Northen Beaches Shopping Center Network Design, Security, and Project Management

Khalid Bakhshi

46392459

Table of Contents

Executive Summary

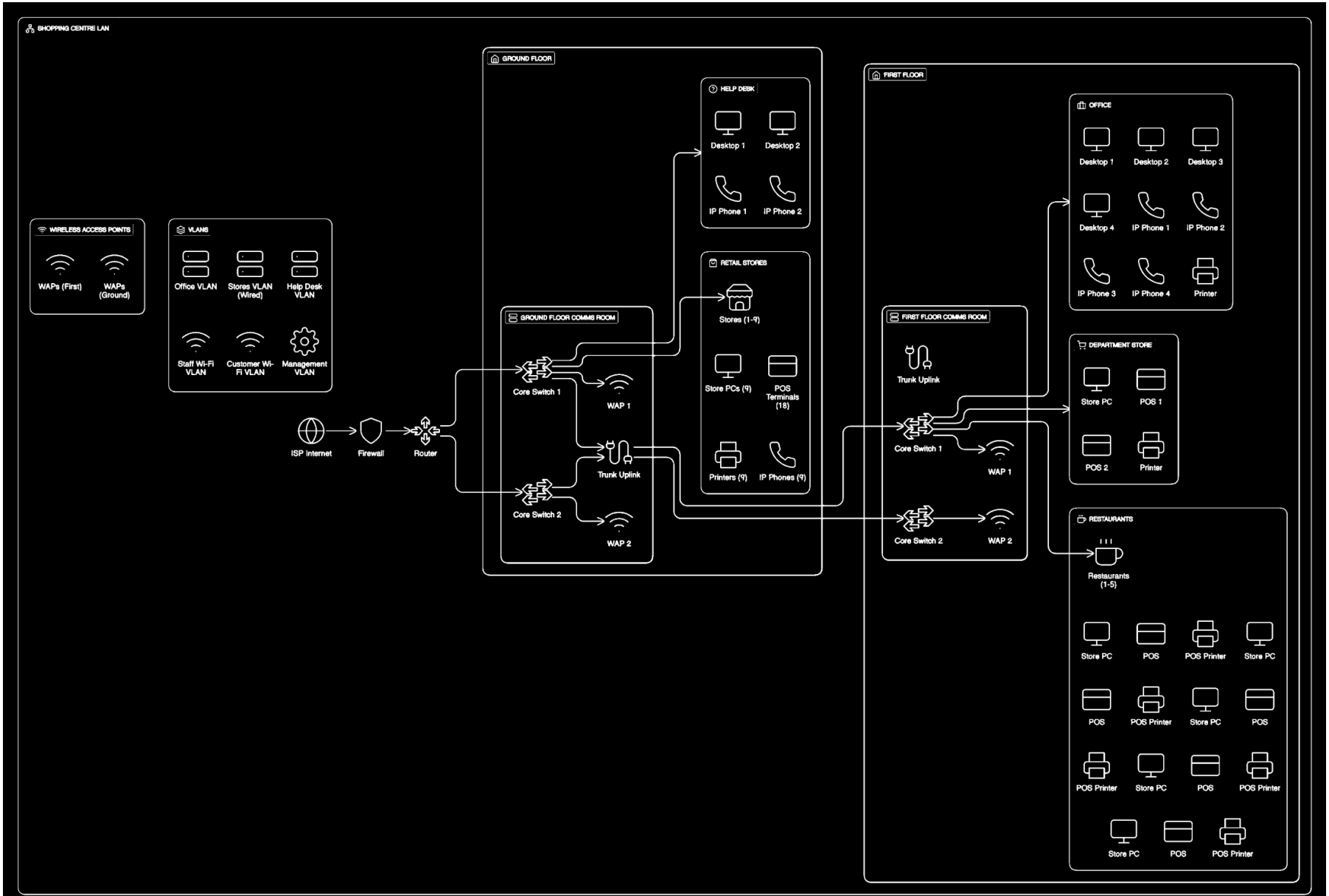
This report shows the proposed upgrade of the Local Area Network infrastructure for a multilevel shopping center, presenting both physical and logical requirements to support an efficient, secure, and resilient ICT environment. The aim is to design and build a scalable, segmented, and performant network that serves retailers, restaurants, center management, office users, and public Wi-Fi users in a way that maintains data protection and system uptime. The proposed LAN has core Layer 3 switches for redundancy on each floor, with its own VLANs for each user group, including stores, restaurants, help desk, administration, and Wi-Fi services. All inter VLAN routing is performed by the core switches, which connect to a centralized firewall and router, enforcing one set of security policies and providing access to the internet. All wireless usage will be served by two sets of WAPs on each floor, with SSIDs mapped to VLANs to maintain isolation.

