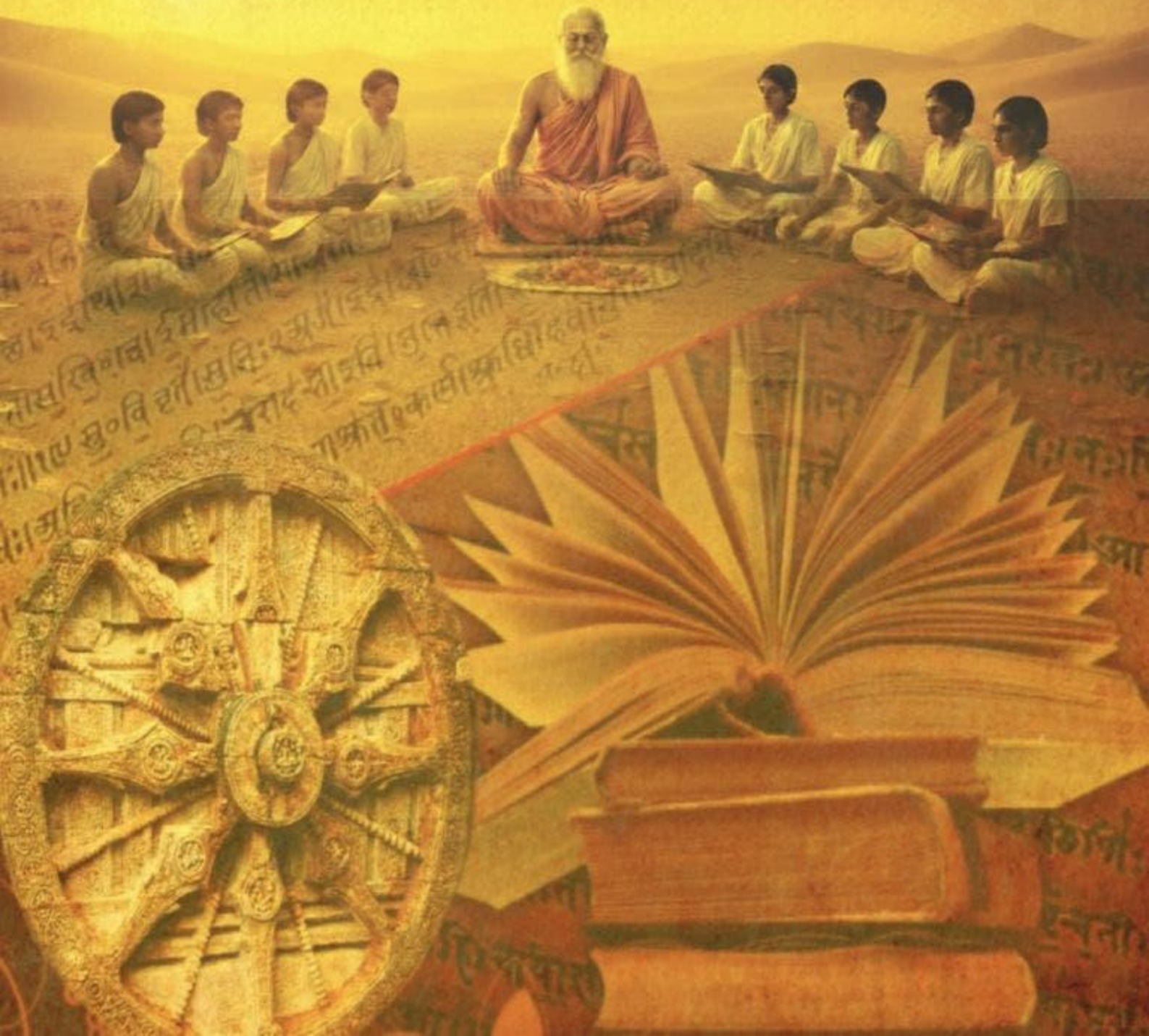
भारतीय ज्ञान प्रणाली
उद्गम और विकास

सम्पादक :
डॉ. दिनेश चन्द्र शर्मा



भारतीय ज्ञान प्रणाली
उद्‌गम और विकास

सम्पादक :

डॉ. दिनेश चन्द्र शर्मा

Ph.D., D.Lit. (Sub.)

