**FACULTY OF**

**COMPUTING AND INFORMATICS**



**CSN4214 DATA COMMUNICATIONS AND NETWORKING**

**TERM 2430**

**GROUP ASSIGNMENT**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Student ID** | **Name** | **Signature** | **Date** |
| **1** | **1231201977** | **TEN YONG XIANG** | ***TYX*** | **21/1/2025** |
| **2** | **1231201419** | **CHEW BOON LOONG** | ***CHEW*** | **21/1/2025** |
| **3** | **1231203446** | **TAN GUAN MING** | ***T*** | **21/1/2025** |
| **4** | **1231200883** | **DERECK WONG ZHUAN ZECK** | ***DERECK*** | **21/1/2025** |

**LECTURE:Ms. Noor Farah Shahida Binti Mohd Haris**

**TOTAL MARKS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Student name** | **#1** | **#2** | **#3** | **#4** |
| **PART A (80 Marks)** | **TEN YONG XIANG** | **DERECK WONG ZHUAN ZECK** | **CHEW BOON LOONG** | **TAN GUAN MING** |
| Question 1 (20 marks) |  |  |  |  |
| Question 2 (20 marks) |  |  |  |  |
| Question 3(15 marks) |  |  |  |  |
| Question 4 (10 marks) |  |  |  |  |
| Question 5(10 marks) |  |  |  |  |
| Format & References (5 marks) |  |  |  |  |
| **PART B** |  |  |  |  |
| Individual Presentation (20 marks) |  |  |  |  |
| **Total (100)** |  |  |  |  |
| **Penalty** |  |  |  |  |
| **Final Marks (20%)** |  |  |  |  |

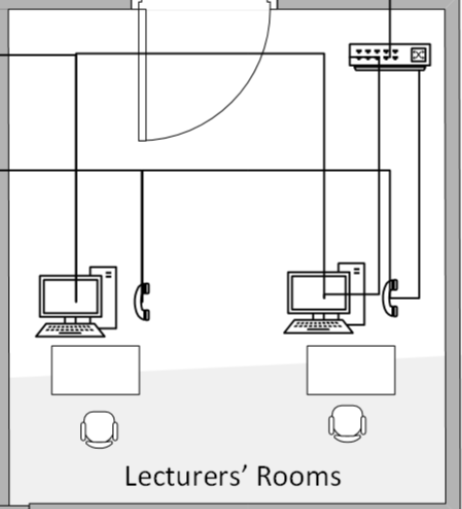
**ASSIGNMENT RUBRIC (PART A)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **CRITERIA** | | | **WEAK** | **MODERATE** | **GOOD** | **EXCELLENT** | **Marks** |
| **LAN network design (wired and**  **wireless)** | | | Include minimal/no floor plan design for  all the rooms criteria    There is a lack of or inadequate wired and wireless LAN network design for every room, each floor, and between floors.    The structured cabling design for the building is wrong/ inadequate for each floor, and between floors.    **(0 - 4 marks)** | Includes incomplete floor plan design for all the rooms criteria.    There is a brief wired and wireless LAN network design for every room, each floor, and between floors.    The structured cabling design for the building is incomplete for each floor, and between floors.        **(5 – 10 marks)** | Contains most of floor plan design for all the rooms criteria.    Good wired and wireless LAN network design for every room, each floor, and between floors.    The structured cabling design for the building is almost complete for each floor, and between floors.      **(11 – 15 marks)** | Contains complete floor plan design for all the rooms criteria.    Excellent wired and wireless LAN network design for every room, each floor, and between floors.    The structured cabling design for the building is complete for each floor, and between floors.          **(16 – 20 marks)** |  |
|  | **(20 marks)** |  |
| **LAN**  **implementation (internetworking devices and communication**  **media)** | | | None or insufficient  description of the  LAN  implementations especially internetworking devices, and communication media.    Include minimal/no example of the LAN implementations.            **(0-4 marks)** | Basic/Minimal explanation related to  LAN implementations  Especially internetworking devices, and communication media.    Includes incomplete examples of the LAN implementations.              **(5 - 10 marks)** | The description contains clear  explanations related to  the LAN implementations especially internetworking devices, and communication media.    The explanation contains most of  examples of the  LAN  implementations.    **(11 – 15 marks)** | Excellent and precise  explanation related to  the LAN implementations especially internetworking devices, and communication media.    The description contains all examples of the LAN implementations.            **(16 – 20 marks)** |  |
|  | **(20 marks)** |  |
| **IP address** | | | Fails to differentiate or mentions only one of the IP versions or offers a vague/partial explanation of the differences between IPv4 and IPv6. | Provides basic differentiation with some inaccuracies or missing important aspects of IPv4 and IPv6. | Differentiates IPv4 and IPv6 with mostly accurate explanations. | Clearly and accurately differentiates IPv4 and IPv6 with detailed explanations of key features (e.g., address format, size, etc.). |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | Provides minimal or incorrect benefits for IPv4 and IPv6. Mentions only one or two drawbacks with little or no explanation.      Does not identify which IP version will be used for the college. Identifies an IP version with little or no explanation or justification for the choice.          **(0 - 3 marks)** | Mentions a few benefits of IPv4 and IPv6 but lacks detailed explanation or misses key points. Lists a few drawbacks of IPv4 and IPv6 but with limited explanation or some inaccuracies.    Identifies the IP version but provides limited or unclear rationale for the choice.              **(4 – 7 marks)** | Lists and explains most benefits of IPv4 and IPv6 but may lack some depth or details. Discusses most drawbacks of IPv4 and IPv6 with some explanation.    Identifies the IP version and offers a reasonable explanation, though some details may be missing or not fully justified.              **(8 – 11 marks)** | Provides a comprehensive list of benefits with clear and relevant explanations (e.g., established, compatibility, simplicity). Identifies and explains several major drawbacks of IPv4 and IPv6 with clarity (e.g., limited address space, exhaustion).    Clearly and accurately identifies which IP version (IPv4 or IPv6) will be used for the college, providing a solid rationale based on context.    **(12 - 15 marks)** |  |
|  | **(15 marks)** |  |
| **Client and**  **Network**  **Operating System** | | | None or insufficient description of the chosen Client and Network Operating System.    **(0 - 2 marks)** | Basic or minimal explanation of the chosen Client and Network Operating System.    **(3 – 5 marks)** | Good explanation of the chosen Client and Network Operating System.      **(6 – 8 marks)** | Excellent explanation of the chosen Client and Network Operating System.      **(9 - 10 marks)** |  |
|  | **(10 marks)** |  |
| **Centralized network**  **management &**  **network security**          **(10 marks)** | | | There is a lack of or inadequate explanation of the centralized network management and network security.      **(0 - 2 marks)** | There is a brief explanation of the centralized network management and network security.        **(3 - 5 marks)** | The description contains clear explanations related to the  centralized network management and network security.    **(6 – 8 marks)** | Excellent and precise explanation of the centralized network management and network security.        **(9 – 10 marks)** |  |
| **Format &**  **References** | | | Fails to follow format and assignment requirements; incorrect margins, spacing and indentation; neatness of essay needs attention. | Meets format and assignment requirements; generally correct margins, spacing, and indentations; essay is neat but may have some assembly errors.    Use of sufficient range of sources. | Meets format and assignment requirements; margins, spacing, and indentations are correct; essay is neat and correctly assembled.    Good selection and critical interpretation | Meets all formal and assignment requirements and evidences attention to detail; all margins, spacing and  indentations are correct; essay is neat and correctly assembled with professional look. |  |
| **(5 marks)** | | | Incomplete breadth of readings of relevant sources.        **(0 -2 marks)** | **(3 marks)** | of range of appropriate readings demonstrating familiarity with key texts and articles.    **(4 marks)** | Skilled selection and synthesis of reading materials drawn from a wide range of sources including critical evaluation.  **(5 marks)** |  |
|  | | |  |  |  | **PART A (80 Marks)** |  |