The project schedule spans from 01 June 2025 to 31 October 2025, with a timeline approach covering procurement, delivery, installation, configuration, and testing. External projects at Parramatta, Lower North Shore, and Bathurst are integrated into the timeline to prevent conflict of resources. Labor, equipment, and configuration have been budgeted, with industry standard devices such as Cisco switches, Ubiquiti WAPs, HP desktops, and IP phones selected for quality and cost efficiency. Also, through risk assessment, threats such as power loss, fire, circuit failure, malware, physical disasters, external and internal intruders, and social engineering. Reduction strategies include uninterruptable power supply usage, VLAN isolation, free open-source RADIUS based Wi-Fi authentication, endpoint protection, surveillance, and regular staff awareness training. Security and privacy concerns, specifically for tenant data such as POS and inventory, were addressed by introducing VLANs, ACLs (Access Control Lists), and encrypted management protocols. These changes needed minor configuration overhead and did not significantly affect the existing cost model.

Furthermore, the ACS code of Professional Ethics, the project ranks honesty, trustworthiness, respect, and professionalism at its highest. Clear communication of capabilities, privacy and confidentiality of stakeholders, and system robustness and inclusivity are a must as these principles have allowed for informed actions and decisions throughout the project.

Overall, this LAN upgrade will improve the shopping center into a secure, efficient, and future ready environment capable of supporting evolving tenant needs, customer services and operational efficiency, whilst attaining industry standards for reliability and privacy.

Diagram


SHOPPING CENTRE LAN
WIRELESS ACCESS POINTS
WAPs (First)
WAPs (Ground)
VLANS
Office VLAN
Stores VLAN (Wired)
Help Desk VLAN
Staff Wi-Fi VLAN
Customer Wi-Fi VLAN
Management VLAN
ISP Internet
Firewall
Router
GROUND FLOOR
GROUND FLOOR COMMS ROOM
Core Switch 1
WAP 1
Trunk Uplink
Core Switch 2
WAP 2
HELP DESK
Desktop 1
Desktop 2
IP Phone 1
IP Phone 2
RETAIL STORES
Stores (1-9)
Store PCs (9)
POS Terminals (18)
Printers (9)
IP Phones (9)
FIRST FLOOR
FIRST FLOOR COMMS ROOM
Trunk Uplink
Core Switch 1
WAP 1
Core Switch 2
WAP 2
OFFICE
Desktop 1
Desktop 2
Desktop 3
Desktop 4
IP Phone 1
IP Phone 2
IP Phone 3
IP Phone 4
Printer
DEPARTMENT STORE
Store PC
POS 1
POS 2
Printer
RESTAURANTS
Restaurants (1-5)
Store PC
POS
POS Printer
Store PC
POS
POS Printer
Store PC
POS
POS Printer
Store PC
POS
POS Printer
Store PC
POS
POS Printer

Physical & Logical Network Design Description

This diagram effectively shows the proposed physical network design for the shopping centers LAN upgrade. Both Layer 2 and 3 Devices, VLAN segmentation, wireless access point coverage, and a secure perimeter have been placed to ensure reliable seamless connectivity for customers, staff, and management.

1. VLAN Segmentation

Each VLAN is named and mapped to separate user groups to guarentee isolation, security, and traffic control.

VLAN Name	Purpose
Store VLAN	Wired PoS system, IP phones, PCs (Stores 1-9)
Office VLAN	Office desktops, phones, printer
Help Desk VLAN	Help desk desktops and IP phones
Staff Wifi VLAN	Authenticated wireless for staff and tenants
Customer Wifi VLAN	Guest Wi-Fi via captive portal (internet only)
Management VLAN	Used for monitoring, switch/router admin

2. Infrastructure core

The network design has two core Layer 3 switches per floor which is in each comms room to provide inter-VLAN routing and make certain that all systems operate smoothly. The ISP connection ends at a firewall in the ground-floor comms room, which enforces perimeter security policies between the Internal LAN and External internet. From the firewall, traffic passes through a router that distributes connectivity to core switches. This enables reliable and secure access across all network segments.

