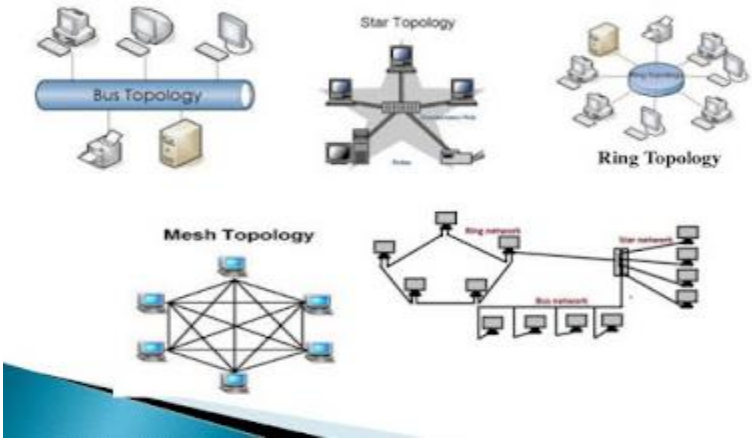
Hardware and Networking Service

Level-III

Based on Nov 2023, Curriculum Version -II



Module Title: - Determine Best Fit Topology

Module code: EIS HNS3 M01 0322

Nominal duration: 50Hour

Prepared by: Ministry of Labour and Skill

November 2023

Addis Ababa, Ethiopia

Table of Contents

Acknowledgment ..... **iii**

Acronym ---------- **iv**

Introduction to the Module ..... **v**

Unit One: Identify key information source **1**

1.1. Basic Concepts of information repository **2**

1.2. Reviewing organizational documentation **2**

1.3. Information gathering techniques **3**

Self-Check 1 ..... **3**

Unit Two: Determine user needs **5**

2.1. Identify user needs and establish requirements **6**

2.2. Identifying network segments for proposed network requirements **9**

2.3. Determining Segment needs using functional analysis **10**

2.4. Estimating network traffics **11**

Self – Check 2 ..... **13**

Unit Three: Develop best topology **14**

3.1. Overview of network topologies **15**

Fig. 3.1. Image that shows Network Topologies **15**

3.2. Determining network resource requirements **15**

3.3. Analysing physical environment features based on network design **18**

3.4. Selecting appropriate network topology **20**

Self-check 3 ..... **24**

Operation Sheet 3.1 ..... **25**

LAP Test 3.1 ..... **26**

Reference Books: **27**

Developers Profile **28**

Acknowledgment

Ministry of Labor and Skills wish to extend thanks and appreciation to the many representatives of TVET instructors and respective industry experts who donated their time and expertise to the development of this Teaching, Training and Learning Materials (TTLM).

Acronym

TTLM - raining, Teaching and Learning Material

LAP - Learning Activity Performance

DMZ - Demilitarized Zone

IP - Internet Protocol

GNS - Global Navigation Satellite

CML - Chronic Myeloid Leukemia

NG - Next Generation

GNS - Global Navigation Satellite

AWS - Amazon Web Services

ISR - Intelligence, Surveillance, and Reconnaissance

MX - Mail Exchange

HPE - Hewlett Packard Enterprise

ASA - Adaptive Security Appliance

NGFW - Next-Generation Firewall

VPN - Virtual Private Network

SPAN - Switched Port Analyzer

UPS - Uninterruptible Power Supply

CCNA - Cisco Certified Network Associate

Introduction to the Module

In Hard ware and Network Servicing field, Determine Best Fit Topology is used to design the physical and Logical Network Layout for various organizations and institutions.

This module is designed to meet the industry requirement under the Hard Ware and Network Servicing occupational standard, particularly for the unit of competency: Determine Best Fit Topology

Module covers the units:

- Identify key information sources
- Determine user needs
- Develop best topology

Learning Objective of the Module

- Identifying information repositories
- Reviewing current organizational documentation
- Information gathering techniques
- Identifying user needs and establish requirements
- Identifying network segments for proposed network requirements
- Determining Segment needs using functional analysis
- Estimating network traffics/loads
- Overview of network topologies
- Determining network resource requirements
- Analysing physical environment features based on network design
- Selecting appropriate network topology

Module Instruction

For effective use this module trainees are expected to follow the following module instruction:

1. Read the information written in each unit
2. Accomplish the Self-checks at the end of each unit
3. Perform Operation Sheets which were provided at the end of units
4. Do the “LAP test” giver at the end of each unit and
5. Read the identified reference book for Examples and exercise

Unit One: Identify key information source

This Unit is developed to provide you the necessary information regarding the following content coverage and topics

- Identifying information repositories
- Reviewing current organizational documentation
- Developing critical questions
- Ensuring information gathering techniques

This guide will also assist you to attain the learning outcome stated in the cover page. Specifically, upon completion of this Learning Guide, you will be able to –

- Identify information repositories
- Review current organizational documentation
- Develop critical questions
- Ensure information gathering techniques

1.1. Basic Concepts of information repository

An information repository is a centralized place where data is stored and maintained in an organized way, usually in computer storage. It may be used for different purposes, such as data analysis, sharing, reporting, archiving, or security. Some basic concepts of information repository are:

- **Types of repositories**: There are different types of repositories, such as data warehouse, data lake, data mart, metadata repository, and data cube. They differ in the structure, format, and scope of the data they store and manage.
- **Benefits of repository**: A repository can provide several benefits, such as faster and easier data access and retrieval, improved data quality and consistency, enhanced collaboration and communication, and increased data security and protection[123]
- **Challenges of repository**: A repository can also pose some challenges, such as data growth and scalability, system reliability and backup, data integration and migration, and data governance and compliance[123]
- **Federated repository**: A federated repository is a type of repository that consists of multiple, networked data storage technologies running on diverse operating systems. It can reduce the maintenance workload and support heterogeneous storage resources[4]

1.2. Reviewing organizational documentation

To review a document repository, you should first identify the purpose of the review. This could be to ensure that the documents are up-to-date, to check that they are being used correctly, or to identify any gaps in the repository. Once you have identified the purpose of the review, you can then create a plan for the review process. This plan should include the following steps:

1. **Identify the documents to be reviewed**: You should identify which documents need to be reviewed and why. This will help you to focus your review on the most important documents.
2. **Create a review team**: You should create a team of people who will be responsible for reviewing the documents. This team should include people who have knowledge of the documents and the processes they relate to.
3. **Establish review criteria**: You should establish criteria for the review process. This could include checking that the documents are up-to-date, that they are being used correctly, and that they are complete.

4. **Conduct the review**: The review team should then conduct the review. This could involve checking the documents against the established criteria, interviewing employees who use the documents, or conducting surveys.
5. **Analyze the results**: Once the review is complete, the results should be analyzed. This will help you to identify any issues with the document repository and to develop a plan for addressing these issues.
6. **Implement changes**: Finally, you should implement any changes that are needed to improve the document repository. This could involve updating the documents, changing the processes that are used, or providing additional training to employees.

1.3. Information gathering techniques

Information gathering is a crucial aspect of various activities, including research, investigations, and decision-making. There are several techniques and methods you can employ to gather information effectively. Here are some common information gathering techniques:

1. **Surveys and Questionnaires**: Design and distribute surveys or questionnaires to collect data from a specific audience. Use online survey tools or conduct in-person interviews.
2. **Interviews**: Conduct one-on-one or group interviews with relevant individuals. Prepare a set of open-ended and closed-ended questions.
3. **Observation**: Directly observe and document behaviors, events, or processes. Use participant observation by immersing yourself in the environment you're studying.
4. **Document Analysis**: Review and analyze existing documents, reports, publications, and records. This includes official documents, academic papers, and historical records.
5. **Internet Research**: Utilize search engines to gather information from online sources. Verify the credibility of the sources and cross-reference information.
6. **Focus Groups**: Bring together a small group of people to discuss a specific topic. Facilitate a guided discussion to gather insights and opinions.
7. **Networking**: Establish and leverage professional networks to gather information. Attend conferences, seminars, and events to connect with experts and peers.

Remember, the effectiveness of these techniques depends on the context of your information needs and the nature of the subject you are investigating. It's often beneficial to use a combination of these methods for comprehensive and reliable information gathering.

Self-Check 1

True/False Questions:

1. An information repository can be used for purposes such as data analysis, sharing, reporting, archiving, or security.
2. A federated repository is a type of repository that operates on a single, centralized data storage technology.
3. One of the challenges of an information repository is related to system reliability and backup.
4. Document analysis is a common information gathering technique that involves direct observation and documentation of behaviours, events, or processes.