**PRESENTATION RUBRIC (PART B)**

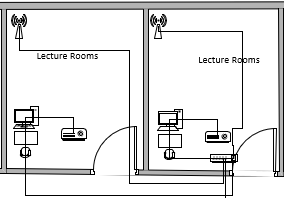
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Criteria** | **0-1 mark** | **2 marks** | **3 marks** | **4 marks** | **5 marks** | **Marks** |
| **Subject**  **Mastery** | The  presentation doesn't show any knowledge of the topic.   It’s short and has basic or no foundation. | The  presentation has some information about the topic.  It is mostly based on basic knowledge. | The content shows some understanding and comprehension of the topics. | The content shows good understanding of all the required tasks. Clearly  explains all the required tasks. | Full knowledge of the topic is demonstrated. Excellent explanation for all the required tasks. |  |
| **Organization** |  The  presentation has no sequence of information.   it is not understood. |  The  presentation is difficult to follow because it jumps back and forth.  it is difficult to understand. |  The  presentation is somewhat  difficult to follow.  the general idea and timeline is understood. |  It is presented in a logical sequence.   It can be followed fairly easily. |  It is presented in a logical, interesting sequence, and effective way.  It can be followed easily. |  |
| **Delivery** |  No eye contact is made, reads from notes  a lot of mumbling and mispronunciation, and speaks quietly. |  Occasional eye contact, mostly reads from notes  speaks quietly and mispronounces. |  Maintains eye contact, reads from notes occasionally  speaks loud enough, pronounces  some words  correctly, and is somewhat  effective and engaging. |  Maintains eye contact throughout, rarely reads from notes  speaks with inflection, pronounces most words correctly, and is somewhat effective and engaging. |  Maintains eye contact, doesn't read from notes  speaks loud with inflection, pronounces all words  correctly, and is very effective and engaging. |  |
| **Creativity** |  There is no true focus which leads to poor or no creativity.  The are no visual aids. |  Presentation is not unique or interesting, but uses of visual  aids in a  somewhat interesting way.  Little or no interest is conveyed in the focus chosen. | Presentation is interesting, but unoriginal and there's a presence of visual aids that somewhat  support the content.   The focus chosen is  somewhat  interesting, but obvious | Presentation information is highlighted with visual aids that are used in an interesting way. The focus chosen is original. | Presentation is unique and innovative, with visual aids that are effectively used to support or demonstrate the content.  The focus chosen is original and inspired. |  |
| **PART B (20 marks)** | | | | |  |  |



**Lecturers’ Rooms**

We have used a 16-port switch to connect all device in these lecturers’ room which have:

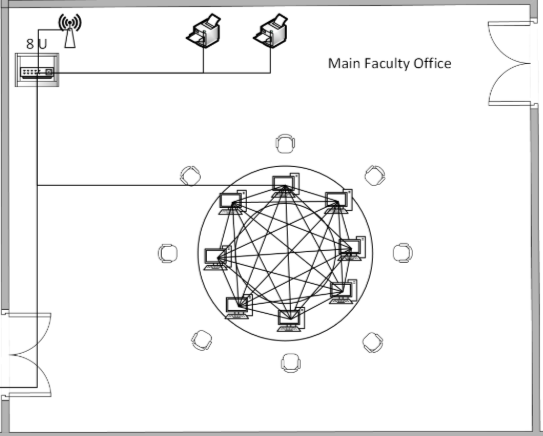
1 computer and 1 telephone. In this design, we have applied bus topology to all floor lecture rooms.



Lecture Rooms

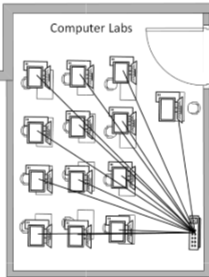
We have used a 16-port switch to connect all device in these lecture room which have:

1 computer and 1 projector. In this design, we have applied star topology to all floor lecture rooms.



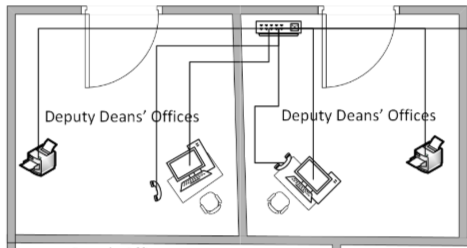
**Main Faculty Office**

We have used an 8-port switch to connect all devices in the main faculty office. These include two computers and Wireless router. In this design, we used a mesh topology to connect eight devices. All the devices are linked together through the switch,



**Computer Labs**

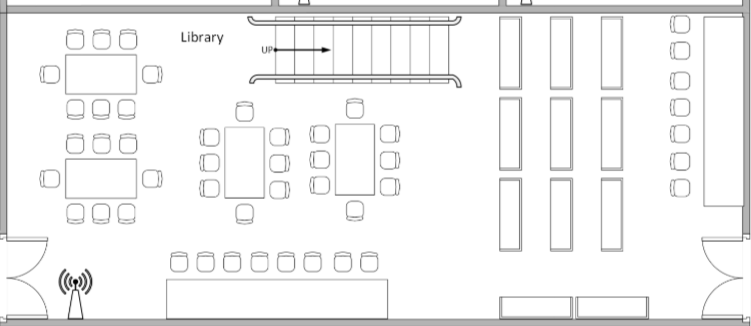
We have used a 16-port switch to connect all devices in the computer lab which have 1 computer and 1 telephone. In this design, we have applied mesh topology to the computer lab, connecting all devices by using a 16-port switch as a connection point.



**Deputy Deans’ Offices**:  
We have connected each Deputy Dean’s office to the network. Each office includes one computer and one telephone. The devices are connected using a star topology, ensuring direct communication with the main switch.

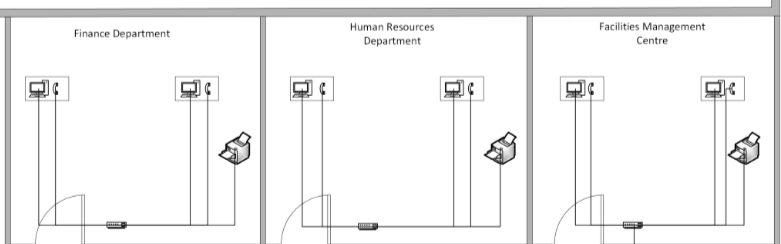


**Head of Department Rooms**:  
Each Head of Department room includes one computer, one printer and one telephone. These devices are connected through a switch in a star topology, providing reliable communication and network access.



**Library**:

The library has been equipped with wireless access points for mobile device connectivity.



* **Facilities Management Center:**

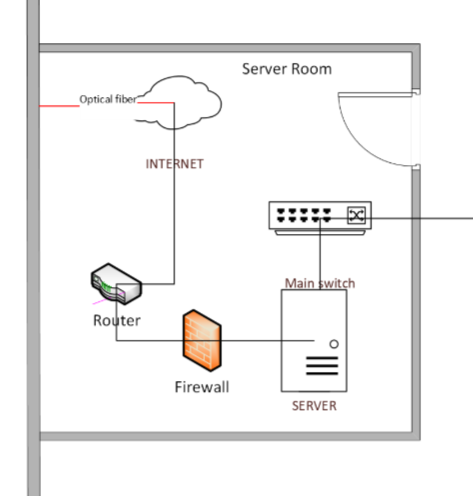
We have used a 8-port switch to connect all devices in the Facilities Management Center, which include 1 computer and 1 telephone, and we have applied a star topology to the Facilities Management Center.

* **Finance Department:**

We have used an 8-port switch to connect all devices in the Finance Department, which include 1 computer and 1 telephone. In this design, we have applied a star topology to the Finance Department, connecting all devices to the switch.

* **Human Resources Department:**

We have used an 8-port switch to connect all devices in the Human Resources Department, which include 1 computer and 1 telephone. In this design, we have applied a star topology to the Human Resources Department, connecting all devices to the switch.



**Servers Rooms:**

In the server room, we have servers, a router, firewall, and main switch.The main switch in the server room links directly to the 24-port switch in the riser room.

Main Switch:

A high-performance switch that connects to all key network segments, including the riser room.

Server:

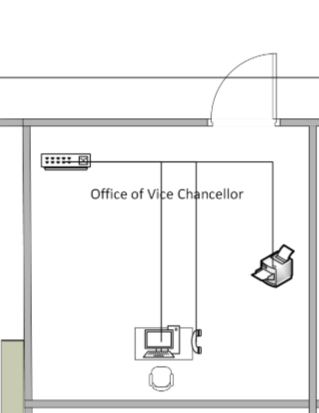
Hosts all critical applications and provides centralized data storage and management.

Firewall:

Protects the network from external threats, ensuring secure and controlled access to resources.

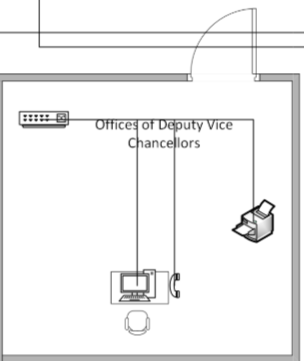
Router:

Connects the internal network to the Internet via an optical fiber connection.



