Computer Networks

1. Networks:

- Definition: A network refers to a collection of computers, devices, or nodes interconnected to facilitate communication and resource sharing. It allows users to share data, hardware, and software resources.
- Components:
    - Computers: Devices that participate in the network and exchange data with other devices.
    - Network Devices: Such as routers, switches, hubs, and access points facilitate communication and data transfer within the network.
    - Cables and Connections: Physical medium used to transmit data, including Ethernet cables, fiber optic cables, and wireless connections.
    - Protocols: Rules and standards governing communication between devices on the network, ensuring compatibility and efficient data transfer.
- Need for Networking:
    - Resource Sharing: Networks enable sharing of hardware resources like printers and scanners, as well as software resources like files and databases, leading to increased efficiency and productivity.
    - Communication: Facilitates real-time communication among users, both within an organization and externally, enhancing collaboration and decision-making.
    - Data Management: Networks support centralized data storage and management, allowing easy access, backup, and security of data.
    - Cost Reduction: By sharing resources, networks reduce the need for duplicate equipment and software licenses, leading to cost savings.
- Advantages:
    - Improved Resource Utilization
    - Enhanced Communication
    - Centralized Data Management
    - Cost Efficiency
    - Scalability
- Disadvantages:
    - Security Concerns
    - Dependency on Network Infrastructure
    - Maintenance Overhead
    - Potential for Network Congestion

Advantages of Networks:

Resource Sharing:

- Advantage: Networks allow for the sharing of hardware resources like printers, scanners, and storage devices, as well as software resources such as applications and databases. This leads to cost savings and increased efficiency as resources are utilized more effectively.

Communication:

- Advantage: Networks facilitate communication among users, both within an organization and externally. Email, instant messaging, video conferencing, and other communication tools enable real-time collaboration, improving productivity and decision-making.

Centralized Data Management:

- Advantage: Networks support centralized data storage and management, allowing users to access and share data from a centralized location. This improves data security, consistency, and backup processes, reducing the risk of data loss.

Cost Efficiency:

- Advantage: By sharing resources such as printers, internet connections, and software licenses, networks help reduce costs associated with purchasing and maintaining duplicate equipment. Additionally, networks enable cost-effective communication and collaboration, reducing the need for travel and physical meetings.

Scalability:

- Advantage: Networks can easily scale to accommodate growing numbers of users, devices, and resources. This flexibility allows organizations to adapt to changing business needs and accommodate expansion without significant infrastructure changes.

Disadvantages of Networks:

Security Risks:

- Disadvantage: Networks introduce security vulnerabilities such as unauthorized access, data breaches, malware infections, and denial-of-service attacks. Protecting networks from these threats requires implementing robust security measures such as firewalls, encryption, and access controls.

Dependency on Network Infrastructure:

- Disadvantage: Organizations become reliant on network infrastructure for day-to-day operations. Any disruptions or failures in the network infrastructure, such as outages or equipment malfunctions, can lead to downtime, loss of productivity, and financial losses.

Maintenance Complexity:

- Disadvantage: Networks require ongoing maintenance, monitoring, and troubleshooting to ensure optimal performance and security. Managing network hardware, software, configurations, and updates can be complex and time-consuming, requiring skilled IT professionals.

Potential for Network Congestion:

- Disadvantage: As the number of users and devices on a network increases, network congestion may occur, leading to slower data transmission speeds and reduced performance. This can impact user experience and productivity, especially during peak usage periods.

Privacy Concerns:

- Disadvantage: Networks may raise privacy concerns related to the collection, storage, and transmission of sensitive information. Unauthorized access to data, interception of communications, and data breaches can compromise user privacy and confidentiality, leading to legal and reputational consequences.

