COMPUTER NETWORK

COMPUTER NETWORK

A computer network is a collection of interconnected computers and other devices that can communicate and share resources with each other. These networks can be as small as a local area network (LAN) within a single building or as vast as the internet, which connects computers and devices worldwide.

APPLICATIONS

A computer network is a collection of interconnected computers and other devices that can communicate and share resources with each other. These networks can be as small as a local area network (LAN) within a single building or as vast as the internet, which connects computers and devices worldwide. Computer networks serve a variety of purposes and have numerous applications, some of which include:

1. File Sharing: One of the fundamental uses of computer networks is to enable the sharing of files and resources among connected devices. This can be for individual users in a home network or for large organizations to facilitate collaborative work.

2. Communication: Networks allow for communication between devices. This includes email, instant messaging, video conferencing, and VoIP (Voice over Internet Protocol) services.

3. **Internet Access:** Most people use computer networks to access the internet, which is a vast global network of interconnected computers and information resources.

4. **Data Storage and Backup:** Network-attached storage (NAS) devices and cloud storage services use networks to provide centralized data storage and backup solutions.

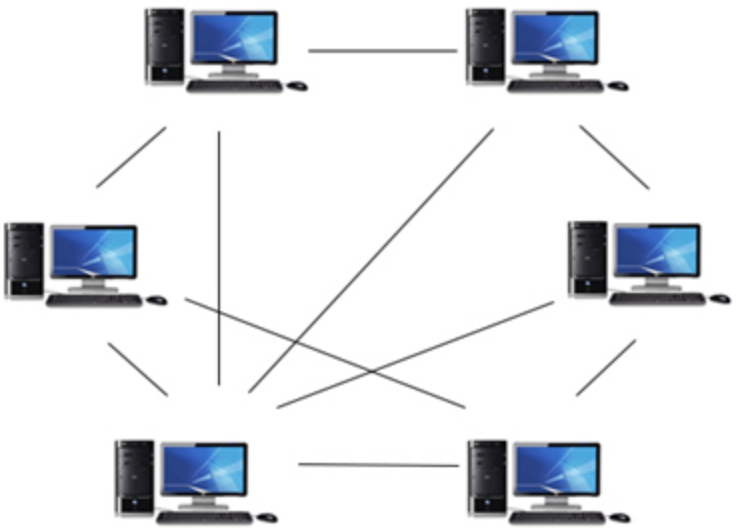
5. Remote Access:Networks enable remote access to devices and systems, allowing users to work from home or access their systems from anywhere with an internet connection.

6. Printing: Network printers allow multiple users to print to a single device over the network.

7. Online Gaming:Multiplayer online games rely on computer networks to connect players from around the world in real-time gaming experiences.

8. **Smart Home Automation:** Many smart home devices, such as thermostats, lights, and security systems, are connected to home networks to allow remote control and automation.

NETWORK STRUCTURE AND ARCHITECTURE



Computer network architecture refers to the design and layout of a computer network, including its components, protocols, and how they are organized. The architecture of a computer network can vary widely depending on its purpose and scale. However, there are common components and architectural principles that are typically used in network design. Here are some key elements of network architecture:

1. Network Topology: Network topology defines how devices are connected and the physical or logical structure of the network. Common topologies include:

- Bus Topology: All devices are connected to a central cable or bus.
- Star Topology: Devices are connected to a central hub or switch.
- Ring Topology: Devices are connected in a circular fashion.
- Mesh Topology: Every device is connected to every other device.

2. Network Protocols: Network protocols are the rules and conventions that govern how data is transmitted, received, and processed in a network. Examples of network protocols

include TCP/IP (Transmission Control Protocol/Internet Protocol), HTTP (Hypertext Transfer Protocol), and Ethernet.

3. Network Components:

- Devices:These include computers, servers, routers, switches, hubs, and other hardware that make up the network.

- Cabling and Connectivity: The physical cables and connectors used to link devices together.

- Network Infrastructure:This includes the core components that enable network connectivity, such as routers, switches, and access points.

- Firewalls and Security Devices:These components are essential for network security and protect against unauthorized access and threats.

- Servers: Servers provide various services, such as file storage, email, and web hosting.

- Clients: End-user devices like laptops, desktop computers, smartphones, and tablets.

4. Network Segmentation: Networks are often divided into segments to improve performance and security. This can involve creating subnets, VLANs (Virtual LANs), and separate network segments for different purposes.

5. Network Addressing: Every device on a network has an IP address or another type of address that helps in routing data. IPv4 and IPv6 are common addressing schemes for the internet.

6. Redundancy and Load Balancing: Implementing redundancy and load balancing techniques ensures network reliability and balanced traffic distribution.

