COMPUTER ENGINEERING DEPARTMENT

1. COURSE DETAILS

Programme: CSE/IT	**Semester: IV/IV**
Course: #Network Administration	**Group: AEC**
Course Code: NWA238918	**Duration:16 Weeks**

2. LEARNING AND ASSESSMENT SCHEME

Learning Scheme				Credits	Assessment Scheme									
Actual Contact Hrs./Week			Self-Learning (SL) (Term Work + Assignment) (Hrs)		Paper Duration (Hrs.)	Theory (Marks)			Based on LL & TL			Based on Self Learning	Total Marks
									Practical (Marks)				
CL	TL	LL				FA-TH	SA-TH	Total	FA-PR	SA-PR	SA-OR	SLA (Marks)	
02	-	04	-	03	03	30	70	100	50	-	25	-	175

Total IKS Hrs for the course :00

3. COURSE OBJECTIVE

This Course will help the students to comprehend the fundamentals of network administration and tools. This course will also familiarize the students in details of ADS. It covers vital issues related to network like Virtual private network, network management tools. It emphasizes on practical approach to administration and monitoring the network using different tools.

4. SKILL COMPETENCY/INDUSTRY/EMPLOYER EXPECTED OUTCOME

- **Configure ADS and DHCP**
- **Install and use network monitoring tools**
- **Network Troubleshooting**

5. COURSE OUTCOMES (COs): At the end of the semester student will be able to: -

CO No.	COURSE OUTCOME
CO1	Identify roles of network administrator, duties of network engineer
CO2	Install windows server edition, configure DHCP, DNS
CO3	Implement Routing and Network management Protocols
CO4	Use remote network access services and monitoring tools
CO5	Configure Directory Services and information models

Chapter 1

- **Network Admin**
- 1.1 Network Related jobs
- 1.2 Network Architecture/Designer
- 1.3 Administrator Responsibility
- 1.4 Duties of Network Engineer
- 1.5 Network Design Overview
- 1.6 Designing a Home or small Office Network
- 1.7 Designing an Internetwork

Network Admin

- A **Network Administrator** is responsible for **installing, managing, maintaining, and securing computer networks** in an organization. The administrator ensures smooth communication, data availability, and network security.

Network Related jobs

Network-related jobs primarily focus on managing, maintaining, designing, and optimizing computer networks to ensure efficient data communication and secure connectivity.

- **Network Administrator**
- **Network Engineer**
- **Network Security Specialist**
- **Systems and Network Analyst**
- **Wireless Network Engineer**
- **Cloud Network Engineer**
- **Network Support Technician**
- **Data Centre Networking Specialist**
- **VoIP Engineer**
- **Network Architect**

Responsibilities and skills needed

1. Network Administrator

- **Responsibilities**:
  - Install and configure network hardware and software.
  - Monitor network performance and troubleshoot issues.
  - Manage firewalls, routers, and switches.
  - Maintain network security protocols.
- **Skills Needed**: Networking fundamentals, Cisco/Juniper knowledge, troubleshooting.

2. Network Engineer

- **Responsibilities**:
  - Design and implement network systems.
  - Develop solutions to optimize network performance.
  - Integrate new technologies into existing networks.
  - Plan for network expansions and upgrades.
- **Skills Needed**: Network design, VPN, VLAN, cloud networking, certifications like CCNA/CCNP.

3. Network Security Specialist

- **Responsibilities**:
  - Ensure the integrity and security of network systems.
  - Protect against cyber threats such as malware and phishing attacks.
  - Conduct security audits and implement improvements.
  - Monitor for unauthorized access and breaches.
- **Skills Needed**: Cybersecurity tools, penetration testing, knowledge of firewalls, security certifications (e.g., CEH, CISSP).

4. Systems and Network Analyst

- **Responsibilities**:
  - Analyze existing network systems and suggest optimizations.
  - Research and evaluate new networking technologies.
  - Collaborate with IT teams to enhance infrastructure.
- **Skills Needed**: Data analysis, network protocols, system integration.

