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** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Table of Contents**

1. Discussion and justification of proposed solution addressing user needs
   1. Discussion
   2. Justification
2. Discussion and justification of proposed hardware
   1. Discussion
   2. Justification
3. Discussion and justification of proposed software
   1. Discussion
   2. Justification
4. Discussion and justification of proposed network circuits
   1. Discussion
   2. Justification
   3. Network Diagrams
5. Discussion and justification of proposed cloud-based services
   1. Discussion
   2. Justification
6. Discussion and justification of proposed detailed costings
   1. Discussion
   2. Justification
   3. Table of Detailed Costings
7. Conclusions & future recommendations
   1. Conclusions
   2. Future Recommendations

# Introduction

# 1. Proposed Solution Addressing User Needs

## 1.1 Discussion

This section outlines a modern, scalable network design for the two new buildings (Building 1 and Building 2) at the University of the West of Scotland (UWS). The system aims to provide seamless connectivity for administrative staff, academics, and students while balancing their requirements for performance, security, and future growth.

**Networking Floors within Each Building**

Every building 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 will provide secure wired internet connections in their offices. Since they handle important university data, their network will be kept separate from others to prevent unauthorized access. We will also install backup power systems to make sure their work is never interrupted.
* **First and Second Floor:** These floors are mainly used for academic activities, including lecture halls, tutorial rooms, and computer labs. Each floor will use managed switches to provide wired connections for devices like desktops and lab equipment. Wi-Fi 6 access points (APs) will offer fast wireless connectivity for laptops, tablets, and smartphones used by students and staff. The network will support digital learning tools, online resources, and collaboration platforms for multiple users at the same time.

**Connecting the Two Buildings**

To enable effective collaboration and resource sharing between both buildings, a high-performance inter-building network link is crucial. Our solution utilizes fibre optic cabling to interconnect the facilities. This technology provides distinct benefits such as exceptional bandwidth capacity, minimal latency, and long-term scalability.

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

**Integrating Building with Network**

The new buildings need to connect smoothly to the university’s existing network. This will let 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 supports easy upgrades, allowing bandwidth and capacity to expand as needed without major redesigns.
* **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 delivers fast, secure connectivity for all users while supporting future growth. It balances performance and security with scalable infrastructure. The design meets current needs and adapts to emerging technologies.

* **Administrative Staff Offices:** The dedicated wired connections and isolated VLAN ensure secure, uninterrupted access to sensitive systems like student records and financial data. Redundant power and network paths prevent disruptions to critical operations. Strict access controls protect confidential information while maintaining high-speed performance.
* **Academics Offices**: High bandwidth wired/Wi-Fi 6E connectivity supports research data transfers and hybrid teaching tools. Quality of Service prioritizes video calls and cloud collaboration platforms. Future-ready multi-gigabit ports accommodate evolving academic workloads.
* **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 collaboration with low-latency screen sharing. Wired ports for tutors enable stable connections to presentation 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 simulations. Each workstation gets dedicated bandwidth to prevent slowdowns during class activities. The system supports quick software deployments and secure logins for students and instructors.
* **Future Needs:** The proposed network is designed to scale effortlessly as user demands grow, with modular infrastructure that adapts to emerging 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 smoothly while making it easy to upgrade later. The system works perfectly today but is also ready for future improvements.

# 2. Proposed Hardware

## 2.1 Discussion

Choosing the right hardware is very important to make sure the network works well in the new Buildings 1 and 2 at UWS. This section talks about the main hardware devices we will use and why we selected them. The network will follow the standard 3-layer design (core, distribution, and access) for better performance.

**Core Switches**

To manage the university's high-volume data traffic with minimal delay, we require powerful core switches capable of handling heavy workloads. The Cisco Catalyst 9500 Series is ideal for this role, offering superior routing functions, exceptional data transfer speeds, and compatibility with multiple network standards.

* **Cisco Catalyst C9500-48Y4C** is a high-performance core switch designed for enterprise networks, featuring 48x 25G/10G ports and 4x 100G uplinks for ultra-fast data transfer.



Fig 2.1

**Distribution Switches**

The distribution layer utilizes high-performance switches like the Cisco Catalyst 9300 Series to consolidate traffic from access switches and link to the core. These switches enable fast uplink speeds, QoS prioritization for critical applications, and VLAN-based network segmentation. Their scalable design ensures efficient traffic flow between layers while supporting advanced campus-wide features.

* **Cisco Catalyst C9300-48UXM** offers 48 multi-gigabit ports (up to 10G) with PoE++ support and 100G uplinks, ideal for bandwidth-heavy areas like lecture halls and labs. Its StackWise-480 technology provides seamless scalability for growing networks.