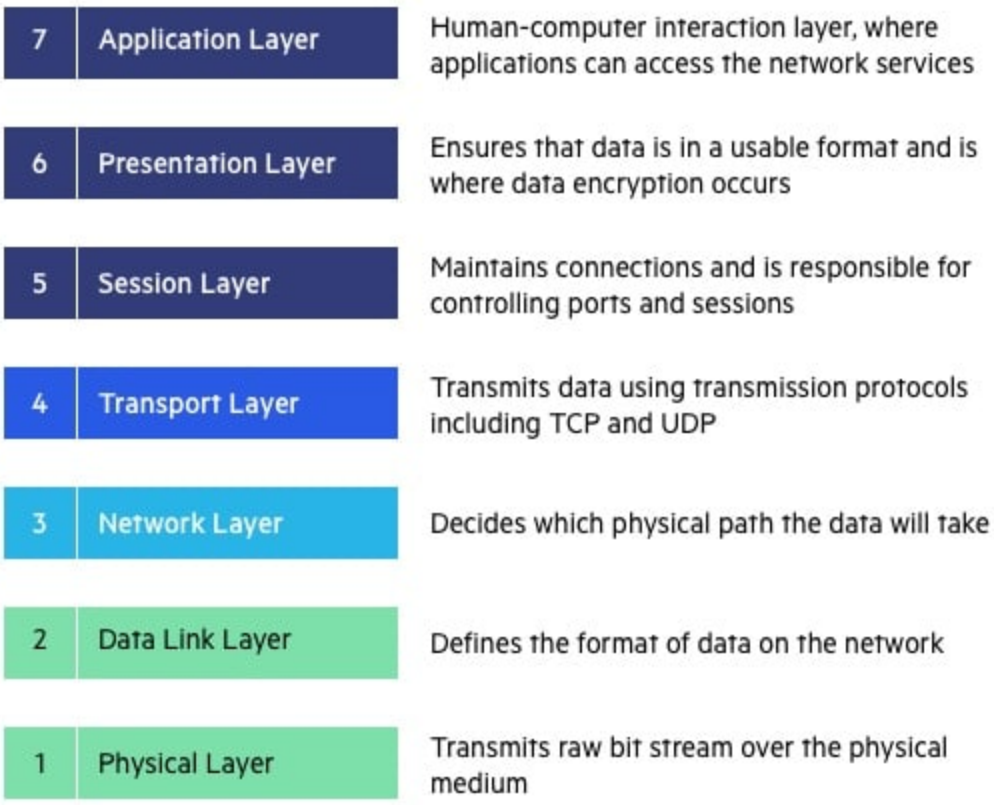
7. Scalability: Network architecture should be designed to accommodate growth and increased demand for network resources.

8. Security: Security is a critical aspect of network architecture. This includes measures like firewalls, intrusion detection systems, encryption, and access controls to protect the network from unauthorized access and attacks.

9. Bandwidth and Performance Management: Network architects must consider the required bandwidth and implement measures to optimize network performance.

10. Quality of Service (QoS): QoS mechanisms are used to prioritize and manage network traffic to ensure that critical applications and services receive the necessary resources.

OSI MODEL



The OSI (Open Systems Interconnection) model is a conceptual framework used to understand and standardize the functions of a telecommunication or networking system. It divides the networking process into seven distinct layers, each responsible for specific tasks. The OSI model is not a practical implementation but rather a theoretical guideline to help understand how different networking protocols and technologies work together. Here are the seven layers of the OSI model, from the lowest (Layer 1) to the highest (Layer 7):

1. Physical Layer (Layer 1): This is the lowest layer and deals with the physical transmission of data on the network. It specifies the characteristics of the physical medium, such as cables, connectors, and signaling. It defines aspects like voltage levels, cable types, and data transmission rates. Devices at this layer include network cables, hubs, and repeaters.

2. Data Link Layer (Layer 2): The data link layer is responsible for error detection and correction on the physical layer. It provides a way to access the physical medium, manages the flow of data frames between devices, and handles addressing (e.g., MAC addresses). Devices at this layer include switches and network interface cards (NICs).

3. Network Layer (Layer 3): The network layer is responsible for routing data packets from the source to the destination across multiple networks. It uses logical addressing (e.g., IP addresses) to make routing decisions. Routers operate at this layer, and it also involves routing protocols like IP, ICMP (Internet Control Message Protocol), and OSPF (Open Shortest Path First).