3. Wireless Access Design

Each floor contains four wireless access points (WAPs). Two WAPs are positioned in each comms room to ensure comprehensive wireless coverage, specifically in high density areas such as the food court and retail walkways. These WAPs broadcast multiple SSIDs, and each one is placed to its respective VLAN through trunk links, to allow secure and segmented wireless access [1]. Supporting 802.1Q VLAN tagging, the WAPs Connect to the network through a centralized backhaul to the core switches, allowing for improved management and traffic separation for different user groups.

4. Redundancy and Trunking

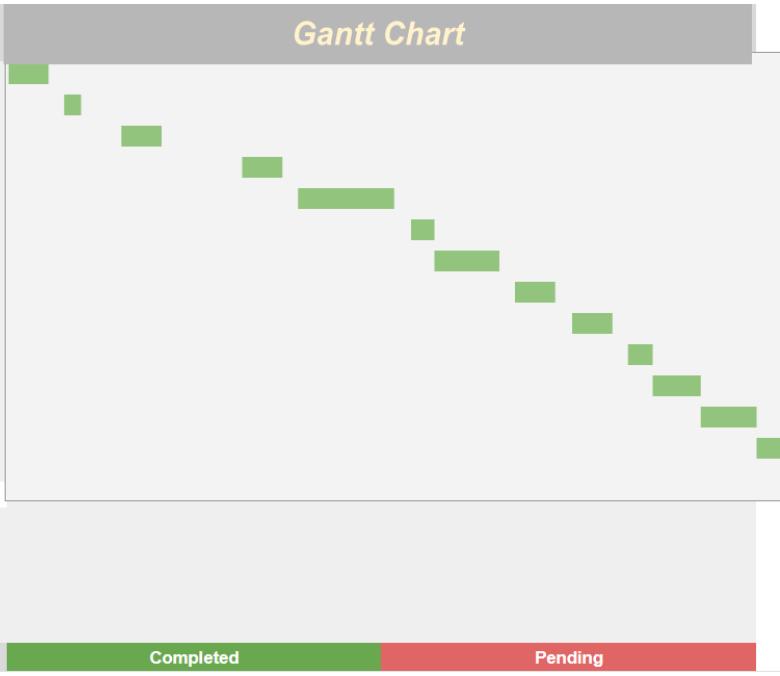
By placing trunk uplinks between floors redundancy in the network is achieved through trunk uplinks between floors, allowing streamlined communication and failover reduction across the core switches. These inter switch trunk links carry 802.1Q VLAN tagged traffic, which efficiently enables data distribution and flexible routing between network segments [2]. Lastly, to ensure efficient dependable internet access, dual uplinks from the router and firewall provide WAN redundancy, which reduces the risk of downtime as it is a single point of failure.

Timeline Implementation Plan and Costing

Item	Cost per item (AUD)	Quantity	Total Cost (AUD)
Computers (Dell OptiPlex 7010)	$959.00	18	$17262.00
Display (Dell 24 inch P2422H)	$263.00	18	$4734.00
IP Phones (Cisco 8841)	$489.00	15	$7335.00
Printers (HP LaserJet Pro M404dn)	$399.00	16	$6384.00
POS terminals (Square Register)	$1099.00	25	$27475.00
Layer 3 Switches (Cisco Catalyst C0300-24T-E)	$1570.00	4	$6280.00
Wireless Access Points (Ubiquiti UniFi 6 LR)	$300.00	8	$2400.00
Router (Ubiquiti EdgeRouter 4)	$416.00	1	$416.00
Firewall appliance (Fortinet FortiGate 60F)	$1100.00	1	$1100.00
Rack Mount Cabinets (12U Wall-Mount Rack)	$170.00	2	$340.00
Cabling (Cat6 with faceplates and ducts)	$50.00	2	$100.00
Patch Panels (24 port Cat6 Panels)	$50.00	1	$50.00
Labor (Delivery and Installation)	$4000.00	1	$4000.00
Labor (Configuration and VLAN setup)	$3500.00	1	$3500.00
Labor (Testing and Documentation)	$3000.00	1	$3000.00

Total cost: $84,374 AUD

Task	Start Date	End Date	Progress
Parramatta Network Upgrade	6/2/2025	6/6/2025	100%
Parramatta Network Testing	6/9/2025	6/10/2025	100%
Lower North Shore Rewiring	6/16/2025	6/20/2025	100%
Bathurst Network Test & Plan	7/1/2025	7/5/2025	100%
Procurement of Equipment	7/8/2025	7/19/2025	100%
Delivery of Equipment	7/22/2025	7/24/2025	100%
Installation (Cabling & Racks)	7/25/2025	8/1/2025	100%
Installation (Core Network Devices)	8/4/2025	8/8/2025	100%
Install End Devices	8/11/2025	8/15/2025	100%
Wireless AP Installation	8/18/2025	8/20/2025	100%
Configuration of VLANs & Routing	8/21/2025	8/26/2025	100%
System Testing & Troubleshooting	8/27/2025	9/2/2025	100%
Final Documentation & Handover	9/3/2025	9/5/2025	100%
Overall Status	**6/2/2025**	**9/5/2025**	**100.00%**



