UNIVERSITY OF NAIROBI
FACULTY OF SCIENCE AND TECHNOLOGY
DEPARTMENT OF COMPUTING AND INFORMATICS

SCS 3309: NETWORK MANAGEMENT (2024/2025)

PROJECT TITLE: ‘KOITALEL ARAP SAMOEI UNIVERSITY COLLEGE (KSUC)NETWORKING IMPLEMENTATION

Submission Date: 22nd December 2024

•

Table of Contents

SECTION 1: LAB PROJECT DELIVERABLES SUMMARY

i. List and explain four factors that you will consider when designing this campus network (5 marks)

Four Factors to Consider in Network Design (5 marks)

1. **Scalability**
   - The network should support future growth in terms of users, devices, and services without requiring a complete redesign.
2. **Reliability**
   - Ensure minimal downtime using redundant links, reliable hardware, and efficient failover mechanisms.
3. **Performance**
   - High-speed connectivity with efficient bandwidth utilization to avoid congestion and ensure smooth operations for all users.
4. **Cost Efficiency**
   - Use cost-effective equipment while ensuring that the performance, scalability, and reliability needs are met.

ii. Develop a project plan clearly showing the steps and milestones you will take in executing this project from start to finish (5 marks).

Phase 1: Requirement planning and analysis (2nd - 6th Dec): ● **2nd December to 6th December 2024:** Research on the network requirements and discussing the network topology ● **The research was guided by the four key design considerations:** scalability, security, availability and manageability. The design ensured that all these are taken into account. ● Develop initial topology and high-level design defining network requirements and **Deliverables**: Network topology
Phase 2: Design and discussion of the implementation (9th December to **13th December 2024):** ● Preparing draft design document network topology on paper ● **Implementing the network topology and devices in a packet tracer.** The process include iteration on the devices such as he switches, routers and end devices in line with the needs ● **Addressing and subnetting:** after drawing the physical topology and representing in the Cisco packet tracer, we discussed the network and address allocation through technologies such as subnetting and use of VLANs after development of the subnets, we embarked on documenting addressing and configuration decisions to promote management, communicating and security between the network devices **Deliverables:** o Comprehensive IP addressing scheme (Private: 172.16.0.0/16 and subnet allocation o VLAN segmentation.

Phase 3: Construction Phase: Connecting the Campus network (16th December to 20th December 2024): This phase included actual configurations or the network to establish connectivity. Tasks include • Configuration of the access, core and distribution routers • Set up NAT and DHCP • Configuring protocols such as the sop an VLANs • Static configuration of devices • Develop authentication mechanisms. • **Service and Server Integration** • Configuration of connections to WAN
Phase 4: Cutover Phase: Simulation, Testing and Optimization (21st - 22nd December 2024): **The final phase involved final testing of the captures network and finalist ion before submission. Tasks included:** • Testing the network for connectivity and errors • Final testing and recording videos • presentation of the final project and report

iii. Design the IP address scheme for the entire campus. The IP address scheme will be based on private IP addresses (10.X.X.X); (10 marks)

IP Allocation Phases

1. WAN Links and Core Routing:
    - Point-to-point links use /30 subnets to minimize waste (only 2 usable addresses per link).
2. Servers:
    - We developed dedicated /24 subnets for critical server operations (Web, Email, ERP, SMIS), allowing for scalability.
3. Departments and Device Subnets:
    - /25 subnets provide up to 126 usable addresses, sufficient for departmental devices while leaving space for growth.
4. Access Points and Wireless:
    - Each access point uses a departmental VLAN IP range, with devices connecting via DHCP.

2. IP Addressing Table

IP Address Device/Use

105.12.32.8	Network ID (Reserved)
105.12.32.9-11	Point-to-Point Links (Border Router and Data Centre Switch)
105.12.32.12	NAT Pool
105.12.32.13	Web Server
105.12.32.14	Email Server
105.12.32.15	Broadcast Address (Reserved)

Private IP addressing with VLSM

Building	Department	Subnet	Network Address	First Usable IP	Last Usable IP	Broadcast Address	Total Hosts	VLAN ID
Building 1	Finance	172.16.1.0/26	172.16.1.0	172.16.1.1	172.16.1.62	172.16.1.63	62	101
Building 1	Human Resource	172.16.1.64/26	172.16.1.64	172.16.1.65	172.16.1.126	172.16.1.127	62	102
Building 1	Administration	172.16.1.128/26	172.16.1.128	172.16.1.129	172.16.1.190	172.16.1.191	62	103
Building 1	Procurement	172.16.1.192/26	172.16.1.192	172.16.1.193	172.16.1.254	172.16.1.255	62	104
Building 2	Civil Engineering	172.16.2.0/25	172.16.2.0	172.16.2.1	172.16.2.126	172.16.2.127	126	201
Building 2	Mechanical Engineering	172.16.2.128/25	172.16.2.128	172.16.2.129	172.16.2.254	172.16.2.255	126	202

Building 2	Electrical Engineering	172.16.3.0/25	172.16.3.0	172.16.3.1	172.16.3.126	172.16.3.127	126	203
Building 2	Computer Lab	172.16.3.128/25	172.16.3.128	172.16.3.129	172.16.3.254	172.16.3.255	126	204
Building 3	Computer Science	172.16.4.0/25	172.16.4.0	172.16.4.1	172.16.4.126	172.16.4.127	126	301
Building 3	Physics	172.16.4.128/25	172.16.4.128	172.16.4.129	172.16.4.254	172.16.4.255	126	302
Building 3	Mathematics	172.16.5.0/25	172.16.5.0	172.16.5.1	172.16.5.126	172.16.5.127	126	303
Building 3	Computer Lab	172.16.5.128/25	172.16.5.128	172.16.5.129	172.16.5.254	172.16.5.255	126	304
Building 4	IT Department	172.16.6.0/26	172.16.6.0	172.16.6.1	172.16.6.62	172.16.6.63	62	401
Building 4	Data Centre Servers	172.16.6.64/26	172.16.6.64	172.16.6.65	172.16.6.126	172.16.6.127	62	402
Building 5	Male Hostel Wireless	172.16.7.0/25	172.16.7.0	172.16.7.1	172.16.7.126	172.16.7.127	126	501
Building 5	Female Hostel Wireless	172.16.7.128/25	172.16.7.128	172.16.7.129	172.16.7.254	172.16.7.255	126	502

Device IPs

Device Category	Device Name	IP Address	Subnet	VLAN ID	Purpose
Border Router	Management Interface	172.16.0.1	172.16.0.0/24	1	ISP Connection Management
Core Switches	Core Switch 1	172.16.0.2	172.16.0.0/24	1	Core Network Management
	Core Switch 2	172.16.0.3	172.16.0.0/24	1	Core Network Management

Distribution Switches	Building 1	172.16.1.254	172.16.1.0/24	101-104	Building Distribution
	Building 2	172.16.2.254	172.16.2.0/24	201-204	Building Distribution
	Building 3	172.16.3.254	172.16.3.0/24	301-304	Building Distribution
	Building 4	172.16.6.126	172.16.6.0/24	401-402	Data Center Distribution
	Building 5	172.16.7.254	172.16.7.0/24	501-502	Hostel Distribution
Access Points	Male Hostel AP	172.16.7.1	172.16.7.0/25	501	Male Hostel Wireless
	Female Hostel AP	172.16.7.129	172.16.7.128/25	502	Female Hostel Wireless

iv. Using the Hierarchical Network Design model, design a Network with the above mentioned Requirements and which takes into account the factors considered in (i) above. Avoid security concerns except where explicitly stated as required. The network design should be drawn using any suitable modeling tool e.g. MS visio and clearly showing the details below. (10 marks)

Page 1 of 2

a. Locations/buildings

b. Network devices

c. Links

d. IP blocks |

- **a. Locations/buildings**
  1. the locations and buildings were simulated in the topology showing the hierarchy from the access switches and distribution and core layer switches.
     - **Core Layer Switches**: Handle high-speed traffic between distribution switches and WAN connections.
     - **WAN Router**: Provides connectivity to external networks such as the internet.

- **Distribution Switches**: Connect core switches to access switches in individual buildings, segregating traffic for specific areas.
- **Access Layer Access Points and PCs**: Provide end-user connectivity, including departmental PCs, printers, and access points for wireless devices.
  The details are further explained further on page 11 of the report

b. Network devices

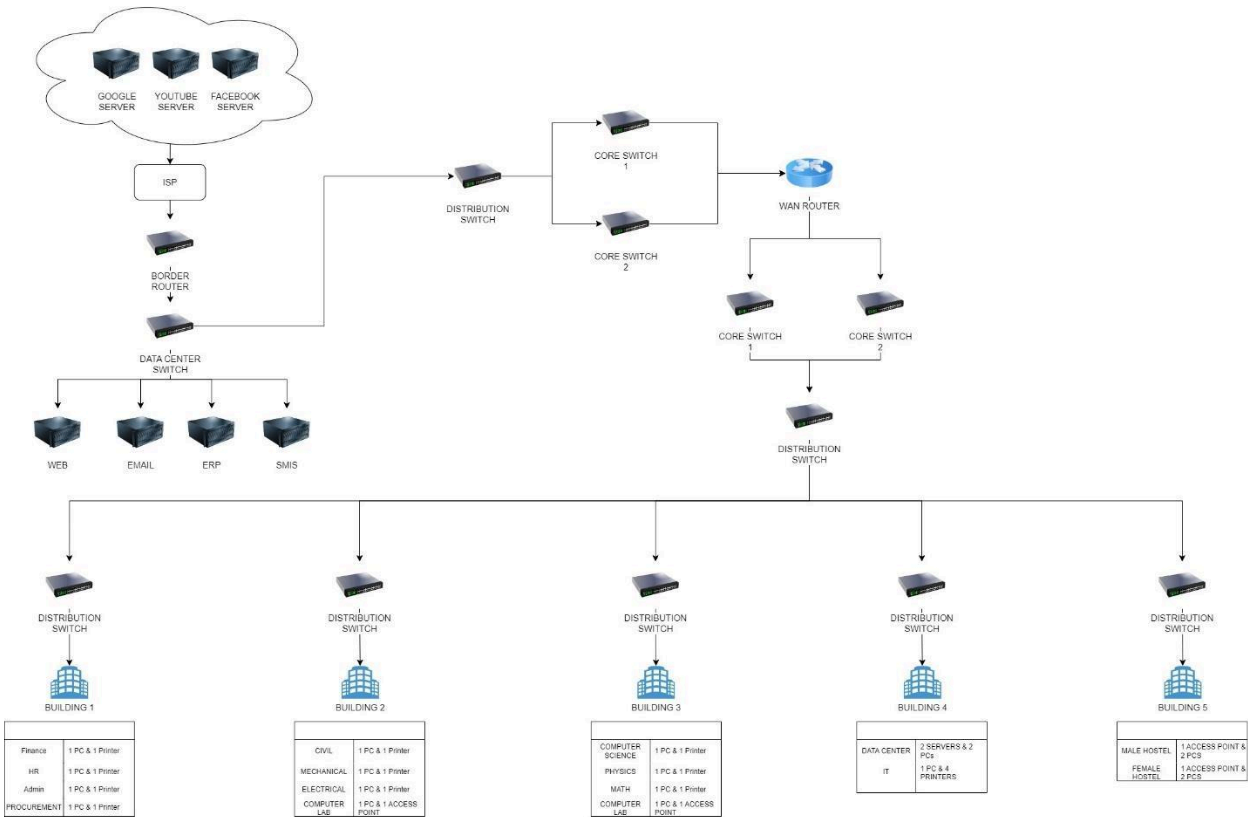
- these include the layer 2 and 3 switches used at access, distribution and core and border router which played the role of connecting devices
- End devices such as computers and laptops provided services to the end user such as students and faculty to communicate and do their work.
- the servers provided storage an access of information and data