Multiple-Choice Questions:

1. What is a federated repository?
   a) Single, centralized data storage c) Hierarchical data storage
   d) Cloud-based data storage b) Multiple, networked data storage technologies
2. What is a benefit of an information repository?
   a) Increased data growth c) Decreased collaboration and communication
   d) Limited data security and protection b) Improved data quality and consistency
3. Which step is part of the process for reviewing organizational documentation?
   a) Conducting surveys c) Creating information gathering techniques
   d) Implementing changes b) Establishing review criteria

Essay Questions:

1. Describe three types of repositories mentioned in the document and provide an example use case for each.
2. Explain the importance of creating a review team when reviewing organizational documentation. How does having a diverse team contribute to the effectiveness of the review process?

Unit Two: Determine user needs

This Unit is developed to provide you the necessary information regarding the following content coverage and topics

- Identifying user needs and establish requirements
- Identifying network segments for proposed network requirements
- Determining Segment needs using functional analysis
- Estimating network traffics/loads

This guide will also assist you to attain the learning outcome stated in the cover page. Specifically, upon completion of this Learning Guide, you will be able to –

- Identify user needs and establish requirements
- Identify network segments for proposed network requirements
- Determine Segment needs using functional analysis
- Estimate network traffics/loads

2.1. Identify user needs and establish requirements

Identifying user needs and establishing requirements are critical steps in determining the best-fit network topology for a given scenario. The choice of network topology depends on factors such as the size of the organization, the nature of communication between devices, scalability requirements, fault tolerance, and cost considerations. Here's are things we have to consider:

- User Needs Assessment:
  - Interview Stakeholders:
    Talk to key stakeholders to understand their requirements and expectations.
    Identify the different user groups and their specific needs.
  - User Surveys:
    Conduct surveys to gather input from end-users regarding their connectivity requirements and preferences.
  - Review Existing Infrastructure:
    Assess the current network infrastructure to identify pain points and areas for improvement.
    Consider the types of devices used and their connectivity requirements.
- Functional Requirements:
  - Define Network Functions:
    List the essential functions the network must support (e.g., data sharing, application access, internet connectivity).
  - Bandwidth Requirements:
    Determine the required bandwidth for different types of communication within the network.
  - Scalability:
    Identify growth expectations and scalability requirements to ensure the network can accommodate future expansion.
- Performance Requirements:

- Latency and Response Time:
  Determine acceptable latency and response time for critical applications.
- Reliability and Availability:
  Define requirements for network reliability and availability, considering redundancy and failover mechanisms.
- Throughput:
  Specify the required throughput for various network segments.

- Security Requirements:

  - Access Control:
    Define access control policies and requirements for user authentication and authorization.
  - Data Encryption:
    Identify the need for data encryption to ensure secure communication.
  - Intrusion Detection/Prevention:
    Specify requirements for intrusion detection and prevention mechanisms.

- Cost Considerations:
  - Budget Constraints:

2.2. Identifying network segments for proposed network requirements

Network segmentation is a crucial step in designing a network that meets specific requirements. Network segmentation involves dividing the network into smaller, more manageable parts, often based on functional or security considerations. Here's a guide to identifying network segments for proposed network requirements:

1. **Understand Network Requirements**:
   - User Needs: Identify the different user groups and their specific requirements. Consider the types of devices used and their connectivity needs.
   - Applications and Services: Determine the critical applications and services that the network must support. Classify applications based on their importance and bandwidth requirements.
   - Security Requirements: Define security and access control requirements for different segments.
2. **Categorize Network Segments**:
   - User Segmentation: Group users based on their roles and responsibilities. Create segments for different departments or teams.
   - Function-Based Segmentation: Identify segments based on the functions or tasks performed by devices and users.
   - Critical Infrastructure: Designate separate segments for critical infrastructure, such as servers and network management systems.
   - Guest Networks: If applicable, create a separate segment for guest access to ensure security.
3. **Traffic Analysis**:
   - Identify Data Flows: Analyze the flow of data between devices and applications. Determine which devices need to communicate with each other.
   - Bandwidth Requirements: Assess the bandwidth requirements for different types of traffic. Allocate sufficient bandwidth for critical applications.
4. **Security Considerations**:
   - Sensitive Data Segmentation: If handling sensitive data, create segments to isolate and protect this data. Remember, the effectiveness of these techniques depends on the context of your information needs and the nature of the subject you are investigating.

