Text

Description automatically generated

**MSc Information Technology**

**COMP11107 - Business Data Communication & Networks**

**Coursework Report**

**Modern Network for Two New University Buildings**

**by**

|  |  |  |
| --- | --- | --- |
| **NAME** | **BANNER ID** | **Individual contribution** |
| **Prajwalaradhya Shivakumaraswamy Kesaramadu** | **B01759301** | **2,4,6** |
| **Sayyar Hayat** | **B01772768** | **1,5** |
| **Aman Misra** | **B01746656** | **2,3** |
| **Sreeraj Karuvanthodi Ramachandran** | **B01764963** | **2,3** |
| **Muhammed Ali Panthalingal** | **B01755979** | **6,7** |
| **Qaiser Sajawal** | **B01794675** | **4** |

**Contents**

[1. Proposed Solution Addressing User Needs 3](#_Toc194946403)

[1.1 Discussion 3](#_Toc194946404)

[1.2 Justification 4](#_Toc194946405)

[2. Proposed Hardware 6](#_Toc194946406)

[2.1 Discussion 6](#_Toc194946407)

[2.2 Justification 10](#_Toc194946408)

[3. Proposed Software 12](#_Toc194946409)

[3.1 Discussion 12](#_Toc194946410)

[3.2 Justification 13](#_Toc194946411)

[4. Proposed Network Circuits 15](#_Toc194946412)

[4.1 Discussion 15](#_Toc194946413)

[4.2 Justification 20](#_Toc194946414)

[5 Proposed Cloud-Based Services 22](#_Toc194946415)

[5.1 Discussion 22](#_Toc194946416)

[5.2 Justification 23](#_Toc194946417)

[6. Proposed Detail Costings 24](#_Toc194946418)

[6.1 Discussion 24](#_Toc194946419)

[6.2 Justification 24](#_Toc194946420)

[7. Conclusion & Future Recommendations 25](#_Toc194946421)

[7.1 Conclusion 25](#_Toc194946422)

[7.2 Future Recommendations 25](#_Toc194946423)

[References 26](#_Toc194946424)

# 1. Proposed Solution Addressing User Needs

## 1.1 Discussion

This section outlines an innovative, scalable network design for the two new buildings (Building 1 and Building 2) at the University of the West of Scotland (UWS). The system objective is to provide smooth connectivity for administrative staff, academics, and students while making sure everything runs fast, stays secure, and can grow in the future.

**Networking Floors within Each Building**

Each structure has three floors. Each floor has different facilities and is used by different groups of people. To make sure everyone in the building stays connected without issues, we suggest using both wired (like Ethernet cables) and Wi-Fi networks together.

* **Ground Floor:** For administrative staff working on the ground floor, we are providing secure wired internet connections in their offices. As they are handling important university data, their network should be kept separate from others to prevent unauthorized access. The system also provides backup power systems to make sure their work is never interrupted.
* **First and Second Floor:** These floors are mostly used for academic activities, including lecture halls, tutorial rooms, and computer labs to maintain reliable connectivity, each floor will be equipped with managed switches, providing wired internet access for desktop computers and lab devices. In addition, Wi-Fi 6 access points (APs) will provide fast wireless connectivity for laptops, tablets, and smartphones used by students and staff. The network will support digital learning tools, online resources, and co-operation platforms for multiple users at the same time.

**Connecting the Two Buildings**

To enable effective association and resource sharing between both buildings, a high-performance inter-building network link is crucial. Our solution develops fibre optic cabling to interconnect the amenities. This technology brings plenty of benefits, like super-fast bandwidth, quick response times, and the flexibility to grow and adapt as needs change over time.

* **Fibre Optic Backbone:** A dedicated single-mode fibre link will connect both buildings, supporting 10Gbps data transfer, video conferencing, and real-time interactions. The enterprise-grade infrastructure ensures low-latency performance for both academic and administrative tasks. The scalable design accommodates future bandwidth upgrades while upholding compatibility with surviving systems.
* **Redundancy:** Dual fibre paths with automatic failover ensures uninterrupted connectivity. This fault-tolerant design disregards single points of failure for critical operations.

**Integrating Building with Network**

The new buildings need to connect efficiently to the university’s present network. This will allow users access shared resources, administrative systems, and the internet. The connection will use both hardware (like routers) and software (like network management systems) to work properly.

* **Switches & Routers:** Routers direct traffic between networks and buildings, while switches connect all devices within each building. Together they enable seamless communication across the entire campus network.
* **VPNs:** VPNs create secure encrypted tunnels for all data moving between buildings, protecting sensitive information from external threats.
* **Network Segmentation:** VLANs separate network traffic by user groups and purposes, improving security and performance across different departments.

**Future Proofing the Network**

To ensure long-term usability, the network will be designed to adapt to growing demands and emerging technologies.

* **Scalable Infrastructure:** The architecture promotes easy developments, letting bandwidth and capability to increase as needed without major reforms.
* **New Technology Advancements:** The system will accommodate innovations like IoT, AI tools, and higher-speed standards (e.g., Wi-Fi 7, 100Gbps fibre) through modular hardware and flexible configurations.

## 1.2 Justification

This network solution transports fast, secure connectivity for all users while supportive future growth. Its stabilities performance and security with scalable infrastructure. The architecture is optimized for current demands and scalable to accommodate future technological developments.