5. Wireless Network Engineer

- **Responsibilities**:
  - Design and implement wireless networks.
  - Manage Wi-Fi systems and troubleshoot connectivity issues.
  - Optimize wireless performance in diverse environments.
- **Skills Needed**: Wireless standards (e.g., 802.11), RF engineering, network design.

6. Cloud Network Engineer

- **Responsibilities**:
  - Develop and manage cloud-based networking systems.
  - Implement secure and scalable cloud solutions.
  - Work with platforms like AWS, Azure, or Google Cloud.
- **Skills Needed**: Cloud networking, SD-WAN, load balancing.

7. Network Support Technician

- **Responsibilities**:
  - Provide support for network-related issues.
  - Assist in setting up and maintaining hardware.
  - Perform routine maintenance and updates.
- **Skills Needed**: Problem-solving, hardware knowledge, basic networking.

8. Data Centre Networking Specialist

- **Responsibilities**:
  - Manage data centre network operations.
  - Ensure efficient data routing and server connectivity.
  - Optimize storage networking.
- **Skills Needed**: SAN((Storage Area Network) provides **block-level storage** to servers. /NAS (Network Attached Storage) **file-level storage system** connected to a standard network and shared among multiple users. systems, data centre hardware, virtualization.
- (Supports protocols like NFS, SMB, CIFS) **SMB** (Server Message Block) is a **network file-sharing protocol** that allows computers to **share files, folders, printers, and other resources** over a network. **(Common Internet File System)**
- **CIFS** is an **older version of the SMB protocol** developed by Microsoft.

9. VoIP Engineer

- **Responsibilities**:
  - Manage and maintain Voice over IP systems.
  - Optimize call quality and reduce latency.
  - Integrate VoIP with other systems.
- **Skills Needed**: VoIP protocols (SIP, RTP), QoS, telecommunications knowledge.

10. Network Architect

- **Responsibilities**:
  - Develop long-term strategies for network infrastructure.
  - Design scalable and resilient networks.
  - Oversee the implementation of complex network projects.
- **Skills Needed**: Advanced design, leadership, enterprise networking, certifications like CCIE.
- Each role requires specific certifications, technical knowledge, and often hands-on experience. Popular certifications in networking include Cisco's CCNA/CCNP, CompTIA Network+, and Juniper Networks certifications.

Network Architect/Designer

- A **Network Architect** (also known as a Network Designer) is a senior-level role in networking, focusing on designing and building complex and scalable network systems.
- They plan the framework that ensures efficient communication and data exchange across an organization's IT infrastructure

Responsibilities

- **Network Design**:
  - Create blueprints for LAN, WAN, cloud-based, and hybrid networks.
  - Design high-performance, secure, and scalable network architectures.
  - Incorporate redundancy and failover mechanisms to ensure uptime.
- **Technology Selection**:
  - Evaluate hardware and software solutions (routers, switches, firewalls, SD-WAN, etc.).
  - Recommend tools and technologies based on organizational needs.
- **Strategic Planning**:
  - Assess current network systems and plan for future growth or migration.
  - Collaborate with business leaders to align network capabilities with organizational goals.
- **Implementation Oversight**:
  - Lead teams in deploying the network architecture.
  - Ensure smooth integration with existing systems.
  - Troubleshoot deployment issues.
- **Security and Compliance**:
  - Design networks to adhere to cybersecurity best practices and compliance standards.
  - Implement security measures like VPNs, firewalls, and intrusion detection/prevention systems.
- **Performance Optimization**:
  - Design for high availability and minimal latency.
  - Plan for load balancing, bandwidth optimization, and efficient data routing.
- **Documentation**:
  - Develop detailed documentation for the network infrastructure.
  - Update network diagrams and configurations for future reference.

