2025
MODERNIZATION OF COLLAGE NETWORK

NET-TECH
SOLUTIONS

Prepared for :
Technical Collage Gampaha

Prepared by :
Piyusha Akash
NETWORK TECHNICIAN

OVERVIEW

This project aims to upgrade and modernize the existing network infrastructure of Technical College Gampaha, which currently suffers from outdated hardware, obsolete software systems, unplugged cabling, and poor connectivity. The objective is to establish a robust, secure, and high-performance network to meet the academic and administrative demands of a modern technical education environment.

Current Issues Identified:
- Outdated software: Legacy operating systems and unsupported applications pose security and performance risks.
- Old networking components: Aging switches, routers, and access points reduce reliability and scalability.
- Disconnected cables and improper topology: Poorly maintained and unplugged cables lead to unstable connections and downtime.
- Lack of central management and monitoring tools: No visibility over network performance or device health.
- Limited Wi-Fi coverage: Weak or no wireless access in classrooms and labs.
- Security vulnerabilities: No firewall or updated antivirus systems for endpoint protection.

Proposed Upgrades:
- Replace old switches and routers with managed, high-speed gigabit devices.
- Re-cable the network using structured CAT cabling with proper labeling.
- Upgrade servers and client systems with the latest OS and licensed productivity tools.
- Implement a central firewall and antivirus for better security.
- Deploy wireless access points to ensure full Wi-Fi coverage.
- Introduce network monitoring tools for real-time management and troubleshooting.

Expected Outcomes:
- Enhanced network speed and reliability.
- Improved cybersecurity and data protection.
- Better connectivity for students, staff, and administrators.
- Scalable infrastructure to support future expansion (e.g., smart classrooms, cloud learning platforms).
- Increased overall productivity and reduced downtime.

CONCLUSION

This upgrade is essential to align the college's digital infrastructure with modern educational standards. The new network will provide a stable, secure, and scalable environment that supports digital learning, administration, and campus growth.

BACKGROUND INFORMATION:

The Technical College Gampaha is currently operating with a highly outdated network infrastructure that no longer meets the demands of modern education and administration. The college has a Campus Area Network (CAN) that spans 7 buildings, out of which 6 buildings contain classrooms and computer labs that are actively used for academic purposes.
The current computer lab setup includes:

- 2 PC labs, each equipped with 31 computers
- 1 lab with 26 computers
- 1 smaller lab with 4 computers
- A central server room, where the college's servers and core networking equipment are located.

The existing network consists of legacy components, including outdated switches, routers, and disconnected or unmanaged cabling. The physical condition of the network is poor, with unplugged cables, software that is no longer supported, and no centralized network management.

The current Internet Service Provider (ISP) contract is ending, requiring an immediate solution for continued connectivity. There is no structured documentation of the number of teaching or administrative staff, but the network is expected to support multiple users across all computer labs and classrooms, with potential for further expansion to support wireless access and smart learning environments.

The college urgently needs a network upgrade to:

- Transition from legacy systems to modern networking standards
- Support current and future teaching technologies
- Enhance performance, security, and reliability
- Provide consistent connectivity across all buildings

This project will modernize the entire campus network, bringing it in line with today's IT standards and supporting a more productive, digital-focused educational experience.

REQUIREMENTS FOR NETWORK UPGRADE:

To upgrade the college's legacy network to modern-day standards, the Network Manager must fulfill the following requirements:

1. Define the communication methods used by the college:
   - a. Must follow current industry standards (e.g., Ethernet LAN for wired communication).
   - b. Must support all computer labs and classrooms across 6 academic buildings.
   - c. Must define and implement IEEE standard protocols such as IPv4 and/or IPv6 addressing to ensure compatibility and scalability.

1. Develop a solution for upgrading the current network infrastructure:
   - a. Must upgrade:
     - 92+ desktops located across 4 computer labs
     - Servers in the central server room
     - Printers across multiple buildings (north, south, east, and west locations)
   - b. A new ISP contract must be established, capable of handling the total bandwidth needs for all labs and administrative operations.
   - c. Must implement low-cost, reliable Wi-Fi access points (no need for Wi-Fi 6) to provide basic wireless connectivity where required (e.g., teacher/admin areas or shared zones).

3. Identify all required network equipment and justify their use, such as:
   - Unmanaged or smart switches, routers, CAT5 or CAT5e cabling, patch panels, racks, and basic firewall/router combo
   - Must ensure selections are cost-effective, sufficient for current demand, and within project budget.

