Tender Proposal for Northern Beaches Shopping Centre Network Infrastructure Upgrade

Prepared by:

Abrar Walid Ahmed
21 May 2025

Executive Summary

This report proposes a detailed plan for upgrading the Northern Beaches Shopping Centre's network infrastructure to enhance customer experience, improve connectivity, and secure sensitive data. The design includes robust wired and wireless networks, a detailed project implementation plan with budget and timeline, a comprehensive risk assessment, explicit security protocols, and adherence to ethical standards.

Table of Contents

1. LAN Design

Network Design

The LAN design satisfies the operational needs of both stores and customers across two floors. All the devices such as POS terminals, staff PCs, printers, and IP phones, use wired connections for speed and reliability. Wireless Access Points (WAPs) are strategically placed to ensure full wireless coverage for customers and mobile staff throughout the centre.

The layout includes 15 WAPs distributed between the ground and first floors, with one or more per section to ensure overlapping wireless signal coverage. Wired switches are placed near endpoint clusters, connected to a central Layer 3 router and firewall in the ground floor communications room.

A total of 7 VLANs are implemented to segment traffic based on department, device type, and purpose. Each VLAN uses a /24 subnet, allowing up to 254 devices, with room for future expansion.

Assumptions and Design Considerations

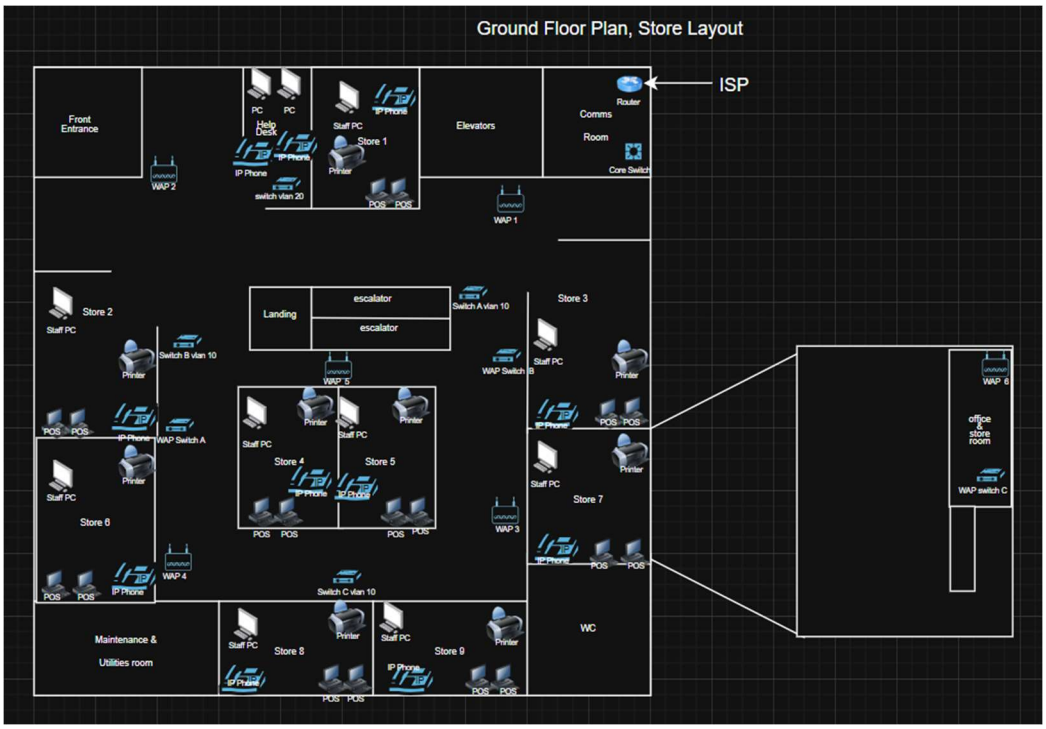
- All cabling is routed through the ceiling and structured via network cabinets on both floors.
- The Layer 3 router handles inter-VLAN routing.
- VLAN trunking is applied between the core switch and floor switches using IEEE 802.1Q tagging [3].
- Wireless clients connect through VLANs 50 (ground floor) and 70 (first floor).
- The network is designed to scale, with spare switch ports and IP address space available for future endpoints.