A white device with many ports

AI-generated content may be incorrect.

Fig 2.2

**Access Switches**

For connecting computers, phones, and Wi-Fi access points, we use Cisco Catalyst 9200 switches. These switches provide Power over Ethernet (PoE) to run devices like wireless access points and IP phones without extra power cables. They are simple to manage and work well for classrooms, labs, and offices.

* **Cisco Catalyst C9200L-48P-4X-A** has 48 PoE ports to support devices like Wi-Fi 6 access points and IP phones, plus 4 high-speed uplinks for fast data transfer. It’s perfect for areas needing both power and strong network performance.

A close-up of a device

AI-generated content may be incorrect.

Fig 2.3

**Firewalls**

To protect the entire network, we use advanced firewalls like Cisco Firepower at the core layer. These firewalls block cyber threats, prevent attacks, and inspect all data traffic for safety. They keep the network secure while maintaining fast performance for all users.

* **Cisco FPR2130-ASA-K9 Firepower** is a powerful firewall that protects large networks like universities from cyber threats. It combines Cisco ASA security with Firepower threat detection to block attacks in real-time while supporting fast VPN access. Ideal for 1000+ users, it integrates smoothly with the existing Cisco switches and future upgrades.

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 delivers blazing speeds up to 3.5Gbps using the 6GHz band. It effortlessly 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 wired connections in offices and classrooms, supporting 10Gbps speeds and PoE++ for devices like Wi-Fi access points. Fiber optic cables (OS2) will link buildings and server rooms for high-speed, long-distance connections. This hybrid approach balances cost, 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 reliable wired networks. Its shielded 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 fiber optic cable supports 10Gbps to 100Gbps speeds over 10km+, ideal for connecting buildings. The tight-buffered design makes it durable 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'll deploy rack-mounted Dell PowerEdge servers with high-performance processors and SSD storage to handle academic databases, virtual labs, and shared resources. These servers will ensure 24/7 uptime with redundant power and cooling for critical university operations.

* **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 deploy UPS systems to protect servers, switches, and critical hardware from power outages, ensuring 24/7 uptime and safe shutdowns during failures.

**Eaton 9PX 2000VA 1800W 120V Online** is high-efficiency online UPS delivers 1800W/2000VA pure sine wave power, ensuring 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:** High-volume enterprise printers will be installed in admin offices and labs for staff/student use, supporting secure, networked printing with user authentication to reduce waste.
* **IP Phones:** Cisco IP phones (PoE-powered) will provide crystal-clear voice calls across campus, integrated with your network for seamless internal communication.

## 2.2 Justification

**Core Switches**

Core switches are the backbone of the network, connecting all buildings and handling 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 advanced features, like redundancy and scalability, prevent 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 separate 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 provides 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 prevent 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 deliver 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. Provides 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.

# 2. Proposed Software

**2.1 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.

**2.2 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 offers secure remote access for staff and students, encrypting data even on public Wi-Fi. It’s included with your Cisco firewall license, avoiding extra costs, and features one-click login for easy use. Military-grade encryption and malware blocking add extra layers of protection.

**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.

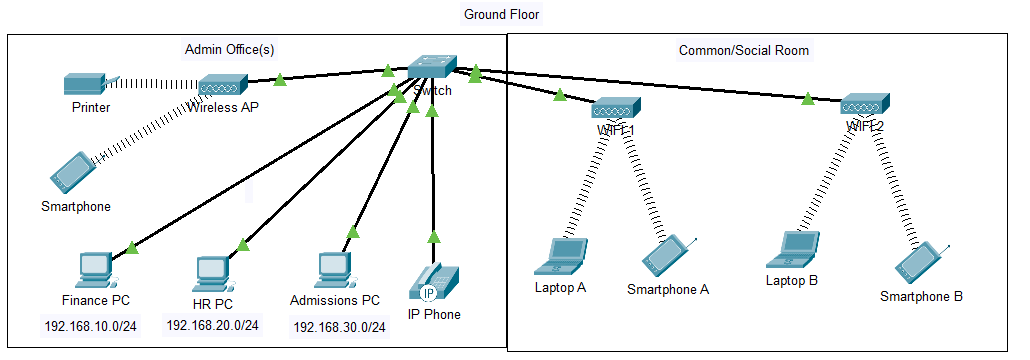


Fig 4.2 Image of Ground Floor in Packet Tracer

**First Floor**

ssd

Servers: 2x Dell PowerEdge R740 512GB ram 2 Xeon gold 14 core 1TB SSD cache. each cost 1500 pound. Seagate Exos X16 16TB HDD x4, each cost 350 pound.