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** | **TOTAL MARK** |
| **Maultice Appiah-Sae** | **B01657566** |  |
| **Emmanuel Etse Kudalor** | **B01733081** |  |
| **Ali Mirzaei** | **B01662151** |  |
| **Eta Besong Emmanuel** | **B01649696** |  |
|  |  |  |
|  |  |  |

**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

The University of The West of Scotland is expanding its infrastructure with the addition of two new buildings on its campus. These buildings are designed to accommodate the needs of administrative staff, academics, and students, particularly those in the School of Computing, Engineering, and Physical Sciences. The primary function of these buildings will be to provide offices for administrative staff, classrooms for lectures and tutorials, and computer labs for practical learning activities. However, despite their state-of-the-art design, these buildings currently lack the necessary network infrastructure to support their intended use. This report aims to present a comprehensive networking solution to address this gap, focusing on three critical aspects: networking the floors within each building, connecting the two buildings to each other, and integrating the buildings with the rest of the University network.

The challenge at hand is multifaceted. Internally, each building must have a robust network that connects all floors efficiently, ensuring seamless communication and resource sharing between different levels. Externally, the two buildings need a reliable connection to each other to facilitate inter-building collaboration and resource access. Finally, both buildings must be integrated into the existing University network to ensure cohesive operations, access to shared resources, and connectivity to the wider internet.

Given the rapid pace of technological advancement, it is imperative that the proposed network solution is both current and future-proof. This means adopting the latest networking technologies and anticipating the needs of the University over the next five years. The proposed solution will leverage high-speed wired and wireless connections, modern security protocols, and scalable cloud-based services to ensure that the network remains reliable, secure, and capable of handling increasing data demands.

In developing this proposal, we have considered the specific requirements of different user groups. Administrative staff need secure and reliable network access for financial transactions, human resources activities, and admissions processing. Academics require a stable and high-speed network for research, teaching, and collaboration, both within the University and with external partners. Students, on the other hand, depend on robust internet access for online resources, virtual learning environments, and lab activities.

This report is structured to provide a detailed overview of the proposed networking solution. It begins with a discussion of user needs and justifications for the proposed approach. Following this, we delve into the specifics of the hardware and software required to implement the solution. Detailed network circuit designs will be presented, with a focus on how they will connect the floors within each building, link the two buildings to each other, and integrate them with the existing University network. Network diagrams will be included to illustrate the layout and connectivity.

We also explore the role of cloud-based services in enhancing the network's capabilities and flexibility. These services will provide scalable storage, applications, and backup solutions that are essential for modern academic and administrative functions.

Cost considerations are an integral part of this proposal. We provide a thorough cost analysis, ensuring that the project stays within budget while meeting all user requirements. This analysis will include a breakdown of costs for hardware, software, network circuits, and cloud services.

The report concludes with a summary of the proposed solution and recommendations for future network upgrades and enhancements. By adopting a proactive approach to network management and staying abreast of technological advancements, the University of The West of Scotland can ensure that its new buildings are not only well-connected today but also ready to meet the challenges of tomorrow.

In summary, this report aims to provide a comprehensive and future-proof networking solution for the University of The West of Scotland's new buildings. It addresses the immediate connectivity needs of administrative staff, academics, and students while also considering the long-term requirements of a modern educational institution. By implementing the proposed solution, the University will be well-equipped to support its academic and administrative functions, fostering an environment of collaboration, innovation, and excellence.

# 1. Proposed Solution Addressing User Needs

## 1.1 Discussion

The network solution for the University of The West of Scotland's two new buildings must cater to the diverse needs of administrative staff, academics, and students. This section discusses how the network will be designed to meet these needs, ensuring robust, high-speed connectivity and future scalability.

**Networking Floors within Each Building**

Each building has three floors, with various facilities and user groups on each level. To ensure seamless connectivity within each building, we propose a combination of high-speed wired and wireless networking solutions.

* **Ground Floor:** The ground floor houses 20 administrative staff and a social/common room with a capacity of 50. For this floor, we will install wired connections to ensure reliable and secure network access for administrative tasks. Wireless access points (APs) will be strategically placed to provide comprehensive Wi-Fi coverage, especially in the common room, to support mobile devices and guest access.
* **First and Second Floors:** These floors are primarily dedicated to academics, lecture classrooms, tutorial classrooms, and computer labs. Each floor will have managed network switches to provide wired connections for fixed devices like desktops and lab equipment. Additionally, Wi-Fi 6 APs will be deployed to ensure high-speed wireless connectivity for laptops, tablets, and smartphones used by students and staff. The network infrastructure will support the simultaneous use of digital learning tools, online resources, and collaborative platforms.

**Connecting the Two Buildings**

To facilitate collaboration and resource sharing between the two new buildings, a high-speed inter-building network connection is essential. We propose using fiber optic cables to link the buildings. Fiber optic technology offers several advantages, including high bandwidth, low latency, and future scalability.

* **Fiber Optic Backbone:** A fiber optic backbone will be laid between the two buildings, providing a dedicated and high-capacity link. This connection will support high-speed data transfer, video conferencing, and real-time collaboration tools used by both buildings.
* **Redundancy and Reliability:** To ensure network reliability, we will implement redundant fiber paths. This redundancy will help maintain network uptime in case of a single point of failure, ensuring continuous connectivity between the buildings.

**Integrating Buildings with the University Network**

The new buildings must be seamlessly integrated with the existing University network to provide access to shared resources, administrative systems, and the internet. This integration will be achieved through a combination of hardware and software solutions.

* **Core Routers and Switches:** High-performance core routers and switches will be installed to connect the new buildings to the University’s main network. These devices will manage network traffic efficiently and provide the necessary routing capabilities for data exchange between the buildings and the broader campus network.
* **Virtual Private Network (VPN):** A VPN will be established to secure the data transfer between the new buildings and the University network. This setup will ensure that sensitive information, such as administrative data and academic research, is protected from external threats.
* **Network Segmentation:** To enhance security and manage network traffic effectively, we will implement network segmentation. Different user groups (administrative staff, academics, and students) will have separate network segments, each with tailored security policies and bandwidth allocations.

**Future-Proofing the Network**

Considering the rapid pace of technological advancements and increasing data demands, the proposed network solution is designed to be future-proof.

* **Scalable Infrastructure:** The network infrastructure will be scalable, allowing for easy upgrades and expansions. Additional APs, switches, and routers can be added as needed to accommodate growing user numbers and new technologies.
* **Adoption of Emerging Technologies:** The network design will be flexible enough to integrate emerging technologies, such as Internet of Things (IoT) devices, advanced security measures, and new communication tools.

**1.2 Justification**

The proposed network solution is justified by the specific needs of various user groups within the University buildings and the requirement for a robust, scalable, and secure network infrastructure.

* **Administrative Staff Offices:** The administrative staff need reliable and secure network access for handling sensitive information related to financial transactions, HR activities, and admissions processing. Wired connections in their offices ensure stable and secure access, while network segmentation provides an additional layer of security by isolating administrative traffic from other network traffic.
* **Academics Offices:** Academics require high-speed and stable network connections for research, teaching, and collaboration. The proposed wired and wireless networks on the first and second floors, combined with high-capacity inter-building links, ensure that academics can seamlessly access online resources, communicate with colleagues, and conduct research activities.
* **Social/Common Room:** The social/common room on the ground floor will benefit from comprehensive Wi-Fi coverage, supporting the connectivity needs of up to 50 users. This area will serve as a hub for social interactions and informal meetings, where staff and students can access the internet and University resources using their mobile devices.
* **Lecture Classrooms:** Lecture classrooms require robust wireless connectivity to support large numbers of students accessing online learning materials, digital whiteboards, and interactive platforms simultaneously. The deployment of Wi-Fi 6 APs ensures that these classrooms have the capacity to handle high-density usage without performance degradation.
* **Tutorial Classrooms:** Similar to lecture classrooms, tutorial classrooms need reliable wireless access for small group activities and collaborative learning. Wi-Fi 6 technology ensures that students and tutors can engage with digital tools and resources without connectivity issues.
* **Computer Labs:** Computer labs require high-speed wired connections to support intensive computing tasks and access to specialized software. Managed network switches with high port density will be installed in these labs to ensure that all computers have stable and high-speed network access. Additionally, Wi-Fi coverage in the labs will support the use of mobile devices and allow for flexible learning environments.
* **Future Needs:** The scalable and flexible design of the network ensures that it can accommodate future technological advancements and increasing data demands, providing a sustainable solution for the next five years and beyond.

