ZNOTES.ORG

UPDATED TO 2023-2025 SYLLABUS

CAIE AS LEVEL

COMPUTER SCIENCE

SUMMARIZED NOTES ON THE THEORY SYLLABUS

1. Communication

1.1. Networks, including the Internet

LAN	WAN
A network that connects devices within a small geographical area, often within the same building.	A network that connects devices within a larger geographical area, such as a city, country, or globally.
Only private ownership.	Private or public ownership.
Transmission medium: Twisted Pair Cables , Coaxial Cables or Wi-Fi.	Transmission medium: PSTN or Satlink.
Higher data transfer rate.	Lower data transfer rate.
Less congestion.	Higher congestion.

- **Networking devices**: Interconnected devices that enable fast data transmission within a network.
- **Networking benefits**:
  - **File sharing**: Easily share data between different interconnected devices.
  - **Resource sharing**: Use network-connected output devices like printers or share software within the network.
  - **Higher storage**: Files can be stored in network-connected storage mediums.
- **Client-Server Model**
  - **Server-based network**: A dedicated server provides applications (administration of users, security, and resources) for the client computer to utilize.
  - **Client-server Applications**:
    - **Printer**: Manages print jobs from client computers.
    - **File Sharing**: Clients access software and user data files stored on the server.
    - **Proxy server**.
    - **Email server**: For sending, receiving, and storing emails.
    - **Database server**: Manages DBMS.
    - **Domain controller server**:
      - Manages user accounts (IDs & passwords).
      - The client sends a login request to the server, which processes and grants the request if the user ID & password are recognized.

Thin Clients	Thick Clients
A client that solely runs on the resources provided by the server and has no local storage.	An independent client that does not require the server to run.
Only provides input and receives output; processing is done by the server.	Thick client processes most of the application locally.
Smaller purchase cost: expensive, demanding hardware is not required.	Can function even if no server is connected (works offline).
Improved security: Cannot run unauthorized, harmful software.	No lag related to network problems.

- **Thin Clients vs. Thick Clients**
- **Peer-to-Peer network model (P2P)**
  - **Definition**: A decentralized network where each connected computer stores data and operates independently as a 'peer', acting as both a client and a server.
  - **Applications**: Internet and Ad hoc networks.

Client-Server	Peer-to-Peer
Centralized backup.	Lesser initial setup cost.
Files & resources centralized in server: Prevents illegal resource usage.	Lesser network traffic: Each peer can simultaneously receive data from different sources.
Improved security: Files are stored on a central server, which would be regularly scanned for malware.	It can work even if a device goes down, but the client-server model can't work if the server goes down.

- **Client-Server vs. Peer-to-Peer models**
- Network Topologies
  - **Bus**
    - A single line (bus) connects all devices with terminators at each end.
    - Other computers can read data being sent between any two computers.
    - Unsuitable for heavy traffic due to frequent collisions.
  - **Star**
    - Consists of a central server (switch) with all other computers connected via dedicated connections.
    - The server can send packets to different devices simultaneously and bidirectionally.
    - No collisions are possible.
  - **Mesh**
    - Every device (node) is directly interconnected with each of the other devices (nodes).
    - Commonly used for wireless networks, such as the Internet, through the mesh connection of routers.
  - **Hybrid**
    - A combination of two or more topologies.
    - Example: A connection between two or more LANs of different topologies.

	Benefits	Drawbacks
Copper Cable	Less expensive and easier to install. Flexible. Easier to make terminations.	Doesn't perform well with small charges. Affected by electromagnetism.
Fiber-Optic Cables	Greater bandwidth, improved security, lightweight, easy to install, and less signal boosting are required; used in long-distance communications.	Needs expensive optical transmitters and receivers.

- **Wired Networks**
  - Use copper (twisted-pair cable or coaxial cable) or fiber-optic cables.
  - Cables are connected to an Ethernet port on the network router.

	Benefits	Drawbacks
Radio waves	Can travel over large distances with a wide range of wavelengths. Relatively inexpensive. Used for TV signals and mobile phone communications.	Low frequency means less data can be transmitted at one time. Affected by interference from radio stations with similar frequencies.
Microwaves	Larger bandwidth allows more data transfer.	Expensive to build emitting towers. Physical obstacles can interfere with signals.
Satellites	Cost-effective for long-distance communication, used in satellite phones and radio broadcasts.	Susceptible to interference. Expensive setup.

