**Title: Switch Implementation in a University Network for Network Policy Server (NPS)**

**Introduction:**

* **Overview:** This document outlines the role of switch implementation in the integration of Network Policy Server (NPS) within a university network. It emphasizes how network switches, alongside NPS, ensure secure, reliable, and controlled access for users.
* **Objective:** To examine how switches can be configured and integrated with NPS to enforce network access policies through features like VLANs, 802.1X authentication, and RADIUS, ensuring seamless access control for students, staff, and guests.

**Background:**

* **University Network Structure:** The university network consists of multiple departments, faculties, and common areas, requiring a segmented and secure network for diverse users. The network relies on managed switches to handle communication between different network segments.
* **NPS Role:**   
  Network Policy Server (NPS) is used to manage network authentication, authorization, and access control by working in tandem with switches to enforce network policies and provide secure access to the network based on user credentials.

**Problem Statement:**

* + **Challenges:**
  + Providing secure network access for a large number of users.
  + Managing traffic from various devices in a scalable and efficient manner.
  + Ensuring that unauthorized users do not access sensitive university resources.
  + Applying different policies to different user groups (students, faculty, guests).

**Proposed Switch Implementation for NPS Integration:**

* + **VLAN Configuration:**
  + **Overview:** Virtual LANs (VLANs) are used to segment the network based on departments or user groups, isolating traffic for security and performance.
  + **Implementation:**
    - Create VLANs for different user categories (e.g., staff, students, guests).
    - Assign appropriate VLANs based on the user's credentials, as verified by NPS.
    - **Example:**
      * VLAN 10: Staff
      * VLAN 20: Students
      * VLAN 30: Guests
  + **Benefits:** Enhances security by isolating traffic, simplifies network management, and optimizes resource utilization.

1. **802.1X Authentication:**  
   * **Description:** 802.1X is a port-based network access control standard that uses NPS as a RADIUS server to authenticate devices before granting network access.
   * **Process:**
     + End devices (e.g., computers, smartphones) connect to the network through switch ports.
     + Switches request user authentication credentials and forward them to NPS for validation via RADIUS.
     + Based on the authentication result, the switch grants or denies network access.
   * **Benefits:**
     + Provides strong access control, ensuring that only authenticated users gain access to the network.
     + Reduces the risk of unauthorized access to critical university resources.
2. **RADIUS Configuration on Switches:**  
   * **Overview:** RADIUS (Remote Authentication Dial-In User Service) is used by NPS to communicate with network switches to enforce network policies.
   * **Implementation:** Configure the switches to forward authentication requests to NPS, defining the RADIUS server’s IP address, shared secret, and authentication protocols.
   * **Benefits:** Centralizes authentication, authorization, and accounting for all devices connected to the network, improving security and management.
3. **Switch Port Security:**
   * **Description:** Implement switch port security features to prevent unauthorized devices from connecting to the network through unused or unmonitored switch ports.
   * **Implementation:**
     + Use MAC address filtering to restrict access to known devices.
     + Configure port security on switch interfaces to limit the number of MAC addresses learned dynamically.
     + Automatically disable ports if suspicious or unauthorized activity is detected.
   * **Benefits:** Prevents unauthorized devices from connecting to the network and minimizes the risk of rogue devices or attacks.

**Implementation Process:**

1. **Step 1: Configure VLANs:** Segment the university network using VLANs for different user groups (e.g., faculty, students, guests).
2. **Step 2: Enable 802.1X Authentication:** Configure switches to use 802.1X for port-based access control. Define authentication and authorization policies in NPS for each user group.
3. **Step 3: RADIUS Server Configuration:** Set up RADIUS communication between NPS and network switches. Ensure each switch is correctly configured to forward authentication requests to NPS.
4. **Step 4: Implement Port Security:** Secure switch ports to prevent unauthorized access using MAC filtering and port security configurations.
5. **Step 5: Testing and Validation:** Test user authentication and network access for different user groups to ensure the configuration is working as expected. Perform security and performance audits to verify proper implementation.

**Results and Analysis:**

* **Improved Security:** Implementation of VLANs, 802.1X, and RADIUS significantly reduces the risk of unauthorized access by enforcing strict authentication protocols.
* **Enhanced Network Management:** Centralized control through NPS allows for more streamlined management of user authentication and network policies.
* **Scalability:** The use of VLANs and 802.1X makes it easy to scale the network as the number of users increases while maintaining security.
* **Performance Metrics:** Evaluate improvements in network performance, including reduced unauthorized access, faster authentication, and better bandwidth utilization.

**Conclusion:**

The integration of switches with NPS in a university network provides a secure, scalable, and manageable solution for controlling network access. The use of VLANs, 802.1X authentication, and RADIUS ensures that only authenticated users can access the network, enhancing both security and performance. Future recommendations include ongoing monitoring, regular updates to security protocols, and expanding the system to accommodate emerging technologies.