4. Define at least 2 VLANs and justify their implementation:
   - VLAN 10 – Academic/Admin Network (e.g., staff and server access)
   - VLAN 20 – Student Labs (for isolated student activity)
   - VLANs will improve security, bandwidth control, and performance separation.

5. Write a professionally formatted business proposal including:
   - Project goals, justification, benefits, cost summary, and implementation plan.

6. Include a detailed network layout diagram:
   - Visualize all computer labs, server room, and building interconnectivity across the Campus Area Network (CAN) using Visio or equivalent software.

7. Prepare an Excel spreadsheet listing:
   - All items to be purchased (e.g., switches, cabling, routers, access points)
   - Their individual prices, total cost breakdown, and
   - Web links to verified sources/vendors

NETWORK ISSUES AND LIMITATIONS:

The current network infrastructure at Technical College Gampaha presents several critical issues and limitations that hinder the effectiveness, security, and scalability of digital learning and administrative operations.

1. Outdated Network Components
Most networking hardware in use is obsolete. Devices such as switches, routers, and hubs are aged and fail to meet modern performance or reliability standards. This results in frequent disconnections, network lags, and limited throughput. Many systems still rely on legacy connections, and the absence of proper firmware or software updates exposes them to vulnerabilities.

2. Poor Cabling Infrastructure
The physical cabling system across the campus is in disrepair. Many Ethernet cables (likely CAT5) are unplugged, damaged, or routed improperly. Cable management is nearly non-existent in some labs, which increases the risk of disconnections and accidents. A lack of labeling further complicates troubleshooting and maintenance.

3. Limited Network Segmentation
Currently, all devices seem to exist on a flat network topology, without VLANs or logical segmentation. This causes performance bottlenecks and significantly increases the attack surface, as any compromised machine could potentially reach all other devices on the network.

4. No Wireless Connectivity in Key Areas
While Wi-Fi is not a priority in all areas, the absence of even basic wireless access points in staff or shared zones limits mobility and access to cloud-based or collaborative platforms. Instructors and administrative staff are forced to rely on fixed-line PCs, restricting flexibility.

5. ISP and Internet Reliability
The existing ISP contract is expiring, and the current internet setup is not scalable. Bandwidth limitations, high latency, and inconsistent uptime affect daily operations, especially in labs where multiple systems require simultaneous internet access for research, virtual labs, or cloud applications.

6. Server Room Limitations
Although there is a central server room, it lacks proper ventilation, structured racks, and power backup systems. The servers are aging and may not meet the hardware requirements for virtualization, centralized authentication, or backup systems, limiting future scalability.

7. Lack of Monitoring and Management Tools
There is no centralized system in place for monitoring, logging, or controlling the network. Issues often go unnoticed until users report them. Without proper visibility, proactive troubleshooting and capacity planning are impossible.

8. Software Compatibility Issues
Many desktops in the labs are still running outdated operating systems and applications, which are no longer supported by vendors. This limits compatibility with modern tools and exposes systems to critical vulnerabilities and performance issues.

PROPOSED SOLUTIONS:

To overcome the existing limitations in the network infrastructure at Technical College Gampaha, the following comprehensive solutions are proposed. These are designed to modernize the college's Campus Area Network (CAN), improve reliability, ensure security, and support future academic and administrative growth.

1. Hardware Upgrades
A complete refresh of all critical network hardware is essential. The following upgrades are recommended:
- Core and Access Switches: Replace existing outdated switches with unmanaged or smart switches that support VLANs and PoE (if needed). Each building should have one or more access switches connecting labs and staff areas, linked back to a core switch in the server room.
- Routers and Firewalls: Implement a modern router with built-in firewall features, or a dedicated firewall appliance, to provide network security and traffic control.
- Desktops: Upgrade the 92+ lab desktops with new or refurbished systems that meet current performance standards (minimum i3 or Ryzen 3, 8GB RAM, SSD recommended).
- Printers: Ensure existing printers are connected via network (Ethernet or Wi-Fi), and properly assigned static IPs or reserved DHCP leases.

