Project Title:

Network Design for a Large University

Ade Abujade

Overview

This report outlines the design and implementation of a network topology to support a main campus and a smaller campus. The network will serve various departments, faculties, and labs, ensuring efficient communication, security, and scalability. Both campuses will be interconnected, with an external cloud-hosted email server integrated into the network.

Objectives

The objective of this network design is to:

- Provide seamless and secure communication across departments and faculties.
- Ensure logical separation using VLANs and IP subnetting.
- Support dynamic IP address allocation for devices in Building A.
- Implement RIPV2 for internal routing and static routes for external communication with the cloud-hosted email server.
- Optimize network performance, scalability, and security.

Implementation Plan

Main Campus

Building A: Administrative Staff and Faculty of Business

- **Departments: Management, HR, Finance, and the Faculty of Business.**

- **Network Configuration:**
    - Devices will be assigned to separate VLANs for each department and the Faculty of Business.
    - VLANs:
        - VLAN 10: Admin
        - VLAN 20: HR
        - VLAN 30: Finance
        - VLAN 40: Business
    - A router-based DHCP server will provide dynamic IP addresses for all devices in Building A.
    - Switches will be configured to support VLAN tagging and inter-VLAN communication.

Building B: Faculty of Engineering and Computing, Faculty of Art and Design

- **Network Configuration:**
    - VLANs:
        - VLAN 50: Faculty of Engineering and Computing
        - VLAN 60: Faculty of Art and Design
    - Separate IP networks will be assigned to each faculty.
    - Switches will be configured with VLANs for traffic segmentation.

Building C: Student Labs and IT Department

- **Network Configuration:**
    - VLANs:
        - VLAN 70: Student Labs
        - VLAN 80: IT Department
    - The IT department will host critical servers, including the university web server and other internal servers.
    - Port security will be configured on the switches to prevent unauthorized access to the servers.

External Email Server

- The university's email server is hosted externally in the cloud.
- A static route will be configured on the main campus router to communicate with the cloud-hosted email server.

Smaller Campus: Faculty of Health and Sciences

- **Network Configuration:**
    - VLANs will be created for each department within the Faculty of Health and Sciences.
    - Separate IP networks will be assigned to each department.
    - The smaller campus router will use RIPV2 for routing internal traffic and static routing for communication with the main campus and the external email server.

Routing and IP Configuration

RIPV2 for Internal Routing

- RIPV2 will be implemented on the routers within the main and smaller campuses to handle dynamic routing of internal traffic.
- This ensures efficient route updates and supports scalability for future expansion.

Static Routing for External Communication

- A static route will be set up on both campus routers to facilitate communication with the cloud-hosted email server.

Switch and VLAN Security Settings

- VLAN tagging and trunking will be configured to ensure inter-VLAN communication via the routers.
- Port security will be implemented to:
    - Limit the number of MAC addresses per port.
    - Prevent unauthorized devices from accessing the network.
- Access Control Lists (ACLs) will be used to restrict traffic to specific VLANs and sensitive servers.

IP Addressing Plan

Each VLAN will have a unique subnet to ensure efficient IP allocation and avoid conflicts. For example:

- VLAN 10: 192.168.1.0/24 (Management)
- VLAN 20: 192.168.2.0/24 (HR)

- VLAN 30: 192.168.3.0/24 (Finance)
- VLAN 40: 192.168.4.0/24 (Faculty of Business)
- VLAN 50: 192.168.5.0/24 (Faculty of Engineering and Computing)
- VLAN 60: 192.168.6.0/24 (Faculty of Art and Design)
- VLAN 70: 192.168.7.0/24 (Student Labs)
- VLAN 80: 192.168.8.0/24 (IT Department)
- VLAN 90: 192.168.9.0/24 (Staff Lab)
- VLAN 100: 192.168.10.0/24 (Student Lab)

Testing and Verification

- DHCP functionality will be tested in Building A to ensure devices acquire dynamic IP addresses correctly.
- Inter-VLAN communication will be verified using ping tests between devices in different VLANs.
- RIPV2 routes will be checked using the show ip route command on routers.
- Static routes to the external email server will be tested by accessing the server from a test device.
- Port security will be tested by attempting to connect unauthorized devices to secure ports.

Conclusion

This network topology provides a robust and secure framework for the university's main and smaller campuses. By leveraging VLANs, RIPV2, and static routing, the design ensures efficient communication and scalability. Security measures, such as port security and ACLs, further protect critical resources from unauthorized access.