VLAN Segmentation

- VLAN 10 (Retail Stores): 192.168.10.0/24
- VLAN 20 (Help Desk): 192.168.20.0/24
- VLAN 30 (Office): 192.168.30.0/24
- VLAN 40 (Restaurants): 192.168.40.0/24
- VLAN 50 (Ground Wi-Fi): 192.168.50.0/24
- VLAN 60 (Department Store): 192.168.60.0/24
- VLAN 70 (First Floor Wi-Fi): 192.168.70.0/24

Hardware Placement and Configuration

- Layer 2 Switches: 15 × 24-port switches — 7 on the ground floor, 8 on the first floor, placed near clusters of wired endpoints.
- Core Switch and Router: Located in the ground floor comms room, it handles VLAN trunking, routing, and connection to the ISP via the firewall.
- Firewall: Located next to the router in the comms room, it provides perimeter protection and inter-VLAN access control.
- Wireless Access Points (WAPs): 15 total, ceiling-mounted throughout both floors to provide overlapping coverage.



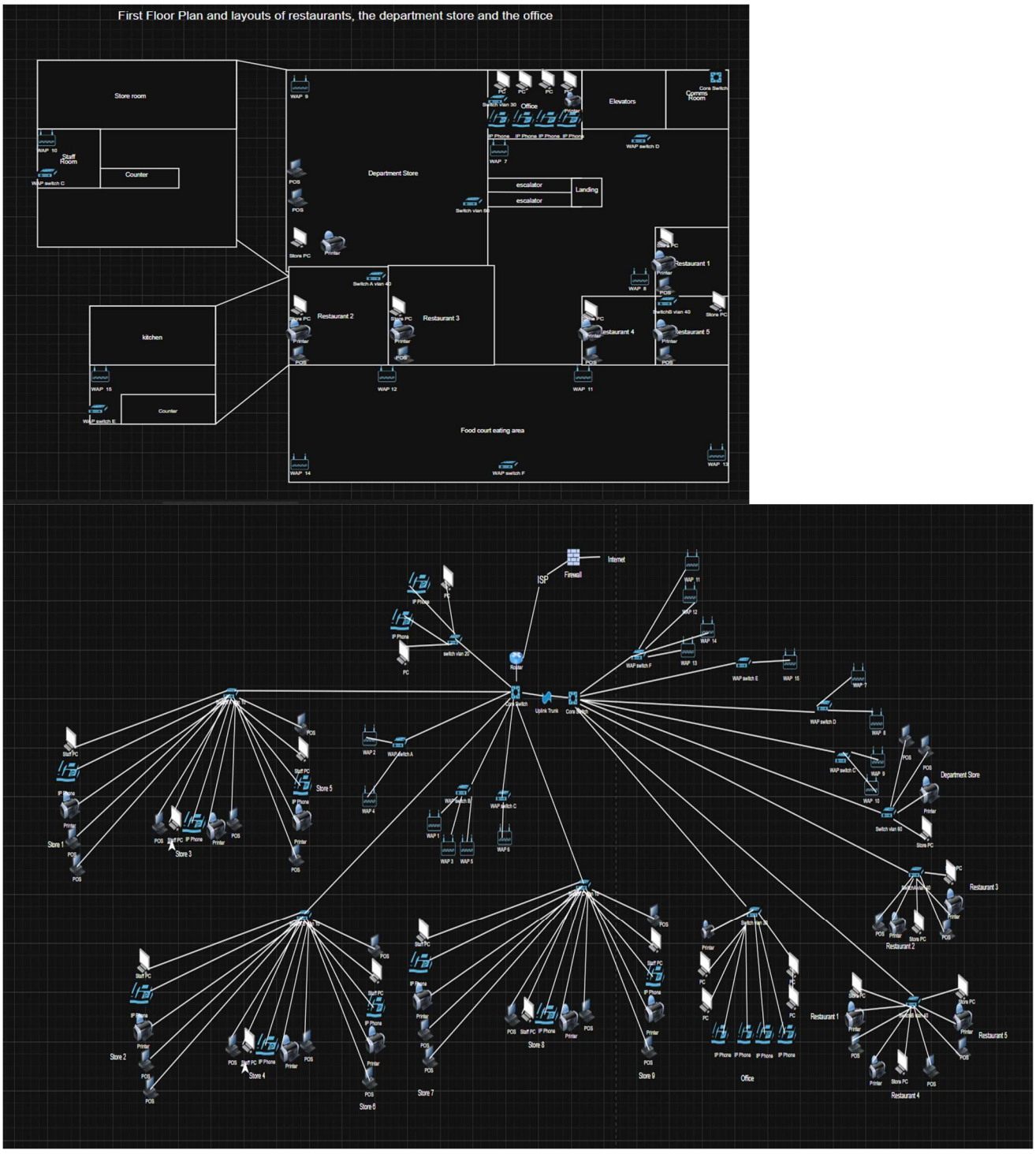


Diagram Overview

The attached diagrams illustrate the following:

- Ground Floor Layout: Shows 9 retail stores, help desk, and network endpoints connected via switches to a central comms room housing the router, core switch, and firewall.
- First Floor Layout: Includes a department store, 5 restaurants, office space, and a food court area with WAP coverage.