It’s often beneficial to use a combination of these methods for comprehensive and reliable information gathering

2.2.1. Identifying network segments for proposed network requirements

Network segmentation is a crucial step in designing a network that meets specific requirements. Network segmentation involves dividing the network into smaller, more manageable parts, often based on functional or security considerations. Here are common types of network segments:

- **User Segments:** Grouping users based on their roles and responsibilities. Allows for tailored access control and security policies.
- **Departmental Segments:** Dividing the network based on different departments within an organization. Enhances network management and supports department-specific applications.
- **Functional Segments:** Creating segments based on the functions or tasks performed by devices and users. Useful for optimizing network performance and applying specific policies.
- **Server Segments:** Isolating servers into dedicated segments for improved performance and security. Common servers include file servers, application servers, and database servers.
- **Wireless Segments:** Separating wired and wireless networks to enhance security. May include a dedicated segment for guest wireless access.
- **DMZ (Demilitarized Zone):** A segment positioned between the internal network and the external network (usually the internet). Hosts public-facing servers like web servers and email servers.
- **VoIP (Voice over Internet Protocol) Segments:** Segregating voice traffic from data traffic to ensure quality and reliability. Prioritizing voice data using Quality of Service (QoS) measures.
- **IoT (Internet of Things) Segments:** Creating segments for devices in the IoT ecosystem. Ensures that IoT devices are isolated from critical network resources.

- **Guest Network Segments:** Designing a dedicated segment for guest access to prevent unauthorized access to internal resources. Often includes limited access and increased monitoring.
- **Security Zones:** Establishing segments with varying levels of security. High-security zones for sensitive data and lower-security zones for less critical resources.

Remote Access Segments: Creating segments for remote access to the network. Ensures secure access to network resources from remote locations. Remember, the effectiveness of these techniques depends on the context of your information needs and the nature of the subject you are investigating. It's often beneficial to use a combination of these methods for comprehensive and reliable information gathering

2.3. Determining Segment needs using functional analysis

Functional analysis is a valuable approach for determining segment needs in a network. It involves breaking down the network's requirements based on the functions and tasks performed by users, devices, and applications. Here are common types of network segments:

- User Segments: Grouping users based on their roles and responsibilities. Allows for tailored access control and security policies.
- Departmental Segments: Dividing the network based on different departments within an organization. Enhances network management and supports department-specific applications.
- Functional Segments: Creating segments based on the functions or tasks performed by devices and users. Useful for optimizing network performance and applying specific policies.
- Server Segments: Isolating servers into dedicated segments for improved performance and security. Common servers include file servers, application servers, and database servers.
- Wireless Segments: Separating wired and wireless networks to enhance security. May include a dedicated segment for guest wireless access.
- DMZ (Demilitarized Zone): A segment positioned between the internal network and the external network (usually the internet). Hosts public-facing servers like web servers and email servers.

- VoIP (Voice over Internet Protocol) Segments: Segregating voice traffic from data traffic to ensure quality and reliability. Prioritizing voice data using Quality of Service (QoS) measures.
- IoT (Internet of Things) Segments: Creating segments for devices in the IoT ecosystem. Ensures that IoT devices are isolated from critical network resources.
- Guest Network Segments: Designing a dedicated segment for guest access to prevent unauthorized access to internal resources. Often includes limited access and increased monitoring.
- Security Zones: Establishing segments with varying levels of security. High-security zones for sensitive data and lower-security zones for less critical resources.
- Remote Access Segments: Creating segments for remote access to the network. Ensures secure access to network resources from remote locations. Remember, the effectiveness of these techniques depends on the context of your information needs and the nature of the subject you are investigating. It's often beneficial to use a combination of these methods for comprehensive and reliable information gathering.

2.4. Estimating network traffics

Estimating network traffic is a critical aspect of network planning, capacity management, and resource allocation. Accurate traffic estimation helps ensure that the network can handle current and future demands. Here are common methods and considerations for estimating network traffic:

- **Data Collection**: How to collect historical and application-specific data on network usage using monitoring tools.
- **User and Device Analysis**: How to understand the number of users, their roles, and the types of devices they use on the network.
- **Application Traffic Patterns**: How to identify and prioritize critical applications and their bandwidth requirements, and how to consider new application rollouts.
- **Predictive Modeling**: How to use mathematical and machine learning models to predict future network traffic based on historical data and other factors.
- **Peak vs. Average Traffic**: How to determine peak and average network usage times and use them for capacity planning.

