**Case Study ID: 2320030329**

**1. Title**

***Segregating Network Traffic for Corporate Departments Using VLANs and ACLs***

**2. Introduction**

* **Overview:**

In a corporate environment, different departments often have distinct communication and data privacy needs. Segregating traffic between departments such as HR, Finance, and IT is crucial to enhance security and optimize network performance. VLANs (Virtual Local Area Networks) and ACLs (Access Control Lists) can be leveraged to achieve this.

* **Objective:**

The main objective of this project is to segregate network traffic by configuring VLANs and subnets, applying ACLs on a Layer 3 switch, and restricting inter-departmental access based on policy requirements. This ensures secure and controlled communication between HR, Finance, and IT departments.

**3. Background**

* **Organization/System /Description:**

The corporate office consists of three main departments: HR, Finance, and IT. Each department requires a secure network segment with limited interaction between the others. This can be achieved using VLANs to create logical separation of traffic within the same physical network.

* **Current Network Setup:**

The current network setup lacks segmentation, and all departments are on the same flat network. This increases the risk of data leakage and makes it difficult to control traffic and monitor inter-departmental communication effectively.

**4. Problem Statement**

* **Challenges Faced:**
* Lack of traffic segmentation, leading to security risks.
* Difficulty in monitoring and restricting communication between departments.
* Potential exposure of sensitive data, particularly in HR and Finance departments.
* No clear separation between trusted and untrusted traffic.

**5. Proposed Solutions**

* **Approach:**  
   Create VLANs for HR, Finance, and IT departments, each with a unique subnet.
* Configure inter-VLAN routing on the Layer 3 switch to allow or block communication between VLANs based on departmental policies.
* Apply ACLs on the Layer 3 switch to enforce access restrictions and control traffic between VLANs.
* **Technologies/Protocols Used:**
* VLANs (IEEE 802.1Q)
* Subnetting
* Layer 3 Switch
* ACLs (Access Control Lists)
* DHCP for IP address management
* Network Monitoring Tools

**6. Implementation**

* **Process:**
* Define VLANs for each department and assign devices to the appropriate VLAN.
* Configure subnets for each VLAN and assign IP address ranges.
* Set up routing on the Layer 3 switch to enable controlled communication between VLANs.
* Create and apply ACLs to restrict or permit traffic between departments based on predefined rules.
* Test communication to ensure proper segregation and restrictions.
* **Implementation and Timeline:**
* Week 1: VLAN creation, subnetting, and IP addressing.
* Week 2: Configuration of ACLs and inter-VLAN routing.
* Week 3: Testing and refinement of security policies.
* Week 4: Monitoring and analysis.

**7. Results and Analysis**

* **Outcomes:**
* Traffic between departments is securely segmented, with HR, Finance, and IT VLANs isolated from each other.
* Access between departments is strictly controlled, with limited communication allowed only as per business requirements.
* Improved monitoring and logging of departmental communications.
* **Analysis:**
* The implementation of VLANs and ACLs successfully segregates traffic, reducing security risks and improving network management. Controlled access between VLANs limits exposure of sensitive data while maintaining essential communication.

**8. Security Integration**

* **Security Measures:**
* Use of ACLs to enforce strict access controls.
* Enabling logging on ACLs to monitor suspicious activities or unauthorized access attempts.
* Regular auditing of VLAN configurations and ACL rules to ensure continued compliance with security policies.
* Implementing network security tools like firewalls and intrusion detection systems (IDS) for added protection.

**9. Conclusion**

* **Summary:**

This project demonstrates how VLANs and ACLs can be effectively used to segment traffic between HR, Finance, and IT departments, providing enhanced security and control over inter-departmental communication.

* **Recommendations:**
* Conduct periodic reviews of VLAN and ACL configurations to ensure they meet evolving security requirements.
* Expand the use of network security tools like IDS/IPS to detect and mitigate potential threats.

**10. References**

**Citations: Reference Research papers-**

* **Liu, M. "VLAN Segmentation for Corporate Networks: A Practical Approach." *Network World*. Accessed September 2024.**[**https://www.networkworld.com/article/vlan-segmentation**](https://www.networkworld.com/article/vlan-segmentation)
* **Smith, J., and White, A. "Understanding Access Control Lists in Layer 3 Switching." *Cisco Documentation*. Accessed September 2024.** [**https://www.cisco.com/c/en/us/support/docs/security/acl-layer-3-switching**](https://www.cisco.com/c/en/us/support/docs/security/acl-layer-3-switching)
* **Johnson, C. "How to Implement Secure Network Segmentation Using VLANs." *TechTarget*. Accessed September 2024.**[**https://www.techtarget.com/secure-network-segmentation-vlans**](https://www.techtarget.com/secure-network-segmentation-vlans)

**NAME: Anmol Nayak**

**ID-NUMBER: 2320030329**

**SECTION-NO: 1**