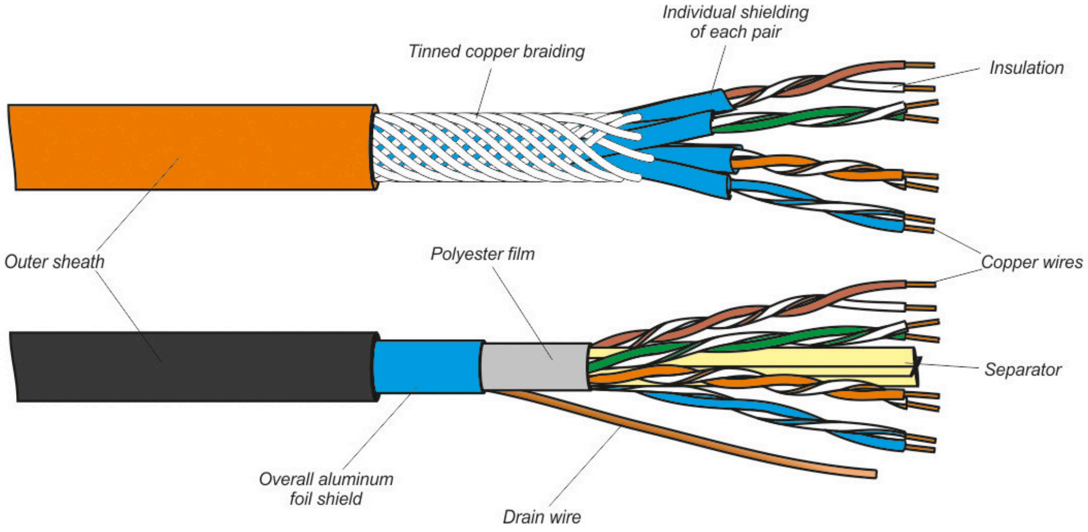
Overall, while computer networks offer numerous advantages in terms of resource sharing, communication, and efficiency, they also present challenges related to security, maintenance, and privacy that must be carefully managed to ensure their effective and secure operation.

2. Types of Networks:

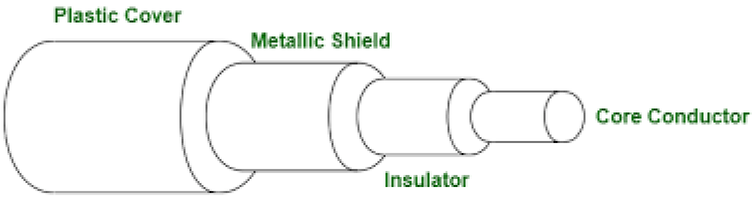
- LAN (Local Area Network): A LAN covers a small geographic area, typically within a single building or campus. It offers high-speed connectivity and is commonly used in offices, schools, and homes.
- MAN (Metropolitan Area Network): MANs span a larger geographic area, such as a city or a town. They connect multiple LANs and are often used by internet service providers to offer broadband services.
- WAN (Wide Area Network): WANs cover vast geographical distances, such as across countries or continents. They connect LANs and MANs over long distances, utilizing technologies like leased lines, satellites, and the internet.

3. Communication Channel:

- Physical Channel:
    - Twisted Pair Cable: Consists of pairs of insulated copper wires twisted together, offering flexibility and cost-effectiveness. Commonly used in Ethernet networks for connecting computers and other devices.

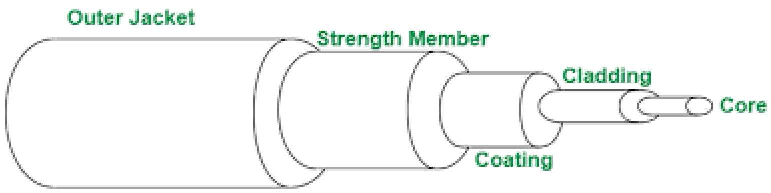


    - Coaxial Cable: Features a central conductor surrounded by insulation, a metallic shield, and an outer insulating layer. It offers better shielding and higher bandwidth than twisted pair cables, commonly used in cable television and broadband internet.



Coaxial Cable

    - Optical Fiber Cable: Utilizes glass or plastic fibers to transmit data using light signals. It offers high bandwidth, low attenuation, and immunity to electromagnetic interference, making it suitable for long-distance communication and high-speed internet connections.



OPTICAL FIBER CABLE

- Wireless Channel:
    - Microwave: Uses high-frequency radio waves for communication over short to medium distances. It's commonly used for point-to-point communication, such as in microwave links for connecting buildings or cellular backhaul.
    - Radio Wave: Utilizes lower-frequency radio waves for wireless LANs, cellular networks, and other short-range communication applications. It offers mobility and flexibility, making it suitable for mobile devices and IoT applications.
    - Satellite Links: Involves communication through satellites orbiting the Earth. It enables long-distance communication, connecting remote locations or providing internet access in rural areas where wired infrastructure is unavailable.