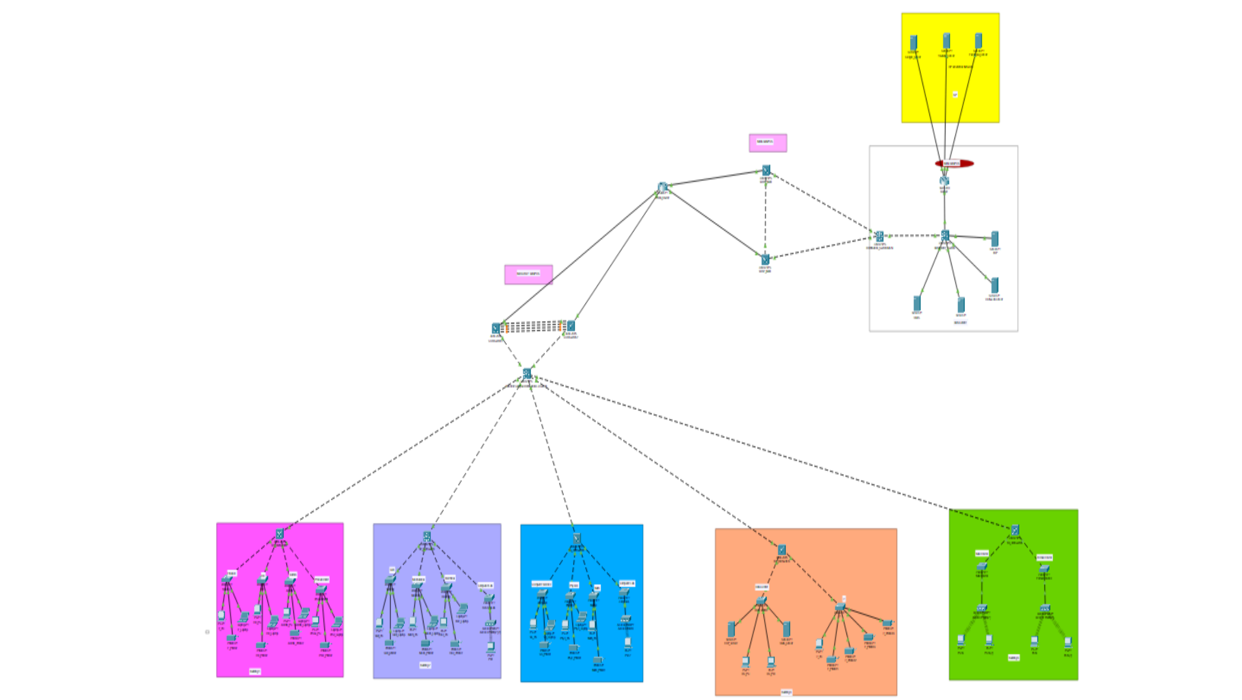
c. Links

- The links were varied depending on the devices and the rules therein.
- The links between access switches and the end devices were mainly fast Ethernet and were sufficient for data transfer and management
- At the hostel and computer lab level, because of the large number of the students, we used wireless access point links that were flexible to allow more people access. The mobility of students also guided the dynamic routing
- The links between the switches were implements through Gigabit Ethernet to provide a higher bandwidth for the data from the different subnets
- Links between the core switches were aggregated into an ether channel to provide even greater bandwidth for the network

d. IP blocks

- The network 1172.16.0.0 was divided into 11 blocks of subnetworks and each block further divided into variable length through vlans to accommodate the available PCs without wasting much addresses. This if explained further in the report


GOOGLE SERVER
YOUTUBE SERVER
FACEBOOK SERVER
ISP
BORDER ROUTER
DATA CENTER SWITCH
WEB
EMAIL
ERP
SMIS
DISTRIBUTION SWITCH
CORE SWITCH 1
CORE SWITCH 2
WAN ROUTER
CORE SWITCH 1
CORE SWITCH 2
DISTRIBUTION SWITCH
DISTRIBUTION SWITCH
BUILDING 1
Finance 1 PC & 1 Printer
HR 1 PC & 1 Printer
Admin 1 PC & 1 Printer
PROCUREMENT 1 PC & 1 Printer
DISTRIBUTION SWITCH
BUILDING 2
CIVIL 1 PC & 1 Printer
MECHANICAL 1 PC & 1 Printer
ELECTRICAL 1 PC & 1 Printer
COMPUTER LAB 1 PC & 1 ACCESS POINT
DISTRIBUTION SWITCH
BUILDING 3
COMPUTER SCIENCE 1 PC & 1 Printer
PHYSICS 1 PC & 1 Printer
MATH 1 PC & 1 Printer
COMPUTER LAB 1 PC & 1 ACCESS POINT
DISTRIBUTION SWITCH
BUILDING 4
DATA CENTER 2 SERVERS & 2 PCs
IT 1 PC & 4 PRINTERS
DISTRIBUTION SWITCH
BUILDING 5
MALE HOSTEL 1 ACCESS POINT & 2 PCS
FEMALE HOSTEL 1 ACCESS POINT & 2 PCS



v. The network should subsequently be implemented in the Cisco packet tracer simulation software, with necessary devices and full configuration. Install at least 2 PC/Laptop for each individual network. (video recording) (30 marks)

a. You will be required to do a presentation of your simulation

b. Save the commands on a notepad

c. Ensure you save your network configuration.

Deliverables:

1. Packet Tracer simulation file.
2. Cnfiguration commands.
3. Presentation video demonstrating the simulation and network tests.

Simulation presented include:

1. Overview of the network topology
2. Explaining the 3-level implementation
3. Implementation using design considerations
   - **a. Scalability**
     - o Demonstration of sub netting and vlans
     - o Implemented VLANs and configured inter-VLAN routing
     - o Assigning of IPs as per the scheme
     - o DHCP for dynamic IP allocation
   - **b. Availability**
     - o Connection links implementation – fa, gig, EtherChannel
     - o Protocol used EIGRP
     - o Routing tables
     - o Redundancy technologies
   - **c. Security**
     - o Security implemented (passwords)
     - o firewall
   - d. **Management-** naming of the PCs , blocks etc; patterned allocation of addresses, devices and cables e.g. allocation of addresses starts with first computer, then printer then the DHCP computers

Testing:

- Test inter-department communication (VLANs).
- Validate internet restrictions (Google/YouTube).
- Check server access and dynamic IP allocation for hostels.

v. After completion of your implementation you should be able to test the conditions imposed.(video recording). (10 marks)

Testing and Validation (video recording) include

- Conduct ping tests across VLANs.
- Verify access restrictions for Google/YouTube.
- Confirm dynamic IP allocation via DHCP in hostels.
- Ensure server access policies are enforced.
- Connectivity between the same vlan, different vans and buildings and
- Access point connections
- Connection to main campus
- Routing protocols
- Network address translation

SECTION2: PROJECT REPORT

1. INTRODUCTION

Koitalel Arap Samoei University College (KSUC) is a constituent college of the University of Nairobi located in the expansive Nandi County. The university wishes to install networking infrastructure at its Mosoriot campus. The work includes setting up LANs on both copper (inside buildings) and fiber for backbone interconnecting all buildings, server-room LAN, and wireless LAN. Further details and conditions for setting up the network is attached in appendix 1.

This report represents group 4 implementation of the task and development of the Koitalel Arap Samoei University College campus network.

a. Project Objectives and Scope

As we developed the Koitalel Arap Samoei University College campus network the main goal was to develop a campus network that is scalable, available secure and manageable. The campus network would also be able to communicate and connect with the main campus. In order to achieve the goal, were guided by the following objectives:

1. To implement a network that is scalable to accommodate more students and staff
2. To ensure availability of the network connectivity for students and staff and critical services
3. To implement basic security features
4. To ease network manageability

The project was implemented in CISCO packet tracer Vs 8 using the available technologies and services. The implementation was largely used LAN technologies with a WAN connection form Mosoriot to the main campus.

b. Project Plan

Table 1: Project Timeline

Phase 1: Requirement planning and analysis (2nd - 6th Dec): ● **2nd December to 6th December 2024:** Research on the network requirements and discussing the network topology ● **The research considerations were guided by the four key design considerations:** scalability, security, availability and manageability. The design ensured that all these are taken into account.
Phase 2: Design and discussion of the implementation (9th December to **13th December 2024):** ● Drawing the draft network topology on paper ● **Implementing the network topology and devices in a packet tracer.** The process include iteration on the devices such as the switches, routers and end devices in line with the needs ● **Subnetting discussions**, after drawing the physical topology and representing in the Cisco packet tracer, we discussed the network and address allocation through technologies such as subnetting and use of VLANs these were to be implemented to promote management, communicating and security between the network devices ● **Addressing:** after development of the subnets, we made addressing and configuration decisions

Phase 3: Construction Phase: Connecting the Campus network (16th December to 20th December 2024):

This phase included actual configurations or the network to establish connectivity. Tasks were:

- Configuration of the access, core and distribution routers
- Configuring protocols such as the sop an VLANs
- Static configuration of devices
- Configuration of connections to WAN

Phase 4: Cutover Phase: Simulation, Testing and Optimization (21st - 22nd December 2024):

The final phase involved final testing of the captures network and finalist Tasks included:

- Testing the network for connectivity and errors
- Final testing and recording videos
- presentation of the final project and report

2. METHODOLOGY

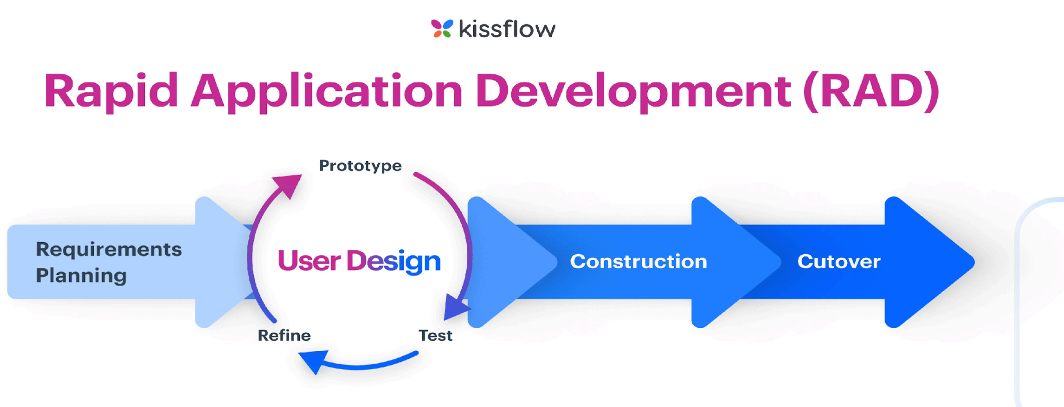
a. Project Analysis and Design

The project was implemented as part of the requirements submitted in partial fulfilment of the requirements for the_SCS 3309 Network Design- Lab 1-2024-2025 contributing to the award of Bachelor of Science in Computer Science of the University of Nairobi. The project aimed at implementing a network for a satellite Campus. Before agreeing on the design methodology, we discussed the task and agreed on the **final** model of the network and topology, considering the group's capability and skills to implement the project.

b. Network Design Methodology: Rapid Application Development Model (RAD)

Based on the academic requirement, the output was a network implementation simulated on a Cisco packet tracer, which is a software product. The team thus selected Rapid Application Development (RAD) model, which is a software development methodology to guide the process. The RAD is a model that uses an incremental but iterative approach to software development. The RAD model in implemented in four stages: **1)** Requirement planning **2)** Design **3)** Construction and **4)** Cutover phase.

Figure 1: The Rapid Application Development Model (RAD)



The team selected the RAD Model for the implementation of the project, as it is suitable for applications which are developed in quickly. In addition, the design and construction phases are iterative, which mapped well with our project process plan of providing the chance for refining the design and construction of the network.

c. Development Process

1) ***Requirement planning and analysis phase:*** At this phase the activities included documenting all the requirements that were needed to undertake the successful project and create the network
   - **The design considerations:** Gathering the requirements for developing the network was guided by the four key design considerations: **scalability, security, availability and manageability.** Reviewing and deciding on the design considerations ensured that all these are taken into account to develop a workable Mosoriot Campus network
     - **Scalability:** The network had to be scalable to accommodate more students and staff and provide room for expansion to different departments or within the campus. This was implemented through technologies such as subnetting and use of addressing that would accommodate more devices without wasting many Ip addresses as well as adding redundancy for devices such as switches that allowed for further connections.
     - **Availability:** To ensure availability of the network connectivity for students and staff and critical services we implemented protocols such a s as LAG and Spanning Tree Protocol. At the higher level we also created redundant core and distribution switches to allow for linkages and avoid failures
     - **Security:** we implemented basic security features such as use of passwords
     - **Manageability**: To ease network manageability, we named the various devices to reflect their positions as well as standardized configurations to form a manageable pattern
   - **Hardware and software requirements:** Based on the agreement of the design considerations, we listed and grouped the hardware and software requirements, as well as the team resources.

2) ***Design phase:*** The design phase involved developing the models and prototype that would best present our network. Much of the effort was on development of the different sections and integrating them to culminate into a flowing network. These building blocks included at each layer of access, distribution and core layers. The key activities therein included.
   - **Drawing the network topology on paper:** after establishing the hardware and software requirements, we first drew the high-level network topology on paper to represent the basic structure and flow. This was then refined through iterations as we discussed the devices need and rationale.
   - **Implementing the network topology on Cisco packet tracer:** the paper designed network topology were then transferred and implement on Cosco packet tracer. The packet tracer included details such as the specific routers, switches and end devices with their proposed connections.
   - **Subnetting and VLAN addressing:** this involved discussion on division of the private network and allocation of addresses to cover all the sections. Technologies and protocols used included subnetting and use of Volans division to address the different grouped blocks of devices.

3) ***Construction phase:*** The construction phase was the heart of the network development project as it involved configuring the actual linkages and connection of the devices in the CISCO Packet Tracer. The activities included

- Configuration of the access, core and distribution routers – to connect to each other and to the devices

- Configuring protocols such as the OSPF an VLANs to enable dynamic routing and excluding local network access for different departments.
- Static and dynamic configuration of devices
- Configuration of connections to WAN to the internet and the main campus

4) ***Cutover phase:*** This phase involved mainly the completion of the networking project and included wo key activities:
   - **Testing:** after completion of the design and construction of the network in Cisco packet tracer and inclusion of the different technologies the network was tested by different colleagues, each testing a protocol used and then final testing to ensure integration of the network. Few changes were made at this stage, mainly with minor configuration to ensure full connectivity. by different team members, the modules were brought together for simulation and interactive element in
   - **Final Presentation:** This phase included recording videos to simulate the network and demonstrating the different methods and technologies to ensure a successful campus network.