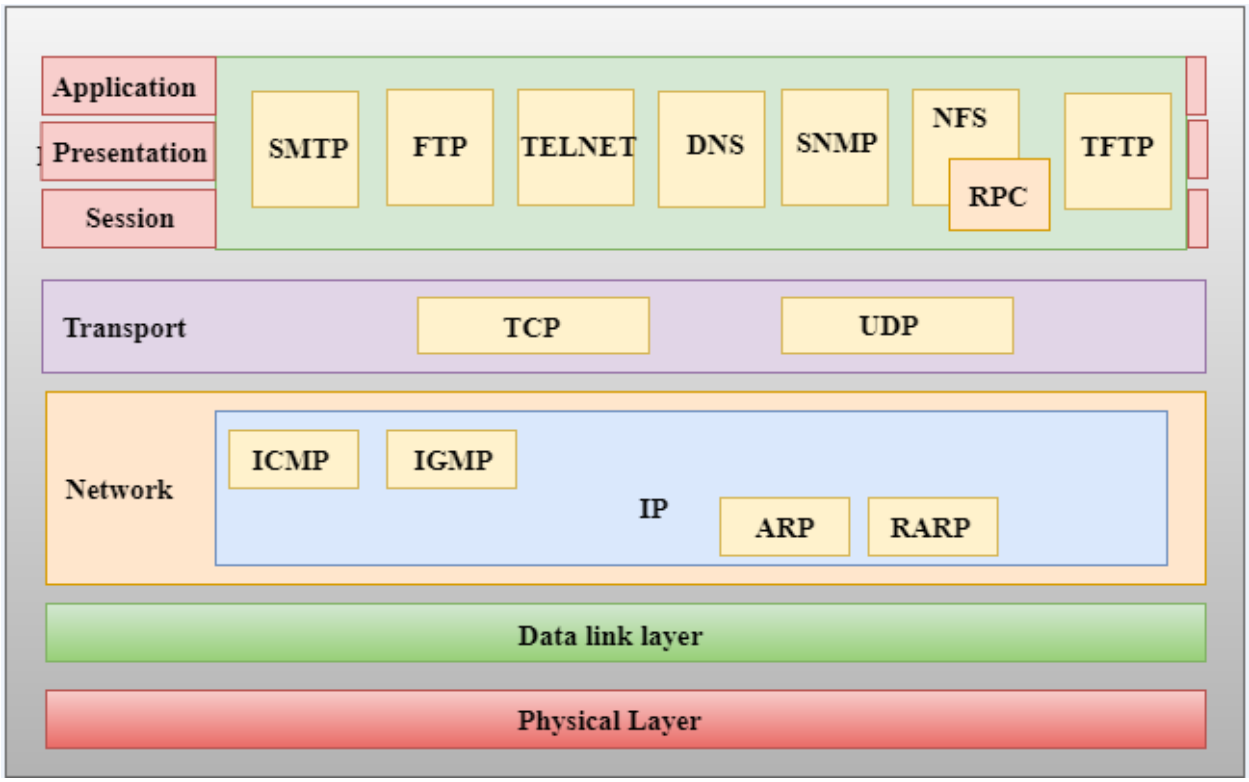
4. Transport Layer (Layer 4): The transport layer is responsible for end-to-end communication, ensuring data is reliably delivered between two devices. It manages data segmentation, error recovery, and flow control. Common transport layer protocols include TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

5. Session Layer (Layer 5): The session layer establishes, manages, and terminates communication sessions between two devices. It handles tasks such as session setup, maintenance, and teardown. This layer is responsible for dialog control and synchronization. It ensures that data is properly synchronized and organized for communication.

6. Presentation Layer (Layer 6): The presentation layer deals with data translation, encryption, and compression. It ensures that data is presented in a readable format for the application layer. Tasks include data encryption, data compression, and character encoding translation.

7. Application Layer (Layer 7): The application layer is the top layer of the OSI model and interacts directly with end-user applications. It provides network services directly to user applications and serves as the interface between the application and the lower layers. Protocols at this layer include HTTP, FTP, SMTP, and DNS.

TCP/IP MODEL



The TCP/IP model, also known as the Internet protocol suite, is a networking framework that serves as the foundation for the internet and most modern networking. It is a more practical and simplified model compared to the OSI model. The TCP/IP model has four layers, as follows:

1. Network Interface Layer: This layer corresponds to the combination of the OSI model's Physical and Data Link layers. It deals with the physical connection to the network and includes functions like addressing, data framing, and error detection. It often involves the use of hardware devices, such as network cards and switches. Ethernet and Wi-Fi are examples of technologies used in this layer.

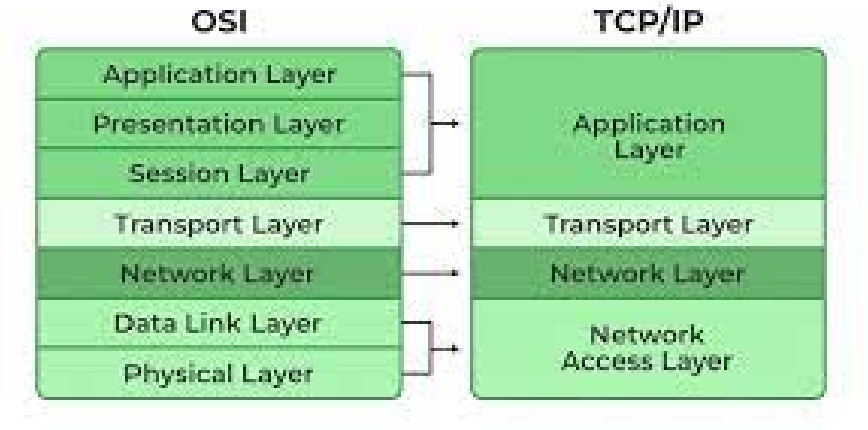
2. Internet Layer: This layer corresponds to the OSI model's Network layer. It is responsible for logical addressing (e.g., IP addresses), routing, and packet forwarding. The Internet Layer is where the Internet Protocol (IP) operates, and it allows data to be transmitted across networks, including the internet. Key protocols in this layer include IPv4 and IPv6.

