

**FINAL PROJECT**

**DOCUMENTATION:**

**Design a campus network for a Mansoura University Using Cisco Packet Tracer**

**team members :**

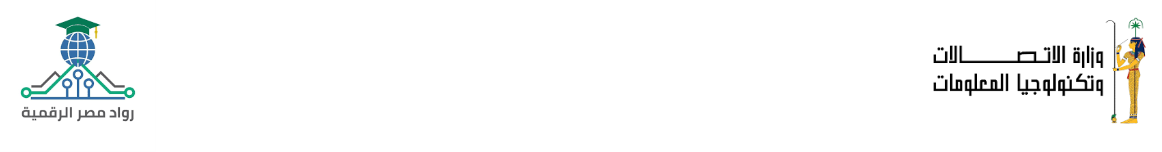
1) sobhy rafik samy

2) Abdelrahman Ragab Ahmed El-Hodairi

3) Ahmed Tarek El-Sayed Helmy

4) Kamal Ahmed Abdelmageed Ali

5) Mohamed Ashraf Mohamed Ali

****

**Table of Contents :**

1) Abstract

2) Introduction

3)Problem Statement

4)Goals and Objectives

5)Current System Overview

6)New System Design and Features

7)Proposed Methodology

1) Hierarchical Network Design

2)VLANs and IP Addressing Scheme

3)Network Devices and Components

4)Advanced Network Security Features

8) Project show

9)Implementation Phases

1)Planning and Design Phase

2)Configuration and Installation Phase

3)Testing and Validation Phase

4)Rollout and Training Phase

10) Risk Assessment and Mitigation

1) Risk Analysis

2)Mitigation Strategies

11) Business Model Overview

12) Expected Outcome

13) Conclusion

**1) Abstract :**

This project involves designing and implementing a comprehensive network topology for Mansoura University, which consists of a main campus and a branch campus. The main campus includes three buildings (A, B, and C) housing various departments such as administration, HR, finance, business, engineering, arts, and IT. The branch campus includes the faculty of health and sciences with separate networks for staff and student labs. The network design follows a hierarchical model with core, distribution, and access layers, ensuring efficient and secure connectivity. Key configurations include VLANs for departmental separation, dynamic IP addressing via DHCP, and routing protocols for internal and external communication. The project is executed using Cisco Packet Tracer, providing a detailed prototype and configuration to meet the specified requirements.

**2) Introduction:**

we embark on the fourth enterprise networking project, focusing on designing and implementing a campus network using Cisco Packet Tracer. This project involves creating a comprehensive network topology for Mansoura University, which consists of a main campus with three buildings and a branch campus. Each building hosts various departments, and the network design incorporates hierarchical models, VLAN configurations, and security settings to ensure efficient and secure connectivity. The project aims to provide end-to-end connectivity and access to internal and external servers, meeting the specific requirements outlined in the case study

**3)Problem Statement :**

Mansoura University, a large institution with two campuses situated 20 miles apart, requires a comprehensive network design to support its diverse departments and faculties. The main campus consists of three buildings (A, B, and C) housing various departments such as administrative staff, finance, engineering, computing, and arts. The branch campus includes the faculty of medicine and sciences, with staff and student labs situated. The network must ensure secure and efficient connectivity for all departments, support VLAN configurations, and provide dynamic IP addresses via a router-based DHCP server. Additionally, the network should facilitate access to internal and external servers, including an externally hosted email server on the cloud. The project involves planning, designing, and prototyping the network topology using Cisco Packet Tracer, followed by configuring core and end devices to achieve the required connectivity and functionality.

**4) Goals and Objectives:**

**Goals:**

**Design a network topology:** Create a comprehensive network layout for Albion University, including both the main and branch campuses.

**Implement network configurations:** Set up and configure core and end devices to ensure seamless connectivity and functionality

**Objectives:**

**Create a network topology:** Include main components to support various departments and faculties across different buildings.

**Configure core devices:** Ensure end-to-end connectivity and access to internal and external servers.

**Separate networks:** Assign each department or faculty to its own network with appropriate VLANs and security settings.

