3. Hardware Requirements

3.1 Overview

Two newly constructed buildings can support secure, scalable, and high-performance connectivity. The proposed solution must accommodate the technological demands of both administrative and academic functions while preparing for future growth over the next five years. As detailed in the BDCN solution document, the network design follows a three-tier architecture—Core, Distribution, and Access layers—combined with modern technologies such as SD-WAN, Wi-Fi 6E, and VLAN segmentation. Each layer requires specific hardware to meet the performance, security, and redundancy expectations of a modern educational institution (Murad et al., 2024).

The decisions are based on a combination of real-world requirements: user density (up to 1,000 students across two buildings), floor layouts, lab/classroom distribution, and the need for seamless connectivity between buildings and the wider university network.

The proposed hardware ensures:

- **High bandwidth and low-latency communication** between users and services
- **Scalable wired and wireless access** for dense academic environments
- **Robust security** at the perimeter and internal network levels
- **Redundancy and reliability** through failover-ready components
- **Support for cloud integration, remote access, and future technologies**

The subsequent sections will break down each category of hardware, from core infrastructure to access layer devices and edge technologies, explaining both technical function and strategic justification.

3.2 Core Network Devices

The core network layer serves as the backbone of the entire network infrastructure, enabling high-speed interconnectivity between buildings, floors, and external networks such as the main university campus and the internet. As outlined in the BDCN solution, the core layer is responsible for ensuring **high availability, minimal latency, and efficient routing** between key network segments.

3.2.1 Core Routers

Abu, Chowdhury and Jang (2023) two high-capacity core routers are proposed to serve as the central nodes connecting the new buildings to the rest of the university's network and to external

internet services. These routers will also manage traffic between SD-WAN edge devices and the local network, providing dynamic path selection and failover support.

- **Function:** Direct high-volume inter-campus traffic, support site-to-site VPNs, and integrate SD-WAN overlays.

- **Justification:** Redundancy is essential at this layer to ensure uninterrupted connectivity in case of hardware failure or maintenance. Deploying two routers in an active-passive setup enhances resilience and supports future bandwidth demands from growing student and staff populations (Hassan, Gregory and Li, 2023).

- **Specification & Cost (from BDCN):**
    - Quantity: 2
    - Estimated Unit Cost: £6,000
    - Total: £12,000

The selected routers must support advanced routing protocols (e.g., OSPF, BGP), SD-WAN integration, and security features such as Access Control Lists (ACLs) and IPsec.

Figure 3.1 Enterprise Core Router (SD-WAN Integrated)

Source: Cisco page

3.2.2 Core Switches

Four Layer 3 core switches will be deployed to manage internal routing between distribution layers and to enable high-speed communication between buildings. These switches will form the backbone for both wired and wireless infrastructure, allowing for efficient VLAN segmentation and traffic prioritisation.

- **Function:** Facilitate intra-campus data flow, inter-VLAN routing, and connect major network nodes (e.g., firewalls, distribution switches, SD-WAN devices).
- **Justification:** With six floors and a high density of users across two buildings, the network requires core switches with a minimum of 10Gbps throughput and support for

virtualization and stacking. Four switches allow for redundancy and load balancing, reducing single points of failure and providing room for scaling.

- **Specification & Cost (from BDCN):**
    - Quantity: 4
    - Estimated Unit Cost: £6,000
    - Total: £24,000

These devices must support QoS (Quality of Service) for traffic prioritisation (e.g., VoIP), advanced security features, and integration with cloud-based management platforms like Cisco DNA Center.

Figure 3.2 Layer *3 Core Switch (10Gbps Backbone)*

Source: Cisco page

3.3 Distribution and Access Layer Hardware

The distribution and access layers of the network architecture bridge end-user devices with the core infrastructure. These layers are critical for maintaining performance, managing traffic, and enforcing security policies across different floors, departments, and user groups. Based on the hierarchical network design proposed in the BDCN solution, this section outlines the required

hardware for providing both wired and wireless connectivity across all functional areas within the two new university buildings.

