1. As a network administrator of your college, you are required to upgrade your college network, explain the factors you consider while designing the network. [10marks]

As a network administrator upgrading the college network, it is essential to follow a systematic approach to design a network that meets current demands and supports future growth. The key factors to consider are:

1. Requirement Analysis and Objectives

Before starting the design, collect detailed information about:

- **Number of users, devices, and applications** (students, faculty, staff, labs, library systems, etc.).
- **Type of traffic** (video conferencing, VoIP, e-learning portals, cloud applications).
- **Peak usage times** and expected growth rate. This helps determine network size, performance needs, and future scalability.

---

2. Scalability and Flexibility

- The network should support future expansion without requiring major redesigns.
- Choose **modular devices** (stackable switches, scalable routers) and consider IPv6 addressing for long-term growth.
- Include sufficient IP address planning and subnetting to handle device growth.

---

3. Network Topology Design

- Use a **hierarchical network model** (core, distribution, access layers) for better performance and easy management.
- Implement **redundant links and paths** to avoid single points of failure.
- A **hybrid topology** combining wired (for stability) and wireless (for mobility) is suitable for college environments.

---

4. Performance and Bandwidth Planning

- Estimate total bandwidth required for academic activities, online classes, multimedia, and administrative tasks.
- Provide **dedicated backbone links** (fiber optic connections) between buildings.
- Implement **Quality of Service (QoS)** to prioritize latency-sensitive services like VoIP or exam servers.

---

5. Security Considerations

- Deploy **firewalls, intrusion detection/prevention systems (IDS/IPS)**, and secure access controls.
- Use **network segmentation** (VLANs) to isolate traffic (student, faculty, guest).
- Implement **data encryption** (VPN for remote access) and enforce strong authentication policies.

---

6. Reliability and Redundancy

- Install **backup power supplies (UPS, generators)** to ensure uptime.

- Configure **link aggregation and failover mechanisms** to minimize downtime during hardware or link failures.
- Regular backups of configurations and disaster recovery planning are essential.

---

7. Hardware and Cabling Infrastructure

- Choose **enterprise-grade routers, switches, and servers** with high throughput and PoE (Power over Ethernet) support for APs.
- Use **Cat6/Cat6a cables for horizontal wiring** and **fiber optics for backbone connections** to support high speeds.
- Plan structured cabling layouts to make future troubleshooting easier.

---

8. Wireless Network Planning

- Deploy **Wi-Fi 6/6E access points** to handle dense user environments such as classrooms and libraries.
- Perform a **wireless site survey** to ensure proper coverage and avoid dead zones.
- Enable a **Guest Wi-Fi network** for visitors, separate from internal traffic.

---

9. Cost, Budget, and Resource Allocation

- Create a cost-effective plan by balancing performance needs and budget constraints.
- Consider **leasing hardware, using cloud services**, and adopting open-source network management solutions.
- Plan for **training IT staff** for long-term maintenance.

---

10. Standards, Compliance, and Documentation

- Follow **IEEE standards (802.3, 802.11)** and best practices to ensure compatibility.
- Comply with data protection regulations and institutional IT policies.
- Maintain **detailed documentation** of network diagrams, device configurations, and addressing schemes.

---

2. You have been appointed as the Network Manager of the newly opened department store, which does not have a computer network. As a Network Manager your job is to setup a network. The department store have three floor. With the given requirement, design a effective network by mentioning different networking devices you will use with its purpose.[10marks]

As the Network Manager for the new three-floor department store, I would design an effective **Local Area Network (LAN)** that ensures **connectivity, security, scalability, and centralized management**. Below is the proposed design and networking devices with their purposes:

1. Network Topology Design

- Adopt a **Hierarchical Star Topology**:
  - **Core Layer:** Main router and core switch in the server room.
  - **Distribution Layer:** Floor-wise distribution switches to manage each floor.
  - **Access Layer:** End devices (PCs, POS systems, printers, IP cameras) connected to access switches.
- Use **Fiber Optic backbone cabling** between floors for high-speed connectivity, and Cat6 cables for device connections.

---

2. Networking Devices and Their Purposes

Device	Purpose
Router	Connects the store’s network to the Internet, manages routing between internal networks, applies NAT, and controls traffic flow.
Core Switch	A high-performance managed switch that acts as the central point of connection for all floors, enabling VLANs for traffic segmentation.
Distribution/Access Switches (per floor)	Provide network connections for wired devices (cash counters, PCs, IP phones, printers, inventory systems).
Wireless Access Points (WAPs)	Offer Wi-Fi connectivity for staff handheld devices, barcode scanners, and guest Wi-Fi for customers.
Firewall	Protects the network from cyber threats, filters traffic, and enforces security policies.
DHCP Server (or router with DHCP)	Automatically assigns IP addresses to all devices, reducing manual configuration.
DNS Server	Resolves domain names to IP addresses for seamless internet browsing.
Servers (File, Inventory, POS, Backup)	Centralized storage, billing system, inventory management, and backup.
Network Attached Storage (NAS)	Provides centralized backup and file-sharing services for all departments.
Patch Panels and Racks	Organize and manage cables neatly, simplifying maintenance and troubleshooting.
UPS (Uninterruptible Power Supply)	Ensures continuous power to critical networking devices during outages.
IP Cameras & NVR	For store surveillance, integrated into the network for remote monitoring.

---

3. Logical Design and IP Addressing

- Use **VLANs** for better traffic management:
  - VLAN 10: POS and Billing Systems
  - VLAN 20: Staff Computers and Admin
  - VLAN 30: Security and Surveillance
  - VLAN 40: Guest Wi-Fi
- Assign **private IP address ranges** (e.g., 192.168.x.x) and subnetting for efficient use.

---

4. Wireless Network Planning

- Deploy multiple **Wi-Fi 6 access points per floor** to ensure seamless coverage.
- Use **SSID separation** for staff and customers to secure the internal network.

---

5. Security and Monitoring

- Install a **Firewall** and **Intrusion Detection/Prevention System (IDS/IPS)** to protect customer data and POS transactions.
- Enable **switch port security** and strong authentication.
- Implement a **Network Monitoring Tool** (e.g., Nagios, PRTG) for real-time performance tracking.

---

6. Scalability and Future Proofing

- Use stackable switches for easy expansion.
- Keep spare fiber backbone capacity for future network growth as the store expands.

---

3. Encode the digital bit stream 101101 with ASK, PSK and FSK in coding techniques.

Analog Transmission

Digital - to - Analog Conversion

Types : ASK, FSK, PSK