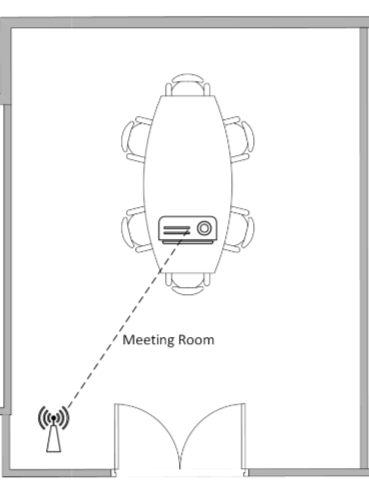
**Offices of Vice Chancellors:**

We have used an 8-port switch to connect all devices in the office of Vice Chancellors, which include 1 computer, 1 telephone and 1 printer. In this design, we have applied a star topology to the Senate Room, connecting all devices to the switch.



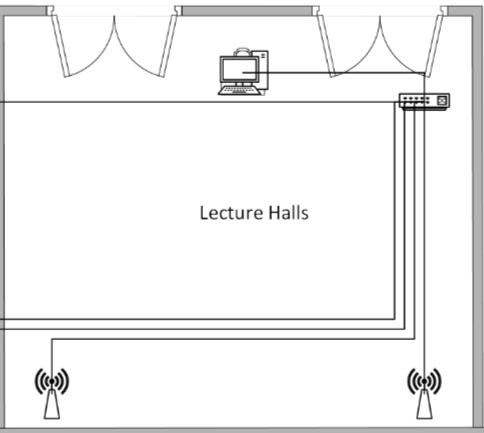
**Offices of Deputy Vice Chancellors:**

We have used an 8-port switch to connect all devices in the office of Deputy Vice Chancellors, which include 1 computer, 1 telephone and 1 printer. In this design, we have applied a star topology to the Senate Room, connecting all devices to the switch.



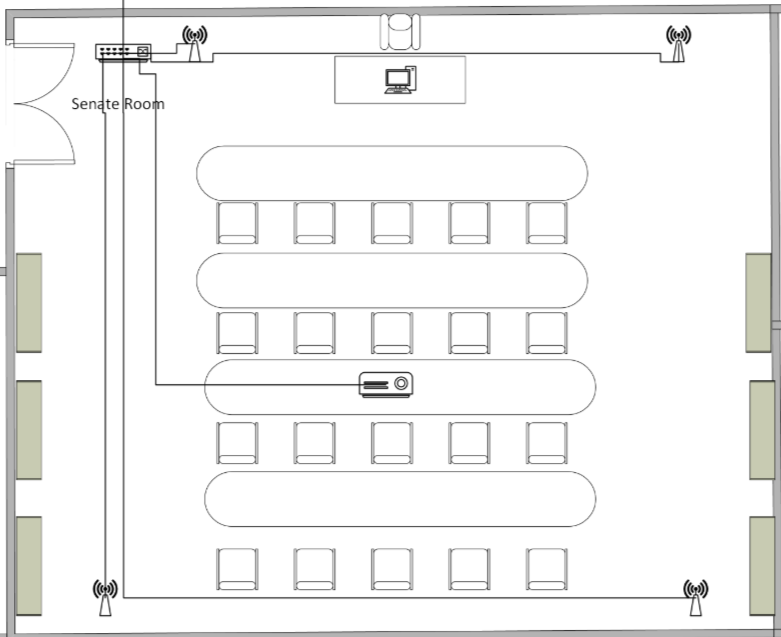
**Meeting room:**

The meeting room has been equipped with wireless access points for mobile device connectivity.



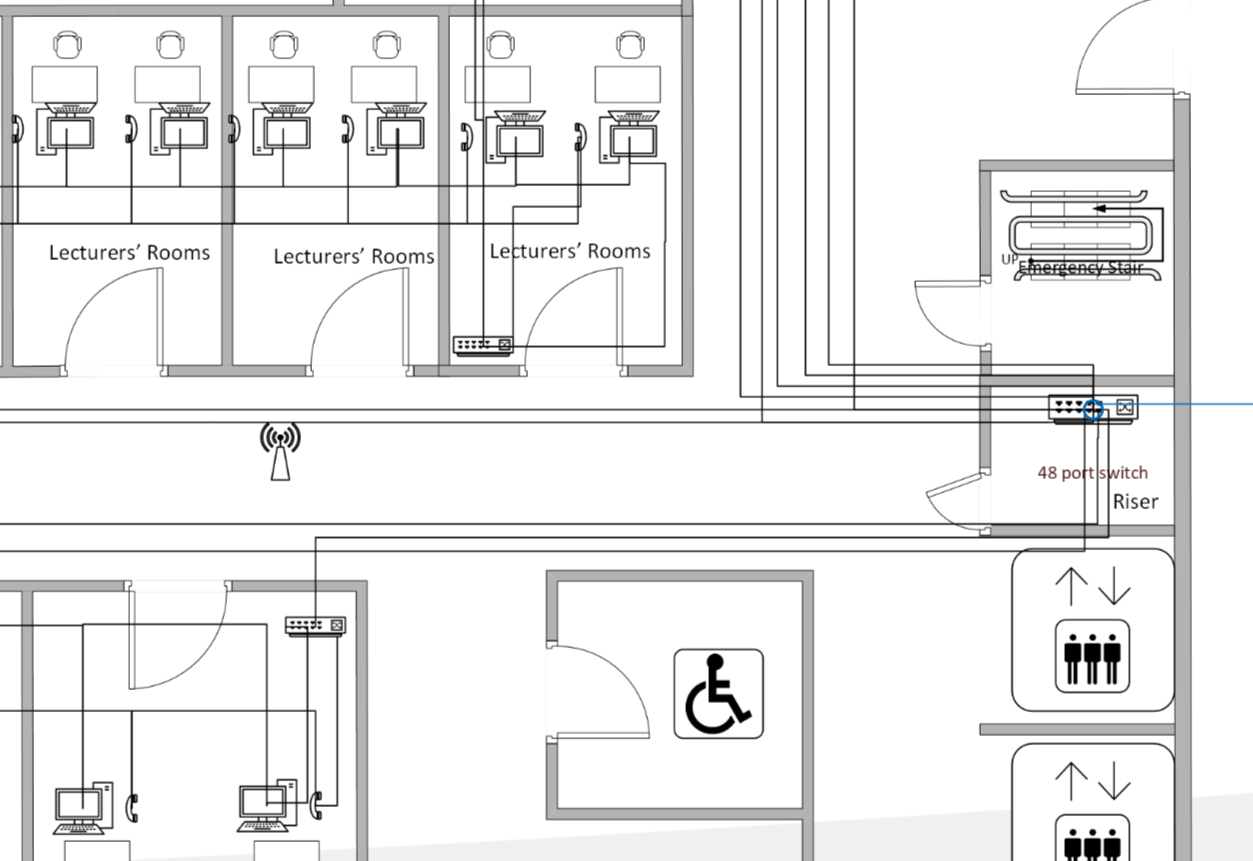
**Lecture Halls:**

We have used a 16-port switch to connect all devices in the Lecture Halls, which include 1 computer, 2 wireless router. In this design, we have applied a star topology to the Lecture Halls, connecting all devices to the switch.



**Senate Room:**

We have used an 8-port switch to connect all devices in the Senate Room, which include 1 computer and 1 telephone. In this design, we have applied a star topology to the Senate Room, connecting all devices to the switch.



**Ground floor riser room**:  
The riser room is the central hub for network connectivity in the ground floor, linking it to the second floor riser room 48-port switch and which includes a 48-port switch that connects devices to all the rooms on the ground floor include:

4 Head of Department rooms

1 meeting room

20 lecturers’ rooms

6 lecture rooms

1 Main faculty office

1 IT services office

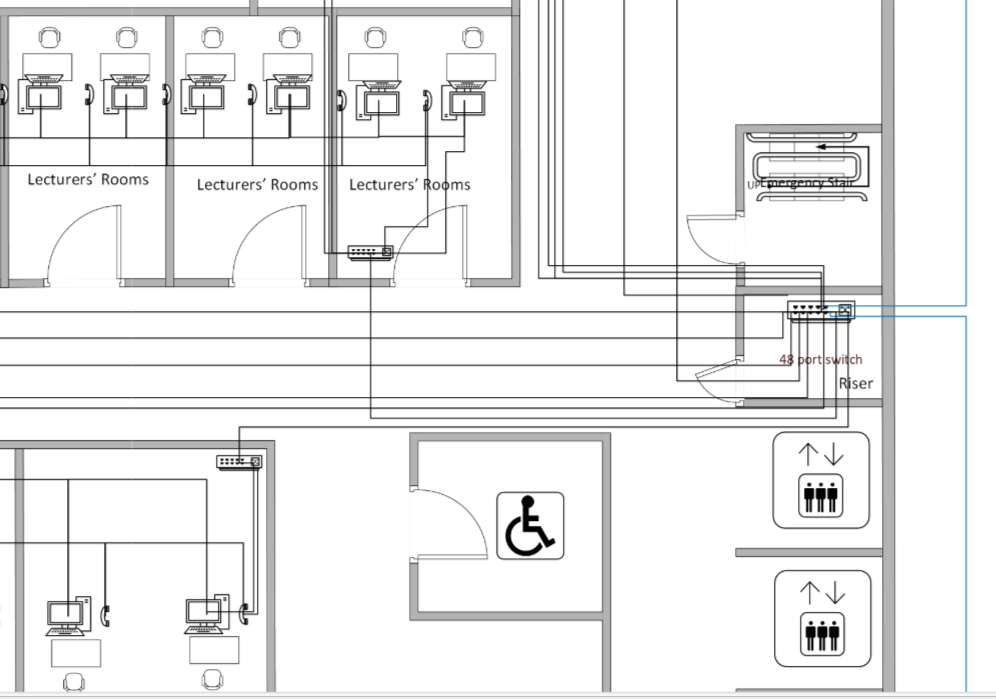
1 Dean’s Office

1 Deputy Deans Office

7 Tutorial rooms

5 Computer Labs

1 Library



**Second floor riser room**:  
The riser room is the central hub for network connectivity on the second floor, linking it to the third floor riser room 48-port switch and which includes a 48-port switch that connects devices to all the rooms on the second floor including:

4 Head of Department rooms

1 meeting room

20 lecturers’ rooms

8 lecture rooms

1 Main faculty office

1 IT services office

1 Dean’s Office

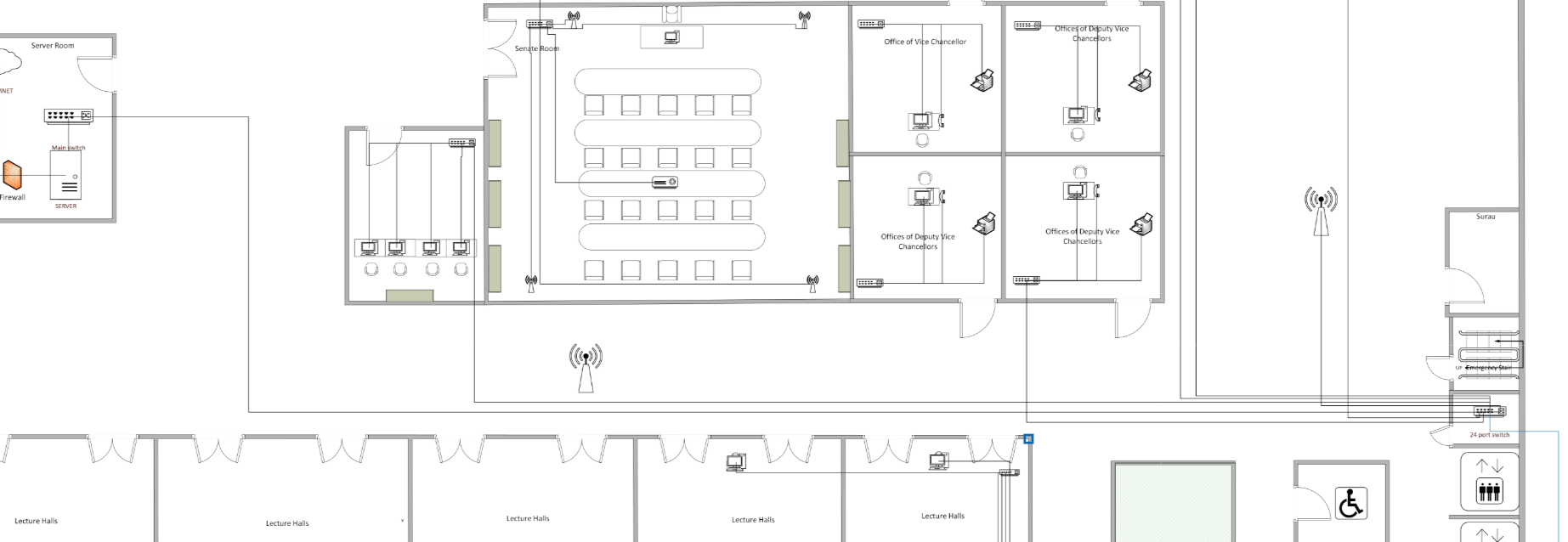
2 Deputy Deans Office

7 Tutorial rooms  
3 Computer Labs

1 Library

1 Research centre

1 Academic and Admission Centre



**Third riser room**:

The riser room is the central hub for network connectivity in the third floor, this switch is directly connected to the main switch located in the server room, creating a backbone for the entire network.which includes a 24-port switch that connects devices to all the rooms on the third floor which including:

1 Finance Department

1 Human Resources Department

1 Facilities Management Centre

5 Lecture Halls

4 Office of deputy Vice Chancellor

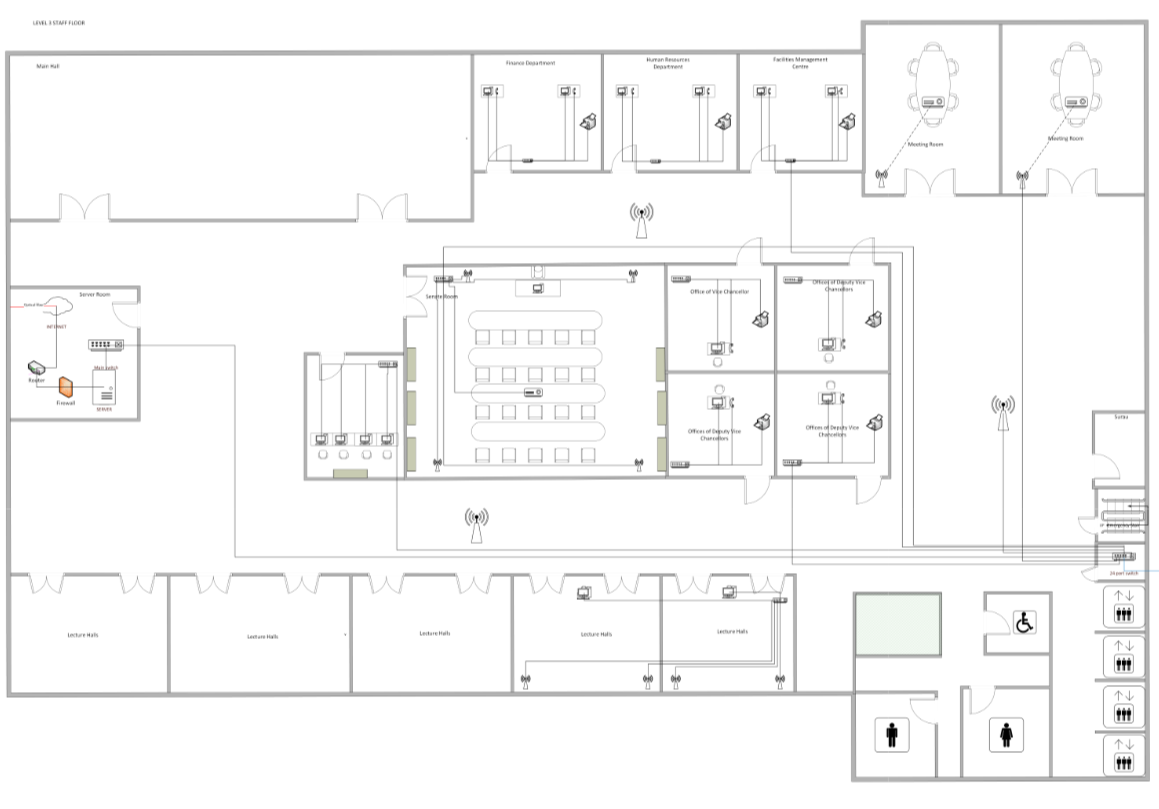
1 Register room

2 meeting room

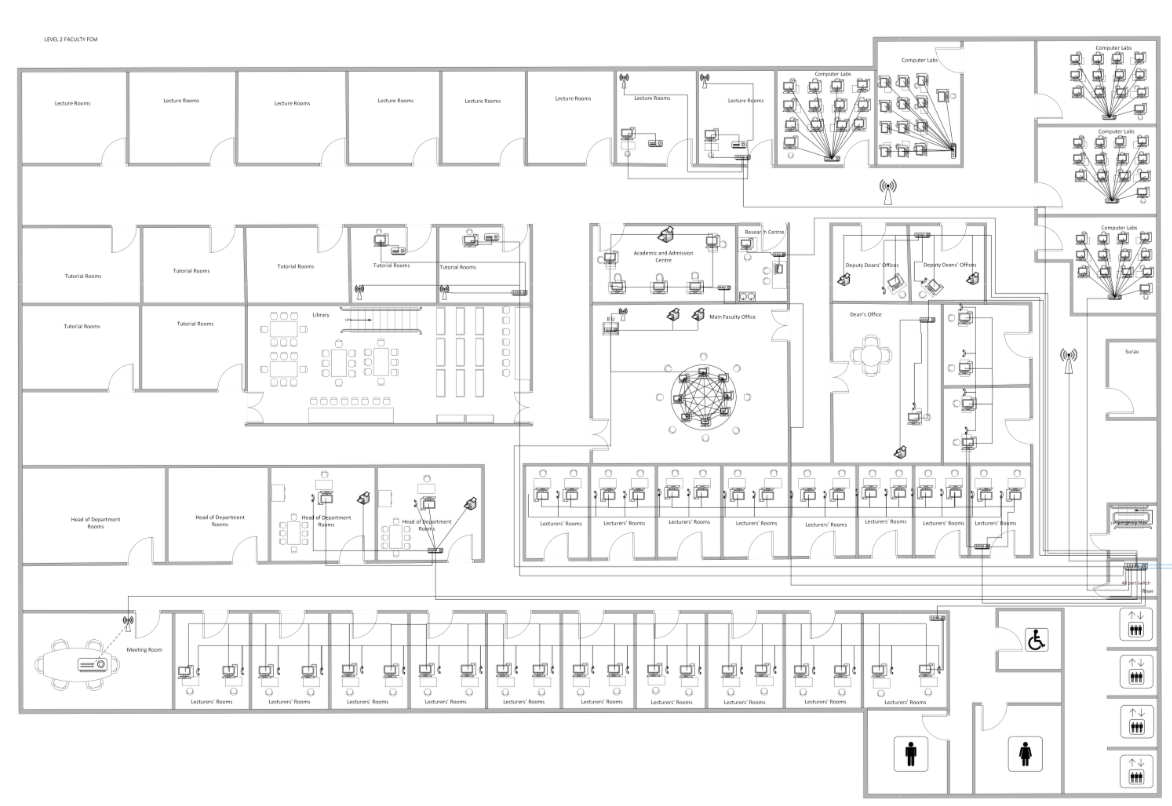
1 Senate room

**Floor Plan**

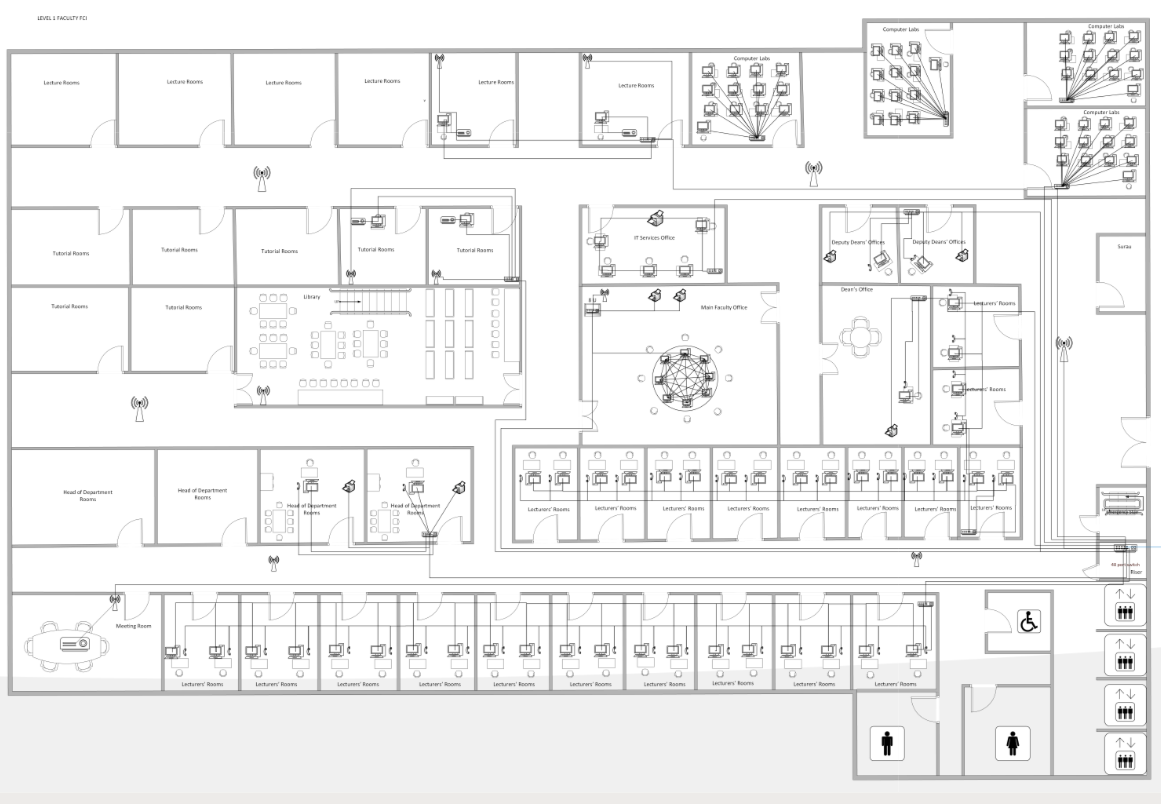
Third Floor



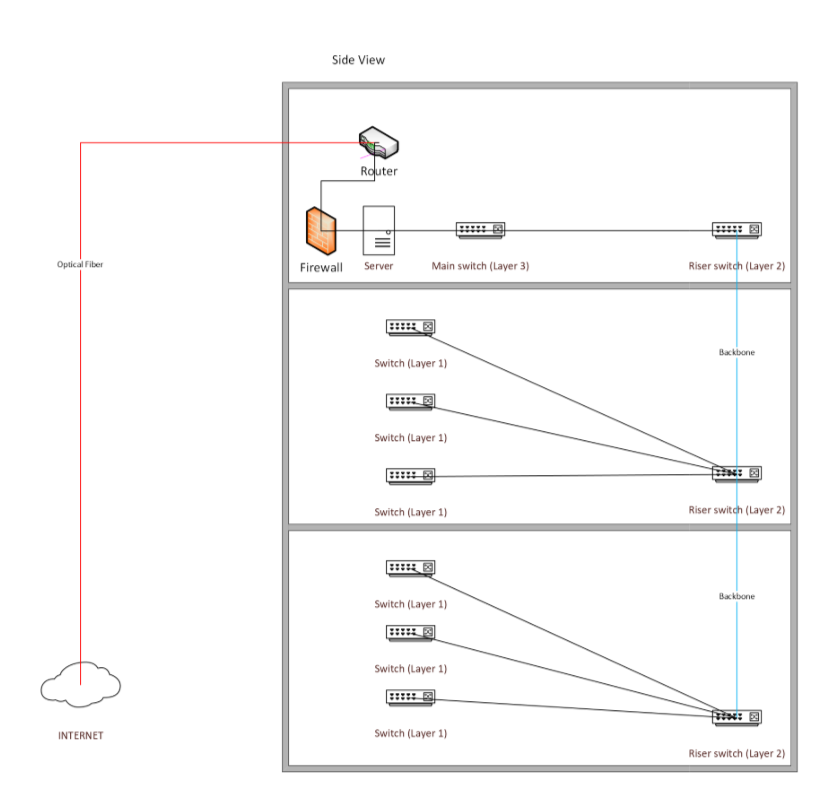
Second Floor



First Floor



Side view



**2. Elaborate in terms of internetworking devices and communication media used. Provide one example for each.**

Internetworking devices are essential components in establishing and maintaining a reliable and efficient network. These devices ensure that data packets are transmitted seamlessly between different parts of a network or across multiple networks. The most used internetworking devices include routers, switches, bridges, hubs, and gateways. Below, we elaborate on these devices and provide examples for each, alongside a discussion of communication media.

**Internetworking Devices**

**Routers:** Routers are critical in connecting different networks and directing data packets to their intended destinations. They operate at the network layer (Layer 3) of the OSI model and use IP addresses to determine the best path for data transmission. Routers are crucial for interconnecting different networks, such as Local Area Networks (LANs) and Wide Area Networks (WANs), enabling communication between devices on disparate segments. For instance, a home router connects a home network to the internet, acting as a gateway between the local network and the broader internet infrastructure

**Switches:** Switches function within a single network by connecting multiple devices, such as computers, printers, and servers. Operating at the data link layer (Layer 2), switches manage data traffic efficiently, ensuring that packets are delivered only to their intended devices. Managed switches, such as the Net gear GS308T, allow administrators to configure VLANs (Virtual Local Area Networks) and optimize network performance. In a college lab, switches facilitate high-speed connections between devices, ensuring smooth operations for activities like file sharing and remote learning.

