

## 2. Communication

### 2.1 Networks

- **Purposes and benefits** of networking computers and devices
  - **Resource sharing**: devices, such as printers, can be **shared** (thus reducing cost)
  - **Data Transfer and Communication**: users can **share files and data**, and **communicate** with each other instantly
  - **Centralized Data Management**: data and files can be **backed up centrally** at the end of each day
  - **Scalability and Flexibility**: networks provide the flexibility to add or remove devices as needed

### LANs and WANs

	Local Area Networks (LANs)	Wide Area Networks (WANs)
<b>Scope</b>	Typically spans a small area like a <b>building or campus</b>	Covers a broad area, potentially <b>worldwide</b>
<b>Speed and Latency</b>	<b>High</b> data transfer speeds, <b>Low</b> latencies	<b>Slow</b> data transfer speed, <b>High</b> latencies due to large distances
<b>Structure</b>	A number of computers and devices connected to <b>hubs</b> and <b>switches</b> , and one of the hubs or switches is connected to a <b>router</b> and/or a <b>modem</b> to connect the LAN to a WAN	A number of LANs joined together using a router or a modem
<b>Usage</b>	Sharing resources such as printers, files, and software within a small geographical area	Suitable for connecting devices across cities, countries; commonly used by businesses and governments for large-scale communications
<b>Security</b>	Easier to manage and secure due to limited size	More complex to manage and secure, often requires specialized

### Networking Models

- **Client-Server**: networks that use separate dedicated servers and specific client workstations; all clients are connected to the dedicated servers
  - **Client**: a device that requests information or services from a server
  - **Server**: a computer that provides data, services, or resources to clients
  - **Benefits**:
    - **Centralized Management**: Easier to manage data, users, and security
      - when the user logs in to the server, they only have access to the data that they are permitted to view by the administrator
    - **Scalability**: Can handle an increasing number of clients by upgrading server capabilities, and it is easy to add a client device to the network
    - **Efficiency and Specialization**: Servers can be optimized for specific tasks, providing better performance
  - **Drawbacks**:
    - **Cost**: Setting up and maintaining servers can be expensive
    - **Single Point of Failure**: If the server goes down, clients lose access to important resources
    - **Bottleneck**: Client-server networks can become bottlenecked if there are several client requests at the same time
- **Peer-to-Peer**: networks in which each node can share its files with **all the other nodes**; each node has its own data and there is no central server
  - **Benefits**
    - **Cost-Effective**: No need for expensive server hardware

- **Data Perseverance:** Data can be stored on multiple peers, reducing the risk of data loss
- **Decentralization:** Eliminate single points of failure and bottlenecks
- *Drawbacks:*
  - **Security Risks:** More vulnerable to cyber threats as each peer has the data and is exposed; there are no real authentication procedures
  - **Inconsistent Performance:** The performance depends on the capabilities and availability of individual peers
  - **Complex Management:** Need to manage resources and security for every peer in the network

## Thin-Clients and Thick-Clients

	Thin-Client	Thick-Client
<b>Definition</b>	A <b>minimal and low-performance</b> computer that relies on a server for processing and storage; devices that <b>need internet</b> to do its work	Devices that can run applications and perform tasks independently, even <b>without a network connection</b>
<b>Processing and Storage</b>	Depends on the server for processing and storage	Can handle them <b>locally</b>
<b>Network Dependency</b>	Relies on a good, stable, and fast network connection for it to work	More tolerant of a slow network connection
<b>Cost</b>	Generally cheaper and require less maintenance	More expensive to set up and maintain
<b>Usages</b>	Idealized for <b>centralized</b> environments with <b>consistent network connectivity</b>	Requiring <b>robust computing power at the user end</b>