निदेशक, कॉम्पिटिशन प्लस ग्रुप ऑफ इन्स्टीट्यूशन,
अजमेर

Books n Books

51/1509, आचमन, वेदविहार,
लोहाखान, अजमेर-305001

प्रकाशक :

पुष्पा शर्मा

Books n Books

51/1509, आचमन, वेदविहार,

लोहाखान, अजमेर-305001

ई-मेल : bnbajmer@gmail.com

मो. 9660111549

संस्करण

प्रथम 2026

***ISBN :* 978-81-993854-1-2**

मूल्य - 400/-

रचना - भारतीय ज्ञान प्रणाली-उद्गम और विकास

सम्पादक - डॉ. दिनेश चन्द्र शर्मा

आवरण - श्रीनिवास प्रिन्टोग्राफिक्स, अजमेर

मुद्रक

श्रीनिवास प्रिन्टोग्राफिक्स, अजमेर

25

Computer Network Devices

Gorav Palasia
Assistant Professor (Deptt. of Science and Technology)
Hukumchand Noble Institute of Science and Technology

Introduction:

Computer network devices play a vital role in enabling communication and data exchange between computers, servers, and other digital systems. In today's interconnected world, almost every application-such as the internet, cloud computing, online banking, e-commerce, social media, and mobile communication-depends on efficient and reliable computer networks. Network devices form the backbone of these networks by managing, directing, and securing the flow of data from one point to another. A computer network consists of multiple devices connected together to share information and resources. Network devices are the hardware components that make this connectivity possible. They help in transmitting data signals, controlling network traffic, extending network range, and ensuring that data reaches the correct destination. Without these devices, computers would not be able to communicate with each other effectively.

Different network devices perform different functions based on their design and purpose. For example, a Network Interface Card (NIC) allows a computer to connect to a network, while switches and routers manage data flow within and between networks. Devices such as hubs and repeaters help extend network coverage, whereas firewalls and gateways provide security and protocol translation. Each device operates at specific layers of the OSI model, contributing to the overall efficiency and reliability of the network. As technology advances, network devices have become more intelligent and powerful. Modern networks require high-speed data transfer, strong security, and reliable connectivity to support applications like IoT, video conferencing, and cloud services. Understanding computer

network devices is therefore essential for students, IT professionals, and anyone interested in networking. A clear knowledge of these devices helps in designing, managing, and maintaining secure and efficient communication networks in both small and large-scale environments.

What are Computer Network Devices?

Computer network devices are hardware components that connect various computers, servers, and other digital devices within a network. These devices enable communication by transmitting, receiving, and managing data between connected systems. They play a crucial role in ensuring that information flows smoothly and efficiently across the network.

Network devices control how data is sent from one device to another and determine the correct path for data transmission. They help manage network traffic, reduce data collisions, and maintain reliable communication. In addition, many network devices are responsible for providing security by monitoring data flow and preventing unauthorized access. By using computer network devices, data is delivered to the correct destination at the right time and in a secure manner. Without these devices, modern computer networks and internet-based services would not be possible.

Classification of Network Devices :

Network devices can be classified based on their functions and the layers of the OSI (Open Systems Interconnection) model at which they operate. This classification helps in understanding how different devices contribute to data communication and network management. Each category performs specific tasks to ensure efficient, reliable, and secure networking.

1. Physical Layer Devices :

Physical layer devices operate at the lowest layer of the OSI model. Their main function is to transmit raw data bits in the form of electrical, optical, or radio signals over the physical medium. These devices do not understand data frames or addresses; they simply handle signal transmission.

Common physical layer devices include repeaters, hubs, and network cables. Repeaters regenerate weak signals to extend network distance, while hubs broadcast incoming data to all connected

devices. These devices are simple, cost-effective, and mainly used to increase network reach, but they offer no data filtering or security features.

2. Data Link Layer Devices :

Data link layer devices operate at the second layer of the OSI model. Their primary role is to manage data frames and ensure error-free communication between devices on the same network. These devices use MAC (Media Access Control) addresses to identify source and destination devices.

Examples of data link layer devices include bridges and switches. Bridges divide a network into segments to reduce congestion, while switches intelligently forward data only to the intended recipient. This improves network performance, reduces collisions, and enhances security compared to physical layer devices.

