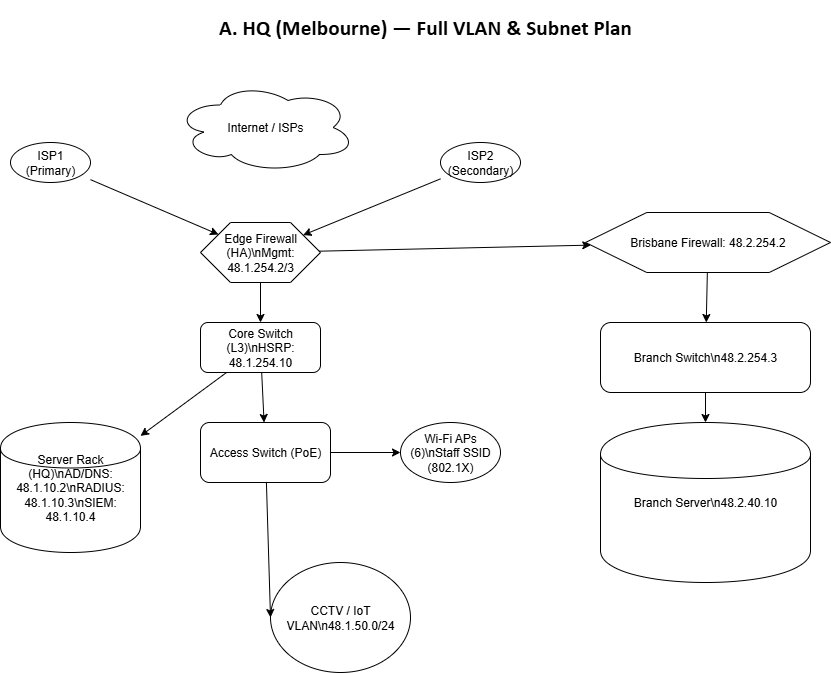
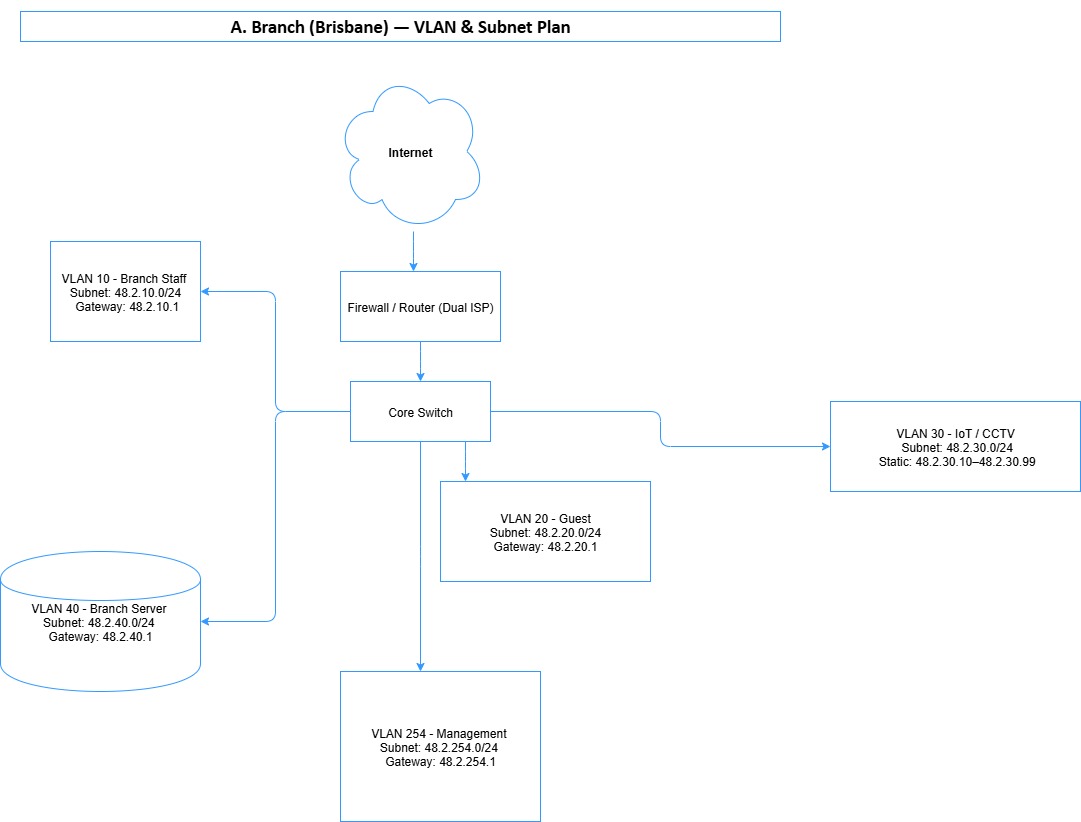
# Assumptions

To this project I have assumed that Truelec’s headquarters is in Melbourne, Victoria, because that is the campus I attend. The company maintains three main branch offices in Brisbane, Perth and Hobart. The new headquarters will accommodate approximately 70 staff members including administrative, ICT, marketing and senior leadership teams. The Brisbane branch, which I have chosen as the sample branch for network design, has 20 staff consisting of electricians, site supervisors and support personnel. In accordance with the project requirements, all IPv4 addresses used in my design begin with the first octet “78”, which corresponds to the last two digits of my student ID.

