**Case Study ID: 52**

**1. Title**

Secure Traffic Segmentation for Corporate Departments using VLANs, Subnets, and ACLs

**2. Introduction**

**• Overview:**

This report outlines a solution to segregate network traffic within a corporate office between HR, Finance, and IT departments. While maintaining necessary communication channels, the proposed solution aims to enhance network security, performance, and manageability.

**• Objective:**

The primary objective is to implement a secure and segmented network environment for improved departmental communication and data protection.

**3. Background**

**• Organization/System Description:**

This report focuses on a typical corporate office network with a mix of devices used by HR, Finance, and IT personnel.

**• Current Network Setup:**

The existing network infrastructure consists of a flat network with a single subnet, using a Layer 2 switch and no access control mechanisms.

**4. Problem Statement**

**• Challenges Faced:**

* Unrestricted communication across all departments exposes sensitive data to unauthorized access.
* Broadcast storms can negatively impact network performance due to a large single broadcast domain.
* Difficulty in implementing granular security policies across the entire network.

**5. Proposed Solutions**

**• Approach:**

The proposed solution utilizes a combination of VLANs, subnets, and Access Control Lists (ACLs) to achieve network segmentation and secure communication channels.

**• Technologies/Protocols Used:**

* VLANs (Virtual Local Area Networks): logically segment the physical network based on department affiliation.
* Subnets: further divide VLANs into smaller address blocks for efficient IP address management.
* ACLs: define access rules at the Layer 3 switch to control traffic flow between VLANs.

**6. Implementation**

**• Process:**

1. **VLAN Configuration:** Create separate VLANs for HR, Finance, and IT departments on the Layer 3 switch.
2. **Subnet Allocation:** Assign subnets within each VLAN to accommodate the number of devices in each department.
3. **Device Assignment:** Connect devices belonging to each department to switch ports associated with their respective VLANs.
4. **ACL Implementation:** Define ACLs on the Layer 3 switch to allow specific communication between departments as per business requirements. (e.g., HR to Finance for payroll processing, IT to all for server maintenance)
5. **Testing and Validation:** Thoroughly test the network configuration to ensure proper communication within departments while restricting unauthorized access.

**• Implementation Timeline:**

* Planning and Design: 1 week
* Configuration and Testing: 2 weeks
* Implementation and Cutover: 1 weekend (planned outage).

**7. Results and Analysis**

**• Outcomes:**

* Network traffic is securely segmented between departments, minimizing the risk of unauthorized access to sensitive data.
* Broadcast traffic is confined within each department's VLAN, improving network performance.
* Granular security policies for access control can be implemented for each department.

**• Analysis:**

The implemented solution effectively addresses the challenges of a flat network by creating secure boundaries between departments. Improved network performance and easier management are achieved through segmentation and targeted security measures.

**8. Security Integration**

**• Security Measures:**

* Strong password policies for user accounts.
* Regular network vulnerability assessments.
* Intrusion Detection/Prevention Systems (IDS/IPS) monitoring network activity.
* Encryption of sensitive data at rest and transit.

**• Summary:**

This report presented a solution for secure traffic segmentation within a corporate office network using VLANs, subnets, and ACLs. The implemented solution enhances network security, performance, and manageability while catering to departmental communication needs.

**• Recommendations:**

* Regularly review and update ACLs based on evolving business requirements.
* Implement additional security measures as needed based on security assessments.
* User training on network security best practices.

**\*10. References/Citations\***

- "VLANs and Virtual Networks" (Cisco Systems, 2020)

- "Access Control Lists" (Juniper Networks, 2020)

- "Network Segmentation" (SANS Institute, 2019)

**NAME: ALLAM SUBHASH**

**ID-NUMBER:2320030424**

**SECTION-NO:1**