WELCOME TO LEARN COMPUTER NETWORK

```
AUTHOR:         Yatharth Chauhan  (Github: YatharthChauhan2362)
SUBJECT:        Computer Network
REPOSITORY:     Learning-Computer-Network
```

CHAPTER-1: Computer Networks and the Internet

OSI Model

Computer networks are typically organized into layers, with each layer responsible for a specific set of functions that interact with other layers to provide end-to-end communication. The most commonly used reference model for network layering is the Open Systems Interconnection (OSI) model, which consists of seven layers.

The seven layers of the OSI model are as follows:

1. Physical Layer:

- This layer is responsible for the transmission and reception of raw bit streams over a physical medium, such as a copper or fiber optic cable.

2. Data Link Layer:

- This layer is responsible for providing error-free transmission of data frames over the physical layer, as well as detecting and correcting errors.

3. Network Layer:

- This layer is responsible for routing packets between different networks, and for addressing and forwarding packets based on logical addresses.

4. Transport Layer:

- This layer is responsible for providing reliable end-to-end communication between applications, as well as for managing flow control and congestion control.

5. Session Layer:

- This layer is responsible for establishing and maintaining communication sessions between applications, and for managing session synchronization and recovery in the event of failures.

6. Presentation Layer:

- This layer is responsible for transforming data from the format used by the application into a format that can be transmitted over the network, and vice versa. It is also responsible for encryption and decryption of data.

7. Application Layer:

- This layer is responsible for providing network services to applications, and for interacting with the user through application interfaces.

TCP/IP model

The TCP/IP model is a networking protocol suite that is used to establish communication between devices on a network. It is composed of four layers, each of which is responsible for a different aspect of network communication:

1. Application layer:

- This layer is responsible for providing services to applications that are running on the network. Some of the protocols that operate at this layer include HTTP, FTP, SMTP, and Telnet.

2. Transport layer:

- This layer is responsible for ensuring that data is transmitted reliably between devices. The two most common protocols that operate at this layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

3. Internet layer:

- This layer is responsible for routing data between networks. The Internet Protocol (IP) operates at this layer, and it is used to address and route data packets across the internet.

4. Link layer:

- This layer is responsible for transmitting data between adjacent network nodes. It includes the physical and data link layers, which are responsible for transmitting data over a physical medium and providing error detection and correction mechanisms.

Types of Network

A computer network is a group of interconnected devices that can communicate with each other to share resources and information. The most common types of computer networks are:

1. Local Area Network (LAN):

- A LAN is a network that is limited to a small geographic area, such as a single building or campus. It typically uses wired or wireless connections to connect devices together.

2. Wide Area Network (WAN):

- A WAN is a network that spans a large geographic area, such as a city, country, or even the entire world. It typically uses a combination of wired and wireless connections, such as telephone lines, satellite links, and fiber optic cables, to connect devices together.

3. Metropolitan Area Network (MAN):

- A MAN is a network that covers a larger geographic area than a LAN but is smaller than a WAN. It is typically used to connect multiple LANs together within a city or metropolitan area.

4. Personal Area Network (PAN):

- A PAN is a network that connects devices in close proximity to each other, such as a smartphone, tablet, and laptop. It typically uses wireless connections, such as Bluetooth or Wi-Fi, to connect devices together.

Components of Network

There are several components that make up a computer network, including:

1. Network Interface Cards (NICs):

- NICs are hardware devices that enable computers to connect to a network. They typically use Ethernet cables to connect to a LAN and Wi-Fi to connect to a wireless network.

2. Switches:

- Switches are hardware devices that enable devices to communicate with each other within a network. They route data between devices based on their unique MAC addresses.

3. Routers:

- Routers are hardware devices that enable devices to communicate with each other across different networks. They route data between networks based on their unique IP addresses.

4. Modems:

- Modems are hardware devices that enable devices to connect to the internet through a WAN. They typically use telephone lines or cable lines to connect to the internet service provider (ISP).

5. Firewalls:

- Firewalls are software or hardware devices that protect a network from unauthorized access. They control access to a network by monitoring and filtering incoming and outgoing traffic.

Protocols

In networking, a protocol refers to a set of rules or standards that govern the way devices communicate with each other over a network. A protocol determines how data is transmitted, received, and processed over the network.

Protocols are essential for enabling communication between different devices and ensuring that the data is transmitted correctly and reliably. There are many different types of protocols used in networking, including:

1. Transmission Control Protocol/Internet Protocol (TCP/IP)

- This is the most widely used protocol suite for communication on the internet.

2. User Datagram Protocol (UDP)

- A lightweight protocol used for quick data transmission where reliability is not the primary concern.

3. Hypertext Transfer Protocol (HTTP)

- A protocol used for transmitting web pages and other data over the internet.

4. Simple Mail Transfer Protocol (SMTP)

- A protocol used for sending email messages over the internet.

5. File Transfer Protocol (FTP)

- A protocol used for transferring files between computers over the internet.

Each protocol has its own specific set of rules and standards that devices must follow to ensure successful communication.

Access Networks

Access networks, in networking, refer to the portion of a telecommunications network that connects subscribers or end-users to the core network or the internet.

