Project Plan

University Network Design

Unit: COIT13236

Student 1: Krishan Himesh Abeyrathne Tennakoon Mudiyanselage (12217274)

Student 2: Narayan Parajuli (12144248)

Project Mentor: Sunil Seneviratne

Date: 20.07.2024

CQUniversity Australia

# Overview

The project is focused on planning and carrying out an advanced network infrastructure for a multi-campus KN University (KNU). This network infrastructure is expected to give strong network security and adaptability across various campus locations. It incorporates pioneering technologies, including Internet of Things (IoT) gadgets and distributed computing, to upgrade the university’s functional effectiveness and academic abilities. The project includes making a network architecture connecting various campus buildings and supporting modern educational and administrative functions. Making a total network solution that meets the different requirements of a KN university with numerous grounds is the fundamental objective of this task. This involves creating a network architecture that upholds administrative and scholastic tasks while consolidating advanced innovations to ensure reliable and quick access through all grounds. Key targets incorporate making a Scalable Network where a planned network can extend with the university development and adjust to developing mechanical necessities. Another is upgrading connectivity, guaranteeing consistent and dependable web access for students, personnel, and staff across all campus areas.

The project tackles several important problems that universities encounter:

* Difficulties with connectivity: Providing reliable, fast internet access at several sites might be difficult because of different network requirements and physical distances.
* Security concerns: Security concerns incorporate shielding delicate information access and protecting the organization against online assaults. This includes putting encryption procedures, interruption discovery frameworks, and firewalls into place.
* Reconciliation of IoT Gadgets: Applying IoT innovation to develop student experience and campus tasks further. This includes regulating a wide assortment of sensors and gadgets all over the campus.
* Needs for Cloud Computing: Seamlessly integrating cloud services with the current network to support scalable applications and data storage.

To achieve the objectives of network design and execution, the project involves the following key stages:

* Design Network Architecture: Draft an exhaustive arrangement that incorporates all the fundamental network equipment, like firewalls, switches, and routers. This includes organising the data flow, network design, and availability among the numerous campus buildings.
* Integrate IoT Technology: Find and incorporate IoT gadgets into the network, like smart building frameworks and environmental sensors. This involves setting up these gadgets for productive communication with different parts of the network and the core.
* Create Prototype Network: Utilizing the lab's current equipment, for example, Cisco switches and routers, make a network model or get more equipment. This involves assembling and configuring the network's component parts according to the design guidelines.

This project's principal stakeholders are the IT and administrative departments of KN University. The project aims to provide these stakeholders with a dependable, safe, and expandable network environment by offering a solution that satisfies their objectives. The benefits of the project for the KN university are:

* Improved Connectivity: Dependable, fast internet connectivity that supports administrative and scholastic tasks on all campuses.
* Enhanced Security: Sophisticated security protocols to guard against online attacks and guarantee privacy and data integrity.
* IoT Integration: Using smart devices and sensors to improve campus management improves operational effectiveness and student experiences.

The project won't consist of:

* Acquisition of Non-Network Hardware: This project does not cover purchasing or installing end-user hardware, such as computers or printers.
* Physical Infrastructure alterations: Building renovations and new construction are examples of physical infrastructure alterations not included in this project.
* End-User Training: Although the network will be easily navigable, this project does not include any training programmes for end users on how to use the new network.

# Tasks

We are using the Top-down Network design methodology, a structured approach that starts the process of the upper layer of the OSI model before moving to the lower layers. The following tasks for KN University have been carefully listed following the phases of the Top-down network development methodology.

