

Group Assessment Coversheet

To be attached to the front of the assessment.

Campus: Midrand_____

Faculty: Information Technology_____

Module Code: ITNSA2-B33_____

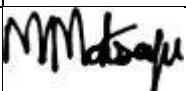
Group: 3_____

Lecturer's Name: Amakhan Agoni_____

Indicate	Yes	No
Plagiarism report attached		

Declaration:

I declare that this assessment is my own original work except for source material explicitly acknowledged. I also declare that this assessment or any other of my original work related to it has not been previously, or is not being simultaneously, submitted for this or any other course. I am aware of the AI policy and acknowledge that I have not used any AI technology to generate or manipulate data, other than as permitted by the assessment instructions. I also declare that I am aware of the Institution's policy and regulations on honesty in academic work as set out in the Conditions of Enrolment, and of the disciplinary guidelines applicable to breaches of such policy and regulations.

			% Participated
1	Student Full Name	Njabulo Ncube	100%
	Student Number	Con-852316-t3l3	
	Contact Number	0727068105	
	Signature	N.N	
2	Student Full Name	Masego Oratiloe Matsafu	100%
	Student Number	MD.2022.X8J9S4	
	Contact Number	0699209836	
	Signature		
3	Student Full Name	Luthando Raji	100%
	Student Number	Eduv4844015	
	Contact Number	0618124217	
	Signature	L.R	
4	Student Full Name	Thabiso Nxumalo	100%
	Student Number	Eduv4820263	
	Contact Number	0782109644	
	Signature	T.N	

Lecturer's Comments:

Marks Awarded: %

Signature	Date
------------------	-------------

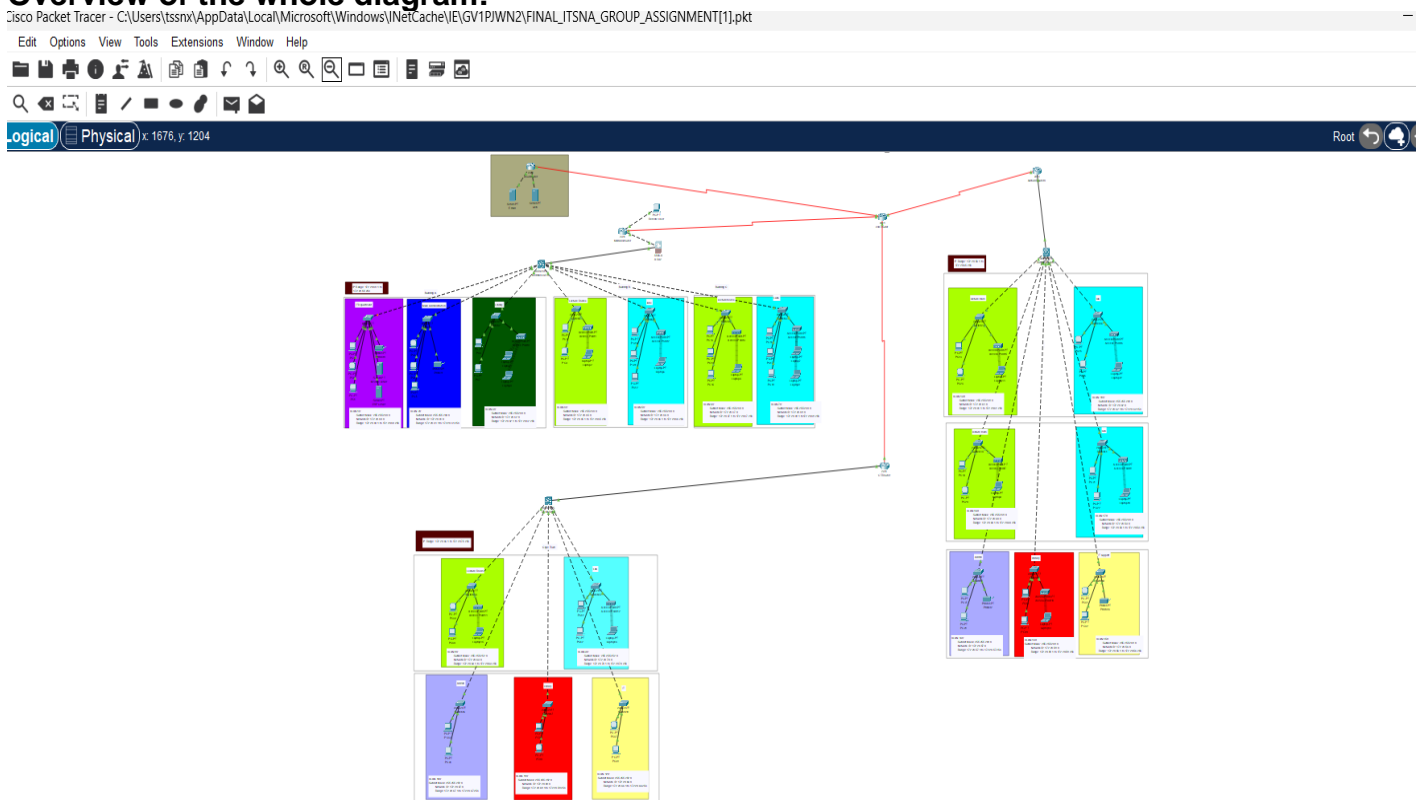
Section A:

Deliverable 1:

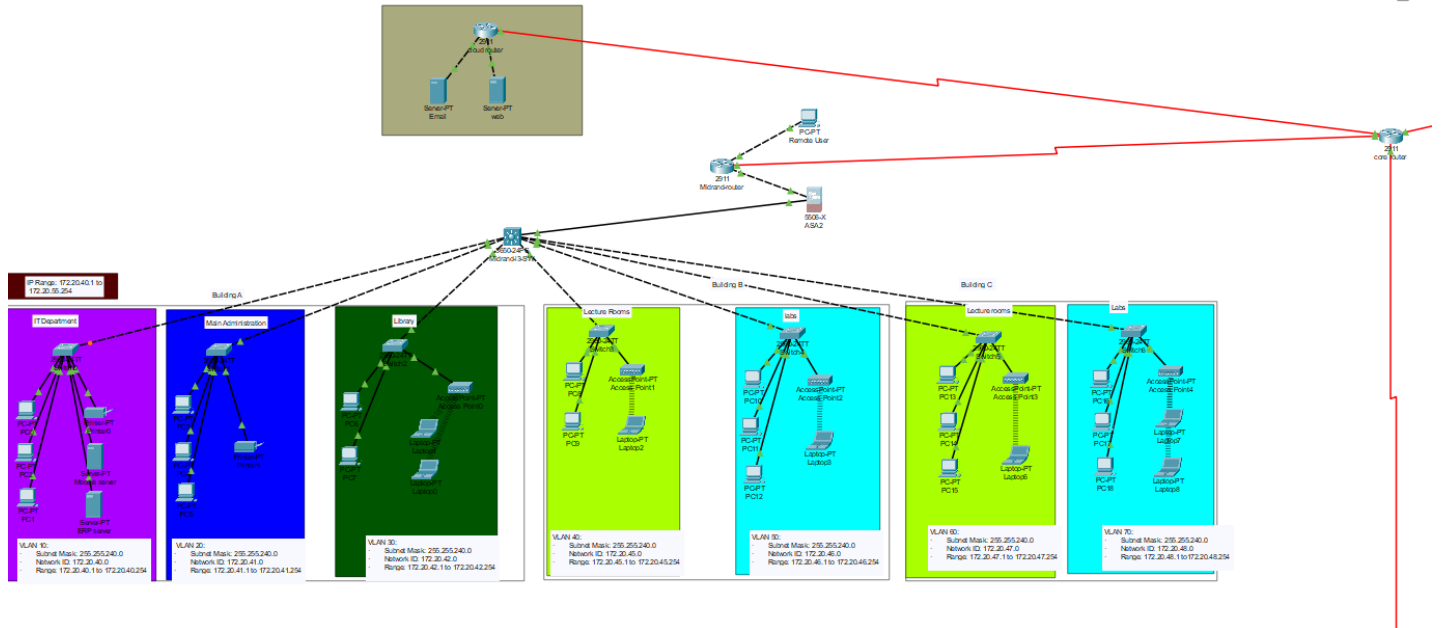
a) ZinTech College's network plan uses a hierarchical model with core, distribution, and access layers to ensure high-speed and secure connectivity across all campuses. The core layer will be made up of Cisco Nexus 9000 Series Switches, which are high-performance, low-latency switches designed for data centre and campus core networks. The distribution layer will rely on Cisco Catalyst 9500 Series Switches for high-density, high-performance switching with advanced security capabilities. The access layer will be equipped with Cisco Catalyst 9300 Series Switches, which provide flexible and scalable access switching with integrated security. The Cisco Aironet 3800 Series will be used to provide high-performance wireless access points with advanced security and management features. Firewalls will use Cisco Firepower 2100 Series for strong security, advanced threat protection, and VPN functionality.

Connection mediums such as fibre optic cables will be used for high-speed backbone connections between buildings and campuses, as well as Cat6a Ethernet Cables for internal building connections. A network diagram will show the topology, with the core layer centralised in Building A and replicated on the Durban and Cape Town campuses. Each building will have a distribution layer that will manage traffic between the core and access layers. The network will also include an IP address plan, with subnetting for large devices and VLANs for various departments and functions. Authentication, encryption, access control, and a hybrid cloud model will all be used to ensure security.