3.3.1 Access Switches

Twenty managed Layer 2 access switches will be deployed across the two buildings to connect end-user devices such as desktop PCs, IP phones, printers, and wireless access points. These switches will be located on each floor, primarily in IT cabinets, and will serve classrooms, labs, administrative offices, and social spaces.

- **Function:** Deliver Ethernet connectivity to endpoint devices and serve as the gateway for VLAN-segmented network traffic.

- **Justification:** The access layer must support high device density, PoE+ (Power over Ethernet) for wireless access points and VoIP phones, and robust VLAN configuration capabilities. With 12 classrooms, 8 labs, and multiple offices per building, 20 switches provide adequate port availability and allow for future expansion. The selection also accounts for redundancy, load distribution, and the ability to support a minimum of 1Gbps per port with uplinks to the distribution layer at 10Gbps.

- **Specification & Cost (from BDCN):**
    - Quantity: 20
    - Estimated Unit Cost: £2,000
    - Total: £40,000

The switches must support SNMP, port mirroring for diagnostics, and integration with cloud-based monitoring tools such as Cisco DNA Center.

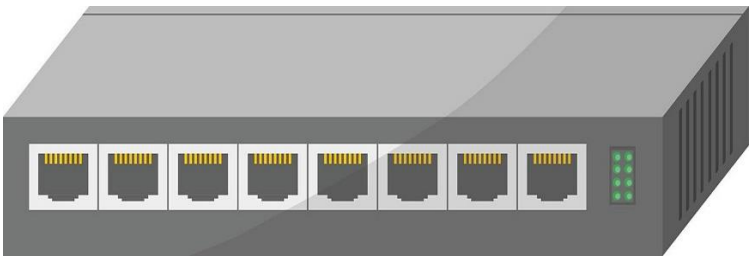

Figure 3.3 Managed Layer 2 Access Switch (PoE+ Enabled)

Source: Cisco page

3.3.2 Wi-Fi 6E Access Points

Forty enterprise-grade Wi-Fi 6E access points will be deployed across the two buildings to ensure comprehensive wireless coverage and support high user concurrency in dense environments. These will be installed in classrooms, labs, lecture halls, administrative spaces, and common rooms.

- **Function:** Provide wireless access for mobile devices, laptops, and IoT devices, supporting seamless roaming and high-throughput applications.

- **Justification:** Each building supports up to 500 students, plus academic and administrative staff, many of whom will be simultaneously connected to the network. Wi-Fi 6E provides better spectral efficiency, lower latency, and increased capacity over previous standards, making it ideal for classrooms and labs that may host bandwidth-intensive activities such as streaming, video conferencing, and cloud-based lab environments. Deploying 40 access points ensures high-density coverage with proper overlap and minimal dead zones.

- **Specification & Cost (from BDCN):**
    - Quantity: 40
    - Estimated Unit Cost: £1,500
    - Total: £60,000

These devices must support WPA3 encryption, dynamic bandwidth management, and centralised control through a cloud-based dashboard.

