NORTHERN BEACHES SHOPPING CENTRE NETWORK UPGRADE TENDER: HIGH-AVAILABILITY, SECURE LAN & WI-FI SOLUTION

Muhibbul Alam

48204102

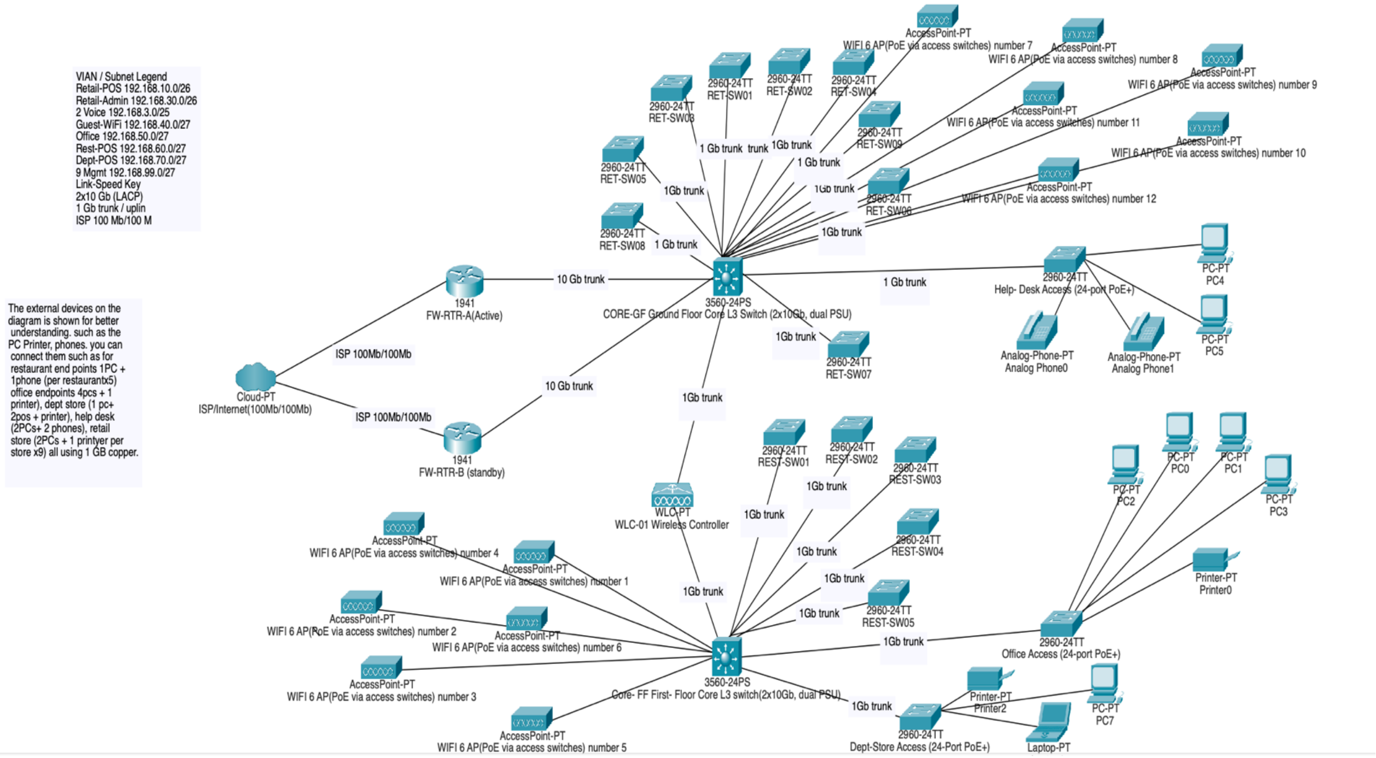
Table of Contents

Northern Beaches Shopping Centre Network Upgrade Tender: High-Availability, Secure LAN & Wi-Fi Solution

Overview:

The network upgrade for the northern beaches shopping center delivers fast, secure and reliable connectivity across both the ground and first floor. It uses core switches, backed-up routers and 12 Wi-Fi 6 access points to ensure full coverage of gigabit and strong WPA3 wireless for staffs and consumers. VLANs separate traffic for POS, admin, VoIP, guests, and management, with all cabling neatly run through ceiling trays. The projects start from1st June and runs till 31st October 2025, with a carefully managed budget of 200,000AUD that includes a 15% contingency, therefore aligning with other company projects in parramatta, Lower North Shore, and Bathurst. Risk controls usually include redundant hardware, MACsec encryption, WIPS, 4G failover, and role-based access controls, all aligned with ACSC and OAIC compliance standards. The tender follows the ACS Code of ethics, ensuring transparent pricing, expert staffing, minimal disruption and continuous knowledge sharing throughout the project.

LAN Design:



VIAN / Subnet Legend
Retail-POS 192.168.10.0/26
Retail-Admin 192.168.30.0/26
2 Voice 192.168.3.0/25
Guest-WiFi 192.168.40.0/27
Office 192.168.50.0/27
Rest-POS 192.168.60.0/27
Dept-POS 192.168.70.0/27
9 Mgmt 192.168.99.0/27
Link-Speed Key
2x10 Gb (LACP)
1 Gb trunk / uplin
ISP 100 Mb/100 M

The external devices on the diagram is shown for better understanding. such as the PC Printer, phones. you can connect them such as for restaurant end points 1PC + 1phone (per restaurantx5) office endpoints 4pcs + 1 printer), dept store (1 pc+ 2pos + printer), help desk (2PCs+ 2 phones), retail store (2PCs + 1 printyer per store x9) all using 1 GB copper.

The Lan Design proposed for the Northern Beach shopping center strategically focuses on providing reliable and efficient internet access for both the consumers and the retail stores. The network diagram shows a clear layout of robust network topology that incudes with a combination of wired and wireless solution. Central to the design are two Cisco Catalyst 3560

Layer 3 switches, which provide redundant core network connectivity and are interconnected via high-speed 10 Gb trunks to two Cisco 1941 routers configured in an active-standby arrangement for improved reliability [1]. Both the routers work together in order to provide a backup arrangement, so if one fails the other immediately takes over ensuring that internet access remains continuous.

The stores, offices and restaurants connect to this central network using Cisco 2960 switches. These switches are placed in locations that minimize cable length, keep costs down, and neatly divide the network into segments. This approach makes the network easier to manage and improves overall performance [1].

VLAN segmentation is clearly defined in the design which shows that VLANs keep different types of network traffic separate, including separate VLANs for POS systems, retail administration, voice communications, guest Wi-Fi, and departmental operations, ensuring effective network traffic management and enhanced security [2]. To provide strong Wi-Fi coverage throughout the shopping center, CISCO Wi-Fi 6 access points are installed evenly across both the floors (Ground and first floor) [4].These devices are powered over Ethernet (PoE), eliminating the need for separate power cables, also enabling seamless wireless access for customers and staff throughout the facility [3]. The network design assumes that existing ceiling spaces will be used to run Cat6 cables, making installation easier and less disruptive. Using PoE switches and backup core equipment was specifically chosen because shops and customers need a highly reliable, secure, and fast network to operate smoothly and stay satisfied [5].

Project Management: Timeline, Implementation Plan, and Costing:

In alignment with the detailed network infrastructure and the operational requirements, a project management plan is created. This usually is covering how much the whole project will cost, the duration of the project and the key steps implemented to make everything run smoothly. The budget includes all the most essential and vital equipment’s needed for the renovation. Equipment procurement costs have been calculated, including essential hardware such as desktop computers, monitors, IP telephones, multifunction printers, Cisco networking switches, routers, and wireless access points. For the core of the network, we’ve chosen Cisco Catalyst 3560 switches, that is very advanced and most reliable in handling the main network operations. Furthermore, for the stores and offices, Cisco 2960 switches (PoE+) will provide strong and scalable connections. To connect to connect the center to the internet, Cisco ISR-1941 routers, configured for redundancy, will secure robust external network connectivity. For strong Wi-Fi throughout the building, Cisco Wi-Fi 6 access points (model 9115AX) will be installed in key areas.