2. Cabling and Physical Infrastructure
The current cable infrastructure is disorganized, outdated, and partially disconnected. The following steps are necessary:
- Replace or reterminate existing CAT5 cabling where damaged, and re-organize cable routing in all labs.
- Use structured cabling with proper labeling, patch panels, and cable trays to ensure long-term manageability.
- Establish a central backbone link between each building and the server room using shielded CAT5e or fiber (if within budget), depending on distance.
- Use RJ45 wall ports and patch panels for clean and reliable physical connections in all rooms.

3. Network Segmentation (VLANs)
To improve security and network efficiency, implement at least two VLANs across the CAN:
- VLAN 10 – Admin/Staff Network: For administrative computers, servers, and confidential data access.
- VLAN 20 – Student/Lab Network: Isolated from the admin VLAN, used for lab computers and general internet access.This segmentation limits internal threats, controls broadcast traffic, and enables better traffic monitoring and policy enforcement.

4. Internet and ISP Setup
As the current ISP contract is ending, a new connection must be established with the following considerations:
- Choose an ISP that offers reliable business-class broadband with symmetrical speeds and a static IP address (if hosting internal services).
- Bandwidth should be sufficient for simultaneous use in all labs, server backups, updates, and possible future cloud-based learning platforms.
- Use a load-balancing or failover router if budget permits, for backup connectivity in case of outages.

5. Wireless Access
While Wi-Fi 6 is not required, affordable and stable wireless coverage is still essential in staff rooms, shared study areas, and admin offices. Recommendations:
- Deploy 2.4GHz/5GHz dual-band access points in areas with foot traffic or shared use.
- Use low-cost brands like TP-Link Omada, Ubiquiti, or MikroTik that support centralized control without high licensing fees.
- Secure all wireless networks with WPA3 or WPA2-PSK, and hide SSIDs for internal use.

6. Network Security Enhancements
To protect the upgraded network and sensitive college data, the following security measures should be implemented:
- Install a dedicated firewall appliance at the network edge to control and monitor incoming and outgoing traffic.
- Deploy antivirus and endpoint protection software on all desktops and servers for real-time threat detection.
- Implement centralized user authentication and access control to restrict network and resource access only to authorized personnel.
- Establish network access policies, including VLAN-based segmentation and guest access restrictions.
- Conduct regular security training and awareness programs for staff and students to promote safe computing practices.

7. Network Monitoring Tools
Introduce basic network management to track device health and bandwidth usage:
- Use tools such as PRTG Network Monitor, Zabbix, or The Dude (by MikroTik) for real-time monitoring.
- Maintain IP documentation, network diagrams, and device logs for faster diagnostics and auditing.

8. Software Updates and Licensing
Many systems currently run outdated or unsupported operating systems. The following upgrades are proposed:
- Install latest Windows 10/11 or Linux distributions on all lab machines depending on license availability and use case.
- Replace any pirated software with open-source or licensed alternatives (LibreOffice, GIMP, Visual Studio Code, etc.)
- Set up centralized update policies using WSUS (Windows Server Update Services) or similar to ensure timely patching.

By implementing these proposed solutions, Technical College Gampaha will gain a modern, secure, and scalable network infrastructure, enabling better academic delivery, smoother administrative operations, and support for future expansion.