- WAPs have been implemented in less occupied places like staff room and office room as well, to ensure there is proper coverage throughout the whole place.

- Logical Network Diagram: Illustrates the full topology including all Layer 2/3 devices, endpoint connections, VLAN IDs, and IP subnets.

The diagram adheres to IEEE standards including IEEE 802.3 for Ethernet and IEEE 802.1Q for VLANs [2][3], and the segmentation aligns with data confidentiality and access control best practices.

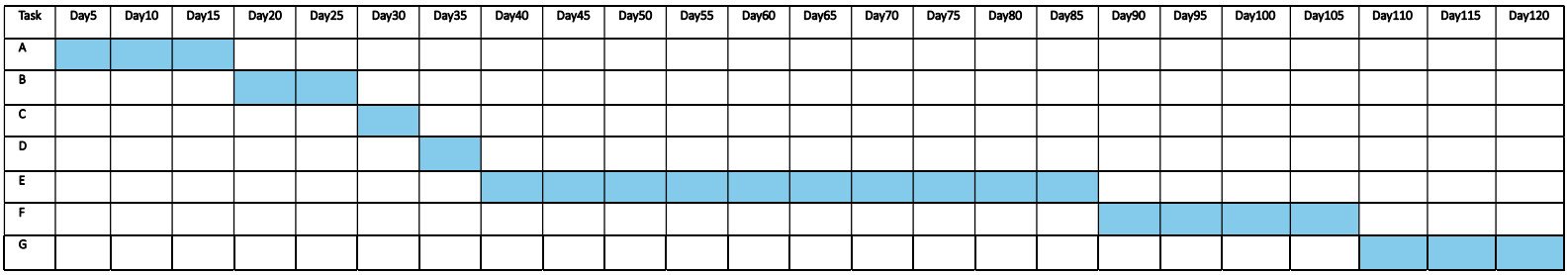
2.1 Project Management

Costing:

Item	Quantity	Unit Cost ($)	Total Cost ($)
Computers	**21**	**800**	**16,800**
IP Phone	**15**	**150**	**2,250**
Printer	**16**	**300**	**4,800**
POS	**25**	**1,000**	**25,000**
Switches(24-port)	**15**	**600**	**9,000**
WAPs	**15**	**400**	**6,000**
Core Switch	**2**	**3,000**	**6,000**
Router	**1**	**2,000**	**2,000**
Firewall	**1**	**2,500**	**2,500**
Uplink trunk	**1**	**300**	**300**
Cabling & Accessories	**3600**	**1/sqm**	**3600**
Labour (Installation & Testing)	**120**	**80/hour**	**9,600**
Total			**87,850**

- The total estimated cost for the LAN upgrade is $87,850. This includes all necessary hardware such as computers (21 units), POS systems (25 units), printers, IP phones, and networking equipment including 15 WAPs, 15 switches, a router, core switches, and a firewall. Additional costs cover structured cabling across 3,600 sqm and labour for installation and testing (120 hours). This budget ensures a fully operational, secure, and scalable network infrastructure for the shopping centre.

2.2 Timeline (Gantt Chart):



Start Date: 01/06/2025
End Date: 25/10/2025

	Task/Activity	Duration	Start Date	End Date
A.	Initial Planning & Procurement	2 weeks	01/06/2025	14/06/2025
B.	Parramatta Upgrade	9 days	15/06/2025	23/06/2025
C.	Lower North Shore Maintenance	5 days	24/06/2025	28/06/2025
D.	Bathurst Network Test/Upgrade	5 days	29/06/2025	03/07/2025
E.	Installation at Shopping Centre	7 weeks	04/07/2025	21/08/2025
F.	Network Configuration & Testing	3 weeks	22/08/2025	11/09/2025
G.	Final Review and Documentation	2 weeks	12/09/2025	25/10/2025