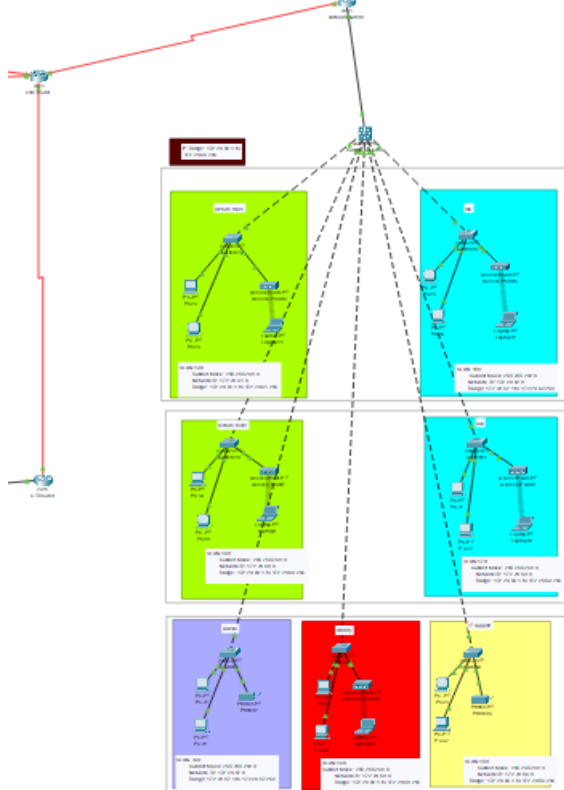
Overview of the whole diagram:



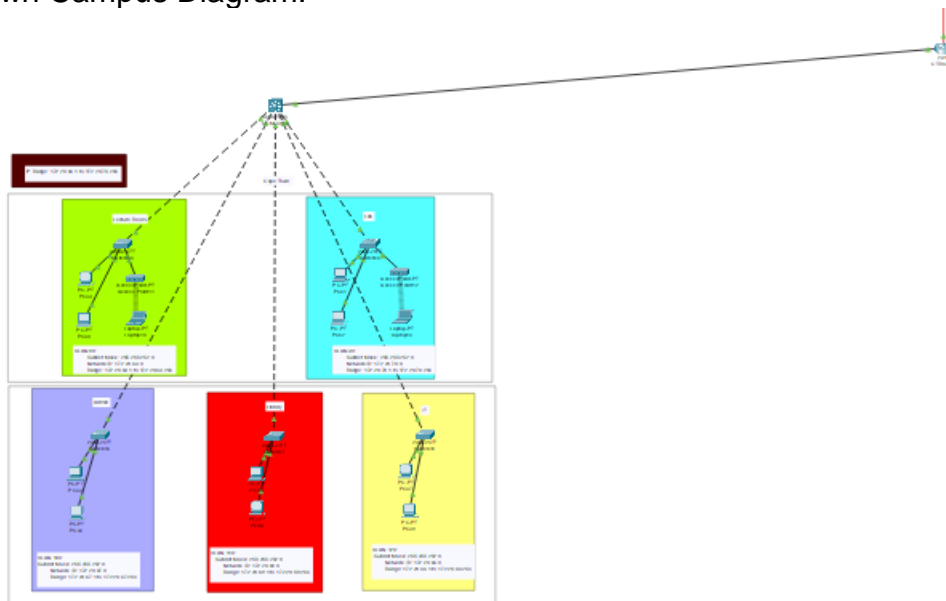
Downloaded from <http://ajph.org/> on November 10, 2015



Durban Campus Diagram:



Cape Town Campus Diagram:



b)
ZinTech College intends to use a Class B private IP address range (172.20.46.1 to 172.20.46.254) to enable efficient and secure network segmentation. To improve security and manageability, the range will be divided into subnets based on department, function, and location, each with its own VLAN. The plan includes VLANs for the administrative and IT departments, a library, lecture halls and labs, and Wi-Fi for students and faculty.

The chosen Class B IP address range allows for future expansion without having to reconfigure the entire network. VLANs help to isolate traffic, lowering the risk of unauthorised access and improving overall network security. Subnetting for departments and functions makes network management and troubleshooting easier.

The total IP addresses per subnet are 256, with each /20 subnet providing 256 IP addresses (254 usable addresses after). Excluding network and broadcast addresses. A centralised authentication system based on RADIUS servers will provide seamless access to campus resources such as Wi-Fi across campuses.

IP ADDRESSING

Midrand:

Building A:

IT:

- Subnet Mask: 255.255.240.0
- Network ID: 172.20.40.0
- Range: 172.20.40.1 to 172.20.40.254
- Broadcast ID: 172.20.40.255

Admin:

- Subnet Mask: 255.255.240.0
- Network ID: 172.20.41.0
- Range: 172.20.41.1 to 172.20.41.254
- Broadcast ID: 172.20.41.255

Library:

- Subnet Mask: 255.255.240.0
- Network ID: 172.20.42.0
- Range: 172.20.42.1 to 172.20.42.254
- Broadcast ID: 172.20.42.255

Building B:**Lecture Rooms:**

- Subnet Mask: 255.255.240.0
- Network ID: 172.20.45.0
- Range: 172.20.45.1 to 172.20.45.254
- Broadcast ID: 172.20.45.255

Labs:

- Subnet Mask: 255.255.240.0
- Network ID: 172.20.46.0
- Range: 172.20.46.1 to 172.20.46.254
- Broadcast ID: 172.20.46.255

Building C:**Lecture Rooms:**

- Subnet Mask: 255.255.240.0
- Network ID: 172.20.47.0
- Range: 172.20.47.1 to 172.20.47.254
- Broadcast ID: 172.20.47.255

Labs:

- Subnet Mask: 255.255.240.0
- Network ID: 172.20.48.0
- Range: 172.20.48.1 to 172.20.48.254
- Broadcast ID: 172.20.48.255

IP Range: 172.20.40.1 to 172.20.55.254

Durban:**Ground Floor:****IT:**

- Subnet Mask: 255.255.248.0
- Network ID: 172.20.56.0
- Range: 172.20.56.1 to 172.20.56.254
- Broadcast ID: 172.20.56.255

Admin:

- Subnet Mask: 255.255.248.0
- Network ID: 172.20.57.0
- Range: 172.20.57.1 to 172.20.57.254
- Broadcast ID: 172.20.57.255

Library:

- Subnet Mask: 255.255.248.0
- Network ID: 172.20.58.0
- Range: 172.20.58.1 to 172.20.58.254
- Broadcast ID: 172.20.58.255

First Floor:**Lecture Rooms:**

- Subnet Mask: 255.255.248.0
- Network ID: 172.20.59.0
- Range: 172.20.59.1 to 172.20.59.254
- Broadcast ID: 172.20.59.255

Labs:

- Subnet Mask: 255.255.248.0
- Network ID: 172.20.60.0
- Range: 172.20.60.1 to 172.20.60.254
- Broadcast ID: 172.20.60.255

Second Floor:**Lecture Rooms:**

- Subnet Mask: 255.255.248.0
- Network ID: 172.20.61.0
- Range: 172.20.61.1 to 172.20.61.254
- Broadcast ID: 172.20.61.255

Labs:

- Subnet Mask: 255.255.248.0
- Network ID: 172.20.62.0
- Range: 172.20.62.1 to 172.20.62.254
- Broadcast ID: 172.20.62.255

IP Range: 172.20.56.1 to 172.20.65.254

Cape Town:
Ground Floor:
IT:

- Subnet Mask: 255.255.252.0
- Network ID: 172.20.66.0
- Range: 172.20.66.1 to 172.20.66.254
- Broadcast ID: 172.20.66.255

Admin:

- Subnet Mask: 255.255.252.0
- Network ID: 172.20.67.0
- Range: 172.20.67.1 to 172.20.67.254
- Broadcast ID: 172.20.67.255

Library:

- Subnet Mask: 255.255.252.0
- Network ID: 172.20.68.0
- Range: 172.20.68.1 to 172.20.58.254
- Broadcast ID: 172.20.68.255

First Floor:

Lecture Rooms:

- Subnet Mask: 255.255.252.0
- Network ID: 172.20.69.0
- Range: 172.20.69.1 to 172.20.69.254
- Broadcast ID: 172.20.69.255

Labs:

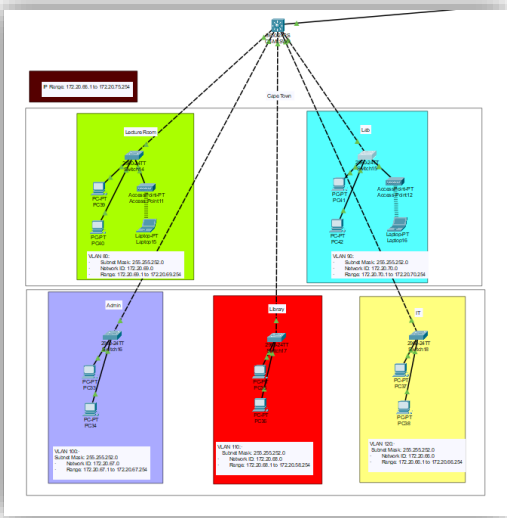
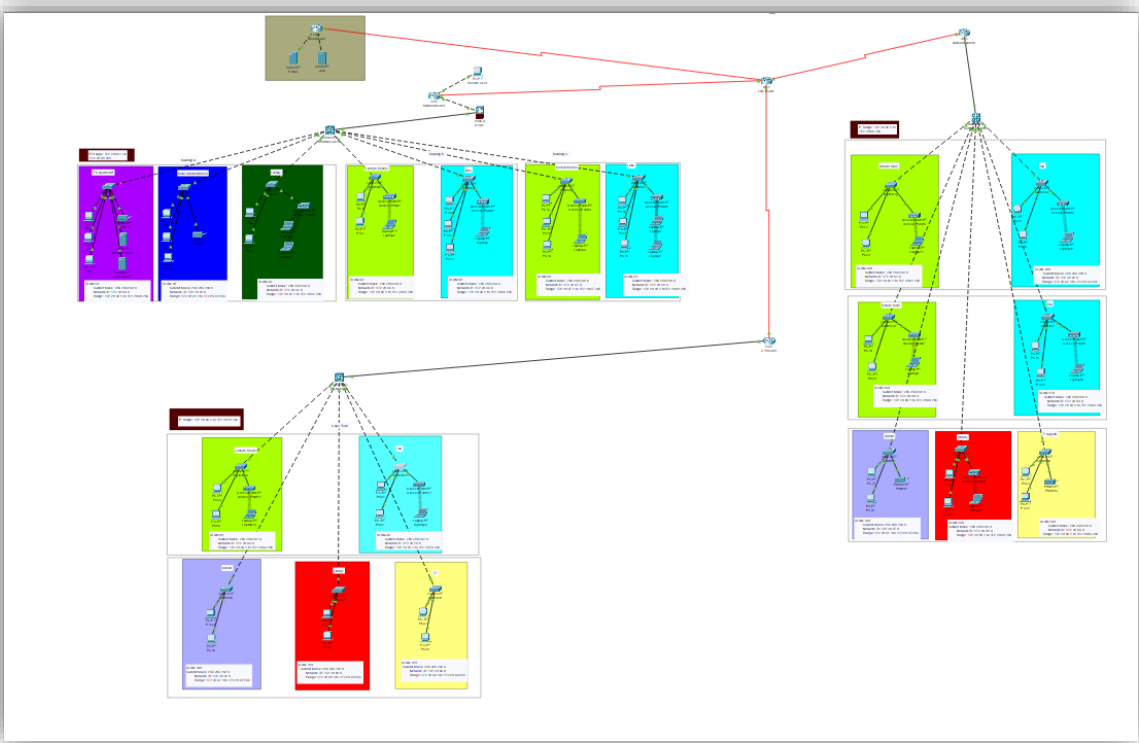
- Subnet Mask: 255.255.252.0
- Network ID: 172.20.70.0
- Range: 172.20.70.1 to 172.20.70.254
- Broadcast ID: 172.20.70.255