- **Application and Protocol Analysis**: How to understand the characteristics and impact of different protocols and applications on network performance using deep packet inspection.
- **Network Topology**: How to segment the network into smaller subnets to reduce congestion and improve security.

Self – Check 2

True False Questions

1. Network segmentation involves dividing the network into smaller, more manageable parts based solely on functional considerations.
2. Functional analysis is a method used for determining segment needs in a network by focusing on the roles and responsibilities of users only.
3. Peak vs. Average Traffic analysis is essential for determining network capacity planning and resource allocation.

Multiple-Choice Questions:

1. Which method involves breaking down the network's requirements based on the functions and tasks performed by users, devices, and applications?
   A. Predictive Modelling C. Peak vs. Average Traffic Analysis
   B. Functional Analysis D. Data Collection
2. What is the purpose of a DMZ (Demilitarized Zone) in network segmentation?
   A. Enhance network management C. Host public-facing servers
   B. Isolate and protect sensitive data D. Provide secure remote access
3. Which of the following is a consideration for estimating network traffic?
   A. User and Device Analysis
   B. Bandwidth Requirements
   C. Scalability
   D. Latency and Response Time

Essay Questions:

1. Explain the significance of conducting user surveys and interviewing stakeholders in the process of identifying user needs and establishing network requirements.
2. Describe the role of network segmentation in designing a network that meets specific requirements.
3. Discuss the importance of estimating network traffic in network planning and capacity management.

Unit Three: Develop best topology

This Unit is developed to provide you the necessary information regarding the following content coverage and topics

- Overview of network topologies
- Determining network resource requirements
- Analysing physical environment features based on network design
- Selecting appropriate network topology

This guide will also assist you to attain the learning outcome stated in the cover page.
Specifically, upon completion of this Learning Guide, you will be able to –

- Explain overview of network topologies
- Determine network resource requirements
- Analyse physical environment features based on network design
- Select appropriate network topology

3.1. Overview of network topologies

Network topology refers to the physical or logical layout of interconnected devices in a computer network. It defines how different nodes or devices are arranged and how they communicate with each other. There are several types of network topologies, each with its own advantages and disadvantages.

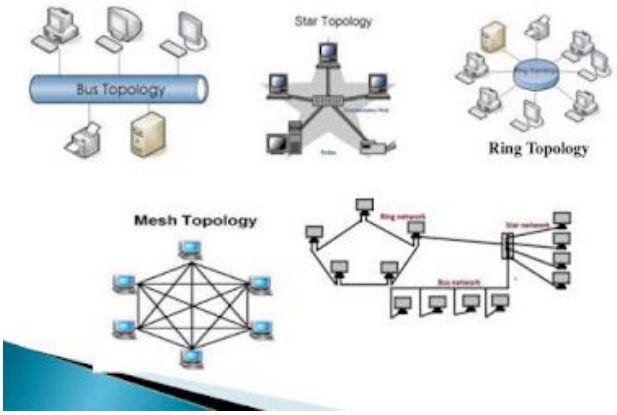


Fig. 3.1. Image that shows Network Topologies

3.2. Determining network resource requirements

Determining network resource requirements is a crucial step in network planning and design. It involves assessing the needs of the organization in terms of bandwidth, storage, processing power, and other resources to ensure that the network can effectively support current and future demands.

Here are some tools and equipment commonly used in designing network topology:

Software Tools:

- Graphical Network Design Software:
  - Cisco Packet Tracer: Simulates network configurations, making it easy to design, configure, and troubleshoot networks.
  - GNS3 (Graphical Network Simulator-3): Allows for the emulation of network devices and is particularly useful for testing complex network designs.