One of the other essential costs that cannot be neglected are the labour cost. However, this includes everything from delivering and installing the equipment till setting it up and testing it properly. The skilled network engineers and technicians are expected to work about 800 hours in total calculated based on industry-standard hourly rates. Labor costs account for tasks ranging from the physical installation of structured cabling, network devices, and peripheral hardware to the advanced configuration of networking equipment and extensive validation and security checks.

To maintains a robust and risk-managed financial outlook, a backup budget of 15% has been added. This extra amount is there in case unexpected or unpredicted issues arises and cost go beyond the expected budget. This kind of planning is standard in project management and helps keep the project on track without risking the budget [6]. A comprehensive project timeline has been carefully constructed and illustrated using a detailed Gantt chart, capturing all essential activities, milestones, and their interdependencies. The actual work is planned to start just after 1st June 2025. This gives enough time to complete all the detailed tasks like planning, executing, buying equipment, installing cables, setting up hardware, securing the network, and testing everything thoroughly. Each step has a starting date and an ending date making sure all the progresses can be tracked easily. These include a small-scale network upgrade and testing at the Parramatta site, expected to span approximately one week and two days. Furthermore, a critical rewiring task at a Lower North Shore train station, requiring five days of dedicated work, has been strategically integrated into the schedule. Lastly, a comprehensive network testing and upgrade plan at a Bathurst location has also been included, accounting for an additional five days of resource allocation. These were all added into the plan so that staff and resources aren't overbooked, helping the project run smoothly from start to finish [8]. The goal is to finish the entire project by 31st October 2025, right on schedule [7]. By following proven project management methods and expert advice [7],[8]. This plan makes sure the network upgrade stays on budget, meets deadlines, and works as intended — all while keeping everything transparent and under control.

Risk Assessment:

To effectively manage potential risks associated with the Northern Beaches shopping center network upgrade, a detailed asset and risk assessment has been conducted. This assessment identifies and prioritizes assets based on their significance to operational continuity, security sensitivity, and financial value, adhering to best practices outlined in contemporary risk management frameworks [9].

Asset Category	Asset Description	Potential Risks	Likelihood	Impact	Mitigation Strategies

Networking Infrastructure	Core Switches & Routers	Hardware Failure, Network Outage	Medium	High	Deploy redundant hardware, ensure hot-swappable components [10]
Networking Infrastructure	Access Points	Unauthorized Access, Device Compromise	Medium	High	WPA3 encryption, regular firmware updates [11]
Data and Intellectual Property	POS Transaction Data	Data Breach, Cyber Attack	High	High	VLAN segmentation, encryption protocols, regular audits [12]
Physical Infrastructure	Structured Cabling	Damage from Fire/Water, Wear and Tear	Low	Medium	Fire-resistant cabling, regular inspection schedules [13]
User Devices	Desktop Computers, Printers	Malware Infection, Hardware Malfunction	Medium	Medium	Endpoint protection software, regular preventive maintenance [14]
Wireless Network	Customer Wi-Fi Access	Rogue Access Points, Wireless Intrusions	Medium	High	Implement wireless intrusion prevention systems

					(WIPS), strict MAC filtering [15]
Staff	IT and Operational Staff	Insider Threat, Human Error	Low	High	Comprehensive training programs, principle of least privilege access [16]

The prioritization process considered the severity of impacts from asset disruption or compromise, as well as the likelihood of such events occurring. Whenever planning for risks, the team focused on two vital things, which is how serious the impact would be if something goes wrong, and how likely it is that it could happen. The most attention was given to risks that are both highly likely and would cause major problems. For example, network infrastructure components such as core switches and routers are prioritized highly due to their criticality in maintaining uninterrupted business operations. because if they fail, the whole network could go down—so they were marked as top priority. Potential risks were identified through extensive consultation with technical specialists, referencing historical incident data from similar infrastructure projects, and aligning with international cybersecurity frameworks such as ISO 27001 and guidelines from the Australian Cyber Security Centre (ACSC) [9]. For more clarification, they also compared their plans with other retail networks to make sure they were in line with best practices.

