Network Design for International University of Rwanda, Kigali

Submitted By: Archana Balachandran
Dec 2, 2016

Table of Contents:

1. Project Overview
2. Area 1: Definition of Organization
3. Area 2: Application Requirements
4. Area 3: Local Area Network Design
5. Area 4: Local Backbone Network Design
6. Area 4-1: WAN Backbone Network Design
7. Area 5: Network Security and Management

Project Overview:

The project aims at designing the network infrastructure for a geographically distributed organization in Africa. The organization considered for the purpose of this project is International University of Rwanda(IUR), which is spread across four countries, spanning 6 campuses.

The aim is to design a network infrastructure with high reliability, scalability and backup and recovery for business continuity.

The areas addressed with respect to the organization are:

- Definition of the Organization
- Application Requirements
- Local Area Network Design
- Local Backbone Network Design
- WAN Backbone Network Design
- Network Security and Management

Area 1: Definition of the Organization

Organization definition

Organization type: International University with distributed campuses and Office locations with Online Capabilities, and also includes a teaching hospital.

Primary purpose: Provision of higher education facilities in the Medical and Engineering fields

Primary employee types: Management board officials, Administrative board staff, Academic staff, Information Technology staff, Accounts staff, Admissions staff, Support Staff, Doctors, Medical Staff

Primary client type: Students, Patients,

Physical Infrastructure:

1. Diagram of organization's worldwide layout

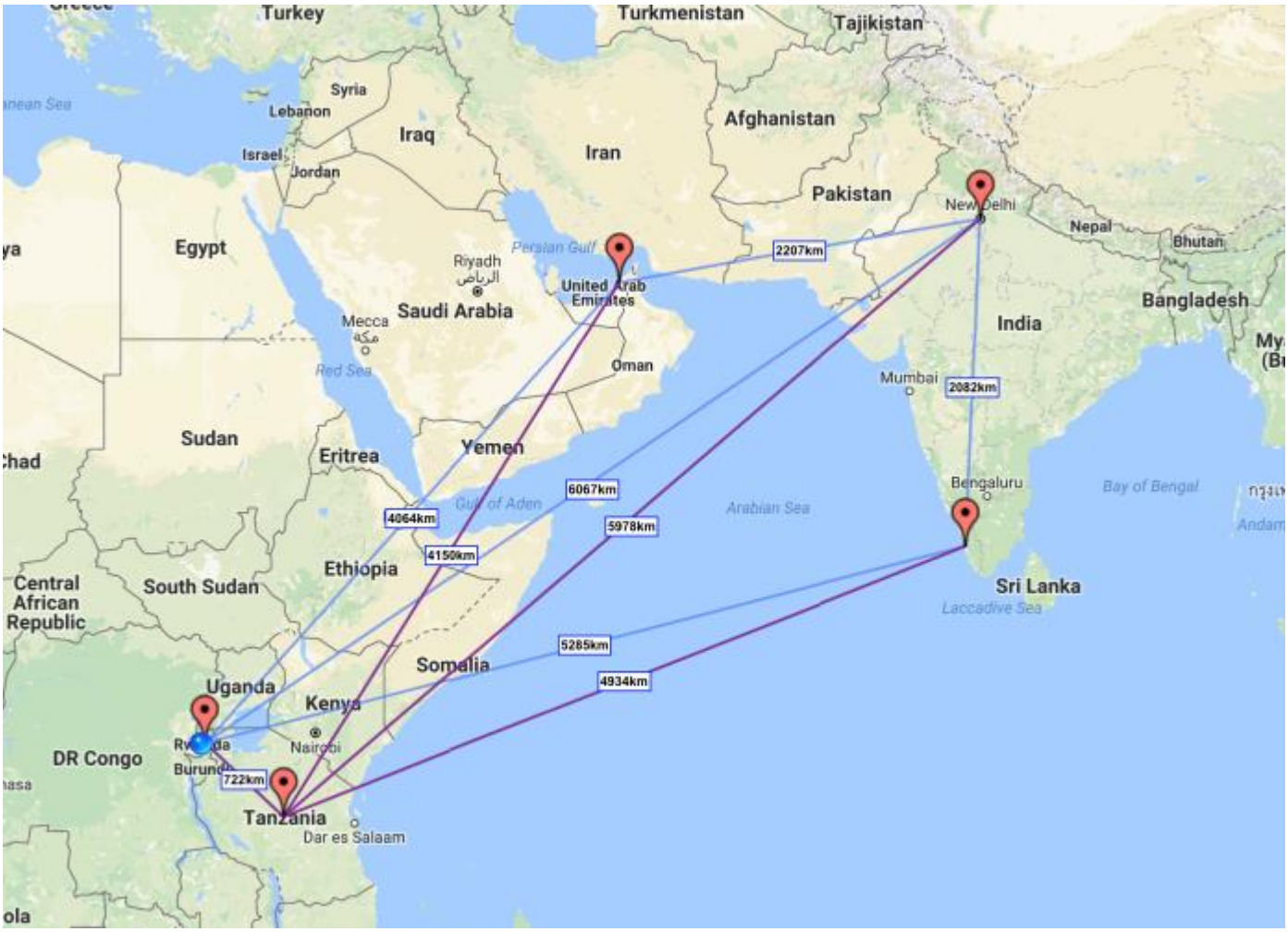


Figure 1: Map showing all campus locations. Campuses with at least 1600 km are indicated above.

The map above clearly indicates the 6 campus locations for International University of Rwanda in four countries, along with the distances between each location.

Campuses 1 and 2 are located in Kigali. Campus 1 is the Main Campus, while Campus 2 is a Regional office. Campus 3 is located in Tanzania, which is a Regional Office. Campuses 4,5 and 6 are also Regional Offices which are located in Dubai(United Arab Emirates), New Delhi(India) and Cochin(India).

As per the project requirements, the selected Campus 1 and Campus 2 are within 40 km distance from each other.

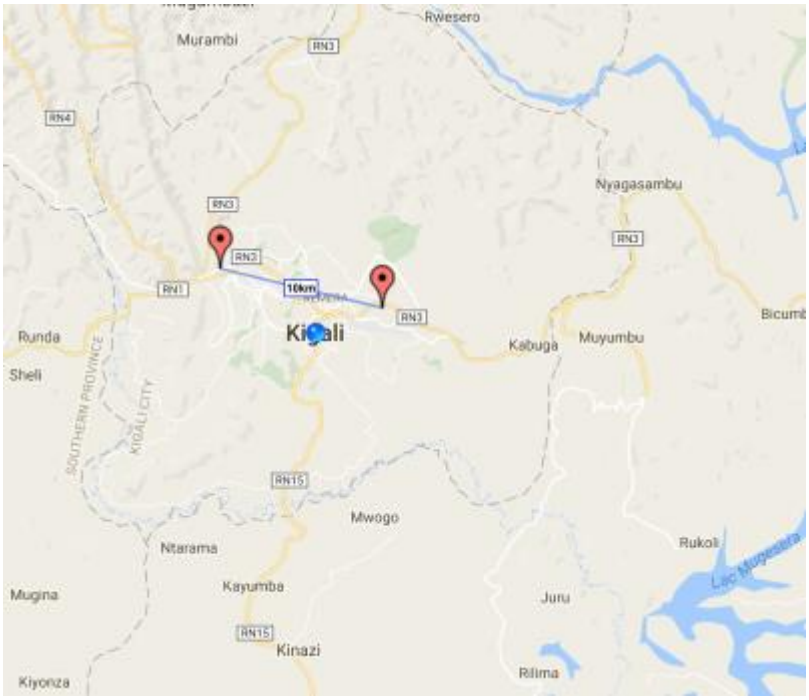


Figure 2 Campuses within 40 km distance

2. Relative Campus Building Locations:

Only the main campus (Campus 1) has multiple buildings, because all other campuses are Regional offices spanning only one building.

Figure 3 Main Campus map. Buildings circled in yellow are the selected buildings for the networking project.

The figure above shows the map of the Main Campus in Kigali, Rwanda. Circled in yellow are the three buildings selected for the purpose of this project, and a few other relevant buildings, and does not include every building on the campus. The campus primary consists of the Administration Block, classroom Blocks(6 blocks) , Research Lab, Dining Block, Recreation Center and one on-campus Residence Block.

The Buildings with 500 feet range: Classroom Block and Research Lab
Buildings with 50 feet range: Classroom Block and Administration Block

The matrix below shows some of the buildings and their distances from each other.

