Case Study ID: 13

1.Title

Wireless Network Deployment in a University

2. Introduction

The demand for wireless connectivity in educational institutions has grown significantly, driven by the need for mobility, access to online resources, and the integration of digital learning tools. This case study examines the deployment of a wireless network across a university campus to provide reliable and secure internet access to students, faculty, and staff.

The primary objective of this project was to design and deploy a robust wireless network that covers the entire university campus, ensuring high-speed connectivity, secure access, and the ability to handle a large number of concurrent users.

3. Background

- The university is a mid-sized institution with a student population of approximately 15,000. The campus spans over 200 acres, including academic buildings, dormitories, administrative offices, and recreational areas. Prior to the deployment, the university relied on a combination of wired and limited wireless networks that were insufficient to meet the growing demand for connectivity.
- The existing network infrastructure included Ethernet connections in classrooms and offices, along with limited Wi-Fi coverage in specific areas such as libraries and lecture halls. The lack of a campus-wide wireless network led to connectivity issues, especially in outdoor and less frequented areas.

4. Problem Statement

The university faced several challenges, including:

- Limited wireless coverage, resulting in dead zones across the campus.
- Insufficient bandwidth to support the increasing number of devices connecting to the network.
- Security vulnerabilities due to outdated network protocols.
- Difficulty in managing and scaling the network to accommodate future growth.

5. Proposed Solutions

- The proposed solution involved a comprehensive redesign of the university's network infrastructure, focusing on deploying a campus-wide wireless network. The approach included:

- Conducting a site survey to determine optimal access point locations.
- Implementing high-density access points in areas with a large number of users.
- Upgrading the backbone network to handle increased traffic.
- Introducing advanced security protocols to protect against unauthorized access.
- **Technologies/Protocols Used**
- **Wireless Access Points (APs):** High-performance APs supporting the latest Wi-Fi standards (Wi-Fi 6).
- **Network Management System (NMS):** For monitoring and managing the wireless network in real-time.
- **Security Protocols:** WPA3 for enhanced security, along with a network segmentation strategy to isolate sensitive traffic.
- **Bandwidth Management:** Implementing Quality of Service (QoS) to prioritize critical traffic and ensure smooth performance.

6. Implementation

The implementation process was divided into several phases:

- **Planning:** Conducting site surveys, defining requirements, and selecting hardware.
- **Deployment:** Installing access points, upgrading network infrastructure, and configuring the NMS.
- **Testing:** Verifying network performance, coverage, and security.
- **Training:** Educating IT staff and users on the new system
- **Implementation Timeline**
    - **Phase 1 (Planning):** 2 months
    - **Phase 2 (Deployment):** 3 months
    - **Phase 3 (Testing and Optimization):** 1 month
    - **Phase 4 (Training and Rollout):** 1 month

7. Results and Analysis

- The wireless network now covers 100% of the campus, including outdoor areas.
- Network performance improved significantly, with average speeds increasing by 50%.
- The number of concurrent users supported increased by 300%, with no noticeable drop in performance.
- The deployment successfully addressed the challenges faced by the university, providing a scalable and secure network solution that meets current and future demands.

8. Security Integration

- **WPA3 Encryption:** Enhanced protection for users connecting to the network.
- **Network Segmentation:** Isolating academic, administrative, and guest traffic to minimize security risks.

- **Regular Audits:** Implementing periodic security audits and penetration testing to ensure ongoing protection.

9. Conclusion

- The deployment of the wireless network at the university was a critical step in modernizing its infrastructure. It provided students, faculty, and staff with reliable access to the internet and university resources, supporting the institution's educational mission.

For continuous improvement, it is recommended that the university:

- Regularly update the network hardware and software.
- Monitor the network to anticipate future needs and scale accordingly.
- Provide ongoing training to IT staff to maintain the network effectively.

10. References

1.https://web.archive.org/web/20101008154326id_/http://cluteinstitute-onlinejournals.com/PDFs/2004171.pdf

2. https://d1wqtxts1xzle7.cloudfront.net/32996383/csn2003-libre.pdf?1393932059=&response-content-disposition=inline%3B+filename%3DWIRELESS_LAN_DEPLOYMENT_IN_LARGE_EXTENSI.pdf&Expires=1724645614&Signature=WVSsFjAUnp3RFo80IjOEx3~XkXP6w~GwO3EbhZAXORoJiLb~jXL~vLKOm38XZh6phRxYuMLYPA~tgwFDBTM1b7SP8lWqKVibTkCiT0nIXnsgo6ISVvU0hWokmfxSUZR-Jngvt1Gv8OxVbZMzHXOJmbfbMeTGWi0UnpRsHD20qHbry~k1HQt1B27scYxjI8~c9tJ2D2G6vRUclp-UWvfxFM3--ddCkIve10mrwmTzixiiL4YI2IRXwstPDfEjDbgFSV9Ih34rS62zhZYylSVV9Icoj4Tcw11Av83sd2LerRxC7oJm2cyjeV53satarvmMMc1vxWc4EIKfvZxgTurZNw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

NAME: B. Navya

ID-NUMBER:2320030174

SECTION-NO:1