Case Study ID: -2320030120

**Segregation of Network Traffic in Corporate Office through VLANs and ACLs**

Introduction

Overview: -

In a corporate environment, effective communication and data security are paramount. The need for segregating network traffic among different departments—HR, Finance, and IT—ensures that sensitive information is protected while allowing necessary interactions.

Objective: -

The primary objective is to implement VLANs and Access Control Lists (ACLs) to create a secure and efficient network infrastructure that meets the specific communication needs of each department.

Background

Organization/System Description

The corporate office comprises three main departments: HR, Finance, and IT. Each department has distinct functions, data sensitivity levels, and communication requirements, necessitating a tailored approach to network management.

Current Network Setup

The existing network setup features a flat architecture with no segmentation, leading to potential security vulnerabilities and inefficient traffic management. All departments share the same broadcast domain, increasing the risk of data breaches and unauthorized access.

Problem Statement

Challenges Faced

- Lack of network segmentation leading to data exposure.

- Difficulty in monitoring and controlling inter-departmental traffic.

- Increased risk of unauthorized access to sensitive information.

Proposed Solutions

Approach: -

The proposed solution involves creating separate VLANs for each department, applying ACLs on the Layer 3 switch to control traffic flow, and ensuring that communication adheres to departmental needs.

Technologies/Protocols Used: -

- VLANs (IEEE 802.1Q): For logical segmentation of networks.

- ACLs (Access Control Lists): To enforce security policies and control traffic between VLANs.

- Layer 3 Switches: For routing between VLANs while maintaining security.

Implementation

Process

1. Network Assessment: Evaluate current network infrastructure and identify requirements.

2. VLAN Configuration: Create VLANs for HR, Finance, and IT.

3. ACL Development: Define access rules based on departmental needs.

4. Testing: Validate configurations in a controlled environment.

Implementation

- Configure VLANs on the Layer 3 switch.

- Apply ACLs to restrict traffic between VLANs.

- Monitor traffic to ensure compliance with security policies.

Timeline

- Week 1-2: Network assessment and planning.

- Week 3: VLAN configuration and ACL development.

- Week 4: Testing and validation.

- Week 5: Full deployment and monitoring setup.

Results and Analysis

Outcomes

- Successful segregation of network traffic among departments.

- Enhanced security and reduced risk of data breaches.

- Improved network performance due to reduced broadcast traffic.

Analysis

Post-implementation analysis indicates a significant reduction in unauthorized access attempts and improved monitoring capabilities.

Security Integration

Security Measures

- Regular audits of ACL configurations.

- Implementation of additional security protocols (e.g., 802.1X for port security).

- Continuous monitoring of network traffic for anomalies.

Conclusion

Summary

The implementation of VLANs and ACLs has successfully segmented the network, ensuring secure communication between the HR, Finance, and IT departments while minimizing security risks.

Recommendations

- Regularly review and update ACLs to adapt to changing departmental needs.

- Consider further segmentation or additional security measures as the organization grows.

References

-Research papers on VLAN implementation and security protocols.

- Industry standards for network segmentation and access control.

**NAME: V. Charan Sai**

**ID-NUMBER:2320030120**

**SECTION-NO: 1**