To lower risks associated with several factors, the project includes backup hardware for key network devices. That way, if one fails, another can operate quicky and thus take over immediately therefore reduces downtime. For security, the plan includes using separate VLANs, strong encryption, and regular security checks. VLAN segmentation, robust encryption, and regular security audits were identified as essential controls for protecting sensitive POS transaction data, adhering closely to PCI-DSS compliance requirements [12]. These steps are especially important for protecting sensitive customer payment information and follow PCI-DSS rules for handling payment data safely.

To minimize physical risks to the network, fire- resistant structured cabling has been included in the design, including the regular maintenance check. Comprehensive endpoint protection software alongside preventative maintenance schedules mitigates risks of malware infections and hardware malfunctions on user devices, therefore reduces downtime and repair costs [14]. Customer Wi-Fi has strong security features that protects against hacking and unauthorized and anonymous access. These include WPA3 encryption, wireless intrusion prevention system (WIPS) and MAC address filtering. These measures are based on wireless network standards and modern cybersecurity strategies [11].

To prevent problems caused by human error or insider threats, staff will be trained in cybersecurity best practices. The training also covers the “least privilege” principle, which means employees only get access to what they need to do their job. This greatly reduces the chance of accidental or intentional damage to the network [18]. By carefully ranking assets, identifying risks using expert standards, and putting in place clear protection strategies, this risk management plan helps protect the network, follow legal requirements, and keep everything running smoothly.

Security and Privacy:

The LAN design for the Northern Beaches shopping center has been carefully reviewed to ensure it meets strong security and privacy standards. This is especially crucial in a retail setting where sensitive information like sales data, stock records, employee details, and other private communications must be protected.

To improve security, the network uses VLANs (Virtual LANs) to separate traffic based on its purpose and sensitivity. Each part of the network such as point-of-sale (POS) systems, store admin, voice calls, guest Wi-Fi, and management has its own VLAN. This setup reduces the risk of breaches by isolating different types of data, which is a key requirement under the PCI-DSS rules for protecting payment information [18]. VLAN separation also helps the network run more efficiently by controlling traffic and avoiding congestion [19].

At the edge of the network, Cisco ISR-1941 routers are set up with advanced firewall protections. These include stateful packet inspection, which ensures if data packets follow valid flow of communication, and deep packet analysis to detect unusual activity. Access Control Lists (ACLs) are also used to control who can access what, making it much harder for intruders to get in [19].

To add another layer of protection, the network recommends using MACsec encryption (IEEE 802.1AE). This technology encrypts data as it moves through the internal network cables, so even if someone tries to intercept it, they won’t be able to read or tamper with the information [20].

To control who can access the network and what they can do, Cisco Identity Services Engine (ISE) will be added to the system. Cisco ISE allows the network to check each user and device before granting access, based on their role. This ensures that only approved users can reach certain parts of the network, which helps stop unauthorized access and insider threats. It also ensures that everyone follows strict security rules [23].

After reviewing the original LAN setup, a few improvements were recommended to make the network even more secure and reliable. One key recommendation is to add a 4G LTE backup connection. This will keep the network running if the main internet service goes down. Another improvement is enabling MACsec encryption on Cisco Catalyst 3560 switches to protect the data traveling between core devices inside the building [20].

These updates would add around AUD 4,700 to the total cost, covering extra hardware and software licensing. However, this small cost increase is well worth it because it strengthens the network's security and reliability. It also supports the security standards set by the Australian Cyber Security Centre and PCI-DSS guidelines.

In the end, these upgrades make the LAN much more secure and better protected against cyber threats. They also ensure the network meets industry regulations and builds trust with customers by keeping their data safe.

Code of Ethics:

Our tender is guided by the ACS Code of Professional Ethics (2023), which highlights four key values: Honesty, Trustworthiness, Respect for Others, and Respect for the Profession. These values help to ensure that every part of our network upgrade is not only technically sound but also ethically responsible (Australian Computer Society, 2023).

