# Chapter 1 Explore the network

## 1. Forms of communication

- **Texting**: It enables instant *real-time communication* between two or more people
- **Social media**: Interactive websites where people and communities create and share *user-generated* content with friends, family, peers, and the world.
- **Collaboration tools**: allow individuals to communicate with each other, *without the constraints of location or time zone*
- **Blogs** or weblogs: web pages that are *easy to update and edit*.
- **Wikis**: Web pages that groups of people can edit and view together. *A wiki is a group creation.*
- **Podcasting**: allows people to deliver their audio recordings to a wide audience.
- **Peer to Peer (P2P) file sharing**: allows people to share files with each other without having to store and download them from a central server.

## 2. Networks of Many Sizes

- **Small Home Networks**: Connect a few computer to each other and the Internet.
- **Small Office/Home Office (SOHO)**: Enables computers within a HO or a remote office to connect to a corporate network or access centralized shared resources.
- **Medium to large networks**: Corporations or schools with hundreds of interconnected computers.
- **World Wide Networks**: Internet (connects a lot of computer world-wide)

## 3. Clients and servers

- **HOSTS** or end devices: Computers connected to a network that participate in network communication.
- **Clients** are computers with software installed that enable them to *request and display information* (e.g. a web browser), from a server.
- **Servers** are computers with software installed that enable them to provide information or services (email, storage, etc)

## 4. Peer To Peer

When a computer works as both, client and server

- **Pros**
  - Easy to set up • Less complexity
  - Lower cost (client and server in one) • Used to simple task (sharing files)
- **Cons**
  - No centralized administration
  - Not as secured
  - Not scalable
  - Slow performance

## 5. Components of a network

**Services, devices and media**

- **Services** include many of the common network *applications* people use every day
- **Processes** provide the *functionality* that directs and moves the messages through the network.
- **Devices and media** are the physical elements, or hardware, of the network.

### Media

The medium *provides the channel* over which the message *travels from source to destination.*

- **Types of media**
  - **Wireless transmission**: Data is encoded using wavelengths from the electromagnetic spectrum
  - **Metallic wires within cables (Copper)**: Data is encoded into electrical impulses
  - **Glass of plastic fibers (fiber optic cable)**: Data is encoded as pulse of light
- **criteria to consider when choosing network media.**
  - • Distance
  - • Environment
  - • Amount of data and speed
  - • Cost of installation

### Devices

An end device is either the source or destination of a message transmitted over the network

- To **distinguish** one end device from another, each end device on a network is identified by an **address**.
- **End Devices**: The network devices that people are most familiar with are called end devices (PC, phone, etc).
- **Intermediary devices**: Connect the individual end devices to the network, and can connect multiple individual networks to form an internetwork
  - e.g. Switch, router (determining the path that messages should take through internetworks), firewall, server, etc.
  - • Regenerate and re-transmit data signals
  - • Maintain info about paths
  - • Notify other devices of errors
  - • Direct data along alternative pathways
  - • Classify and direct message
  - • Permit or deny the flow of data

## 6. Topology diagram

It is a "picture" that represents the devices and connections that make up a network

- **Terminology to remember:**
  - **NIC** (Network Interface Card) or LAN adapter: provides the physical connection to the network.
  - **Physical Port**: A connector or outlet on a network device *where the media is connected to an end device or another networking device.*
  - **Interface**: Specialized port, *that connect to individual networks*
- **Types**
  - **Physical topology**: Identify the physical location of intermediary devices and cable installation
  - **Logical Topology**: Identify devices, ports, and addressing scheme

## 7. Types of networks

- **LAN**: A network infrastructure that provides access to users and end devices in a small geographical area.
- **WAN**: provides access to other networks over a wide geographical area
  - Managed by service providers (SP) or Internet Service Providers (ISP).
- **Other Types**: Metropolitan Area Network (MAN), Wireless LAN (WLAN), Storage Area Network (SAN), etc.

## 8. The Internet

It is a worldwide collection of interconnected networks

- The Internet is **not** owned by any individual or group
  - There are organizations that have been developed for the purpose of helping to maintain structure and standardization of Internet protocols and processes (IETF, ICANN, IAB, etc.)
- The term internet (with a lower case "i") is used to describe multiple networks interconnected.
- The term Internet (with a capital "I") is used referring to the global system of interconnected computer networks or the World Wide Web

## 9. Intranets and Extranets

- **Intranet**: It refers to a private connection of LANs and WANs that belongs to an organization. and is designed to be accessible only by members with authorization.
- **Extranet**: It provides secure and safe access to individuals who work for a different organization, but require access to the organization's data.

## 10. Internet access technologies:

- e.g. broadband cable, broadband DSL, wireless WANs, and mobile services
- Popular business-class services: include business DSL, leased lines, and Metro Ethernet.

## 11. Home and Small Office Internet Connections

- **Cable**:
  - • Typically offered by cable television service providers.
  - • The Internet data signal is carried on the same cable that delivers cable television.
  - • It provides a high bandwidth, always on, connection to the Internet.
- **DSL, Digital Subscriber Line**:
  - • Provide a high bandwidth, always on, connection to the Internet
  - • Runs over a telephone line.
  - • Small office and home office users connect using Asymmetrical DSL (ADSL), which means that the download speed is faster than the upload speed.
- **Cellular**:
  - • Uses a cell phone network to connect.
  - • Performance will be limited by the capabilities of the phone and the cell tower to which it is connected
- **Satellite**:
  - • Is a real benefit in those areas that would otherwise have no Internet connectivity at all.
  - • Satellite dishes require a clear line of sight to the satellite.
- **Dial-up Telephone**:
  - • An inexpensive option that uses any phone line and a modem.
  - • low bandwidth, but useful for mobile access while traveling.