|  |  |  |
| --- | --- | --- |
| **Task** | **Description** | **Deliverable(s)** |
| **Phase 1: Analyse Business and Technical Requirements** | | |
| 1. Network Documentation | Produce detailed records of the current and planned state of the network architectures, configurations, and security for KN University. | * Network design documentation. * Configuration guide. * Policy manual. |
| 1. Compliance and Regulatory Requirements | Make sure that the requirements of the local regulations and standards, which concern the KN University, are met during the network design. | * Compliance documents and reports. * Regulatory checklist. |
| 1. Stakeholder Training and Handover | Ensure stakeholders are trained on the new network and pass all documents and access related to KN University. | * Documents used during training. * Reports on training sessions. * Documents to be handed over. |
| **Phase 2: Local Network Design development** | | |
| 1. Wired Network Infrastructure design for KNU. | Develop the installation plan for Ethernet cabling, switches, and router installations for all the KN University campuses and the VLAN configuration and addressing plan. | * Network topology diagram for every campus. * Configuration scripts of switches & routers and VLAN assignment tables. |
| 1. Wireless Network Infrastructure Design for KNU. | Determine the coverage area and the number of APs for each KN University campus; decide on the protocols and standards to be applied; address the scheme; and determine desirable settings for the APs and clients. | * A physical map with marked AP locations for each campus. * Table of AP settings. * Table of client settings. * IP address table and a Logical network design diagram. |
| 1. IoT Device Integration | Determine IoT solutions for security and environmental monitoring in KN University campuses; identify device location and decide on the collection and analysis of data. | * The details regarding the specifications of each IoT device. * The deployment plans of the campus. * The data integration plans. |
| 1. Cloud Service Integration | Perform cloud provisioning for KN University, define the specific services that need to be set up, establish the VPN connection, and configure the load balancing. | * Diagram for cloud service architecture. * VPN and load balancer settings. * Usage policies. |
| 1. Security Framework Development | Planning of risk and creating security policies of KN University network; setting of Firewall and IDS/IPS. | * Risk analysis report. * compliance and security policies. * Firewall configuration files. * IDS/IPS configuration files. |
| 1. User authentication and access control. | Develop user authentication and access controls for individuals and devices to be allowed to connect to the KN University network. | * The Authentication system configuration. * Access control policy documents. * User role assignments. |
| **Phase 3: Design the Physical Network** | | |
| 1. Prototype Implementation | Establish the physical topology with Cisco switches, routers and Ubiquiti APs and incorporate selected cloud services for a KN University campus. | * Initial network configuration on the prototype. * Results of tests and verifications. * Documentation of implementation. |
| 1. Vendor and Equipment Selection for KNU. | Identify vendors and equipment needed for the project and suggest ones that best fit the needs of KN University as per its budget. | * Vendor assessment report. * The list of equipment purchases. |
| **Phase 4: Implementation and Testing of the Network.** | | |
| 1. Network Performance Testing. | Carry out tests to determine the efficiency of the network at KN University during the various loads and conditions. | * Test results of observations made during the performance tests. * Test Results of recommendations for performance improvement. |
| 1. Network Security Testing. | Assess the KN University’s network using penetration testing and vulnerability assessment tests. | * A penetration test report. * A vulnerability assessment report. * Security improvements recommendation report. |
| 1. Setting up of Network Management and Monitoring | Adopt network management and monitoring tools to track all the campuses of KN University in real-time. | * Network management system. * Configuration, monitoring, and alerting setup. * Monitoring and alerting procedures. |
| 1. Quality Assurance and Testing | Establish quality control mechanisms and thoroughly test all the network components of KN University. | * QA plan. * Testing schedules. * Quality assurance and testing documents. |
| **Phase 5: Optimise and Document** | | |
| 1. The backup and disaster recovery plan | Propose a business continuity and disaster recovery plan for KN University so that data is always protected and can be recovered in the event of a disaster. | * Backup strategy document. * Disaster recovery plan. * Testing and validation reports. |
| 1. Network Scalability Plan. | Creating a procedure for expanding the network to accommodate growth at KN University in the future. | * Upgrade strategy proposal. * Integrated scaling plan. |
| 1. Environmental Impact Assessment | Evaluate the network infrastructure's consequences within KN University and identify measures for reducing the impact. | * Environmental assessment document. * Management of measures document. |
| **Phase 6: Continuous Processes** | | |
| 1. Budget and Cost Analysis | Evaluate the costs related to the establishment of the network and the project financials of KN University. | * Budget flow report. * Cost control report. * Cost calculation report. |
| 1. Project Management and Coordination | Plan out every process necessary for a project, control the time factor, and ensure that KN University's set goals and objectives are achieved within the specified period. | * Project plan. * Gantt charts. * Progress reports. |