Risk Assessment

Assets (with value/priority)	Fire	Flood	Power loss	Circuit Failure	Hardware failure	Virus/Malware	Internal Intruder	External Intruder	Social Engineering
Client Database (CRM / PoS Systems)	Back up to cloud	Elevate equipment	Offsite/cloud backup	Redundant cabling	Scheduled maintenance	Regular updates and patches	Role-based access control (RBAC)	Firewall with IDS	Staff training & phishing simulations
Financial Database / Billing System	Offsite/cloud backups	Cloud hosting	Water-resistant cases	Redundant database links	High-availability setup	Isolate billing systems	Separate financial network	Encrypt billing traffic	Billing team awareness training
Core Network Switches (L3)	Install fire suppression	Wall-mounted racks	Leak detectors	Redundant links between switches	Spare switches ready	Switch OS hardening	Restrict CLI access	MAC address filtering	Limit support access to CLI
Router	Fire-resistant enclosures	Rack elevation	Ceiling cabling	Backup router ready	Backup router in stock	Router firmware updates	Lock admin credentials	Harden router ACLs	Lock router configuration access
Firewall Appliance	Isolated, cooled rack	Raised cabinets	Elevated power paths	Fail-open policies	Redundant firewall unit	Deep packet inspection	Segregate management network	Keep firmware updated	Admin credentials rotated regularly
Wireless Access Points (WAPs)	Certified WAPs	Ceiling mount only	Elevate PoE sources	Connect to multiple switches	AP redundancy via controller	Secure controller access	WAP admin portal lockdown	Disable open SSIDs	Restrict WAP config access
PoS Terminals (Retail & Restaurants)	Surge protectors	Elevate PoS	Use waterproof covers	Connect to switch pairs	Maintain spare units	Limit USB use	Restrict device login	Network isolation	Staff training for PoS use
Office & Admin PCs	Keep area clear	Raised desks	Unplug during alerts	Multiple uplinks per PC	Routine hardware checks	Disable local admin rights	Group policy restrictions	Antivirus + endpoint firewall	Login banners & lock screens
Printers (Shared and PoS)	Avoid heat zones	Shelf printers	Avoid plumbing zones	Alternate power and data links	Service contract for repairs	Print from secure network	Physical access control	Printer admin access passworded	Admin-only printer config
IP Phones (Help Desk & Office)	Use PoE protection	Wall/desk mounting	Moisture-resistant cabling	Switch through multiple ports	PoE switch redundancy	Isolate VoIP VLAN	Network segmentation for VoIP	SIP firewall rules	Staff awareness on fake IT calls
Technical Staff (Admin/Support Team)	Train in protocols	Train in flood protocol	Install floor sensors	Hot spare equipment	Cross-train support staff	Cybersecurity awareness training	Background checks	Remote access VPN only	Mandatory awareness sessions
Network Management Software	Host virtually	Cloud-based	Sensor-integrated alerts	Secondary management interface	Cloud redundancy	Access control & audit logs	Two-factor authentication	Restrict NMS to management VLAN	Restrict NMS access to few admins

Risk Assessment Spreadsheet Analysis

All Assets were prioritized based on their importance to business operations, sensitive data, and their potential effect on factors such as customer service and revenue streams in the shopping center. The most critical assets identified included CRM/POS'S systems, Financial Billing Systems, Core switches, Routers, Firewalls, Wireless Access Points, and Technical Staff and Network Management Software.