3. Network Layer Devices :

Network layer devices function at the third layer of the OSI model and are responsible for routing data between different networks. They use IP addresses to determine the best path for data transmission.

The most common network layer device is the router. Routers connect multiple networks, manage traffic efficiently, and enable internet access. They also support features such as traffic control, load balancing, and basic security functions.

4. Security and Management Devices :

Security and management devices are designed to protect networks and optimize performance. These include firewalls, proxy servers, Intrusion Detection/Prevention Systems (IDS/IPS), and load balancers. They monitor traffic, prevent unauthorized access, and ensure reliable and secure network operations.

1. Network Interface Card (NIC) :

A Network Interface Card (NIC) is a hardware component that enables a computer or device to connect to a network. It is also known as a LAN card or network adapter. Without a NIC, a computer cannot communicate with other devices over a network. The NIC acts as an interface between the computer and the network medium, such as cables or wireless signals.

Types Of NIC :

Wired NIC (Ethernet Card): Uses physical cables like Ethernet

to connect to a network. It provides high speed, stable, and secure communication.

Wireless NIC (Wi-Fi Card): Uses radio waves to connect to a wireless network. It provides mobility and flexibility but may be affected by interference.

Functions of NIC :

* Converts data into digital signals suitable for transmission
* Provides a unique MAC (Media Access Control) address
* Establishes communication between the computer and the network

2. Repeater

A repeater is a networking device that operates at the Physical Layer (Layer 1) of the OSI model. When data is transmitted over long distances, the strength of the signal gradually decreases due to attenuation, noise, and interference. As a result, the signal may become too weak to be correctly received at the destination. A repeater is used to solve this problem by regenerating and strengthening the signal.

The repeater receives the weak or distorted signal, cleans it, and then retransmits it in its original form. In this way, it helps data travel longer distances without loss of quality. Repeaters are commonly used in long cable networks and wireless communication systems to extend the coverage area.

Functions of a Repeater :

1. Amplifies weak signals:

The primary function of a repeater is to regenerate weak signals. It restores the signal to its original strength and shape before forwarding it.

2. Extends network length:

By placing repeaters between network segments, the overall length of the network can be increased beyond the normal cable limitations.

Limitations of a Repeater

1. Does not filter data:

A repeater does not examine the data it transmits. It simply forwards all signals, including corrupted or unwanted data.

2. Cannot control network traffic:

Since a repeater has no intelligence, it cannot manage traffic,

reduce congestion, or prevent collisions in the network.

3. Cannot improve network security:

A repeater does not provide any security features. It allows all data to pass through without authentication or access control, making it unsuitable for secure networks.

3. Hub :

A hub is a basic networking device that works at the Physical Layer (Layer 1) of the OSI model. It is often referred to as a multi-port repeater because it connects multiple devices such as computers, printers, and servers within a network. All devices connected to a hub share the same communication medium.

When a hub receives data from one connected device, it broadcasts the data to all other devices connected to it, regardless of the intended destination. The receiving devices check the destination address, and only the correct device accepts the data while others discard it. Due to this broadcasting nature, hubs are mostly used in small and simple networks.

Types of Hub :

1. Active Hub:

An active hub not only forwards data but also regenerates and amplifies weak signals before sending them to other ports. It requires an external power supply and helps improve signal strength.

2. Passive Hub:

A passive hub simply forwards incoming signals to connected devices without amplifying or regenerating them. It does not require power and does not improve signal quality.

3. Intelligent Hub:

An intelligent hub includes basic management and monitoring features. It allows network administrators to observe traffic, detect faults, and perform limited control operations.

Disadvantages of Hub :

1. Broadcast traffic causes congestion:

Since a hub sends data to all connected devices, unnecessary traffic increases, leading to network congestion and frequent collisions.

2. Low security:

All data is visible to every device connected to the hub, making

it easy for unauthorized users to capture sensitive information.

3. Poor performance in large networks:

As the number of connected devices increases, performance decreases significantly due to excessive collisions and shared bandwidth.

4. Bridge :

A bridge is a networking device that operates at the Data Link Layer (Layer 2) of the OSI model. It is used to connect two or more network segments and make them work as a single network. The main purpose of a bridge is to divide a large network into smaller segments, which helps improve overall network performance.