* **Administrative Staff Offices:** The wired connections and remote VLAN ensure secure, continuous access to sensitive systems like student records and financial data. Redundant power and network paths ensure uninterrupted critical operations, while strict access controls secure confidential information without negotiating high-speed performance.
* **Academics Offices**: High bandwidth wired/Wi-Fi 6E connectivity provides research data allocations and hybrid teaching tools. Quality of Service arranges video calls and cloud association platforms. The ports are also ready for the future, so they can handle more schoolwork as needs grow.
* **Social/Common Room:** Bandwidth-throttled Wi-Fi 6E allows 50+ concurrent users for casual browsing without impacting critical networks. Separate guest VLAN protects core systems while enabling device flexibility.
* **Tutorial Classrooms:** Reliable Wi-Fi 6 handles small-group association with low-latency screen sharing. Wired ports for tutors enable stable connections to demonstration systems. Device isolation prevents cross-interference during simultaneous logins.
* **Computer Labs:** The wired network in computer labs ensures fast and stable connections for resource-intensive tasks like programming and recreations. Each workstation gets its own bandwidth, so classes don’t slow down. The system supports quick software deployments and secure logins for students and staff.
* **Future Needs:** The proposed network is intended to scale effortlessly as user needs grow, with integrated infrastructure that adapts to growing technologies.

This network solution gives each user group exactly what they need - fast internet for teachers, secure connections for office staff, and strong Wi-Fi for students. It keeps everything safe and running efficiently while making it easy to advancement later. The system works perfectly today but is also ready for future developments.

# 2. Proposed Hardware

## 2.1 Discussion

Picking the right hardware is crucial to ensure the network works smoothly in the new Buildings 1 and 2 at UWS. This section explains the main hardware devices we will use and why we chose them. The network will follow a standard 3-layer setup (core, distribution, and access) to improve performance.

**Core Switches**

The university needs to move a lot of data without slowing down. To do this, we need powerful switches. The Cisco Catalyst 9500 Series is a good option because it moves data fast, works well with other systems, and can handle a lot of work.

* **Cisco Catalyst C9500-48Y4C** is a powerful main switch made for big business networks. It has 48 ports that support 25G or 10G speeds, and 4 super-fast 100G ports for quick data transfer**.**



Fig 2.1

**Distribution Switches**

The distribution layer uses powerful switches like the Cisco Catalyst 9300 Series to gather data from smaller switches and connect to the main network. These switches provide fast connection speeds, give priority to important apps, and separate the network into sections using VLANs. They are built to handle growing networks and help data move smoothly between parts of the network while supporting advanced features across the entire campus.

* **Cisco Catalyst C9300-48UXM** is a network switch with 48 very fast ports. It can send power and data through the same cable. It's great for busy places like classrooms and labs. You can also connect more switches easily as your network grows.

A white device with many ports

AI-generated content may be incorrect.

Fig 2.2

**Access Switches**

We use Cisco Catalyst 9200 switches to connect computers, phones, and Wi-Fi. These switches give power to devices like Wi-Fi points and phones through the same cable that connects them to the network, so no extra power cords are needed. They are easy to use and work well in classrooms, labs, and offices.

* **Cisco Catalyst C9200L-48P-4X-A** has 48 power-over-Ethernet (PoE) ports to connect devices like Wi-Fi 6 access points and IP phones, along with 4 fast uplinks for quick data transfer. It’s ideal for places that need both power and a strong network connection.

A close-up of a device

AI-generated content may be incorrect.

Fig 2.3

**Firewalls**

We use strong firewalls, like Cisco Firepower, to protect the network. These firewalls stop online threats, block attacks, and check all data for safety. They keep the network secure while making sure everything runs fast for users.

* **Cisco FPR2130-ASA-K9 Firepower** is a strong security tool that keeps big networks, like those in universities, safe from online dangers. It uses Cisco ASA security and Firepower to block attacks right away and allows fast VPN connections. It's great for networks with over 1000 users and works well with current Cisco equipment and future updates.

A close up of a device

AI-generated content may be incorrect.

Fig 2.4

**Wireless Access Points (WAP)**

We'll use Cisco Catalyst 9136 wireless devices to give strong internet all over the buildings. These support the latest Wi-Fi 6 technology, which means faster speeds for everyone. They work well in crowded areas like classrooms where many students connect at once.

* **Cisco Catalyst 9136I** is a top-tier Wi-Fi 6E access point that provide blazing speeds up to 3.5Gbps using the 6GHz band. It easily handles 150+ concurrent devices in high-density areas like lecture halls, while its smart antenna design ensures full coverage. Perfect for future-proofing the campus network.

A white electronic device with a black handle

AI-generated content may be incorrect.

Fig 2.5

**Cabling Infrastructure**

We’ll use Cat6a cables for connections in offices and classrooms. These cables can handle speeds up to 10Gbps and power devices like Wi-Fi access points. Fiber optic cables (OS2) will connect buildings and server rooms for fast, long-distance connections. This mix of cables is cost-effective while still meeting performance and future needs.

* **Cat6a Ethernet Bulk Cable Shielded** is high-quality 23AWG solid copper cable supports 10Gbps speeds up to 100m and 750MHz bandwidth, ideal for dependable wired networks. Its protected design reduces interference, perfect for offices and classrooms with PoE devices like Wi-Fi APs.

A cable and a box

AI-generated content may be incorrect.

Fig 2.6

* **Single Mode (OS2) 2.0mm, Tight Buffered** is a long-distance fibre optic cable supports 10Gbps to 100Gbps speeds over 10km+, ideal for connecting buildings. The tight-buffered design makes it long-lasting and easy to install in tight spaces.

A close up of a cable

AI-generated content may be incorrect.

Fig 2.7

**Rack-Mounted Servers**

We will set up Dell PowerEdge servers in racks to store academic data, run virtual labs, and share resources. These servers will have fast processors and SSD storage to handle the tasks, and they will be designed to stay running 24/7 with backup power and cooling to support important university work.

* **Dell PowerEdge R740 512GB 2 Xeon Gold** is high-performance server delivers extreme processing power for virtualization, databases, and campus-wide applications. With 512GB RAM and dual Xeon Gold CPUs, it handles heavy workloads while ensuring reliability for 24/7 university operations.

A silver computer device with a white background

AI-generated content may be incorrect.