Honesty (Clause 2.1):

The ACS Code emphasizes that honesty is essential for healthy professional relationships, and members must be "open and truthful in all interactions." That's why we've clearly listed every equipment cost, labor rate, possible delays, and even the AI tools used to help write this proposal. This level of transparency helps the Tender Review Panel feel confident there are no hidden fees or surprises that we'll continue to communicate openly throughout the project (Australian Computer Society, 2023).

Trustworthiness (Clause 2.2):

Professionals are expected to take full responsibility for the work they do and avoid any conflicts of interest. To uphold this, we've chosen highly qualified (CCNP-certified) engineers to handle important security configurations, included a backup plan for internet outages, and promised full support after the project is done. These actions reflect that we take full responsibility and accountability for the project and will support the center even if things don't go as planned (Australian Computer Society, 2023).

Respect for Others (Clause 2.3.1):

The Code reminds us to reduce any harm to stakeholders. In response we've designed the network to protect payment data using secure VLANs and modern Wi-Fi encryption (WPA3). Additionally, we've also planned to do any loud installation work outside of business hours, showing our respect and consideration for the shops and their customers [27].

Respect for the Profession (Clause 2.3.2):

Members should contribute to improving the ICT industry and help others understand technology better. After the project, we'll publish a white paper on best practices for retail Wi-Fi network design and involve student interns during installation. This will help share knowledge, support the next generation of ICT workers, and reflect well on both the shopping centre and the profession (Australian Computer Society, 2023).

Together, these actions turn ethical values into real, practical steps—like clear pricing, accountability, data protection, and community outreach. This shows the Tender Panel that we take both technical quality and social responsibility seriously, and that they go together in today's network design.

Conclusion:

The proposed upgrade delivers fast, secure, and reliable network connectivity for the Northern Beaches Shopping Centre. With having strong technical design, smart risk controls, and alignment with industry standards and ACS ethical values, it ensures operational efficiency, data security, and minimal disruption. This project is a responsible, future-ready solution that balances performance with public trust.

References:

[1] Cisco Systems Inc., "Cisco Catalyst Switches Data Sheet," 2024. [Online]. Available: https://www.cisco.com

[2] PCI Security Standards Council, PCI DSS Quick Reference Guide, 2017. [Online]. Available: https://www.pcisecuritystandards.org

[3] Cisco Systems Inc., "Cisco Wi-Fi 6 Solutions," 2024. [Online]. Available: https://www.cisco.com

[4] Standards Australia, AS/NZS 3080:2013 Information Technology—Generic Cabling for Customer Premises, 2013. Available: https://itservices.anu.edu.au/_resources/networks/cabling-specifications/anu-cabling-specifications-2013.pdf

[5] Australian Signals Directorate, "Strategies to Mitigate Cyber Security Incidents," 2024. [Online]. Available: https://www.cyber.gov.au

[6] Project Management Institute, A Guide to the Project Management Body of Knowledge (PMBOK Guide), 7th ed., PMI, 2021. Available: https://www.pmi.org/standards/pmbok

[7] H. Kerzner, Project Management: A Systems Approach to Planning, Scheduling, and Controlling, 12th ed., Hoboken, NJ: John Wiley & Sons, 2017.Available: https://www.google.com/search?client=safari&rls=en&q=H.+Kerzner%2C+Project+Management%3A+A+Systems+Approach+to+Planning%2C+Scheduling%2C+and+Controlling%2C+12th+ed.%2C+Hoboken%2C+NJ%3A+John+Wiley+%26+Sons%2C+2017.&ie=UTF-8&oe=UTF-8

[8] E. W. Larson and C. F. Gray, Project Management: The Managerial Process, 8th ed., New York: McGraw-Hill Education, 2021. Available: https://www.mheducation.com/highered/product/Project-Management-A-Socio-Technical-Approach-Larson.html