3. IMPLEMENTATION RESULTS AND DISCUSSION

The implementation of the project was undertaken in line with the methodology outlined, and presented within the four stages of the RAD model. The design and construction phase had a lot of iterations and cycles to support refining of the final product.

a. Requirement Planning and Analysis Phase

1) Functional Requirements

- **System Qualities**

Reliability: the system should be able to be accessed by different formats video players
Availability: the clip should be accessed from anywhere and anytime using different gadgets
Scalability: the clip should allow for additional of more scenes and viewpoints for rendering

2) Non-Functional Requirements

These were the requirements that the network was supposed to do for the successful implementation. The functional requirements were mapped into the **design considerations** that were important needed to the network. The four key design considerations were scalability**, security, availability and manageability.** Reviewing and deciding on the design considerations ensured that the Mosoriot Campus network would be able to perform its tasks.

Scalability: The network had to be scalable to accommodate more students and staff and provide room for expansion to different departments or within the campus. Key technologies implemented to allow scalability included:

- **subnetting** the system would be able to accommodate as many subnetworks and addresses as possible under the network 172.16.10.0/16. subnetting enabled the campus to use the same network and divide it into smaller subnetworks within its campus use of addressing that would accommodate more devices without wasting many Ip addresses as well as adding redundancy for devices such as switches that allowed for further connections. The subnet was implemented at building level with each building having a different subnet. This was so because a building was an area to host a subnetwork The subnets were connected by layer 3 witches a building level and int departments level.

- **Use of vans:** the use of vans was implemented to further partition the subnets in each building into different departmental networks and making use of the user ids since the different departments had fewer people thus giving room or further subdivision of the subnets.

Availability and reliability: To ensure availability of the network connectivity for students and staff and critical services we implemented protocols such as LAG and Spanning Tree Protocol.

- **Redundant devices:** At the higher level we also created redundant core and distribution switches to allow for linkages and avoid failures
- **EtherChannel (LAG).** the EtherChannel was implemented between the access switches and distribution switches to allow for more bandwidth and thus better availability of the network.
- **The spanning tree protocol** (STP) was implemented to reduce factors that reduce network efficiency such as duplicate messages and broadcast storm, while still allowing for redundancy and increase availability of the network, and optimize bandwidth for the network and devices.
- **The RIP** was implemented to enable dynamic routing, which would save time and reduce errors due to static configuration especially in large networks. As the net hop is limited, the rip would still accommodate the network which has less than 10 routers

All these technologies were aimed at increasing availability of the network devices such as static configuration of shared network devices such as printers and servers also increased availability.

Security: the campus network had to be secure and allow only authorized access to its network and different end devices. This was addressed through implementing basic security features including as use of passwords to limit access to the network connection devices such as switches and routers. Others included static configuration of shared devices such as printers and servers and managers computers.

Manageability: To ease network manageability, we named the various devices to reflect their positions as well as standardized configurations to form a manageable pattern

Hardware and software requirements: Based on the agreement of the design considerations, we listed and grouped the hardware and software requirements, as well as the team resources.

- **Software components and technologies**

In addition to the basic operating system such as windows, two program software were key to the successful implementation of the work.

✔ CISCO Packet tracer - this was the simulation software where the virtual campus network was designed, drawn and configured. The team used the latest packet tracer version 8 ✔ The packet tracer offers the network devices and connections and protocols for simulation of networks	

✔ **Draw.io** – the software was used to draw and represent the top-level topology of the Mosoriot Campus network. The software was used as it was free, and user-friendly for drawing geometric and other shapes and objects.	

- **<u>Hardware requirements</u>**

For the hardware requirements, we analysed the components needed to implement the projects. The minimal hardware requirements recommended for the use of the Cisco packet tracer were

- Microsoft Windows 8.1, 10, 11 (64bit), Ubuntu 20.04 LTS (64bit) or macOS 10.14 or newer.
- amd64(x86-64) CPU
- 4GB of free RAM
- 1.4 GB of free disk space

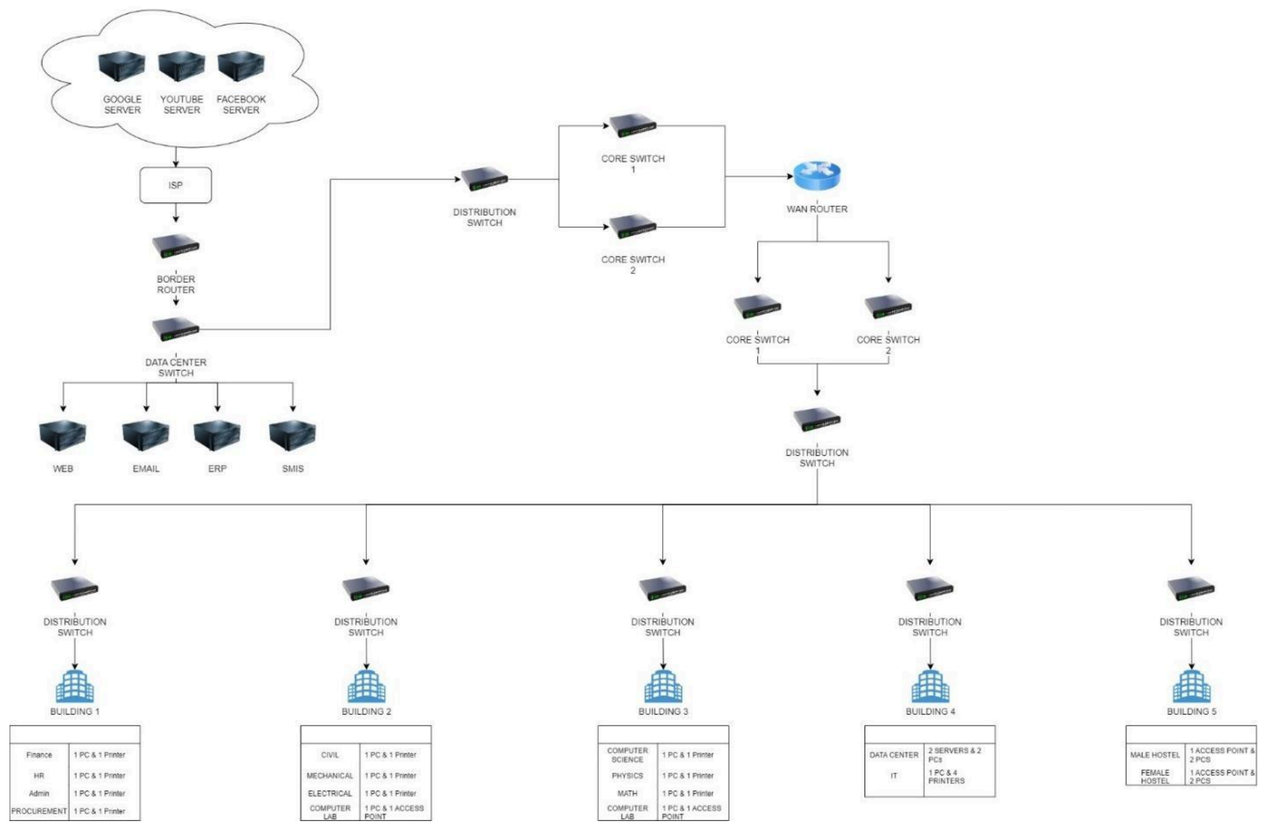
b. System Design Phase

***1) Drawing the high-level network topology*:** after establishing the hardware and software requirements, we first drew the high-level network topology on paper to represent the basic structure and flow. This was then refined through iterations as we discussed the device's need and rationale.

Osorio Campus Network Topology

The topology shows a high-level view of the topology consisting of networks from the 5 buildings each connected to a distribution switch which then connected to the core switch. Also connected to the network are the servers in the main campus, google Facebook and YouTube servers connected through a WAN router.

<u>Figure 2: Overview of Group 4 Mosoriot Campus Network Topology</u>



Key Components and Their Purpose

The network begins with the **Cloud and ISP Connection**, which provides internet access and external connectivity. The ISP serves as the primary link between the organization and the broader internet, ensuring centralized management of data flows. This connection allows the institution to monitor and control internet usage, guaranteeing secure and reliable access for all users.

Next is the **Border Switch**, which acts as the intermediary between the ISP and the internal network. This device is responsible for securely managing traffic entering and leaving the network, ensuring that data flows are properly regulated and unauthorized access is prevented. It provides a critical layer of protection and control for the network's perimeter.

The **Data Center Switch** serves as the central hub for institutional services, interconnecting key servers such as Web, Email, ERP, and SMIS. This centralization allows for efficient access to essential services, high availability, and easier management of critical resources. By hosting these servers in one location, the design simplifies troubleshooting and ensures users can reliably access the tools they need for daily operations.

At the core of the network are the **Core Switches**, which aggregate traffic from all distribution switches and handle high-speed data routing within the network. These switches ensure minimal latency and provide the capacity to manage large volumes of traffic, making them essential for maintaining a high-performance infrastructure. The core switches are designed for reliability, with redundancy to prevent single points of failure.

The **WAN Router** connects the internal network to external networks, enabling internet access and communication with other external systems. It serves as the gateway for wide area network, WAN connectivity, ensuring seamless integration with external services and remote resources.
The switches at the Mosoriot campus and main campus are added for redundancy and avoiding failure at three different levels :

- **Core Layer** is the highest-level in the hierarchy and includes the Core Switches that handle high-speed traffic between distribution switches and WAN connections, and the WAN Router which provides connectivity to external networks such as the internet.
- **Distribution Layer**: layer three Connect core switches to access switches in individual buildings, segregating traffic for specific areas.
- **Access Layer:** Provide end-user connectivity, including departmental PCs, printers, and access points for wireless devices.

The **Distribution Switches** form the middle layer of the hierarchy, connecting the core layer to individual buildings and departments. They manage the distribution of traffic, segregating it to prevent bottlenecks and ensuring efficient data delivery to various areas of the network. This layer also isolates faults to specific segments, enhancing overall network resilience.
Finally, the **Access Layer Devices**, which include PCs, printers, and wireless access points, provide direct connectivity to end-users. These devices are strategically deployed in buildings and floors to meet user needs, enabling seamless access to network resources and services. By placing these devices according to the organizational structure, the design ensures users in all departments can communicate and collaborate effectively.

Rationale for the choice

- **Scalability**: the hierarchical topology allows seamless addition of new devices or expansion of existing infrastructure.
- **Redundancy**: Dual core switches ensure fault tolerance and high availability.
- **Efficiency**: Segmentation using distribution switches optimizes traffic flow and reduces bottlenecks.
- **Security**: the centralized WAN connection and data center ensure secure data flow and access control.
- **Cost-Effectiveness**: Deploying a mix of wired and wireless access minimizes overhead costs while providing flexibility.

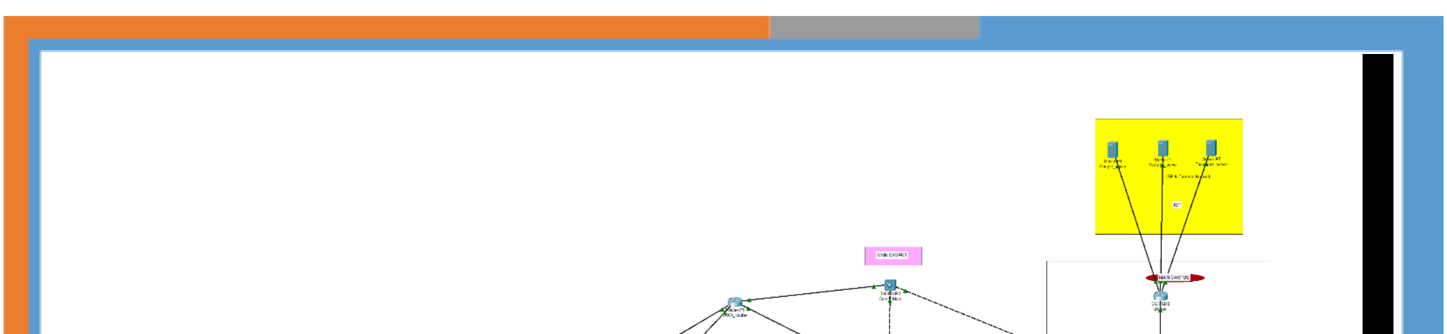
Advantages of the Design

- **Ease of Management** The layered structure ensures that network maintenance and troubleshooting are manageable and localized.
- **Flexibility** The design allows the addition of new departments or devices without disrupting the existing infrastructure.
- **Performance Optimization** Traffic segregation minimizes congestion, while core switches provide high-speed interconnectivity.
- **Reliability** Dual core switches and multiple distribution switches enhance network reliability and fault tolerance.

2) ***Implementing the network topology on Cisco packet tracer:***

The implementation of the network in the packet tracer included details such as the specific routers, switches and end devices with their proposed connections. With the final storyline and models, we developed a graphical presentation of the system architecture below on the packet tracer.

Figure 3: Diagram showing the implementation of the Mosoriot Campus Network on Cisco Packet tracer



Key network design features:
The key features for the network included:

- Buildings interconnected via fiber backbone.
- VLANs segregate departmental traffic.
- OSPF for internal dynamic routing; static routing for ISP.
- NAT/PAT on border router for public IP translation.