- Network Diagramming Tools:
  - Microsoft Visio: Popular for creating visual representations of network topologies. It provides a range of templates for different network components.
  - Lucidchart: A cloud-based diagramming tool that supports network diagram creation.
- Network Planning and Design Tools:
  - SolarWinds Network Topology Mapper: Automates the discovery and mapping of network topology.
  - NetBrain: Offers network automation and mapping capabilities.
- Prototyping Tools:
  - Cisco Modeling Labs (CML): Allows for the creation of virtual network prototypes for testing and validation.
  - EVE-NG: An open-source network emulator that supports the emulation of various network devices.
- Network Simulation and Emulation:
  - Wireshark: A network protocol analyzer that helps in understanding and troubleshooting network issues.
  - GNS3 and Packet Tracer (mentioned earlier): Besides design, these tools also provide simulation capabilities.
- Cloud-Based Design Tools:
  - AWS Diagram Tool: An online tool provided by Amazon Web Services for designing AWS-based network architectures.
  - Azure Diagrams: Part of Microsoft Azure, this tool assists in creating diagrams for Azure-based networks.

Hardware Equipment:

- Routers:
  - Cisco ISR (Integrated Services Router): Commonly used for connecting different network segments.
  - Juniper MX Series Routers: Suitable for high-performance networking environments.

- Switches:
  - Cisco Catalyst Series Switches: Widely used for building scalable and secure networks.
  - HPE Aruba Switches: Known for their flexibility and scalability.
- Firewalls:
  - Cisco ASA (Adaptive Security Appliance): Offers security features and controls traffic between different network segments.
  - Palo Alto Networks Firewalls: Known for advanced threat prevention capabilities.
- Wireless Access Points:
  - Cisco Aironet Series: Provides wireless connectivity for devices within a network.
  - Ubiquiti UniFi Access Points: Known for their scalability and management features.
- Network Security Appliances:
  - Cisco Firepower Next-Generation Firewall (NGFW): Combines firewall and intrusion prevention capabilities.
  - Fortinet FortiGate: Offers a range of security services, including firewall and VPN.
- Cabling and Connectors:
  - Ethernet Cables: Cat5e, Cat6, or Cat6a cables for wired connections.
  - Fiber Optic Cables: For high-speed and long-distance connections.
  - Connectors and Adapters: Used to connect different types of cables and devices.
- Network Monitoring Equipment:
  - Network Taps: Allow passive monitoring of network traffic.
  - SPAN Ports (Switched Port Analyzer): Enable the monitoring of network traffic on a switch.
- Power and Cooling Systems:
  - Uninterruptible Power Supply (UPS): Provides backup power during outages.
  - Rack Cooling Systems: Ensure that networking equipment remains within optimal temperature ranges

3.3. Analysing physical environment features based on network design

Analysing the physical environment is a crucial aspect of network design, as the physical characteristics of a location can significantly impact the performance and reliability of a network. Here are some key physical environment features to consider when designing a network:

1. **Location and Geographic Factors:**
    - **Distance Between Locations:** The physical distance between network locations affects the choice of networking technologies. For example, long-distance connections may require fiber optic cables or wireless solutions.
    - **Geographical Layout:** Consider the layout of buildings, campuses, or branches, as it influences the placement of networking equipment and the design of the network topology.
2. **Cabling Infrastructure:**
    - **Cable Pathways:** Analyze the routes for running network cables, considering factors like avoiding interference, minimizing cable lengths, and adhering to safety standards.
    - **Cable Types:** Choose appropriate cable types (e.g., Cat6, fiber optics) based on the distance and bandwidth requirements of the network.
3. **Power and Electrical Considerations:**
    - **Power Outlets:** Ensure that there are sufficient power outlets for networking equipment and consider the placement of uninterruptible power supply (UPS) units.
    - **Electrical Noise:** Identify and mitigate sources of electrical noise that can interfere with network signals.
4. **Climate and Environmental Conditions:**
    - **Temperature Control:** Ensure that networking equipment is placed in environments with controlled temperatures to prevent overheating.
    - **Humidity Levels:** Extreme humidity can damage networking equipment. Choose equipment with appropriate environmental specifications.
    - **Physical Security:** Consider security measures to protect networking equipment from environmental hazards and unauthorized access.
5. **Structural Considerations:**

- **Building Materials:** Different building materials can affect wireless signal propagation. Concrete and metal may impede wireless signals, requiring careful placement of access points.
- **Physical Barriers:** Identify and address physical barriers that may impact network connectivity, such as walls, floors, or partitions.

6. **Expansion and Scalability:**
    - **Room for Growth:** Design the network with scalability in mind to accommodate future expansion. Consider the availability of space for additional equipment and cabling.
    - **Modular Design:** Opt for a modular network design that allows for easy upgrades and expansion without significant disruption.
7. **Physical Security Measures:**
    - **Access Control:** Implement access control measures to secure network equipment from unauthorized access.
    - **Surveillance Systems:** Consider the placement of surveillance cameras to monitor the physical security of networking infrastructure.
8. **Accessibility and Maintenance:**
    - **Equipment Accessibility:** Ensure that networking equipment is easily accessible for maintenance and troubleshooting.
    - **Serviceability:** Design the network with serviceability in mind, making it easy to replace or upgrade components when necessary.
9. **Regulatory and Compliance Considerations:**
    - **Building Codes:** Adhere to local building codes and regulations when installing networking equipment.
    - **Health and Safety Standards:** Comply with health and safety standards to ensure the well-being of personnel working with networking equipment.
10. **Natural Disasters and Redundancy:**
    - **Disaster Recovery Planning:** Consider the potential impact of natural disasters on network infrastructure and develop plans for disaster recovery.
    - **Redundancy:** Implement redundancy in critical components to ensure network availability even in the face of hardware failures.

By carefully analyzing these physical environment features, network designers can develop robust and resilient networks that meet the specific needs of the organization and its operating environment.

3.4. Selecting appropriate network topology

Selecting the appropriate network topology is a critical decision in network design, as it influences factors such as performance, scalability, reliability, and ease of management. The choice of topology depends on the specific requirements and goals of the organization. Here are several common network topologies, along with considerations for their selection:

1. **Bus Topology:**
    - **Advantages:**
        - Simple and easy to implement.
        - Cost-effective for small networks.
    - **Considerations:**
        - Performance may degrade as more devices are added.
        - Susceptible to cable failures, as a single break can disrupt the entire network.

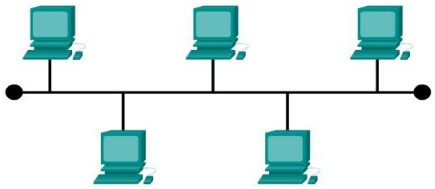


Fig. 3.2. Bus Topology

2. **Star Topology:**
    - **Advantages:**
        - Centralized management and easy troubleshooting.
        - Isolation of device issues without affecting the entire network.
    - **Considerations:**
        - Dependency on the central hub; its failure can disrupt the network.
        - Requires more cabling compared to bus topology.

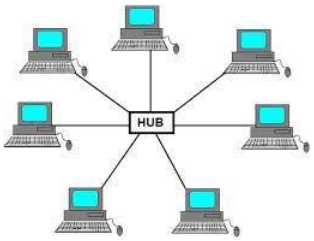


Fig. 3.3. Star Topology

2. **Ring Topology:**
    - **Advantages:**
        - Equal access to network resources.
        - No central hub, reducing the risk of a single point of failure.
    - **Considerations:**
        - Network expansion can be challenging.
        - Failure in one device or connection can disrupt the entire network.

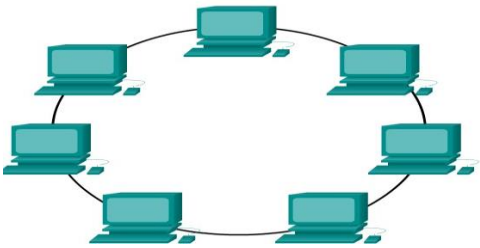


Fig. 3.4. Ring Topology

3. **Mesh Topology:**
    - **Advantages:**
        - High redundancy and fault tolerance.
        - Scalable and supports a high volume of traffic.
    - **Considerations:**
        - Complex to design and implement.
        - Expensive due to the high number of connections.

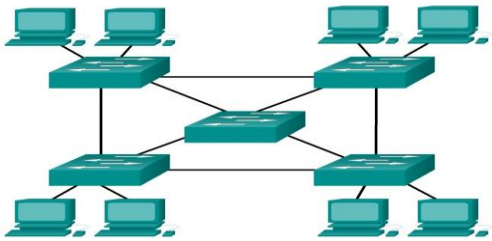


Fig. 3.5. Mesh Topology

4. **Hybrid Topology:**
    - **Advantages:**
        - Combines the strengths of different topologies.
        - Offers flexibility and scalability.
    - **Considerations:**
        - Can be more complex to manage.
        - Cost implications based on the combination chosen.