SERVER ROOM PHYSICAL DIAGRAM
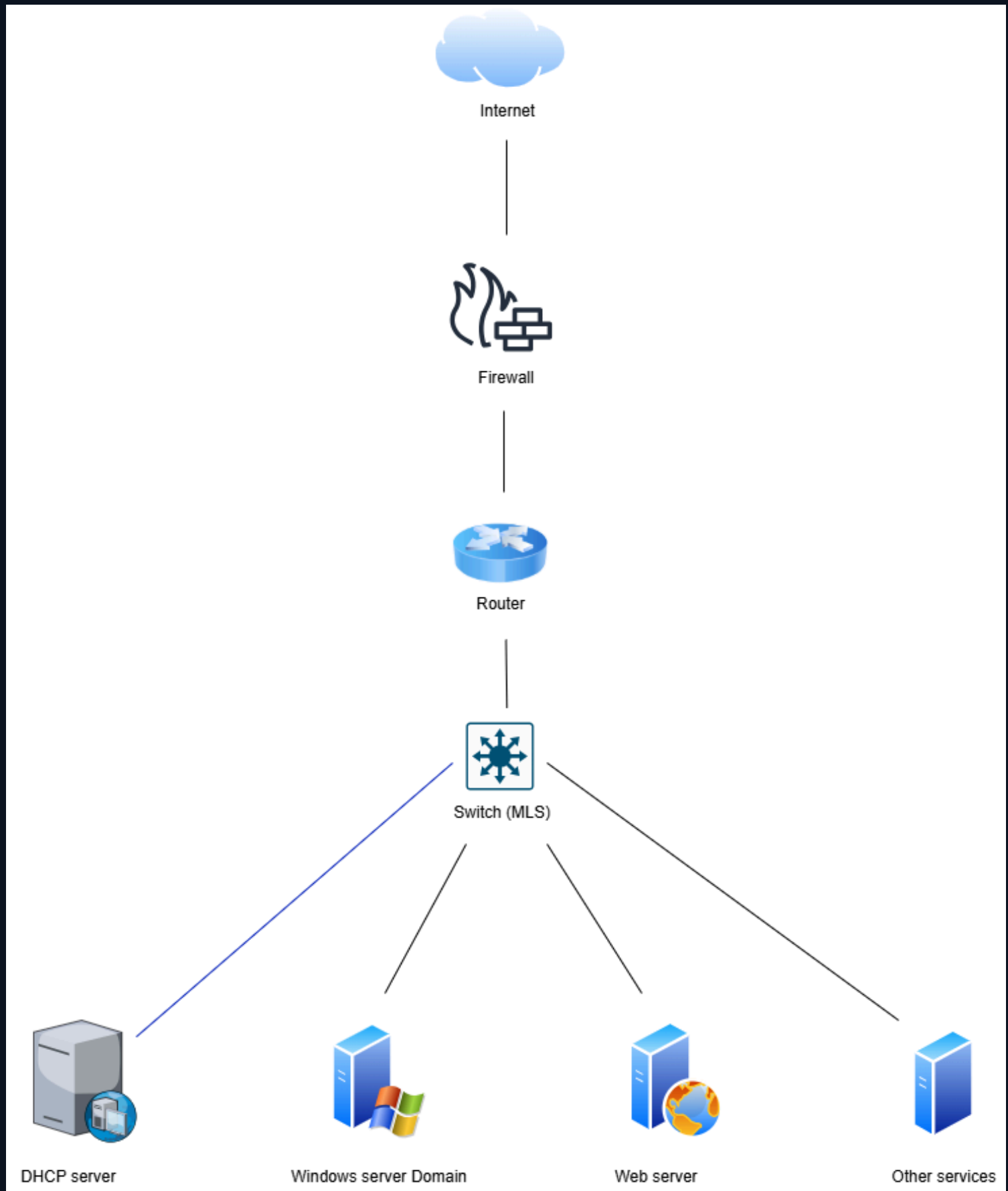
PROJECT OBJECTIVES:

Upgrade or install new network devices, test connectivity, and remove legacy hardware within 8 weeks of the start date without affecting normal business operations. Stay under LKR 2,000,000 budget.

Success Criteria:

1. Network upgrade is fully upgraded within 8 weeks of the start date.
2. Business operations are not negatively affected.
3. Project is completed within LKR 2,000,000 budget.

WEEKMILESTONKEY OUTCOMES:

1st Week:
- Plan & Schedule Project
- Scope, roles, timeline, and standards defined

2nd Week:
- Install Network Hardware Infrastructure
- Racks, rack accessories, structured power & cooling in server room

3rd Week:
- Deploy Core Network Devices & Servers
- Firewall, router, multilayer core switch, Windows Server (domain), Web Server, DHCP Server

4th & 5th Weeks:
- Install Network Cabling
- CAT5/CAT5e runs to labs & classrooms, inter-building backbone, patch-panel terminations

6th Week:
- Configure Network Devices & Services
- VLANs, IP schemas, server roles (DNS, DHCP, file share), basic Wi-Fi APs

7th Week:
- Connect & Validate Endpoints
- Upgrade/confirm NICs, plug in desktops & printers, functional tests, monitoring baseline

8th Week:
- Decommission Legacy Hardware
- Remove obsolete switches, hubs, stray cabling; recycle / store as required

DETAILED TASK LIST:

1 — Plan and Schedule Project (Week 1)
1.1 Define communication methods (Ethernet LAN, basic Wi-Fi)
1.2 Research current industry standards (IEEE 802.3, 802.11)
1.3 Choose IPv4/IPv6 plan, VLAN design
1.4 Assign project roles & responsibilities
1.5 Publish detailed Gantt / calendar schedule