The switches at the Mosoriot Campus and main campus were added for redundancy and avoiding failure at three different levels :

- **Core Layer** is the highest-level Iin the hierarchy and includes the Core Switches that handle high-speed traffic between distribution switches and WAN connections, and the WAN Router which provides connectivity to external networks such as the internet.
- **Distribution Layer**: layer three Connect core switches to access switches in individual buildings, segregating traffic for specific areas.
- **Access Layer:** Provide end-user connectivity, including departmental PCs, printers, and servers

3) Subnetting and VLAN addressing

The subnetting and Vlan development included critical discussion involved discussion on division of the private network and allocation of addresses to cover all the sections. Technologies and protocols used included subnetting and use of Vlans division to address the different grouped blocks of devices. We used variable length subnetting (VLSM) to subnet to ensure that we did not waste much Ip addresses per building.

<u>BUILDING 1</u>

Design goal

- All departments to communicate
- All PCs per department are access to a printer
- Security for critical departments

Design considerations.

- **Scalability.** Submitting to allocate sufficient slots for PC without much wastage Allocation of 16 addresses giving 3 extra addresses with 11 devices, without wasting many IP addresses.

- **Availability:** All PCs in a department can communicate
- **Security:** VLANs to restrict departmental communication. Static configuration for managers PC
- **Manageability**. Naming of PCs and departments,

Implementation

- **Connecting devices used:**

o Two layer-2 switches (2960) to connect the devices in each building. Each building has a maximum of 11 devices so the 24 port 2096 switch is enough to cover the building and leave for a few additional slots switch

o One distribution layer 3 switch to allow inter-VLAN routing and also connect and route to the core switch

o **Scalability:** ***Subnetting and IP addressing*****:** For the network ID 172.16.0.0/16. and a requirement of supporting 11 devices with room for future growth, we used a /26 subnet mask to provide 64 total IP addresses which includes 62 usable host addresses, 1 network address and 1 broadcast address as follows in the table below

- **Availability:** to ensure all PCs in a department can communicate, we implemented two-layer 2 access switches (2960) each with 24 ports to provide VLANS for the 4 departments in the building.

Building	**Department**	**Subnet**	**Network Address**	**First Usable IP**	**Last Usable IP**	**Broadcast Address**	**Total Hosts**		[illegible]
Building 1	Finance	172.16.1.0/26	172.16.1.0	172.16.1.1	172.16.1.62	172.16.1.63	62		[illegible]
Building 1	Human Resource	172.16.1.64/26	172.16.1.64	172.16.1.65	172.16.1.126	172.16.1.127	62		[illegible]
Building 1	Administration	172.16.1.128/26	172.16.1.128	172.16.1.129	172.16.1.190	172.16.1.191	62		[illegible]
Building 1	Procurement	172.16.1.192/26	172.16.1.192	172.16.1.193	172.16.1.254	172.16.1.255	62		[illegible]

<u>BUILDING 2</u>

Design Considerations:

1. Scalability:
   - o Subnetting is used to allocate sufficient slots for PCs without much wastage.
   - o Allocation of subnet /25 for Civil Engineering, Mechanical Engineering, and Electrical Engineering departments.
   - o The computer lab subnet is allocated /25 to provide 126 addresses.
2. Availability:
   - o All PCs in a department can communicate.

Civil Engineering

- Connected to B2_Switch_1 ports 1-12 under VLAN 201.
- Ports:

- o Port 1 (Head of Department): Static IP 172.16.2.1/25.
  - o Port 11 (Printer): Static IP 172.16.2.29/25.
  - o Ports 2-10 (Dynamic allocation): IP range 172.16.2.2 - 172.16.2.28/25.
  - o Port 12 (Connects to distribution switch via OSPF): IP 172.16.2.30/25.
- Wireless connection implemented for all addresses.

Mechanical Engineering

- Connected to B2_Switch_1 ports 13-24 under VLAN 202.
- Ports:
  - o Port 13 (Head of Department): Static IP 172.16.2.129/25.
  - o Port 23 (Printer): Static IP 172.16.2.157/25.
  - o Ports 14-22 (Dynamic allocation): IP range 172.16.2.130 - 172.16.2.156/25.
  - o Port 24 (Connects to distribution switch via OSPF): IP 172.16.2.158/25.
- Wireless connection implemented for all addresses.

Electrical Engineering

- Connected to B2_Switch_2 ports 1-12 under VLAN 203.
- Ports:
  - o Port 1 (Head of Department): Static IP 172.16.3.1/25.
  - o Port 11 (Printer): Static IP 172.16.3.29/25.
  - o Ports 2-10 (Dynamic allocation): IP range 172.16.3.2 - 172.16.3.28/25.
  - o Port 12 (Connects to distribution switch via OSPF): IP 172.16.3.30/25.
- Wireless connection implemented for all addresses.

Computer Lab

- Connected to B1_Switch_2 ports 13-24 under VLAN 204.
- Ports:
  - o Port 13 (Department Assistant PC): Static IP 172.16.3.129/25.
  - o Ports 14-22 (Dynamic allocation): IP range 172.16.3.130 - 172.16.3.254/25.
  - o Port 24 (Connects to distribution switch via OSPF): IP 172.16.3.126/25.
- Wireless connection implemented for all addresses.

Building 2	Civil Engineering	172.16.2.0/25	172.16.2.0	172.16.2.1	172.16.2.126	172.16.2.127	126		201
Building 2	Mechanical Engineering	172.16.2.128/25	172.16.2.128	172.16.2.129	172.16.2.254	172.16.2.255	126		202
Building 2	Electrical Engineering	172.16.3.0/25	172.16.3.0	172.16.3.1	172.16.3.126	172.16.3.127	126		203
Building 2	Computer Lab	172.16.3.128/25	172.16.3.128	172.16.3.129	172.16.3.254	172.16.3.255	126		204

<u>BUILDING 3</u>

• **Computer Science:** connected to B3_Switch_1 ports 1-12 under VLAN 301. Ports 1 10, and 11 are configured statically to the PC for the head of the department and the 2 printers with addresses 172.16.4.1, 172.16.4.28/25, and 172.16.4.29/25 respectively. The remaining 8 ports (2,3,4,5,6,7,8,9) are configured dynamically to allow 26 addresses 172.16.4.2 - 172.16.4.27/25. We will also implement a wireless connection for all the addresses. Port 12 with address 172.16.4.30/25 connects to the distribution switch (implemented through OSPF).
• **Physics:** connected to B3_Switch_1 ports 13-24 under VLAN 302. Ports 13 and 23 are configured statically to the PC for the head of the department and printer with addresses 172.16.4.129 and 172.16.4.157/25 respectively. The remaining 9 ports (14,15,16,17,18,19,20,21,22) are configured dynamically to allow 27 addresses 172.16.4.130 - 172.16.4.156/25. We will also implement a wireless connection for all the addresses. Port 24 with address 172.16.4.158/25 connects to the distribution switch (implemented through OSPF).
• **Mathematics:** connected to B3_Switch_2 ports 1-12 under VLAN 303. Ports 1 10, and 11 are configured statically to the PC for the head of the department and the 2 printers with addresses 172.16.5.1, 172.16.5.28/25, and 172.16.5.29/25 respectively. The remaining 8 ports (2,3,4,5,6,7,8,9) are configured dynamically to allow 26 addresses 172.16.5.2 - 172.16.5.27/25. We will also implement a wireless connection for all the addresses. Port 12 with address 172.16.5.30/25 connects to the distribution switch (implemented through OSPF).
• **Computer Lab:** connected to B3_Switch_2 ports 13-24. Ports 13 - 24 under VLAN 304. Port 13 is configured statically to address 172.16.5.129 for the computer department assistant PC, etc. The remaining 11 ports (14,15,16,17,18,19,20,21,22) are configured dynamically to accept 124 addresses 172.16.5.130 - 172.16.5.253/25. Address 172.16.5.254/25 connects to the distribution switch through port 24 (implemented through OSPF). There is a wireless network connection for all PCs.

Building 3	Computer Science	172.16.4.0/25	172.16.4.0	172.16.4.1	172.16.4.126	172.16.4.127	126		301
Building 3	Physics	172.16.4.128/25	172.16.4.128	172.16.4.129	172.16.4.254	172.16.4.255	126		302
Building 3	Mathematics	172.16.5.0/25	172.16.5.0	172.16.5.1	172.16.5.126	172.16.5.127	126		303
Building 3	Computer Lab	172.16.5.128/25	172.16.5.128	172.16.5.129	172.16.5.254	172.16.5.255	126		304

BUILDING 4

Design goal

- All departments to communicate
- Data centre to communicate with the Main Campus

- Security for critical departments

IT Department:

- connect two switches B4_Switch_1 and B4_Switch_2 via 2 Gigabit Ethernet channels. can use Cisco 3650-24PS which supports EtherChannel and can also perform layer 3 switching between the departments
- IT departments allowed access to both SMIS and ERP

For the two switches, we connected ports 1- 24 on switch 1 and 1- 18 under VLAN 40. Ports 1 configured statically to the PC for the head of the department ports 23 and 24 on switch and ports 16 and 17 on switch 2 allocated to printers with addresses 172.16.40.1, 172.16.40.58/26, 172.16.40.59/26, 172.16.40.60/26, 172.16.40.61/26, respectively. The remaining 36 ports are configured dynamically to allow **56** addresses 172.16.40.2 - 172.16.40.57/26. We will also implement a wireless connection for all the addresses. Port 18 on switch 2 with address 172.16.40.62/26 connects to the distribution switch (implemented through OSPF).

Datacenter

- The servers should have static addresses.
- the data centre has 4 servers that run local copies of SMIS, ERP software, the UoN web server, and the email server and connect to the main servers on the main campus.
- Use the remaining 6 slots for switch 2 from 19-24
- Ports 19-22 on B4_Switch_2 configured statically to the 4 data centre PCs with addresses 172.16.41.1 -172.16.41.4
- Port 24 B4_Switch_2 with address 172.16.41.6/29 connects to the distribution switch (implemented through OSPF).

Building 4	IT Department	172.16.6.0/26	172.16.6.0	172.16.6.1	172.16.6.62	172.16.6.63	62		401
Building 4	Data Center Servers	172.16.6.64/26	172.16.6.64	172.16.6.65	172.16.6.126	172.16.6.127	62		402

<u>BUILDING 4</u>

The wireless access point is available in the hostel with both the ground and first floor connected to the access point providing a wireless network connection for all PCs

Building 5	Male Hostel Wireless	172.16.7.0/25	172.16.7.0	172.16.7.1	172.16.7.126	172.16.7.127	126		501
Building 5	Female Hostel Wireless	172.16.7.128/25	172.16.7.128	172.16.7.129	172.16.7.254	172.16.7.255	126		502

<u>DEVICE IPS</u>

In addition to subnetting and allocating a pool of addresses per department. We also configured statically some key devices such as the routers and distribution switches to enable easier manageability. These devices played a big role in connecting between VLANs and subnets.

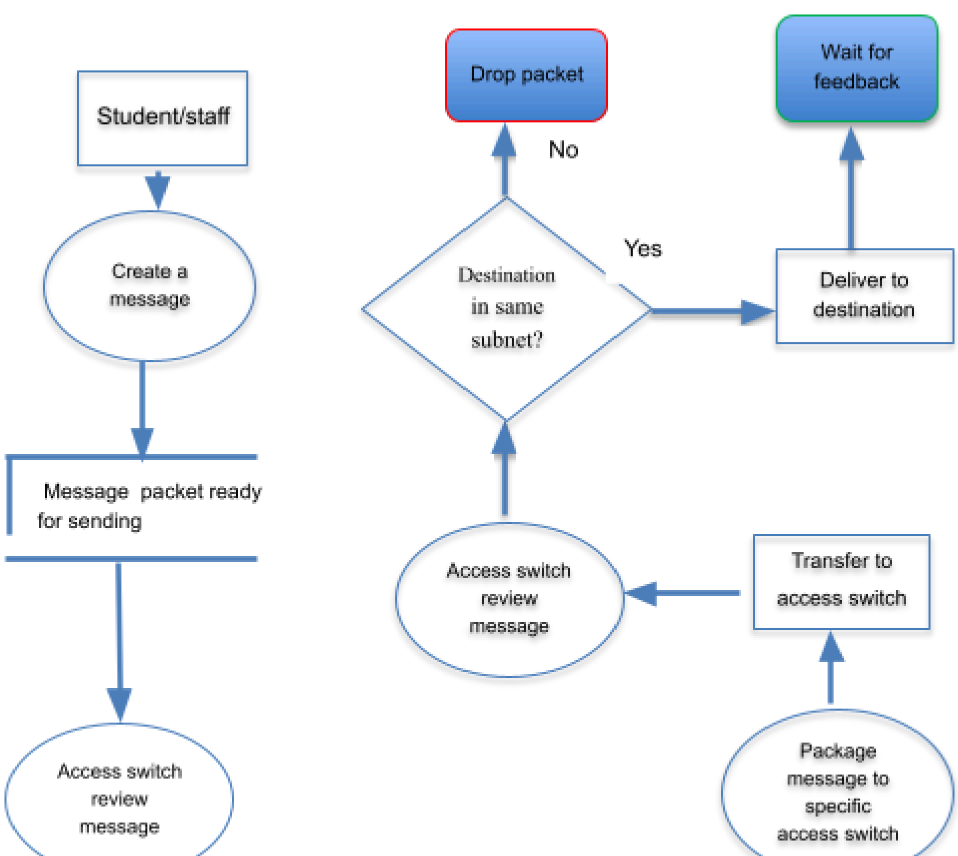
Device Category	Device Name	IP Address	Subnet	VLAN ID	Purpose
Border Router	Management Interface	172.16.0.1	172.16.0.0/24	1	ISP Connection Management
Core Switches	Core Switch 1	172.16.0.2	172.16.0.0/24	1	Core Network Management
	Core Switch 2	172.16.0.3	172.16.0.0/24	1	Core Network Management
Distribution Switches	Building 1	172.16.1.254	172.16.1.0/24	101-104	Building Distribution
	Building 2	172.16.2.254	172.16.2.0/24	201-204	Building Distribution
	Building 3	172.16.3.254	172.16.3.0/24	301-304	Building Distribution
	Building 4	172.16.6.126	172.16.6.0/24	401-402	Data Centre Distribution
	Building 5	172.16.7.254	172.16.7.0/24	501-502	Hostel Distribution

Access Points	Male Hostel AP	172.16.7.1	172.16.7.0/25	501	Male Hostel Wireless
	Female Hostel AP	172.16.7.129	172.16.7.128/25	502	Female Hostel Wireless

1) Data Flow Diagram

With the final storyline and models, we developed a graphical presentation of the system architecture below.