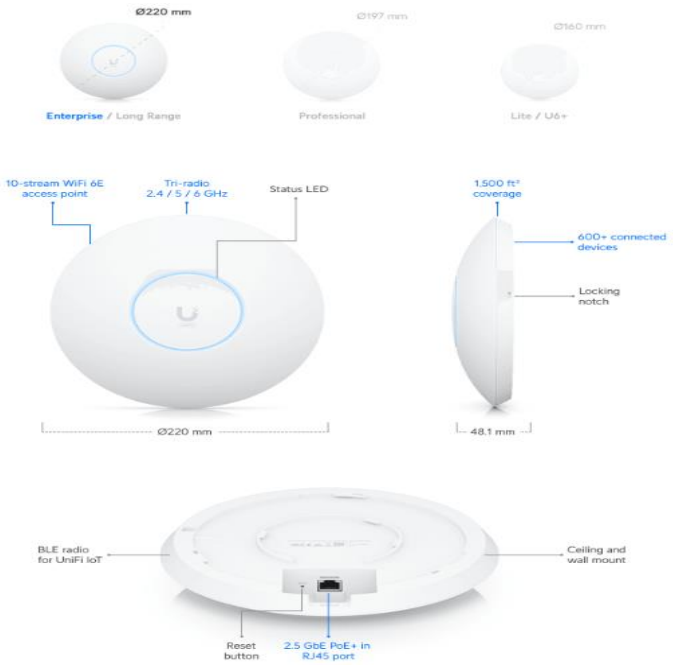

Figure 3.4 Wi-Fi 6E Enterprise Access Point

Source: Google

3.4 Network Security Hardware

In a modern academic network environment, robust perimeter and internal security is essential to protect sensitive institutional data, ensure regulatory compliance, and safeguard users against cyber threats. The proposed network incorporates multiple layers of defense, with enterprise firewalls playing a central role in network segmentation, threat prevention, and policy enforcement.

3.4.1 Firewalls

Four enterprise-grade firewalls are proposed to secure the campus network perimeter and monitor traffic between VLANs. These devices will be strategically placed at the network edge and between critical segments such as the academic, administrative, guest, and VoIP VLANs.

- **Function:** Perform packet inspection, intrusion prevention, application control, and enforce access control policies. Firewalls also enable secure VPN connections and prevent lateral movement of threats within the internal network.

- **Justification:** With two buildings and multiple VLANs supporting sensitive academic and administrative data, deploying four firewalls allows for both perimeter defense and internal segmentation. This setup ensures resilience against external attacks, protection of academic intellectual property, and secure access to cloud-based services. Additionally, the increasing reliance on hybrid learning and BYOD (Bring Your Own Device) environments demands more granular traffic control and anomaly detection.

- **Specification & Cost (from BDCN):**
    - Quantity: 4
    - Estimated Unit Cost: £5,000
    - Total: £20,000

The selected firewalls must support stateful inspection, next-generation threat protection, deep packet inspection, VPN passthrough, and integration with centralised security management platforms.

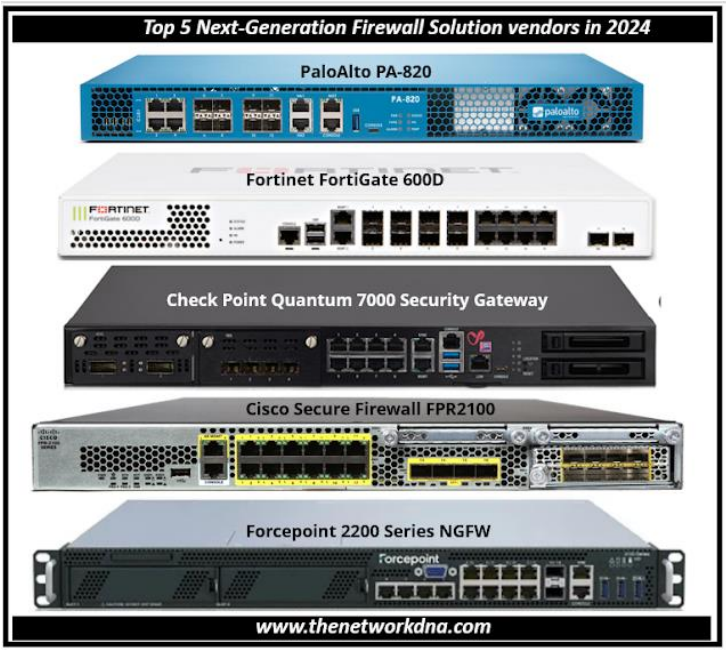

Figure 3.5 Next-Generation Firewall (Enterprise)

Source: Cisco page

3.5 WAN and Remote Access Hardware

As part of the University of the West of Scotland's (UWS) digital transformation strategy, reliable and intelligent wide-area networking (WAN) is essential to connect the new buildings not only to each other, but also to the wider university network. The integration of SD-WAN edge devices and a secure Virtual Private Network (VPN) setup ensures cost-effective, high-performance, and secure communication across locations while supporting modern remote access requirements.

3.5.1 SD-WAN Edge Devices

Four SD-WAN edge devices will be deployed to optimise WAN traffic and replace legacy MPLS circuits. These devices dynamically route traffic based on real-time performance metrics and provide automatic failover to ensure service continuity.