CRM/POS'S systems and Financial Billing Systems directly handle sensitive customer and financial data. They are important to all sales activities. If compromised the shopping center could potentially face financial loss, and legal consequences due to data breaches, loss of customer trust, and disruption of business operations [3]. Furthermore, Core Network Infrastructure such as Core Switches, Routers, and Firewalls underpin all internal communications and data flow. These are the backbones of internal and external communication, which enables traffic routing and enforce perimeter security. Compromission of this infrastructure could result in complete network outages, and exposure to external attacks which can severely impact all tenants and management. Also, Wireless Access Points are vital for customer and staff connectivity; and maintaining customer and staff satisfaction. However, if compromised, it allows for unauthorized access to internal networks, eavesdropping on traffic, and network disruption which negatively affects customer experience and store operations [4]. Lastly, Technical Staff and Network Management Software

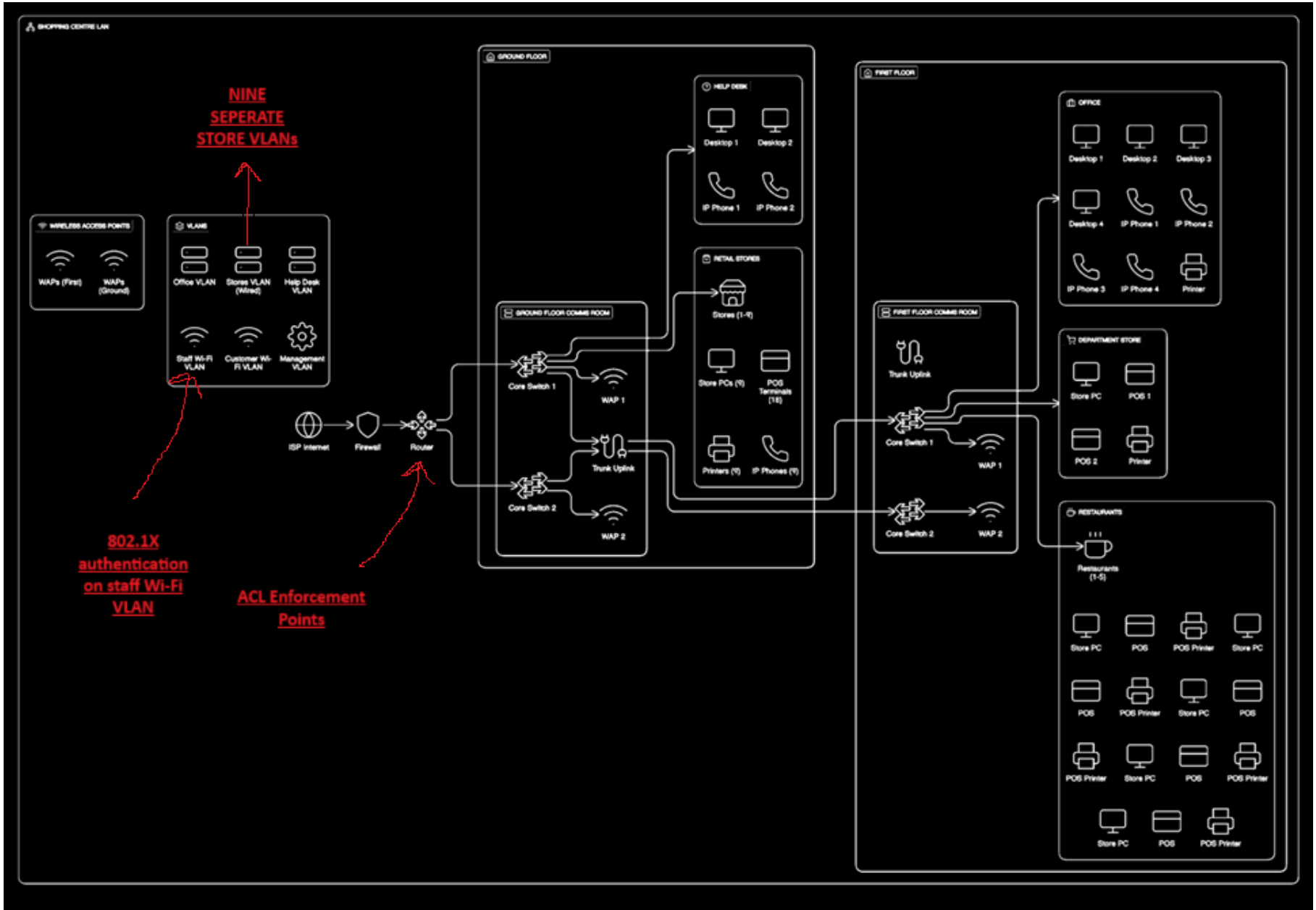
ensures operations integrity and rapid response to incidents. If threat actors can access, they can gain full control of network infrastructure, allowing for traffic manipulation, VLAN breaches, and shutdowns.