1. Data Switching Techniques:

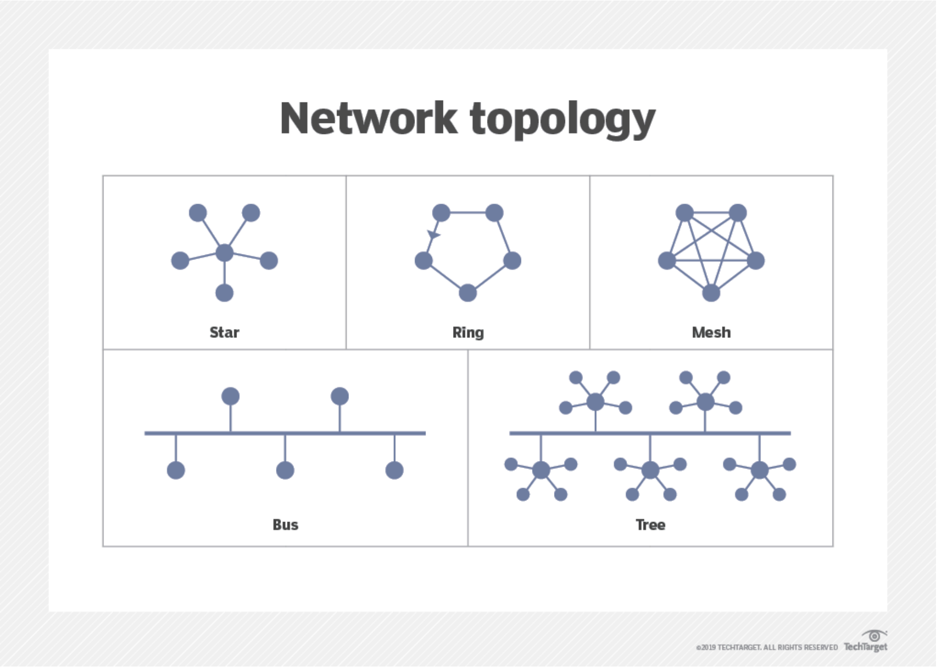
- Circuit Switching: In circuit switching, a dedicated communication path is established between two nodes for the duration of the communication session. This path remains reserved and unused by other users until the session ends. Examples include traditional telephone networks.
- Message Switching: In message switching, data is divided into fixed-size messages and transmitted independently through the network. Each message is forwarded from node to node until it reaches its destination. This technique is inefficient as messages can take different routes and may experience delays.
- Packet Switching: Packet switching breaks data into smaller units called packets, which are then routed independently through the network. Each packet contains addressing information, allowing routers to dynamically determine the best path for delivery. Packet switching is the basis for modern computer networks, including the internet.

2. Network Devices and their uses:

- Modem: Modem (Modulator-Demodulator) converts digital data from a computer into analog signals for transmission over telephone lines (or vice versa). It enables communication between computers over telephone lines.
- Hub: A hub is a basic networking device that connects multiple devices in a network, allowing them to communicate with each other. However, it operates at the physical layer of the OSI model and simply broadcasts data to all connected devices, leading to network congestion.
- Repeaters: Repeaters regenerate and amplify signals to extend the range of a network. They are used to overcome attenuation and signal loss in long-distance communication.
- Bridge: A bridge connects multiple network segments and filters traffic based on MAC addresses. It improves network performance by reducing collision domains and segmenting network traffic.
- Router: A router is a networking device that forwards data packets between computer networks. It operates at the network layer of the OSI model and uses routing tables to determine the best path for packet delivery.
- Gateway: A gateway acts as an interface between different networks, translating protocols to enable communication between incompatible networks. It is often used to connect a local network to the internet.
- Switch: A switch is a networking device that connects multiple devices in a network and forwards data packets only to the intended recipient, improving network efficiency. It operates at the data link layer of the OSI model.

3. Network Topologies:

- Definition: Network topology refers to the arrangement of nodes and connections in a network.



©2019 TECHTARGET. ALL RIGHTS RESERVED TechTarget

- Types of Topologies:
  - Bus Topology: All devices are connected to a single backbone cable. It's simple and inexpensive but susceptible to single-point failures.
  - Advantages:
    - Simple to set up and implement.
    - Requires less cabling compared to other topologies, making it cost-effective.
    - Well-suited for small networks with a limited number of devices.
  - Disadvantages:
    - Susceptible to a single-point failure: If the main cable (backbone) fails, the entire network goes down.
    - Limited scalability: Adding more devices can degrade performance and increase the chances of collisions.
    - Difficult to troubleshoot and locate faults.

  - Star Topology: All devices are connected to a central hub or switch. It offers better performance and scalability but requires more cabling.
  - Advantages:
    - Centralized management: Easy to add or remove devices without affecting the rest of the network.