## Network Topologies

- **Bus Topology:** All devices are connected to a **central cable**, the bus
  - *Packet Transmission:* Data packets travel along the bus and are received by all devices, but **only the intended recipient** processes them
  - *Use Case Justification:* **Small businesses with light traffic occurring**
    - Cost-effective for small networks
    - Performance would deteriorate with a high traffic load; the whole network fails if the cable is broken
- **Star Topology:** Each device is connected to a **central hub or switch**
  - *Packet Transmission:* Data packets are sent to a central hub/switch, which then forwards them to the appropriate device
  - *Use Case Justification:*
    - Highly reliable - if one connection fails, others remain unaffected
    - Ideal for networks where **frequent addition or removal of devices occurs**
      - it is easy to add and remove devices
    - Ideal for networks that have a high traffic load
      - data collisions are avoided in star networks
- **Mesh Topology:** Each device is connected to **every other device** in the network; a type of peer-to-peer network
  - *Packet Transmission*
    - **Routing:** data is directed to its destination by the shortest route
    - **Flooding:** data is sent to all the nodes in the network
  - *Use Case Justification:*
    - Provides high redundancy and reliability
    - Suitable for networks where communication availability is critical
      - used in monitoring and controls to supervise each component in the network
    - Often used in wireless networks (like Wi-Fi) and **WANs**
- **Hybrid Topology:** Combination of two or more different topologies

- **Packet Transmission:** Depends on the specific topologies involved; generally, it follows the rules of the individual topologies within the hybrid network
- **Use Case Justification:**
  - Offers flexibility and scalability
  - Tailored to specific needs and constraints of larger or complex networks
  - Ideal for organizations with diverse and evolving networking requirements

## Cloud Computing

- The delivery of computing services over the internet, including storage, processing power, and software application
- **Advantages**
  - **Accessibility:** Files stored on the cloud can be accessed at **any time** from **any device anywhere** in the world provided **internet access is available**
    - No need for a customer/client to carry an **external storage device** with them, or use the same computer to store and retrieve information
  - **Back-up:** Remote back-up of data against data loss and disaster recovery
  - **Flexibility:** Easily scales resources to meet changing demands
  - **Cost-efficiency:** Reduces the need for physical hardware and associated maintenance costs
- **Disadvantages**
  - **Dependence on Network Connectivity:** Problems accessing the cloud files if the internet situation is inferior
  - **Data Transfer Costs:** Substantial costs associated with transferring large volumes of data to and from the cloud; expensive to pay the ISP/cloud providers for high download/upload data limits
  - **Failure of 3rd-Party:** Potential failure of the cloud company is possible - posing a risk of loss of all backup data

## Public and Private Clouds

	Public Clouds	Private Clouds
<b>Definition</b>	Services offered over the public internet and available to everyone	Infrastructure operated solely for a <b>single</b> organization, whether managed internally or by a third-party
<b>Use Cases</b>	Suitable for businesses needing <b>high scalability without the cost of hardware and software maintenance</b>	Ideal for organizations with <b>high data security, privacy, and regulatory compliance needs</b>

## Wireless and Wired Networks

Feature	Wireless Networks	Wired Networks
<b>Medium</b>	Uses wireless signals (radio waves, microwaves, satellites)	Utilizes physical cables
<b>Interference</b>	Susceptible to interference from physical barriers and signals	Less affected by external interference
<b>Security</b>	Higher risk of unauthorized access	More secure, with reduced risk of interception
<b>Flexibility</b>	High mobility; networks can be easily expanded	Limited mobility; expansion requires additional cabling
<b>Reliability</b>	Potential for fluctuating connectivity	Consistently high data transfer speeds and stability
<b>Installation</b>	Easier and less costly to set up and modify	Installation is more complex and costly
<b>Range</b>	Typically limited; affected by distance from signal source	Defined by cable length; suitable for long distances

Feature	Wireless Networks	Wired Networks
Speed	Varies; generally lower than wired networks	Typically offers higher and more consistent speeds
Cost	Generally lower initial costs	Higher initial costs due to cabling and installation

