SCD for Network Devices for Saral

1. Introduction: This System Configuration Document (SCD) outlines the network devices used by XYZ Inc and their respective configurations. The network devices play a critical role in the organization's technology infrastructure, and it is important that they are configured and maintained properly to ensure optimal performance and security.

2. Network Devices: The following network devices are used by XYZ Inc:

a. Routers: Routers are used to manage the flow of data between different networks and subnets. They are responsible for forwarding packets between networks and providing security measures such as firewalls.

b. Switches: Switches are used to provide connectivity within a network. They are responsible for forwarding data between devices on the same network and ensuring that data is transmitted reliably.

c. Firewalls: Firewalls are used to provide security to the network by controlling access to and from the network. They are responsible for protecting the network from unauthorized access, malware, and other threats.

d. Wireless Access Points (WAPs): WAPs are used to provide wireless connectivity within the organization. They are responsible for transmitting data wirelessly between devices and ensuring that data is transmitted securely.

3. Configuration: The following configurations are applied to the network devices used by XYZ Inc:

a. Routers: Routers are configured with the latest security updates and patches. They are also configured with access control measures such as firewalls and Virtual Private Network (VPN) connectivity.

b. Switches: Switches are configured with the latest security updates and patches. They are also configured with access control measures such as VLANs (Virtual Local Area Networks) to segment the network for security and performance reasons.

c. Firewalls: Firewalls are configured with the latest security updates and patches. They are also configured with access control measures such as Access Control Lists (ACLs) to control access to the network.

d. WAPs: WAPs are configured with the latest security updates and patches. They are also configured with wireless encryption measures such as WPA2 (Wi-Fi Protected Access) to ensure that data transmitted wirelessly is secure.

4. Maintenance: The network devices used by XYZ Inc must be regularly maintained to ensure optimal performance and security. This includes installing software updates and patches, monitoring performance, and conducting regular backups.

5. User Access: User access to the network devices must be controlled and monitored to ensure that only authorized personnel have access to sensitive information. The IT department must implement user access control measures such as setting up user accounts, assigning roles and privileges, and periodically reviewing user access logs.

6. Disaster Recovery Plan: The IT department must have a disaster recovery plan in place to ensure that the network devices can be quickly restored in the event of a disaster. This includes regular backups of the network devices, hardware, and data.

7. Review: The network devices used by XYZ Inc must be regularly reviewed to ensure that they are configured and maintained properly. This includes conducting security audits, monitoring performance, and identifying areas for improvement.