By addressing the specific needs of each user group and facility, the proposed network solution ensures that the University of The West of Scotland’s new buildings are equipped to support administrative functions, academic activities, and student learning. The combination of high-speed wired and wireless networks, secure inter-building connections, and integration with the University’s main network provides a comprehensive and future-proof solution. This approach fosters an environment of collaboration, innovation, and excellence, meeting the University's needs for the next five years and beyond.

**2. Proposed Hardware**

**2.1 Discussion**

The selection of appropriate hardware is critical to ensuring the efficiency, reliability, and scalability of the proposed network solution for the University of The West of Scotland’s new Buildings 1 and 2. This section discusses and justifies the hardware components that will be utilized in the network infrastructure, aligning with the hierarchical 3-tier model design.

**Core Layer Hardware**

**Core Switches:**

For the core layer, high-performance core switches are essential to handle large volumes of data traffic with low latency. Core switches, such as the Cisco Catalyst 9500 Series, are chosen for their advanced routing capabilities, high throughput, and support for a wide range of network protocols. These switches provide the necessary backbone connectivity and ensure the network's high availability and redundancy.

* **Cisco Catalyst 9500 Series:** Offers advanced features like high-density 10/25/40/100 Gigabit Ethernet ports, modular design for scalability, and support for advanced routing protocols ( OSPF, BGP).



*Image 1: Cisco Catalyst 9500 Series*

**Firewalls:**

Next-generation firewalls (NGFWs) are deployed at the core layer to provide comprehensive security. Devices like the Cisco Firepower Series offer advanced threat protection, intrusion prevention, and deep packet inspection, ensuring the network's security and integrity.

* **Cisco Firepower Series:** Provides comprehensive threat defense, including intrusion prevention, advanced malware protection, and detailed threat intelligence.



*Image 2: Cisco Firepower Series*

**Distribution Layer Hardware**

**Distribution Switches:**

At the distribution layer, robust and scalable distribution switches, such as the Cisco Catalyst 9300 Series, are used to aggregate traffic from the access layer and provide interconnectivity to the core layer. These switches support high-speed uplinks and advanced features like Quality of Service (QoS) and VLAN segmentation.

* **Cisco Catalyst 9300 Series:** Designed for high performance and flexibility in medium to large enterprise networks, offering stackability, PoE+ support, and advanced security features.



*Image 3: Cisco Catalyst 9300 Series*

**Access Layer Hardware**

**Access Switches:**

For the access layer, switches like the Cisco Catalyst 9200 Series are selected. These switches connect end devices to the network and provide features like Power over Ethernet (PoE), necessary for powering devices like IP phones and wireless access points.

* **Cisco Catalyst 9200 Series:** Offers robust performance, PoE support, easy management through intuitive interfaces, and enhanced security features.



*Image 4: Cisco Catalyst 9200 Series*

**Wireless Access Points (WAPs):**

To provide wireless connectivity throughout the buildings, high-performance WAPs such as the Cisco Aironet 2800 Series are deployed. These devices support the latest Wi-Fi standards (Wi-Fi 6) and offer high throughput and coverage.

* **Cisco Aironet 2800 Series:** Known for its excellent performance, scalability, and reliability, supporting high-density environments and advanced security protocols.

  
*Image 5: Cisco Aironet 2800 Series*

**End Devices and Additional Hardware**

**End Devices:**

End devices such as computers, printers, and IP phones will be connected to the access switches. These devices must be reliable and capable of handling the daily operational needs of administrative staff, academics, and students.

* **Enterprise-Grade Computers:** High-performance desktops and laptops from reputable manufacturers ensure reliability and compatibility with advanced network features.
* **Printers and IP Phones:** Reliable and high-performance printers and IP phones from trusted manufacturers support daily administrative and academic activities.

**servers**

* **Dell PowerEdge R740 Servers:** These on-premise servers are equipped with Intel Xeon Scalable processors, offering high performance and flexibility. They support server virtualization technologies, allowing multiple virtual servers to run on a single physical server. This capability maximizes resource utilization and reduces hardware costs. These servers will host critical applications, academic databases, and local file storage.



*Image6: Dell PowerEdge R740 Servers*

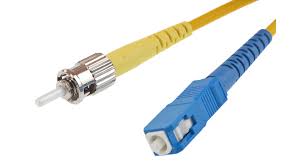
**Cabling Infrastructure**

* **Cat6a Ethernet Cabling:** This cabling supports 10 Gigabit Ethernet over longer distances compared to Cat5e or Cat6 cables, ensuring high-speed and stable connections for wired devices. It is suitable for the extensive internal network requirements of the new buildings.



*Image 7: Cat6a*

* **Single-Mode Fiber Optic Cables:** For the backbone connection between the two buildings and to the University network, single-mode fiber optic cables will be used. These cables provide higher bandwidth, longer transmission distances, and better resistance to electromagnetic interference, making them ideal for high-capacity inter-building links.



*Image 8: Cat6a*

**UPS (Uninterruptible Power Supply):**

To protect network equipment from power outages and ensure continuous operation, UPS systems like the APC Smart-UPS series are used. These systems provide backup power and protect against power surges and spikes.

* **APC Smart-UPS 1000VA:** Offers reliable backup power, protecting critical network hardware from power disturbances, ensuring network services remain available during power interruptions.



*Image 8: APC Smart-UPS 1000VA*

## 2.2 Justification

**Core Layer Hardware**

**Core Switches:**

The Cisco Catalyst 9500 Series is an industry-leading core switch designed for enterprise networks. It offers advanced features like high-density 10/25/40/100 Gigabit Ethernet ports, modular design for scalability, and support for advanced routing protocols ( OSPF, BGP). Its robust hardware ensures maximum uptime and performance, which is crucial for the core layer. The high throughput and low latency provided by these switches are essential for handling large volumes of data traffic, ensuring a reliable and efficient network backbone.

**Firewalls:**

Next-generation firewalls (NGFWs) such as the Cisco Firepower Series are essential for protecting the network from sophisticated cyber threats. These devices offer integrated security features, such as application awareness, user identity management, and advanced malware protection, which are critical for safeguarding sensitive university data and maintaining network security. Their advanced threat protection and deep packet inspection capabilities ensure comprehensive security for the core network layer.

**Distribution Layer Hardware**

**Distribution Switches:**

The Cisco Catalyst 9300 Series switches are designed for high performance and flexibility in medium to large enterprise networks. They offer features like PoE+ support for connected devices, and advanced security features, making them suitable for handling the diverse needs of the distribution layer. These switches ensure reliable and high-speed connectivity, supporting the aggregation of traffic from the access layer and providing seamless interconnectivity to the core layer.

**Access Layer Hardware**

**Access Switches:**

The Cisco Catalyst 9200 Series switches are ideal for access layer deployments. They offer robust performance, PoE support, easy management through intuitive interfaces, and enhanced security features. These switches ensure reliable connectivity for end-user devices and simplify network management and troubleshooting. Their PoE capabilities are essential for powering devices like IP phones and wireless access points, reducing the need for additional power sources and simplifying installation.

**Wireless Access Points (WAPs):**

The Cisco Aironet 2800 Series is known for its excellent performance, scalability, and reliability. They support high-density environments, advanced security protocols, and seamless roaming, ensuring robust wireless connectivity for students and staff. These WAPs provide high throughput and coverage, supporting the increasing demand for wireless access in classrooms, common areas, and administrative offices.

**End Devices and Additional Hardware**

**End Devices:**

Reliable and high-performance end devices are necessary for maintaining productivity and ensuring seamless network connectivity. Selecting enterprise-grade computers, printers, and IP phones from reputable manufacturers ensures compatibility, longevity, and support for advanced network features. These devices support the daily operational needs of administrative staff, academics, and students, providing a stable and efficient work environment.

**UPS (Uninterruptible Power Supply):**

The APC Smart-UPS series offers reliable backup power, protecting critical network hardware from power disturbances. This ensures that network services remain available during power interruptions, safeguarding data integrity and minimizing downtime. The use of UPS systems is crucial for maintaining continuous operation and protecting network equipment from power surges and spikes.