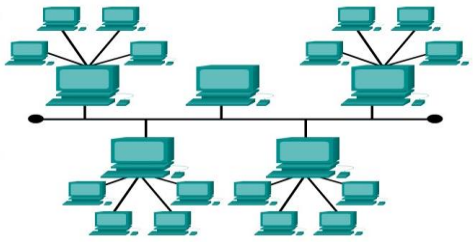


Fig. 3.6. Hybrid Topology

Considerations for selecting an appropriate network topology include:

- The size of the organization
- The volume of network traffic
- Scalability requirements
- Budget constraints, and
- The need for fault tolerance.

A comprehensive understanding of these factors will guide the choice of topology that best aligns with the organization's objectives. In many cases, a combination of topologies or a hybrid approach may be the most suitable solution. Also refer point to point and tree topologies.

Self-check 3

True/False Questions:

1. Bus topology is cost-effective for small networks but may experience performance degradation as more devices are added.
2. GNS3 (Graphical Network Simulator-3) is a software tool used for creating virtual network prototypes for testing and validation.
3. Consideration of climate and environmental conditions in the physical environment analysis involves ensuring sufficient power outlets for networking equipment.

Multiple-Choice Questions:

1. Which network topology is known for being simple and easy to implement but may experience performance degradation as more devices are added?
   A. Ring Topology C. Bus Topology
   B. Star Topology D. Mesh Topology
2. Which software tool automates the discovery and mapping of network topology?
   A. Microsoft Visio C. SolarWinds Network Topology Mapper
   B. Cisco Packet Tracer C. SolarWinds Network Topology Mapper
   D. Lucid chart
3. What is the primary purpose of a Network Tap in network monitoring equipment?
   A. Active monitoring of network traffic C. Emulation of network devices
   B. Passive monitoring of network traffic D. Wireless connectivity for devices

Essay Questions:

1. Explain the significance of analyzing the physical environment features when designing a network.
2. Discuss the role of software tools in designing network topology.
3. Elaborate on the considerations for selecting appropriate network topology.

Operation Sheet 3.1

Operation Title: Designing Network Topology

Purpose: To acquire the trainees with the skill of Designing Network Topology

Equipment, tools and materials required: Computer, Visio Software

Procedures: To design Network Topology, Follow the following procedures

Step 1. Install Microsoft Visio

Step 2. Open a New Diagram

Step 3. Drag and Drop Shapes

Step 4. Connect Shapes

Step 5. Label Shapes

Step 6. Group and Align

Step 7. Use Layers

Step 8. Customize Shapes

Step 9. Include Icons and Symbols

Step 10. Add Data

Step 11. Validate Design:

Step 12. Save and Share:

LAP Test 3.1

Task 1 : Design the Appropriate Topology Using the following Scenario

Scenario: Small Business Network Topology

Business Overview: Imagine a small consulting firm called "Tech Solutions Inc." The company has 30 employees and is expanding its operations. The business requires a robust and secure network infrastructure to support its day-to-day operations, including file sharing, email communication, and access to shared resources.

Reference Books:

1. "Computer Networking: Principles, Protocols and Practice" by Olivier Bonaventure
2. "Computer Networks" by Andrew S. Tanenbaum and David J. Wetherall
3. "Network Warrior" by Gary A. Donahue
4. "CCNA Routing and Switching Complete Study Guide: Exam 100-105, Exam 200-105, Exam 200-125" by Todd Lammle

Websites:

1. Cisco Learning Network (learningnetwork.cisco.com)
2. Network World (networkworld.com)
3. Packet Tracer Tutorials on Cisco Networking Academy (netacad.com)
4. NetworkTopology.com
5. TechNet - Microsoft's Network Topologies Documentation (docs.microsoft.com)

Developers Profile

NO	Name	Qualif	Field of Study	Organization/ Institution	Mobile	E-mail
1	Zerihun Abate	MSc	ITM	Sebata PTC	0911858358	zedoabata2017@gmail.com
2	Abebe Mintafa	MSc	ITM	Ambo TVETC	0929362458	tolabula@gmail.com
3	Endale Bereket	Bsc	Co. Science	M/G/M/B/P/T/C	0915439694	zesaron1221@gmail.com
4	Yinebeb Tamiru	BSC	Co. Science	APTC	0936325182	yinebebtamiru07@gmail.com