Case Study ID: UNI-VLAN-STU-FAC-1024

1.Title: University VLANs for Student and Faculty Networks: Enhancing Security and Network Efficiency

2. Introduction

- Overview: This case study explores how a university can implement VLANs (Virtual Local Area Networks) to separate student and faculty networks, improving performance, security, and management.
  VLANs allow logical segmentation of devices connected to the same physical network infrastructure but operate in isolated virtual networks.
- Objective : The objective is to design an efficient, secure, and scalable network structure through VLANs to:
  Isolate student and faculty traffic.
  Improve network management.
  Enhance security by limiting access between different network segments.

3. Background

- Organization/System /Description : The university hosts thousands of students, faculty members, and administrative staff. It offers several network-enabled services such as Wi-Fi, computer labs, faculty portals, and e-learning platforms.
- Current Network Setup:
  A single flat network shared among students, faculty, and other departments.
  Congestion and slow response times are common during peak hours.
  No segmentation, making it hard to monitor and control data access.

4. Problem Statement

- Challenges Faced :
  Security Risks: Sensitive faculty and administrative data are vulnerable due to the lack of isolation.
  Complex Management: Managing all devices on a flat network is time-consuming.
  Limited Access Control: Difficulty in restricting services based on user roles (student, faculty, staff).

5. Proposed Solutions

- Approach : Implementing VLANs to segment traffic logically:
  Create separate VLANs for students, faculty, administration, and guest networks.

Use Layer 3 switches to route traffic between VLANs where necessary.
Apply Access Control Lists (ACLs) to limit communication between VLANs.

Technologies/Protocols Used :

VLAN Protocols: IEEE 802.1Q tagging.
Switches: Managed Layer 2/3 switches.
Routing Protocols: OSPF or static routing for inter-VLAN communication.
Authentication: RADIUS or LDAP for network access control.
Monitoring Tools: SNMP and network monitoring dashboards.

6. Implementation

- Process :

  Network Assessment: Evaluate current network infrastructure and identify devices.
  VLAN Design: Define specific VLANs for students, faculty, administration, and guests.
  Switch Configuration: Set up switches to support VLAN tagging and trunk ports.
  Security Policy Setup: Create Access Control Lists (ACLs) and define Quality of Service (QoS) policies.
  Testing: Conduct connectivity tests and validate security measures.
  Final Deployment: Roll out the VLAN configuration and monitor the network post-deployment.
- Implementation :

  Designing and configuring VLANs according to the needs of different user groups.
  Setting up managed switches and applying security measures like ACLs.
  Testing the entire setup to ensure functionality and security.
  Deploying the VLAN configuration across the university's network and monitoring for performance and security.
- Timeline :

  Network Assessment: 2 weeks
  VLAN Design: 1 week
  Switch Configuration: 1 week
  Security Policy Setup: 2 weeks
  Testing: 1 week
  Final Deployment: 1 week

7. Results and Analysis

- Outcomes :
- Reduced Congestion: Traffic isolated between students and faculty improved network performance.

  Improved Security: Faculty networks are now protected from unauthorized access by students.

Enhanced Control: Policies can limit access to sensitive resources based on roles.

- Analysis :
  Performance: Latency reduced by 30% during peak hours.
  Security Incidents: No unauthorized access reported post-implementation.
  Scalability: Network can easily accommodate new departments or guest users by creating additional VLANs.

8. Security Integration

- Security Measures :
  Network Access Control (NAC): Devices are authenticated before joining the network.
  Firewall Rules: Only approved VLANs can communicate through Layer 3 routing.
  Intrusion Detection Systems (IDS): Monitors traffic for potential threats.

9. Conclusion

- Summary : The implementation of VLANs at the university solved several challenges, such as congestion, security risks, and management complexity. The new setup provides a more organized and secure environment for students, faculty, and administration.
- Recommendations :
  Regular Network Audits: Conduct periodic audits to maintain network security.
  Training Sessions: Educate staff and students on secure network practices.
  Monitoring Tools: Use dashboards to monitor VLAN traffic in real-time.

10. References

Citations : Reference Research papers :

IEEE Std 802.1Q-2018: Standard outlining VLAN tagging specifications for network implementation.

Tanenbaum, A. S., & Wetherall, D. J. (2013). *Computer Networks*: Comprehensive textbook covering networking principles, including VLANs.

Cisco Systems. (2021). "VLAN Configuration and Troubleshooting": Practical guide for configuring and troubleshooting VLANs using Cisco switches.

NAME: G.Varshitha

ID-NUMBER:2320030364

SECTION-NO:07