By selecting and deploying these carefully chosen hardware components, the proposed network solution will provide a robust, high-performance, and scalable infrastructure for the University of The West of Scotland’s new Buildings 1 and 2. This hardware will support the diverse needs of administrative staff, academics, and students, ensuring reliable and secure network connectivity throughout the campus.

# 3. Proposed Software

## 3.1 Discussion

Selecting the appropriate software components is crucial for ensuring the efficient operation, security, and management of the University of The West of Scotland’s new network infrastructure in Buildings 1 and 2. This section discusses the proposed software solutions that will be implemented across the network layers to ensure seamless connectivity, robust security, efficient management, reliable backup and recovery, antivirus protection, and secure remote access.

**Network Operating System (NOS)**

**Cisco IOS-XE**

Cisco IOS-XE will serve as the network operating system (NOS) for the Cisco Catalyst switches deployed across the core, distribution, and access layers. IOS-XE provides a unified software image that supports advanced features such as high availability, enhanced security, and comprehensive network management. Its programmability capabilities through APIs enable automation and orchestration of network operations, improving operational efficiency and scalability.

**Network Security Software**

**Palo Alto Networks PAN-OS**

Palo Alto Networks' PAN-OS will be deployed on next-generation firewalls to ensure robust network security against evolving cyber threats. PAN-OS integrates advanced threat detection and prevention services, including intrusion prevention system (IPS), malware protection, URL filtering, and application control. This comprehensive security suite provides continuous protection and real-time threat intelligence updates, enhancing the network's security posture.

**Network Monitoring and Management**

**SolarWinds Network Performance Monitor (NPM)**

SolarWinds NPM will function as the network monitoring tool, providing detailed insights into network performance, availability, and health. NPM offers real-time visibility, advanced alerting, and reporting capabilities. It integrates with various network devices, enabling administrators to proactively monitor network conditions, troubleshoot issues, and optimize performance across Buildings 1 and 2.

**Wireless Management**

**Aruba ClearPass**

Aruba ClearPass will manage and secure wireless access across the campus, ensuring policy-based control and identity services for wired, wireless, and VPN networks. ClearPass centralizes authentication, authorization, and accounting (AAA) services, enforcing consistent access policies based on user identities, device types, and contextual attributes. It integrates with Aruba's wireless infrastructure to provide enhanced visibility and control over network access, facilitating compliance with regulatory requirements and organizational policies.

**Backup and Recovery Software**

**Veeam Backup & Replication**

Veeam Backup & Replication will provide backup and recovery capabilities for the network configurations and critical data. It offers comprehensive data protection, ensuring that network settings and organizational data are securely backed up and can be restored quickly in the event of a disruption. Veeam’s solution supports various recovery options, minimizing downtime and ensuring data integrity and availability.

**Antivirus Software**

**Symantec Endpoint Protection**

Symantec Endpoint Protection will be deployed across all network endpoints, including administrative staff and academic offices, lecture classrooms, tutorial classrooms, and computer labs. This software provides comprehensive antivirus protection, including real-time malware detection, threat analysis, and automatic updates. It helps protect against viruses, worms, Trojan horses, and other malicious software.

**Virtual Private Network (VPN)**

**Fortinet FortiClient**

Fortinet FortiClient will be implemented to provide secure remote access for staff and students. This VPN solution supports various operating systems and devices, ensuring secure connectivity to the university network from remote locations. FortiClient offers features like multi-factor authentication, endpoint posture enforcement, and secure tunneling, enhancing the security of remote access connections.

## 3.2 Justification

**Network Operating System (NOS)**

**Cisco IOS-XE**

Cisco IOS-XE is selected for its reliability, scalability, and comprehensive feature set, ensuring consistent operations across all Cisco Catalyst switches. It supports advanced routing protocols, high-density Ethernet ports, and modular design for scalability, meeting the university's current and future network requirements. The programmability features of IOS-XE enable automation and integration with third-party applications, enhancing operational efficiency and enabling rapid service deployment.

**Network Security Software**

**Palo Alto Networks PAN-OS**

Palo Alto Networks PAN-OS provides robust protection against advanced cyber threats with its integrated security features and real-time threat intelligence updates. It offers comprehensive threat prevention, including malware protection and advanced intrusion detection capabilities, ensuring continuous security monitoring and proactive threat mitigation. PAN-OS’s unified management interface simplifies security policy enforcement and incident response, bolstering the overall security posture of the university's network infrastructure.

**Network Monitoring and Management**

**SolarWinds Network Performance Monitor (NPM)**

SolarWinds NPM enhances network visibility and management through its detailed insights into network performance and health. It reduces operational complexity by providing real-time monitoring, advanced alerting, and comprehensive reporting. NPM’s integration with various network devices supports scalability and future network expansion, enabling administrators to optimize network operations and enhance user experience across Buildings 1 and 2.

**Wireless Management**

**Aruba ClearPass**

Aruba ClearPass ensures secure and efficient management of wireless access, enforcing policy-based controls and identity services. It enhances network security by authenticating and authorizing user access based on defined policies, thereby preventing unauthorized network access and ensuring compliance with regulatory requirements. ClearPass’s integration with Aruba’s wireless infrastructure provides comprehensive visibility and control over network access, supporting dynamic policy enforcement and maintaining a secure wireless environment.

**Backup and Recovery Software**

**Veeam Backup & Replication**

Veeam Backup & Replication offers automated backup and recovery capabilities for network configurations and critical data. It safeguards critical network settings and configurations, ensuring rapid restoration in the event of network disruptions or configuration errors. Veeam’s solution reduces downtime and operational risks by providing reliable backup solutions and maintaining data integrity and availability. This capability is essential for preserving network reliability and supporting uninterrupted network services for administrative staff, academics, and students.

**Antivirus Software**

**Symantec Endpoint Protection**

Symantec Endpoint Protection is essential for protecting network endpoints from malicious software. It offers real-time malware detection and prevention, automatic updates, and comprehensive threat analysis. Deploying this software across all network endpoints ensures robust protection against viruses, worms, and other malicious software, safeguarding the integrity and security of the university's network and data.

**Virtual Private Network (VPN)**

**Fortinet FortiClient**

Fortinet FortiClient is chosen for its ability to provide secure remote access to the university network. It supports various devices and operating systems, ensuring seamless connectivity for staff and students working remotely. FortiClient's features, such as multi-factor authentication and endpoint posture enforcement, enhance the security of remote connections, protecting the network from unauthorized access and ensuring data confidentiality.

By integrating these software solutions into the network infrastructure of Buildings 1 and 2, the University of The West of Scotland establishes a robust, secure, and scalable network environment. The combination of Cisco IOS-XE, Palo Alto Networks PAN-OS, SolarWinds Network Performance Monitor, Aruba ClearPass, Veeam Backup & Replication, Symantec Endpoint Protection, and Fortinet FortiClient ensures efficient network operations, proactive threat management, reliable backup and recovery, comprehensive antivirus protection, and secure remote access, supporting the university’s mission of delivering high-quality education and administrative services effectively.

# 4. Proposed Network Circuits

## 4.1 Discussion

The University of The West of Scotland’s network design for Buildings 1 and 2 will adopt the Three-Tier Hierarchical Network Design model. This model consists of the Access Layer, Distribution Layer, and Core Layer, each serving distinct roles to ensure scalability, performance, and manageability. Below, we discuss how this model is applied to our network design.

**Three-Tier Hierarchical Network Design**

1. **Access Layer**

The Access Layer is responsible for providing end devices with network connectivity. This layer includes the network infrastructure on each floor of Buildings 1 and 2, connecting PCs, printers, IP phones, projectors, and wireless access points (WAPs) to the network.

