**Sir Syed University of Engineering & Technology**

# (SSUET)Software Engineering Department

***Course Name:* Computer Communication & Networks (SE- n**

**306L)**

***Semester: 5th***

***Batch: 2022F***

***Section: “F”***

**PROJECT REPORT**

|  |  |  |  |
| --- | --- | --- | --- |
| **STUDENT’S NAME Yagome Hina** |  |  | **2022F-SE-305** |
| **STUDENT’S NAME Tineshia Dsouza** |  |  | **2022F-SE-265** |
| **STUDENT’S NAME Ayesha Ghouri** |  |  | **2022F-SE-284** |
| **STUDENT’S NAME Syeda Asfa Naveed**  **STUDENT’S NAME Aiza Asif** |  |  | **2022F-SE-354**  **2022F-SE-050** |

***Project Title: Campus Network System (CNS)***



***Submitted To: Shazia Ilyas***

***Submitted By:***

## TABLE OF CONTENTS

|  |  |  |
| --- | --- | --- |
| S. No. | TOPICS | PAGE No. |
| 1 | PROBLEM DOMAIN | 3-4 |
| 2 | Security Measures | 5 |
| 3 | Deliverables | 6 |
| 4 | SOFTWARE AND HARDWARE SPECIFICATIONS | 6 |
| 5 | Project Results | 7 |

**PROBLEM DOMAIN**

### Project Overview

This project involves the design and implementation of a **School Management System Network** to provide secure, reliable, and scalable connectivity for different departments within a school campus. The network design ensures efficient communication between Boys Campus, Girls Campus, Academic Blocks, IT Consulting, Library, and other functional areas while integrating automation, security, and optimized routing.

### Network Design Statements

1. **Topology Structure**:
   * The network follows a hierarchical topology with centralized routing and distributed switches connecting various campus zones. o Key zones include:
     + **Boys Campus** (192.168.3.0/24)
     + **Girls Campus** (192.168.3.0/24)
     + **Academic Blocks** (192.168.1.0/24)
     + **IT Consulting** (192.168.1.0/24)
     + **Library** (192.168.1.0/24) o Access points are deployed for wireless connectivity.

1. **Routing and Switching**:
   * **Routing**: Implemented via three main routers:
     + **Campus Router** (192.168.3.1 as gateway)
     + **Main Router** (192.168.2.1 as gateway for Server Center)
     + **Academic Router** (192.168.1.1 as gateway for Academic Blocks, IT

Consulting, and Library)

* + **Switching**: Core and access layer switches handle VLAN segmentation, interVLAN routing, and network redundancy using STP.

1. **IP Addressing and Subnetting**:
   * Efficient subnetting is used for department-level segmentation.
   * Each zone uses a separate IP range:
     + Boys Campus: 192.168.3.0/24
     + Girls Campus: 192.168.3.0/24
     + Academic Blocks, IT Consulting, Library: 192.168.1.0/24
     + Server Center: 192.168.2.0/24
2. **Device Connectivity**:
   * Devices like PCs, laptops, and smartphones are connected via wireless access points or directly through switches.
   * Key configurations:
     + **Access Points** provide wireless connectivity with a password ("1234567890").
     + **Servers** (Email, DNS, and Web) are centralized in the Server Center (192.168.2.x).

### Security Measures

1. **Access Control**:
   * ACLs are implemented to restrict communication between VLANs.
   * Secure SSH is configured for router and switch management (e.g., ssh password:

admin).

1. **Password Policies**: o Console and SSH passwords are enforced (e.g., muj@123 for Campus Router).
2. **Encryption**:
   * Wireless networks are secured with WPA2/WPA3 encryption protocols.
3. **Firewall Implementation**:
   * Firewalls secure the core router (Main Router) to control external access to the server center.

**Automation**

1. VLAN configurations and IP assignments can be automated using Python scripts or REST APIs.
2. Scripts can manage repetitive tasks, such as creating VLANs, assigning devices to VLANs, and updating ACLs.

**Network Performance and Testing**

1. **Testing Tools**:
   * Connectivity testing between zones using ping and traceroute. o Debugging misconfigurations using router/switch commands.
2. **Performance Optimization**:
   * **EtherChannel** is implemented for link aggregation between switches to enhance throughput. o STP prevents loop issues in the switching infrastructure.
3. **Network Troubleshooting**:
   * Regular monitoring and quick resolution of routing or VLAN misconfigurations.
   * Connectivity to servers is verified from all zones.

### Deliverables

1. **Network Diagram**:
   * A clear, well-labeled topology of all devices, IP addresses, and connections (provided in the image).
2. **Configuration Details**:
   * Command sets for router, switch, VLAN, and ACL configurations.
3. **Security Implementation**:
   * A summary of passwords, ACLs, and wireless security measures.
4. **Automation Scripts**:
   * Python scripts for automating VLAN and ACL configurations.
5. **Project Report**:
   * Include objectives, configurations, testing results, and future scalability suggestions.
6. **Presentation**:
   * Highlight problem statement, key features (e.g., VLAN segmentation, security), testing outcomes, and challenges faced.

**SOFTWARE AND HARDWARE SPECIFICATIONS**

**Hardware:**

* **Routers**: Cisco 1941 ISR (3 units) for dynamic routing, secure management, and inter-

VLAN routing.

* **Switches**: Cisco Catalyst 2960-24TT (3 units) supporting VLANs, STP, and EtherChannel.
* **Access Points**: Cisco Aironet 1832i (6 units) for wireless connectivity.
* **Servers**: Rack-mounted (3 units for Email, DNS, Web).
* **Client Devices**: PCs, laptops, smartphones (4GB RAM, Core i3 minimum).
* **Cabling & Accessories**: Cat5e/Cat6, fiber optics, UPS, and rackmounts.
* **Software Operating Systems**: Windows/macOS/Android/iOS for clients.
* **Simulation Tools**: Cisco Packet Tracer, GNS3.
* **Protocols**: OSPF, EIGRP, RIP, VLANs, and VPN.
* **Security**: WPA2/WPA3 encryption, ACLs, SSH.
* **Automation & Monitoring**: Python, REST APIs, Ansible, Wireshark, SolarWinds.

**Project Output:**