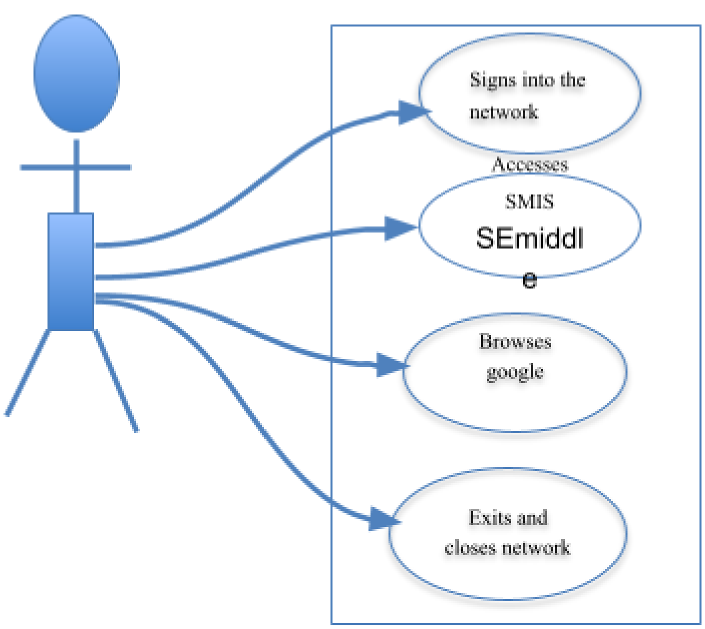
Figure 5: Example of Data Flow Diagram for a packet sent



2) Use Case:

The use cases were aimed at depicting the user of the network. The use case below shows the interactions with the clip.

Figure 6: Use Case: Student interacting with the Mosoriot Campus Network



Actors: enrolled students accessing the campus network
Preconditions: have authorized access to the computer lab or hostel wireless access network.
Events Flow:

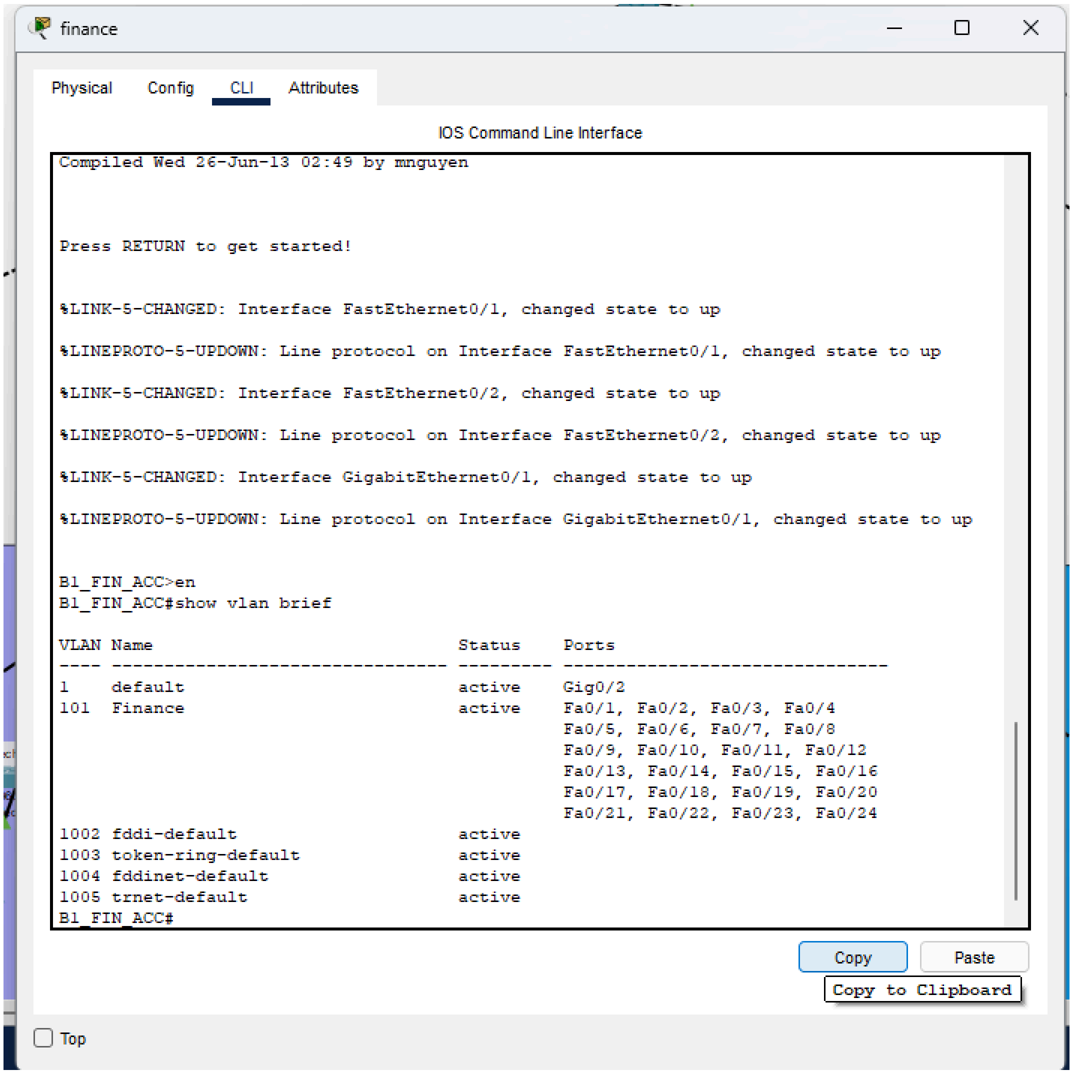
- The user opens the authentication page to access the network
- Student browses through page of choice such as Google or SMIS service
- Student closes the page and exits from the network

c. Construction Phase

The construction phase was the heart of the network development project as it involved configuring the actual linkages and connection of the devices in the CISCO Packet Tracer. The key configurations included:

- **Configuring VLANs to enable dynamic routing and excluding local network access for different departments.**

Figure: Showing finance department devices configured to Vlan 101



- **Configuring subnets to the different buildings**
  Figure showing buildings 1 and building 2 having different subnetworks:
  Building 1: 172.16.1.1/26
  Building 2: 172.16.2.1/25

Device Name: B1_DistSwitch
Device Model: 3650-24PS
Hostname: B1_DIST

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet1/0/1	Up	--	<not set>	<not set>	0030.F282.A9A2
GigabitEthernet1/0/2	Up	--	<not set>	<not set>	0003.E43D.7565
GigabitEthernet1/0/3	Up	--	<not set>	<not set>	000D.BDE9.E3DC
GigabitEthernet1/0/4	Up	--	<not set>	<not set>	0050.0F5E.D204
GigabitEthernet1/0/5	Up	--	<not set>	<not set>	0001.43C9.03B2
GigabitEthernet1/0/6	Down	1	<not set>	<not set>	00E0.F76B.D5E7
GigabitEthernet1/0/7	Down	1	<not set>	<not set>	0060.2F4B.A3B5
GigabitEthernet1/0/8	Down	1	<not set>	<not set>	0000.0C02.D703
GigabitEthernet1/0/9	Down	1	<not set>	<not set>	0001.4298.34E4
GigabitEthernet1/0/10	Down	1	<not set>	<not set>	0090.0CBC.2742
GigabitEthernet1/0/11	Down	1	<not set>	<not set>	0050.0F7A.0AD9
GigabitEthernet1/0/12	Down	1	<not set>	<not set>	0007.EC3D.2709
GigabitEthernet1/0/13	Down	1	<not set>	<not set>	0001.438C.DB19
GigabitEthernet1/0/14	Down	1	<not set>	<not set>	000D.BD62.85D9
GigabitEthernet1/0/15	Down	1	<not set>	<not set>	0001.9676.7C6C
GigabitEthernet1/0/16	Down	1	<not set>	<not set>	0005.5E55.0AC1
GigabitEthernet1/0/17	Down	1	<not set>	<not set>	0001.63A2.2361
GigabitEthernet1/0/18	Down	1	<not set>	<not set>	00E0.F907.B94B
GigabitEthernet1/0/19	Down	1	<not set>	<not set>	0060.7005.D03C
GigabitEthernet1/0/20	Down	1	<not set>	<not set>	0010.1174.0974
GigabitEthernet1/0/21	Down	1	<not set>	<not set>	0004.9A96.E8B1
GigabitEthernet1/0/22	Down	1	<not set>	<not set>	0001.C9AE.3424
GigabitEthernet1/0/23	Down	1	<not set>	<not set>	000C.CF94.3AC5
GigabitEthernet1/0/24	Down	1	<not set>	<not set>	00E0.F992.90DA
GigabitEthernet1/1/1	Down	1	<not set>	<not set>	000B.BEEA.861A
GigabitEthernet1/1/2	Down	1	<not set>	<not set>	00D0.BC5A.734B
GigabitEthernet1/1/3	Down	1	<not set>	<not set>	000C.85CE.5098
GigabitEthernet1/1/4	Down	1	<not set>	<not set>	0002.4A04.697E
Vlan1	Down	1	<not set>	<not set>	00E0.B059.09B4
Vlan101	Up	101	172.16.1.1/26	<not set>	0001.4259.BB10
Vlan102	Up	102	172.16.1.65/26	<not set>	000D.BD41.19C5
Vlan103	Up	103	172.16.1.129/26	<not set>	00D0.BC36.2DEB
Vlan104	Up	104	172.16.1.193/26	<not set>	0005.5E12.2D62