Table 2.1 Tasks List of the KNU Network Design

# Roles

In our project, each member will assume certain roles as illustrated in the NICE (National Initiative for Cybersecurity Education) framework. This framework gives a far-reaching guide for the different roles important to addressing cybersecurity challenges productively. The following areas will detail the roles with justifications.

|  |  |  |
| --- | --- | --- |
| **Student Name** | **Role** | **Justification** |
| Narayan Parajuli | System Security Analyst | The system security analyst is responsible for ensuring the overall security posture of KN University's network infrastructure and protecting the network from security threats. |
| Krishan Himesh Abeyrathne | System Administrator | The Systems Administrator maintains and manages servers and critical infrastructure components, ensuring reliability and performance. |

Table 3.1 Roles List of the Group Members

# Responsibilities

Effective task management is essential for the progress of our project. To guarantee exhaustive execution and quality confirmation, each task in Section 2 will have an assigned Technical Lead and a Reviewer. This approach guarantees responsibility and meticulousness, as both the Technical Lead and the Reviewer share liability regarding the task's successful completion.

|  |  |  |
| --- | --- | --- |
| **Task** | **Technical Lead** | **Reviewer** |
| 1. Wired Network Infrastructure design | Krishan Himesh | Narayan Parajuli |
| 1. Vendor and Equipment Selection for KNU. | Krishan Himesh | Narayan Parajuli |
| 1. Project Management and Coordination | Krishan Himesh | Narayan Parajuli |
| 1. Prototype Implementation | Narayan Parajuli | Krishan Himesh |
| 1. Network Scalability Plan | Narayan Parajuli | Krishan Himesh |
| 1. Network Documentation | Krishan Himesh | Narayan Parajuli |
| 1. Compliance and Regulatory Requirements | Narayan Parajuli | Krishan Himesh |
| 1. Stakeholder Training and Handover | Narayan Parajuli | Krishan Himesh |
| 1. Wireless Network Infrastructure Design for KNU. | Krishan Himesh | Narayan Parajuli |
| 1. IoT Device Integration | Krishan Himesh | Narayan Parajuli |
| 1. Cloud Service Integration | Narayan Parajuli | Krishan Himesh |
| 1. Security Framework Development | Narayan Parajuli | Krishan Himesh |
| 1. User authentication and access control. | Krishan Himesh | Narayan Parajuli |
| 1. Network Performance Testing. | Narayan Parajuli | Krishan Himesh |
| 1. Network Security Testing. | Krishan Himesh | Narayan Parajuli |
| 1. Setting up of Network Management and Monitoring | Krishan Himesh | Narayan Parajuli |
| 1. Quality Assurance and Testing | Narayan Parajuli | Krishan Himesh |
| 1. The backup and disaster recovery plan | Krishan Himesh | Narayan Parajuli |
| 1. Environmental Impact Assessment | Krishan Himesh | Narayan Parajuli |
| 1. Budget and Cost Analysis | Narayan Parajuli | Krishan Himesh |

Table 4.1 Responsibilities list of the tasks

# Resource Requirements

In this part, we will frame the resources expected for our project, arranged into in-kind, money, and personnel. For every resource, we will clarify its need, relate it to project tasks, and detail the related expenses or licenses. This definite breakdown guarantees that we have a far-reaching comprehension of the assets required and the financial implications, helping with powerful project planning and budgeting.