    - Scalable: Can accommodate a large number of devices without significantly affecting performance.
    - Fault isolation: If one device fails, it does not affect the rest of the network.
- Disadvantages:
    - Dependency on central hub/switch: If the hub/switch fails, the entire network becomes inaccessible.
    - Costlier than bus topology due to the requirement for more cabling and central devices.
    - If the central hub/switch fails, the entire network becomes inaccessible.

- Ring Topology: Devices are connected in a closed loop, with each device connected to two others. It's efficient but can be disrupted by a single device failure.
- Advantages:
    - Efficient data transmission: Data flows in one direction, reducing collisions and improving performance.
    - Simple design: Each device is connected to only two neighbors, making it easy to understand and implement.
    - No collisions: Data packets circulate in a single direction, reducing the likelihood of collisions.
- Disadvantages:
    - Single-point failure: If one device or connection fails, it can disrupt the entire network.
    - Limited scalability: Adding more devices can degrade performance and increase latency.
    - Difficult to reconfigure or modify the network without disrupting operations.

- Tree Topology: A combination of bus and star topologies, with multiple star networks connected to a bus backbone. It's scalable but can be complex to manage.
- Advantages:

        - Scalable: Can accommodate a large number of devices and subnetworks.
        - Fault tolerance: Failure of a single branch or device does not necessarily disrupt the entire network.
        - Flexibility: Allows for the creation of hierarchical structures, facilitating management and organization.
    - Disadvantages:
        - Complex design and implementation: Requires careful planning and management of multiple branches.
        - Dependency on root nodes: Failure of the root nodes can affect all connected devices.
        - Costlier than other topologies due to the need for more cabling and networking equipment.

Each network topology has its own set of advantages and disadvantages, and the choice of topology depends on factors such as the size of the network, the number of devices, budget constraints, and the level of fault tolerance required.

4. Application of Networks:

- Email: Electronic mail allows users to exchange messages and files over a network.
- E-commerce: Online buying and selling of goods and services over the internet.
- Chat Services: Real-time messaging applications for communication over networks.
- Video Conferencing: Allows multiple users to participate in virtual meetings and conferences using audio and video.
- Usenet: A distributed discussion system for exchanging messages on various topics.

5. Protocols:

- Definition: Protocols are rules and standards that govern communication between devices on a network.
- FTP (File Transfer Protocol): Used for transferring files between computers on a network.
- HTTP (Hyper Text Transfer Protocol): Used for accessing and retrieving resources on the World Wide Web.

- TCP/IP (Transmission Control Protocol/Internet Protocol): The foundational protocol suite for communication on the internet.
- Telnet: Allows remote login and access to computers over a network.

1. File Transfer Protocol (FTP):

- Definition: FTP is a standard network protocol used to transfer files between a client and a server on a computer network.
- Functionality: It allows users to upload, download, and manage files stored on remote computers over a TCP/IP network, typically the internet.
- Modes of Operation: FTP operates in two modes: Active mode and Passive mode. In Active mode, the client initiates the data connection, while in Passive mode, the server initiates the data connection.
- Security: FTP does not encrypt data during transmission, making it vulnerable to interception. However, FTPS (FTP Secure) and SFTP (SSH File Transfer Protocol) are secure alternatives that provide encryption and authentication mechanisms.

2. Hyper Text Transfer Protocol (HTTP):

- Definition: HTTP is an application protocol used for transmitting hypertext documents (such as web pages) over the World Wide Web.
- Functionality: It defines how clients (such as web browsers) request resources from servers (such as web servers) and how servers respond to these requests.
- Stateless Protocol: HTTP is stateless, meaning each request-response cycle is independent, and the server does not maintain session information between requests.
- Security: HTTP does not provide encryption by default, making it vulnerable to eavesdropping and data tampering. However, HTTPS (HTTP Secure) uses SSL/TLS encryption to secure communication between clients and servers.

3. Transmission Control Protocol/Internet Protocol (TCP/IP):

- Definition: TCP/IP is a suite of protocols used for communication over networks, including the internet.
- Functionality: TCP/IP defines how data is transmitted, routed, and received between devices on a network. It consists of two main protocols: TCP for reliable, connection-oriented communication, and IP for addressing and routing packets across networks.

- TCP: Provides reliable, ordered, and error-checked delivery of data packets between devices. It establishes a connection, sends data, and ensures data integrity through sequence numbers and acknowledgments.
- IP: Responsible for addressing and routing packets across networks. It assigns unique IP addresses to devices and determines the best path for packet delivery based on routing tables.
- Versions: TCP/IP has two primary versions: IPv4 and IPv6. IPv4 is the most widely used version, but IPv6 offers a larger address space and improved security features to accommodate the growing number of devices connected to the internet.