## 12. Business Internet Connections

- **Dedicated leased line**:
  - • They are reserved circuits within the service provider's network that connect geographically separated offices for private voice and/or data networking.
  - • They can be expensive
  - • SLA (service level agreement)
- **Ethernet WAN**:
  - • The benefits of Ethernet (a LAN access technology) are now being extended into the WAN.
- **DSL**:
  - • Symmetric Digital Subscriber Lines (SDSL) provides uploads and downloads at the same speeds.
- **Satellite**:
  - • Provide a connection when a wired solution is not available.

## 13. Converged Networks

They are capable of delivering data, voice, and video between many different types of devices *over the same network infrastructure*

## 14. Networks Architecture

- **Fault Tolerance**
  - " always available":
  - • Limits the impact of a failure
  - • Quick recovery when a failure occurs
  - • redundancy: Having multiple paths to a destination
  - This is not the case in **circuit-switched** networks traditionally used for voice communications, it establishes a dedicated circuit between the source and destination before the users may communicate. If the call is unexpectedly terminated, the users must initiate a new connection.
- **Scalability**
  - A scalable network can *expand quickly* to support new users and applications *without impacting the performance* of the service being delivered to existing users
- **Quality of service (QoS)**
  - QoS becomes a primary mechanism for managing congestion and ensuring reliable delivery of content to all users.
  - **Congestion** occurs when the demand for bandwidth exceeds the amount available.
- **Security**
  - **Network infrastructure security**
    - It includes the *physical securing* of devices that provide network connectivity, and *preventing unauthorized access* to the management software that resides on them
  - **Information security**
    - It refers to protecting the information within the packets being transmitted, and the information stored.
    - **Confidentiality**: only the intended and authorized recipients can access and read data
    - **Integrity**: having the assurance that the information has not been altered in transmission
    - **Availability**: timely and reliable access to data services for authorized users

## 15. New Trends

- **BYOD**: Bring Your Own Device means any device, with any ownership, used anywhere to access information and communicate across a business or campus network
- **Video communication**: Video conferencing is a powerful tool for communicating with others at a distance
- **Online Collaboration**: Cisco WebEx
- **Cloud Computing** allows us to store files (backups) on servers over the Internet. Applications such as word processing and photo editing can be accessed using the Cloud.
  - • Extends IT's capabilities without requiring investment in new infrastructure, training new personnel, or licensing new software
  - **Types**
    - **Public Clouds**
    - **Private Clouds**
    - **Hybrid Clouds** (part custom part public, etc.)
    - **Custom Clouds**

## 16. Technology trends in the home

- **Wireless Broadband**: Wireless Internet Service Provider (WISP) is an ISP that connects subscribers to a designated access point or hot spot using similar wireless technologies found in home wireless local area networks (WLANs)
  - An antenna is installed outside the house providing either wireless or wired connectivity for devices in the home
- **Wireless Broadband Service**: This uses the same cellular technology used to access the Internet with a smart phone or tablet.
- **Powerline Networking** uses existing electrical wiring to connect devices
  - "no new wires" means the ability to connect a device to the network wherever there is an electrical outlet
- **Smart home** technology is technology that is integrated into every-day appliances allowing them to interconnect with other devices, making them more 'smart' or automated.

## 17. Network Security

### Internal threats:

- Most common data breaches happen because of internal users of the network.
- This can be attributed to lost or stolen devices, accidental misuse by employees, and in the business environment, even malicious employees.

### External Threats to networks

- **Data interception and theft** - an attack to capture private information from an organization's network
- **Identity theft** - an attack to steal the login credentials of a user in order to access private data
- **Zero-day attacks**, also called zero-hour attacks - an attack that occurs on the first day that a vulnerability becomes known
- **Denial of service attacks** - attacks designed to slow or crash applications and processes on a network device
- **Hacker attacks** - an attack by a knowledgeable person to user devices or network resources
- **Malware** (Malicious Software): harmful software that aims to infiltrate or damage a computer or information system
  - **Spyware**: it is designed to track and spy on the user.
  - **Adware**: Advertising supported software is designed to automatically deliver advertisements
  - **Bot**: is malware designed to automatically perform action, usually online, a set of bot that work together to perform an attack is called a Botnet
  - **Ransomware**: designed to hold a computer system or the data (it encrypts data) it contains captive until a payment is made
  - **Scareware**: designed to persuade the user to take a specific action based on fear
  - **Rootkit**: designed to modify the operating system (by privilege escalation and modify system files) to create a backdoor.
  - **Virus**: it is malicious *executable code* that is *attached to other executable files*. Most viruses require end-user activation
  - **Worms**: Worms are malicious code that replicate themselves by independently exploiting vulnerabilities in networks, they usually slow down networks. *Worms can run by themselves*
  - **Trojan Horse**: is malware that carries out malicious operations under the guise of a desired operation. A Trojan horse differs from a virus because it *binds itself to non-executable files.*

### Security solutions

- **Corporate networks**
  - • Dedicated Firewalls Systems
  - • Access Control Lists
  - • Intrusion Prevention Systems: used to identify fast-spreading threats, such as zero-day or zero-hour attacks.
  - • Virtual Private Networks **VPN**: used to provide secure access to remote workers.
- For a home or **small office network**:
  - • Antivirus, antispyware
  - • Firewall filtering

No single solution can protect the network from the variety of threats that exist, **Security is a process, not a product**