These risks were identified based on common threats observed in similar retail/commercial network environments, known infrastructure vulnerabilities such as power loss and hardware failure, environmental risks due to physical placement such as flood and fire in comms rooms, and human centric risks including social engineering and internal or external intruders. These were mapped to each asset by evaluation of exposure, importance and previous case studies in retail networks. In April 2025 Marks and Spencer suffered a significant cyberattack which was attributed to the hacking group "Scattered Spider" [5] [6]. The threat actors use social engineering to compromise a third-party supplier, which allowed attackers to access Mark and Spencer systems. This resulted in the theft of customer data and disruption of online services, including contactless payments and click and collect options. caused Mark and Spencer 750-million-pound loss in market capital. Another example of a case study which involved an environmental threat is the Ocado Warehouse Fire. In February 2019 a fire broke out at Ocado Andover CFC which was attributed to an electrical fault in a battery charging unit [7]. This caused the plastic lid of a grocery carrying robot to catch fire leading to a fire that destroyed the facility and disrupted 10% of Ocado's capacity.

Lastly, the strategies were chosen based on industry's best practices, feasibility and cost effectiveness, and layered security principles. Strategies such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and ISO/IEC 27001 provide structured guidance on how to identify, protect, detect, respond, and recover from these threats [8]. For example, ISO 27001 recommends continuous risk assessments, access control and security awareness training, which is reflected in the controls selected for this project. Also, every strategy was evaluated based on its technical viability and the financial burden it would place on the project budget. Controls such as automated backup systems, cloud-based virus scanning, and rack mounted fire retardants offer high protection whilst being scalable and reasonably priced. For lower priority assets, cost effective methods such as policy update and staff training were favored over expensive technical solutions. Lastly, Layered Security Principles which combine physical, technical, and administrative controls reduce risk substantially. Physical controls such as surveillance, locks, and server room restrictions are a crucial layer of protection to prevent internal threats [4]. Technical controls such as Firewalls, VLAN segmentation and endpoint protection and administrative controls such as security policies, access logs, and routine audits allow for a multifaceted approach which ensures that if one control fails, others still offer protection.

Overall, the proposed measures tailor the unique, real-world challenges of a multi-tenant, customer-facing retail environment. This approach balances security with usability and cost efficiency, ensuring the shopping center remains operational, secure, and trusted by its users.

Revised Diagram



Security and Privacy Recommendations

The original diagram shows VLANS logically separated for Office, Stores, Help Desk, Customer Wi-Fi, Staff Wi-Fi, and Management. This segmentation reduces broadcast traffic and isolates sensitive store data from public traffic. Also, redundant core switches are used on both floors, allowing for high availability and fault tolerance. Firewall and Router at Network Edge allows internet traffic to pass through a firewall before hitting internal systems, which provides perimeter security. Lastly, Trunk Uplinks between switches suggest VLAN tagging is in place, which allows for streamlined inter VLAN routing through a Layer 3 device.

Despite it having a strong foundation, there are still problems that need to be addressed to meet privacy expectations for store-sensitive data. Firstly, the stores shared a common VLAN, which can allow inter store traffic to be sniffed or intercepted if compromised, exposing competitor data [9]. This has been amended by making the VLANs separate from each store to isolate traffic completely. Secondly, the failure to address Access Control Lists (ACL) with the router restricts traffic flow between sensitive segments. The Wireless Access Points lack Roled Based Authentication due to Staff Wi-Fi being accessible to unauthorized guest devices. By using 802.1X authentication in the Staff Wi-Fi VLAN this can be prevented as it requires authentication before allowing network connectivity.

The proposed security and privacy improvements will have a low effect on the project's overall cost. By using separate VLANs per store, it involves only minor configuration work due to no additional hardware being required. Enabling ACLs at the router level also introduces no extra hardware cost but will require labor for configuration and testing. Also Introducing 802.1X authentication for staff Wi-Fi requires a RADIUS server, which is a central server that takes care of authentication and could be implemented using an open-source solution such as FreeRADIUS [10]. Using an open-source solution will result in minimal added expenses if a new server isn't required. Overall, these amendments are a cost-effective measure to substantially improve the networks security.

Overall, the review of the original LAN design has confirmed a solid foundational structure with essential components such as VLAN segmentation, redundant switches, and perimeter security already in place. However, to fully meet the privacy and security requirements of the shopping center several critical enhancements are needed. This also includes isolating each store into its own VLAN, implementing ACLs, and enforcing 802.1X authentication on staff Wi-Fi. These adjustments are aligned with the industry's best practices and offer secure data confidentiality, integrity, and network segmentation. The cost and time pacts of these changes are minimal, requiring only minimal configuration effort and the possible addition of an open sources RADIUS server. By introducing these changes, the shopping centers network will be prepared to protect sensitive information, support operational flow and comply with standard security expectations.

