**1. Title:**

**Upgrading the Network Infrastructure of a University Campus: A Case Study of Greenfield University**

**2. Introduction:**

**Overview:**

As universities continue to adopt digital learning tools and cloud-based applications, the demand for a robust and secure network infrastructure has become paramount. This case study examines the process of upgrading the network infrastructure at Greenfield University to support increased bandwidth, improved security, and seamless connectivity across the campus.

**Objective:**

The primary objective of this case study is to document the network upgrade project at Greenfield University, focusing on the challenges faced, the solutions implemented, and the overall impact on the university's operations and academic environment.

**3. Background:**

**Organization/System Description:**

Greenfield University is a mid-sized institution with approximately 10,000 students, 500 faculty members, and several administrative departments. The campus spans multiple buildings, including academic halls, dormitories, libraries, and research centres, all requiring reliable network access.

**Current Network Setup:**

Before the upgrade, Greenfield University's network infrastructure was outdated, consisting of a mixture of legacy wired connections and basic wireless access points. The network was frequently overloaded during peak usage times, leading to slow speeds, dropped connections, and limited coverage in certain areas. Additionally, security protocols were insufficient to protect against the increasing number of cyber threats targeting educational institutions.

**4. Problem Statement:**

**Challenges Faced:**

Greenfield University encountered several significant challenges with its existing network infrastructure:

1. **Insufficient Bandwidth:** The network could not handle the growing demand for high-speed internet access, particularly during peak hours when students and faculty were accessing online resources simultaneously.
2. **Limited Coverage:** Many areas on campus, including outdoor spaces and certain buildings, had poor or no Wi-Fi coverage, limiting connectivity for students and staff.
3. **Outdated Security Measures:** The network's security protocols were outdated, making it vulnerable to cyberattacks, data breaches, and unauthorized access.
4. **Scalability Issues:** The existing infrastructure lacked the scalability needed to support future growth in student enrolment and the adoption of new technologies.

**5. Proposed Solutions:**

**Approach:**

To address these challenges, Greenfield University proposed a comprehensive upgrade of its network infrastructure, focusing on increasing bandwidth, expanding coverage, enhancing security, and ensuring scalability.

**Technologies/Protocols Used:**

1. **High-Speed Fiber Optic Backbone:** Upgraded the campus network backbone to fiber optic cables to provide high-speed, low-latency connectivity across all buildings.
2. **Next-Generation Wireless Access Points:** Deployed next-generation Wi-Fi 6 access points to improve wireless coverage, speed, and reliability.
3. **Network Security Upgrades:** Implemented advanced security protocols, including WPA3 encryption, firewall enhancements, and intrusion detection systems (IDS).
4. **Network Segmentation and VLANs:** Introduced network segmentation using VLANs to separate student, faculty, and administrative traffic, enhancing both performance and security.
5. **Cloud-Based Network Management:** Adopted a cloud-based network management platform to monitor and manage the network infrastructure remotely and efficiently.

**6. Implementation:**

**Process:**

The network upgrade was carried out in phases to minimize disruption to campus activities, starting with a thorough assessment of the existing infrastructure, followed by the deployment of new hardware and software solutions.

**Implementation:**

1. **Fiber Optic Installation:** Installed fibre optic cables across the campus, connecting all major buildings and providing a high-speed backbone for the network.
2. **Wireless Access Point Deployment:** Replaced old access points with Wi-Fi 6 devices, strategically placed to ensure comprehensive coverage, including outdoor areas and remote corners of the campus.
3. **Security Enhancements:** Implemented WPA3 encryption across all wireless networks, upgraded firewalls, and installed IDS to monitor and respond to potential threats in real-time.
4. **Network Segmentation:** Configured VLANs to segment the network based on user roles (e.g., students, faculty, administration), ensuring efficient traffic management and improved security.
5. **Cloud Management Integration:** Set up a cloud-based network management system, enabling the IT team to monitor network performance, deploy updates, and troubleshoot issues remotely.

**Timeline:**

The implementation spanned over 12 months:

* **Months 1-2:** Assessment and planning, including stakeholder consultations and infrastructure evaluation.
* **Months 3-6:** Installation of fiber optic backbone and preliminary security upgrades.
* **Months 7-9:** Deployment of Wi-Fi 6 access points and network segmentation.
* **Months 10-12:** Final security integrations, cloud management setup, and comprehensive testing.

**7. Results and Analysis:**

**Outcomes:**

1. **Increased Bandwidth:** The fiber optic backbone significantly boosted network bandwidth, allowing for smooth, uninterrupted access even during peak usage times.
2. **Improved Coverage:** The deployment of Wi-Fi 6 access points extended coverage to all areas of the campus, including previously underserved locations.
3. **Enhanced Security:** The upgraded security protocols, including WPA3 encryption and IDS, provided robust protection against cyber threats, reducing the risk of data breaches and unauthorized access.
4. **Scalable Infrastructure:** The new network infrastructure is scalable, capable of accommodating future increases in student enrolment and the adoption of emerging technologies.

**Analysis:**

The network upgrade at Greenfield University resulted in a more reliable, secure, and scalable network environment, significantly improving the overall user experience for students, faculty, and staff. The integration of modern technologies, such as fiber optics and Wi-Fi 6, along with enhanced security measures, positioned the university to meet current demands and future growth.

**8. Security Integration:**

**Security Measures:**

Greenfield University integrated the following security measures into its upgraded network infrastructure:

* **WPA3 Encryption:** Deployed WPA3 encryption across all wireless networks to protect against unauthorized access and ensure data integrity.
* **Intrusion Detection System (IDS):** Implemented IDS to monitor network traffic for suspicious activities and potential threats.
* **Firewall Enhancements:** Upgraded firewall configurations to provide an additional layer of defence against external attacks.
* **VLAN Segmentation:** Used VLANs to separate network traffic, reducing the risk of cross-network breaches and enhancing data privacy.

**9. Conclusion:**

**Summary:**

The case study of Greenfield University demonstrates the importance of modernizing network infrastructure to support the growing needs of a university campus. By upgrading to a high-speed, secure, and scalable network, the university not only improved current connectivity and security but also laid the foundation for future technological advancements.

**Recommendations:**

To maintain and further enhance network performance, Greenfield University should:

* Regularly monitor and update network security protocols to stay ahead of emerging threats.
* Continuously assess network performance and make adjustments as needed to accommodate increased usage.
* Explore opportunities to integrate new technologies, such as IoT devices and advanced analytics, into the network infrastructure.

**10. References:**

1. A. Tanenbaum and D. Wetherall, "Computer Networks," 5th Edition, *Prentice Hall*, 2010.
2. K. Scarfone and P. Hoffman, "Guidelines for Securing Wireless Local Area Networks (WLANs)," *NIST Special Publication 800-153*, 2012.
3. M. Gast, "802.11ac: A Survival Guide," *O'Reilly Media*, 2013.
4. J. Wiley and D. McDonald, "Network Security: Private Communications in a Public World," *Prentice Hall*, 2010.
5. L. Peterson and B. Davie, "Computer Networks: A Systems Approach," 5th Edition, *Morgan Kaufmann*, 2011.

**NAME:** NEKKANTI NANDINI

**ID- NUMBER:** 2320030459

**SECTION- NO:** 4