol (TCP)

TCP ensures that data is delivered correctly and completely. If data is lost, TCP resends it.

Example:

Used when downloading files or loading web pages.

Internet Protocol (IP)

IP assigns addresses to devices and sends data to the correct destination.

Example:

Sending data from your computer to a website server.

User Datagram Protocol (UDP)

UDP sends data faster than TCP but does not guarantee delivery.

Example:

Used in video streaming, online gaming, and live broadcasts.

Antivirus Software

A program that detects, blocks, and removes viruses and other harmful software from your computer.

Example:

Avast, Norton, or McAfee scanning your computer to stop malware from damaging files.

Previous Lecture # 1

15 Multiple Choice Questions (MCQs) on Network Topologies and OSI Model

1. What does an IP address do?

a. Speeds up the Internet
b. Identifies devices on a network
c. Encrypts data
d. Monitors network traffic

> **Answer: b. Identifies devices on a network**

2. How many unique addresses does IPv4 provide?

a. About 4.3 billion
b. About 100 million
c. About 1 trillion
d. About 128 million

> **Answer: a. About 4.3 billion**