- **Skills Required**
- **Technical Knowledge**:
  - Networking protocols (TCP/IP, BGP, OSPF, MPLS, etc.).
  - Network hardware (Cisco, Juniper, HP, etc.).
  - Cloud networking (AWS, Azure, GCP).
  - Virtualization technologies (SDN, NFV).
- **Design and Analytical Skills**:
  - Expertise in network topology design and layout.
- Ability to analyze requirements and create cost-effective solutions.
  Problem-Solving Skills:
  - Troubleshoot complex network-related challenges during implementation.
- **Soft Skills**:
  - Leadership for guiding teams during large projects.
  - Communication to explain designs to stakeholders and collaborate with IT teams.

Certifications

Certifications play a significant role in validating expertise. Recommended certifications include:

- **Cisco Certified Internetwork Expert (CCIE)** – For advanced network engineering and design.
- **Cisco Certified Design Expert (CCDE)** – Specialized in designing scalable and resilient networks.
- **AWS Certified Advanced Networking** – For cloud network design and management.
- **CompTIA Network+** – Foundational certification for network basics.
- **Juniper Networks Certified Design Specialist (JNCDS)** – Focused on Juniper technologies.

Career Path

1. **Entry-Level Roles**: Network Administrator, Network Engineer.
2. **Mid-Level Roles**: Network Consultant, Senior Network Engineer.
3. **Advanced Roles**: Network Architect, Enterprise Architect

- **Tools Used**
- **Design and Simulation**: Cisco Packet Tracer, GNS3.
- **Monitoring and Management**: Wireshark, Nagios, PRTG Network Monitor. **PRTG** (*Paessler Router Traffic Grapher*) is a network monitoring software developed by Paessler GmbH.
- **Diagramming**: Microsoft Visio, Lucidchart.

Administrator's responsibilities

An administrator's responsibilities can vary depending on the context (e.g., business, education, IT, or public administration). However, general duties and expectations include the following:

1. Management and Organization

- **Oversee Operations**: Ensure that daily operations run smoothly and efficiently.
- **Set Goals**: Define objectives and develop strategies to achieve them.
- **Delegate Tasks**: Assign responsibilities to staff members and monitor progress.

2. Policy Implementation

- **Compliance**: Ensure adherence to laws, regulations, and organizational policies.
- **Update Policies**: Regularly review and update rules to align with evolving needs.

3. Staff Supervision

- **Training and Development**: Provide resources and opportunities for employee growth.
- **Performance Monitoring**: Conduct evaluations and offer constructive feedback.
- **Conflict Resolution**: Mediate disputes and foster a positive work environment.

4. Resource Management

- **Budget Oversight**: Manage finances, approve expenditures, and ensure cost-efficiency.
- **Facilities Maintenance**: Ensure that physical and digital infrastructures are operational.

5. Communication

- **Internal Communication**: Facilitate clear and effective communication between departments and teams.
- **External Representation**: Act as a liaison with stakeholders, clients, or regulatory bodies.

6. Strategic Planning

- **Risk Management**: Anticipate and address potential challenges or threats.
- **Project Coordination**: Oversee project timelines and ensure objectives are met.

7. Technological Oversight (if applicable)

- **System Management**: Maintain and upgrade software, hardware, or other IT infrastructure.
- **Data Security**: Protect sensitive information and ensure proper access control.

8. Ethical Leadership

- **Promote Integrity**: Lead by example and uphold ethical standards.
- **Accountability**: Take responsibility for decisions and outcomes.

Administrator Roles Across Fields:

- **Educational Institutions**: Manage academic programs, staff, and student affairs.
- **Healthcare**: Oversee patient services, compliance, and operational efficiency.
- **Corporate Sector**: Supervise teams, manage budgets, and ensure goal alignment.
- **Public Sector**: Implement government policies, handle community concerns, and manage public resources.

Network Engineer responsibilities

A **Network Engineer** is responsible for designing, implementing, maintaining, and managing an organization's network infrastructure. Their duties encompass ensuring network reliability, security, and optimal performance. Here's a detailed list of their responsibilities:

. Network Design and Implementation

- Plan and design network infrastructure, including LAN, WAN, and cloud networks.
- Select and configure hardware, such as routers, switches, firewalls, and access points.
- Implement network solutions based on organizational needs and growth plans.

2. Network Maintenance and Monitoring

- Monitor network performance using tools to detect and resolve issues.
- Perform regular updates and patches to network hardware and software.
- Troubleshoot connectivity issues and resolve outages promptly.

3. Security Management

- Implement network security protocols to protect data and systems.
- Configure and manage firewalls, VPNs, and intrusion detection/prevention systems.
- Conduct vulnerability assessments and apply appropriate safeguards.

4. Performance Optimization

- Optimize network performance by analyzing traffic and bandwidth usage.
- Configure load balancing and redundancy to ensure high availability.
- Recommend upgrades to improve efficiency and accommodate growth.

5. Documentation and Reporting

- Maintain detailed network diagrams, configurations, and documentation.
- Prepare reports on network performance, incidents, and improvement plans.
- Document troubleshooting procedures for future reference

6. Collaboration and Support

- Work with IT teams to integrate new applications and systems into the network.
- Provide technical support and training to staff regarding network issues.
- Collaborate with vendors for procurement and troubleshooting.

7. Project Management

- Lead network-related projects such as migrations, upgrades, or expansions.
- Define project scope, timelines, and resources needed.

8. Compliance and Standards

- Ensure compliance with industry regulations (e.g., GDPR, HIPAA).
- Adhere to best practices and standards, such as ITIL or ISO/IEC 27001.

9. Research and Development

- Stay updated on emerging networking technologies.
- Evaluate new tools and methods to improve network capabilities and resilience.

Skills Required:

- **Technical Skills:** Expertise in network protocols (TCP/IP, DNS, DHCP), hardware configuration, and troubleshooting.
- **Analytical Thinking:** Ability to diagnose and resolve complex network issues.
- **Communication:** Effectively explain technical concepts to non-technical stakeholders.
- **Certifications:** Often beneficial (e.g., CCNA, CCNP, CompTIA Network+, or AWS certifications).
- By fulfilling these duties, network engineers ensure seamless connectivity, secure communications, and robust infrastructure for the organization.

Network Design overview

Network Design is the process of planning and creating a network infrastructure that meets an organization's specific communication and operational needs. It involves analyzing requirements, choosing the right technologies, and laying out the structure of how devices, systems, and connections will function together. Below is an overview of the key elements of network design.

Network Design overview

1. Goals of Network Design

- **Performance:** Ensure high-speed and low-latency connectivity.
- **Scalability:** Design a network that can grow with organizational needs.
- **Reliability:** Minimize downtime with redundancy and failover mechanisms.
- **Security:** Protect data and systems against unauthorized access and attacks.
- **Cost-Efficiency:** Balance performance with budget constraints.
- **Compliance:** Adhere to industry standards and legal regulations

2. Steps in Network Design

a. Requirement Analysis

- Identify the organization's business and technical needs.
- Determine the number of users, devices, and systems to support.
- Assess current network performance and pain points.

b. Logical Design

- Define the topology (e.g., star, mesh, bus, hybrid).
- Specify IP addressing schemes (e.g., IPv4, IPv6) and subnetting plans.
- Determine protocols and services to be used (e.g., routing, QoS, VLANs).
- Plan network segmentation for improved performance and security.

c. Physical Design

- Choose hardware components like routers, switches, access points, and firewalls.
- Plan the placement of devices and cabling routes (fiber optics, Ethernet).
- Design the data centre, if applicable.

d. Security Design

- Define access control mechanisms (e.g., firewalls, ACLs, NAC).
- Plan for encryption, VPNs, and intrusion detection/prevention systems.
- Implement network monitoring and alerting tools.

e. Redundancy and Failover

- Plan for redundant connections and devices.
- Incorporate load balancing and disaster recovery solutions.

f. Testing and Simulation

- Use tools to simulate and test network designs before deployment.
- Identify potential bottlenecks or vulnerabilities

- **3. Components of Network Design**

a. Core Network

- High-speed backbone connecting major network segments.
- Focuses on scalability and minimal latency.
- *b. Distribution Network*
- Aggregates traffic from access networks and connects to the core.
- Implements routing, filtering, and load balancing.

c. Access Network

- Connects end-users and devices to the network.
- Uses technologies like Ethernet, Wi-Fi, or cellular.

d. Wide Area Network (WAN)

- Links geographically dispersed locations using technologies like MPLS, SD-WAN, or leased lines.

e. Data Center and Cloud Integration

- Includes servers, storage, and virtualized environments.
- Incorporates hybrid or cloud-based resources

Best Practices for Network Design

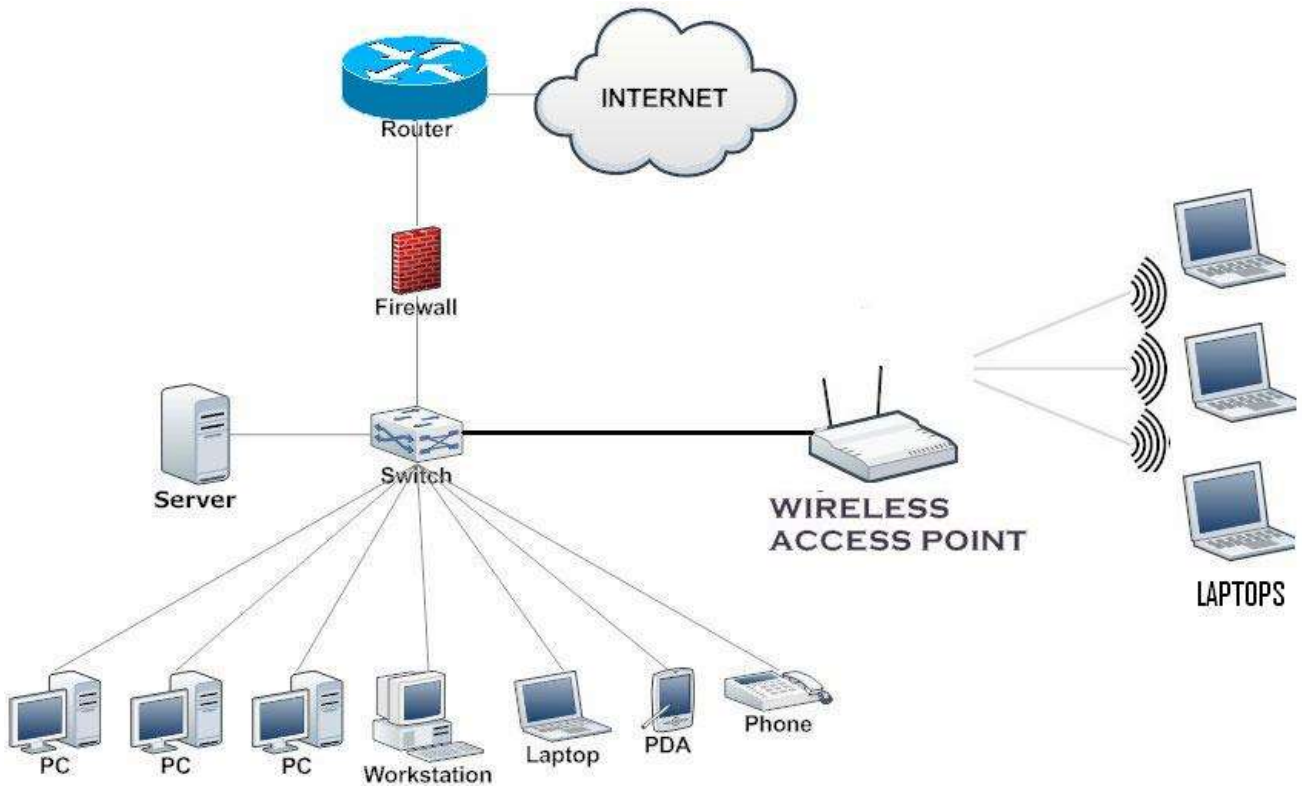
- **Keep it Modular:** Divide the network into manageable sections for easier troubleshooting and upgrades.
- **Plan for Growth:** Anticipate future needs and incorporate scalability.
- **Prioritize Security:** Protect all entry points and ensure data encryption.
- **Use Redundancy:** Avoid single points of failure.
- **Optimize Performance:** Use QoS for critical applications and minimize congestion.

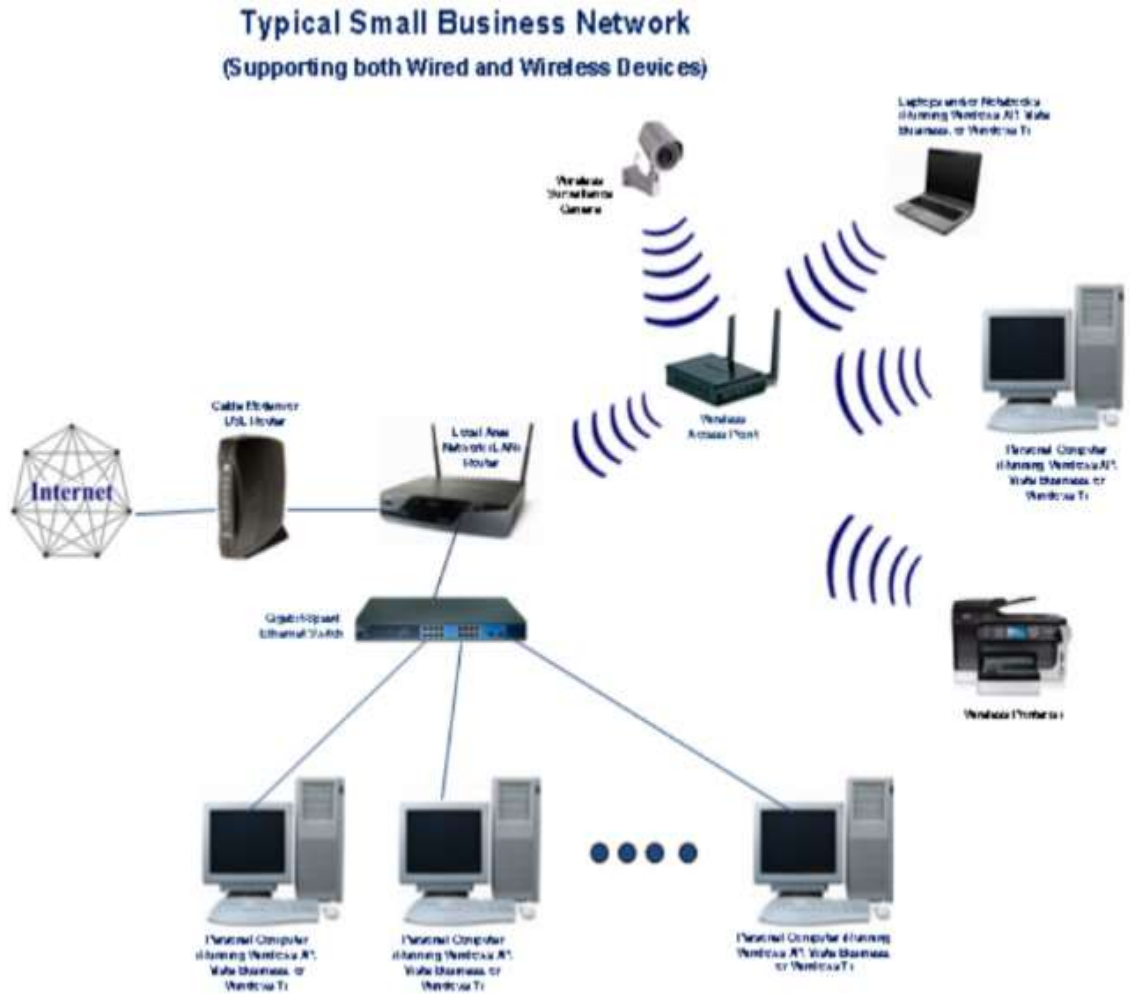
.Tools for Network Design

- **Simulation Tools:** Cisco Packet Tracer, GNS3, or EVE-NG.
- **Diagramming Tools:** Microsoft Visio, Lucidchart, or draw.io.
- **Performance Tools:** SolarWinds, Wireshark, or Nagios.

- **Outcome of Network Design:**
  A well-designed network ensures reliable communication, robust security, optimized performance, and seamless scalability, all tailored to the organization's objectives and constraints.
- Designing a **home** or **small office network**

Designing a **home** or **small office network** involves creating a reliable, cost-effective, and scalable solution to meet basic connectivity, communication, and operational needs. Here's a step-by-step guide to designing such a network.


INTERNET
Router
Firewall
Server
Switch
WIRELESS
ACCESS POINT
LAPTOPS
PC
PC
PC
Workstation
Laptop
PDA
Phone


Typical Small Business Network
(Supporting both Wired and Wireless Devices)
Internet

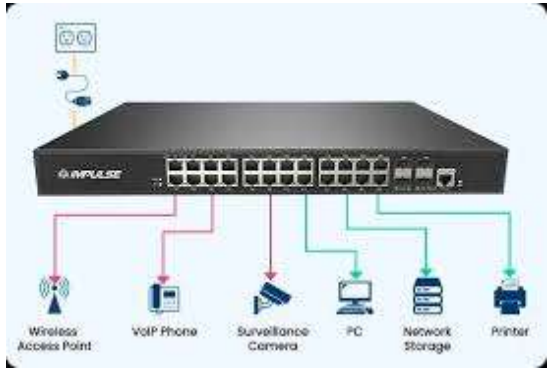
1. Define Requirements

- **Number of Users and Devices:**
  - Count devices like computers, smartphones, printers, and smart devices.
- **Purpose:**
  - Internet browsing, file sharing, video conferencing, or hosting services.
- **Internet Connection:**
- Decide on bandwidth

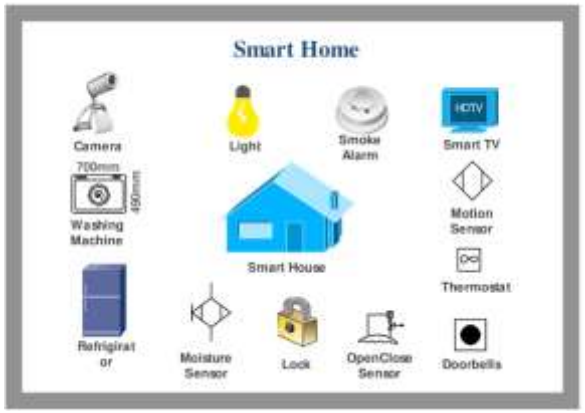
2**. Choose the Network Topology**

For home or small office networks, a **star topology** is most common, where devices connect to a central hub (router or switch). This simplifies setup and troubleshooting

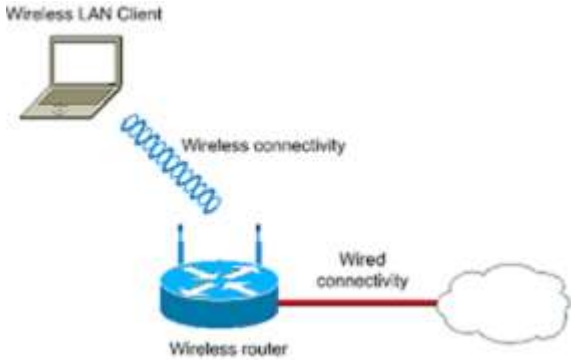
3 .**Key Components**



- **Internet Connection**
- **Modem:** Connects to the ISP (Internet Service Provider) for internet access.
- **Router:** Distributes the internet connection to all devices and manages traffic.
  - Consider a router with dual-band or tri-band Wi-Fi for better coverage.
- ***Network Switch (Optional)***
- Use if there are more wired devices than router ports.
- For small setups, an unmanaged switch with 5–8 ports is sufficient.
- **Wireless Access Points (Optional)**
- **. Cables and Connectors**
- Use **Cat5e or Cat6 Ethernet cables** for wired connections.
- Ensure proper labeling of cables for organization.
- ***. End Devices***
- Computers, printers, IP phones, or IoT devices.
- ***Power Backup***
- Install a UPS (Uninterruptible Power Supply) to ensure continuity during outages



- 4 Network Design
- ***a. IP Addressing***
- Use private IP ranges like **192.168.x.x** or **10.x.x.x**.
- Enable **DHCP** on the router to automatically assign IPs to devices.
- ***b. Wireless Configuration***
- Choose secure Wi-Fi standards (WPA3 or WPA2).
- Use separate SSIDs for guests and employees (e.g., Guest Wi-Fi).
- ***c. Network Segmentation (Optional)***
- For better security, create VLANs (e.g., one for IoT devices and another for workstations).
- ***d. Security***
- Change default admin credentials on the router.
- Enable firewall settings.
- Regularly update firmware.
- ***e. File Sharing and Storage***
- Use a **NAS (Network-Attached Storage)** device or shared folder on a computer.
- ***f. Printer/Peripheral Sharing***
- Configure network printers for access from multiple devices.



5. Network Diagram

- Create a simple network diagram for visualization:
- **ISP --> Modem --> Router.**
- From Router:
  - Wired: Devices like PCs, printers, and switches.
  - Wireless: Smartphones, laptops, IoT devices.

6. Performance Optimization

- Place the router centrally for better Wi-Fi coverage.
- Use wired connections for bandwidth-intensive tasks like gaming or video editing.
- Monitor bandwidth usage to ensure no single device monopolizes resources.

7. Testing and Maintenance

- Test internet speed and connectivity for all devices.
- Periodically check for firmware updates.
- Use tools like **Ping** or **Traceroute** to diagnose connectivity issues.

Design small office or home network

- **Scenario-draw diagram**
- small office network with the following requirements:
- **Devices:** 6 PCs, 1 network printer, and 1 wireless laptop.
- **Server:** A centralized file server.
- **Internet Access:** All devices require internet access.
- **Network Segmentation:** Optional VLAN for better management.
- **IP Addressing:** Dynamic (via DHCP) with static IP for the printer and file server.

- **Network Design:**
- **Devices:**
- **Router:** Cisco ISR 4321 (Internet Gateway).
- **Switch:** Cisco Catalyst 2960 (for wired devices).
- **Access Point:** Cisco WAP (for wireless devices).
- **End Devices:**
  - 6 PCs (wired).
  - 1 network printer (static IP).
  - 1 laptop (wireless).
  - 1 file server (static IP).
- **IP Addressing Plan:**
- Network: 192.168.1.0/24
- Router Gateway: 192.168.1.1
- DHCP Range: 192.168.1.100 to 192.168.1.200
- Printer: 192.168.1.10
- File Server: 192.168.1.20

Write in detail the Implementation Steps:

Physical Layout in Packet Tracer

Router Configuration:

Switch Configuration

File Server and Printer Configuration:

Wireless Access Point Configuration:

Test Connectivity:

block diagram of a small office network setup. It illustrates the connections between key components like the ISP modem, router, switch, and various devices, along with Wi-Fi and VLAN segmentation.