3. Transport Layer: This layer is similar to the OSI model's Transport layer. It ensures end-to-end communication between devices, handling functions like data segmentation, error detection and correction, and flow control. The most common transport layer protocols are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

4. Application Layer:The Application layer in the TCP/IP model is a combination of the Session, Presentation, and Application layers of the OSI model. It serves as the interface between the network and user applications. This layer includes a wide range of application protocols for services like email, file transfer, remote access, and web browsing. Common application layer protocols include HTTP, FTP, SMTP, and DNS.

The TCP/IP model is more commonly used in practice, especially for internet-related communication. It provides a clear and effective framework for understanding and implementing network communication. In contrast to the OSI model, the TCP/IP model directly influenced the development of the internet and its protocols.

DIFFERENCE BETWEEN OSI MODEL AND TCP/IP MODEL



The OSI (Open Systems Interconnection) model and the TCP/IP model are both conceptual frameworks used to understand and standardize the functions of network protocols and communication. While they have similarities in the way they describe networking processes, they have some differences as well. Here's a comparison between the two models:

1. Number of Layers:

- OSI Model: The OSI model has seven layers, which provide a detailed and comprehensive description of network functions.

- TCP/IP Model: The TCP/IP model has four layers, which are more practical and directly aligned with the development of the internet.

2. Specific Layers: - OSI Model: The OSI model includes layers like Session, Presentation, and Data Link, which provide more granularity in understanding network operations.

- TCP/IP Model: The TCP/IP model combines these functions into fewer layers, with the emphasis on practicality.

3. Historical Perspective:

- OSI Model: The OSI model was developed as a theoretical framework in the 1980s by the International Organization for Standardization (ISO).

- TCP/IP Model: The TCP/IP model was developed based on real-world protocols and implementations, and it is the model that influenced the development of the internet.

4. Widely Adopted:

- OSI Model: While the OSI model is used as a reference model and for educational purposes, it is not widely adopted for practical networking and is more of an academic concept.

- TCP/IP Model: The TCP/IP model is the basis for the entire internet and is widely adopted in real-world networking.

5. Layer Equivalents:

- OSI Model: The OSI model's layers have well-defined functions, and it's often used as a reference for understanding various network protocols and their roles.

- TCP/IP Model: The TCP/IP model is practical for describing internet-related communication and is directly associated with key internet protocols like IP, TCP, and UDP.

6. Simplification:

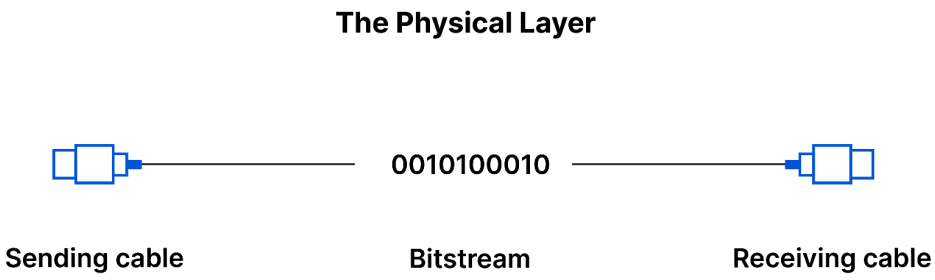
- OSI Model: The OSI model is more detailed and provides a comprehensive framework for understanding network functions but can be complex.

- TCP/IP Model: The TCP/IP model simplifies the framework into four layers, making it easier to understand and implement in practice.

7. Naming and Terminology: - OSI Model: The OSI model uses specific layer names like "Presentation," "Session," and "Data Link."

- TCP/IP Model: The TCP/IP model uses more straightforward and descriptive names like "Application," "Transport," and "Network."

PHYSICAL LAYER



The physical layer is the lowest layer in the OSI (Open Systems Interconnection) model and the TCP/IP model of computer networking. It is responsible for the physical transmission of data over a physical medium, such as a network cable, fiber optic cable, or wireless transmission. The physical layer deals with the actual hardware devices and physical characteristics of the network, including the following key aspects:

1. Physical Medium: The physical layer defines the type of physical medium used for data transmission. This can include various types of cabling, such as copper twisted pair cables (used in Ethernet networks), optical fibers (used in fiber-optic networks), and wireless communication mediums like radio waves (used in Wi-Fi networks).

2. Connectors and Pinouts: It specifies the physical connectors and pinouts used to connect devices to the network medium. For example, in an Ethernet network, it defines the physical connectors like RJ45 connectors and the wiring schemes (e.g., T568A or T568B) used for connecting network devices.