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > B1_DistSwitch

Device Name: B2_DistSwitch
Device Model: 3650-24PS
Hostname: B2_DIST

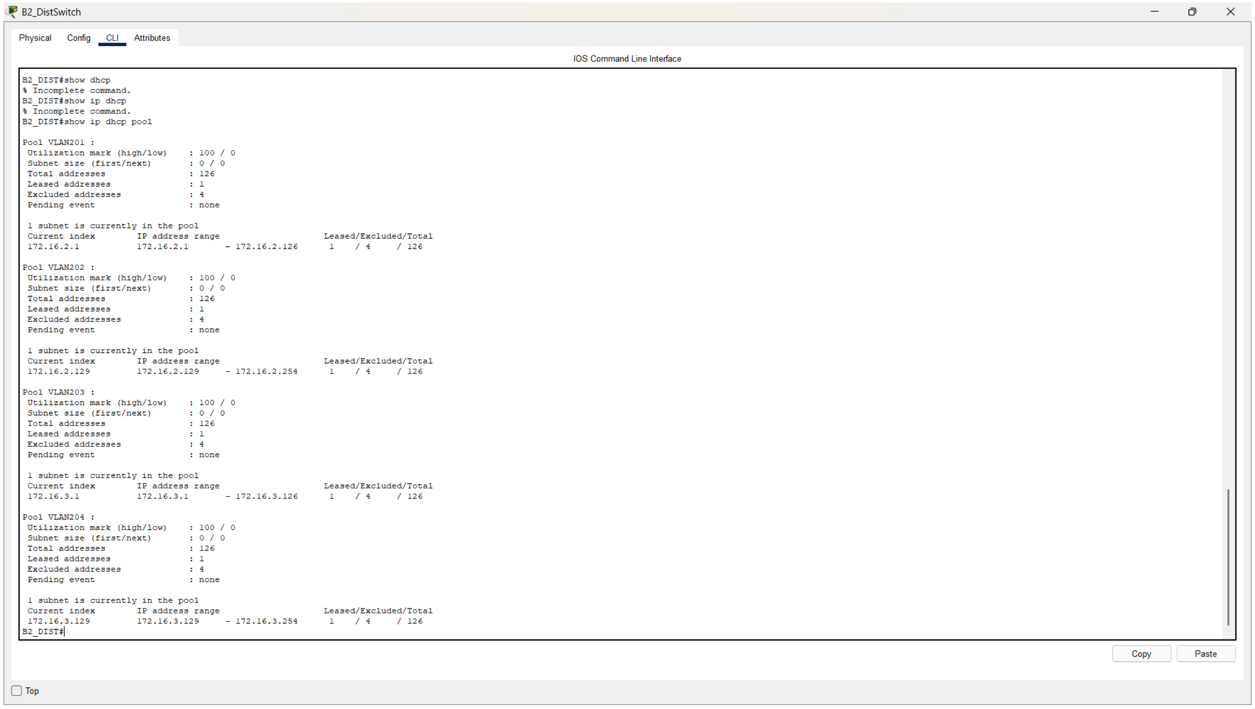
Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet1/0/1	Up	--	<not set>	<not set>	0040.0B3A.BB01
GigabitEthernet1/0/2	Up	--	<not set>	<not set>	0040.0B3A.BB02
GigabitEthernet1/0/3	Up	--	<not set>	<not set>	0040.0B3A.BB03
GigabitEthernet1/0/4	Up	--	<not set>	<not set>	0040.0B3A.BB04
GigabitEthernet1/0/5	Up	--	<not set>	<not set>	0040.0B3A.BB05
GigabitEthernet1/0/6	Down	1	<not set>	<not set>	0040.0B3A.BB06
GigabitEthernet1/0/7	Down	1	<not set>	<not set>	0040.0B3A.BB07
GigabitEthernet1/0/8	Down	1	<not set>	<not set>	0040.0B3A.BB08
GigabitEthernet1/0/9	Down	1	<not set>	<not set>	0040.0B3A.BB09
GigabitEthernet1/0/10	Down	1	<not set>	<not set>	0040.0B3A.BB0A
GigabitEthernet1/0/11	Down	1	<not set>	<not set>	0040.0B3A.BB0B
GigabitEthernet1/0/12	Down	1	<not set>	<not set>	0040.0B3A.BB0C
GigabitEthernet1/0/13	Down	1	<not set>	<not set>	0040.0B3A.BB0D
GigabitEthernet1/0/14	Down	1	<not set>	<not set>	0040.0B3A.BB0E
GigabitEthernet1/0/15	Down	1	<not set>	<not set>	0040.0B3A.BB0F
GigabitEthernet1/0/16	Down	1	<not set>	<not set>	0040.0B3A.BB10
GigabitEthernet1/0/17	Down	1	<not set>	<not set>	0040.0B3A.BB11
GigabitEthernet1/0/18	Down	1	<not set>	<not set>	0040.0B3A.BB12
GigabitEthernet1/0/19	Down	1	<not set>	<not set>	0040.0B3A.BB13
GigabitEthernet1/0/20	Down	1	<not set>	<not set>	0040.0B3A.BB14
GigabitEthernet1/0/21	Down	1	<not set>	<not set>	0040.0B3A.BB15
GigabitEthernet1/0/22	Down	1	<not set>	<not set>	0040.0B3A.BB16
GigabitEthernet1/0/23	Down	1	<not set>	<not set>	0040.0B3A.BB17
GigabitEthernet1/0/24	Down	1	<not set>	<not set>	0040.0B3A.BB18
GigabitEthernet1/1/1	Down	1	<not set>	<not set>	0040.0B32.C401
GigabitEthernet1/1/2	Down	1	<not set>	<not set>	0040.0B32.C402
GigabitEthernet1/1/3	Down	1	<not set>	<not set>	0040.0B32.C403
GigabitEthernet1/1/4	Down	1	<not set>	<not set>	0040.0B32.C404
Vlan1	Up	1	<not set>	<not set>	0060.2F82.BE8D
Vlan201	Up	201	172.16.2.1/25	<not set>	0060.2F82.BE01
Vlan202	Up	202	172.16.2.129/25	<not set>	0060.2F82.BE02
Vlan203	Up	203	172.16.3.1/25	<not set>	0060.2F82.BE03
Vlan204	Up	204	172.16.3.129/25	<not set>	0060.2F82.BE04

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > B2_DistSwitch

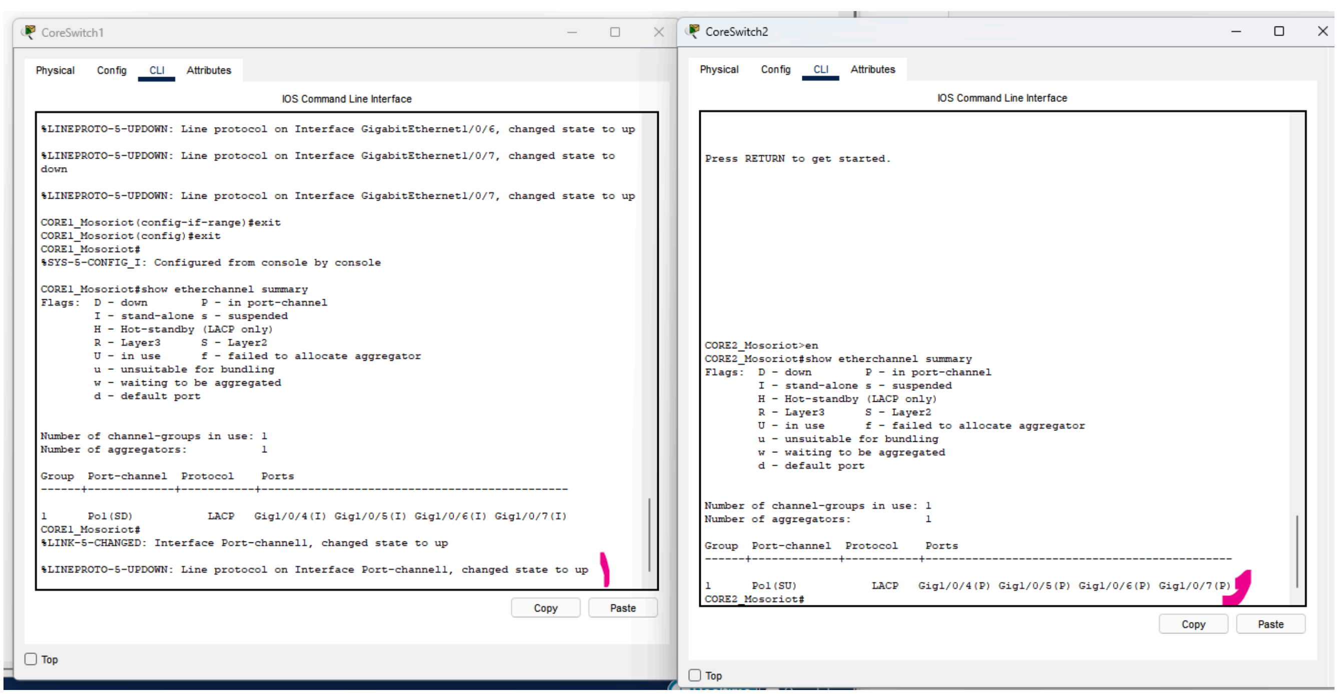
- **Static and dynamic configuration of devices**

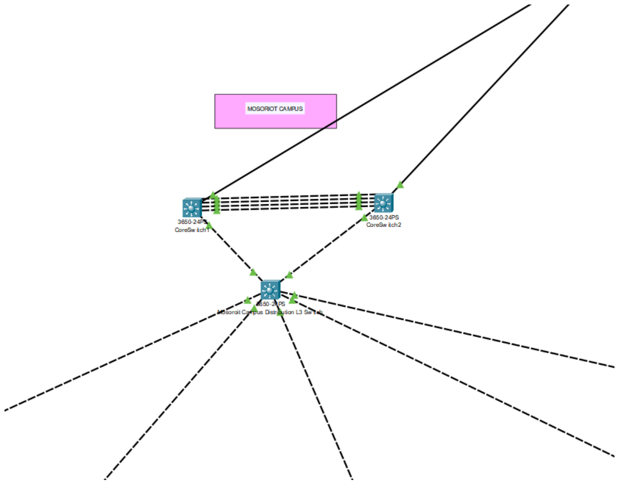
The devices were also configured to allow both static and dynamic routing. The shared devices such as printers were configured statically while other devices like laptops which are mobile were configured. DHCP was configured on each building's distribution switch.