- **Function:** Enable dynamic, secure routing of data across broadband and fiber connections, ensuring optimal path selection for cloud applications, VoIP, and academic services.
- **Justification:** The adoption of SD-WAN significantly improves flexibility and cost efficiency while delivering high availability and redundancy. With two new buildings and multiple ISP connections recommended (e.g., BT, Virgin Media), four SD-WAN edge devices allow for load balancing and redundancy between links. This setup enhances user

experience, particularly for latency-sensitive services such as Microsoft Teams, virtual labs, and remote learning platforms (Murad et al., 2024).

- **Specification & Cost (from BDCN):**
    - Quantity: 4
    - Estimated Unit Cost: £3,000
    - Total: £12,000

These devices must support encryption, policy-based routing, deep application visibility, and compatibility with cloud-managed platforms.

Figure 3.6 SD-WAN Edge Gateway (Cloud-Managed)

Source: Cisco page

3.5.2 VPN Software and Licensing

A site-to-site VPN will connect the new buildings with the main campus securely, while remote access VPN services will be made available to staff and students who need off-campus access to academic and administrative systems.

- **Function:** Ensure secure, encrypted communication over public networks, enabling remote access to internal systems and seamless inter-campus connectivity.
- **Justification:** With hybrid work and study models becoming the norm, VPN access is crucial for remote teaching, learning management systems, and administrative operations. Licensing enterprise-grade VPN software (e.g., Cisco AnyConnect) ensures strong encryption, multi-factor authentication, and centralised user control.
- **Specification & Cost (from BDCN):**
    - Licensing and Setup Cost: £7,500

This component also supports the university's data privacy and security compliance obligations (e.g., GDPR) by encrypting user sessions and maintaining audit logs of access activity.

Figure 3.7 Cisco AnyConnect VPN (Licensing)

Source: Cisco page

3.6 Hardware Requirements & Total Cost

The table below summarises the proposed hardware components, quantities, and associated costs for the complete networking infrastructure of the two new university buildings. This selection supports a scalable, secure, and high-performance environment aligned with modern academic needs.

Hardware Component	**Quantity**	**Unit Cost (£)**	**Total Cost (£)**	**Purpose**
Core Routers	2	6,000	12,000	High-performance routing, inter-campus and internet connectivity
Core Switches	4	6,000	24,000	Core network switching, VLAN routing, backbone traffic

Access Switches	20	2,000	40,000	Endpoint device connectivity on each floor
Wi-Fi 6E Access Points	40	1,500	60,000	High-speed wireless coverage across high-density academic environments
Firewalls	4	5,000	20,000	Perimeter and VLAN security, threat prevention
SD-WAN Edge Devices	4	3,000	12,000	Intelligent WAN traffic routing, link failover
VPN Software & Licensing	–	–	7,500	Remote access and site-to-site VPN for secure communication
Total Estimated Cost	–	–	**£175,500**	

The total hardware cost of **£175,500** represents a strategic investment in the university's digital infrastructure. Each device has been selected to meet current functional demands while allowing for future expansion. This hardware setup, when paired with suitable software, cloud integration, and a robust network design, provides a comprehensive solution to connect and support academic, administrative, and student users across both buildings.

Reference:

Abu, M., Chowdhury, M.Z. and Jang, Y.M. (2023). Software-Defined UAV Networks for 6G Systems: Requirements, Opportunities, Emerging Techniques, Challenges, and Research Directions. *IEEE open journal of the Communications Society*, 4, pp.2487–2547. doi:https://doi.org/10.1109/ojcoms.2023.3323200.

Hassan, M., Gregory, M.A. and Li, S. (2023). Multi-Domain Federation Utilizing Software Defined Networking—A Review. *IEEE Access*, 11, pp.19202–19227. doi:https://doi.org/10.1109/access.2023.3242687.

Murad, S.S., Badeel, R., Abdal, B.B., Rahman, T. and Al-Quraishi, T. (2024). Introduction to Wi-Fi 7: A Review of History, Applications, Challenges, Economical Impact and Research Development. *Mesopotamian Journal of Computer Science*, 2024, pp.128–139. doi:https://doi.org/10.58496/mjcsc/2024/009.