Code of Ethics

2.1 Honesty – (b) Not misrepresent any action, situation, or capability.

Recommendation to Panel:
It is critical that all tender applicants are transparent about their true capabilities and the limitations of their proposed solution. Overpromising or hiding problems in network security, scalability, or ongoing support may lead to long term operational failure [11]. Truth and honesty in capability prevents reputational damage and wasted public or private investment. This prevents misleading claims, protects stakeholder trust, and encourages realistic budgeting outcomes.

2.2 Trustworthiness – (d) Respect the privacy, confidentiality and integrity of any personal or proprietary information

Recommendation to Panel:
Given that the upgraded LAN will transmit sensitive sales, customer, and operational data for multiple businesses, any tender must demonstrate how it protects data privacy and confidentiality. The winning solution must include secure VLAN segmentation, encrypted communication channels, and firm access control policies. This is relevant as it protects sensitive information, reduces risk of data breaches, and aligns with Australian Privacy Obligations [12].

2.3.1 Respect for Others – (f) Identify and mitigate any risks to others associated with your work

Recommendation to Panel: It is essential to choose a solution that not only works, buts actively considers and reduces risks such as downtime for stores, or customer dissatisfaction due to poor Wi-Fi access. Risk mitigation strategies such as planned maintenance windows, disaster recovery plans, and communication protocols should be built into the project. This encourages supplier accountability and protects stakeholders from unintended consequences.

2.3.2 Respect for the Profession – (d) Encourage and support advancing the ICT knowledge and competence of others in the Profession

Recommendation to Panel:
Any winning contractor should leave the shipping center more knowledgeable and self-sufficient. Tender proposals that include documentation, staff training, or knowledge transfers workshops demonstrate a commitment to the profession not just to profit. This is relevant as it promotes sustainability, supports professional development, and reduces dependency on vendors.

Conclusion

The LAN upgrade for the shopping center is a well-considered and effective solution that meets the growing demands of a modern retail environment. It priorities core values such as security, performance, and scalability, making sure each user group from tenants and staff to administrators and customers has efficient and safe access tailored to their specific needs.

Throughout the plan, key risks such as power outages, unauthorized access and malware threats were examined. Steps have also been taken to prevent these through a plethora of preventative technologies, physical protection, and administrative protocols. Importantly the implementation schedule also reflects awareness of existing contractual obligations, striking a balanced commitment fulfilment and quick project delivery.

The project has been led by robust ethical principles, aligned with the standards set out in the ACS Code of Professional Ethics. Respect for data privacy, accountability, and public trust has informed every design and operational decision. Minor amendments to the original design, such as providing greater network separation for individual stores were introduced to enhance data security without it affecting the overall budget.

This network upgrade offers a future ready infrastructure that enhances both business operations and overall experience. It allows the shopping center for lasting success in a fast-moving digital landscape while holding trust and confidence among its stakeholders.

References

[1] X. Ling and K. L. Yeung, "Joint access point placement and channel assignment for 802.11 wireless LANs," *IEEE Transactions on Wireless Communications*, vol. 5, no. 10, pp. 2705–2711, Oct. 2006. Available: https://dl.acm.org/doi/10.1109/INFOCOM41043.2020.9155490 [Accessed: 01 Jun 2025]

[2] Alimi, I. A., & Mufutau, A. O. (2015). Enhancement of Network Performance of an Enterprises Network with VLAN. *American Journal of Mobile Systems, Applications and Services*, 1(2), 82–93. Available: https://www.researchgate.net/publication/321715054_Enhancement_of_Network_Performance_of_an_Enterprises_Network_with_VLAN [Accessed: 01 Jun 2025]

[3] Badgujar, P. (2023). "Securing Customer Data and Best Practices for Retail Point-of-Sale Systems." Journal of Technological Innovations, vol. 4, no. 4, pp. 1–10. Available: https://jtipublishing.com/jti/article/view/73 [Accessed: 01 Jun 2025]

[4] Suroto, "WLAN Security: Threats and Countermeasures," International Journal on Informatics Visualization, vol. 1, no. 4, pp. 232–238, 2017. Available: https://joiv.org/index.php/joiv/article/view/133. [Accessed: 01 Jun 2025]

[5] Assured Digital Technologies, "Cyberattack Lessons: M&S, Harrods, Co-op – What Can We Learn?", *Assured Digital Technologies*, 18-Apr-2024. [Online]. Available: https://assureddigitaltech.com/news/cyberattack-lessons-ms-harrods-coop/?utm_source=chatgpt.com. [Accessed: 03-Jun-2025].