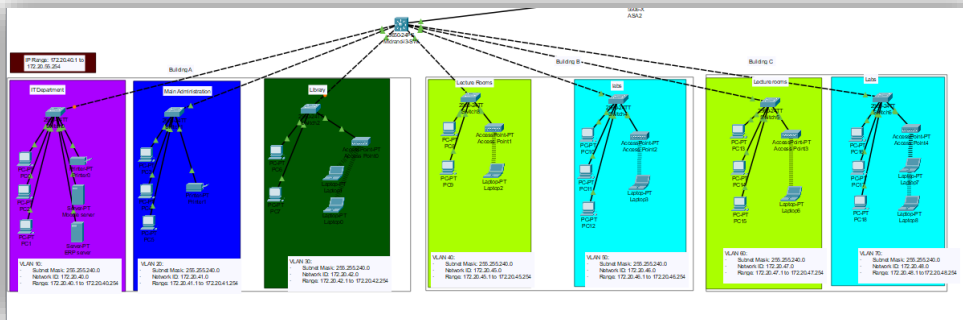
IP Range: 172.20.66.1 to 172.20.75.254

Finally, ZinTech College's IP address plan ensures a scalable, secure, and manageable network infrastructure that will support current operations as well as future expansion. The use of VLANs and subnets improves security while simplifying network management.

Deliverable 2:

a)





b)

```

IOS Command Line Interface

%LINKPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
%LINK-S-CHANGED: Interface FastEthernet0/1, changed state to up
%LINKPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#exit
Switch(config)#int fa0/2
Switch(config-if)#switch mode access
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#int fa0/1
Switch(config-if)#switchport mode
% Incomplete command.
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINKPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINKPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch(config-if)#ex
Switch(config)#do wr
Building configuration...
[OK]
Switch(config)#

Switch con0 is now available

```

```
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch(config-if)#ex
Switch(config)#do wr
Building configuration...
[OK]
Switch(config)#
```

Switch ccm0 is now available

```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet1/0/4 (1), with
Switch FastEthernet0/3 (30).

Switch(dhcp-config)#
Switch(dhcp-config)#network 172.20.40.0 255.255.255.240
Switch(dhcp-config)#
Switch(dhcp-config)#
```

Deliverable 3:

Pick the ASA Firewall Devices:

Drag and put the ASA Firewall device into the workspace by opening Cisco Packet Tracer and selecting it from “Security Devices” category in the device list.

Join Interfaces:

Select the ASA firewall device by clicking on it. Find the ASA firewall device interface ports, which are labelled “Ethernet0/0” for external interface and “Ethernet0/1” for the internal interface. Then drag the cable from the ASA interface to the router or modem to connect the “Ethernet0/0” interface to your internet-facing connection. Then drag a cable from the ASA interface to the internal network switch to connect the “Ethernet0/1” interface.

Configure Interfaces:

To then access the configuration window of the ASA firewall device, click on it and navigating to the “Interface” tab.

You'll then need to set each interface's IP address, security level and subnet mask. Assign the “inside” interface a much higher security level and the “outside” interface a lower security level.

Configure the Default Route:

Open the ASA firewall setup window and go to navigate to the “Routing” tab. Then setup an outgoing default route for the internet traffic that points to the next hop gateway. By doing this, it allows the data to go from the network to the external network.

Configure the Access Control List and Network Address Translation:

Open the ASA firewall setup window and navigate to the “Access Rules” tab.

You will then need to regulate the flow of communication between the inner and outside interfaces, configure access control lists or ACL's. Based on the source and destination IP addresses, ports, and protocols, you may either allow or deny a certain kind of traffic.

Setup NAT rules to change internal private IP addresses to exterior public IP addresses when internet traffic leaves the system.

Testing and Monitoring:

After doing the configuration, traffic from internal devices to external IP addresses and vice versa can be sent to test connection. To then ensure that the security policies are being applied correctly and that traffic is flowing as intended, you should pay attention to the firewall logs and traffic.

Physical Config CLI Attributes

IOS Command Line Interface

```
ciscoasa>en
Password:
ciscoasa#conf t
ciscoasa(config)#hostname security-fw
security-fw(config)#enable password cisco
security-fw(config)#username firewall password cisco
security-fw(config)#
security-fw(config)#clock set?

configure mode commands/options:
set
security-fw(config)#clock set 05:33:10 10 April 2024
security-fw(config)#
security-fw(config)#
security-fw(config)#int gig1/1
security-fw(config-if)#no shut

security-fw(config-if)#exit
security-fw(config)#
security-fw(config)#int gig1/1
security-fw(config-if)#ip address 172.20.40.1 255.255.240.0
security-fw(config-if)#ip address 172.20.41.1 255.255.240.0
security-fw(config-if)#ip address 172.20.42.1 255.255.240.0
security-fw(config-if)#ip address 172.20.45.1 255.255.240.0
security-fw(config-if)#ip address 172.20.46.1 255.255.240.0
security-fw(config-if)#ip address 172.20.47.1 255.255.240.0
security-fw(config-if)#ip address 172.20.48.1 255.255.240.0
security-fw(config-if)#
security-fw(config-if)#nameif ml-switch
INFO: Security level for "ml-switch" set to 0 by default.
security-fw(config-if)#security-level 100
security-fw(config-if)#exit
security-fw(config)#int gig1/2
security-fw(config-if)#no shut

%LINK-5-CHANGED: Interface GigabitEthernet1/2, changed state to down
security-fw(config-if)#no shut
```

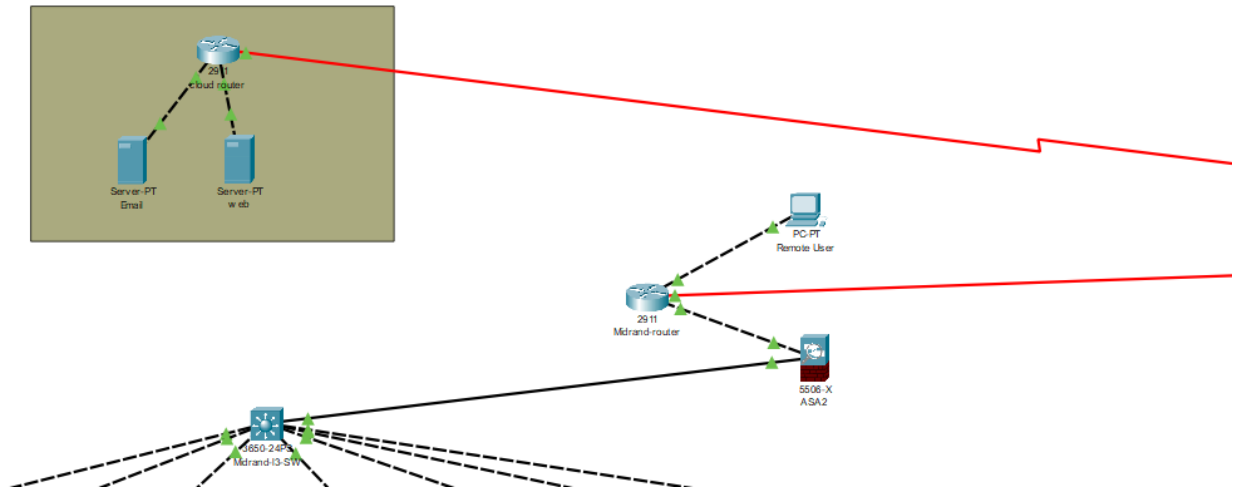
Copy

Paste

☐ Top

Deliverable 4:

The remote access for employees needs to be configured. The requirements are a at home VPN gateway for the user to gain access to the network.



The minimum requirements for configuring a network device that will function as a VPN gateway is a client device in order to connect remotely and a single router.

Step 1: The internet and internal network of the routers interface will need to be set up.

Step 2: The hostname, domain, name and passwords will need to be configured.

Step 3: IPsec VPN will need to be set up. IPsec has strong security advantages hence why it is used for VPNs

Step 4: The VPN will need user authentication the local user authentication will be used which is done through the router.

Physical Config CLI Attributes

IOS Command Line Interface

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.60, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.70, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed state to up

Midrand-router>config-if
Translating "config-if"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

Midrand-router>enable
Midrand-router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Midrand-router(config)#interface GigabitEthernet0/1
Midrand-router(config-if)#aaa authentication login
^
% Invalid input detected at '^' marker.

Midrand-router(config-if)#exit
Midrand-router(config)#aaa new-model
Midrand-router(config)#aaa authentication login ?
WORD      Named authentication list.
default   The default authentication list.
Midrand-router(config)#aaa authentication login one local
Midrand-router(config)#aaa authentication network ?
% Unrecognized command
Midrand-router(config)#aaa authentication network ?
% Unrecognized command
Midrand-router(config)#aaa authorization network ?
WORD      Named authorization list.
default   The default authorization list.
Midrand-router(config)#aaa authorization network two local
Midrand-router(config)#username admin password 1234
Midrand-router(config)#
```

Copy

Paste

☐ Top

Access Point1

Physical Config Attributes

GLOBAL

Settings

INTERFACE

Port 0

Port 1

Port 1

Port Status ☒ On

SSID MLeactureRoomA

2.4 GHz Channel 6

Coverage Range (meters) 140,00

Authentication

☐ Disabled ☐ WEP ☒ WPA2-PSK

WEP Key

PSK Pass Phrase Cisco2024

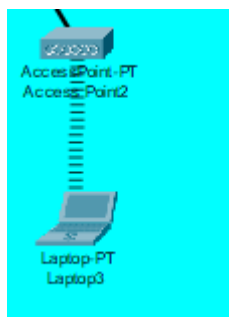
User ID

Password

Encryption Type AES

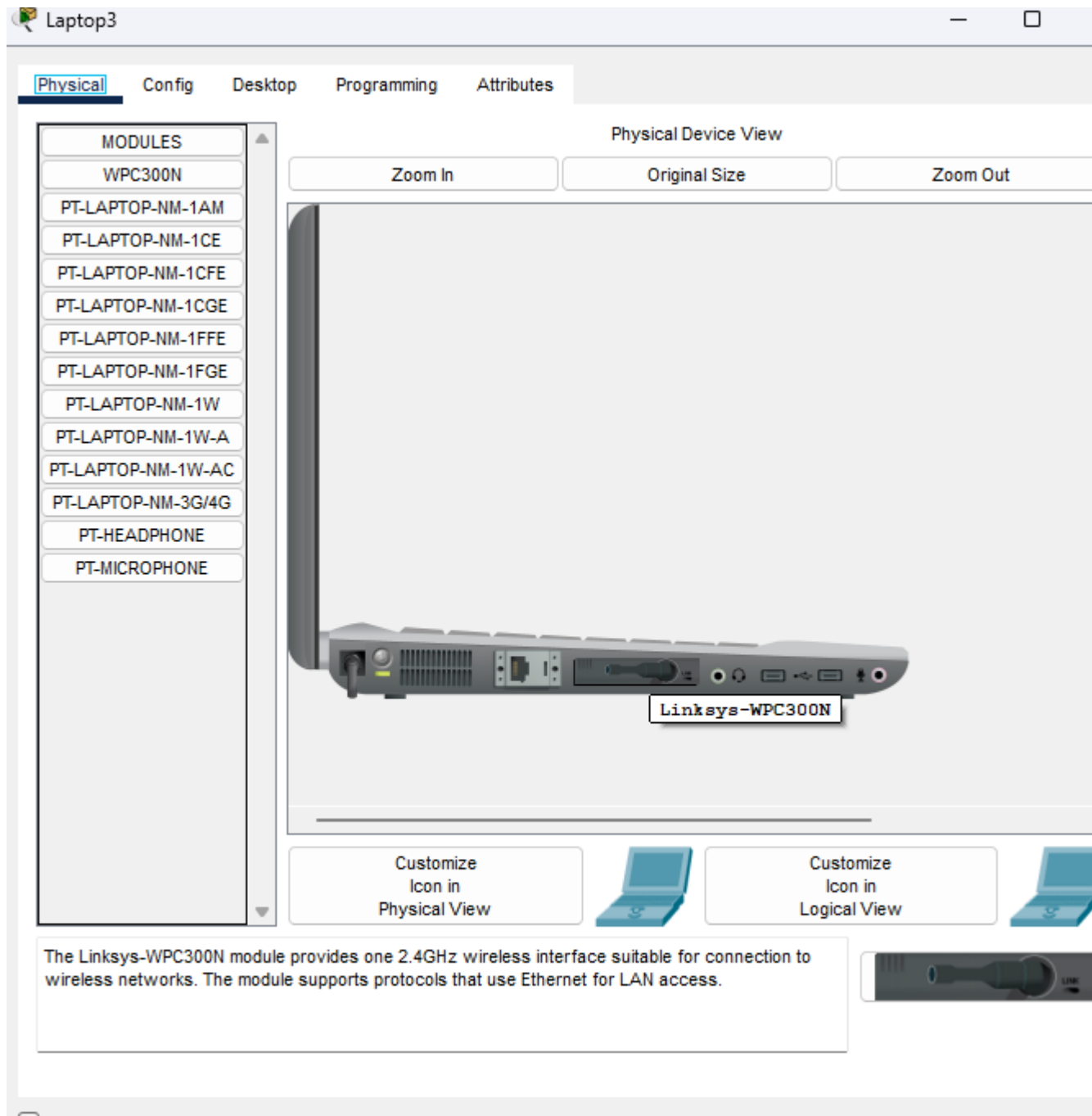
Top

Step 5: Connect the laptops to the access point



Devices that are preconfigured will connect automatically regarding laptops and computers they require us to simulate wireless connectivity by removing:

- Ethernet module from laptop or computer
- Adding a wireless module (WPC300N) and this will enable wireless connectivity.



Laptop3

PhysicalConfigDesktopProgrammingAttributes

Link InformationConnectProfiles

Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

Wireless Network Name	CH	Signal
DurbanLabA	1	31%
CapeTownLRA	1	31%
CapeTownLab	1	31%
MLabsC	1	31%
MLibraryA	1	31%

Site Information

Wireless Mode

Infrastructure

Network Type

Mixed B/G

Radio Band

Auto

Security


WPA2-PSK

MAC Address

00D0.97D0.8663

RefreshConnect

2.4GHz



Adapter is Active

Wireless-N Notebook Adapter

Wireless Network Monitor v1.0

Model No. WPC300N

Top

Physical Config **Desktop** Programming Attributes

WPA2-Personal Needed for Connection

This wireless network has WPA2-Personal enabled. To connect to this network, enter the required passphrase in the appropriate field below. Then click the **Connect** button.

Security WPA2-Personal ▾

Please select the wireless security method used by your existing wireless network.

Pre-shared Key Cisco2024

Please enter a Pre-shared Key that is 8 to 63 characters in length.

Cancel

Connect

Active

Wireless-N Notebook Adapter

Wireless Network Monitor v1.0

Model No. **WPC300N**

Deliverable 5:

This is documentation illustrating the network configurations done from deliverables 1-4.

Network security configurations:

- Firewall was added before Midrand's router, and the function of the firewall is it monitors traffic. In the case of which the firewall detects traffic with malicious software it will reject it therefore keeping the network safe.
- WPA2 and WPA3 is used for wireless connections the reason behind using WPA2 and WPA3 it has a key feature which is encryption protocols. This is an example of the configurations made to the network to ensure wireless connections have security measures in place.
- VLANs were used to segregate the traffic thus improving security of the entire network. If VLANs were not used in the network viruses could have spread throughout the whole network leading to the compromise of the three campuses.
- Configuration of all devices which all need to have a unique IP address for the specific campus which has a network range.
- Configuration of VPNs for remote user access set up by using the correct protocols for the VPN.

Intrusion prevention:

- The configurations that are made throughout the network need to be strict and some form of access control needs to be established such as a password needed to connect to the wireless access point.
- Anomaly detection techniques need to be in place to help in the detection of abnormal behavior e.g. Firewall

Security Monitoring:

- Tools for monitoring network traffic need to be used this is to ensure the confidentiality and integrity of the network is not tampered with.
- Security audits need to be conducted regularly, including tests which will show whether the security of the network is effective or not.

User authentication and authorization:

- The continuous update of user access permissions according to the role throughout the three campuses.
- The use of WEP password in each access point this allows us the network to control the connection of users that have the authorization and users that don't.

Update and patch management:

- Before the patch is issued to the network it needs to be tested in a controlled environment to ensure the patch is compatible with the network.
- Maintenance of the network should be planned reason behind this is to not disturb operations within the network.


Vulnerability scanning:

- Tools such as Nmap which scans ports throughout the network can aid in finding weaknesses in the network. What we then do is put the vulnerabilities in categories from minor to major.
- Major vulnerabilities will be prioritised as they contain a bigger risk to the network

Security reporting, change management and communicating stakeholders:

- Frequent reports should be sent to stakeholders informing them about the security reports regarding the network.
- Annual meeting where all stakeholders are present should be held where an update is given regarding the network.
- Change in management strategy should be developed which includes planning, implantation, embedding of change, review and analysis this will aid in a smooth transition regarding the configuration and changes made to the network.

The documentation above illustrates the plans to improve the network making it more efficient, safe and reliable.



ITNSA2-B33 Summative Project ZinTech College

Njabulo Ncube:
CON-852316-T3L3

Masego Oratilo Matsafu:
MD.2022.X8J9S4

Luthando Raji:
Eduv4844015

Thabiso Nxumalo:
Eduv4820263

2024/09/02



Table of Content

- Introduction
- Network Plan
- IP Address Plan
- Plan Implementation
- Security Implementation
- Remote Access
- Conclusion

Introduction

Purpose:

Developing a network that can provide high speed connection to all the campuses in a secure manner.

Objective:

High-speed network and security infrastructure.

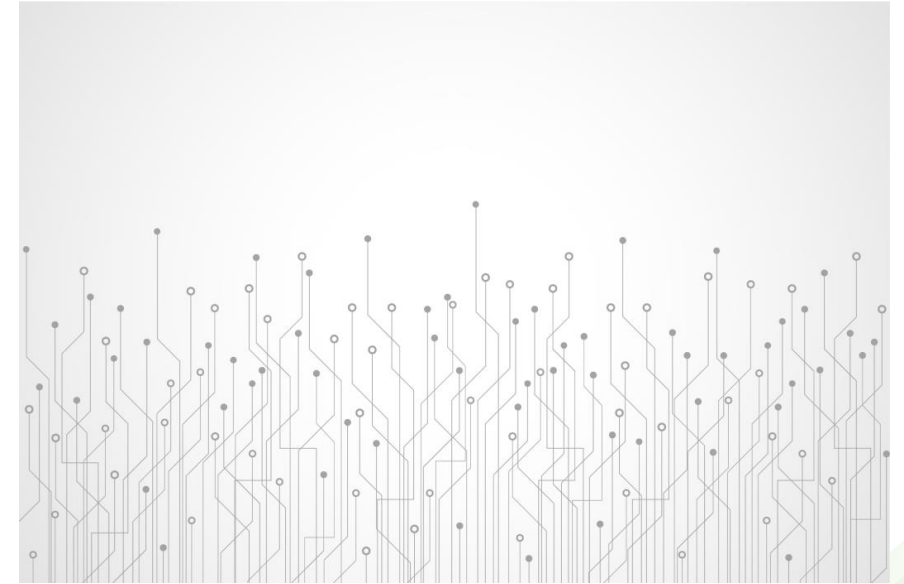
Agenda:

- Network Plan
- IP Address Plan
- Plan Implementation
- Security Implementation
- Remote Access

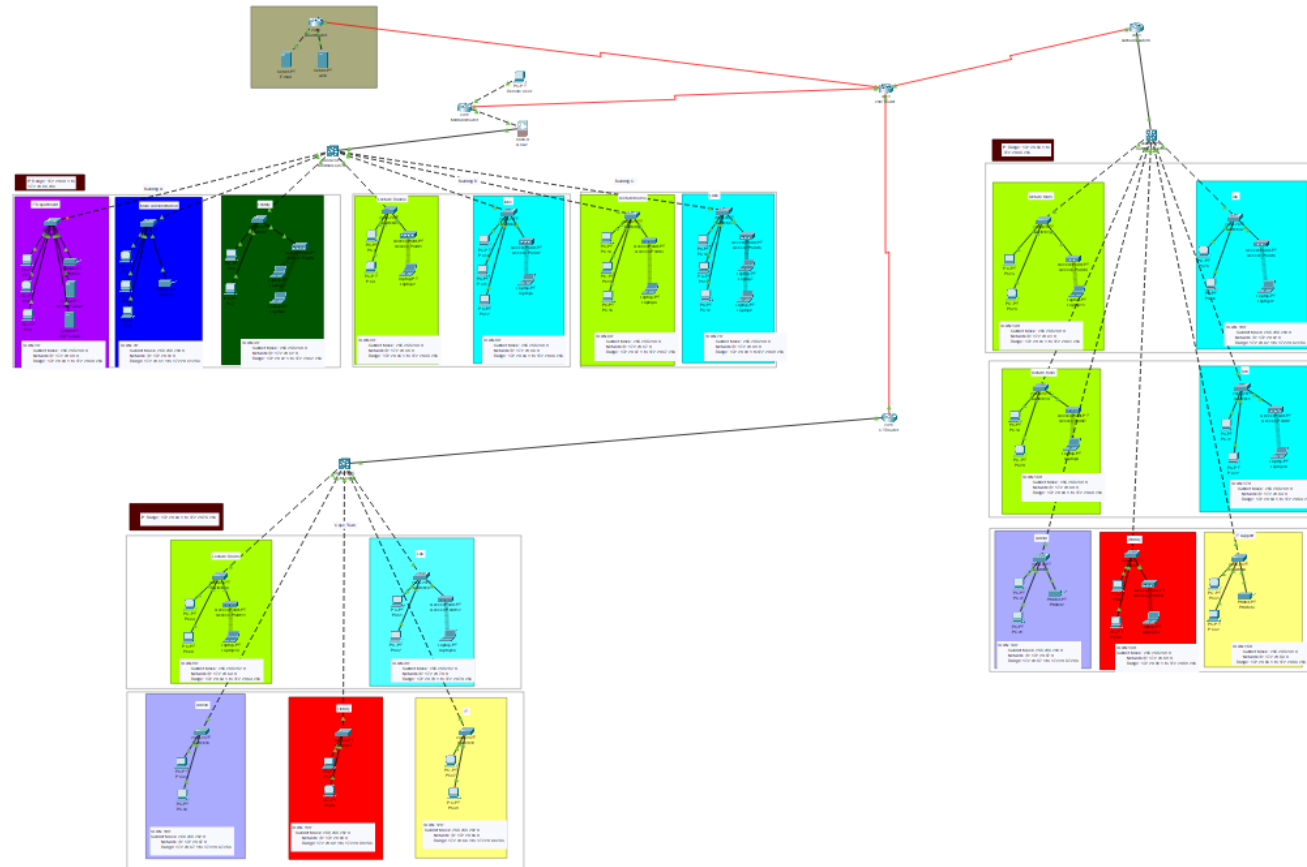
Network Plan

Purpose:

The network plan uses a hierarchical model with core, distribution, and access layers to ensure high-speed and secure connectivity across all campuses. The core layer switches are Cisco Nexus 9000 Series, the distribution layer switches are Cisco Catalyst 9500 Series, and the access layer switches are Cisco Catalyst 9300 Series.

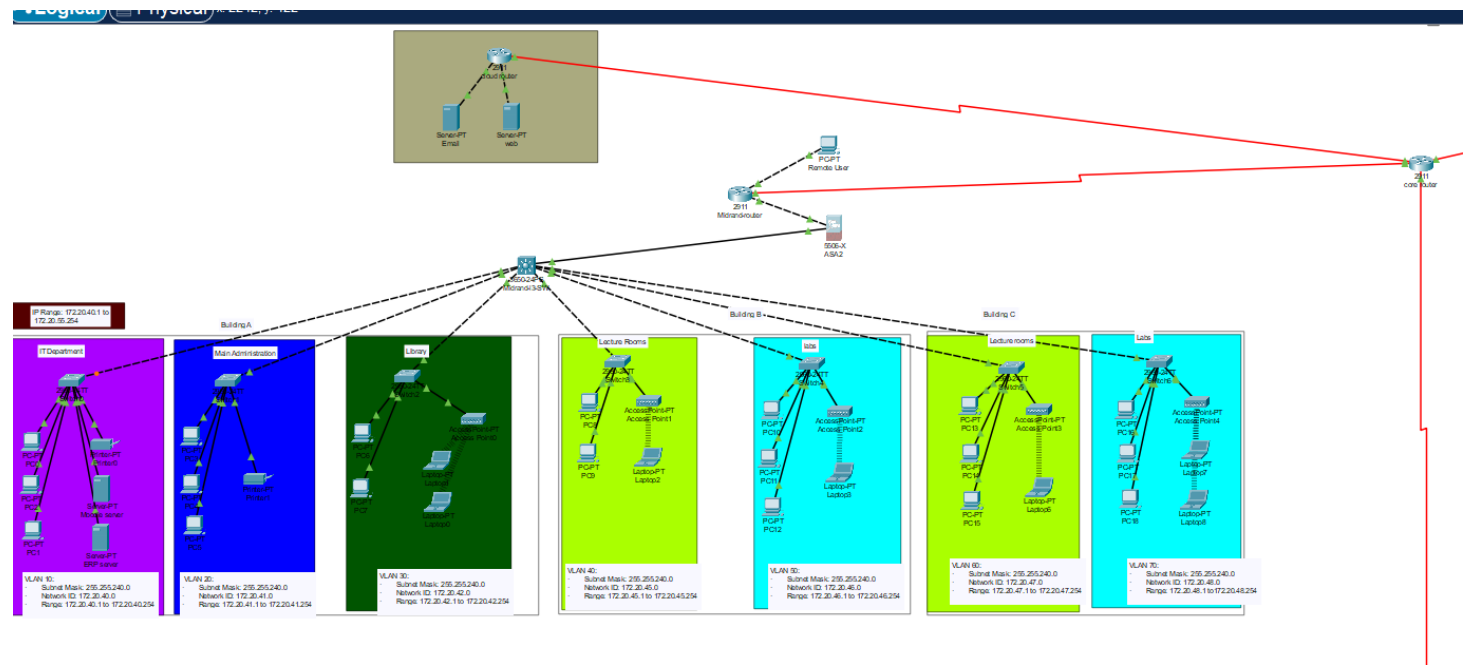


Network Topology



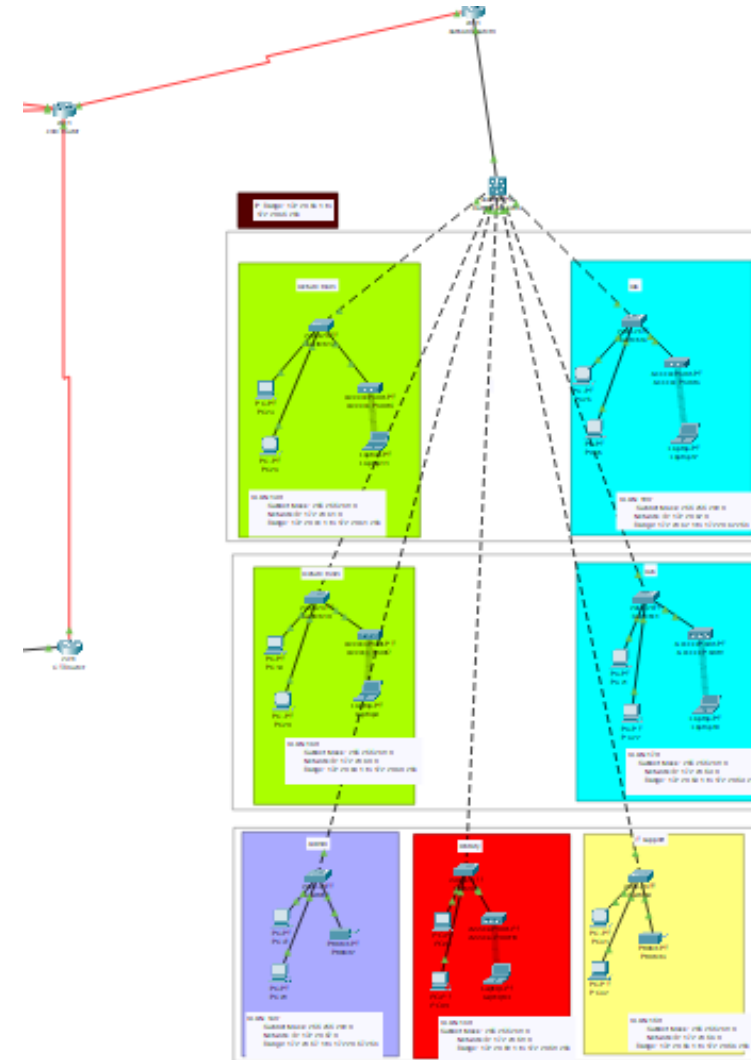
Key Components

Midrand Campus



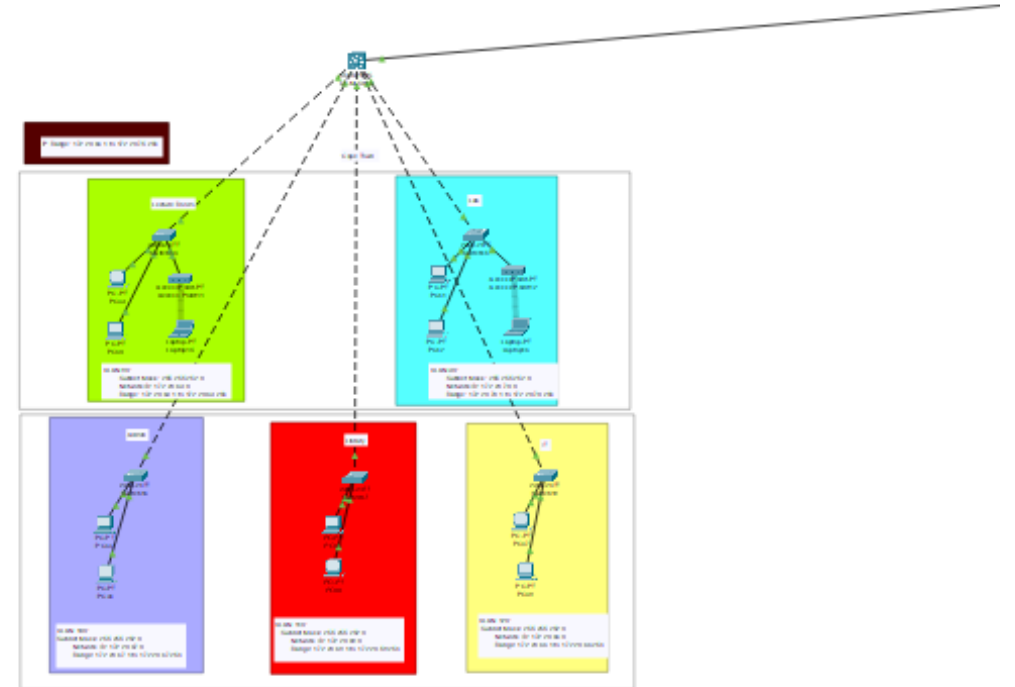
Continuation

Durban Campus



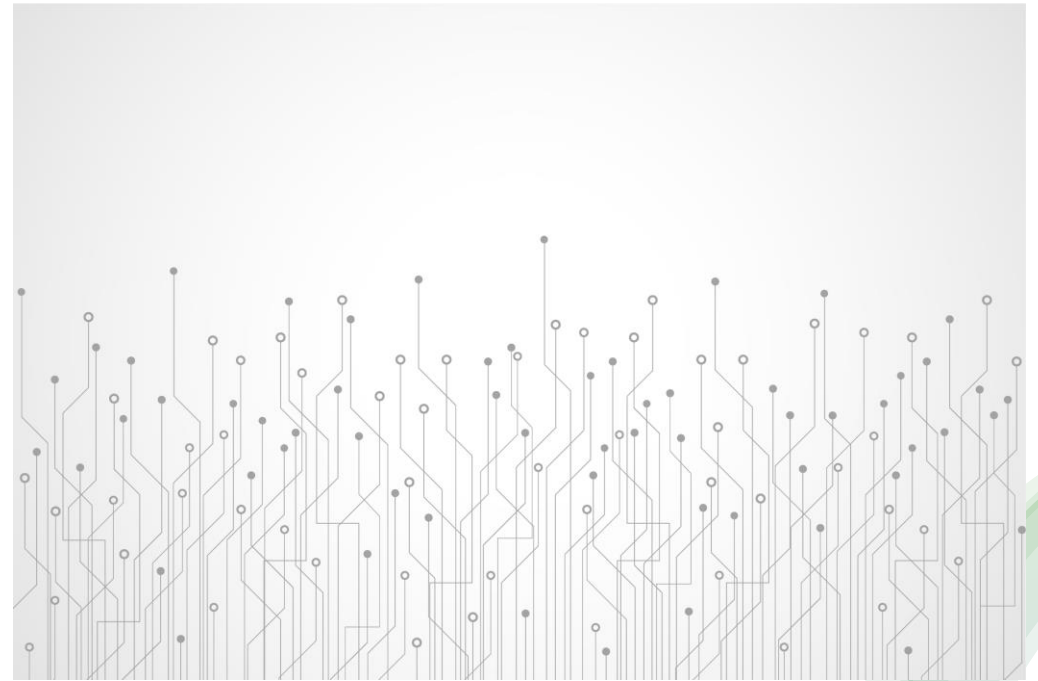
Continuation

Cape Town Campus

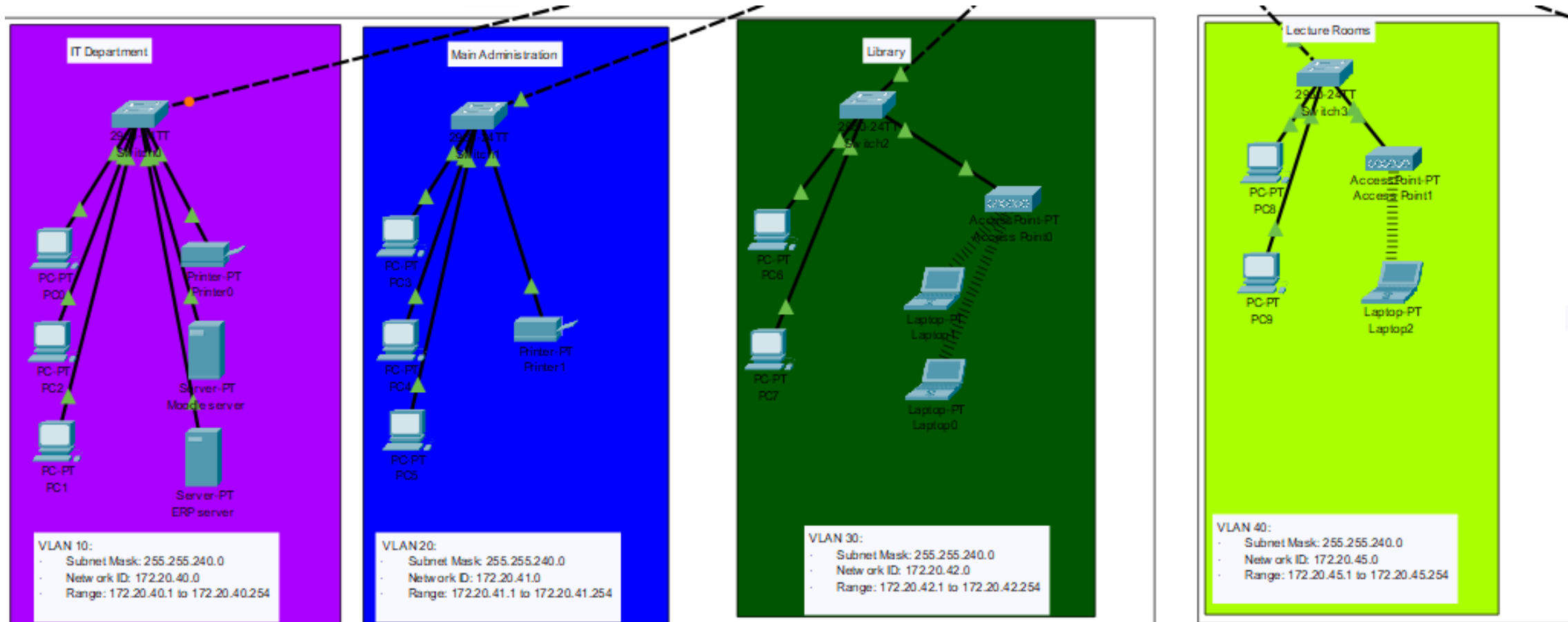


Network Plan

- The network is divided into 256 subnets, each with 256 IP addresses (254 usable afterward), and a centralised authentication system based on RADIUS servers ensures seamless access to campus resources. The Class B IP address range allows for future expansion without having to reconfigure the entire network, which improves security by isolating traffic and simplifies network management and problem solving.



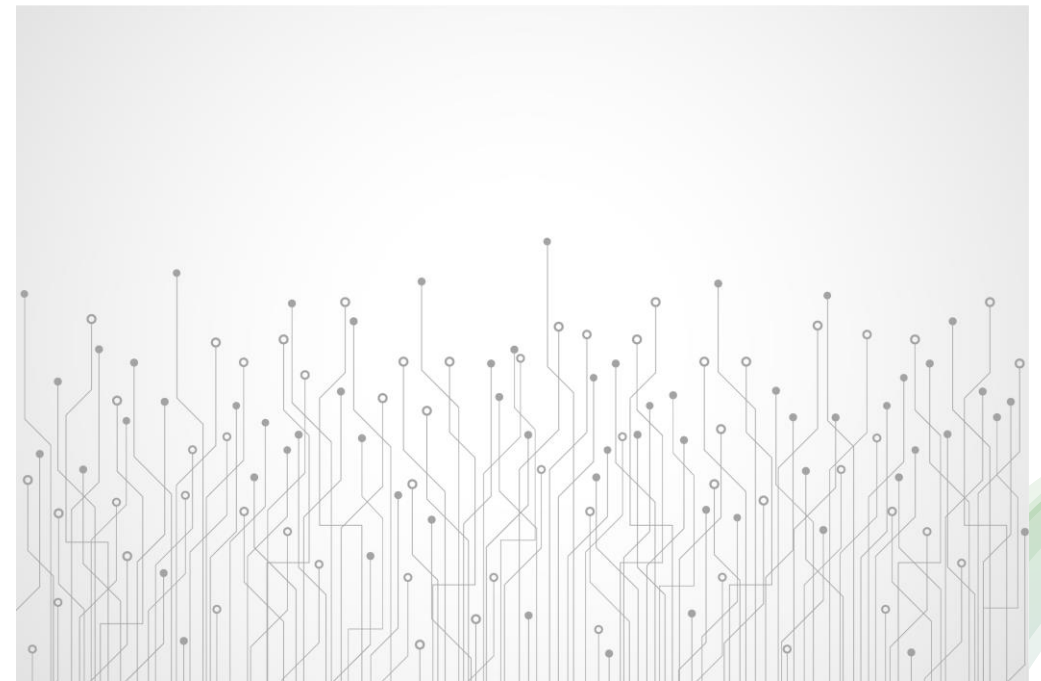
Network Segmentation Visuals



IP Address Plan

Purpose

- Class B private range (172.20.40.0 - 172.20.75.254) is used. The range is divided into subnets based on each campus and department VLAN is used to isolate traffic and enhances the overall security.
- **Midrand:**
 - **Building A:** IT (172.20.40.0), Admin (172.20.41.0), Library (172.20.42.0)
 - **Building B:** Lecture Rooms (172.20.45.0), Labs (172.20.46.0)
 - **Building C:** Lecture Rooms (172.20.47.0), Labs (172.20.48.0)
- **Durban:**
 - **Ground Floor:** IT (172.20.56.0), Admin (172.20.57.0), Library (172.20.58.0)
 - **First Floor:** Lecture Rooms (172.20.59.0), Labs (172.20.60.0)
 - **Second Floor:** Lecture Rooms (172.20.61.0), Labs (172.20.62.0)
- **Cape Town:**
 - **Ground Floor:** IT (172.20.66.0), Admin (172.20.67.0), Library (172.20.68.0)
 - **First Floor:** Lecture Rooms (172.20.69.0), Labs (172.20.70.0)
- 256 IPs is supported by each subnet which includes a RADIUS-based central authentication system guaranteeing secure access.



IP address scheme

IP Address Scheme

Addressing Strategy:

- Using IPv4 within the private Class B range (172.20.40.0 - 172.20.75.254) which guarantees compatibility and manageability.

Subnetting:

- Divided by location and department and offers 256 Ips each. This enhances security and makes the management of the whole IP address scheme manageable making the growth and scalability more simple.



IP address plan continuation

Address allocation

Static vs. Dynamic:

Important infrastructure such as servers, printers, routers and switches are assigned a static IP address.

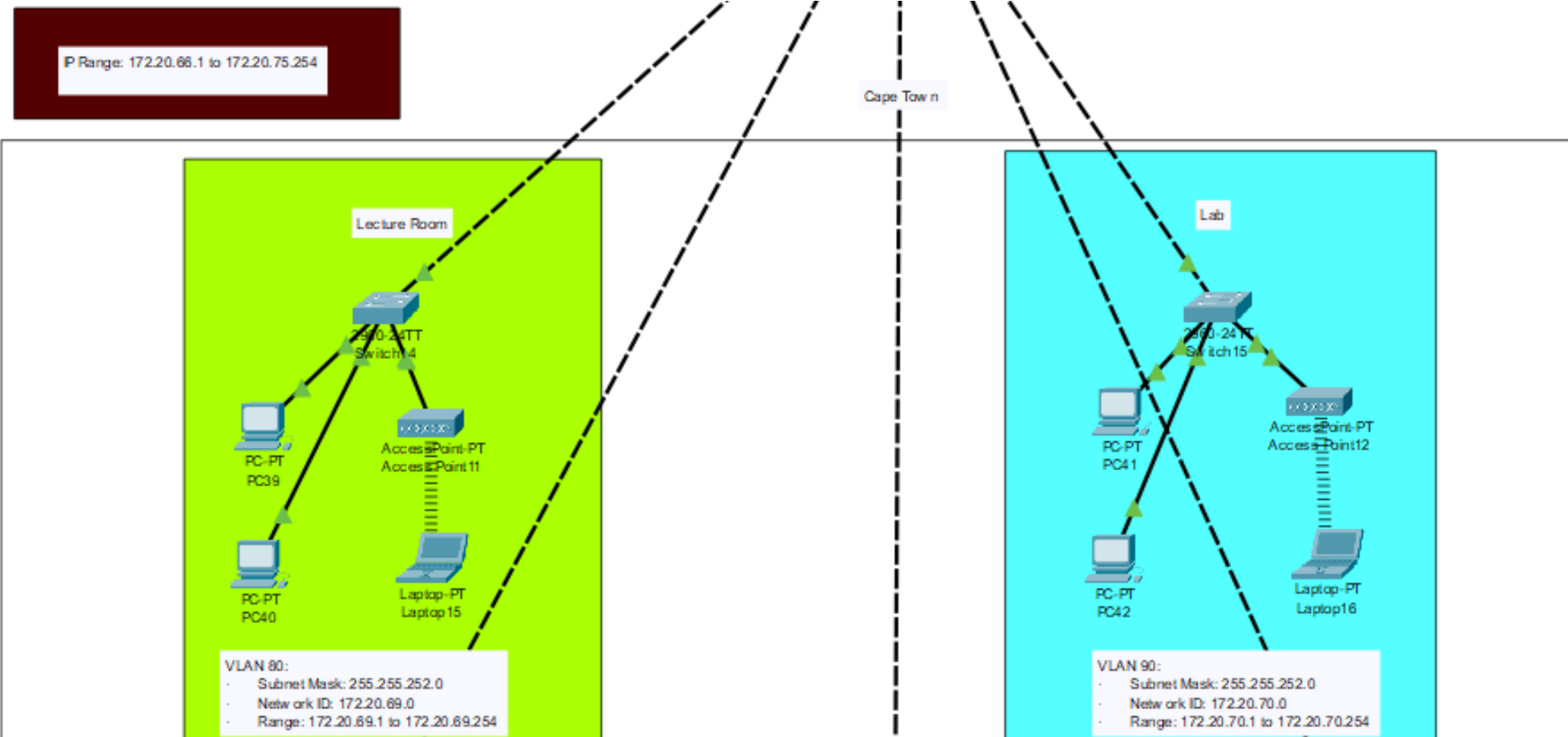
While with end-user devices such as laptops and computers the use of a DHCP server is in place.

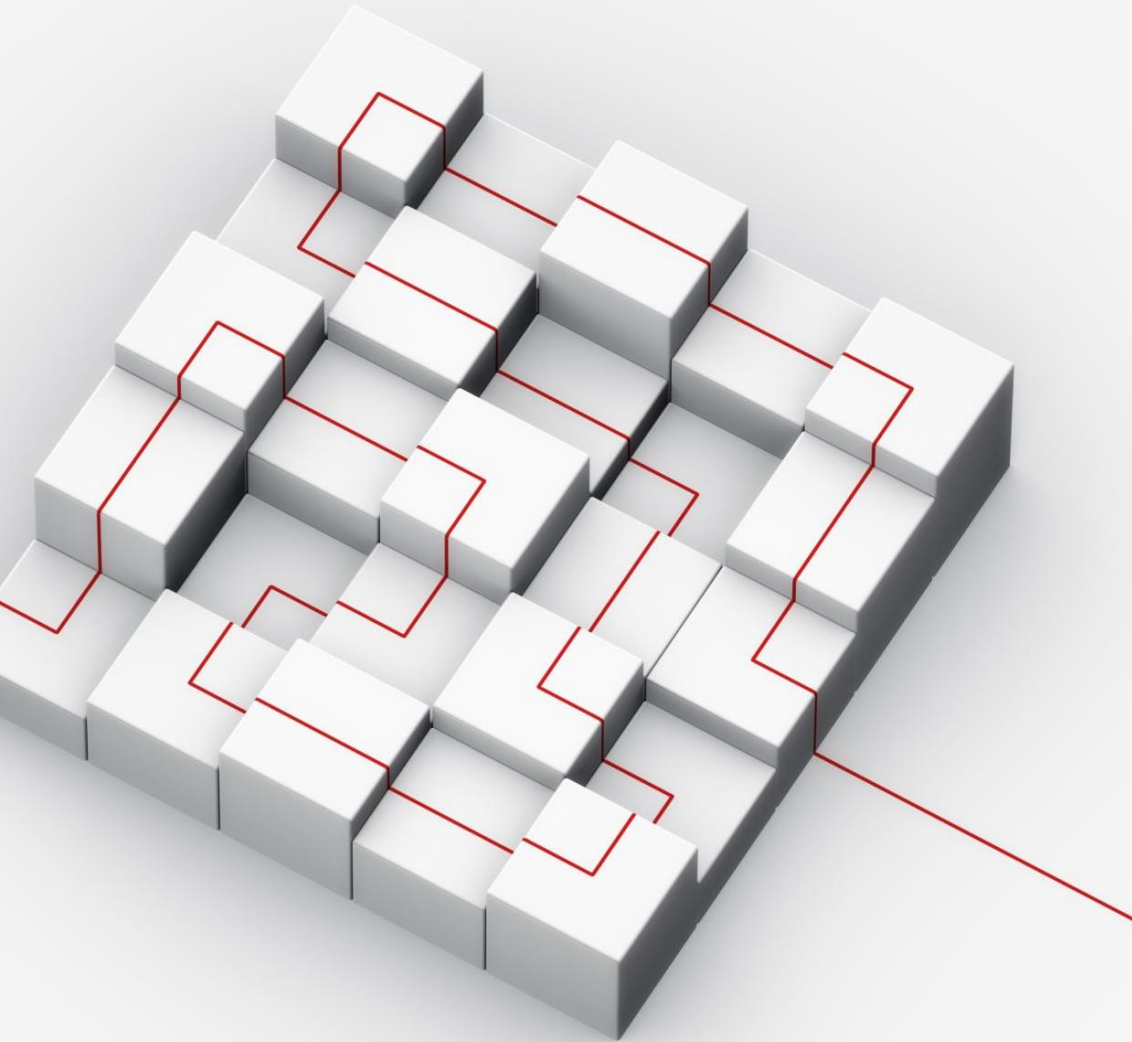
IP Range:

- Midrand: IT (172.20.40.0), Admin (172.20.41.0), Library (172.20.42.0), Lecture Rooms (172.20.45.0), Labs (172.20.46.0)
- Durban: IT (172.20.56.0), Admin (172.20.57.0), Library (172.20.58.0), Lecture Rooms (172.20.59.0), Labs (172.20.60.0)
- Cape Town: IT (172.20.66.0), Admin (172.20.67.0), Library (172.20.68.0), Lecture Rooms (172.20.69.0), Labs (172.20.70.0)



Visuals





Plan implementation

Phases

Planning: Finalization of the network design and security measures. (1 week)

Setup: Installation and configuration of network devices, IPs, VLANs, and VPN. (2 weeks)

Testing: Verification of network connectivity, performance, and security. (1 week)

Deployment: The Rollout of ZinTech college network and connection of devices such as computers and laptops. (1 week)