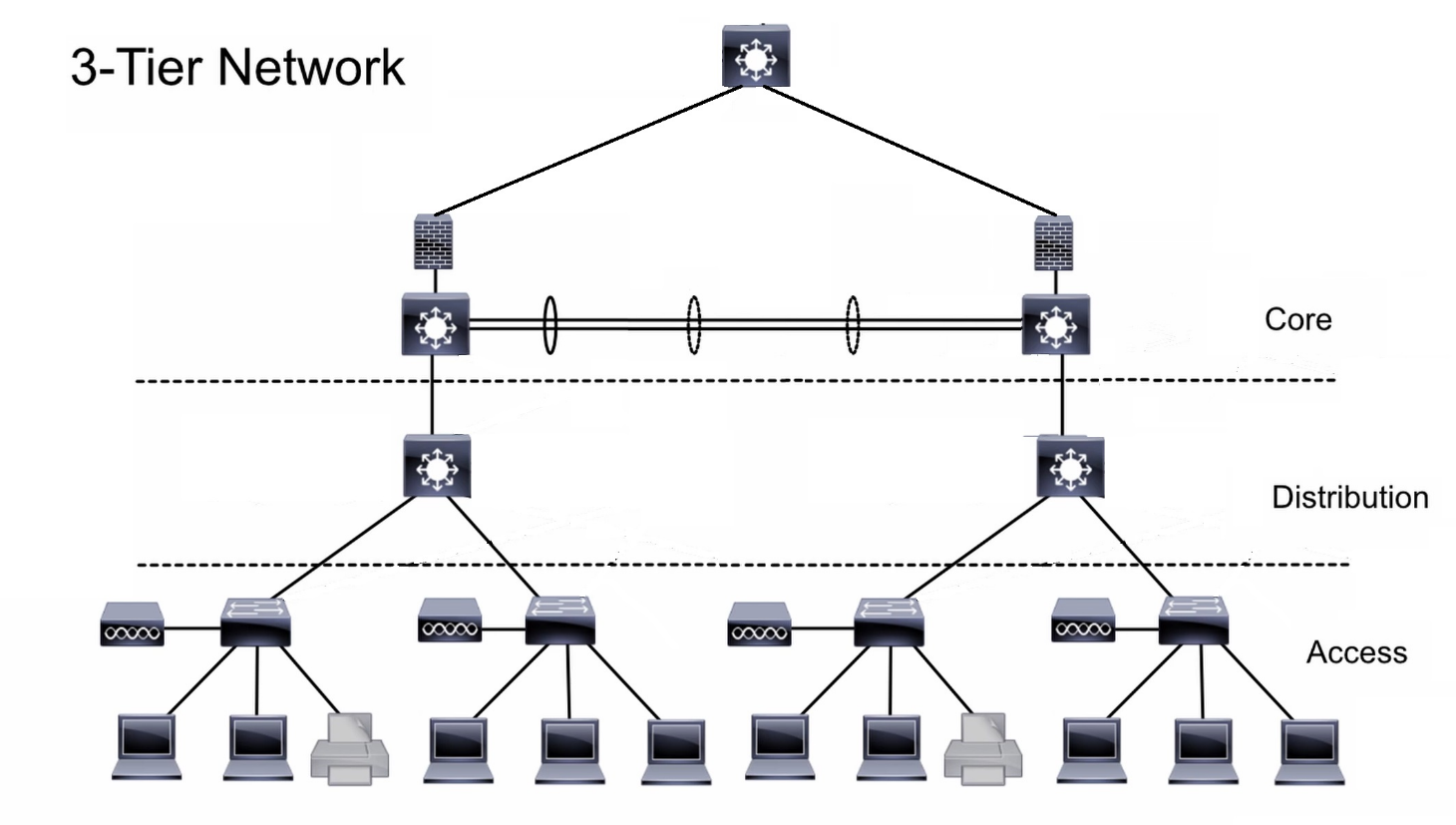


Figure 1: *Image depicting the basic view of our hierarchical design*

**Ground Floor (Administrative Staff Offices and Common Room)**

**Administrative Staff Offices**

The ground floor of each building is primarily dedicated to administrative staff offices, which we assume includes the finance, human resources (HR), and admissions departments. This segmentation allows for more efficient management, security, and network performance.

**1. Finance Computers**

The finance department consists of 10 computers, 1 network printer, and 10 IP phones. Each device is connected to a Cisco Catalyst 9200 Series Access Switch using Cat 6A cables. To ensure network security and proper traffic management, these devices are placed in a dedicated VLAN (VLAN 10 - Finance).

* **VLAN Configuration**: VLAN 10 is configured on the access switch to segregate finance traffic from other departments. This setup provides enhanced security and ensures that sensitive financial data remains isolated from other network traffic.
* **IP Addressing**: Devices in the finance VLAN are assigned IP addresses from a specific subnet, 192.168.10.0/24, ensuring organized and efficient IP management.
* **VPN Access**: Finance staff can securely access financial systems remotely through a VPN. Cisco AnyConnect is used to establish secure VPN connections, providing encrypted communication and ensuring data integrity.

**2. HR Computers**

The human resources department has 5 computers, 1 network printer, and 5 IP phones. These devices are connected to the same Cisco Catalyst 9200 Series Access Switch using Cat 6A cables but are placed in a different VLAN (VLAN 20 - HR).

* **VLAN Configuration**: VLAN 20 is configured to segregate HR traffic. This ensures that sensitive employee data is isolated and secure from other departments.
* **IP Addressing**: Devices in the HR VLAN use IP addresses from the 192.168.20.0/24 subnet.
* **Port Security**: Port security features are enabled on the switch ports connected to HR devices to prevent unauthorized access and protect sensitive data.

**3. Admissions Computers**

The admissions department includes 5 computers, 1 network printer, and 5 IP phones. These are connected to the Cisco Catalyst 9200 Series Access Switch via Cat 6A cables and placed in VLAN 30 (Admissions).

* **VLAN Configuration**: VLAN 30 segregates admissions traffic, enhancing network security and performance.
* **IP Addressing**: The admissions VLAN uses IP addresses from the 192.168.30.0/24 subnet.
* **Network Access Control (NAC)**: NAC policies ensure that only authorized admissions staff can access the network, protecting student data and admissions processes.

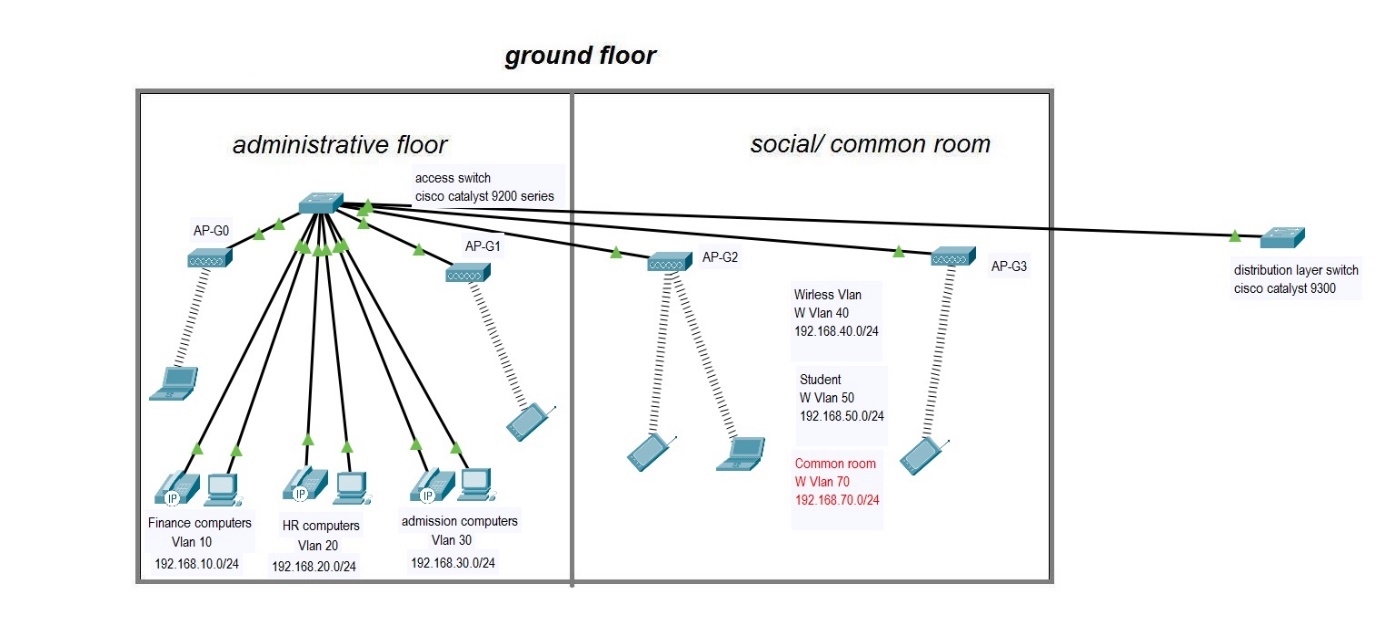
**Common Room**

The common room is designed to accommodate up to 50 people, providing a social and collaborative space for staff and students. It is equipped with 2 projectors and 2 wireless access points (WAPs).