[6] T. Knowles, "Hacking group behind Marks & Spencer cyberattack named," *The Times*, 30-Apr-2025. [Online]. Available: https://www.thetimes.com/business-money/technology/article/hacking-group-behind-marks-and-spencer-cyberattack-named-gpx6rx8sv?utm_source=chatgpt.com&region=global. [Accessed: 02-Jun-2025].

[7] N. Crouch, "Ocado warehouse fire: The questions that need answers," *IFSEC Global*, 08-Feb-2019. [Online]. Available: https://www.ifsecglobal.com/fire-news/ocado-warehouse-fire-the-questions-that-need-answers/?utm_source=chatgpt.com. [Accessed: 02-Jun-2025].

[8] Lokare, A., Bankar, S., & Mhaske, P. (2025). Integrating Cybersecurity Frameworks into IT Security: A Comprehensive Analysis of Threat Mitigation Strategies and Adaptive Technologies. arXiv preprint arXiv:2502.00651. Available: https://arxiv.org/abs/2502.00651 [Accessed: 04-Jun-2025]

[9] Ahmad, I. (2020). "Design and Implementation of Network Security using Inter-VLAN-Routing and DHCP." *Asian Journal of Applied Science and Technology*, vol. 4, no. 3, pp. 37–44. Available: https://www.researchgate.net/publication/346128369_Design_and_Implementation_of_Network_Security_using_Inter-VLAN-Routing_and_DHCP [Accessed: 04-Jun-2025]

[10] F. Chughtai, R. UlAmin, A. S. Malik, and N. Saeed, "Performance Analysis of Microsoft Network Policy Server and FreeRADIUS Authentication Systems in 802.1x based Secured Wired Ethernet using PEAP," *The International Arab Journal of Information Technology*, vol. 16, no. 5, pp. 862–869, Sept. 2019 Available: https://www.researchgate.net/publication/336855071_Performance_Analysis_of_Microsoft_Network_Policy_Server_and_FreeRADIUS_Authentication_Systems_in_8021x_based_Secured_Wired_Ethernet_using_PEAP [Accessed: 05-Jun-2025]

Australian Computer Society, *Code of Professional Ethics*, Mar. 2023. [Online]. Available: https://content.ilearn.mq.edu.au/ab/85/ab85681f17aae2078f00d1a35ec9b6fbb6fb8deb?response-content-disposition=inline%3Bfilename%3D%22CodeOfProfessionalEthics_Mar_2023-2.pdf%22&response-content-type=application%2Fpdf&Expires=1749469860&Signature=OcmaOBIbIN-hMv2NRFtrz-h0hcRl0RP5XO3ZK2rUpeiyVWnwsJ0~DzH3j8NlMcJU8pnzyXcJ7tBDAa2-aYOO-rFYSrqmg8xgB1sztohqxR-fDxmSa3e0aLPHFmQCa1HY3ivC3SHF1vYvQTHvFKGjhQrEb5IfWpQNONqyPxFPrLPxR3aPix1QrBIRcJXJ7pfmxRJQpGt-pLUj~pZh1WxXd~x8AgIo9M9dje4RTnHDHvgYOMQgK6yZ5ab-LikkLSdX7SdEY2hbM4~BuhjvQ~rmir9QSRLDAgJqE-lHuNPwsKRlkvF6vR-xT2wa403mmPiCkctzF2mcdFF1XSlFsFfnYqFA__&Key-Pair-Id=APKAJAEFMXVVB5Z7N4TA [Accessed: 05-Jun-2025]

[11] Perera, S., Jin, X., Maurushat, A., & Opoku, D. J. (2022). Factors Affecting Reputational Damage to Organisations Due to Cyberattacks. *Informatics*, 9(1), 28. Available: https://www.mdpi.com/2227-9709/9/1/28 [Accessed: 05-Jun-2025]

[12] Australian Cyber Security Centre (ACSC), "Implementing Network Segmentation and Segregation," October 2021. Available: https://www.cyber.gov.au/sites/default/files/2023-03/PROTECT%20-%20Implementing%20Network%20Segmentation%20and%20Segregation%20%28October%202021%29.pdf [Accessed: 06-Jun-2025]