4. Remote Login (Telnet):

- Definition: Telnet is a network protocol used to provide terminal emulation services over a network.
- Functionality: It allows users to remotely access and manage devices (such as servers, routers, and switches) as if they were physically connected to them via a command-line interface (CLI).
- Insecurity: Telnet transmits data (including usernames, passwords, and commands) in plain text, making it susceptible to eavesdropping and interception. As a result, it is generally considered insecure for use over untrusted networks, such as the internet.
- Secure Alternatives: Secure Shell (SSH) is a more secure alternative to Telnet, providing encrypted communication and stronger authentication mechanisms for remote access to devices.

These protocols play crucial roles in enabling communication and data transfer across computer networks, each with its own features, functionalities, and security considerations. Understanding these protocols is essential for effectively managing and securing networked systems.

1. Internet:

- Definition: The internet is a global network of interconnected computers and devices that use standardized communication protocols to exchange data and information.
- Functionality: It facilitates communication, collaboration, information sharing, and access to resources and services worldwide.

2. Internet Service Providers (ISPs):

- Definition: ISPs are companies that provide users with access to the internet. They offer various services such as internet connectivity, email hosting, web hosting, and domain registration.
- Functionality: ISPs connect users to the internet through various technologies, including dial-up, DSL, cable, fiber-optic, and wireless connections.

3. Internet Addressing:

- Definition: Internet addressing involves assigning unique identifiers to devices and resources connected to the internet.
- Functionality: Internet Protocol (IP) addresses are used to identify devices on the internet, while Domain Name System (DNS) translates human-readable domain names into IP addresses.

4. World Wide Web (WWW):

- Definition: The World Wide Web is an information system on the internet that allows users to access and interact with multimedia content, web pages, and websites.
- Functionality: It uses hypertext and hyperlinks to navigate between interconnected web pages and resources.

5. Uniform Resource Locator (URL):

- Definition: A URL is a web address used to locate and access specific resources on the internet, such as web pages, files, or services.
- Format: A URL typically consists of a protocol (e.g., http:// or https://), domain name, and optional path or parameters.

6. Web Server:

- Definition: A web server is a software application or hardware device that stores, processes, and delivers web pages and content to clients over the internet.
- Functionality: Web servers use HTTP or HTTPS protocols to handle client requests and serve web pages stored on the server's filesystem.

7. Web Page:

- Definition: A web page is a document or resource accessible on the World Wide Web that contains text, images, multimedia, and hyperlinks.
- Functionality: Web pages are created using HTML, CSS, and JavaScript and are displayed in web browsers.

8. Website:

- Definition: A website is a collection of interconnected web pages and resources hosted on a web server and accessible through a single domain name or URL.
- Functionality: Websites serve various purposes, including informational, educational, e-commerce, entertainment, and social networking.

9. Web Browser:

- Definition: A web browser is a software application used to access, navigate, and interact with content on the World Wide Web.
- Functionality: Web browsers interpret and render HTML, CSS, and JavaScript code to display web pages and execute web-based applications.

10. HyperText Markup Language (HTML):

- Definition: HTML is a standard markup language used to create and structure web pages by defining the layout, formatting, and content of documents.
- Functionality: HTML uses tags and attributes to define elements such as headings, paragraphs, images, links, and forms.

11. Dynamic HyperText Markup Language (DHTML):

- Definition: DHTML is a combination of HTML, CSS, and JavaScript used to create dynamic and interactive web content and user interfaces.
- Functionality: DHTML allows web developers to create effects such as animations, transitions, and interactive elements that respond to user actions.

12. Search Engine:

- Definition: A search engine is a software program or website that allows users to search and retrieve information from the World Wide Web.
- Functionality: Search engines index and organize web pages and resources based on relevance and popularity, providing users with relevant search results in response to their queries.

13. Downloading and Uploading Files:

- Downloading: The process of transferring files or data from a remote server to a local computer or device over the internet.
- Uploading: The process of transferring files or data from a local computer or device to a remote server over the internet.

14. Hacking and Cracking:

- Hacking: The act of gaining unauthorized access to computer systems, networks, or data with the intent to exploit vulnerabilities, steal information, or cause damage.
- Cracking: A subset of hacking that specifically involves breaking into computer systems or software to bypass security measures, copy protected content, or modify software for malicious purposes.

Understanding these internet-related terminologies is essential for navigating the online world, accessing information, and communicating effectively over the internet.