*In-Kind*

|  |  |  |
| --- | --- | --- |
| **Resource** | **Justification** | **Cost/License** |
| Wireshark | Packet capture will be used in the pen-testing task to inspect encrypted packets | Free. GNU GPL2 open source |
| Cisco Switches (Cisco CBS250 24 Port Gigabit Switch) | Required for segmenting and connecting network traffic within and between multiple buildings on each campus. | $449 per switch |
| Cisco Routers (Cisco 1941 Wired Router CISCO1941/K9) | Necessary for routing traffic between the campus network, internet, and cloud services. | $991 per router |
| Network Cables (RJ45 CAT6 UTP Ethernet Networking LAN Cable) and Racks | Used for connecting network devices within and between buildings and for organizing equipment. | $300 estimated |
| Cisco Packet Tracer | It is a powerful network simulation tool providing a safe and virtual environment for experimentation, configuration, and troubleshooting. | Free. Open-Source Software |
| Oracle Virtual Box | It permits clients to simultaneously stretch out existing PCs to run numerous operating systems, including Microsoft Windows, Mac OS, Linux, etc.; | Free. Open-Source Software |
| Physical Firewall (Fortinet FortiGate 60D) | A physical firewall is an actual gadget similar as a server that channels the traffic going to a PC. | $181 |

Table 5.1 In-Kind Resources and Justifications

*Cash*

|  |  |  |
| --- | --- | --- |
| **Resource** | **Justification** | **Cost** |
| Azure | Run IoT management website. Windows VM e1, 10 hrs per week, 8 weeks. | $250 |
| Network Monitoring Software (Spiceworks) | Needed for ongoing monitoring of network performance and security across multiple campuses.  Spiceworks networking software will be used for this project. | $400/yearly |
| Backup Software (AOMEI Backup Technician Plus Unlimited Device and Unlimited Server) | Ensures regular backups of critical data and network configurations for all campuses. AOMEI will be used as a Backup software for this project. | $500/yearly |
| Antivirus Software (Norton) | Protects network devices and servers from malware and other security threats across the campus network. Norton Antivirus will be used for this project. | $200/yearly |

Table 5.2 Cash Resources and Justifications

*Personnel*

|  |  |  |
| --- | --- | --- |
| **Resource** | **Justification** | **Cost** |
| Cyber security analyst | Develops and enforces security policies, monitors network for threats, and responds to incidents across multiple campuses. | $50 per hour; 100 hours =$5,000 |
| System Administrator | Administers servers and network devices perform regular maintenance and supports user issues across all campuses. | $60 per hour; 100 hours= $6,000 |

Table 5.3 Personnel Resources and Justifications

# Project Risks and Mitigation

The following Risks and mitigation strategies are identified while we thoroughly analyse our project.