	Admin Block	Research Lab	Class Block A	Residence Block	Recreational Center	Dining Block
Admin Block	0	40 ft	50 ft	20 ft	45 ft	60 ft
Research Lab	40 ft	0	500 ft	70 ft	10 ft	130 ft
Classroom Block A	50 ft	500 ft	0	30 ft	125 ft	20 ft
Residence Block	20 ft	70 ft	30 ft	0	120 ft.	10 ft
Recreational Center	45 ft	10 ft	125 ft	120 ft	0	100 ft
Dining Block	60 ft	130 ft	20 ft	10 ft	100 ft.	0

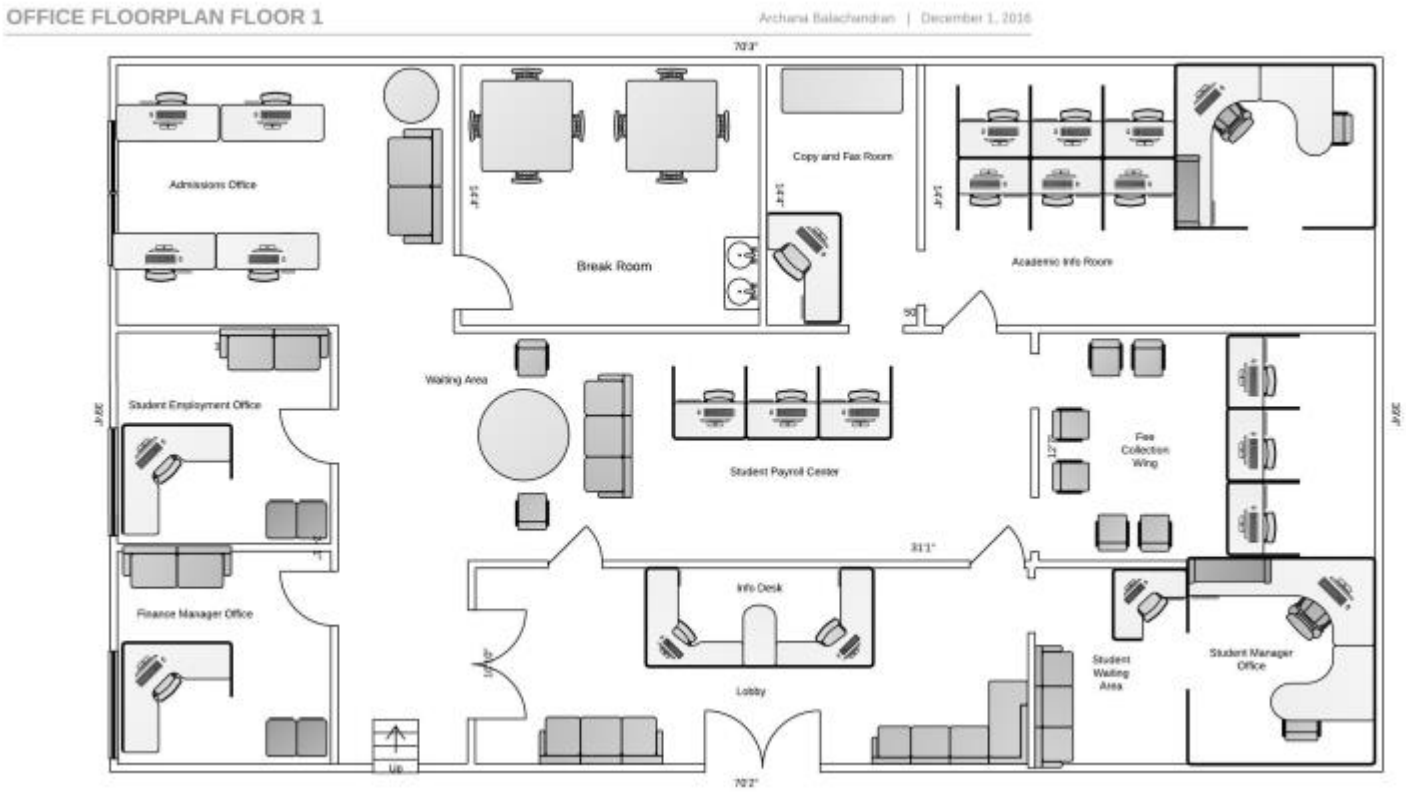
3. Main Campus Buildings Information

For 2 buildings on the Main Campus, the required information is given below:

Building 1: Administration Block
This building is the heart of all operations on the main campus. It handles Admissions, Student Management, Student Employment, Fee Collection, Finance Management and Program Coordination.