**. Wireless Access Points (WAPs)**

The WAPs, such as the Cisco Aironet 2800 Series, provide seamless wireless connectivity throughout the common room. These WAPs are connected to the Cisco Catalyst 9200 Series Access Switch using Cat 6A cables with PoE.

* **SSID Configuration**: Multiple SSIDs are configured on the WAPs to separate network access for staff and students, enhancing security and network management.
* **Wireless VLANs (WVLAN)**: Different VLANs are assigned to each SSID (VLAN 40 for staff and VLAN 50 for students), ensuring secure and isolated wireless traffic.
* **IP Addressing**: Wireless devices are assigned IP addresses from distinct subnets (192.168.40.0/24 for staff, 192.168.50.0/24 for students and 192.168.150.0/24 for guest).

  
Figure 2: *Image of the ground floor design in packet tracer*

**First Floor (Academics Offices, Lecture and Tutorial Classrooms, Computer Labs)**

The first floor of Buildings 1 and 2 at the University of The West of Scotland is dedicated to academic activities, encompassing offices for academics, lecture classrooms, tutorial classrooms, and computer labs. Each area has distinct networking requirements that are addressed through a structured approach using strategically placed Ethernet switches and VLAN segmentation.

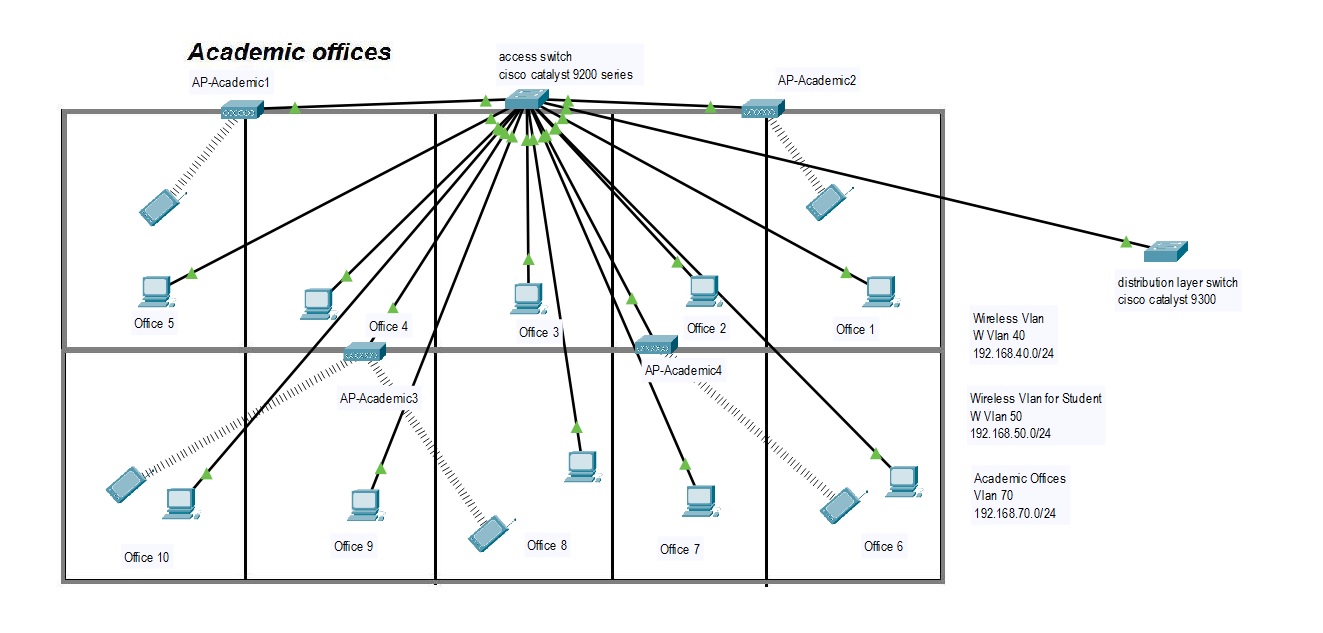
**Academics Offices**

The first floor includes offices for 10 academics. Each office will be equipped with two configured Ethernet ports to accommodate laptops or other devices used by academics. These ports are crucial for providing reliable and fast network connectivity, enabling academics to access university resources, conduct research, and communicate effectively.

**Network Configuration for Academics Offices**

To support the networking needs of the academics’ offices, one Cisco Catalyst 9200 Series switch will be dedicated. This switch is chosen for its robust performance, scalability, and support for advanced features.

* **Ports Allocation**:
  + **Configured Ethernet Lines**: 20 ports (2 per office for 10 offices)
  + **Remaining Ports**: 12 ports reserved for AP extensions and future expansion
* **VLAN Assignment**: Devices in the academics' offices will be segmented into VLAN 70 (Academics). VLAN segmentation ensures that traffic from these offices remains isolated, providing enhanced security and performance.
* **IP Addressing**: Devices in VLAN 70 will be assigned IP addresses from the 192.168.70.0/24 subnet, facilitating efficient network management.
* **Switch Ports Configuration**: The switch ports will be configured with Cat 6A cables to ensure high-speed connectivity and reliability. Port security measures will be implemented to prevent unauthorized access, safeguarding sensitive academic data.
* **VPN Access**: Academics will have secure VPN access to university resources, enhancing remote connectivity and collaboration.

  
Figure 3: *Image of the first floor academic offices with their separate switch design in packet tracer*

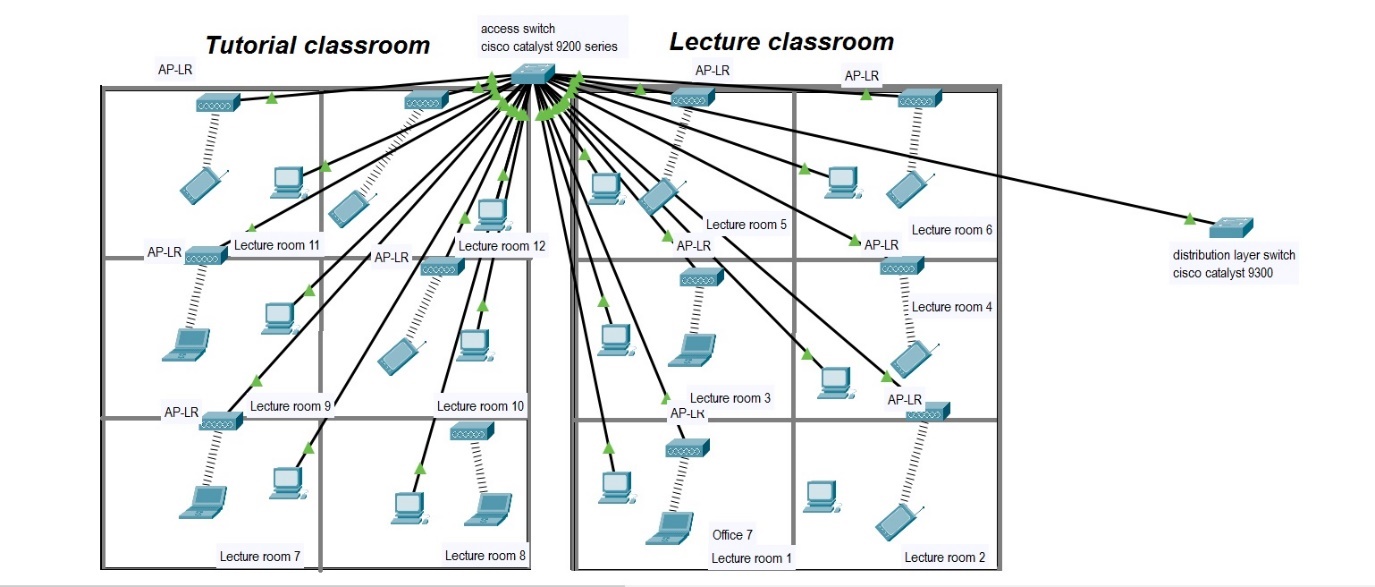
**Lecture and Tutorial Classrooms**

The first floor houses 6 lecture classrooms and 6 tutorial classrooms, each equipped with two configured Ethernet ports for connectivity purposes. These ports support devices used during lectures, tutorials, and academic presentations.

**Network Configuration for Lecture and Tutorial Classrooms**

A single Cisco Catalyst 9200 Series switch will be deployed to serve both lecture and tutorial classrooms. This switch is chosen for its ability to handle high-density environments and its advanced management capabilities.

* **Ports Allocation**:
  + **Configured Ethernet Lines**: 24 ports (2 per room for 12 rooms)
  + **Remaining Ports**: 8 ports reserved for AP extensions and future expansion
* **VLAN Assignment**: Lecture classrooms will be assigned to VLAN 80 (Lecture Classrooms) and tutorial classrooms to VLAN 90 (Tutorial Classrooms). VLAN segmentation ensures traffic isolation, enhancing security and performance.
* **IP Addressing**: Devices in VLAN 80 and VLAN 90 will receive IP addresses from the 192.168.80.0/24 and 192.168.90.0/24 subnets, respectively, facilitating effective network management.
* **Switch Ports Configuration**: Cat 6A cables will connect devices to the Cisco Catalyst 9200 Series switch ports, ensuring reliable and high-speed connectivity. Quality of Service (QoS) configurations will prioritize multimedia traffic for optimal performance during lectures and tutorials.

  
Figure 4: *Image of the ground floor design in packet tracer*

**Computer Labs**

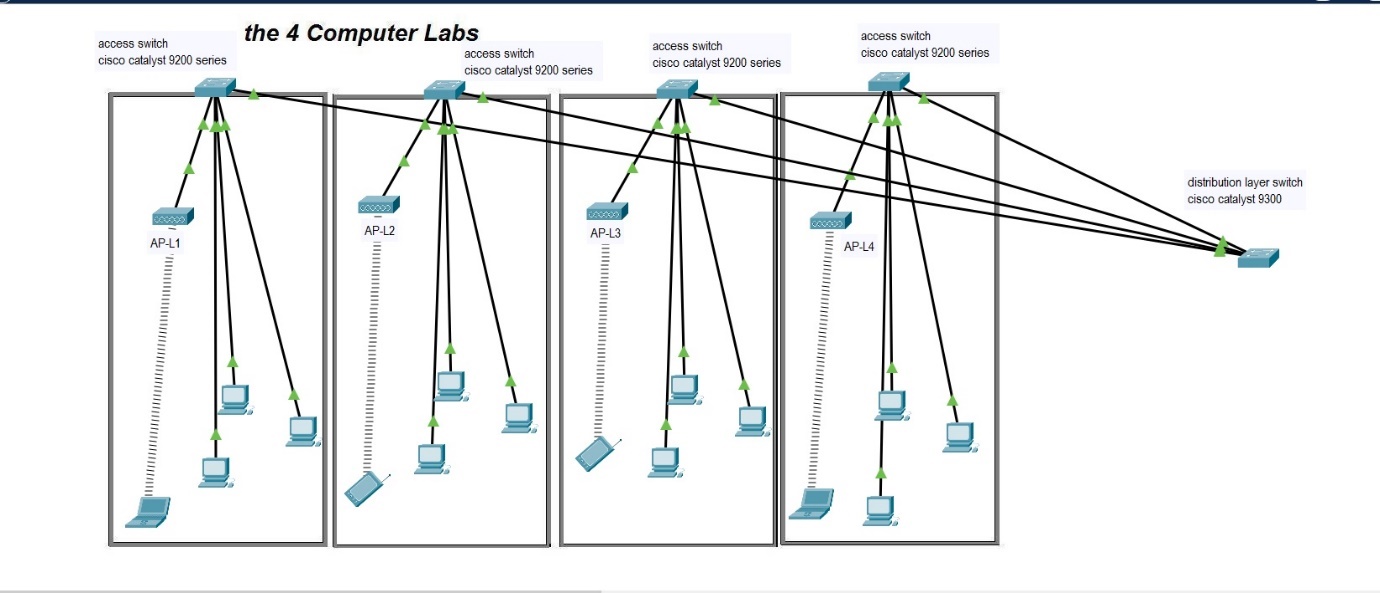
The first floor features 4 computer labs, each equipped with 20 PCs and one network printer. These labs provide students with essential resources for practical learning and research in computing.

**Network Configuration for Computer Labs**

Four Cisco Catalyst 9200 Series switches will be deployed, one for each computer lab. These switches are selected for their scalability, PoE support, and reliability.

* **Ports Allocation per Lab**:
  + **PCs**: 20 ports (each lab)
  + **Printers**: 1 port (each lab)
  + **Remaining Ports**: 11 ports reserved for AP extensions and future expansion (each lab)

The first floor network design for Buildings 1 and 2 at the University of The West of Scotland employs Cisco Catalyst 9200 Series switches and Cat 6A cables to ensure robust and secure connectivity. VLAN segmentation and IP addressing schemes enhance network performance and security, meeting the diverse needs of academics, lecture classrooms, tutorial classrooms, and computer labs effectively. This structured approach supports academic activities with reliable network infrastructure, promoting collaboration, learning, and research across the first-floor facilities.

  
Figure 5: *Image of the ground floor design in packet tracer*

**Second Floor (Academics Offices, Lecture and Tutorial Classrooms, Computer Classrooms)**

The network design for the second floor of Buildings 1 mirrors the approach used on the first floor. Therefore, we propose to use the same network design for the floor because the similarities and purposes intended for.

**Building 2**

For the design and features of Building 2 is are also similar and the intended purpose of these buildings upon completion will be same. In the nutshell, we propose to use same design implement in Building 1 for building 2 as well.

1. **Distribution Layer**

The Distribution Layer aggregates data from the access layer switches and provides connectivity to the core layer. This layer includes inter-building connectivity between Buildings 1 and 2. **Distribution Layer:**

**Inter-Building Connectivity**

To ensure robust inter-building connectivity between the two new buildings on the University of The West of Scotland campus, a star topology network design will be implemented. This design will utilize advanced networking hardware and fiber optic cables to facilitate high-speed, reliable communication and seamless data transmission.

**Deployment of Fiber Optic Cables**

The backbone of the inter-building connectivity will be established using single-mode fiber optic cables. These cables are selected for their ability to transmit data over long distances with minimal signal degradation, making them ideal for this purpose.

At the core of this network design are the Cisco Catalyst 9500 Series core switches. These high-performance switches will be installed in the main network rooms of each building, serving as the primary aggregation points for network traffic between the buildings. Their advanced features, such as high-density 10/25/40/100 Gigabit Ethernet ports, are crucial for ensuring reliable and high-speed backbone connectivity.

Within each building, Cisco Catalyst 9300 Series distribution switches will be deployed. These switches will be placed on each floor, aggregating traffic from the access layer devices and connecting to the core switches via the fiber optic cables. The Cisco Catalyst 9300 Series switches are chosen for their robust performance, scalability, and support for advanced network features like Quality of Service (QoS) and VLAN segmentation.

The network design will follow a star topology at the distribution layer. This means that each building’s network infrastructure will connect to a central point, the core switches, ensuring enhanced reliability and manageability. In this configuration, any issues in one segment will not affect the entire network, allowing for easier troubleshooting and maintenance.

In summary, the inter-building connectivity will be established by running single-mode fiber optic cables between the buildings, directly connecting the Cisco Catalyst 9500 Series core switches. Within each building, Cisco Catalyst 9300 Series distribution switches will aggregate the traffic from the access layer devices and link to the core switches through the fiber optic backbone. This star topology design ensures robust, high-speed connectivity, facilitating efficient communication, resource sharing, and seamless integration with the broader university network infrastructure.

1. **Core Layer**

The Core Layer provides high-speed data transport between distribution layer devices and connects the entire network to the broader university network.

**Core Layer Design**

The core layer will be constructed using high-performance Cisco Catalyst 9500 Series core switches. These switches are selected for their advanced routing capabilities, high throughput, and support for a wide range of network protocols. The Cisco Catalyst 9500 Series switches will be strategically placed in the university’s main data center, serving as the primary aggregation points for network traffic from the new buildings and other parts of the campus.

**Server connection**

This server will be connected to the core layer of the network using high-speed fiber optic cables, ensuring low latency and high reliability. The server will be equipped with advanced security measures, including encryption, access controls, and regular security updates. Additionally, it will be connected to the network through the Cisco Catalyst 9500 Series core switches, ensuring robust and secure connectivity. This setup will facilitate secure access to sensitive data for authorized users while maintaining data integrity and protection from unauthorized access. Regular backups will be conducted using Veeam Cloud Connect to ensure data redundancy and recovery in case of any incidents.

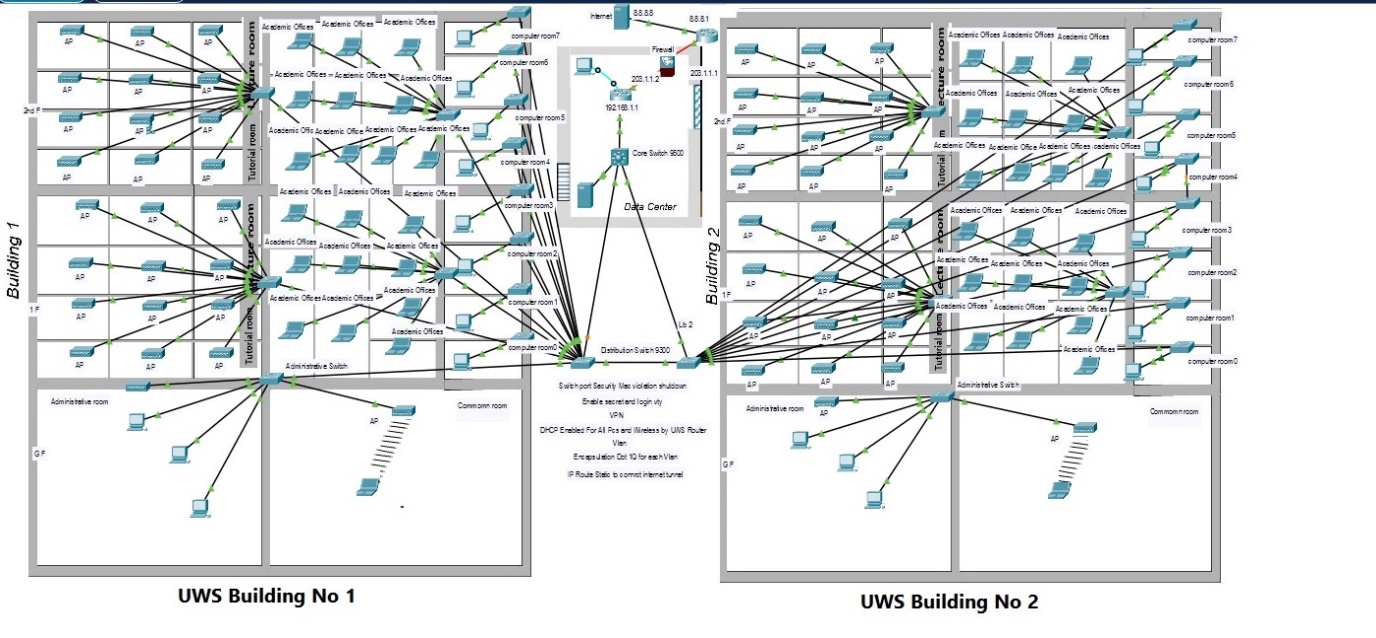
**Campus Connectivity**

To connect the new buildings to the main campus network, a high-speed fiber optic backbone will be utilized. Single-mode fiber optic cables will be used due to their ability to transmit data over long distances with minimal signal loss. These cables will ensure efficient and reliable data transmission between the new buildings and the main data center, supporting high-bandwidth applications and services.

Robust security measures will be implemented at the core layer to protect the network from potential threats. Next-generation firewalls (NGFWs) such as the Cisco Firepower Series will be deployed to provide comprehensive security features, including advanced threat protection, intrusion prevention, and deep packet inspection. These firewalls will monitor and secure all data passing through the core layer against cyber threats.

The core layer will follow a star topology design, where all distribution layer switches in the new buildings connect directly to the central core switches in the main data center. This topology ensures efficient management, optimal performance, and easier troubleshooting. The star topology, combined with redundant links and switches, will provide a stable and reliable network infrastructure.

In summary, the core layer will be built using Cisco Catalyst 9500 Series core switches, connected via a high-speed fiber optic backbone. Advanced firewalls will provide robust security. The core switches will integrate seamlessly with the existing university network, supporting high-speed, secure data transmission across the campus.



**5 Proposed Cloud-Based Services**

**5.1 Discussion**

As the University of The West of Scotland expands its campus with two new buildings, integrating modern cloud-based services becomes crucial to ensure scalability, reliability, and cost-effectiveness. These services will not only meet the current demands but also future-proof the network infrastructure for the next five years. Here’s a detailed look at the key cloud-based services we propose:

1. **Amazon Web Services (AWS) for Data Storage and Backup**
2. **Microsoft 365 for Collaboration Tools**
3. **Datadog for Network Monitoring**
4. **Aula for Learning Management Systems (LMS)**

**Amazon Web Services (AWS) for Data Storage and Backup**

Using AWS for data storage and backup is a smart move. AWS S3 (Simple Storage Service) offers an excellent solution for securely storing vast amounts of data. One of its biggest strengths is scalability. As the university's data grows, AWS S3 can seamlessly accommodate this increase without requiring additional physical infrastructure. Accessibility is another key advantage; data stored on AWS S3 can be accessed from anywhere, facilitating remote work and collaboration among staff and students. Plus, its pay-as-you-go pricing model means the university will only pay for the storage it uses, eliminating unnecessary hardware costs.

When it comes to backing up data, AWS Backup stands out. It provides automated backups, ensuring data is consistently saved without needing manual intervention. In the unfortunate event of a catastrophic failure, AWS Backup offers reliable disaster recovery, allowing for quick restoration of data. Additionally, it ensures data security by encrypting data both in transit and at rest, maintaining its integrity and confidentiality.

**Microsoft 365 for Collaboration Tools**

For enhancing collaboration and productivity, Microsoft 365 is an ideal choice. It includes Outlook and Exchange for robust email and calendar services, helping streamline communication and scheduling. Microsoft Teams is a powerful tool for video conferencing, supporting remote lectures, seminars, and meetings.

The Microsoft Office Suite (Word, Excel, PowerPoint) facilitates real-time document collaboration, enabling multiple users to work simultaneously, track changes, and revert to previous versions as needed. Microsoft SharePoint and OneDrive provide secure and efficient file-sharing capabilities, ensuring documents are easily and securely shared among users.

**Datadog for Network Monitoring**

To maintain the health and performance of the university's network, Datadog is a crucial tool. Datadog offers real-time insights into network performance metrics such as bandwidth usage, latency, and packet loss. Automated alerts and notifications for potential issues allow IT staff to respond quickly, preventing downtime. Detailed analytics and reporting capabilities also help in identifying trends and making data-driven decisions for network optimization.

For security monitoring, Datadog is invaluable. It identifies and responds to potential security threats in real-time, regularly scans for vulnerabilities, and provides recommendations for remediation. Additionally, it ensures compliance with industry standards and regulations through continuous monitoring and reporting.

**Aula for Learning Management Systems (LMS)**

Enhancing the learning experience is critical, and Aula is perfectly suited for this purpose. Aula provides a modern, engaging, and collaborative LMS that supports the delivery of educational content. It allows instructors to create and manage interactive course materials, assignments, and assessments. Aula's tools for discussion forums, quizzes, and real-time feedback engage students and help track their progress.

Aula also integrates chat, video, and document-sharing functionalities to facilitate collaboration between students and instructors. Optimized for mobile devices, it allows access to course content and interactions from anywhere. Moreover, Aula integrates with other educational tools, providing a unified platform for both instructors and students. Features like Single Sign-On (SSO) simplify the login process, and data analytics offer insights into student performance and engagement.