## Wired Mediums

	Copper Cable	Fiber-Optic Cable
Transmission	Electrical signals	Light signals
Bandwidth	Lower than fiber-optic	Higher, supports greater data transmission
Interference	Susceptible to electromagnetic interference	Minimal interference, more secure
Distance	Effective over shorter distances	Suitable for long distances without loss
Cost	Generally cheaper	More expensive due to materials and handling

## Wireless Mediums

- **Radio Waves** (including Wi-Fi)
  - used for **short to moderated** distances
  - **susceptible** to interference from **other devices and physical obstructions**
  - ideal for **WANs**, like Wi-Fis
- **Microwaves**
  - used for **point-to-point** communication
  - requires **line-of-sight** between relay stations
  - affected by **environmental conditions**
  - ideal for **telecommunication networks**
- **\*\*Satellites**
  - used for **global coverage**
  - **high latency** due to the long distance
  - affected by **weather** and costly to set up and maintain
  - ideal for **remote and marine communications**

## LAN Hardware

Hardware Component	Function	Details
Switch	Checks the data packet received, works out its destination MAC addresses and sends the data to the appropriate computers only	A secure and efficient way of distributing data; less data collisions
Server	Provides network services and resources to client devices, for example, helps store data and files centrally	Centralizes data management and resource sharing
Network Interface Card (NIC)	Enables a computer to connect to a wired network	Contains the MAC address of the device generated at the manufacturing stage
Wireless NIC (WNIC)	Allows a device to connect to a wireless network	<b>Infrastructure mode</b> : requires <b>wireless access points</b> and all the data is transferred using the WAPs; <b>Ad hoc mode</b> : devices can interface with each other directly
Wireless Access Point (WAP)	Bridges wireless devices and a wired network	Expands LAN to include wireless devices
Cables	Connects network devices (copper or fiber-	Fundamental for wired connections and data

Hardware Component	Function	Details
	optic cables)	transmission
<b>Bridge</b>	Connects a LAN to another LAN that uses <b>the same protocol</b> , so that they can function as a single LAN	Useful for network segmentation and traffic management; Bridges only forward data to the destination LAN segment, reducing the traffic on segments that don't need the data
<b>Repeater</b>	Amplifies network signals to extend their transmission distance	It is <b>non-logical</b> : it will boost out all the signals that have been selected; it helps bring signals to those Wi-Fi dead zones and <b>increase the operational range</b> of the LAN

## Roles of Routers

- **Packet Forwarding**
  - sends packets to a specific destination in the network
  - decides the best path for the packet to take
- **Security**
  - includes firewall functionality to filter incoming and outgoing traffic
- **Protocol Conversion**
  - converts between Ethernet protocol or wireless protocols, connecting different networks together
- **Handling IP Address**
  - **Network Address Translation**: allows multiple devices on a private network to share a single public IP address for Internet access; conserves global addresses
  - **Creating Subnets**: organizes a larger network into smaller, manageable segments
  - assigns private IP addresses to each individual device

## Ethernet

- A wired **network protocol** that controls how data is transmitted over a LAN
- *Consists of:*
  - **Nodes**: networking devices
  - **Mediums**: wires (fiber optic cables/copper cables)
  - **Frames**: the data packets, containing unique original and destination MAC addresses
- **Ethernet Collisions**
  - occurs when two messages using the **same data channel** could be sent at the same time → it is dealt with CSMA/CD
  - **Collision Detection**: when a frame is sent it causes a **voltage change** on the Ethernet cable

## Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

1. A **workstation/node** listens to the communication channel and sends data **when the channel is free**
2. Because there is **more than one computer** connected to the same transmission medium, two workstations can start to **transmit at the same time**, **causing a collision**
3. If a collision happens, the **workstations** send a **jamming signal**, and each waits a **random** amount of time before attempting to resend

## Bit Streaming

- a **contiguous** transmission of digital bits sent over a network that requires a **high-speed data communication link**
  - usually dealing with very large files (e.g., video) → therefore **compression** and **buffers** are needed