Unlike hubs and repeaters, a bridge is an intelligent device. It can examine incoming data frames and decide whether to forward or discard them based on MAC (Media Access Control) addresses. By doing this, a bridge reduces unnecessary traffic and improves network efficiency.

Functions of a Bridge :

1. Filters data using MAC addresses:

A bridge maintains a MAC address table that records the addresses of devices connected to each network segment. When a frame arrives, the bridge checks the destination MAC address.

* If the destination is on the same segment, the frame is not forwarded.

* If the destination is on a different segment, the frame is forwarded only to that segment.

2. Reduces collisions:

By dividing a large network into smaller segments, a bridge reduces the number of devices competing for the same transmission medium. This helps decrease data collisions and improves communication reliability.

3. Improves network efficiency:

Since only necessary data is forwarded, bandwidth is used more effectively. This results in faster data transmission and better overall network performance.

Advantages of Bridge :

* Improves network performance
* Reduces unnecessary traffic

* Allows network expansion without major changes

5. Switch :

A switch is an advanced networking device that operates mainly at the Data Link Layer (Layer 2) of the OSI model, though some switches also work at the Network Layer (Layer 3). It is widely used in modern Local Area Networks (LANs) to connect multiple devices such as computers, printers, and servers.

Unlike hubs, a switch intelligently forwards data only to the intended destination device. It uses MAC (Media Access Control) addresses to identify devices connected to its ports. When a data frame arrives, the switch checks the destination MAC address in its MAC address table and sends the data only to the correct port. This selective forwarding improves network efficiency and performance.

Types of Switch :

1. Managed Switch:

A managed switch allows configuration, monitoring, and control of the network. Network administrators can manage traffic, set security rules, and monitor performance.

2. Unmanaged Switch:

An unmanaged switch is a plug-and-play device that does not require any configuration. It is commonly used in small networks or homes.

3. Layer 2 Switch:

A Layer 2 switch operates at the Data Link Layer and forwards data using MAC addresses.

4. Layer 3 Switch:

A Layer 3 switch can perform routing functions using IP addresses, combining the features of a switch and a router.

Advantages of Switch :

1. High-speed data transfer:

Switches support fast data transmission and full-duplex communication, improving network speed.

2. Better security:

Data is sent only to the intended device, reducing the risk of unauthorized access.

3. Reduced network traffic:

Since data is not broadcast to all devices, unnecessary traffic

is minimized.

4. No data collisions:

Each port of a switch creates a separate collision domain, eliminating data collisions.

6. Router :

A router is an important networking device that operates at the Network Layer (Layer 3) of the OSI model. It is used to connect two or more different networks and route data packets between them. Routers forward data based on IP (Internet Protocol) addresses, unlike switches which use MAC addresses. One of the most common uses of a router is to connect a local area network (LAN) to the Internet.

When a data packet arrives, the router examines its destination IP address and decides the best possible path for the packet to reach its destination. This decision is made using routing tables and routing algorithms. Because of this capability, routers play a vital role in efficient and reliable data communication.

Functions of a Router :

1. Determines the best path for data transmission:

A router analyzes available routes and selects the most efficient path for forwarding data packets.

2. Provides internet connectivity:

Routers connect home or office networks to Internet Service Providers (ISPs), enabling internet access.

3. Controls traffic flow:

Routers manage network traffic by directing data packets efficiently and preventing congestion.

Types of Router :

1. Wired Router:

A wired router connects devices using Ethernet cables. It is commonly used in offices and fixed network setups.

2. Wireless Router:

A wireless router provides internet access through Wi-Fi, allowing devices such as laptops and smartphones to connect without cables.

3. Core Router:

A core router operates within the backbone of a network and

handles large volumes of data at very high speeds.

4. Edge Router:

An edge router is placed at the boundary of a network and connects it to external networks such as the Internet.

7. Gateway :

A gateway is a networking device that acts as a translator between two different networks or communication protocols. It enables communication between networks that use different architectures, formats, or communication standards. A gateway works at multiple layers of the OSI model, depending on the type of protocol conversion required, making it more advanced than devices like routers and switches.