|  |  |  |
| --- | --- | --- |
| **Risk ID** | **Risk** | **Mitigation** |
| R001 | A group member is sick for multiple weeks | Ensure that all the work done is documented and made available to the other team members so they can continue with the same task they can do so easily. |
| R002 | Equipment delays or unavailability of equipment in the university lab | Make sure to book the lab and equipment in advance and be prepared with a backup timetable in cases where lab times are fully booked. |
| R003 | Azure cloud service costs exceed the planned budget | Ensure that Azure usage is checked frequently and that cost management solutions are employed to prevent exceeding the limit. |
| R004 | Hardware failure of the equipment in a university laboratory | Ensure that laboratory equipment is checked periodically and the lab has backup spare devices. |
| R005 | Limited access to the university lab due to schedule interference and unavailability of the lab. | Contact lab supervisors to discuss how to gain priority access and organise work in periods over off-peak times. |
| R006 | Azure VM integration challenges with the university network | Undergo pre-deployment pilot test and confirm compliance with the university network requirements. |
| R007 | Security vulnerabilities in Azure Machines. | Ensure the cloud resources are secure by setting up firewall procedures, data encryption, and security audit services. |
| R008 | Lack of technical knowledge about complex configurations in Azure | Learn more about Azure, on Azure documentation and other tutorial sites, and consult with the university or Azure support centre. |
| R009 | Power outages in university lab | Use UPS for the Critical lab equipment to save the regular work all the time. |
| R010 | Miscommunications within the team members. | Collaboration tools include WhatsApp, Microsoft Teams, and One Drive. Ensure that there is clear and constant communication and document sharing. |
| R011 | Inaccurate requirement gathering from the stakeholders | Ensure that the project requirements are periodically discussed with other stakeholders and that the plan is modified accordingly. |
| R012 | Software bugs in network management tools | Always check for the latest software version for equipment and perform proper tests before and during implementation. |
| R013 | Environmental factors that likely influence laboratory equipment | Ensure the lab equipment is used in a suitable environment and check the equipment periodically. |
| R014 | Non-compliance with university IT policies | Always interact with university IT teams and ensure they understand all the IT policies to be included in the project. |
| R015 | Loss of data during network transformation or cloud migration | Ensure data integrity through a proper backup plan and conduct migration tests. |
| R016 | Network performance decreases when loads are applied | Perform load testing and adjust and fine-tune the network and the VM settings according to the tests. |
| R017 | Lack of availability for team members because of other commitments | Prepare a work breakdown structure to plan a comprehensive work timeline with potential contingencies. |
| R018 | Unavailability of vendor support on the Azure services | Select Microsoft Azure support options that will give you dependable help and keep records of all communication with the support personnel. |
| R019 | Dynamic stakeholder demands | Define the workflow for change management, including documentation and references to the change request. |
| R020 | Project management difficulties | Implement project management software such as MS Project to track tasks and their due dates. |
| R021 | Natural disasters affecting the timelines of the project | Create a disaster contingency plan and make routine backups of important data kept in other locations or web-based storage. |

Table 6.1 Project Risk and Mitigation Strategies of the KNU Network Design

# Schedule

The following image shows the Gantt Chart and the WBS of the KN University Network project. We plan to start the project on the 22nd of July 2024 and finalise the project on the 07th of October 2024. The Project file is attached to this document.