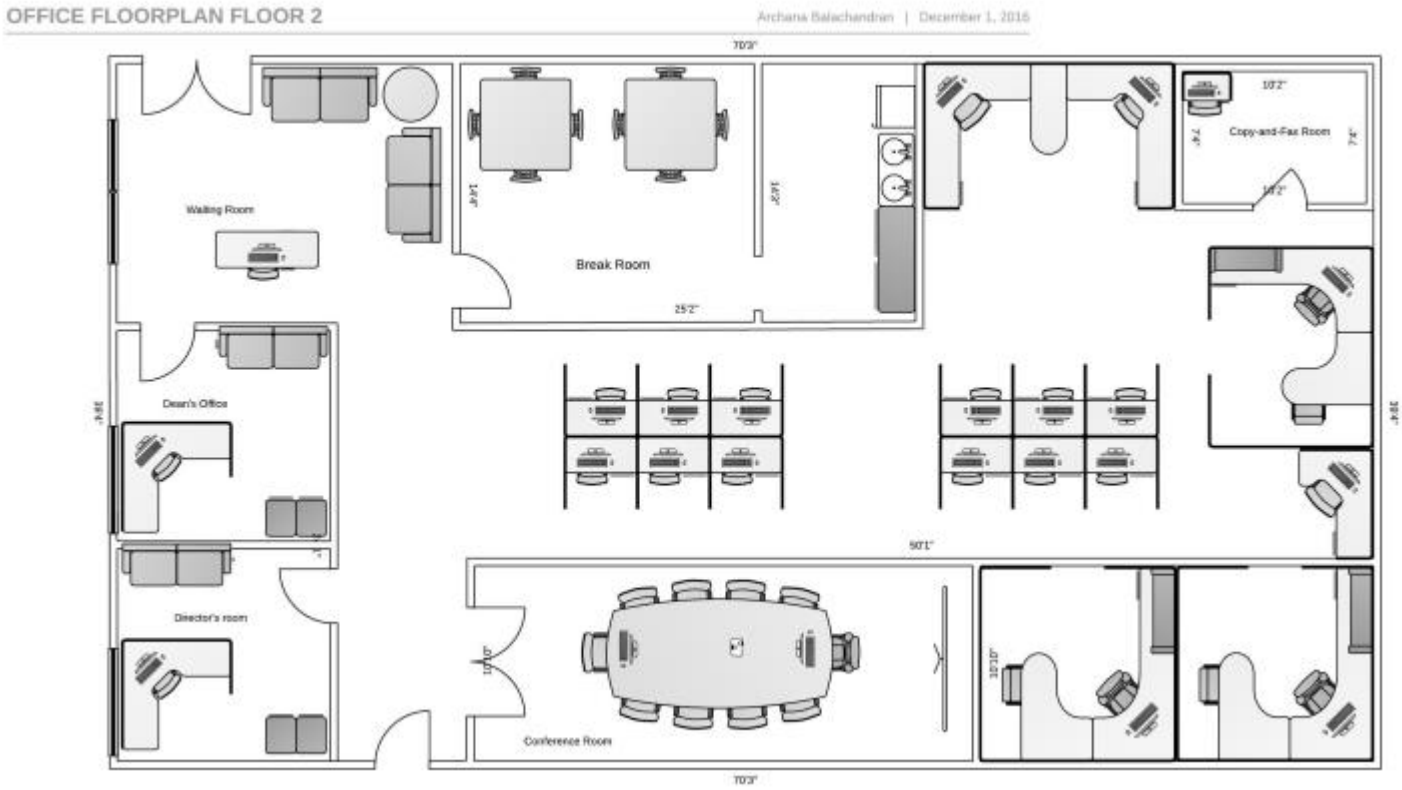
	Building 1- Admin Office
Width	70’30”
Length	39’4”
No of floors	3

Layout and description of ground floor



Description :
This floor is an activity-intensive section of the building where a lot of operational actitivties are conducted. Office staff and students will be present on this floor in a large number. This floow has exactly 24 computers and at least 5 other client nodes including printer, fax machine, file server etc. It is important for this floor to have Wireless Access Points to accommodate large WiFi-enabled devices in the waiting areas and break room. Printers in the Copy and Fax room will also need to be wirelessly set up in the network.