**Implement routing protocols:** Use RIPv2 for internal routing and static routing for external networks.

**Dynamic IP addressing:** Configure DHCP servers to provide dynamic IP addresses for devices in Building A.

**5) Current System Overview:**

Before this project, there was no way to communicate buildings with each other on the campus of Mansoura University. There was no means, even a network, for smooth communication and transferring data in a safe, effective, and fast way. Data was transferred in a traditional way. In this project, we connected the campus buildings through simulation on Cisco packet tracer software

**6) New System Design and Features:**

The new network design for Mansoura University incorporates advanced technologies, including VLAN segmentation, RIPv2 routing, DHCP, and cloud-hosted email servers, to secure communication and optimize network performance. This design replaces the manual system with a scalable, digital infrastructure that supports efficient data flow, redundancy, and secure access to university resources.

**The features of the new system include:**

**VLAN Segmentation**: Separates network traffic between departments, enhancing security and minimizing congestion.

**RIPv2 Routing Protocol:** Ensures reliable data routing between the main and branch campuses.

**DHCP Server:** Provides dynamic IP addresses to devices in Building A, simplifying network management.

**Cloud-Hosted Email Server:** Ensures secure and reliable email communication for staff and students.

**Hierarchical Network Design:** Utilizes core, distribution, and access layers to improve scalability and performance.

**Security Measures:** Configured VLANs and security settings on switches to protect the network from unauthorized access and attacks.

**7) Proposed Methodology**

**1) Hierarchical Network Design:**

The proposed network follows a hierarchical model that separates the network into three main layers: the Core, Distribution, and Access layers. This structure optimizes network performance and simplifies troubleshooting by isolating traffic between buildings and departments. The core layer includes a main router, the distribution layer uses layer 3 switches, and the access layer employs layer 2 switches for each department. This design ensures efficient data flow and robust network management across the university’s main and branch campuses.

**2) VLANs and IP Addressing Scheme:**

Each department is assigned its own VLAN, ensuring secure and isolated communication. The VLANs follow a clear IP addressing scheme for efficient routing and management. For example:

**Admin Department:** Assigned VLAN 10 with an IP range of 192.168.1.0/24, ensuring isolation from other departments.

**HR Department:** Assigned VLAN 20 with an IP range of 192.168.2.0/24, ensuring isolation from other departments.

**Finance Department:** Assigned VLAN 30 with an IP range of 192.168.3.0/24, ensuring isolation from other departments.

**Business Department:** Assigned VLAN 40 with an IP range of 192.168.4.0/24, ensuring isolation from other departments.

**Engineering and Computing Department:** Assigned VLAN 50 with an IP range of 192.168.5.0/24, ensuring isolation from other departments.

**Arts and Design Department:** Assigned VLAN 60 with an IP range of 192.168.6.0/24, ensuring isolation from other departments.

**Student Labs:** Assigned VLAN 70 with an IP range of 192.168.7.0/24, ensuring isolation from other departments.

**IT Department:** Assigned VLAN 80 with an IP range of 192.168.8.0/24, ensuring isolation from other departments.

**Staff Department (Branch Campus):** Assigned VLAN 90 with an IP range of 192.168.9.0/24, ensuring isolation from other departments.

**Student Labs (Branch Campus):** Assigned VLAN 100 with an IP range of 192.168.10.0/24, ensuring isolation from other departments

**3) Network Devices and Components:**

The network devices and components for this project include:

**Main Campus Router**: Central router for the main campus.

**Layer 3 Switch:** Used at the distribution layer.

**Access Layer Switches:** For each department in buildings A, B, and C.

**PCs and Printers:** For each department.

**Servers:** Including web server, FTP server, and external email server.

**Cables:** Various types for connecting devices.

**Cloud Router:** For connecting to the external email server.

These components are used to design and implement the network topology for Mansoura University’s main and branch campuses.

**4) Advanced Network Security Features:**

some important security considerations:

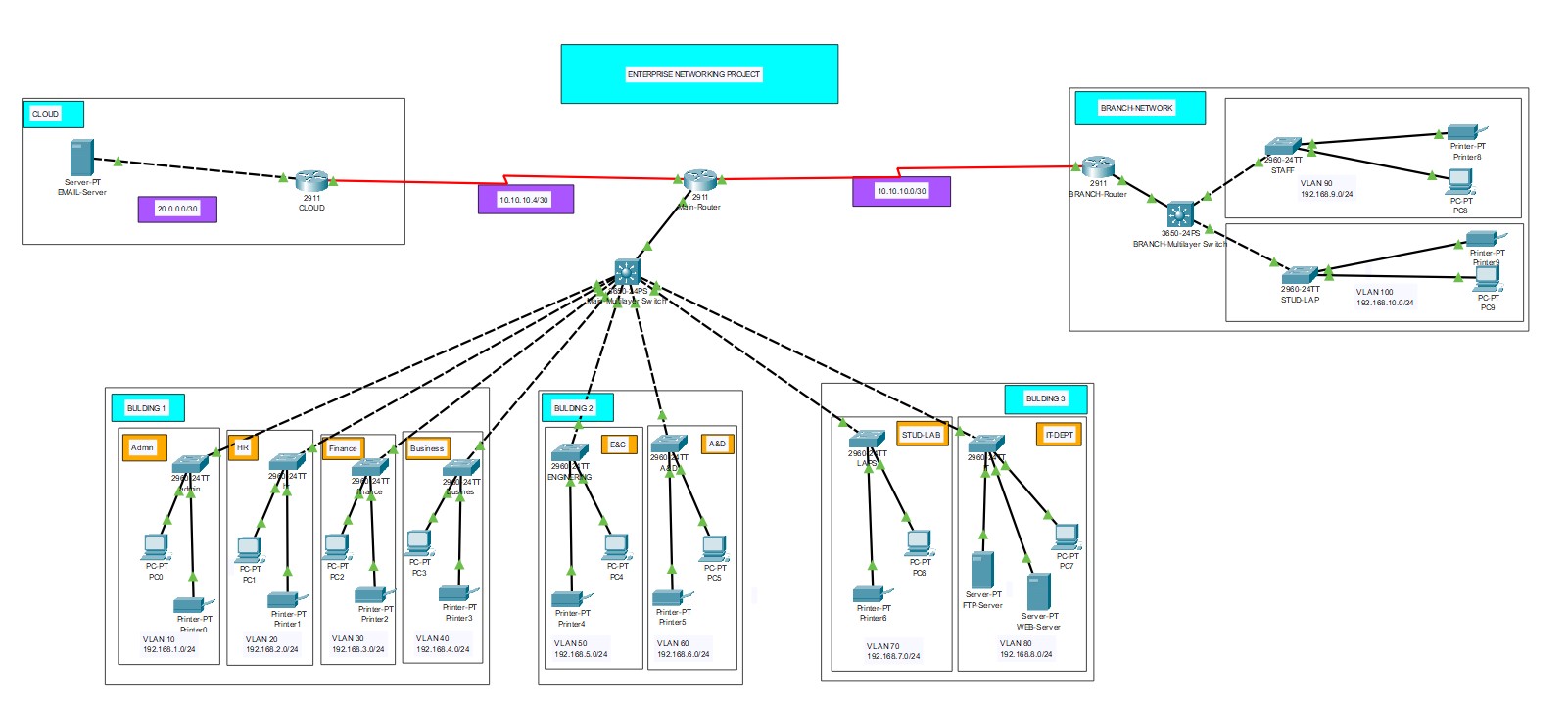
**Separate Networks:** Each department or faculty is on its own separate network, enhancing security by isolating traffic .

**VLAN Configuration:** Switches are configured with appropriate VLANs and security settings to control and secure network traffic .

**Routing Protocols:** RIPv2 is used for internal routing, and static routing is used for external networks, ensuring secure and efficient data routing .