- **Wireless Networks**
  - Use radio waves (including WiFi), microwaves, and satellites to connect devices to networks without cables.

Real-time	On-demand
The event is captured live via a video camera that is connected to a computer.	Existing digital files are converted to encoded bit-streaming format for broadcasting on the internet by uploading to a dedicated server.
Video signal converted to an encoded streaming video signal.	A link for encoded video is placed on the website, and the user clicks on the link to view encoded streaming video.
Encoded video signal uploaded from computer to a dedicated streaming server via cables or high-speed wireless internet connection.	The data is streamed to a buffer in the user's computer, and the buffer stops the video from being paused as the bits are streamed.
The server then sends live images to all users requesting them as a real-time video.	As the buffer is emptied, it's filled again, thus providing continuous viewing.
It cannot be paused, fast-forwarded, etc.	Can be paused, fast-forwarded, etc.

- **Ethernet**
  - The most common wired medium for data transmission in LANs or WANs.
  - Typically used in bus topology; data collisions are managed by the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) method.
  - **CSMA/CD Process:**
    - Device checks if the channel is busy before transmitting.
    - If busy, the device waits a random time before retrying.
    - During transmission, the device listens for other transmissions.
    - If a collision occurs, transmission is aborted, and both devices wait random times before retrying.
- **Bit Streaming**
  - Sequence of digital signals (bits) transferred over a communication path at high speeds, requiring a fast broadband connection and buffers.
  - **Bit Streaming Types:**
    - **Real-time:** Live events captured and transmitted directly.
    - **On-demand:** Pre-existing files are converted and streamed as requested.
  - **Importance of High Broadband Speed/Bit-Rate**
    - The user has to download and display bits at the same time.
    - Higher quality media requires faster speeds due to larger data frames as well.
    - Real-time streaming needs higher speeds due to simultaneous data requests coming from multiple different users.

- **Cloud Computing**
  - On-demand provision of computing services over the internet, including infrastructure, and platforms.
    - Infrastructure: Storage capacity and higher processing power.
    - Platform: Software, testing & debugging resources.

Public cloud vs. Private cloud

Public cloud	Private Cloud
Access provided by third-party service providers, shared among multiple users.	Owned and maintained by a single organization, providing exclusive access.
Managed by cloud service providers using large server farms.	Can be managed internally by the organization itself, or outsourced.

Benefits	Drawback
Less technical knowledge required, easy to implement.	Cannot access the resources/ data stored on the cloud if there are bandwidth issues.
Flexibility to scale with organization's growth mindset.	Poor data privacy, since there may be data leakage in the multi-tenant architecture (public clouds).

- **World Wide Web (WWW):**
  - **Description:** Collection of web pages stored on websites.
  - **Function:** Protocols are used to transmit data across the WWW.
- **Internet (Interconnected Network):**
  - **Description:** Massive, open network of networks.
  - **Protocol:** Uses TCP/IP protocol, which uses IP addresses to identify devices connected to the internet.
  - **Access:** Provided by Internet Service Provider.
  - **Communication Methods:** Wired, radio, and satellite.
- **Router in a Network:**
  - **Function:** Connects two networks together which operate under the same protocols (for example, IP).
  - **Connections:** Allows internal connections between LANs or external connection from the main LAN to a WAN.
  - **Additional Roles:** Acts as a gateway and firewall.
  - **Setup:** Usually attached to a server or switch in a LAN.
  - **IP Address Translation:** Translates private IP addresses to public IP addresses and vice versa.

- **LAN-Supporting Hardware:**
  - **Switch:**
    - Connected to all devices in a LAN.
    - Can simultaneously broadcast information to all devices.
  - **Server:**
    - Device/software that provides specific functions for computers in the network.
  - **Network Interface Card (NIC):**
    - Provides each device (end-system) in the wired LAN with a unique MAC address to uniquely identify it on the network.
    - Allows each device to connect to the network.
  - **Wireless Network Interface Card (WNIC):**
    - Provides each end-system of a wireless (WiFi) LAN a unique network address to identify it.
  - **Wireless Access Points (WAP):**
    - Allows devices to connect to the LAN via WiFi instead of using a cable.
    - Usually built into the router.
  - **Cables:**
    - A wired transmission medium that allows communication in wired networks.
  - **Bridge:**
    - Connects two LANs which work using the same protocol, which can be two segments of the same network.
    - Stores network addresses for all devices (end-systems) between the two networks.
    - Looks for the receiving device before it sends the message.
  - **Repeater:**
    - Connects two cables.
    - Regenerates the sent data signal over the same network before the signal weakens (attenuation) to prevent it from being corrupted.