3. Encoding and Signaling: The physical layer deals with the encoding of digital data into analog signals for transmission over the physical medium and the reverse process of

decoding received analog signals back into digital data. It includes aspects like modulation and demodulation for analog signals.

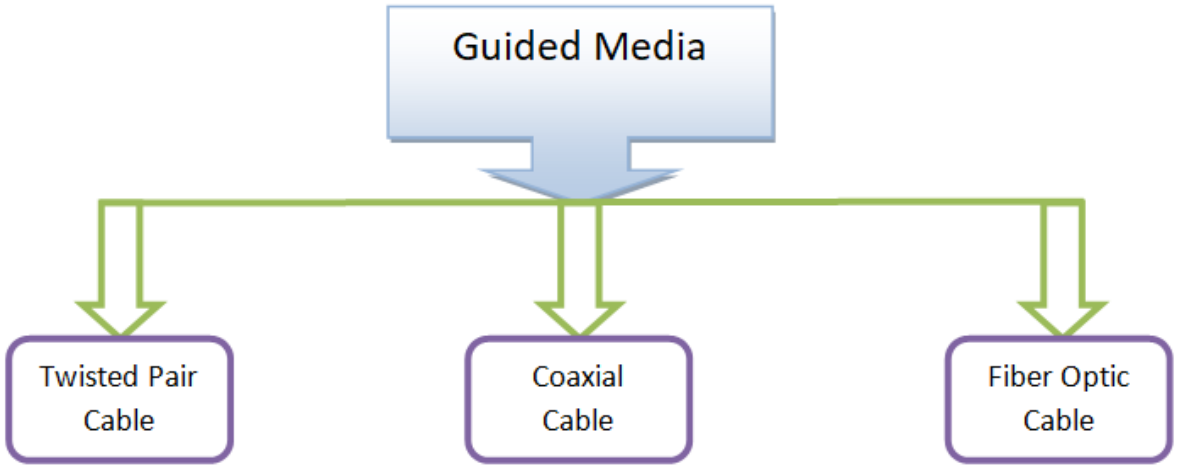
4. Bit Rate: It determines the maximum data transfer rate, also known as the bit rate or data rate, at which data can be transmitted over the physical medium. The bit rate is typically measured in bits per second (bps) and varies depending on the technology and medium used.

5. Transmission Distance: The physical layer specifies the maximum distance over which data can be transmitted on the physical medium. This distance is determined by factors such as signal attenuation and interference.

6. Synchronization: It deals with the synchronization of data transmission, ensuring that both the sender and receiver are operating at the same pace.

7. Error Detection and Correction: Some error detection and correction mechanisms may be employed at this layer to identify and correct transmission errors.

GUIDED TRANSMISSION MEDIA



1. Twisted Pair Cable:

- **Unshielded Twisted Pair (UTP):** UTP cables are commonly used in Ethernet networks. They consist of pairs of insulated copper wires twisted together to reduce

electromagnetic interference. UTP cables come in various categories, such as Cat 5e, Cat 6, and Cat 7, each offering different levels of performance.

- Shielded Twisted Pair (STP): STP cables have an extra layer of shielding to protect against interference. They are used in environments with higher electromagnetic interference.

2. Coaxial Cable: - Coaxial cables consist of a central conductor surrounded by insulation, a metallic shield, and an outer insulating layer. Coaxial cables are commonly used for cable television (CATV) and in older Ethernet networks. They provide better shielding against interference compared to twisted pair cables.

3. Fiber-Optic Cable:

- Fiber-optic cables use light to transmit data signals. They consist of a core made of glass or plastic fibers and are known for their high bandwidth and immunity to electromagnetic interference. Fiber-optic cables are commonly used in long-distance and high-speed data transmission, such as in backbone networks and telecommunications.

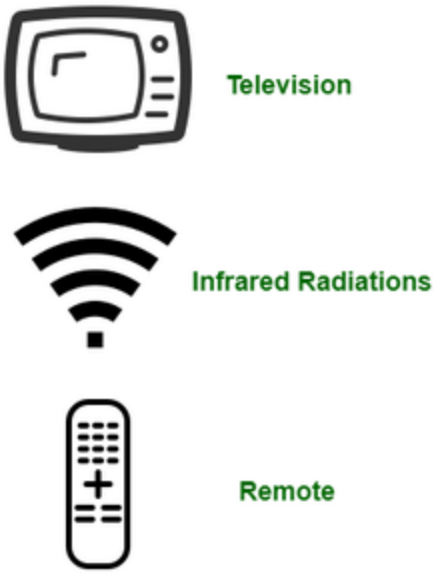
4. Power Line Communication (PLC):

- PLC uses existing electrical power lines for data communication. It allows data signals to be transmitted over the same electrical wires that provide power to devices. PLC is often used for home networking and in certain industrial applications.

power line communication have specific use cases, and their adoption is influenced by factors like legacy infrastructure and cost considerations.