**8) Project show:**

**1)** **Packet tracer:**



**2) Ip ranges**

**Main branch**

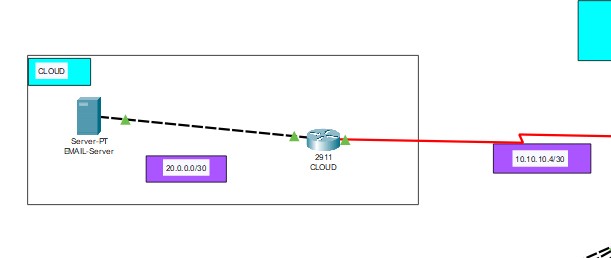
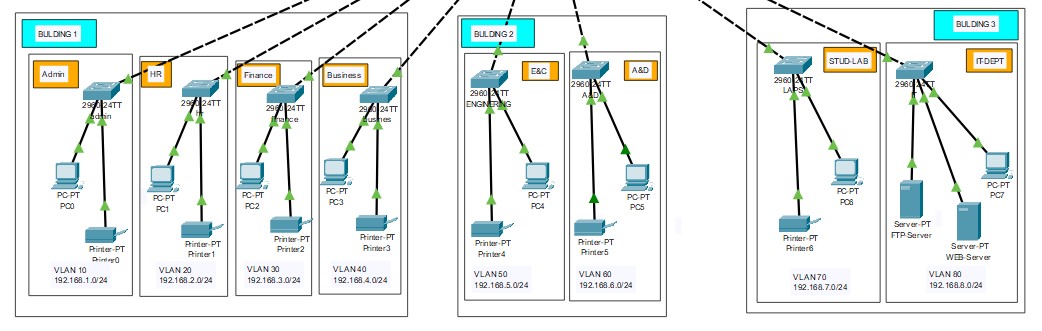
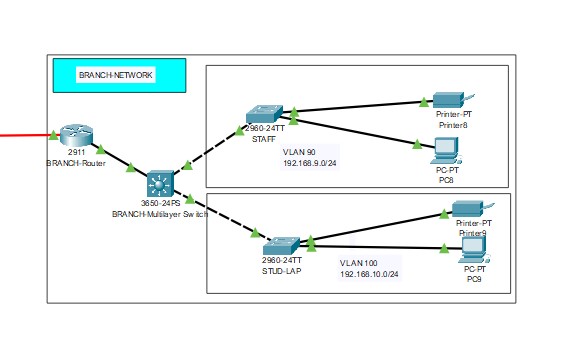
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Department** | **Network address** | | **Subnet mask** | **Host address range** | **broadcast** |
| **Admin** | 192.168.1.0 | | 255.255.255.0 | 192.168.1.1 - 192.168.1.254 | 192.168.1.255 |
| **HR** | 192.168.2.0 | | 255.255.255.0 | 192.168.2.1 - 192.168.2.254 | 192.168.2.255 |
| **Finance** | 192.168.3.0 | | 255.255.255.0 | 192.168.3.1 - 192.168.3.254 | 192.168.3.255 |
| **Business** | 192.168.4.0 | | 255.255.255.0 | 192.168.4.1 - 192.168.4.254 | 192.168.4.255 |
| **Engineering and Computing** | 192.168.5.0 | | 255.255.255.0 | 192.168.5.1 - 192.168.5.254 | 192.168.5.255 |
| **Arts and Design** | 192.168.6.0 | | 255.255.255.0 | 192.168.6.1 - 192.168.6.254 | 192.168.6.255 |
| **Student Labs** | 192.168.7.0 | | 255.255.255.0 | 192.168.7.1 - 192.168.7.254 | 192.168.7.255 |
| **IT** | | 192.168.8.0 | 255.255.255.0 | 192.168.8.1 - 192.168.8.254 | 192.168.8.255 |

**Second branch**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Building A:** | **Building B:** | **Building C:** |
| **Department** | Admin, HR, Finance, Business | Engineering and Computing, Arts and Design | Student Labs, IT Department |
| **Network address** | 192.168.1.0/24 | 192.168.2.0/24 | 192.168.3.0/24 |
| **Subnet mask** | 255.255.255.0 | 255.255.255.0 | 255.255.255.0 |
| **Host address range** | 192.168.1.1 - 192.168.1.254 | 192.168.2.1 - 192.168.2.254 | 192.168.3.1 - 192.168.3.254 |
| **broadcast** | 192.168.1.255 | 192.168.2.255 | 192.168.3.255 |
|  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Department** | **Network address** | **Subnet mask** | **Host address range** | **broadcast** |
| **Staff Department:** | 192.168.9.0 | 255.255.255.0 | 192.168.9.1 to 192.168.9.254 | 192.168.9.255 |
| **Student Lab Department** | 192.168.100.0 | 255.255.255.0 | 192.168.100.1 to 192.168.100.254 | 192.168.100.255 |

**Presentation of network layout:**



**9)Implementation Phases:**

**1) Planning and Design Phase:**

This phase involves a comprehensive analysis of Mansoura University’s network requirements, identifying key resources, and designing the network topology. Key activities include:

**Requirement Gathering:** Analyzing the case study provided by the client to understand the operational needs and gather input on network features.

**Resource Identification:** Assessing the current infrastructure, hardware, and software requirements to determine necessary upgrades and new installations.

**Network Design:** Creating a detailed network topology that outlines VLAN structures, IP addressing schemes, and the layout of all network components.