Unlike routers, which forward data between similar networks, a gateway converts data from one protocol to another so that systems using different technologies can communicate effectively. Because of this translation capability, gateways are commonly used in complex and heterogeneous network environments.

Uses of Gateway :

1. Email systems:

Gateways are used to translate email messages between different email systems and protocols, ensuring smooth message delivery across platforms.

2. VoIP (Voice over Internet Protocol) networks:

In VoIP systems, gateways convert voice signals into digital data and translate between traditional telephone networks (PSTN) and IP-based networks.

3. Internet access between different architectures:

Gateways allow networks with different architectures (such as IPv4 and IPv6 or different operating systems) to communicate with each other over the Internet.

Advantages of Gateway :

* Enables communication between incompatible networks
* Supports protocol conversion
* Essential for large and complex networks

8. Modem :

A modem stands for Modulator-Demodulator. It is a networking device that converts digital signals generated by computers into

analog signals so that they can be transmitted over communication lines such as telephone lines, cable lines, or fiber-optic networks. When signals are received from the network, the modem converts the analog signals back into digital form, allowing the computer to understand the data.

Modems play a crucial role in providing internet connectivity, especially where traditional communication media are used. Without a modem, computers would not be able to communicate over long-distance networks like the Internet.

Working of a Modem :

* Modulation: Converts digital data into analog signals for transmission.

* Demodulation: Converts incoming analog signals back into digital data.

Types of Modem :

1. DSL Modem:

A DSL (Digital Subscriber Line) modem uses existing telephone lines to provide internet access. It allows users to use the internet and telephone simultaneously.

2. Cable Modem:

A cable modem uses cable TV lines to deliver high-speed internet access. It offers faster speeds than DSL and is commonly used in homes.

3. Fiber Modem:

A fiber modem works with fiber-optic cables and provides very high-speed internet connectivity. It is widely used for modern broadband services.

Advantages of Modem

* Enables internet access
* Supports long-distance data communication
* Converts signals accurately for transmission

9. Wireless Access Point (WAP) :

A Wireless Access Point (WAP) is a networking device that allows wireless devices such as laptops, smartphones, and tablets to connect to a wired network using Wi-Fi technology. It acts as a bridge between wired Ethernet networks and wireless users. WAPs are widely used in homes, offices, campuses, and public places to

provide wireless internet access.

A WAP receives data from the wired network and transmits it wirelessly to connected devices. Similarly, it receives data from wireless devices and sends it to the wired network. This makes mobility possible, allowing users to access the network without physical cables.

Uses of Wireless Access Point :

1. Wi-Fi networks:

WAPs are the core devices used to create Wi-Fi networks in homes and organizations. They provide wireless internet connectivity within a defined coverage area.

2. Office and campus networks:

In large offices, colleges, and university campuses, multiple WAPs are installed to ensure seamless wireless coverage and support a large number of users.

3. Public hotspots:

WAPs are commonly used in public places such as airports, cafes, hotels, and shopping malls to offer internet access to visitors.

Advantages of Wireless Access Point :

* Enables wireless connectivity
* Supports multiple devices simultaneously
* Provides mobility and flexibility
* Easy to expand network coverage

10. Firewall :

A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predefined security rules. It acts as a protective barrier between a trusted internal network and untrusted external networks such as the Internet. The main purpose of a firewall is to prevent unauthorized access while allowing legitimate communication.

Firewalls can be implemented as hardware devices, software applications, or a combination of both. They analyze data packets and decide whether to allow or block them based on security policies.

Types of Firewall

1. Hardware Firewall: A hardware firewall is a physical device placed between a network and the Internet. It is commonly used in organizations and provides protection for all connected

devices.

2. Software Firewall: A software firewall is installed on individual computers or servers. It protects a single system by controlling incoming and outgoing traffic.

Functions of Firewall

1. Prevents unauthorized access:

Firewalls block unauthorized users and systems from accessing private networks and sensitive data.

2. Protects the network from attacks:

Firewalls help protect networks from cyber threats such as malware, hacking attempts, and denial-of-service attacks.

3. Monitors network traffic:

Firewalls continuously monitor network activity, log events, and help administrators identify suspicious behavior.

Advantages of Firewall

* Enhances network security
* Controls data access
* Reduces risk of cyber attacks.

☆☆☆