* Headquarters: Melbourne, VIC.
* Branch offices Brisbane (sample), Perth, Hobart.
* Numbers of staff: Brisbane = 20 staff, HQ = 70 staff.
* The first octet of all IPv4 addresses in this design contains the final two digits of student IDs - so: 48 -x.x.x.x and 55 -x.x.x.x. The two ranges can be illustrated, in this document, the 48.x.x.x scheme is illustrated.
* WAN: to provide some resilience, each location will have dual-ISP connectivity (primary fibre/copper + secondary 4G or DSL).
* Cloud: it will migrate three HQ servers + one server per branch to cloud VMs (costing / provider analysis done separately).
* Security: Staff Wi-Fi: RADIUS (802.1X); centralised logging: SIEM, application access: RBAC.
* Budget: small and medium-range hardware is focused on (Ubiquiti / Fortinet alternatives).

# High level logical design

****

****

# VLAN & Subnet Plan (IPv4 addressing)

A VLAN is a mechanism of splitting a physical network into more than one logical network. The equipments of varying switches within a VLAN may still interact with one another as though within a single network. VLAN enhances the security status, traffic control and organization of the network by evolving units such as staff, guest and internet of things into segments. The subnetting is where a large IP network is subdivided and the small manageable network is known as subnet. Each subnet has an IP address pool whose range is determined by a subnet mask which identifies what addresses are in the subnet. The subnetting enhances efficiency of the network, security and congestion by governing the flow of intercommunication in the network.

## HQ (Melbourne) Full VLAN & Subnet Plan

| **VLAN ID** | **VLAN Name** | **Subnet (CIDR)** | **Gateway IP** | **DHCP Range (recommended)** |
| --- | --- | --- | --- | --- |
| 10 | HQ Servers | 48.1.10.0/24 | 48.1.10.1 | 48.1.10.100 – 48.1.10.200 |
| 20 | HQ Staff | 48.1.20.0/24 | 48.1.20.1 | 48.1.20.100 – 48.1.20.250 |
| 30 | HQ Admin | 48.1.30.0/24 | 48.1.30.1 | 48.1.30.100 – 48.1.30.150 |
| 40 | HQ Guest | 48.1.40.0/24 | 48.1.40.1 | 48.1.40.100 – 48.1.40.250 |
| 50 | HQ IoT/CCTV | 48.1.50.0/24 | 48.1.50.1 | Prefer static camera IPs 48.1.50.10 – 48.1.50.99 |
| 60 | HQ Printers | 48.1.60.0/24 | 48.1.60.1 | 48.1.60.100 – 48.1.60.200 |
| 100 | VPN / Remote | 48.1.100.0/24 | 48.1.100.1 | 48.1.100.100 – 48.1.100.200 |
| 254 | Management (OOB) | 48.1.254.0/24 | 48.1.254.1 | 48.1.254.10 – 48.1.254.50 |

## Branch (Brisbane) VLAN & Subnet Plan

| **VLAN ID** | **VLAN Name** | **Subnet (CIDR)** | **Gateway IP** | **DHCP Range** |
| --- | --- | --- | --- | --- |
| 10 | Branch Staff | 48.2.10.0/24 | 48.2.10.1 | 48.2.10.100 – 48.2.10.250 |
| 20 | Guest | 48.2.20.0/24 | 48.2.20.1 | 48.2.20.100 – 48.2.20.250 |
| 30 | Branch IoT/CCTV | 48.2.30.0/24 | 48.2.30.1 | Static cameras 48.2.30.10 – 48.2.30.99 |
| 40 | Branch Server (local) | 48.2.40.0/24 | 48.2.40.1 | 48.2.40.100 – 48.2.40.200 |
| 254 | Management | 48.2.254.0/24 | 48.2.254.1 | 48.2.254.10 – 48.2.254.40 |

# Wifi Design

* **Modern security: Design:**

**SSIDs:**

* Truelec-Staff - WPA2/WPA3 Enterprise (802.1X with RADIUS), VLAN: Servers/Staff VLAN.
* Truelec-Guest - WPA2-Personal or open + captive portal, VLAN: Guest VLAN (cached DNS + HTTPs restrictions).
* Truelec-IoT - WPA2 PSK or independent command of IoT, VLAN: IoT VLAN (can not connect with inner servers).
* **Authentication**: PEAP or EAP-TLS, supported by any of the following: Microsoft AD + Network Policy Server or dedicated RADIUS(FreeRADIUS/Azure AD NPS extension). If you can issue certs (more secure) then prefer EAP-TLS strongly.
* **Encryption:** WPA3 where available, otherwise where AP/client mix prohibits full WPA3, WPA2/WPA3 transition mode.
* **Channel & Power plan:**
* Limit legacy devices to 2.4GHz: reduce channel overlap (channels 1/6/11).
* Capacity (DFS channel allowable with AP).
* Use site survey: Power set: Conserve on first setting of power and adjust where required.
* Band steering: steering on (prefer 5GHz on clients with 5GHz capability).
* AP density:
* HQ (this serves the purpose only of managing size extended across the organization): 6 APs (approximately) - estimate 1 AP every 10-15 employees based on size of the floor area. Use 802.11ac/ax APs.
* Branch (20 staff): 2 APs (a floor/a area) - revise post topography survey.
* RADIUS retries/timeout: default = 5s tmeout, 3 retries (fine tune)