**Outcomes**: This phase ensures that the network is tailored to ’Mansoura University’s operational needs and complies with industry security standards, resulting in a comprehensive design document

**2) Configuration and Installation Phase**

**Hardware Installation**: Setting up routers, switches, and other critical network devices in designated locations.

**Configuration:** Implementing VLANs, routing protocols (such as RIPv2), and security measures (including firewall settings) to create a fully functional network.

**System Integration :** Ensuring all components work together seamlessly to support university operations.

**Outcomes:** This phase results in a fully operational network infrastructure ready for testing, ensuring that all devices are configured correctly to meet the university’s requirements

**3) Testing and Validation Phase:**

The testing and validation phase of this project involves several key activities to ensure the network meets performance and security benchmarks:

**Connectivity Testing:** Verifying connections between all buildings and departments to ensure seamless communication.

**Performance Testing:** Conducting stress tests to assess the network’s performance under expected loads and conditions.

**Security Testing:** Implementing penetration testing to identify potential vulnerabilities in security protocols and validate compliance with security standards.

**Outcomes:** This phase provides a comprehensive testing report detailing findings, including any issues encountered and a plan for remediation, ensuring that the network is secure and performs optimally

**4) Rollout and Training Phase**

After successful testing, the network is rolled out in stages to minimize disruption to university operations. Key activities include:

**Phased Rollout:** Gradually deploying the network across buildings and departments, ensuring that any issues can be addressed without affecting the entire university.

**Staff Training:** Conducting training sessions for administrative and academic personnel to familiarize them with the new system, including its features and security protocols.

**Support Resources:** Providing documentation and resources for ongoing support and establishing a feedback mechanism for users.

**Outcomes:** This phase culminates in a fully functional university network system with staff trained and ready to utilize the network effectively, enhancing operational efficiency and academic activities

**5) Conclusion of Implementation Phases**

The structured approach to the implementation phases is crucial for the successful deployment of the campus network system. By carefully executing each phase, the university can ensure a secure, reliable, and scalable network that enhances educational services and optimizes administrative operations

**10) Risk Assessment and Mitigation**

**1) Risk Analysis**

The network design and implementation project for Albion University faces several risks that could impact its operations and security. As a large educational institution, any interruption in service or data breach could lead to delays in academic activities, financial loss, and reputational damage. The key risks associated with the university network system include:

**Data Breaches:** University data, including student and staff records, is highly sensitive and often targeted by cybercriminals. A breach could result in exposure of confidential information, leading to non-compliance with data protection regulations, potential lawsuits, and a loss of trust.

**Unauthorized Access:** Without proper access control, unauthorized users or malicious actors could gain entry into the university’s network. This access could allow them to tamper with or steal critical information, install malware, or disrupt university services.

**Equipment Failure:** The network relies heavily on hardware, such as routers, switches, servers, and firewalls. Hardware malfunctions or failures could lead to network outages, disrupting university services such as online classes, administrative tasks, and research activities.

**Downtime:** Whether caused by hardware failure, cyberattacks, or software issues, downtime can severely disrupt university operations. Systems that support student registration, academic records, and online learning platforms must be available 24/7. Prolonged downtime could delay academic activities and lead to loss of revenue.

**Cyberattacks:** Ransomware, phishing attacks, and Distributed Denial of Service (DDoS) attacks pose significant risks to the network. Cybercriminals target educational institutions due to the value of the data and the potential willingness to pay ransoms to regain control over operations.

**2)** **Mitigation Strategies**

1. **Regular Security Audits**: Conduct periodic security audits, including penetration testing and vulnerability scanning, to identify and address potential vulnerabilities.
2. **Redundant Systems and Backups**: Implement redundancy in hardware and network paths, including backup servers and alternative communication paths, to minimize downtime and data loss.
3. **Strong Encryption and Access Control**: Use encryption for sensitive data at rest and in transit. Implement multi-factor authentication (MFA) and role-based access control (RBAC) to restrict access to critical systems.
4. **Staff Training and Awareness Programs**: Provide comprehensive training for employees on identifying phishing attacks, maintaining strong passwords, and adhering to security protocols to reduce human error.
5. **Incident Response and Recovery Plans**: Develop and maintain an incident response plan to ensure quick detection, containment, and recovery in case of a cyberattack or breach.
6. **Physical Security Controls**: Restrict physical access to critical network devices using biometric authentication, surveillance, and secure access points to prevent unauthorized tampering.