3. Risk Assessment

Asset (Priority)	Fire	Flood	Power Loss	Circuit Failure	Virus	External Intruder	Internal Intruder	Eavesdrop	Mitigation Strategies
POS Systems (90)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	VLAN isolation, encryption
WAPs (80)	Yes	Yes	Yes	Yes	No	Yes	No	Yes	WPA3, MAC filtering
Staff Computers (85)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Endpoint security, restricted access
IP Phones (70)	Yes	Yes	Yes	Yes	No	No	No	Yes	VoIP encryption, strong network access controls
Core Switch/Router (100)	Yes	Yes	Yes	Yes	No	Yes	Yes	No	UPS backup, firewall, physical security
Customer Wi-Fi (60)	Yes	Yes	Yes	No	No	Yes	No	Yes	Guest VLAN, bandwidth caps
Help Desk Staff (60)	No	No	No	No	No	Yes	Yes	No	Security awareness training, identity verification protocols
Customer Data (100)	No	No	No	No	Yes	Yes	Yes	Yes	AES encryption, access control lists (ACLs)
Network Config Files (90)	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Backup policies, restricted admin access
Office Computers (70)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	VLAN separation, endpoint detection & response

Asset Risk Management Justification

How Assets Were Prioritized Assets were prioritized based on three key criteria:

1)Operational Impact: Devices like POS systems, switches, and routers directly affect daily operations, transactions, and uptime. A failure in these areas can halt business operations, significantly affecting revenue [1].

2)Data Sensitivity: Customer data, employee records, and configuration files are high-value targets. Unauthorized access could violate data protection laws under the Australian Privacy Principles (APPs) [1].

3)Exposure: Public-facing systems such as WAPs and guest Wi-Fi are more susceptible to external threats like unauthorized access and denial-of-service attacks. These systems were evaluated using risk models supported by the ACSC [5].

Risk Identification

Referring to best practices outlined by the Australian Cyber Security Centre (ACSC), which provides guidance on common digital threats such as malware, phishing, and network abuse in public access environments [5].

Mapping the network's architecture to real-world incidents in similar retail and mall environments such as hardware damage from electrical surges or data leaks from unsegmented Wi-Fi networks and applying lessons learned to address them [5].

Mitigation Strategy Selection

Encryption and VLAN segmentation minimize unauthorized movement within the network and protect data in transit [3].

Access controls and firewalls enforce boundaries between network zones, restrict unnecessary exposure, and help ensure integrity [3].

Redundancy measures and UPS systems protect against physical threats like power loss and hardware failure, ensuring continued availability and aligning with IEEE's reliability-focused design principles [2], [3].

All strategies were selected based on their proven effectiveness, low overhead for administration, and ability to scale within the existing infrastructure and budget constraints [4].

4. Security and Privacy

The proposed LAN design fully meets the security and privacy requirements of the shopping centre's stores and operations. The LAN has been built with the CIA triad (Confidentiality, Integrity, and Availability) in mind, ensuring protection of sensitive sales, employee, and logistical data.

Key Design Features Ensuring Security and Privacy:

1.VLAN Segmentation

Each functional group is assigned a unique VLAN to restrict broadcast traffic and prevent lateral movement by attackers. Sensitive devices such as POS systems and staff computers are isolated from public Wi-Fi, following VLAN best practices as outlined in IEEE Std 802.1Q-2018 [3].

2.Firewall and Router Configuration

The firewall controls all traffic between VLANs and the internet, enforcing inter-VLAN security policies such as blocking guest VLAN access to internal servers, which helps uphold network segmentation as per IEEE network architecture guidelines [2].

3.Encryption of Communications

POS systems and IP phones use encrypted protocols, and WAPs are configured for WPA3 encryption to prevent unauthorized access. These encryption practices are consistent with recommendations in IEEE Std 802.3-2018 [2].

4.Access Control and User Authentication

MAC address filtering and multi-factor authentication are used on administrative systems. VLANs restrict device-to-device communication. These security principles align with the ACS Code of Professional Ethics on protecting client and organizational information [4].

5.Physical Security

All core networking equipment is stored in a locked comms room with limited access to minimize risk of tampering or hardware-based breaches [4].

6.Monitoring and Audit Trails

Firewall and switch logs are maintained and monitored to detect and respond to anomalies, forming a part of a continuous security monitoring strategy recommended by enterprise-grade standards [4].