In contrast to guided transmission media, unguided transmission media, such as wireless communication, rely on the transmission of data through the air (e.g., radio waves or

WIRELESS TRANSMISSION MEDIA



Wireless transmission media in computer networks refer to communication methods that transmit data without the need for physical cables or wires. Wireless communication has become increasingly prevalent due to its convenience, flexibility, and the ability to support various devices, including smartphones, laptops, tablets, IoT devices, and more. There are several key wireless transmission media used in computer networks:

1. Wi-Fi (Wireless Local Area Network): Wi-Fi is a widely used wireless technology for connecting devices within a limited area, such as homes, offices, and public spaces. It uses radio waves to transmit data between Wi-Fi-enabled devices and access points (routers). Wi-Fi standards, such as 802.11ac and 802.11ax (Wi-Fi 6), provide various data rates and ranges, making it suitable for both short-range and high-speed connections.

2. Cellular Networks: Cellular networks, including 3G, 4G, and 5G, are used for mobile communication. They provide wireless connectivity to smartphones, tablets, and other mobile devices over large geographic areas. Cellular networks are designed for voice and data services and offer different levels of speed and coverage, with 5G being the latest generation offering ultra-fast data rates.

3. Bluetooth: Bluetooth is a short-range wireless technology commonly used for connecting devices like headphones, keyboards, mice, and IoT devices. It operates in the 2.4 GHz ISM band and supports low-power, short-range communications.

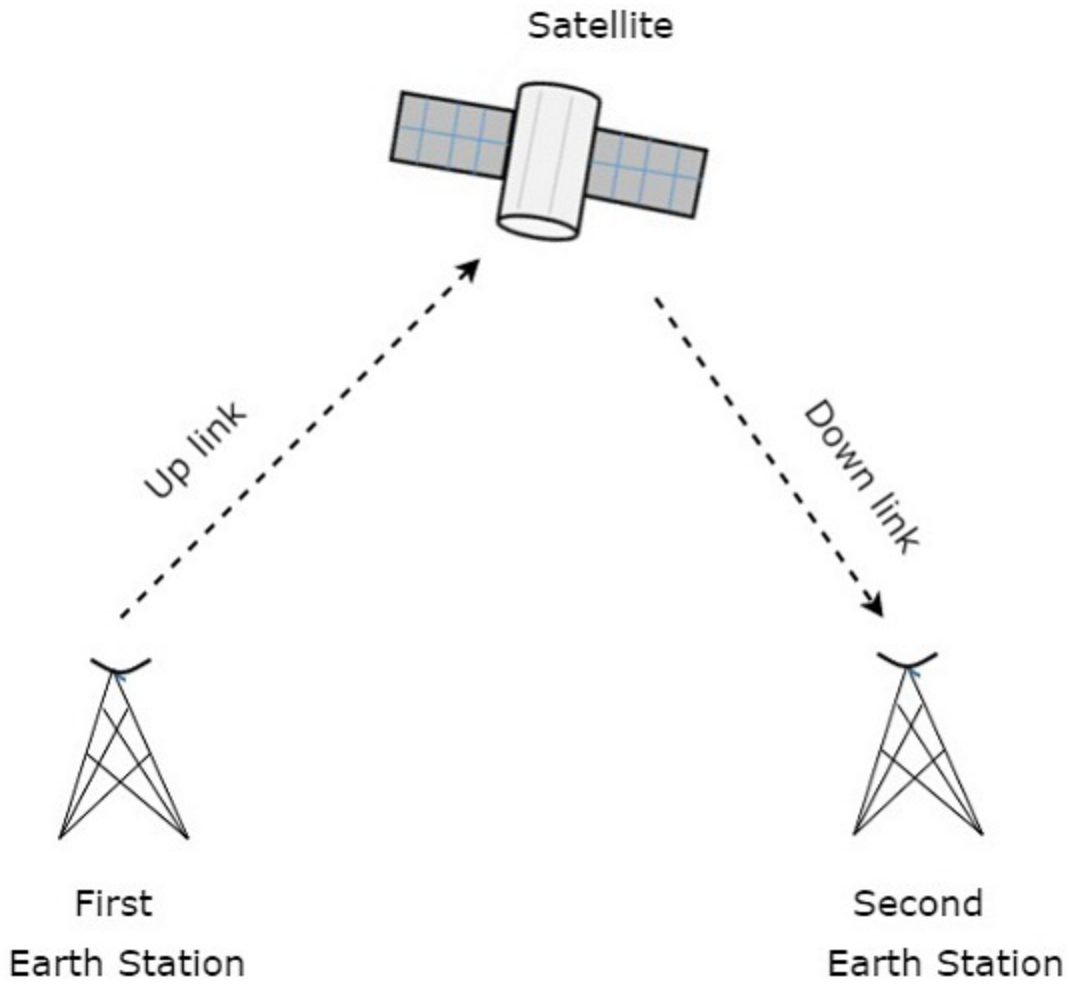
4. Zigbee:Zigbee is a wireless communication protocol designed for low-power, low-data-rate applications in home automation, industrial control, and sensor networks. It is known for its ability to create mesh networks and operate on unlicensed radio frequencies.