**11) Business Model Overview:**

**MAIN PROBLEMS**

1. **Complex Network Topology**:
   * The university’s network spans multiple buildings and campuses.
   * Each building hosts multiple departments with specific networking needs.
   * Ensuring seamless connectivity and communication across all departments is challenging.
2. **Segregation of Networks:**
   * Each department and faculty must be on its own separate network.
   * Configuring VLANs and security settings for each department is complex.
   * Ensuring proper isolation and security for each network segment is crucial.
3. **Dynamic IP Address Allocation**:
   * Devices in Building A need to acquire dynamic IP addresses from a router-based DHCP server.
   * Proper configuration and management of the DHCP server are essential.
   * Ensuring reliable IP address allocation without conflicts is necessary.
4. **External Email Server Integration:**
   * The university’s email server is hosted externally on the cloud.
   * Ensuring secure and reliable access to the external email server is vital.
   * Proper routing and security measures must be in place for external communications.
5. **Routing and Security Protocols:**
   * RIPv2 is used for internal routing, and static routing is used for external networks.
   * Configuring and maintaining these routing protocols requires expertise.
   * Implementing appropriate security protocols to protect the network is essential

**KEY ACTIVITIES**

1. **Planning and Designing the Network Topology:**
   * Analyze the case study and requirements.
   * Design a hierarchical network model with core, distribution, and access layers.
   * Create a network topology using Cisco Packet Tracer.
2. **Configuring Core and End Devices:**
   * Configure routers, switches, and other core devices.
   * Set up VLANs and security settings for each department.
   * Ensure dynamic IP addressing with a router-based DHCP server.
3. **Implementing Routing Protocols:**
   * Use RIPv2 for internal network routing.
   * Implement static routing for external networks.
   * Configure routing to ensure end-to-end connectivity.
4. **Connecting Main and Branch Campuses:**
   * Design and implement connections between main and branch campuses.
   * Use serial connections and appropriate interfaces.
   * Ensure seamless communication between campuses.
5. **Testing and Validating the Network:**
   * Perform comprehensive testing to ensure network reliability and performance.
   * Validate connectivity and access to internal and external servers.
   * Adjust configurations based on test results.
6. **Documentation and Reporting:**
   * Produce detailed reports on network design and implementation.
   * Document configurations and settings for future reference.
   * Provide recommendations for network maintenance and scaling

**REVENUE & COSTS**

**Revenue:**

* **Cost Savings:** By internalizing network management, the university reduces long- term operational costs previously incurred through third-party IT services.
* **Improved Service Quality:** Enhancing network infrastructure can improve educational services, potentially increasing student satisfaction and enrollment, which translates into higher revenues.

**Costs:**

**Initial Investments:** Acquiring network hardware (routers, switches, firewalls), software (monitoring tools, security software), and setting up the infrastructure.

**Training**: Training IT personnel and university staff on using the new systems and ensuring they are aware of security protocols.

**Ongoing Costs:** Maintenance, upgrades, software licensing, and security monitoring services.

**12) Expected Outcome:**

**Enhanced Connectivity:** The new network will provide seamless connectivity across the main and branch campuses, ensuring that students and staff can access resources and communicate effectively.

**Improved Network Performance:** With a hierarchical network design, the system will offer better performance and reliability, reducing latency and improving data transfer speeds.

**Increased Security:** The network will feature VLANs and security settings to protect against unauthorized access and cyber threats, ensuring the safety of sensitive university data.

**Scalability:** The modular design allows for easy expansion, enabling the university to add new departments or services without major disruptions.

**Centralized Management:** The network will support centralized management, making it easier to monitor and maintain, thus reducing the workload on IT staff.

**Compliance with Standards:** The network will adhere to industry standards and best practices, ensuring compliance with relevant regulations and enhancing overall network integrity

**13) Conclusion:**

The transition from a fragmented and inefficient university network to a cohesive, secure, and scalable network architecture marks a significant advancement for Mansoura University’s operations. The implementation of VLAN segmentation, hierarchical design, and robust security settings ensures that each department operates efficiently while maintaining high security standards.

The hierarchical network design, featuring core, distribution, and access layers, guarantees reliable performance and easy scalability as the university expands. By integrating advanced technologies and security protocols, this network infrastructure provides a solid foundation for delivering high-quality educational services now and in the future. The university will benefit from improved operational efficiency, enhanced security, and compliance with industry regulations.This documentation serves as a comprehensive guide to the Mansoura University network system project and is structured to meet the standards expected by stakeholders and relevant authorities