Fig 2.8

**UPS (Uninterruptible Power Supply)**

We’ll set up UPS systems to protect servers, switches, and important equipment from power cuts, making sure everything runs all the time and shuts down safely during power failures.

**Eaton 9PX 2000VA 1800W 120V Online** is high-efficiency online UPS delivers 1800W/2000VA pure sine wave power, make sure zero downtime for critical lab equipment and servers. With double-conversion technology, it protects against surges, outages, and voltage fluctuations.

A black electronic device with a blue screen

AI-generated content may be incorrect.

Fig 2.9

**Additional Hardware**

* **Printers:** Printers will be set up in the admin offices and labs for staff and students to use. These printers will be connected to the network and require user login, helping to keep printing secure and reduce waste.
* **IP Phones:** Cisco IP phones (PoE-powered) will provide crystal-clear voice calls across campus, joined with your network for perfect internal communication.

## 2.2 Justification

**Core Switches**

Core switches are the backbone of the network, connecting all buildings and controlling heavy data traffic. We chose high-performance switches like the Cisco Catalyst 9500 because they support fast speeds (up to 100Gbps) and ensure smooth communication across campus. Their new features, like redundancy and scalability, stop downtime and allow future upgrades. This keeps the network reliable for students, teachers, and staff, even during peak usage. Investing in strong core switches now saves costs later by avoiding frequent replacements.

**Distribution Switches**

These switches connect all floors and buildings while handling heavy traffic. The C9300-48UXM model offers 48 multi-gigabit ports and 100G uplinks, ensuring fast data flow between rooms and labs. It supports VLANs to different staff/student traffic securely. Its stackable design allows easy expansion as the university grows.

**Access Switches**

Used in classrooms and offices, the C9200L-48P-4X-A gives Power over Ethernet (PoE++) to run Wi-Fi 6 access points and IP phones without extra wiring. Its 48 ports support high-speed connections for PCs and printers, while 10G uplinks stop bottlenecks. Easy to manage and scalable for future needs.

**Firewall**

This firewall blocks hackers and malware, keeping student/staff data safe. It combines Cisco ASA security with Firepower threat detection for real-time protection. Supports VPNs for remote access and works smoothly with your switches. Ideal for a campus with 1000+ users.

**Wireless Access Points (WAP)**

The 9136I Wi-Fi 6 access points give fast, reliable internet in crowded lecture halls and labs. Handles 100+ devices at once with speeds up to 1.7Gbps. Easy to set up and manage through Cisco’s cloud tools.

**Cables**

* **Cat6a Shielded:** Supports 10Gbps speeds and PoE++ for devices like APs and phones. Reduces interference in busy areas.
* **OS2 Single-Mode Fiber:** Connects buildings with 10Gbps+ speeds over long distances. Future-proof for upgrades.

**Servers**

The R740 server (with 512GB RAM and dual Xeon Gold CPUs) runs databases, virtual labs, and campus apps without slowing down. 24/7 reliability with redundant power and storage.

**UPS**

Protects servers and switches from power cuts, ensuring no data loss. Gives clean power for 30+ minutes during outages. Easy to monitor via LCD.

**Additional Hardware**

* Printers: Networked printers with secure login for staff/students, reducing waste.
* IP Phones: Cisco PoE phones for clear calls across campus, powered by switches.

This network setup gives every user—students, teachers, and staff—the speed, security, and reliability they need. From high-speed Wi-Fi in classrooms to secure data storage in servers, each part is chosen to work smoothly together. The system is easy to upgrade as the university grows, saving time and money later. With backup power and strong security, the network will run safely for years.

# 3. Proposed Software

## 3.1 Discussion

Picking the right software is key to making the network run smoothly, stay secure, and be easy to manage. In this section, we'll explain the software we plan to use for the switches, Wi-Fi, firewalls, VPN, Antivirus and servers - all chosen to work perfectly with our Cisco hardware. We'll focus on solutions that are powerful yet simple to use, keeping costs reasonable for the university's needs.

**Network OS (Cisco IOS-XE)**

Cisco IOS-XE is the operating system for Cisco's modern switches and routers. It is used across core, distribution, and access layers to manage connectivity, security, and traffic flow. Key features include automation tools (SD-Access), real-time monitoring, and advanced security like MACsec encryption. Its modular design allows updates without downtime, making it ideal for high-availability networks like universities. IOS-XE simplifies management while ensuring reliability for 24/7 operations.

**Firewall (Cisco Firepower Threat Defence)**

Cisco Firepower Threat Defence (FTD) is the security software for your Cisco FPR2130 firewall, combining firewall protection with advanced threat detection. It monitors all network traffic in real-time to block viruses, hackers, and intrusions using features like IPS (Intrusion Prevention System), malware scanning, and VPN support. Easy to manage through a central dashboard, it enforces security policies for staff/student devices while allowing secure remote access. Ideal for campuses, it balances strong protection with simple controls.

**Server OS (Windows 2022)**

Windows Server 2022 is the recommended operating system for your Dell PowerEdge R740 servers. It provides a stable and secure platform for running university applications, databases, and virtual labs. Key features include Active Directory for user management, Hyper-V for virtualization, and built-in security tools to protect sensitive data.

**Monitoring & Backup (Cisco DNA Center)**

Cisco DNA Center is the centralized management platform for your university's Cisco network hardware (switches, routers, wireless). It simplifies configuration, monitoring, and troubleshooting through an intuitive dashboard, while automating tasks like software updates and policy enforcement.

**Antivirus (McAfee)**

This software protects all university devices (PCs, servers) from viruses, ransomware, and spyware. It runs quietly in the background with real-time scanning, automatic updates, and web protection to block dangerous sites. Easy to manage centrally for all campus computers.

