**Case Study ID: 02**

**1. Title: Enhancing the University Campus Network Infrastructure**

**2. Introduction**

* Overview:

A campus network is essential in modern university environments, providing the backbone for educational, administrative, and research activities. It supports seamless communication, access to educational resources, and a variety of applications such as e-learning, research tools, and administrative systems.

* Objective:

The objective of this case study is to evaluate the current network infrastructure of the university campus, identify challenges, and propose solutions that improve network performance, security, and scalability to meet the growing demands of the university community.

**3. Background**

* Organization/System/Description:

The university campus consists of multiple buildings, including academic halls, administrative offices, hostels, and recreational facilities. The current network services approximately 2,000 students, faculty, and staff, connecting to both local resources and the internet.

* Current Network Setup:

The network includes:

- Core Routers: Cisco ASR series for core networking.

- Switches: Layer 2 and Layer 3 switches providing segmentation for academic, administrative, and residential zones.

- Wireless Access Points (APs): Spread across the campus for Wi-Fi access.

- Internet Gateway: A single gateway that handles internet traffic.

Although functional, the network struggles with increased bandwidth demand, limited coverage in certain areas, and security vulnerabilities, including frequent unauthorized access attempts.

**4. Problem Statement**

* Challenges Faced:  
  - Bandwidth Overload: Increased use of streaming, cloud services, and online learning platforms have caused bandwidth congestion, leading to slow network speeds during peak hours.

- Insufficient Coverage: Some areas of the campus, particularly the dormitories and recreational zones, experience poor Wi-Fi coverage.

-Security Vulnerabilities: The network faces issues with unauthorized access and lacks advanced security measures such as intrusion detection systems (IDS) and firewalls capable of handling advanced threats.

-Lack of Scalability: The current infrastructure is not flexible enough to support future expansions or modern technologies like IoT and AI-powered systems.

**5. Proposed Solutions**

* Approach:  
  To address the current challenges, the following solutions are proposed:

1.Upgrade Bandwidth and Optimize Traffic Management: Implement high-speed fiber-optic connections and traffic management tools such as Quality of Service (QoS) to prioritize critical applications.

2.Extend Wi-Fi Coverage: Deploy additional wireless access points with mesh technology to improve coverage, particularly in areas with low signal strength.

3.Strengthen Security: Integrate advanced security protocols such as network segmentation, firewalls, and intrusion prevention systems (IPS) to secure sensitive data and prevent unauthorized access.

4.Implement Scalable Infrastructure: Adopt software-defined networking (SDN) to enable easy network expansion and management of future technologies.

* Technologies/Protocols Used: -

Fiber-Optic Connectivity for high-speed internet.

Quality of Service (QoS) for traffic management.

802.11ax (Wi-Fi 6) access points for enhanced wireless performance.

Firewall and IDS/IPS for advanced security.

Software-Defined Networking (SDN) for scalability and future-proofing.

**6. Implementation**

* Process:

1. Network Audit: Conduct a detailed audit of the current infrastructure.

2. Hardware and Software Acquisition: Procure necessary devices and tools such as new routers, switches, firewalls, and access points.

3. Deployment: Install fiber-optic cables, configure SDN, set up new access points, and implement security measures.

4. Testing: Perform thorough testing to ensure the network is optimized and secure.

5. Training: Provide training to the university’s IT staff on managing the new network architecture.

* Implementation:  
  Network Audit: Assess the current infrastructure to identify weak points.

Hardware and Software Acquisition: Purchase necessary equipment, including routers, switches, firewalls, access points, and fiber-optic cables.

Deployment:

- Install fiber-optic cables for high-speed internet.

- Configure SDN for scalability.

- Set up Wi-Fi 6 access points.

- Implement security with firewalls and intrusion detection systems.

Testing: Conduct speed and security tests to ensure network performance.

Training: Train IT staff to manage the new network and handle future upgrades.

* Timeline:  
  Week 1: Conduct the network audit to assess the current infrastructure and gather requirements for the upgrade.

Week 2: Begin the acquisition of necessary hardware and software, including routers, switches, access points, and security devices.

Week 3-4: Deploy fiber-optic cables across the campus and configure SDN for network scalability. Set up the new access points and update existing network configurations.

Week 5: Implement advanced security measures, including firewalls and intrusion prevention systems. Begin the first phase of network testing.

Week 6: Complete network testing, addressing any performance or security issues. Conduct a second round of testing to ensure stability.

Week 7: Provide training sessions for IT staff on managing the upgraded network, including security protocols, troubleshooting, and future expansion.

**7. Results and Analysis**

* Outcomes:  
  Enhanced Speed: The upgraded infrastructure has reduced congestion and increased network speeds, especially during peak hours.

Expanded Coverage: Wi-Fi coverage now extends to all areas of the campus, ensuring reliable access for students and staff.

Improved Security: The implementation of advanced security protocols has drastically reduced the number of unauthorized access attempts and potential breaches.

Scalability: The SDN framework allows for easy expansion to support future technologies and increased users.

* Analysis:  
  The upgraded network has improved overall performance, with more stable connections and enhanced user experience. The university's IT team reports fewer complaints related to downtime or connectivity issues.

**8. Security Integration**

* Security Measures:

Firewall: Configured for maximum protection against external threats.

Intrusion Detection/Prevention Systems (IDS/IPS): Monitoring the network for suspicious activities.

Data Encryption: Encrypted traffic to secure sensitive communications between the university and external networks.

User Authentication: Implemented multi-factor authentication (MFA) for accessing sensitive administrative systems.

**9. Conclusion**

* Summary: The proposed solutions effectively addressed the network congestion, coverage gaps, and security vulnerabilities. The enhanced infrastructure provides the university with a scalable, secure, and high-performance network that can support future growth.
* Recommendations:  
  Continue to monitor the network for emerging threats and upgrade security measures as needed.

Regularly audit the network to ensure optimal performance and scalability for future technologies.

Invest in training IT staff on the latest technologies and best practices in network management.

**10. References**

**Citations : ChatGPT, Google.**

**NAME: Akshara Budha**

**ID-NUMBER: 2320030377**

**SECTION-NO: 07**