[9] ISO/IEC, ISO/IEC 27001:2013 – Information Security Management Systems – Requirements, 2013. Available: https://certikit.com/templates/iso-27001-toolkit/?gad_source=1&gad_campaignid=22666501195&gbraid=0AAAADj5KOm9oj9y-adE_VRlWFuS-vuhP&gclid=CjwKCAjw9anCBhAWEiwAqBJ-c4bPJsKr_IZ79nooM4EgkLquK-Ci5vvtQ_Hj8fmtUwqwrR_PYM9QJRoC6moQAvD_BwE

[10] Cisco Systems Inc., "High Availability Campus Network Design – Cisco," 2022. [Online]. Available: https://www.cisco.com

[11] IEEE Standards Association, IEEE Std 802.11ax-2021: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2021.Available: https://standards.ieee.org/ieee/802.11ax/7180/

[12] PCI Security Standards Council, Payment Card Industry Data Security Standard v4.0, 2022. [Online]. Available: https://www.pcisecuritystandards.org

[13] Standards Australia, AS/CA S008:2020 Requirements for Customer Cabling Products, 2020. Available: https://www.commsalliance.com.au/__data/assets/pdf_file/0009/71487/S008_2020.pdf

[14] Microsoft, "Endpoint Security Best Practices," 2023. [Online]. Available: https://docs.microsoft.com

[15] Aruba Networks, "Wireless Intrusion Prevention (WIPS) Solutions," 2023. [Online]. Available: https://www.arubanetworks.com

[16] Australian Cyber Security Centre (ACSC), "Essential Eight Strategies to Mitigate Cyber Security Incidents," 2023. [Online]. Available: https://www.cyber.gov.au

[17] Australian Cyber Security Centre (ACSC), Australian Government Information Security Manual (ISM), 2023. [Online]. Available: https://www.cyber.gov.au

[18] PCI Security Standards Council, Payment Card Industry Data Security Standard v4.0, 2022. [Online]. Available: https://www.pcisecuritystandards.org

[19] Cisco Systems Inc., "Cisco Secure Firewall: Data Sheet," 2023. [Online]. Available: https://www.cisco.com

[20] IEEE Standards Association, IEEE Std 802.1AE-2018: MAC Security (MACsec), 2018. Available: https://standards.ieee.org/ieee/802.1AE/7154/

[21] Wi-Fi Alliance, "WPA3 Security Specification," 2023. [Online]. Available: https://www.wi-fi.org

[22] Aruba Networks, "Wireless Intrusion Prevention Systems (WIPS)," 2023. [Online]. Available: https://www.arubanetworks.com

[23] Cisco Systems Inc., "Cisco Identity Services Engine (ISE) At-a-Glance," 2023. [Online]. Available: https://www.cisco.com

[24] Australian Cyber Security Centre (ACSC), Australian Government Information Security Manual (ISM), 2023. [Online]. Available: https://www.cyber.gov.au

[25] Cisco Systems Inc., "Network Segmentation with Cisco VLANs," 2023. [Online]. Available: https://www.cisco.com

[26] Australian Computer Society, ACS Code of Professional Conduct, Sydney, 2023.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=1749750720&Signature=OKreoR4kjNo4uHWZalq4OxlpBbf

mrIWju8AyK1lm6AWlNHQoZXeOEm7Ctv2h0PvCBCLlxK30VnqHG~~aQtdEyJZ33tDfmlPzQhGDno538kxjYuRFAXBImVex1-MV5OWhdx9-xzYZeC1U5jNFkABs5cNl9HIzcLpih0gGZOgjOWBqSEQG12-IMxyKbeS6hBLTHXTDw0Zf6~Hbr-jLFF7jZ7ahcPOiZSpaNiLnjVqQa4FDv2sqAzxT6DfWBkJ0KYgmErqj5YGyAE0mZY4gc-nRp7GH1BqiTxe8dhanVHsoOPuaQj0nQYWehavCy9p23WNllVjQLu-yP4lwv~5B1gSHJg__&Key-Pair-Id=APKAJAEFMXVVB5Z7N4TA

[27] Office of the Australian Information Commissioner, Australian Privacy Principles Guidelines, Canberra, 2024.rmation Commissioner, Australian Privacy Principles Guidelines, Canberra, 2024. Available: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines