|  |  |
| --- | --- |
| A picture of a winding road and trees  Project Planning | Solomon Morongwa Moshokoa: ST10229897  Bornwise Nkateko Baloyi: ST10105509  Roandiswa Mbedzi: ST10064879  Mokgadi Mamabolo: ST10204666  WORK INTEGRATED LEARNING  Group 3  DMT2 |

Table of content

Project Planning

* Project Overview
* Objectives and Focus
* Structured Approach
* Strategies for Network Enhancement
* Project Phases
* Initiation Phase
* Planning Phase
* Execution Phase
* Monitoring & Controlling Phase
* Closing Phase

**What We Will Need to Complete This Project**

* Network Hardware
* Cabling and Infrastructure
* IP Addressing
* Network Security
* Network Monitoring and Management
* Wireless Connectivity
* Bandwidth Management
* Redundancy
* Scalability
* Policy and User Management

**In-Scope Hardware**

* Core Networking Equipment
* Access Points (APs)
* Cabling Infrastructure
* Server Hardware
* End-User Devices
* Internet Sharing Equipment
* Security Hardware

**Out-of-Scope Hardware**

* Individual User Devices
* Non-Network Infrastructure
* Extensive Server Hardware
* Facilities Management

**IP Addressing and Network Design**

* Develop an IP Address Schema
* Wireless Access and Security
* Internet Sharing
* Network Configuration
* Bill of Materials
* Risk Management

**Network Topology and Hardware**

* Network Topology Selection
* Hardware Selection
* Subnetting
* Redundancy
* Security Measures
* Bandwidth Management

**Project Implementation Phases**

* Initiation Phase
* Planning Phase
* Execution Phase
* Monitoring & Controlling Phase
* Closing Phase

**Conclusion**

Project planning

The project endeavours to revamp the organization's IT network to ensure seamless connectivity among 100 users spread across three buildings and lobby areas. This involves acquiring essential network hardware like switches, routers, and access points, alongside robust security measures such as firewalls and encryption. With a focus on scalability, redundancy, and efficient bandwidth management, the project aims to bolster network reliability and security (Paker, 2020). The structured approach encompasses initiation, planning, execution, monitoring, and closing phases, ensuring a systematic overhaul. Strategies involve careful selection of network topology, hardware, subnetting for efficient IP address management, redundancy implementation, stringent security measures, and bandwidth prioritization. Ultimately, this initiative aims to optimize the network infrastructure, ensuring it not only meets current demands but also aligns with future growth and technological advancements, fostering a secure and efficient network environment for the organization (Paker, 2020).

**What we will need to complete this project**

1. **Network Hardware**: This includes switches, routers, access points, and firewalls to connect and manage devices across the campus (Paker, 2020).

 2. **Cabling and Infrastructure**: Reliable cabling (such as Ethernet) and proper infrastructure are necessary for data transmission (Paker, 2020).

 3. **IP Addressing**: A well-planned IP addressing scheme to manage devices and subnets effectively (Paker, 2020).

4. **Network Security**: Implementing firewalls, intrusion detection/prevention systems, and encryption to protect data and systems (Paker, 2020).

 5. **Network Monitoring and Management**: Tools to monitor network health, manage devices, and troubleshoot issues (Paker, 2020).

 6. **Wireless Connectivity**: Access points for Wi-Fi coverage throughout the campus (Paker, 2020).

 7. **Bandwidth Management**: Ensuring fair and efficient distribution of network resources (Spancer, 2021).

 8. **Redundancy**: Backup connections and failover mechanisms for high availability (Spancer, 2021).

 9. **Scalability**: Designing the network to accommodate future growth and modern technologies (Spancer, 2021).

 10. **Policy and User Management**: Implementing user authentication, access controls, and network usage policies and troubleshoot issues (Spancer, 2021).

In-Scope Hardware

22. Core Networking Equipment:

•Routers and switches to establish the network backbone.

•Firewall appliances for network security.

23. Access Points (APs):

•Deploy wireless access points strategically in the main building and both satellite buildings, including lobby areas.

24. Cabling Infrastructure:

•Ethernet cabling to connect devices within each building.

•Fiber optic cabling for high-speed inter-building connectivity.

25. Server Hardware:

•Central server(s) for DHCP (Dynamic Host Configuration Protocol) to provide dynamic IP addressing to all staff.

•Servers for hosting network management and monitoring tools.

26. End-User Devices:

•Computers for each of the 100 active users.

•Printers, including 3 large-speed printers in each building.

27. Internet Sharing Equipment:

•Network load balancers to ensure efficient distribution of the high-speed cable Internet connection among users (Spancer, 2021).

28. Security Hardware:

•Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) devices.

•Access control devices to enforce network security policies.

Out-of-Scope Hardware:(PROJECT PLAN 1)

29. Individual User Devices: The setup and configuration of individual computers and printers for end-users are not part of the network infrastructure project.

30. Non-Network Infrastructure: Physical infrastructure upgrades unrelated to network installation and configuration.

31. Extensive Server Hardware: Server hardware and setup unrelated to core network services.

32. Facilities Management: Facilities maintenance or construction unrelated to network installation and operation.

By defining the hardware requirements, you can ensure that the project focuses on the essential components needed to address the identified issues and challenges while excluding elements that are beyond the scope of the network infrastructure project.

3. IP Addressing and Network Design:

•Develop an IP address schema for the entire campus network.

•Create an IP address management plan to efficiently allocate IP addresses to users and devices.

•Design the logical and physical network topology, considering the distances between buildings.

4. Wireless Access and Security:

• Plan for wireless access points (WAPs) in each building's lobby.

• Implement security measures, such as WPA3 encryption and MAC address filtering, to ensure only authorized personnel can access the wireless network (Spancer, 2021).

5. Internet Sharing:

•Design a network layout that allows all users in the college to share the high-speed cable Internet connection available in the main building (Spancer, 2021).

•Consider load balancing and redundancy options for Internet connectivity (Daniels, 2021).

6. Network Configuration:

•Identify configurations required for network devices, including routers, switches, and access points (Daniels, 2021).

•Implement Quality of Service (QoS) settings to prioritize network traffic if needed (Daniels, 2021).

•Configure DHCP to assign dynamic IP addresses to staff members.

•Set up static routes or routing protocols for interconnecting the buildings.

7. Bill of Materials:

•Create a detailed list of all equipment needed for the network setup, including quantities.

•Include costs associated with hardware, software, and licensing.

8. Risk Management:

•Identify potential risks related to the project, such as equipment failures, budget constraints, or technical challenges (Daniels, 2021).

• Assess the probability and impact of each risk.

• Develop risk mitigation and contingency plans

Network topology:

* Select the appropriate network topology, such as star, bus, or ring topology, to connect the building
* Each has its own benefits, so choose the one that best fits your school's layout and budget

Hardware:

* Choose network equipment such as switches, routers, access points, and cabling that can handle expected traffic and create opportunities for future growth

Subnet:

* Divide the campus into subnets for efficient IP address management
* Make sure each building and user group has a unique subnet

Redundancy:

* Implement redundancy to minimize downtime
* This includes redundant power supplies, Internet connections, and network paths

Security:

* Implement firewalls, intrusion detection systems, and access controls to protect against security threats

Bandwidth management:

* Prioritizes network traffic to ensure that critical applications have enough bandwidth.
* Consider quality of service (QoS) mechanisms
* of your campus with three buildings and 100 active users

The project can function through its various phases, activities, and strategies to achieve the intended objectives:

**1. Initiation Phase:**

* **Project Definition:** Clearly define the project's scope, objectives, stakeholders, and constraints.
* **Identify Challenges:** Acknowledge potential challenges such as network conflicts and compatibility issues.
* **Allocate Resources:** Determine budget, timeframes, and required hardware/software.

**2. Planning Phase:**

* **Scope Management:** Define tasks and activities to ensure secure wireless and wired access, internet sharing, efficient connectivity, and printer integration.
* **Task Allocation:** Assign responsibilities to the IT team for hardware procurement, software acquisition, installation, configuration, testing, and training sessions.
* **Risk Management:** Develop strategies to mitigate potential challenges like network conflicts and software/device compatibility issues (Chen, 2023).

**3. Execution Phase:**

* **Hardware and Software Procurement:** Purchase routers, access points, cables, switches, high-speed printers, network security software, printer drivers, and management tools as per the established budget (Chen, 2023).
* **Installation and Configuration:** IT technicians install and configure hardware and software across the buildings and lobby areas (Chen, 2023).
* **Testing and Optimization:** Conduct thorough tests to ensure network functionality, security protocols, and printer connectivity meet the project goals (Chen, 2023).

**4. Monitoring & Controlling Phase:**

* **Scope Validation:** Regularly validate project activities against the defined scope to ensure they align with the objectives (Daniels, 2021).
* **Budget and Timeline Control:** Monitor expenditure against the allocated budget and adjust timelines if needed (Daniels, 2021).
* **Addressing Challenges:** Implement pre-deployment network assessments and regular updates to prevent and resolve potential conflicts and compatibility issues (Daniels, 2021).

**5. Closing Phase:**

* **Training Sessions:** Conduct comprehensive training for end-users on network usage and printer operations (Daniels, 2021).
* **Project Evaluation:** Assess project performance against the initial objectives, addressing any gaps or discrepancies (Daniels, 2021).
* **Documentation:** Compile project documentation, including achievements, challenges faced, solutions implemented, and lessons learned (Chen, 2023).

Throughout this logical cycle, the Project Manager will oversee the entire process, managing budgets, timelines, and stakeholders' engagement. The IT team will play a pivotal role in executing tasks related to installation, configuration, testing, and training. The end-users, comprising 100 college users, will ultimately benefit from the enhanced network accessibility, security, and efficiency across the college buildings (Chen, 2023).

The budget of R1000,000 and a timeframe of 6 months will be carefully managed to procure the necessary hardware and software, address challenges, and achieve the project's goal of seamless connectivity within the set parameters (Chen, 2023).

# References List

Chen, D. k. (2023, May 02). *Chegg*. Retrieved from Chegg.com: http://www.chegg.com

Daniels, D. (2021, September 22). *ResearchGate* . Retrieved from researchgate.net: http://www.researchgate.net

Paker, J. (2020, August 21). *Google Scholar*. Retrieved from scholar.google.com: http://www.scholar.google.com

Spancer, D. (2021, July 12). *IEEE Xplore*. Retrieved from ieeexplore.ieee.org: http://www. ieeexplore.ieee.org