**Virtual Private Network (Cisco AnyConnect VPN)**

Cisco AnyConnect VPN is the ideal choice for your university as it integrates perfectly with your existing Cisco firewall and switches. It offers secure remote access with military-grade encryption, ensuring staff and students can safely connect from anywhere. The simple one-click login and centralized management save IT time while keeping threats out.

**Access Management (Cisco Identity Services Engine)**

Cisco Identity Services Engine securely manages Wi-Fi access by requiring login via a portal before granting internet. It works with your Cisco network to enforce policies (like blocking guests) and track connected devices. Keeps campus Wi-Fi safe and controlled.

## 3.2 Justification

**Network OS (Cisco IOS-XE)**

We chose Cisco IOS-XE because it’s designed specifically for Cisco switches and routers, ensuring perfect compatibility and smooth performance. It simplifies management with both web and command-line interfaces, while automatic updates keep security tight against new threats. This OS is trusted by universities globally for building stable, scalable networks that grow with student needs.

**Firewall (Cisco Firepower Threat Defence)**

Cisco Firepower is ideal for blocking viruses, hackers, and intrusions in real-time, keeping campus data safe. It integrates seamlessly with your existing switches and VPN, creating a unified security system. As the industry’s top enterprise firewall, it’s proven to handle high-traffic networks like universities without slowing down.

**Server OS (Windows 2022)**

Windows Server 2022 runs smoothly on your Dell PowerEdge servers, supporting academic apps and databases with ease. Its familiar interface reduces training time for IT staff, while built-in tools like Active Directory and Hyper-V simplify user and resource management. Regular updates from Microsoft ensure long-term reliability.

**Monitoring & Backup (Cisco DNA Center)**

Cisco DNA Center provides a single dashboard to monitor and manage all network devices, from switches to Wi-Fi. It automates backups, preventing costly downtime from configuration errors, and includes tools for troubleshooting. This centralized control saves IT teams hours of manual work while keeping the network secure.

**Virtual Private Network (Cisco AnyConnect VPN)**

AnyConnect VPN provides secure remote access for staff and students, encrypting data even on public Wi-Fi. It comes included with the Cisco firewall license, so there’s no extra cost, and it offers one-click login for ease of use. It also has military-grade encryption and malware blocking for added security.

The VPN is also used to connect other university buildings through a secure WAN, which is more cost-effective than setting up a dedicated WAN line. This setup keeps the network safe, reliable, and budget-friendly.

**Access Management (Cisco Identity Services Engine)**

Cisco ISE ensures only authorized users access campus Wi-Fi by requiring login credentials via a captive portal. It tracks connected devices to prevent abuse and enforces policies like bandwidth limits for guests. Tight integration with Cisco APs and switches makes it a no-brainer for your secure network.

Every software chosen is Cisco-branded because it guarantees compatibility, reduces complexity, and leverages industry-trusted security. This all-Cisco ecosystem is cost-effective, easy to maintain, and scales effortlessly as your university grows. From firewall protection to Wi-Fi logins, this setup delivers reliability, safety, and simplicity.

# 4. Proposed Network Circuits

## 4.1 Discussion

To ensure a reliable and scalable network for the university, we propose a three-tier architecture comprising core, distribution, and access layers. This design efficiently manages traffic flow, enhances performance, and simplifies troubleshooting across Buildings 1 and 2. The core layer handles high-speed data transfer between buildings, the distribution layer routes traffic between floors, and the access layer connects end-user devices. Fiber optic cables link the core and distribution layers for speed, while shielded Cat6a cables serve access-layer devices. This structured approach ensures seamless connectivity, security, and future scalability for the entire campus network.

**Three-Tier Network Architecture**

The 3-tier network design splits the system into three layers: the core (connects buildings), distribution (routes traffic between floors), and access (links devices like PCs and phones). This keeps the network fast, organized, and easy to manage.

1. **Core Layer:** The backbone of the network, connecting buildings with high-speed fiber for maximum data flow.
2. **Distribution Layer:** Routes traffic between floors and enforces security policies across the campus.
3. **Access Layer:** Connects end-user devices (PCs, phones, Wi-Fi) with Cat6a cables for reliable daily use.

A group of blue cubes with white circles and arrows

AI-generated content may be incorrect.

Fig 4.1

**Network Configuration by Floor**

This section details the wired/wireless setup, VLANs, and cabling for each floor—ground (admin), first (classrooms), and second (labs)—ensuring optimal performance and security.

**Ground Floor**

This floor handles administrative offices (Finance, HR, Admissions) with dedicated VLANs for secure, high-speed wired connections to protect sensitive data with VLAN 10, 20 and 30. The social/common room uses VLAN 40 for student Wi-Fi, with bandwidth throttling to prevent network slowdowns. Cat6a cables connect all devices, while PoE switches power IP phones and Wi-Fi 6 access points.

1. **Finance Computers:** The finance team uses 10 computers, 1 network printer, and 10 IP phones, all connected via Cat6a cables to a Cisco Catalyst C9200L switch. These devices are isolated in VLAN 10 (Finance) with the subnet 192.168.10.0/24 for secure traffic management. VPN access is enabled for remote work on financial systems, with strict port security (MAC filtering) to prevent unauthorized connections.
2. **HR Computers:** The HR team uses 5 computers, 1 network printer, and 5 IP phones, all connected via Cat6a cables to the same Cisco Catalyst C9200L switch (shared with Finance). These devices are assigned to VLAN 20 (HR) with the subnet 192.168.20.0/24 to isolate sensitive employee data. VPN access is enabled for HR managers, and port security (sticky MAC) restricts unauthorized device connections.
3. **Admission Department Computers:** The admissions team uses 5 computers, 1 network printer, and 5 IP phones, connected via Cat6a cables to the Cisco Catalyst 9200 switch. These devices are assigned to VLAN 30 (Admissions) with the subnet 192.168.30.0/24, keeping student application data secure. Limited VPN access is granted only to senior staff.
4. **Common Rooms for Students:** This shared common space supports 50+ users with 2 Wi-Fi 6 access points (Cisco Catalyst 9136I) for seamless connectivity. Devices connect to VLAN 40 (Common) with subnet 192.168.40.0/24, offering open but throttled Wi-Fi for students/staff. No VPN or port security is applied, as it’s a public zone with limited bandwidth.