There are different types of access networks, including:

1. Wired access networks

- These networks use physical cables, such as copper or fiber optic cables, to connect end-users to the network. Examples of wired access networks include Digital Subscriber Line (DSL), cable modem, and Ethernet.

2. Wireless access networks

- These networks use wireless signals, such as radio waves or microwave, to connect end-users to the network. Examples of wireless access networks include Wi-Fi, cellular networks, and satellite networks.

Access networks are essential for providing users with access to network services, such as the internet, voice, and video. They also play a crucial role in determining the quality of service that end-users receive, including factors such as bandwidth, latency, and reliability.

In summary, access networks are the final link between end-users and the telecommunications network or the internet. They are critical to providing access to network services and determining the quality of service that end-users receive.

Physical media

Physical media in networking refers to the type of cables and wires that are used to transmit data between devices on a network. There are several types of physical media commonly used in networking:

1. Twisted Pair:

- Twisted pair cables are the most commonly used type of cable in networking. They consist of pairs of copper wires twisted together to reduce interference and crosstalk.

2. Coaxial Cable:

- Coaxial cable is a type of cable consisting of a central conductor surrounded by an insulating layer, a conductive shield, and a protective outer jacket. It is used in cable television and some networking

applications.

3. Fiber Optic Cable:

- Fiber optic cable uses thin strands of glass or plastic to transmit data over long distances. It offers very high bandwidth and is used in high-speed networking applications.

4. Wireless:

- Wireless networking uses radio waves to transmit data between devices. It eliminates the need for physical cables but can be affected by interference from other devices.

The choice of physical media depends on factors such as the distance between devices, the speed of the network, and the level of interference present in the environment.

Packet Switching & Circuit Switching

Packet switching and circuit switching are two different methods of transmitting data over a network.

Circuit Switching

- Circuit switching is an older technology that is used in traditional telephone networks. It works by creating a dedicated physical connection, or circuit, between two devices for the duration of the communication. The circuit is reserved exclusively for the two devices and cannot be used by anyone else. This means that the communication is uninterrupted, but it also means that the circuit remains occupied even when no data is being transmitted, leading to inefficient use of resources.

Packet switching

- Packet switching, on the other hand, is the method used in modern computer networks, including the internet. In packet switching, data is broken down into small packets and sent over the network individually. Each packet contains a portion of the data, as well as the address of its destination. The packets travel through the network separately and can take different paths to reach their destination. When they arrive at their destination, they are reassembled into the original message. Packet switching allows multiple devices to share the same network resources, which makes it more efficient than circuit switching.

In summary, circuit switching creates a dedicated physical connection between two devices for the duration of the communication, while packet switching breaks data down into small packets and sends them individually over the network, allowing multiple devices to share the same network resources. Packet switching is the method used in modern computer networks, while circuit switching is an older technology used in traditional telephone networks.

Delay and Loss

Delay refers to the time it takes for data to travel from one point to another in a network. There are several types of delay that can occur in a network:

1. Transmission delay: The time it takes for a node to transmit data onto the network.

2. Propagation delay: The time it takes for data to travel from one end of a network to the other.

3. Processing delay: The time it takes for a node to process data before transmitting it onto the network.
4. Queuing delay: The time it takes for data to wait in a queue before it can be transmitted.
5. Network congestion delay: The time it takes for data to be delayed due to congestion in the network.

On the other hand, loss in networking refers to the situation where some of the transmitted data is not received at the destination. There are several reasons why data loss can occur in a network, including:

1. Network congestion: When the network is congested, packets may be dropped to alleviate the congestion.
2. Interference: Physical interference in the network can cause data loss.
3. Faulty equipment: Malfunctioning hardware can cause packets to be lost.
4. Errors in data transmission: Transmission errors can cause packets to be lost or corrupted.

Both delay and loss can impact the performance and reliability of a network, and therefore it is important to monitor and manage these issues in order to maintain a high-quality network.

Throughput in Packet-switched

Throughput is the amount of data that can be transmitted over a network in a given amount of time. In packet-switched networks, throughput is affected by several factors, including the size of the packets, the available bandwidth, and the number of packets being transmitted.

Packet-switched networks divide data into packets, which are sent individually across the network and reassembled at the destination. The size of the packets can affect the throughput of the network, as larger packets take longer to transmit than smaller packets. However, larger packets can be more efficient, as there is less overhead associated with transmitting a larger number of smaller packets.

Bandwidth is another factor that affects the throughput of packet-switched networks. Bandwidth refers to the amount of data that can be transmitted over the network in a given amount of time. A network with a high bandwidth can transmit more data in a given amount of time than a network with a lower bandwidth.

Finally, the number of packets being transmitted can also affect the throughput of a packet-switched network. As more packets are transmitted, the network may become congested, which can result in delays and packet loss. This can reduce the overall throughput of the network.

To optimize throughput in packet-switched networks, it is important to balance the size of the packets with the available bandwidth and to manage congestion to minimize delays and packet loss. Network administrators may use tools such as Quality of Service (QoS) to prioritize traffic and manage congestion in order to maximize network throughput.

