**Case Study ID: 001**

**1. Title**

**Financial Institution Subnetting for Security**

**2. Introduction**

* **Overview:** Subnetting is the process of dividing a larger network into smaller, more manageable pieces called subnets. This practice is crucial for financial institutions because it helps enhance security and manage network traffic more effectively.
* **Objective:** The main goal of this document is to demonstrate how subnetting can improve the security of financial networks by limiting access and isolating sensitive information.

**3. Background**

* **Organization/System Description:** Financial institutions handle sensitive customer data, transactions, and financial records. They require a secure network to protect this information from unauthorized access and cyber threats.
* **Current Network Setup:** The existing network may consist of a single large network where all departments (like HR, Finance, IT) share the same space, making it vulnerable to security breaches.

**4. Problem Statement**

* **Challenges Faced:**

The current setup poses several challenges, including:

- High risk of unauthorized access to sensitive data.

- Difficulty in managing network traffic and performance.

- Limited ability to monitor and control network activities.

**5. Proposed Solutions**

**Approach:** Implementing subnetting will help create separate networks for different departments. This segmentation will enhance security and control.

* **Technologies/Protocols Used:**

Technologies such as Virtual Local Area Networks (VLANs) and firewalls will be employed to manage traffic between subnets and enforce security policies.

**6. Implementation**

* **Process:**

The implementation will involve:

1. Assessing the current network and identifying departments.

2. Designing the subnet layout based on organizational needs.

3. Configuring routers and switches to create the new subnets.

* **Implementation:**

Each department will be assigned a specific subnet, limiting access to only authorized personnel.

* Timeline:

The implementation is expected to take 4-6 weeks, including planning, configuration, and testing.

**7. Results and Analysis**

* **Outcomes:** After implementing subnetting, the organization can expect:

Improved security through limited access to sensitive data.

- Better network performance due to reduced broadcast traffic.

- Easier monitoring of network activities.

* Analysis: The analysis will show a significant reduction in security incidents and improved compliance with regulations.

**8. Security Integration**

* **Security Measures:**

Security Measures: Additional security measures will include:

- Firewalls between subnets to control traffic.

- Regular audits and monitoring of network activities.

- Employee training on security best practices.

**9. Conclusion**

* **Summary:** Subnetting is an effective strategy for enhancing security in financial institutions. By segmenting the network, organizations can better protect sensitive information and manage network performance.
* **Recommendations:**

It is recommended that financial institutions regularly review and update their subnetting strategies and security measures to adapt to evolving threats.

**10. References**

* Research papers on network security and subnetting.
* Industry standards and best practices for financial institutions.

Name: Addagiri Kowshik

ID-NUMBER: 2320030121

Section: 4