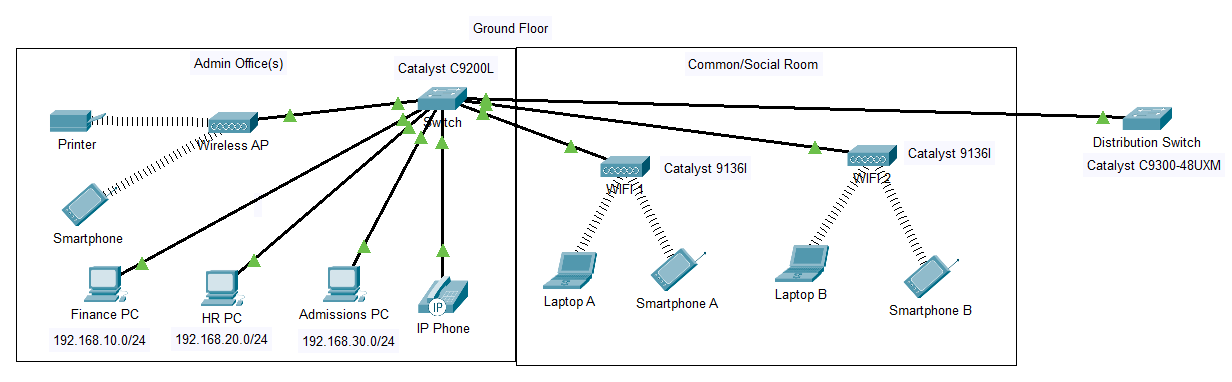


Fig 4.2 Image of Ground Floor in Packet Tracer

**First Floor**

The first floor supports academic offices, lecture halls, tutorial rooms, and computer labs, each with unique connectivity needs. High-speed wired and wireless networks ensure seamless teaching and research, with VLAN segmentation to separate traffic (e.g., faculty, students, lab devices). Cisco Catalyst switches manage connections, while Wi-Fi 6 access points handle dense classroom demands. Structured cabling (Cat6a/fiber) future-proofs the infrastructure.

1. **Academics Offices:**

The first floor accommodates 10 academic offices, each provisioned with two dedicated Ethernet ports to support laptops, desktops, and research devices. These ports are linked with Cat6a shielded cabling and connected to a Cisco Catalyst C9200L-48P-4X-A 48-port PoE+ switch, ensuring reliable 1Gbps+ wired connectivity for resource-intensive tasks like data analysis and video conferencing. All academic devices are segmented into VLAN 50 (subnet: 192.168.50.0/24) to isolate research traffic and prioritize bandwidth. VPN access is enabled for secure remote collaboration, with port security. The switch’s 28 reserved ports future-proof the setup for Wi-Fi 6 AP expansions or additional workstations. This design balances performance, security, and scalability for faculty needs.

A diagram of a computer network

AI-generated content may be incorrect.

Fig 4.3 Image of First floor Academics in Packet Tracer

1. **Lecture and Tutorial Rooms:**

The first floor includes 6 lecture rooms and 6 tutorial rooms, each connected to 2 Ethernet ports to support teaching devices like laptops and presentation systems. These ports connect via Cat6a cables to a Cisco Catalyst C9200L-48P-4X-A 48-port PoE+ switch, with VLAN 60 (192.168.60.0/24) for lectures and VLAN 70 (192.168.70.0/24) for tutorials to separate traffic. Every room has a dedicated Wi-Fi 6 access point and networked projectors, powered by the switch’s PoE+ ports.

A diagram of a computer network

AI-generated content may be incorrect.

Fig 4.4 Image of First Floor Lecture & Tutorial Rooms in Packet Tracer

1. **Computer Labs:**

The first floor includes 4 computer labs, each with 20 PCs and 1 networked printer. Every lab uses a dedicated Cisco Catalyst C9200L-48P-4X-A switch to connect all devices via Cat6a Ethernet cables, ensuring fast and stable wired connections. Wi-Fi 6 access points are installed for wireless devices, while VLAN 80 (192.168.80.0/24) isolates lab traffic for security and performance.

A diagram of a computer network

AI-generated content may be incorrect.

Fig 4.5 Image of First Floor Computer Labs in Packet Tracer

**Second Floor**

Since the second floor has identical usage requirements as the first floor (academic offices, classrooms, and labs), we'll implement the same network design. This ensures consistency in performance, security, and management across both floors while simplifying maintenance.

**Second Building**

Building 2 will use the exact same network architecture as Building 1—matching switches, VLANs, cabling, and security policies—since both buildings serve identical academic and administrative functions. This standardized design ensures consistent performance, easier maintenance, and seamless connectivity across the entire campus.

**Connectivity Between Buildings**

The distribution layer switches (Catalyst C9300-48UXM) in each building aggregate traffic and connect to the core layer via 10G fibre uplinks. At the core, Catalyst C9500-48Y4C switches route data between buildings, while the Cisco Firepower firewall inspects and secures all traffic. The core also links to university servers and the ISP router for internet access. Buildings are interconnected with OS2 single-mode fibre cables, ensuring high-speed, low-latency communication. This design guarantees secure, reliable connectivity across campus while maintaining scalability for future needs.

**Fibre Optic Cables Deployment**

The connectivity between buildings relies on a robust star topology, where each building's network infrastructure connects back to centralized Cisco Catalyst 9500 core switches through OS2 single-mode fibre optic cables. These fibre cables act as the network's backbone, capable of transmitting data at 10Gbps+ speeds over long distances with minimal signal loss, making them ideal for campus-wide links.

At the core layer, the Catalyst 9500 switches serve as the central hub, equipped with high-density 10/25/40/100Gbps ports to handle heavy traffic between buildings. Each floor's Cisco Catalyst 9300 distribution switches aggregate data from access-layer devices (computers, phones, Wi-Fi) and uplink to the core via fibre, ensuring seamless communication.

The star topology ensures reliability—if one link fails, the rest of the network stays operational. Advanced features like QoS (Quality of Service) prioritize critical traffic (e.g., video lectures), while VLAN segmentation keeps departments (admin, faculty, students) securely separated.

The proposed three-tier network design (core-distribution-access) with fibre backbone (OS2) and Cat6a cabling provides a reliable, high-performance infrastructure for the university. By using standardized VLANs, PoE switches, and centralized management, the design ensures security, scalability, and seamless connectivity across all floors and buildings. This future-proof approach minimizes downtime, simplifies troubleshooting, and supports growing tech needs for the next 10+ years.

## 4.2 Justification

Our network design combines a fibre backbone, VLAN segmentation, and star topology to deliver speed, security, and scalability. The fibre ensures fast connectivity, VLANs separate traffic for security, and the star topology simplifies management. Each component was chosen for performance, cost-efficiency, and future readiness, ensuring reliability and easy maintenance while maximizing ROI.

**Choice of Fiber Optic Cables**

We selected OS2 single-mode fibre for its ability to support 10Gbps+ speeds over long distances (up to 10km) with minimal signal loss. Its immunity to electromagnetic interference ensures reliable performance, even in high-traffic campus environments. The tight-buffered design simplifies installation, while LC connectors provide low-loss connections. This future-proof solution accommodates upgrades to 40G/100G+ speeds as needs grow.

**Core Switches (Cisco Catalyst C9500-48Y4C)**

These high-performance switches form the backbone of the network, offering 48x 25G/10G ports and 4x 100G uplinks for ultra-fast data transfer between buildings. Their modular design supports future upgrades, while Software Defined-Access compatibility enables seamless automation. With redundant power and cooling, they ensure 24/7 reliability for critical university operations.

**Distribution Switches (Cisco Catalyst C9300-48UXM)**

These switches act as the middle layer, connecting all the access switches to the main core switches. They offer flexible ports that support everything from basic 1Gbps connections up to 10Gbps for high-demand areas, with powerful 40G/100G uplinks to handle heavy traffic between floors. Features like easy stacking (up to 8 switches) and smart traffic prioritization (QoS) make them perfect for a busy campus, while keeping different groups (students, staff) securely separated with VLANs.

**Star Topology**

We chose a star topology because all distribution switches connect directly to the central core switches (Catalyst 9500), creating a simple and reliable hub-and-spoke design. This setup ensures that if one link fails (e.g., a fibre cut to Building 1), other connections remain unaffected—critical for minimizing downtime in a busy university.

**Why Not Other Topologies?**

* **Ring Topology:** Data must travel through multiple switches, causing delays.
* **Mesh Topology:** Expensive and complex to wire.

The star design strikes the perfect balance between cost, simplicity, and fault tolerance.