5. NFC (Near Field Communication): NFC is a short-range wireless communication technology used for contactless data exchange between devices when they are brought into close proximity. It is often used for mobile payments and data transfer.

6.RFID (Radio-Frequency Identification): RFID is a wireless technology used for identifying and tracking objects, animals, and people. It employs radio frequency signals to exchange data between RFID tags and readers.

7. Satellite Communication: Satellite communication involves the use of geostationary or low Earth orbit (LEO) satellites to provide wireless connectivity for long-distance and global communication. This technology is used for services like satellite TV, global positioning systems (GPS), and satellite internet.

COMMUNICATION SATELLITE



Communication satellites play a crucial role in computer networks and global communication systems by providing long-distance and wide-area connectivity. These satellites are used to transmit data and signals over vast geographical areas, making it possible for devices and networks to communicate across long distances, including regions where traditional wired infrastructure may be impractical or unavailable. Here are key aspects of communication satellites in computer networks:

1. **Transmission of Data:** Communication satellites function as relays in the sky, receiving data signals from one location on Earth and retransmitting them to another location on Earth or to other satellites. They are used to facilitate data transmission for

various purposes, including internet connectivity, television broadcasting, telecommunication, and data backhaul.

2. **Internet Connectivity:** Satellites play a vital role in providing internet connectivity, particularly in remote or underserved areas. Geostationary communication satellites, which orbit the Earth at the same speed as its rotation, can cover large geographic regions, making them suitable for broadband internet access in rural or isolated locations.

3. **Telecommunication:** Communication satellites enable long-distance telecommunication services, including voice calls, video conferencing, and data communication. These services are often delivered through satellite phones and satellite communication systems.

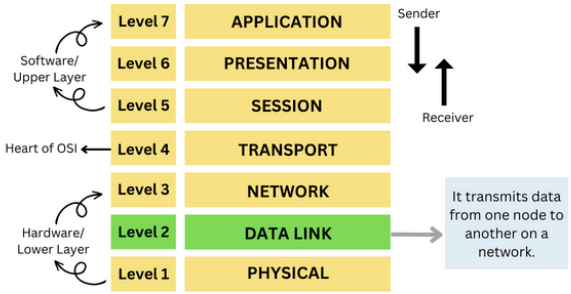
4. **Television Broadcasting:** Many television networks use communication satellites to distribute their programming to a wide audience. Satellite television services transmit signals from broadcasting stations to satellite dishes, which then deliver content to individual viewers' homes.

5. **Global Positioning System (GPS):** The GPS system relies on a constellation of satellites in orbit to provide accurate positioning and timing information to GPS-enabled devices, such as smartphones and navigation systems.

6. **Data Backhaul:** Communication satellites are used for data backhaul in regions where terrestrial connections are limited or not cost-effective. They serve as a means of transmitting data from remote locations to centralized data centers or the internet.

7. **Disaster Recovery and Emergency Communication:** Communication satellites are valuable in disaster recovery scenarios and emergency communication. They provide a means of maintaining communication when terrestrial infrastructure has been damaged or disrupted.

DATA LINK LAYER



The OSI Model: Data Link Layer

The Data Link Layer is the second layer in the OSI (Open Systems Interconnection) model and the TCP/IP model, and it plays a crucial role in computer networks. This layer is responsible for facilitating the error-free and reliable transmission of data between devices on the same network segment. The Data Link Layer is divided into two sublayers: the Logical Link Control (LLC) sublayer and the Media Access Control (MAC) sublayer. Here's an overview of the functions and responsibilities of the Data Link Layer:

1. **Framing:** The Data Link Layer frames data received from the Network Layer above it into smaller, manageable packets for transmission over the physical medium. These frames often include control information, such as source and destination addresses, error-checking codes, and sequence numbers.

2. **Addressing:** Each device on a network segment has a unique MAC address, which is assigned at the Data Link Layer. This address is used for identifying the source and destination devices when data is transmitted within the same network segment.

3. **Error Detection and Correction:** The Data Link Layer performs error detection by adding checksums or cyclic redundancy checks (CRC) to each frame. If errors are detected in received frames, they can be corrected or retransmitted, depending on the specific protocol in use.