Example of DHCP in Building 2 distribution Switch



- **Configuring EtherChannel between core switches**



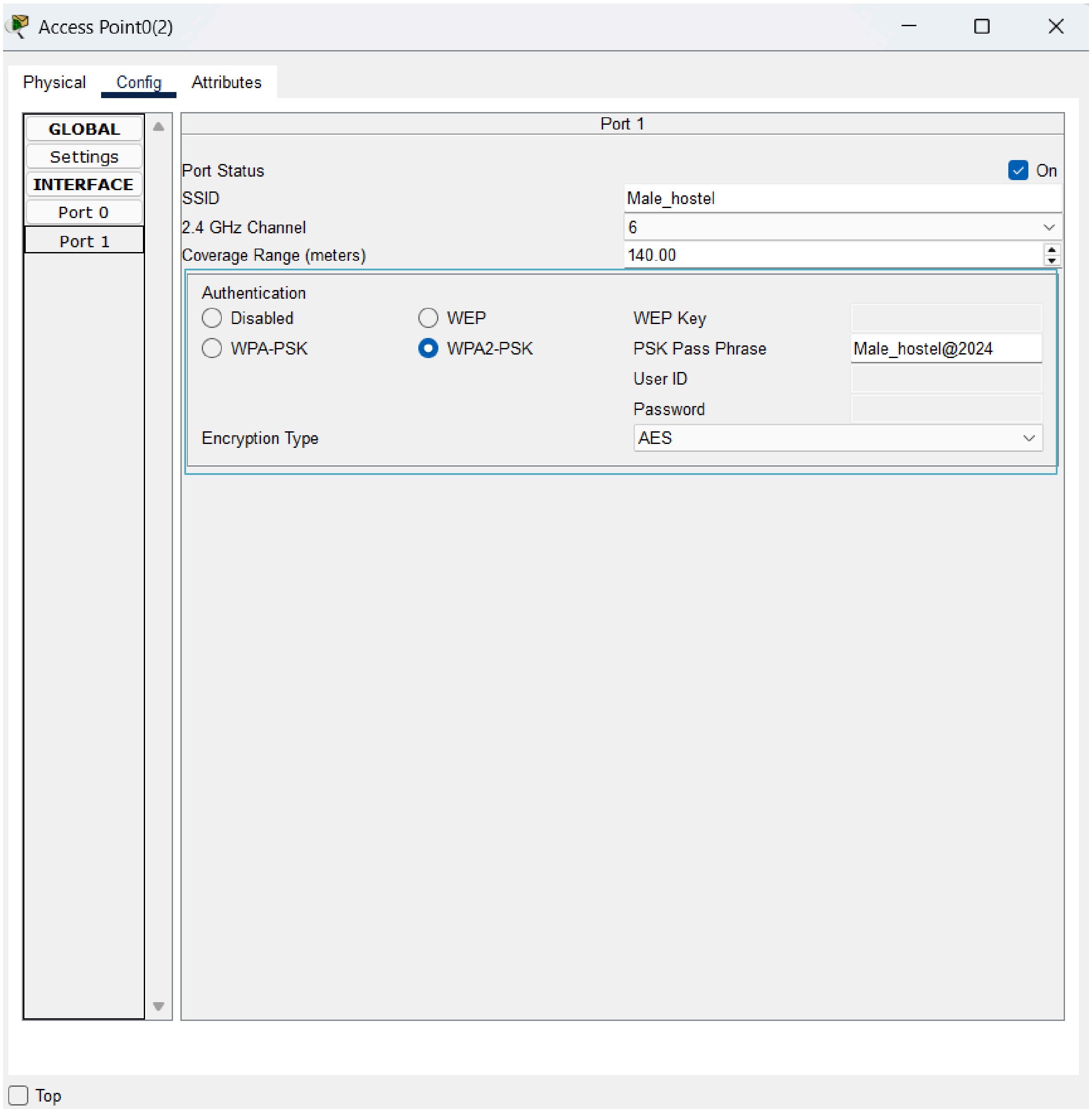


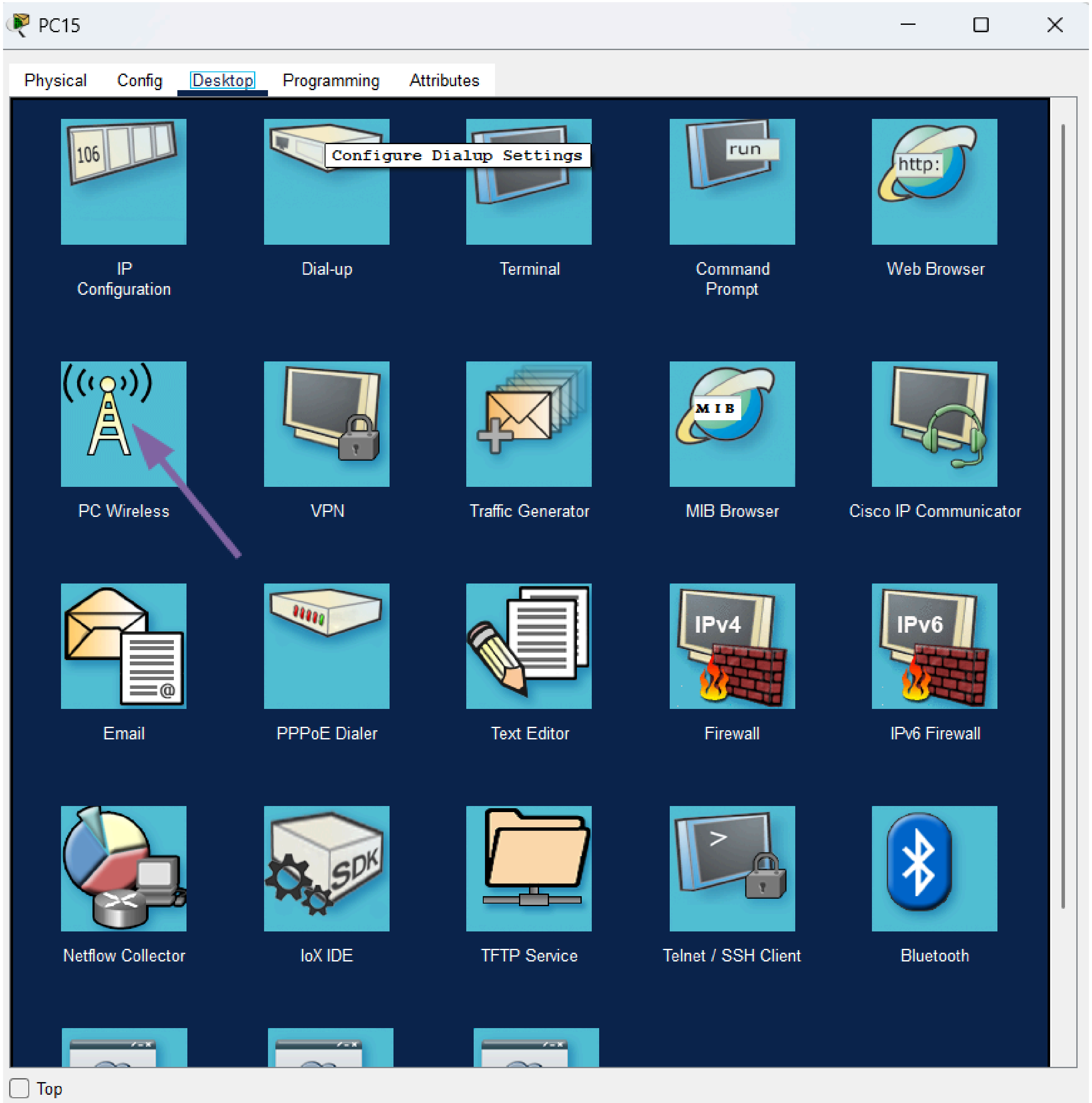
- **Access wireless point configuration**

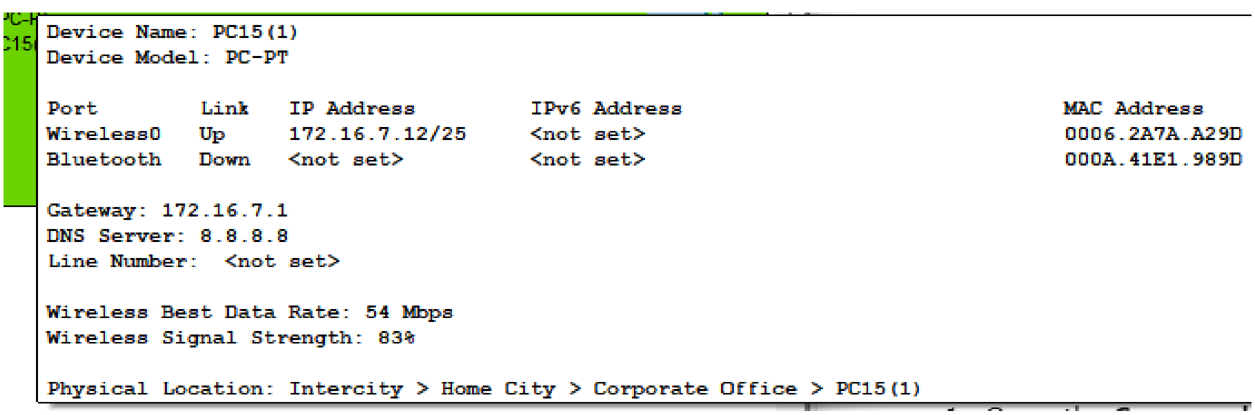
The wireless access points were configured to provide wireless access to the devices.

Wireless configuration on the Male Hostel

1. **Access point**

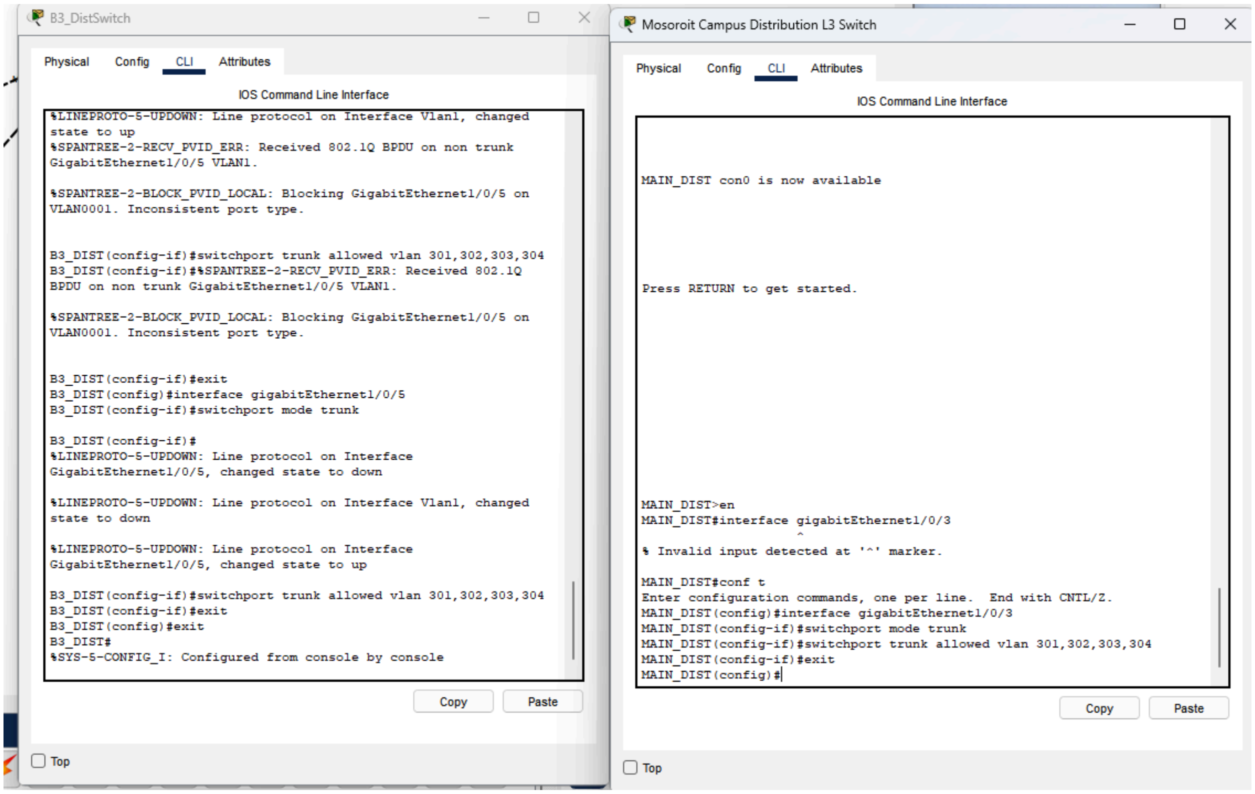



PC15
Physical
Config
Desktop
Programming
Attributes
Configure Dialup Settings
IP Configuration
Dial-up
Terminal
Command Prompt
Web Browser
PC Wireless
VPN
Traffic Generator
MIB Browser
Cisco IP Communicator
Email
PPPoE Dialer
Text Editor
Firewall
IPv6 Firewall
Netflow Collector
IoX IDE
TFTP Service
Telnet / SSH Client
Bluetooth
Top



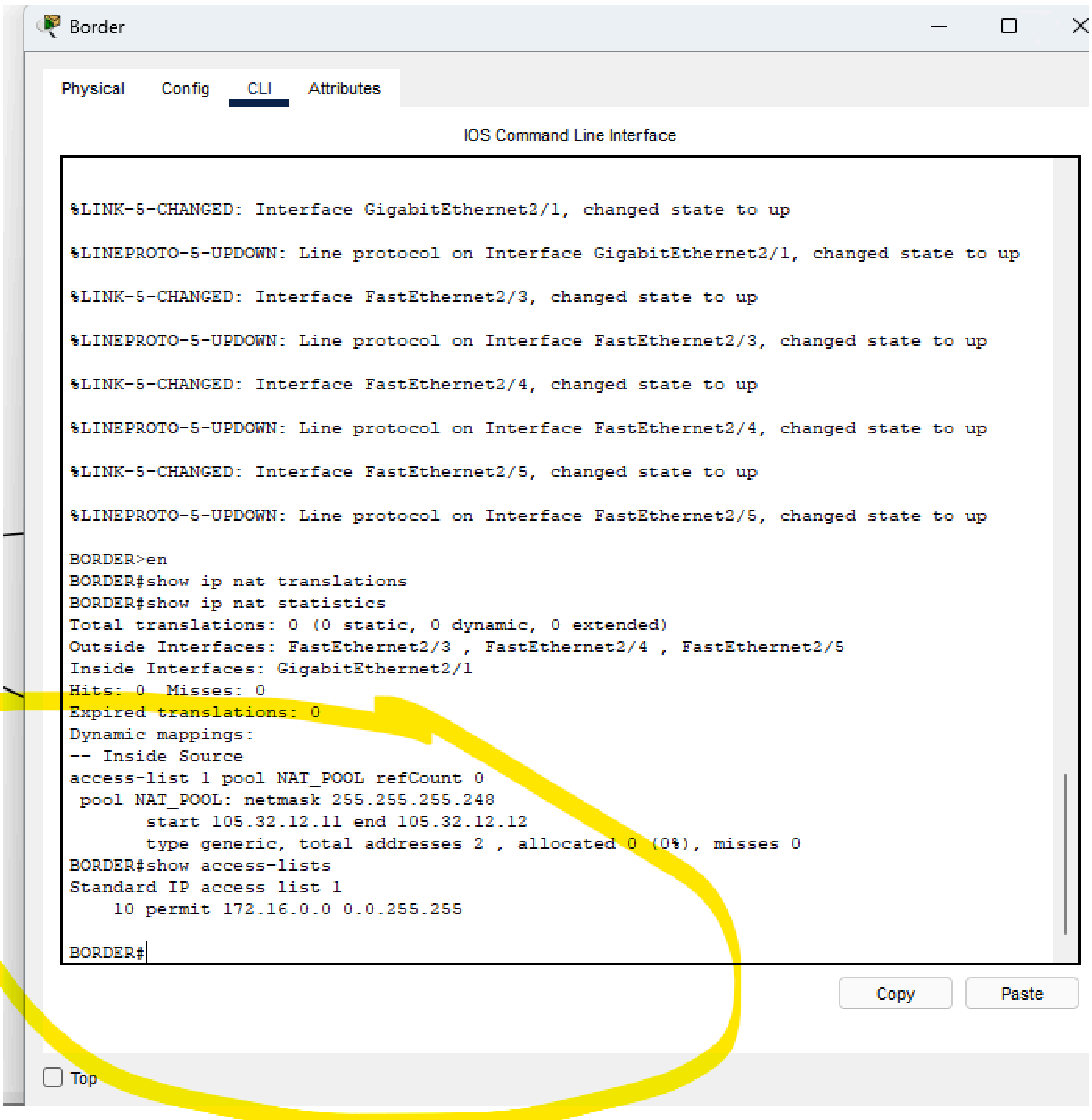
```
Device Name: PC15(1)
Device Model: PC-PT

Port        Link   IP Address         IPv6 Address                                   MAC Address
Wireless0   Up     172.16.7.12/25     <not set>                                      0006.2A7A.A29D
Bluetooth   Down   <not set>          <not set>                                      000A.41E1.989D

Gateway: 172.16.7.1
DNS Server: 8.8.8.8
Line Number: <not set>

Wireless Best Data Rate: 54 Mbps
Wireless Signal Strength: 83%

Physical Location: Intercity > Home City > Corporate Office > PC15(1)
```

Configuration of distribution routers to main distribution router to enable connectivity between subnets



- **Network address translations the boarder router configured with Network address translation to enable communication with the internet**

The border router shows network 172.16.0.0 as the network that is translated to public address 105.32.12.11 to 105.32.12.12



- **Configuration of connections to WAN to the internet and the main campus**

```
UON_WAN#show startup-config
hostname UON_WAN
no ip cef
no ipv6 cef
!
interface GigabitEthernet1/0
description TO-CORE1mosoriot
ip address 172.16.0.14 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet2/0
description TO_CORE2mosoriot
ip address 172.16.0.18 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet3/0
description TO_Core1Main
ip address 172.16.0.22 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet4/0
description TO_Core2main
ip address 172.16.0.26 255.255.255.252
duplex auto
speed auto
!
router rip
version 2
network 172.16.0.0
no auto-summary
!
ip classless
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
login
end
```

- **Configuration of the access, core and distribution routers – to connect to each other and to the devices**

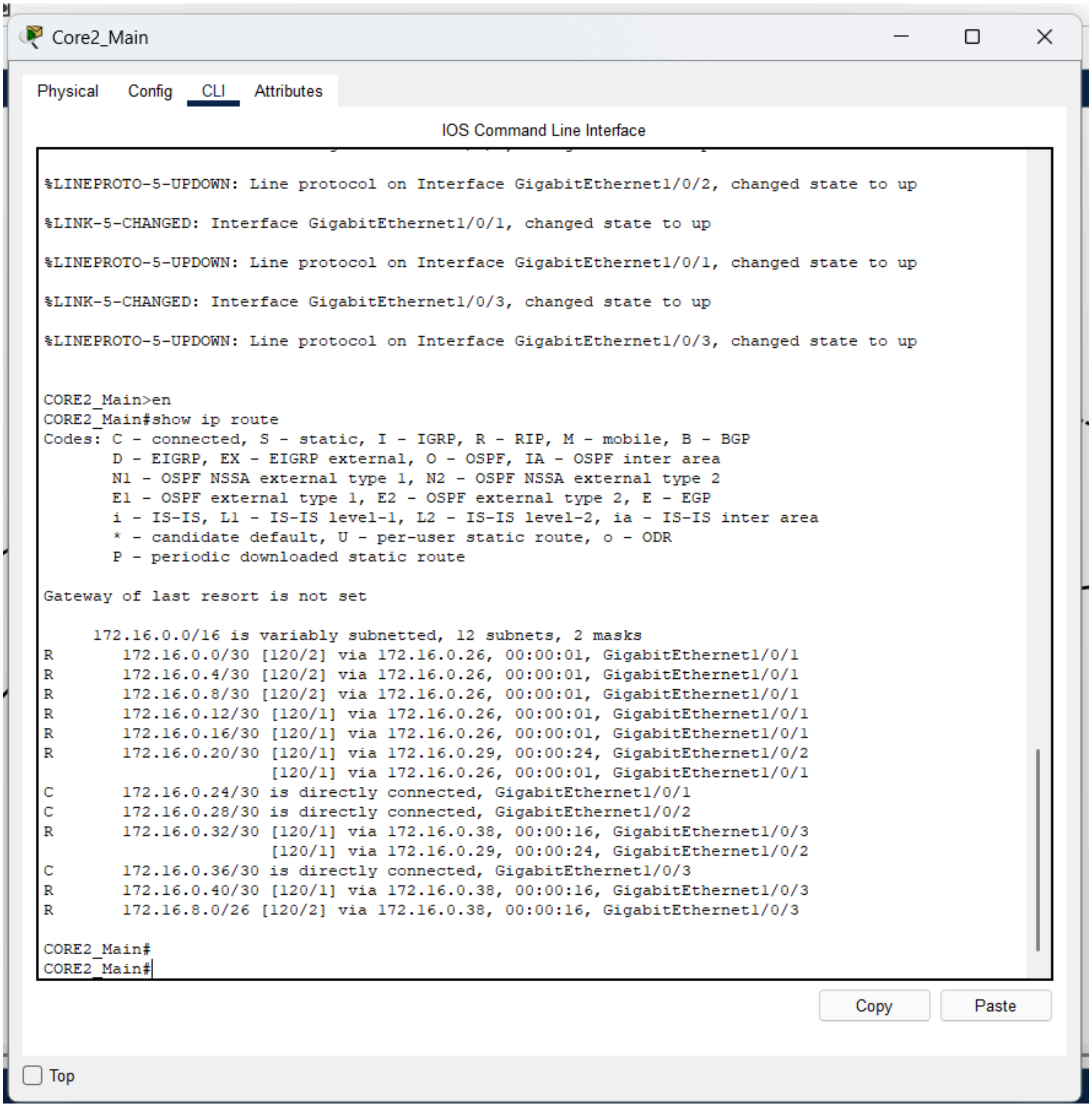
The access, core and distribution routers were configured to be able to connect to each other and to the devices. Configurations included enabling the different vlans and . these is shown below

CORE1_Mosoriot#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 12 subnets, 2 masks
C 172.16.0.0/30 is directly connected, GigabitEthernet1/0/1
R 172.16.0.4/30 [120/1] via 172.16.0.10, 00:00:11, GigabitEthernet1/0/2
[120/1] via 172.16.0.1, 00:00:06, GigabitEthernet1/0/1
C 172.16.0.8/30 is directly connected, GigabitEthernet1/0/2
C 172.16.0.12/30 is directly connected, GigabitEthernet1/0/3
R 172.16.0.16/30 [120/1] via 172.16.0.14, 00:00:15, GigabitEthernet1/0/3
[120/1] via 172.16.0.10, 00:00:11, GigabitEthernet1/0/2
R 172.16.0.20/30 [120/1] via 172.16.0.14, 00:00:15, GigabitEthernet1/0/3
R 172.16.0.24/30 [120/1] via 172.16.0.14, 00:00:15, GigabitEthernet1/0/3
R 172.16.0.28/30 [120/2] via 172.16.0.14, 00:00:15, GigabitEthernet1/0/3
R 172.16.0.32/30 [120/2] via 172.16.0.14, 00:00:15, GigabitEthernet1/0/3
R 172.16.0.36/30 [120/2] via 172.16.0.14, 00:00:15, GigabitEthernet1/0/3
R 172.16.0.40/30 [120/3] via 172.16.0.14, 00:00:15, GigabitEthernet1/0/3
R 172.16.8.0/26 [120/4] via 172.16.0.14, 00:00:15, GigabitEthernet1/0/3

Example of core 1 mosoriot switch configured via RIP to know where it is conneccted to
Next example is the Uon core Switch also configured with RIPv2

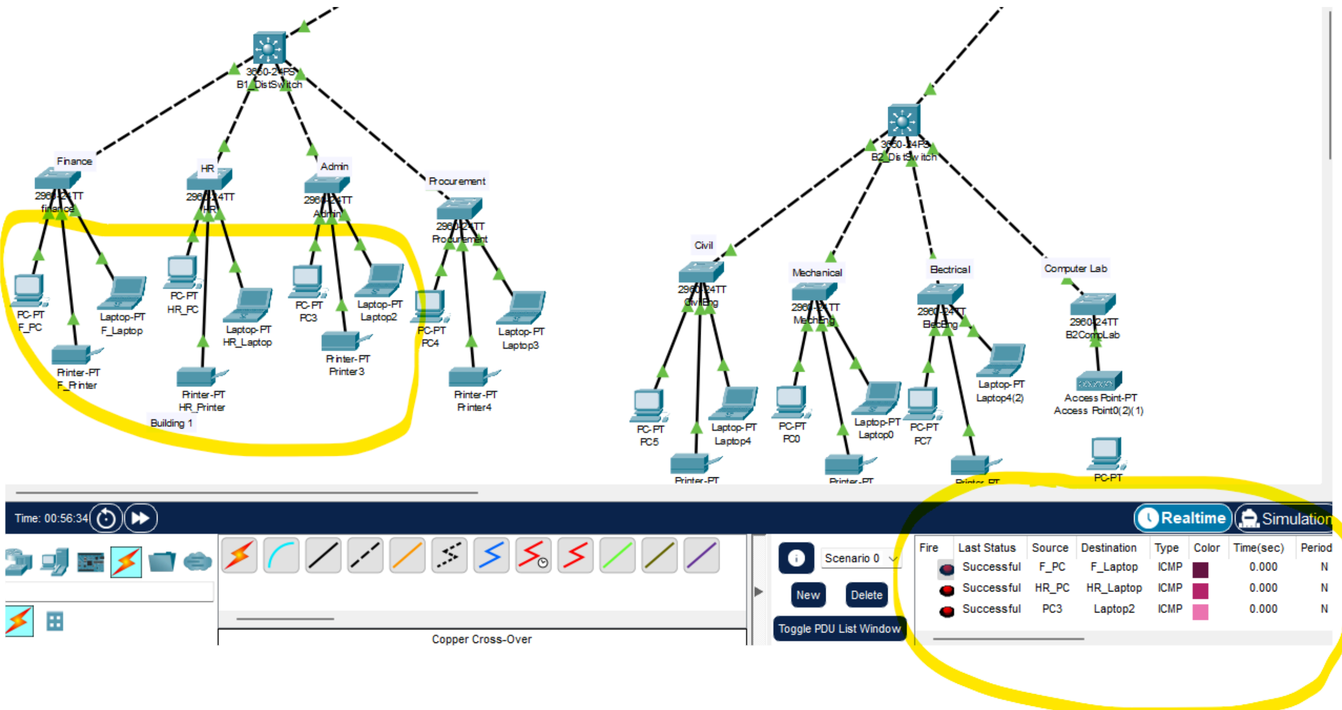

Core2_Main
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet1/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet1/0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to up
CORE2_Main>en
CORE2_Main#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 12 subnets, 2 masks
R 172.16.0.0/30 [120/2] via 172.16.0.26, 00:00:01, GigabitEthernet1/0/1
R 172.16.0.4/30 [120/2] via 172.16.0.26, 00:00:01, GigabitEthernet1/0/1
R 172.16.0.8/30 [120/2] via 172.16.0.26, 00:00:01, GigabitEthernet1/0/1
R 172.16.0.12/30 [120/1] via 172.16.0.26, 00:00:01, GigabitEthernet1/0/1
R 172.16.0.16/30 [120/1] via 172.16.0.26, 00:00:01, GigabitEthernet1/0/1
R 172.16.0.20/30 [120/1] via 172.16.0.29, 00:00:24, GigabitEthernet1/0/2
[120/1] via 172.16.0.26, 00:00:01, GigabitEthernet1/0/1
C 172.16.0.24/30 is directly connected, GigabitEthernet1/0/1
C 172.16.0.28/30 is directly connected, GigabitEthernet1/0/2
R 172.16.0.32/30 [120/1] via 172.16.0.38, 00:00:16, GigabitEthernet1/0/3
[120/1] via 172.16.0.29, 00:00:24, GigabitEthernet1/0/2
C 172.16.0.36/30 is directly connected, GigabitEthernet1/0/3
R 172.16.0.40/30 [120/1] via 172.16.0.38, 00:00:16, GigabitEthernet1/0/3
R 172.16.8.0/26 [120/2] via 172.16.0.38, 00:00:16, GigabitEthernet1/0/3
CORE2_Main#
CORE2_Main#
Copy
Paste
Top

d. Cutover Phase

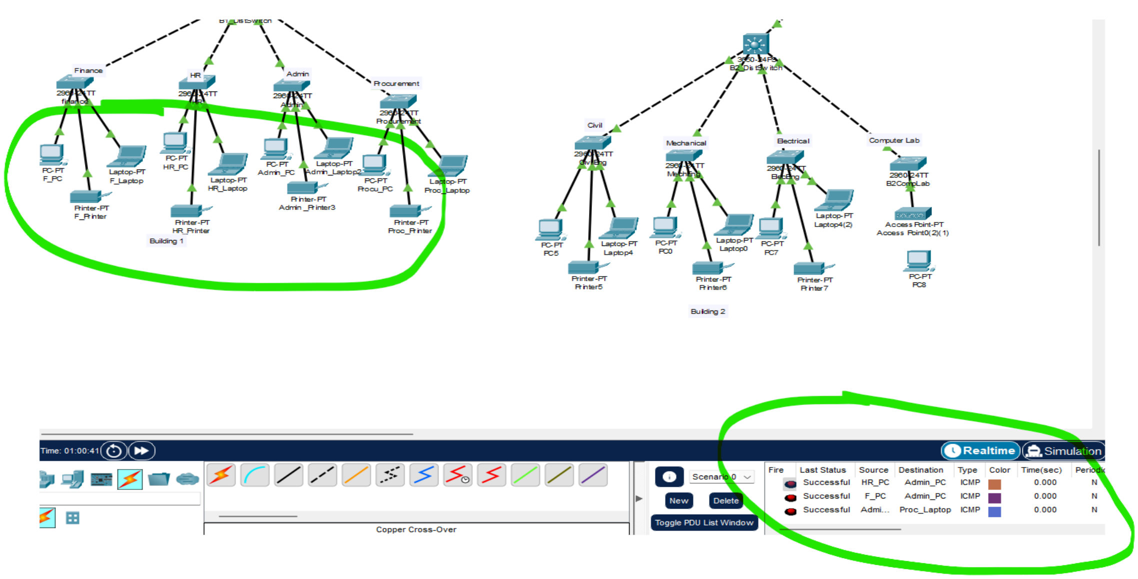
After the configurations, the next stage after completion of the design and construction of the network was to test the connectivity in the Cisco packet tracer. The testing was done at different stages starting from basic packet movements within same Vlan and building to the larger network to ensure full connectivity.

- **Showing connectivity between same vlan and same subnet**

The computers within Finance department can, HR departments and admin departments can communicate with each other within their departments



- **Showing connectiviy between same subnet**



- The computers within Finance department, HR departments and admin departments can communicate with each other in the different departments within the same subnet which is the same building.

CONCLUSION

.

The process of simulating a campus network on cisco packet tracer was rewarding as it gave us a chance to consolidate the lessons learnt in class in a practical scenario. Specific skills learnt included:

- **Variability of network design decisions**: the development of the campus network brought into context the importance of context when developing products for customers. This is because each network and customer had different needs and constratins to be taken into account. In this network, for instance there were constrains in access which necessitated the need of a firewall. Other networks

- **Integration of technologies :** this was a key factor of consideration when designing

- **Team work:** team work was another important factor in building successful network, building on skills

REFERENCES

Lecturers notes

Oppenheimer, P. (2010). *Top-Down Network Design*. Sydney: Cisco Press.

Odom, W. (2016). *CCNA Routing and Switching 200-125 Official Cert Guide Library*. Cisco Press.