**Integrated Campus Network Architecture**

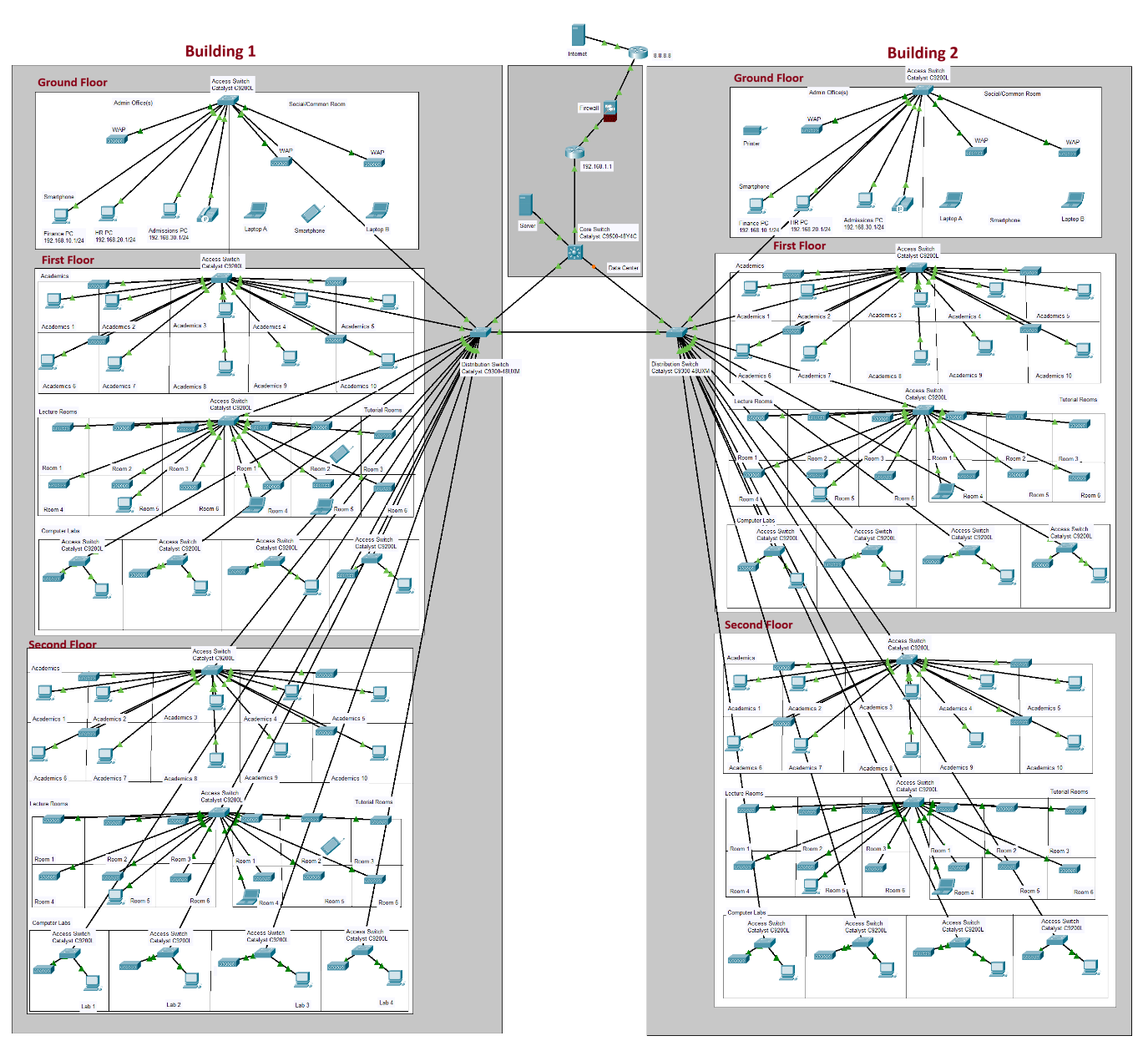


Fig 4.6

# 5 Proposed Cloud-Based Services

## 5.1 Discussion

The University of the West of Scotland wants to transform its two new buildings, to integrating cloud-based services which is key to deliver scalable, resilient, and cost-efficient solutions. The services will address current academic and administrative needs while ensuring long-term adaptability for emerging technologies. Below are some proposed cloud solutions for the campus:

* Microsoft 365 Education:
* Aula Learning Management System
* Microsoft Azure Blob Storage (Backups)
* Datadog Monitoring
* Okta SSO/Identity Management

**Microsoft 365 Education**

This cloud platform equips the users with core utilities supporting both email functionality and online academic collaboration and OneDrive storage platforms. Its licensing provides affordable access to advanced features which ensures adherence to academic data privacy standards. It is integrated with university’s different systems which enables smooth workflows for staff and students. The platform scales effortlessly to accommodate growing user numbers across both new buildings.

**Aula Learning Management System**

Aula is a modern learning management system which provides a captivating digital learning environment through user-friendly course structure and attractive tools. This supports multimedia content, real-time feedback, and student discussion forums while integrating with university’s existing authentication systems. The mobile-friendly interface gives access across devices, that are crucial for today's hybrid learning needs. It customizes data dashboard supports teachers in tracking academic development and student records.

**Microsoft Azure Blob Storage (Backups)**

Azure's enterprise the grade storage solution provides reliable, secure backup for critical university data such as research files, administrative records, and system configurations. its geo-redundant storage options ensure business continuity even during local infrastructure failures. The pay-as-you-go model exclude upfront hardware costs while offering virtually unlimited scalability. Strong data encryption and user access restrictions follows strict privacy regulations.

**Datadog Network Monitoring**

This monitoring platform delivers broad transparency on network operations, application health, and security threats across the university's hybrid infrastructure. It’s customize dashboards provide real-time monitoring of Wi-Fi performance, server status, and bandwidth operations. The automated alerts system enable proactive issue resolution before users are impacted. The solution scales with the university's growing technology footprint while maintaining simple centralized management.

**Okta Identity Management**

Okta's SSO (Single Sign-On) and MFA (Multi-Factor Authentication), this solution gives reliable and secure access to all university cloud applications and services It makes login easier for users with authentication while maintaining strict security standards across devices and locations. The platform connects Aula, Microsoft 365, and other systems through standardized protocols.

By implementing these cloud-based services, the University of the West of Scotland can create a more efficient, secure, and scalable digital environment that supports both academic and operational success.

## 5.2 Justification

We chose these cloud tools because they expand as your needs grow. (no expensive upgrades), keep data safe (with encryption and secure logins), and save money (pay only for what you use). They work smoothly with university’s current systems while simplifies collaboration for both staff and students. —whether they're on campus or learning remotely.

* **Scalability:** The cloud services use elastic computing resources that automatically expand as demand grows - more students, courses, or data won't require hardware upgrades. Microsoft 365 licenses scale instantly, while Azure storage allocates additional capacity through software controls.
* **Cost Efficiency:** Cloud services follow on operational expenditure models with education discounts avoiding capital costs for physical servers while benefiting from Microsoft's academic pricing tiers and Azure's pay-per-use storage billing.
* **Collaboration Tools:** The integrated platform combines Teams for real-time communication with Aula's LMS features, creating a unified collaboration environment with single sign-on (SSO) through Okta.
* **Data Security:** The cloud keeps university data safe with strong protections. Okta verifies every login, while Microsoft encrypts all files and emails. Automatic security rules block leaks of sensitive info like grades or research. These measures meet strict education privacy laws.
* **Backups & Recovery:** All data is automatically saved in multiple locations. If files get deleted or servers fail, the system can quickly restore from backups. Azure guarantees 99.9% uptime, so systems stay available during emergencies.
* **Learning Management:** Aula provides all-in-one teaching tools including Hosts course materials and assignments, Hosts course materials and assignments, Hosts course materials and assignments and Hosts course materials and assignments.

In Conclusion, by integrating these cloud services, the University of The West of Scotland gains a scalable, secure, and cost-effective digital foundation. The solutions enhance collaboration, safeguard data, and ensure reliable performance across both new buildings.

# 6. Proposed Detail Costings

## 6.1 Discussion

The price breakdown for the UWS’s new buildings covers hardware, software, cloud services and installation & labour fees. It contains switches, firewalls, Access Points, fibre optic cables and others. It also includes licensing fees for network management, software and cloud services.