**5.2 Justification**

The proposed cloud-based services are not just about meeting current needs; they are about anticipating future growth and challenges. Here’s why these services are essential:

1. **Scalability and Flexibility**: Cloud services like AWS can easily scale to accommodate growing needs, ensuring the infrastructure can handle increased data, users, and applications over time.
2. **Cost Efficiency**: The pay-as-you-go model helps avoid large upfront capital expenditures on hardware and reduces ongoing maintenance costs.
3. **Enhanced Collaboration**: Tools like Microsoft 365 improve productivity and communication among staff and students, supporting modern educational practices and remote work.
4. **Data Security and Reliability**: Solutions like AWS Backup offer robust security features, ensuring data protection against loss and unauthorized access.
5. **Proactive Network Management**: Datadog provides real-time insights and proactive management capabilities, maintaining a high level of network performance and security.
6. **Disaster Recovery and Business Continuity**: Cloud-based backup and recovery solutions ensure quick data restoration in the event of a disaster, minimizing downtime and disruption.
7. **Enhanced Learning Experience**: Aula offers an engaging and collaborative platform for learning management, significantly enhancing the educational experience for students and faculty.

In conclusion, integrating cloud-based services into the University of The West of Scotland's network infrastructure for the two new buildings provides a comprehensive, scalable, and future-proof solution. Leveraging the benefits of cloud technology, the university can enhance collaboration, ensure data security, and maintain a high level of network performance and reliability, setting a solid foundation for future growth and innovation.

**6. Proposed Detailed Costings**

**6.1 Discussion**

The detailed costings for the network infrastructure of the University of The West of Scotland’s new buildings have been carefully considered, encompassing hardware, software, cloud services, and installation. The cost estimations include the procurement of high-performance switches, firewalls, wireless access points, fiber optic cabling, and associated networking equipment. Additionally, licensing fees for network management software, security solutions, and cloud-based services are included. Labor costs for installation, configuration, and ongoing maintenance are also accounted for to ensure a comprehensive and reliable network setup.

**6.2 Justification**

Costing considerations take into account potential discounts, warranties, and support options offered by vendors. Leading vendors, such as Cisco and Palo Alto Networks, often provide educational discounts and extended warranties to academic institutions, which can significantly reduce the overall expenditure. Additionally, these vendors offer robust technical support and training packages, ensuring the university’s IT staff can efficiently manage and maintain the network infrastructure. By leveraging these vendor offerings, the university can achieve a high-quality, cost-effective network solution that meets both current and future needs.

**6.3 Table of Detailed Costings**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Description** | **Quantity** | **Unit Cost** | **Total Cost** |
| Cisco Catalyst 9500 Series Core Switches | High-performance core switches for core layer | 2 | £12,000 | £24,000 |
| Cisco Catalyst 9300 Series Distribution Switches | Switches for inter-building connectivity | 4 | £8,000 | £32,000 |
| Cisco Catalyst 9200 Series Access Switches | Switches for access layer | 12 | £5,000 | £60,000 |
| Palo Alto Networks PA-Series Firewalls | Next-generation firewalls for security | 2 | £7,000 | £14,000 |
| Cisco Aironet 2800 Series Wireless Access Points | High-performance WAPs for wireless connectivity | 30 | £800 | £24,000 |
| Fiber Optic Cables and Installation | High-speed fiber optic cables | 1 | £20,000 | £20,000 |
| Network Management Software | Cisco Prime Infrastructure | 1 | £10,000 | £10,000 |
| Antivirus Software | Bitdefender GravityZone | 1 | £5,000 | £5,000 |
| VPN Software | NordVPN Teams | 1 | £3,000 | £3,000 |
| Backup and Recovery Software | Veeam Cloud Connect | 1 | £8,000 | £8,000 |
| Cloud Services | Google Drive, Canvas, AWS, Cisco Umbrella | 1 | £15,000 | £15,000 |
| *Dell PowerEdge R740 Servers* |  |  | £26,400 | 26,400 |
| Labor and Installation Costs | Installation and configuration of hardware and software | - | - | £25,000 |
| **Total** |  |  |  | **£266,400** |

By integrating vendor discounts, warranties, and support options, the University of The West of Scotland ensures a cost-effective and efficient network infrastructure, capable of meeting the institution's technological needs for the foreseeable future.

**7. Conclusions & Future Recommendations**

**7.1 Conclusions**

In conclusion, the proposed network solution for the University of The West of Scotland's new Buildings 1 and 2 is a robust, scalable, and secure infrastructure that effectively addresses the current and future needs of administrative staff, academics, and students. Utilizing a three-tier hierarchical design ensures optimal performance, manageability, and redundancy. The implementation of high-performance hardware, including Cisco Catalyst switches and Palo Alto firewalls, guarantees reliable connectivity and comprehensive security across all layers of the network.

The integration of modern software solutions, such as Cisco Prime for network management, Bitdefender GravityZone for antivirus protection, and Veeam Cloud Connect for backup and recovery, further enhances the network's resilience and efficiency. Additionally, cloud-based services from reputable providers like AWS, Google Drive, Canvas, and Cisco Umbrella offer scalable and flexible solutions for data storage, online learning, and security.

Cost considerations have been meticulously planned, leveraging vendor discounts, extended warranties, and comprehensive support options to ensure a cost-effective deployment. The detailed costings table provides transparency and clarity, showcasing the financial feasibility of the proposed solution.

**7.2 Future Recommendations**

To ensure the network infrastructure remains future-proof and continues to meet the evolving needs of the university, several recommendations are proposed:

1. **Regular Network Audits and Upgrades**: Conduct periodic network audits to assess performance, security, and capacity. Implement necessary upgrades to hardware and software to keep pace with technological advancements and increasing demands.
2. **Advanced Security Measures**: Continuously update and enhance security protocols to protect against emerging threats. Consider incorporating AI-driven security solutions and real-time monitoring tools to proactively identify and mitigate risks.
3. **Scalable Cloud Services**: Expand the use of cloud services to support growing data storage needs, facilitate collaborative research, and enhance online learning platforms. Evaluate new cloud offerings to optimize cost and performance.
4. **Training and Development**: Invest in ongoing training and development for IT staff to ensure they are proficient in managing and maintaining the network infrastructure. Encourage certifications and participation in industry conferences to stay abreast of best practices and innovations.
5. **User Feedback and Support**: Establish a feedback mechanism for users to report issues and suggest improvements. Provide robust support services to address user concerns promptly and effectively.
6. **Green IT Initiatives**: Explore and implement energy-efficient technologies and practices to reduce the environmental impact of the network infrastructure. Consider virtualization and consolidation strategies to optimize resource utilization.

By following these recommendations, the University of The West of Scotland can maintain a cutting-edge network infrastructure that supports its mission of providing high-quality education and research, fostering a secure, efficient, and innovative environment for all users.

# REFERENCES

#### FitzGerald, J., Dennis, A., & Durcikova, A. (n.d.). Business Data Communications and Networking. Jerry FitzGerald & Associates; Indiana University; University of Arizona.

#### Crume, C. E., & Maddux, C. D. (1990). Educational Computer Networks: An Overview. Educational Technology, 30(7), 26–30. Available at <http://www.jstor.org/stable/44426292> [ Accessed 20 Jun.2024].

#### Pawar, Swati & Nirmal, Ankita & Borade, Swapnali & Badgujar, Pallavi & Ugale, Vivek. (2020). NETWORK DESIGN FOR COLLEGE CAMPUS. 7. 323-326.

#### Staff Contributor (October 4, 2019) What Is QoS? Meaning and Best Quality of Service Tools.[online] | DNSstuff Available at <https://www.dnsstuff.com/what-is-qos> [Accessed 3 Jul.2024]

#### Cisco (2023) Cisco NX OS [online] | Cisco. Available at <https://www.trustradius.com/products/cisco-nx-os/reviews?q=Easy%20to%20configure#overview> [ Accessed 25 Nov.2023].

#### Solarwind [2023]. What is Hyper-V [online] |Solarwind. Available at <https://www.solarwinds.com/resources/it-glossary/hyper-v> [ Accessed 25 Nov.2023].