- Internet-Supporting Hardware:
  - **Modems:**
    - Allows a device to connect to the Internet via a telephone line.
    - **Function:** A transmitter uses a modem to convert digital signals (from the transmitting device) to analogue signals sent down the telephone line. A receiver uses a modem on the other end to convert the analogue signals to digital signals so the receiving device can understand the data.
  - **PSTN (Public Switched Telephone Network):**
    - Refers to all telephone networks.
    - **Channel:** Used between two endpoints for the call duration via circuit switching.
    - **Resilience:** Lines are active even during a power outage.
    - **Communication:** Bi-directional.
  - **Dedicated Lines:**
    - Telecommunication path between endpoints.
    - Not shared with multiple users; it's bought/ leased.
    - **Function:** Able to host websites as well as carry phone calls. Allows continuous, uninterrupted access to the Web.
  - **Cell Phone Network:**
    - Wireless networks spread over land areas divided into (hexagonal) cells.
    - **Base Stations:** Each cell is served by at least one base station (transceiver), which uses a different frequency range compared to adjacent cells to transmit data.
    - **Capacity:** Larger capacity is possible since the same frequencies can be used in non-adjacent cells.
    - **Transmission:** Radio waves are usually used for transmission. Can be broadcast in all directions over a wide area.
    - **Portable Transceivers:** Devices like mobile phones can communicate and access the internet via base stations.

IPv4	IPv6
32-bit address, split into 4 blocks by "."	The 128-bit address is divided into eight 16-bit blocks by ":"
Each block could have a value between 0 and 255 (00 to FF in hex).	Each block can have 4 hex values ranging from 0000 to FFFF.
For example, 255.0.1.255.	IPv6 can be shortened by removing at least (≥) 2 blocks containing only zeroes. For example: "2001:0db8:85a3:0000:0000:8a2e:0070:7334" can be shortened to "2001:0db8:85a3::8a2e:0070:7334"

- **IPv4 vs. IPv6**
- **IPv4 Functionality:**
  - **IP Address Structure:**
    - **Network Identifier (netID):** Identifies the network to which the host (device) is connected.
    - **Host Identifier (hostID):** Identifies the host within the network.
    - **Classful Addressing:** Used for IPv4, where different bit lengths for identification impose restrictions on available addresses.
  - **Subnetting:**
    - **Definition:** The practice of dividing a network into two or more networks.
    - **Structure:** IP addresses are broken down into three parts by not changing the netID but partitioning the host ID into a subnet ID and host ID.
      - **Subnet ID:** These bits are used to identify each subnet within the network.
      - **Subnet Masks:** Numbers that hide (mask) the netID of a system's IP address and leave only the host part as the machine identifier, allowing data to be routed within the subnet to the appropriate host.

- **Public and Private IP Addresses:**
  - **Public IP:**
    - Provided by the ISP.
    - Unique and can be accessed across the internet.
  - **Private IP:**
    - Issued by the LAN's router.
    - Unique within the LAN and can only be accessed within the LAN.
    - **NAT (Network Address Translation):** Required for private IP addresses to access the internet directly.
    - **Security:** Private IPs are more secure than public IPs since they are not directly accessible on the Internet and are hidden by NAT.
    - **Address Range:** The range of IP addresses used for private IP addressing can never be assigned to public IP addresses.

Static	Dynamic
IP address never changes.	The IP address will change at regular periods.
Static IP addresses are valid when websites need to remember a device for a long time, e.g VPNs whitelisting.	Dynamic IP address is relatively more secure, hence used where data privacy is quite important.
Faster upload/download speeds.	Maintaining the cost of the dynamic IP address is a lesser.

- **Static vs. Dynamic IP addresses**

- **URL (Uniform Resource Locator)**
- Unique reference address for the exact location of an internet resource on the WWW
- **Protocol:** Enables the browser to know what protocol is used to access information in the domain.
- **Host-name:** The domain name.
- **Location of Server:** The path indicating the server location.
- **Domain Name Service (DNS)**
  - **Definition:** A naming system used for computers or resources having an internet connection.
  - **Structure:** Consists of a hierarchy of DNS servers which have a URL database and their corresponding IP addresses.

CAIE AS Level

Computer Science