Validation: Monitoring the performance and resolving issues such as Users not being able to connect remotely . (1 week)

Plan implementation continuation

Timeline

Week 1: Planning the network design

Weeks 2-3: Configuring all the network

Week 4: Testing by sending packets

Week 5: Deployment

Week 6: Validation

Resources

Tools: Cisco Packet Tracer

Testing & Validation

Performance: Speed and bandwidth checks.

Reliability: Stability and downtime monitoring.

Security: Firewall and VPN validation.



Security Implementation

Purpose: The security measures protect the network from unauthorised users and potential hacking attempts using ASA firewalls, role-based access controls, MFA, encryption, and IDS/IPS for real-time threat detection.

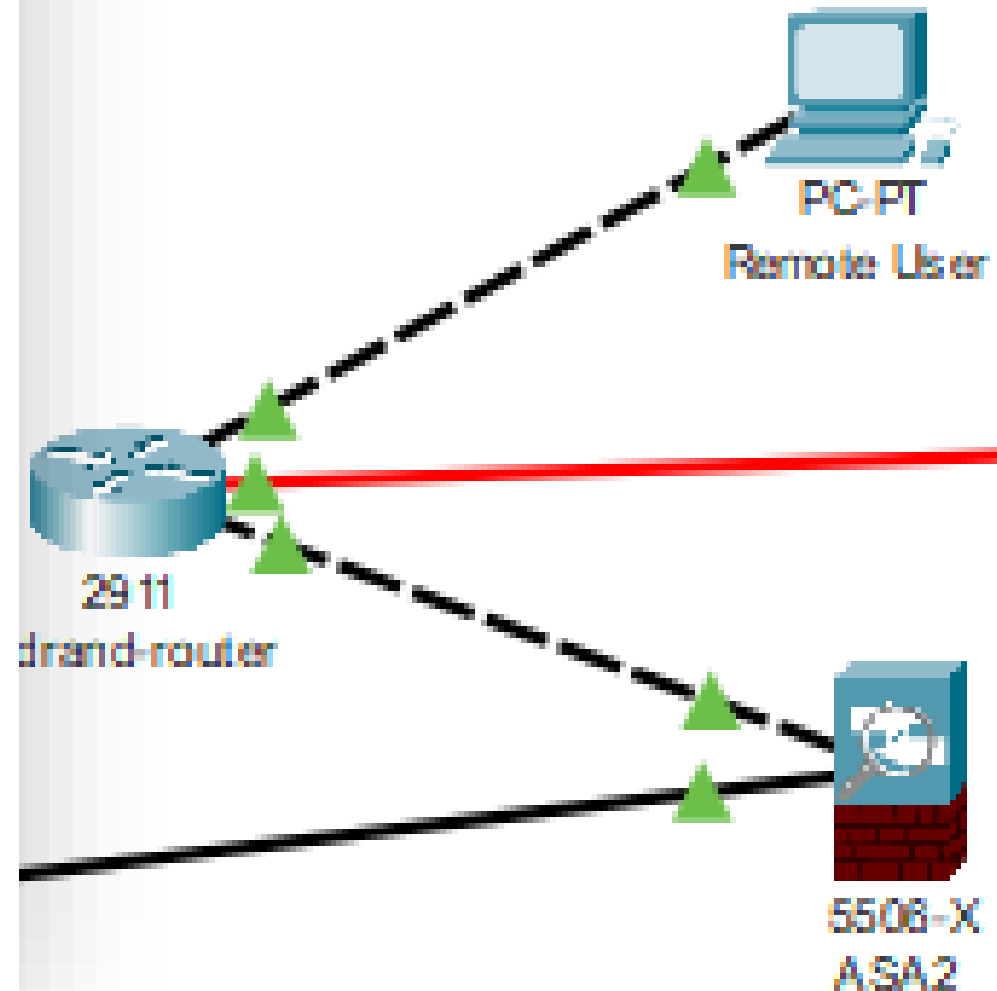
Firewalls:

ASA firewall uses NAT, ACLs to protect the network. Also, monitors traffic and regulates it.

Access controls: Role based access (RABC) uses RADIUS and MFA for secure access.

Encryption: Uses SSL/TLS, IPsec, and encryption protocols to protect data.

Intrusion Detection/Prevention Systems (IDS/IPS): Blocks unauthorised users by monitoring them.



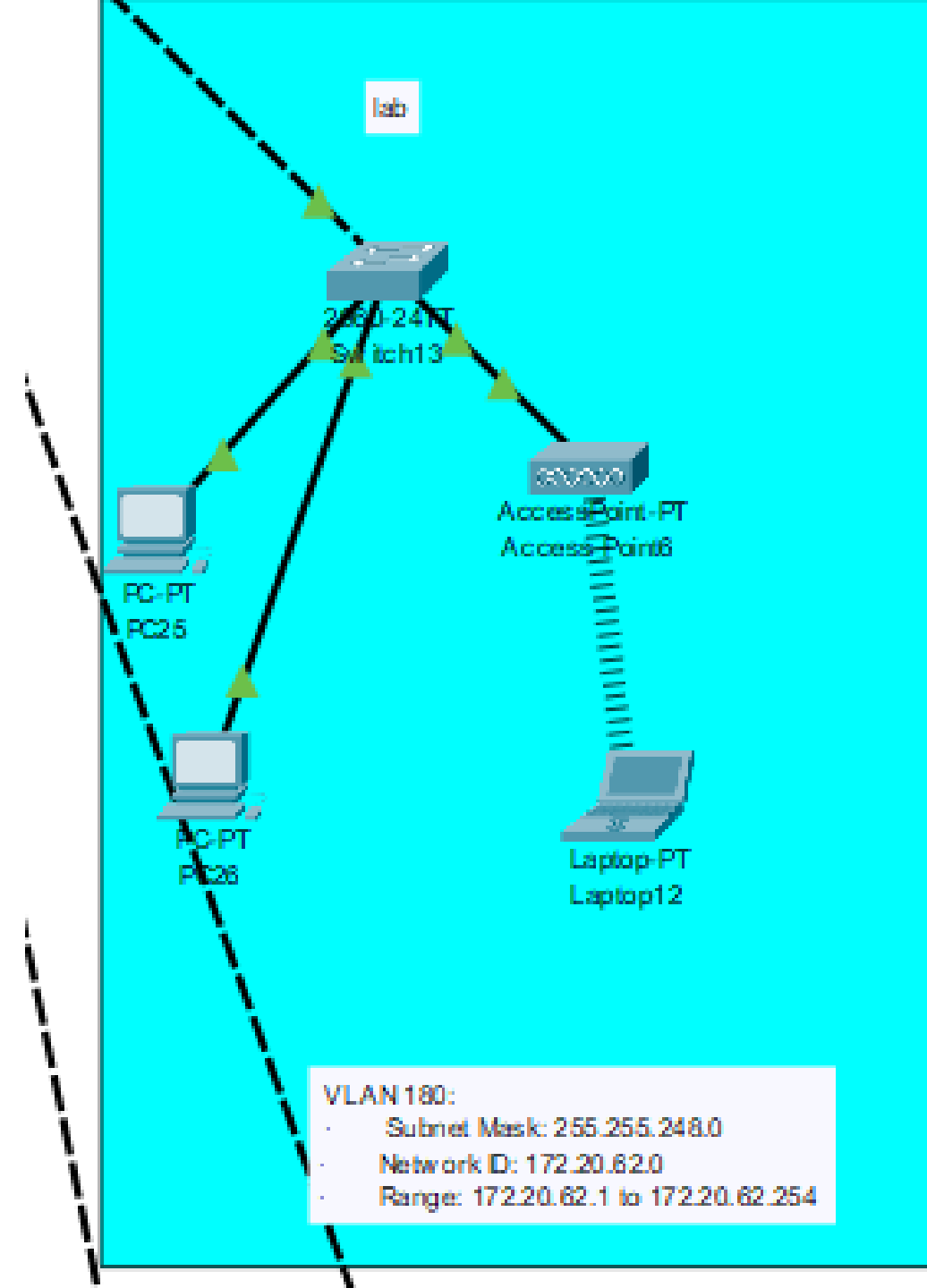
Remote Access

VPN Solutions: IPsec VPN is used for securing remote connections it has encryption and authentication features that are advanced ensuring the remote user's data is confidential between the network.

Authentication: Remote users authenticate using credentials managed on the local router.

Access Policies: Remote users can only access the specified resources based on the role that has been assigned to them.

Tools & Software: Laptops are configured with wireless modules for VPN connectivity which the user can connect to the wireless access point.



Conclusion

Recap

- The network design for ZinTech College includes IP addressing scheme, segmented into subnets with VLANs for different departments such IT and Labs.
 - ASA firewalls secure the Midrand campus.
 - IPsec VPN provides secure remote access.

Benefits

- The network design offers fast and easy scalability, security, and access for remote users thus allowing the network to grow with the college's exponential growth while ensuring the safeguarding of data and user access.
- Next Steps: Future considerations potentially adding a new campus to the network and the potential transition to IPv6. Rolling out updates to address new vulnerabilities.

Closing Statement

- ZinTech college network design is a secure, scalable and efficient network which aligns with the goals of ZinTech college wanting to grow.