7.Guest Access Controls

Customer Wi-Fi is isolated with VLANs, bandwidth limits, and content filtering, ensuring customer traffic does not interfere with business-critical operations [3].

Conclusion:

The current LAN design addresses all security and privacy concerns effectively and aligns with the Australian Privacy Principles (APPs) [1]. No amendments are required. The cost remains unchanged at $87,850.

5. Code of Ethics

As part of our submission, we have aligned this proposal with the ACS Code of Professional Ethics [4], ensuring that our approach to planning and delivering the LAN upgrade is both technically sound and ethically grounded. We draw attention to the following key ethical principles that will guide our implementation:

1. Honesty (Section 2.1, a–c)
   We are committed to being honest, open, and transparent in all interactions with the client and stakeholders. Our tender includes realistic cost estimates, hardware specifications, and timelines. "Not misrepresenting any action, situation, or capability" [4] ensures that we do not promise unrealistic outcomes, helping the shopping centre management make well-informed decisions.

2. Trustworthiness (Section 2.2, b–d)
   We take full responsibility for our work and are transparent about our team's capabilities. We will not accept tasks outside our expertise and will be proactive in updating the client on changes, constraints, or issues. For example, we use role-based access and data encryption to maintain the confidentiality of customer data, aligning with the principle to "respect the privacy, confidentiality and integrity of any personal or proprietary information" [4].

3. Respect for Others (Section 2.3.1, b–g)
   Our team promotes inclusivity and respect in all professional interactions. We design network systems that are accessible and non-discriminatory, and we mitigate harm by isolating guest Wi-Fi and applying firewall rules to protect sensitive business operations. This supports the principle of "developing mitigation strategies for unavoidable harm" and "respecting others' intellectual property" [4].

4. Respect for the Profession (Section 2.3.2, a–g)
   We contribute to improving ICT understanding by educating the client on system risks and best practices. We also participate in continuous professional development and sustainability practices (e.g., recommending energy-efficient hardware). This aligns with "endeavouring to educate the public about the benefits and drawbacks of ICT systems" and "contributing to advancing ICT systems for the greater good" [4].

   Our adherence to the ACS Code ensures that all stakeholders from retail managers to customers benefit from a LAN that is secure, trustworthy, and delivered by professionals who uphold integrity in both technical execution and ethical responsibility.

6. Conclusions and Recommendations

Our proposal presents a robust, secure, scalable LAN infrastructure, aligned with best practices, thorough risk management, and rigorous ethical standards. The network design ensures reliable operations, customer satisfaction, and futureproof capabilities.

Recommendations:

1. Approve the Tender Immediately:
   To meet the strict implementation window (June–October 2025), we recommend prompt approval to allow sufficient time for procurement, installation, and testing.

2. Adopt the Proposed VLAN and Security Structure:
   The segmented VLAN approach, supported by Layer 3 routing and firewall rules, provides strong isolation and security. We recommend its full implementation as proposed.

3. Maintain Scalability Considerations:
   Spare switch ports and address space should be preserved for future expansion. Any future store additions or renovations should consult the existing network plan for seamless integration.

4. Establish Ongoing Monitoring and Maintenance:
   We recommend scheduling regular network monitoring and equipment audits to ensure continued performance and security compliance.

5. Conduct Staff Training:
   IT staff and help desk operators should receive training on network usage policies, access control procedures, and basic troubleshooting to maximize operational efficiency.

7. References

[1] Office of the Australian Information Commissioner, *Australian Privacy Principles*, Australian Government, Mar. 2021. [Online]. Available: https://www.oaic.gov.au/privacy/australian-privacy-principles/.

[2] IEEE, *IEEE Standard for Ethernet*, IEEE Std 802.3-2018, Jun. 2018. [Online]. Available: https://standards.ieee.org/standard/802_3-2018.html.

[3] IEEE, *IEEE Standard for Local and Metropolitan Area Networks- Bridges and Bridged Networks (VLANs)*, IEEE Std 802.1Q-2018, Jul. 2018. [Online]. Available: https://standards.ieee.org/standard/802_1Q-2018.html.

[4] Australian Computer Society, *ACS Code of Professional Ethics*, Mar. 2023. [Online]. Available: https://www.acs.org.au/content/dam/acs/rules-and-regulations/ACS-Code-of-Professional-Ethics.pdf.

[5] Australian Cyber Security Centre, *Cyber Security Guidance for Small Businesses*, Australian Government. [Online]. Available: https://www.cyber.gov.au.