**IP Printer:** IP Printers provide network-based printing solutions, allowing multiple users to print documents efficiently over a shared network. They are assigned unique IP addresses for easy access and management. For instance, an HP LaserJet IP Printer can be used in an office to handle high-volume printing needs, offering secure, high-speed, and remote printing capabilities.

**IP Phone:** IP Phones enable voice communication over the internet, eliminating the need for traditional telephone lines. They support advanced features like call forwarding, conferencing, and voicemail. For example, a Cisco IP Phone can be deployed in an office to ensure clear and reliable communication between departments, leveraging features like HD audio and integration with office communication platforms.

**Firewall:** Firewalls are essential for securing a network by monitoring and controlling incoming and outgoing traffic based on predefined security rules. They act as a barrier between internal networks and external threats. For example, a Fortinet Firewall can be installed in a college network to protect sensitive data, block unauthorized access, and ensure secure communication between administrative and academic networks.

**Communication Media**

Communication media are the physical or wireless pathways through which data travels. They can be broadly categorized into wired and wireless media. Each type has its advantages and is chosen based on the specific requirements of the network.

**Fiber-Optic Cables:** Fiber-optic cables are among the fastest and most reliable forms of communication media. They use light to transmit data, offering high bandwidth and low latency. These cables are ideal for connecting buildings on a college campus, as they can deliver high-speed internet access to the building’s network infrastructure over long distances without signal degradation. For example, Corning’s fiber-optic cables can be used to ensure reliable internet connectivity for academic blocks and administrative offices.

**Twisted-Pair Cables:** Twisted-pair cables, such as RJ45 CAT6 Ethernet cables, are widely used for internal wiring in buildings. They are cost-effective and capable of supporting gigabit speeds over short distances. In a college, these cables can connect computers, printers, and switches within classrooms and offices.

**Wireless Communication:** Wireless media, such as Wi-Fi and Wireless Access Point, use radio waves to transmit data. This method provides flexibility and is especially beneficial in environments like libraries, cafeterias, and common areas where mobility is required. Devices like TP-Link’s wireless access points ensure wide coverage and high-speed internet for students and staff.

**3. Differentiate between IPv4 and IPV6.**

**Introduction IPv4**

An IP address is a collection of numbers that's assigned to devices and computers to make communication over the internet possible, and it is highly important. Without an IP address, you cannot send and receive information. In other words, the Internet-just as we know and use it today-is not possible without IP addresses. There are two types: IPv4 and IPv6.

The development of IPv4 began in the early 1980s. Although a more advanced protocol known as IPv6 has been introduced, it is estimated that most network traffic in the world today still runs on IPv4. IPv4 utilizes a 32-bit address structure capable of supporting up to 232 addresses, about more than 4 billion IP addresses.

An IPv4 address is composed of four blocks of numbers between 0 and 255, separated by dots. It is very likely that your IP address is in IPv4 format. Here is an example of an IPv4 address: 192.168.1.1

However, after nearly 40 years of use, IPv4 has also brought a problem: it can only provide a maximum of 4.3 billion addresses. At the time in the early 1980s, this number was considered more than enough. However, as the use of the Internet expanded around the world, IPv4 addresses quickly ran low. By the mid-1990s, engineers had to develop solutions to increase the supply of IP addresses.

Nowadays, almost all people use many devices to connect to the Internet, including smartphones, laptops, tablets, and traditional desktop computers. In addition, with the development of IoT, there are more and more devices that need to use IP addresses, so the developers have to find a more permanent solution to deal with this problem.

**The benefits of IPv4:**

-Connectionless network service-datagrams are transmitted without preceding handshake, though it can use TCP for reliable transmission

-Pretty simple virtual communication layer above various devices including those utilizing address resolution protocol

-It requires less memory and ease of remembering the addresses

-Allows the creation of simple virtual communication layer over diversified devices

-IPv4 addresses are compatible with all current hardware and software applications.

-Most ISPs still utilize IPv4 since it is the most widely deployed standard.

These are the reasons why most businesses would rather stick with using IPv4 than upgrade to IPv6, despite losing out on some of the benefits associated with using the IPv6 addressing system.

**The drawbacks of IPv4:**

-Complex Configuration: IPv4 requires DHCP or manual configuration to assign addresses. It is complex and therefore error-prone, but also extremely time-consuming.

-Limited Address Space: IPv4 has a limited number of addresses. This is not enough for the large number of devices connecting to the Internet daily.

-Security Concerns: Some of the built-in security features that are required today are lacking in IPv4. Therefore, it is more prone to attacks and requires additional security measures.

-Inefficient Routing: The structure of IPv4 makes routing more complex, hence slowing down data transmission and increasing latency.

-Reduced Performance: IPv4 uses broadcasting to communicate with multiple devices on a network. This unnecessary network traffic reduces its performance.

-Fragmenting Packets: This allows IPv4 routers to fragment packets. It raises the chances of data corruption or loss due to increased transmission inefficiencies.

-Limited Support: The QoS support is not available in IPv4. The standard prioritizes only certain kinds of data, thus affecting the performance of several real-time applications.

-IPv4 needs arrangement either physically or naturally. Designing IPv4 physically must be done through Dynamic Host Arrangement Convention (DHCP). Setups of DHCP are perplexing since independent administration should be accomplished for its framework.

**Introduction IPv6**

Furthermore, IPv6 was developed in the late 1990s to replace IPv4 before its address depletion reached critical levels. Yet the migration towards it has been slow. The major reason for this slowness in migration is that replacing the routers, servers, and switches that have long relied on IPv4 will be expensive and very laborious. Even though IPv6 is now technically ready for full deployment, its complete implementation is still gradual.

IPv6 stands for Internet Protocol version 6, meaning the sixth version of the Internet Protocol. It was developed to address the upcoming exhaustion of the IPv4 addresses. Like IPv4, IPv6 allocates a unique alphanumeric IP address that enables various devices to share information on the Internet.

That said, IPv6 addresses are significantly longer in length compared to IPv4 addresses, which offers the possibility of producing far more unique IP addresses. When we say "far more," we really mean it: IPv6 uses a 128-bit address, allowing for 340 undecillion possible IP addresses, compared to IPv4's 4.3 billion.

Despite the advantages of IPv6, its deployment by an ISP or network administrator sometimes leads to leaks or security gaps. This may disclose some confidential information, but many of such risks can be reduced using a VPN.

For the interested reader, let's note that an IPv6 address is composed of eight groups, each comprising four hexadecimal digits. The groups are separated by colons instead of periods. The following is an example of an IPv6 address:

2001:0db8:82a3:0000:0000:4a2e:0370:7337

**The benefits of IPv6:**

-Huge number of possible unique addresses, compatibility with new devices, and no more subnetting issues.

-Routing is more efficient because of the routing tables reduced in size.

-Support for multicast rather than broadcast means that bandwidth-intensive packet flows can be sent to many destinations at the same time, saving bandwidth.

-Auto-configuration means configuration tasks, such as IP address assignment and device numbering, can take place automatically.

-Security features providing data integrity, authentication, and confidentiality are baked into IPv6.

-Reliability: IPv6 is more reliable than IPv4.

-More Robust Security: IPSecurity, which provides confidentiality, and data integrity, is embedded into IPv6.

-Routing efficiency: IPv6 can efficiently manage the packets.IPv6 establishes Internet Service Providers, which are used to reduce the size of the routing tables.

-Faster Speeds: IPv6 supports multicast, which allows flows of bandwidth-intensive packets.

**The drawbacks of IPv6:**

-Much longer compared to an IPv4 address; not all websites support it, which may create system problems in very rare cases.

-Costs: It may need a new investment in hardware, software, and other network infrastructure components.

-Compatibility problems: IPv6 may not support older devices and some software; these must be updated or replaced.

-Training needs: There is a training need for the IT staff and network administrators to get a good understanding of IPv6 networks.

-No backward Compatibility: IPv6 is not available on IPv4 machines, which means one can not run IPv6 on IPv4-supported machines.

-Conversion Time: The other major disadvantage of IPv6 is identifying the device on the network uniquely, and converting to IPV4 is very much.

-Communication: Communication between IPv4 and IPv6 is also not possible, which means cross-protocol communication is prohibited.

After considering the technical requirements, compatibility, and practical limitations, IPv4 will become the main IP addressing system to be utilized by the college. These are the reasons for this choice:

1. Compatibility with the Existing Systems: Most hardware, software applications, and network devices that have already been installed at the college are capable of supporting IPv4. A shift to IPv6 would therefore involve upgrading or replacing equipment, which is an expensive and time-consuming affair.
2. Supported by ISPs: ISPs that the college relies on support IPv4 as their main addressing system for network services. The adoption of IPv4, therefore, guarantees smooth connectivity without compatibility problems.
3. Cost-Effectiveness: The most important reason for sticking with IPv4 is that it requires no upfront investment in new infrastructure. It would save money that could be utilized in migrating to IPv6, such as hardware upgrade, software upgrade, and personnel training.
4. Easy of Management: IPv4 addresses are easy to configure and manage for the current network team because the team is already quite conversant with IPv4. It reduces administrative overhead.
5. Addressing the Current Needs: Currently, the number of devices connected to the college network is manageable within the IPv4 address space. For internal networks, private IPv4 addresses like 192.168.x.x and their combination with NAT can guarantee that enough IP addresses are available, not requiring IPv6.

Conclusion, The reason the college will use IPv4 for its network is because it is more practical and suitable for the systems already in place. IPv4 works well with the current hardware and software, ensuring smooth operations without requiring costly upgrades. It's also widely supported by internet service providers and is easier for the IT team to manage, given their experience with IPv4. While IPv6 supports more features and a much larger address space, the needs of the college for now are perfectly within the IPv4 capabilities. Private IPv4 addresses with NAT are sufficient for connecting all the devices without exhausting the available addresses. This approach is also cost-effective and does not have to handle the complexity of an immediate migration to IPv6.The college recognizes IPv6 because it is the future and shall transition gradually when it becomes highly adopted and financially viable. For now, IPv4 is the most reliable and cost-effective solution.

**4. Provide the Client Operating System and Network Operating System**

I chose Windows 11 as the Client Operating System, which is to be installed, and Windows Server as the Network Operating System. A detailed explanation of my selection and the reasons behind this decision are given below.

**Client Operating System: Windows 11**

It will be released on October 5, 2021. Windows 11 is a recently developed version by Microsoft, and many discussions are running among geeks and ordinary people. As happens with any significant technological upgrade, the reactions have ranged from enthusiasm to skepticism. It's the newest in a series of Windows, aimed at redefining our way of using the computer and raising the bar regarding operating systems. Many people, from gamers and office workers to any users of their computer for work or amusement, will love these new Windows 11 features.

Reasons for Selection:

1. User Friendly Interface: Windows 11 comes with a fresh design that is modern and intuitive. Hence, it's pretty easy for users to find their way around It. therefore, enhances productivity and reduces extensive training.
2. Software Compatibility: It supports a wide range of enterprise and professional software, including Microsoft Office Suite, Adobe products, and various proprietary applications.
3. Security Features: Some of the key security features in Windows 11 include such as built-in Windows Defender for malware protection and support for Secure Boot and TPM 2.0 ensuring system integrity.
4. Regular Updates: Microsoft regularly releases updates and patches to fix vulnerabilities and improve functionality.
5. Optimized for Hybrid Work: The operating system is fully designed to support hybrid work, with features supporting both in-office and remote work.
6. Window and app grouping: The new Snap Groups and Snap Layouts are just a few features included in window and app grouping, making task switching smoother. For example, you wouldn't have to minimize all the different windows; now, you could group them according to their related tasks and then enable/disable at the same time. And that will save much time in use and keep it neat and clean for a user.
7. Faster Load Times: Optimizations in code, along with smarter management of resources, result in speedier startup times and snappier applications.
8. Efficient Memory Management: Advanced algorithms in memory allocation in Windows 11 provide better use of system resources, reducing lag and improving multitasking.

**Network Operating System: Windows Server**

Microsoft Windows Server includes some super-powerful computers. It was launched in April 2003. It generally possesses robust servers which support most IT businesses, apps, and services installed as the core. The server manages the operational group-related tasks on a network. It sends, stores, arranges, and receives files from network-connected devices.

Windows Server aims at applications in data centers and other high-performance computing environments. Compared to other operating systems for servers, it is much more effective and scalable. Besides, Windows Server has some features necessary for the operation of important programs and services.

Reasons for Selection:

1. Integration with Microsoft Products: Seamless compatibility with other Microsoft software enhances operational efficiency.
2. Optimize for Future-Ready Infrastructure: Light up new possibilities with improved scalability, larger virtual machines, and GPU partitioning across VMs built to support AI workloads.
3. Protect with multilayered security: Help protect data and business-critical applications with modernized identity management and new safeguards against brute-force and lateral attacks.
4. Scalability: It can be easily scaled to small, medium, and large network environments.
5. Support and Documentation: Full Microsoft support, plus an enormous IT community with lots of troubleshooting/enhancing contributions
6. Hyper V: The live migration and dynamic resource allocation of Hyper-V enable easy, scalable, and flexible management of virtual machines. This allows businesses to boost their productivity, save on equipment costs, and reduce technological complexity thanks to Hyper-V.
7. Remote Desktop Services: It enables efficiency and collaboration by allowing users to connect to resources from anywhere using a variety of devices. Remote Desktop Services allows the authorization of users and deployment of programs uniformly with highly secured consolidated management. It provides Virtual Desktop Infrastructure, VDI and session-based virtualization for effective resource utilization.
8. Security Update: Security updates automatically keep the user updated regarding the latest threats and vulnerabilities in their system. The updates ensure that all known threats have been patched against and may help prevent malware from taking hold in your system. Security updates can also help to improve performance and better configure options within your system.

Conclusion, The combination of Windows 11 and Windows Server ensures a robust, secure, and user-friendly environment for both end-users and administrators. This selection will align with the organization's goals of maintaining efficiency, scalability, and a secure IT infrastructure. With these solutions, we will ensure that the performance, reliability, and integration of all systems are seamless.

**5.Centralized Network Management and Secured Internet Access**

Such implementation areas include, centralized network management, secured access to the internet, a strong intranet and comprehensive network security. Below are analyses of such components with their benefits in relation to improved network performance as well as their impacts supported by relevant references.

**Centralized Network Management**

A centralized network is created around one master central server that hosts the majority of the management and data processing functions. Other types of servers can connect to this master server and control other specific functions, but other servers cannot independently function without the central server.

Client systems and users cannot directly access resources or services on other servers unless they are routed through the centralized master server. If the central server crashes, the whole network crashes with it. A small business with a single domain controller (DC) is an example of a centralized network. They may have a separate database server or print server, but that server relies on the DC for clock synchronization, identity management and authentication, DHCP, and other vital network services.

**Benefits of Centralized Network Management:**

1. One central server is quicker to deploy because you have to configure one with no load balancing or orchestration.
2. You can add and remove client systems, users, and other servers with ease, instead of having to wait for replication across decentralized or distributed servers.
3. Centralized networks are less expensive because you use a limited number of servers; that means fewer licenses and less equipment.
4. Simplified Administration: Centralized control limits the complexity of managing multiple devices and allows consistent configuration across the network.
5. Enhanced Monitoring: In real time, monitoring allows IT staff to quickly pinpoint and resolve performance bottlenecks or security incidents.
6. Improved Control:The IT organization will have a better understanding and control of the enterprise WAN, which ensures proper delivery of services with close to zero downtime.

**Secured Internet Access**

Secure Internet Access can be termed as all those measures and technologies put in place that secure the path between the endpoint and the Internet. SIA ensures the privacy and integrity of data and a safe browsing experience. It consists of practices and technologies put in place to protect networks, devices, and data.

The concept of SIA has evolved with the progress of the internet, and till the turn of the last decade, especially around the late 1990's, when some security protocols like the Secure Sockets Layer and Transport Layer Security made people start taking cognizance of this factor, malicious hackers continuously launched new viruses, Trojans, and other forms of attacks. Security technologies continued to further develop and propagate, creating anti-virus/spyware software, web filters, firewalls, and web browsers that utilized encryption-otherwise known as HTTPS-and other security tools. Finally, Zero Trust Security arrived, and the paradigm around SIA shifted, with internet security becoming a larger domain of threat protection.

Modern SIA is also made up of many components and functions, but these components and functions are more accessible, and stronger than ever. Most of the end-user business traffic is web-based and sending data across the internet using the HTTPS protocol. The good thing is that SIA practices and technologies are a must for companies and people who rely on web applications and internet-based activities to run their business.

**Benefits of Secured Internet Access:**

1. Increased security posture: SIA has dramatically reduced the incident of cyber-attacks, data breach, and unauthorized access. Secure Internet Access solutions make sure that the remote and hybrid workers operate in a secure environment.
2. Enhanced productivity: Employees will be able to operate from anywhere without compromising security. It would return to uninhibited use of corporate resources, effective collaboration, and assurance of high performance.
3. Cost efficiency: The cloud-based security solutions replace the expensive on-premise hardware. They have, as a rule, a centralized management which helps the IT team to save their time spent on administrative work. Scalability of cloud solutions enables companies to scale up and down the cloud consumption so they do not pay for more than what is used.
4. Improved User Experience: Remote browser isolation and cloud security technologies provide seamless, secure access to web and cloud applications without interfering with the user experience.
5. Regular intelligence, security, and feature updates are given to the SIA solutions. These updates fix new vulnerabilities to keep abreast of the latest standards and regulations for security.
6. Extensive SIA audit trails provide a record of all activities relating to security, thus facilitating compliance verification and incident investigations.
7. The user training and awareness programs included with some SIA solutions help employees understand and adhere to regulatory requirements.
8. SIA solutions provide detailed logging and reporting capabilities that capture and record all network activities, making it easier to demonstrate compliance during audits.