Queuing Delay and Packet Loss

Queuing delay and packet loss are common issues in packet-switched networks.

Queuing delay occurs when packets are stored in a buffer or queue before they can be forwarded to their destination. The amount of time a packet spends in the queue depends on the network traffic and the available network resources. When the queue is full, packets are dropped, resulting in packet loss.

Packet loss can also occur due to other factors, such as:

1. Network congestion: When the network is congested, packets may be dropped to prevent the network from becoming overloaded.
2. Transmission errors: Errors in the transmission medium or interference can cause packets to be lost.
3. Faulty network hardware: Faulty hardware, such as routers or switches, can also cause packet loss.

Packet loss can have a significant impact on network performance, as lost packets need to be retransmitted, resulting in additional delay and network congestion. To mitigate packet loss, various techniques can be used, such as congestion control algorithms, packet retransmission mechanisms, and network redundancy.

End-to-End Delay

End-to-end delay in networking refers to the time it takes for a packet to travel from the source to the destination, including all the delays incurred in the intermediate network devices such as routers, switches, and links. It is a critical performance metric that impacts the quality of service (QoS) experienced by the end-users.

End-to-end delay can be divided into four components:

1. Transmission delay: The time taken to transmit the packet over the physical link, which is proportional to the size of the packet and the bandwidth of the link.
2. Propagation delay: The time taken for the packet to travel from the source to the destination, which is proportional to the distance between the two endpoints.
3. Processing delay: The time taken by the network devices to process the packet headers and perform routing and switching operations.
4. Queuing delay: The time taken by the packet to wait in the buffer of a network device before it is forwarded to the next hop.

The total end-to-end delay is the sum of these four components. Minimizing end-to-end delay is crucial for time-sensitive applications such as real-time communication, online gaming, and video streaming, which require low latency to provide a smooth user experience.

Throughput in Computer Networks

Throughput in computer networks refers to the amount of data that can be transmitted through the network in a given time period. It is typically measured in bits per second (bps), kilobits per second (Kbps), megabits per second (Mbps), or gigabits per second (Gbps).

Throughput is affected by a number of factors, including the available bandwidth, the latency of the network, the size of the data packets being transmitted, the number of devices on the network, and the efficiency of the network protocols being used.

There are various methods used to measure throughput, including network performance testing tools like iperf, which can generate traffic and measure the resulting throughput, and network analyzers, which can capture and analyze the traffic on a network to determine its throughput.

Network administrators and engineers often monitor throughput to ensure that the network is performing optimally and to identify and troubleshoot any performance issues that may arise. They may also use techniques like traffic shaping and Quality of Service (QoS) to manage the flow of network traffic and prioritize critical applications and services.

Primer on Latency and Bandwidth

Latency and bandwidth are two key concepts that are fundamental to understanding how computer networks operate. In this primer, we'll define what latency and bandwidth are, explore how they affect network performance, and provide some examples of each.

1. Latency

Latency is the time it takes for a packet of data to travel from one point to another in a network. Latency is often referred to as "delay" and is usually measured in milliseconds (ms). Latency can be affected by a variety of factors, including the physical distance between devices, the speed of the devices, the amount of traffic on the network, and the quality of the connection.

Latency can have a significant impact on network performance, particularly for real-time applications such as video conferencing, online gaming, and VoIP (Voice over Internet Protocol) calls. High latency can result in delays and lag, which can make these applications difficult or impossible to use.

2. Bandwidth

Bandwidth is the amount of data that can be transmitted over a network in a given amount of time. Bandwidth is usually measured in bits per second (bps), kilobits per second (kbps), or megabits per second (Mbps). The higher the bandwidth, the more data that can be transmitted at once.

Bandwidth can be limited by the capacity of the network infrastructure, such as the cables or routers used, as well as the amount of traffic on the network. Bandwidth can also be affected by network congestion, which occurs when there are too many devices trying to use the network at the same time.

Bandwidth is important for applications that require the transfer of large amounts of data, such as video streaming, file sharing, and cloud computing. Higher bandwidth can also improve the overall speed and responsiveness of a network.

3. Latency vs. Bandwidth

Latency and bandwidth are both important factors that can affect network performance, but they are not the same thing. Latency refers to the delay in transmitting data from one point to another, while bandwidth refers to the amount of data that can be transmitted at once.

In general, low latency is important for real-time applications that require fast response times, while high bandwidth is important for applications that require the transfer of large amounts of data. However, both factors are important for overall network performance, and network administrators need to balance both factors when designing and maintaining a network.

Examples

Here are some examples of how latency and bandwidth can affect network performance:

- A video conference call may experience lag and delays if there is high latency on the network.
- A file transfer may take a long time to complete if the network has low bandwidth.
- Online gaming may be difficult to play if there is high latency, as the game may not respond quickly to player actions.
- Video streaming may be slow and buffer frequently if there is low bandwidth on the network.

In summary, latency and bandwidth are two key concepts that are fundamental to understanding how computer networks operate. Latency refers to the delay in transmitting data from one point to another, while bandwidth refers to the amount of data that can be transmitted at once. Both factors are important for overall network performance, and network administrators need to balance both factors when designing and maintaining a network.