2 — Install Network Hardware (Week 2)
2.1 Install server-room racks (42U)
2.2 Fit rack accessories (shelves, PDUs, cable managers)
2.3 Verify adequate ventilation / AC and UPS capacity

3 — Deploy Network Devices & Servers (Week 3)
3.1 Mount and cable multilayer core switch
3.2 Install edge firewall and router (ISP hand-off)
3.3 Rack servers:
 • Windows Server (Active Directory / PC control)
 • DHCP Server (or DHCP role on Windows Server)
 • Web Server (college portal / intranet)
 • Additional services/backup unit
3.4 Label and document all ports

4 — Install Network Cabling (Weeks 4 – 5)
4.1 Mount RJ-45 keystone patch panels in each rack
4.2 Run CAT5/CAT5e data cables from labs (92 PCs) to patch panels
4.3 Pull inter-building backbone (shielded CAT5e or fiber if budget allows)
4.4 Cable printers to nearest data patch ports (≈ 5 units)
4.5 Run AP drops for basic Wi-Fi in staff/common zones
4.6 Dress cables in trays; label both ends

5 — Configure Network Devices (Week 6)
5.1 Configure core switch: VLAN 10 (Admin/Staff), VLAN 20 (Student Labs)
5.2 Configure firewall rules and NAT, set up secure remote management
5.3 Configure router WAN/LAN, static routes, DNS forwarders
5.4 Configure Windows Server roles (AD, DNS, file shares, GPOs)
5.5 Enable DHCP scope, reservations for printers/servers
5.6 Deploy low-cost dual-band APs; set WPA2/WPA3 security

6 — Upgrade Legacy Endpoints (Week 7)
6.1 Check / replace NICs on 92 desktops where needed for 100/1000 Mb
6.2 Verify printer NICs (≈ 5) support current speeds; upgrade if required
6.3 Confirm server NICs (6) at gigabit; add second NICs if bonding required

7 — Connect Endpoints & Baseline (Week 7)
7.1 Patch each workstation to its data port; join to domain
7.2 Patch printers; assign static IP or DHCP reservation
7.3 Run connectivity tests per VLAN (ping, file share, AD login)
7.4 Test internet access through firewall
7.5 Capture baseline performance with monitoring tool (e.g., PRTG, Zabbix)

8 — Remove Legacy Hardware (Week 8)
8.1 Obtain stakeholder approval for decommissioning
8.2 Remove obsolete hubs, unmanaged switches, stray cabling
8.3 Recycle or securely dispose of outdated equipment

MATERIAL, EQUIPMENT AND SERVICES BREAKEDOWN

Item	Quantity	Unit Price (LKR)	Estimated Cost (LKR)
92 Desktop Upgrades / Replacements	92	LKR 90,000.00	LKR 8,280,000.00
5 Printers (Network-ready)	5	LKR 100,000.00	LKR 500,000.00
6 Servers (Web, Windows AD, DHCP, Backup)	6	LKR 500,000.00	LKR 3,000,000.00
Firewall Appliance	1	LKR 300,000.00	LKR 300,000.00
Router (Business-class)	1	LKR 250,000.00	LKR 250,000.00
Multilayer Core Switch (1 unit)	1	LKR 400,000.00	LKR 400,000.00
Edge Switches (for 6 buildings)	6	LKR 175,000.00	LKR 1,050,000.00
Network Rack + Accessories (AC, UPS, trays)	1	LKR 700,000.00	LKR 700,000.00
CAT5e Cabling, Patch Panels, Accessories	1	LKR 600,000.00	LKR 600,000.00
Basic Wi-Fi APs (5–7 units)	6	LKR 29,166.67	LKR 175,000.00
Labor/Installation & Testing	1	LKR 800,000.00	LKR 800,000.00
Spare NICs, Connectors, Tools	1	LKR 200,000.00	LKR 200,000.00
			LKR 16,255,000.00

How the figures map to the original roles
- Network Engineer: 8 days × LKR 12,000 = 96,000
- Technicians: 20 tech-days × LKR 7,000 = 140,000
- Electrician: 6 days × LKR 5,000 = 30,000
- Testing Staff: 4 days × LKR 6,000 = 24,000
- Project Supervisor: 5 days × LKR 8,000 = 40,000
- Grand Total: 96k + 140k + 30k + 24k + 40k ≈ LKR 330,000