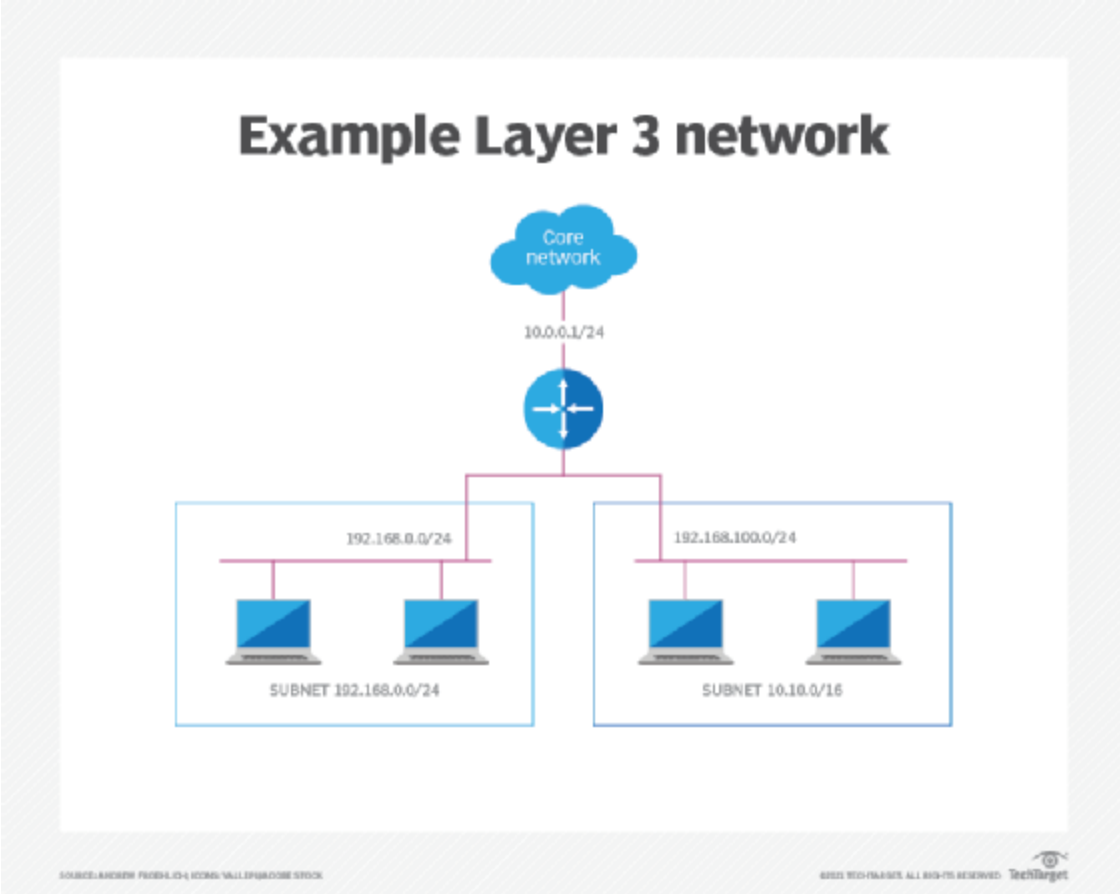
4. **Flow Control:** Flow control mechanisms are used to manage the rate of data transmission between devices to ensure that the sender does not overwhelm the receiver. This is important in preventing data loss due to buffer overflows.

5. **Access Control:** In shared network segments, the Data Link Layer is responsible for managing access to the transmission medium. It uses Media Access Control (MAC) protocols, such as Ethernet's CSMA/CD (Carrier Sense Multiple Access with Collision Detection) or CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) for wireless networks.

The Data Link Layer ensures that data is reliably transmitted within a network segment and provides the foundational framework for the higher-layer protocols to function. Different types of data link protocols may be used, depending on the specific network technology in

use, such as Ethernet, Token Ring, or wireless protocols like Wi-Fi. This layer helps create a reliable communication channel within a single network segment or broadcast domain, making it a fundamental part of network communication.

NETWORK LAYER



The Network Layer is the third layer in the OSI (Open Systems Interconnection) model and the TCP/IP model of computer networking. It plays a vital role in the process of routing data packets from the source to the destination across multiple networks. The Network Layer provides logical addressing, routing, and data fragmentation and reassembly, among other key functions. Here are the primary responsibilities and functions of the Network Layer:

1. **Logical Addressing:** The Network Layer assigns logical addresses to devices on a network. The most common type of logical address is the IP address (e.g., IPv4 or IPv6). These addresses are used to uniquely identify devices on a network and to determine the network to which they belong.

2. **Routing:** The Network Layer is responsible for determining the best path for data packets to travel from the source to the destination. This involves selecting the appropriate routes and routers to forward the packets. Routing decisions are made based on the destination IP address, network topology, and routing algorithms.

3. **Forwarding:** Once a router in the network makes a routing decision, it forwards the data packets to the next hop along the chosen path. Forwarding is the process of actually moving data packets from one router to another until they reach their final destination.

4. **Data Fragmentation and Reassembly:** The Network Layer can break down large data packets into smaller fragments for transmission over networks with lower Maximum Transmission Unit (MTU) sizes. It also handles the reassembly of these fragments at the destination.

The Network Layer is critical for enabling end-to-end communication between devices on different networks and for ensuring that data packets find their way to their intended .