### 1. Real-Time Bit Streaming

- Data is streamed and consumed simultaneously
  - Common in live broadcasts or conferencing
- Requires stable and fast network connections
- Sensitive to latency and buffering issues
- *Procedure:*
  1. An event is captured by camera and microphone, and is sent to a computer
  2. The video signal is encoded and uploaded to the streaming server
  3. The server sends the video to the user's device

### 2. On-Demand Bit Streaming

- Data is streamed upon request
  - Common in video-on-demand services
- Allows buffering and pre-loading of data
  - if is possible to **pause**, **rewind**, or **fast forward**
- More forgiving of variable network speeds
- *Procedure:*
  1. Digital files are encoded and uploaded to a streaming server
  2. A link to the encoded file is placed on the web server
  3. The file is downloaded when the user clicks the link

### Factors of Bit Streaming

1. **Bit Rates:** the amount of data transmitted per second in a bit stream
  - **Higher** bit rates result in **higher quality streaming** (the resolution of the videos would be better) → requires faster broadband speeds to avoid buffering
  - **Lower** bit rates lead to **low quality** but are more **accessible on slower connections**
2. **Broadband Speed:** the rate at which data is downloaded or uploaded from the internet to your device
  - **High** broadband speed results in **low latency** and allows **high bit rates**
  - **Low** broadband speed can lead to **buffering and interruptions**, reducing **streaming quality** as the number of bits downloaded to your computer is smaller at a time

## 2.2 The Internet

- **Internet:** the **infrastructure** (the physical devices)
  - a massive network of networks that allows users to access the *World Wide Web*
- **World Wide Web (WWW):** a collection of **websites and webpages** accessed using the *Internet*

### Internet Hardware

1. **Modems:** *modulator-demodulators* convert **digital signals** from a computer into **analog** signals for transmission over telephone lines, and vice versa
  - allows connection of a network to external networks (e.g. the Internet)
2. **Public Switched Telephone Network (PSTN):** network used by **traditional telephones** when making calls or when sending faxes
  - provides the infrastructure and services for public telecommunication
  - telephone lines remain active even during a power cut; they have their own power source
  - *Role in the Internet:* Initially used for dial-up internet access; still used in rural areas where the ISPs haven't developed the infrastructure for newer technologies

3. **Dedicated Lines**: **private network connections** that provide direct, continuous connectivity
  - **exclusively** used by a single customer or organization → low latency, guaranteed bandwidth, high quality of service and reliability
  - Ideal for organizations needing reliable, constant, and high-speed internet connectivity
4. **Cell Phone Network**: a type of wireless communication network that is distributed over land areas called cells
  - *Components*:
    - **Cell Towers**: send and receive signals to and from cell phones
    - **Mobile Switching Centers**: manages communications; responsible for **routing** and handling the setup, control, and termination of calls
  - *Examples*: 3G, 4G, LTE, 5G

## IP (Internet Protocol) addresses

- a **unique identifying** number assigned to every device connected to the internet
  - **Assignment**: devices on a network receive an IP address either statically (assigned manually) or dynamically (assigned by a DHCP server)
  - **Identification**: the IP allows

### Types of IP Addresses

- **IPv4**: **32-bit** split into **four groups of 8-bit**: e.g., 254.0.128.77
  - divided into **netID** (identifies the **specific network** on which the device is located) and **hostID** (identifies the **specific device** within the network)
    - The data is routed to a specific network using netID, which then decides where to forward the data according to the hostID
  - the netID and hostID range is determined by the network class of the IP address
- **IPv6**: **128-bit** split into **eight groups of 16-bit**
  - e.g., A8FB:7A88:FFF0:0FFF:3D21:2085:66FB:F0FA

### Classes of IP Addresses

Network Class	IPv4 range	Number of netID bits	Number of hostID bits	Types of network
A	0.0.0.0 - 127.255.255.255	8	24	very large
B	128.0.0.0 - 191.255.255.255	16	16	medium
C	192.0.0.0 - 223.255.255.255	24	8	small
D	224.0.0.0 - 239.255.255.255	-	-	multi-cast
E	240.0.0.0 - 255.255.255.255	-	-	experimental