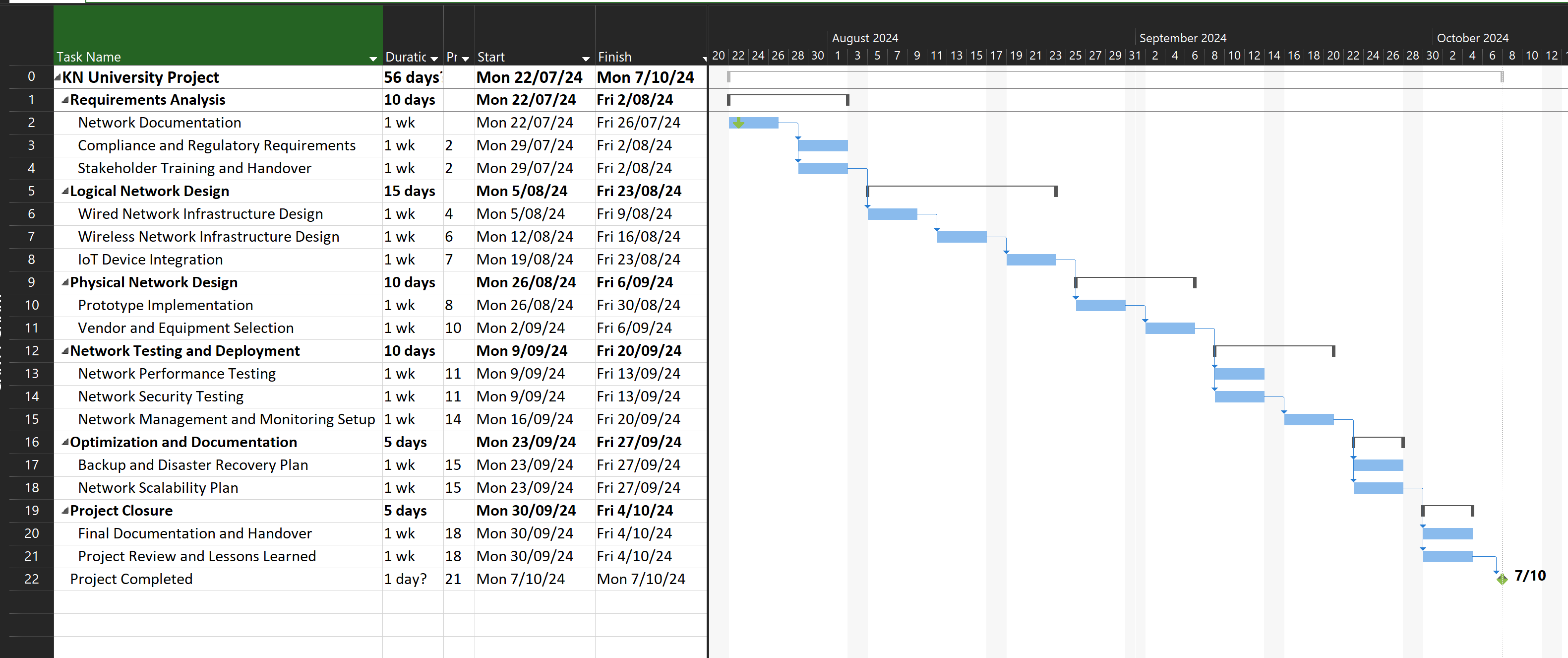


Image 7.1 WBS and the Gantt chart of KNU Network Design

# Ethical and Professional Issues

A project that involves many stakeholders always has a potential for Ethical and Professional issues. The following issues that we identified and addressed are the mitigation strategies for sustainability and the professionalism of the project.

1. Data Breach and Confidentiality

The data from the university could be exposed and accessed by unauthorized personnel during or after the completion of the project, resulting in data leakage.

Mitigation Strategy:

* All the information that will be entered into the system should be backed by high levels of security; access to the data should be limited, and all information should be encrypted.
* This includes conducting routine security audits and vulnerability assessments.
* All collected data should be protected by data protection laws and by the policies of the university.

1. Network Downtime Impact.

Negativity and network interruptions during implementation can hinder the university, its students, personnel, and various research activities.

Mitigation Strategy:

* Organise maintenance or implementation activities at times other than busy production periods.
* Provide a detailed schedule and expected effects of the planned downtimes to all the relevant audiences.
* Ensure that services are backed up and can be restored immediately in case of any problems.

1. Ethical management and processing of personal information.

Data collected from IoT and network flow records must be managed and collected ethically and in compliance with legal obligations.

Mitigation Strategy:

* Minimize or eliminate personal data where possible.
* Students and staff should be told specifically what data is being collected and for what purpose.
* Adhere to applicable data protection regulations, including those of the General Data Protection Regulation (GDPR) or any other local laws.

1. Consent And Transparency.

Ensure all network users are fully informed and consent to the observation and data-gathering processes.

Mitigation Strategy:

* Ensure privacy policies and terms of use are properly communicated and understandable to the common customer.
* Obtain prior permission from the users whenever deemed necessary.
* Regularly assess and modify the consent procedures to conform to the current standards.

1. Analysis of Professional Integrity and Accountability.

The employees should follow professional standards and ethical requirements while completing the project.

Mitigation Strategy:

* All decisions, changes, and approvals made throughout the project must be documented.
* Establish and maintain a policy of openness and honesty with team members.
* Ensure that all team members professionally conduct themselves by acting according to the ACS Code of Conduct and other professional standards where appropriate.

1. Support and Maintenance after Implementation

Making provisions for post-implementation network support that may be required in the future.

Mitigation Strategy:

* Produce comprehensive handover documentation and guided workshops for IT staff within the university.
* Develop detailed maintenance and support schedules with duties and timeframes agreed upon with the vendors.
* Ensure that stakeholders are also willing to provide feedback and report issues of concern.