Conclusion, This can be achieved by implementing centralized network management, secured internet access, and a robust intranet that provides improved network performance, enhanced security, and greater operational efficiency. It will also be aligned with the organizational goals to provide security, scalability, and high performance in IT infrastructure.

**Intranet**

An intranet is a private computer network that assists employees in the sharing of information, resources, and applications securely within the organization. It's a digital workspace exclusive to an organization, which serves as a central platform for communication, collaboration, and knowledge management.

Many businesses, from the smallest to large corporations, among others, rely on intranets for everyday business. Intranets are home portals of those organizational sites from which employees can upload files, view any notices put out by the company, or send messages to other employees.

In fact, according to the State of the Intranet and Future of Employee Technology report by Simple, nearly nine in ten respondents, or 87%, agree that intranets facilitate strong communication in the workplace. This cements its role in fostering a sense of community and employee involvement.

**Benefits of Intranet:**

1. 1.Improves Internal Communication: The primary benefit of using an intranet is that it supports internal team communication. Intranets are highly effective for this purpose, as evidenced by the 87% of respondents who acknowledge their role in facilitating strong communication.Intranets enable your company to centralize all workplace communication, thus allowing employees to communicate with each other and collaborate easily across departments. More directly, they help streamline communication channels. They allow teams to share updates, work on projects together, and create stronger working relationships.
2. Connects Your Company Across Locations and Time Zones: A modern business is likely to have a distributed workforce. You may be a medium-sized company with multiple offices, a large enterprise with teams around the world, or a fully remote organization across several time zones. In such scenarios, centralized communication keeps everyone on the same page and up to speed regardless of where they are located or their working hours. A well-functioning intranet allows for easy information sharing, provides a platform for team collaboration, and ensures everyone has access to the same resources and updates. This not only bridges geographical gaps but also helps to create a stronger sense of community and shared purpose within the organization.
3. Simplifies Employee Onboarding: Hiring and onboarding often involve a considerable investment of time and resources from various departments, including human resources, management, and IT. Traditional onboarding processes can be lengthy, involving multiple forms, training sessions, and information overload for new hires. This can lead to delays in productivity and a less-than-ideal first impression for new employees. Leveraging intranets effectively can lead to a significant reduction in employee onboarding time, with organizations seeing an average decrease of 20%. Intranets allow employees to quickly go through onboarding by accessing important resources. Newly joined employees can self-learn company policies, onboarding training videos, and much more. As such, these workers feel that they will be integrated well into the working culture faster while their onboarding is sped up due to self-determination.

**Network Security**

It is every company or organization dealing with a large amount of data which has an extent of solutions against most cyber threats. Again, this is a general term that encompasses software and hardware solutions together with procedures, guidelines, and setups when it comes to network usage, accessibility, and general threat protection.

The most basic example of Network Security is password protection which the user of the network chooses. In recent times, Network Security has become the central topic of cyber security with many organizations inviting applications from people who have skills in this area. The network security solutions protect various vulnerabilities of the computer systems such as users, location, data, devices, and applications.

Network Security protects your network and data from breaches, intrusions and other threats. This is a vast and overarching term that describes hardware and software solutions as well as processes or rules and configurations relating to network use, accessibility, and overall threat protection.

Network Security involves access control, virus and antivirus software, application security, network analytics, types of network-related security (endpoint, web, wireless), firewalls, VPN encryption and more.

**Benefits of Network Security**

1. Network security helps in protecting clients information and data, ensuring reliable access helps in protecting the data from cyber threats.
2. Network Security protects the organization from heavy losses that may have occurred from data loss or any security incident.
3. It overall protects the reputation of the organization because it protects the data and all confidential items.
4. Protection against unauthorized access: Firewalls and authentication systems prevent unauthorized users from accessing sensitive information or disrupting network operations.
5. Data confidentiality: Encryption technologies ensure that data transmitted over the network remains confidential and cannot be intercepted by unauthorized parties.
6. Malware and Viruses Prevention: Network security measures such as antivirus software and intrusion detection systems (IDS) help in the detection of malware, viruses, among other malicious threats before they could infect systems.
7. Secure Remote Access: Virtual private networks (VPNs) and other secure remote access measures allow the employees to work remotely without compromising the security of the organizational network and data.

**References**

Hiley, C. (2023, November 15). *IPv4 vs IPv6: The Difference Explained*. CyberNews.<https://cybernews.com/what-is-vpn/ipv4-vs-ipv6/>

Margaret. (2021, September 30). *IPv4 Vs IPv6, What Is IPv4, What Is IPv6, IPv6 to IPv4 Basis - FS.COM | FS Community*. Knowledge. <https://community.fs.com/article/ipv4-vs-ipv6-whats-the-difference.html>

Kapoor, A. (2023, May 5). *Understand the Difference Between IPv4 and IPv6 | Simplilearn*. Simplilearn.com. <https://www.simplilearn.com/tutorials/cyber-security-tutorial/difference-between-ipv4-and-ipv6>

*IPv4 versus IPv6: the difference explained*. (2025). Prefixbroker.com. <https://www.prefixbroker.com/news/ipv4-versus-ipv6-the-difference-explained/>

Hosting, S. W. (n.d.). *IPv4 vs. IPv6 - What’s the difference, and which is faster?* SiteGround Knowledge Resources. <https://www.siteground.com/kb/ipv4-vs-ipv6/>

www.naukri.com. (2024). *Code 360 by Coding Ninjas*. Naukri.com. <https://www.naukri.com/code360/library/ipv6>

Raymond, D. (2024, January 10). *Top 10 Pros and Cons of Windows 11*. AceProject. <https://www.aceproject.com/blog/top-10-pros-and-cons-of-windows-11-9387815/>

Computer Trouble Shooters Admin. (2022, December 21). *Windows 11 Advantages, Disadvantages and differences over Windows 10? - Computer Troubleshooters Australia*. Computer Troubleshooters Australia - Just Another Brandicoot Site. <https://computertroubleshooters.com.au/windows-11-advantages-disadvantages-and-differences-over-windows-10/>

*The Benefits & Flexibility of Windows Server*. (n.d.). MyChoiceSoftware.com. <https://www.mychoicesoftware.com/blogs/news/the-benefits-flexibility-of-windows-server>

Solarwinds. (n.d.). *What Is Windows Server?—IT Glossary | SolarWinds*. Www.solarwinds.com. <https://www.solarwinds.com/resources/it-glossary/windows-server>

Microsoft. (n.d.). *Windows Server 2019 | Microsoft*. Www.microsoft.com. <https://www.microsoft.com/en-us/windows-server>

*Windows Server*. (2020, October 26). Wikipedia. <https://en.wikipedia.org/wiki/Windows_Server>

*What is Windows Server? Definition, Key Features*. (2024, June 5). Motadata.<https://www.motadata.com/it-glossary/windows-server/>

*Everything You Need to Know about Windows 11 Features*. (2023). Wondershare.com. <https://repairit.wondershare.com/windows-tips/windows-11-new-features.html>

Systems, Z. P. E. (2021, September 1). *Centralized vs. Distributed Network Management: Which One to Choose?* ZPE Systems. <https://zpesystems.com/centralized-vs-distributed-network-management-zs/>

*Barracuda*. (2025, January 2). Barracuda Networks. <https://www.barracuda.com/support/glossary/sia>

Data, S. (2022, November 29). *Stronghold Data*. Stronghold Data. <https://strongholddata.com/network-security-management-benefits>

*The Advantages and Disadvantages of an Intranet*. (2022, November 21). Bloomfire. <https://bloomfire.com/resources/advantages-disadvantages-of-intranet/>

‌

Mehdi. (2025). *Intranet Security Best Practices*. Intranet Security Best Practices. <https://www.dotcms.com/blog/intranet-security-best-practices>

*Intranet: Definition, Use, Benefits, and Examples*. (2024). Threado.com. <https://www.threado.com/blog/intranet-definition-use-benefits-and-examples>

ajith. (2024, July 12). *Top Benefits of Network Security*. Digitdefence. <https://digitdefence.com/blog/top-benefits-of-network-security>

*What is Network Security*. (2022). Check Point Software. <https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/>

geeksforgeeks. (2020, January 30). *Network Security*. GeeksforGeeks. <https://www.geeksforgeeks.org/network-security/>

‌