### Subnetting

- dividing a network into **smaller, manageable pieces** (subnets)
- *Advantages*:
  1. **Improved Network Performance**: data packets are only sent to intended subnets instead of the whole network, decreasing traffic load
  2. **Improved Security**: segments of the network are isolated → if one subnet is hacked, the others are still fine
  3. **Improve Troubleshooting**: network issues can be identified and resolved more quickly when they are confined to a small, more manageable network segment
- *Determining subnet addresses*:



- **Requirement:** split the IP address range of 192.168.100.0 with a mask of 255.255.255.0 to create **four** subnets
1. **Determine the Number of Bits for the subnet mask:** to create four subnets, we need **2** bits ( $2^2 = 4$ )
  2. **Modify the Subnet Mask**
    - The original subnet mask is 255.255.255.0, which in binary is 11111111.11111111.11111111.00000000
    - Borrowing 2 bits from the hostID for subnetting: 11111111.11111111.11111111.11000000
    - The new subnet mask in decimal is 255.255.255.192
      - The first 26-bit are netID; the last 6-bit are hostID → There are a total of  $2^6 = 64$  hostIDs available for each subnet
  3. **Create the subnets**
    - **Subnet 1 Devices:** 192.168.100.1 to 192.168.100.62
      - 192.168.100.0 and 192.168.100.63 are used for network address and broadcast address respectively, and therefore are not for the devices
    - **Subnet 2 Devices:** 192.168.100.65 to 192.168.100.126
    - **Subnet 3 Devices:** 192.168.100.129 to 192.168.100.190
    - **Subnet 4 Devices:** 192.168.100.193 to 192.168.100.254

#### Private IP v.s. Public IP

	Public IP Address	Private IP Address
<b>Assignment</b>	Assigned by an Internet Service Provider (ISP)	Assigned within a private network (e.g., home or office network) by the router or DHCP devices
<b>Uniqueness</b>	Unique across the entire internet	Not unique globally; reused in different private networks
<b>Reachability</b>	Accessible over the internet; used for external communication	Only accessible within a private network; not directly reachable from the internet

#### Static IP v.s. Dynamic IP

	Static IP Address	Dynamic IP Address
<b>Assignment</b>	Permanently assigned to a device	Temporarily assigned from a pool; often via a DHCP server
<b>Change Frequency</b>	Does not change; remains the same unless manually modified	Changes periodically; the duration depends on the network configuration
<b>Suitability</b>	Ideal for servers, printers, or devices that require constant IP for remote access and direct access	Suitable for most personal devices, especially in environments where IP addresses are limited
<b>Use Case Examples</b>	Hosting websites, VPNs, remote access services	Residential internet connections, temporary devices in a network

#### Uniform Resource Locator (URL)

- a specific character string that is used to locate a resource on the World Wide Web
- **protocol://website address/page**
  - **protocol:** HTTP or HTTPS
  - **website address:** (domain host).(domain name).(domain type)
    - (e.g. [www.scie.com](http://www.scie.com))
  - **page:** The specific path to the resource that you are querying (e.g. a webpage or a specific file)

#### Domain Name Service (DNS)



- DNS translates human-readable domain names (like [www.example.com](http://www.example.com)) into IP addresses (like 192.0.2.1) that computers use to identify each other on the network
- *Procedure of DNS* (suppose there are 2 DNS servers):
  1. The user types in the URL and the **web browser** asks the DNS server (1) for the IP address of the website
  2. The DNS server (1) can't find the URL in its database or its cache and sends out a request to the DNS server (2)
  3. The DNS server (2) finds the matching IP address to the URL; the IP address is sent back to DNS server (1) which now puts the IP address and associated URL into its cache/database
  4. The IP address is then sent back to the user's computer
  5. The user's computer then queries the web server using the returned IP address