## 6.2 Justification

The cost includes discounts, warranties and technical support from vendors. Major vendors like Cisco, Microsoft offer educational discounts and warranties which can be extended to universities which helps us to reduce costs. They provide better technical support and training for IT employees to manage and maintain the network. By gaining these offers, the university is able to receive cost-effective network which meets both current and future needs.

**6.3 Costing Breakdown**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Description** | **Quantity** | **Per Unit Cost** | **Total** |
| Cisco Catalyst C9500-48Y4C | Core Switch | 1 | £14,000 | £14,000 |
| Cisco Catalyst C9300-48UXM | Distribution Switch | 2 | £7,500 | £15,000 |
| Cisco Catalyst C9200L-48P-4X-A | Access Switch | 26 | £2,000 | £52,000 |
| Cisco FPR2130-ASA-K9 Firepower | Firewall | 1 | £10,000 | £10,000 |
| Cisco Catalyst 9136I | Access Points | 86 | £1,000 | £86,000 |
| Cat6a Cable | Copper Cable | 1 | £1,000 | £1,000 |
| OS2 Cable | Fibre Optic cable | 1 | £200 | £200 |
| Dell PowerEdge R740 512GB 2 Xeon Gold 14 CPU 1TB SSD 64TB HDD | High Performance Server | 2 | £3,000 | £6,000 |
| Eaton 9PX 2000VA 1800W 120V Online | UPS | 1 | £1,800 | £1,800 |
| Cisco Firepower Threat Defence | Software Firewall | - | £2,500 | £2,500 |
| McAfee Antivirus | Antivirus | - | £1,500 | £1,500 |
| Cisco AnyConnect | VPN | - | £200 | £200 |
| Cloud Services | MS 365, Azure Storage, Datadog Monitoring, Aula, Okta Identity | - | £10,000 | £10,000 |
| Installation | Labour Charge | - | £15,000 | £15,000 |
| **Total** |  |  |  | £212,000 |

# 7. Conclusion & Future Recommendations

## 7.1 Conclusion

The proposed network solution for the University of the West of Scotland’s new Buildings 1 and 2 is designed to be strong, scalable, and secure, meeting the needs of staff and students now and in the future. The three-tier network structure ensures high performance, easy management, and backup options in case of failures.

High-quality hardware like Cisco Catalyst switches and firewalls ensures strong security and stable connections. Software tools such as Cisco DNA Center for network management and backup, along with McAfee for antivirus, help keep the network efficient and safe. Cloud services like Azure Blob Storage, OneDrive, and Aula LMS offer flexible and scalable options for storage, learning, and security. A VPN is also included to connect other university buildings through a secure WAN. Costs have been planned well, using vendor discounts, extended warranties, and support options to keep it affordable. The detailed costing makes the plan clear and shows it is financially practical.

## 7.2 Future Recommendations

To make sure the network infrastructure remains future-proof and continues to meet the growing requirements of the university, some recommendations are proposed.

1. **Regular Check-ups & Updates:** Doing regular network checks and identification of weak areas and bottlenecks. Upgrading software/hardware when needed to handle growing demands.
2. **Scalable Cloud Services:** Using more cloud services for storage, teamwork, and online learning tools such as Aula.
3. **Training & Development:** Providing training to IT staff to make sure they are professional in managing and maintaining network.
4. **Advanced Security Measures:** Monitoring network continuously and improving the security of the systems from potential threats. Using AI solutions to find the patterns of risks and issues which may arise.

By taking these steps, the university can ensure a reliable, modern network that supports learning, research while providing secure, efficient network infrastructure for all the users.

# References

Alam, M. (2023). UNIVERSITY NETWORK A Cisco Packet Tracer Showcase. [online] ResearchGate. Available at: https://www.researchgate.net/publication/376513199\_UNIVERSITY\_NETWORK\_A\_Cisco\_Packet\_Tracer\_Showcase.

Cisco (2025). Cisco Secure Firewall: First Line of Defense. [online] Cisco. Available at: https://www.cisco.com/site/uk/en/learn/topics/security/what-is-a-firewall.html.

Cisco. (n.d.). Networking Software (IOS & NX-OS) - Networking Software (IOS & NX-OS). [online] Available at: https://www.cisco.com/c/en\_uk/products/ios-nx-os-software/index.html.

Fitzgerald, J., Dennis, A. and Durcikova, A. (2017). Business data communications and networking. Hoboken, Nj: Wiley.

Leslie (2025). What is Three Tier Architecture in Switch Networking? [online] Qsfptek.com. Available at: https://www.qsfptek.com/qt-news/what-is-three-tier-architecture-in-switch-networking.html?srsltid=AfmBOoo2PQ60Kaj5\_hLWZr9C5Ql5mLpEUb\_nXGt\_YgXkwJLduTVGlLmg [Accessed 2 Apr. 2025].

Palmer, M.J. and Sinclair, R.B. (1999). Guide To Designing And Implementing Local And Wide Area Networks. Cambridge.

Rivon, S. (2019). Network Design and Specifications for a University. [online] Shashendra Rivon. Available at: https://rivon.home.blog/2019/09/08/network-design-and-specifications-for-a-university/.

S. Gillis, A. (n.d.). What is Cisco Identity Services Engine (ISE)? - Definition from WhatIs.com. [online] SearchMobileComputing. Available at: https://www.techtarget.com/searchmobilecomputing/definition/Cisco-Identity-Services-Engine-ISE.

Varne, P.N., J, P., V, S.S., K, T.A. and Gowda, N.C. (2023). Campus Network Design and Implementation using Cisco Packet Tracer. International Journal of Computational Learning & Intelligence, [online] 2(4), pp.163–168. doi:https://doi.org/10.5281/zenodo.10254264.

Wolf, T. and Dimitrios Serpanos (2011). Architecture of Network Systems (The Morgan Kaufmann Series in Computer Architecture and design). Morgan Kaufmann Publishers.