Layout and description of 2nd floor:



Description of 2nd floor:

This floor has reduced wireless activity because students do not have access to this floor, and only the employees will be connected to the Wireless Network. This floor also has at most 24 computers and other devices connected to the network such as printers, fax machine, file server, etc. The Conference Room will require a dedicated bandwidth network for uninterrupted performance.

Building 2: Classroom Block A

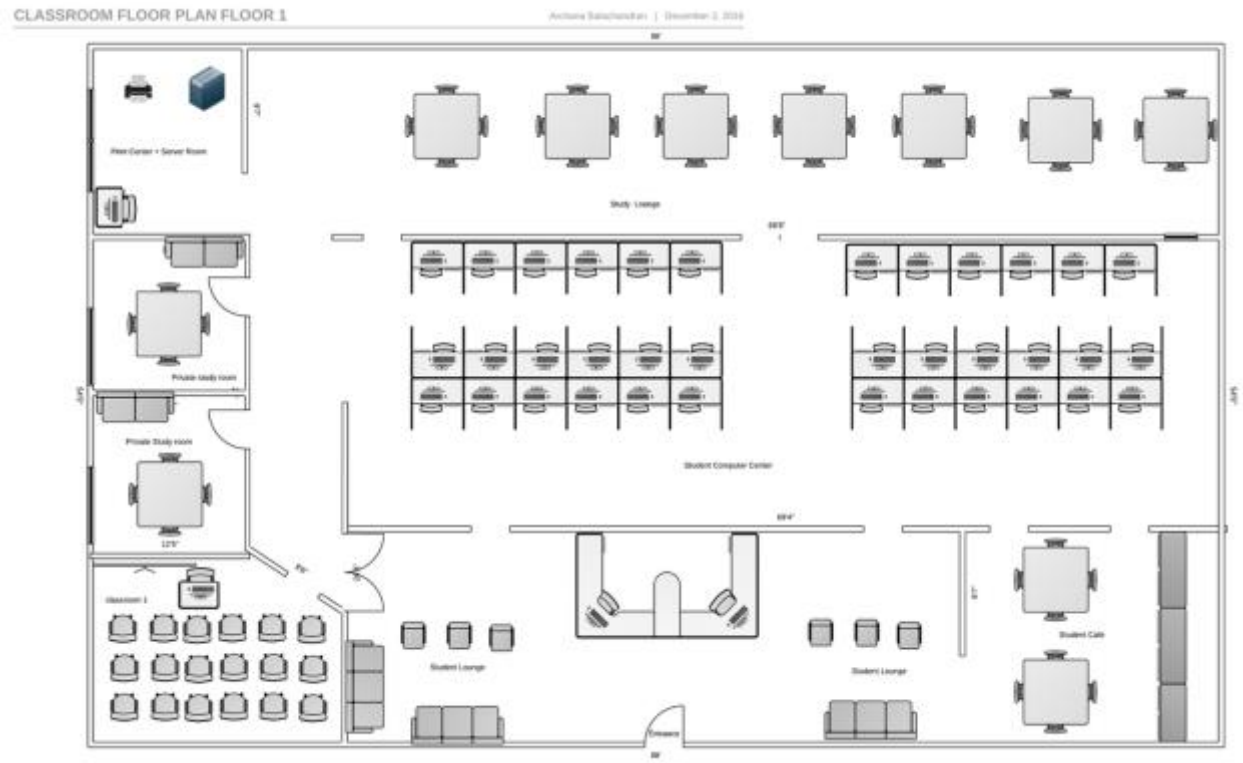
This building has 5 floors, and a total of 15 classrooms. Therefore, there will be a high network traffic in this block. Multiple wireless Access Points are required on each floor to accommodate students who are accessing WiFi on their mobile devoces.

Building Info:

	Building 1- Admin Office

Width	88’
Length	54’5”
No of floors	5

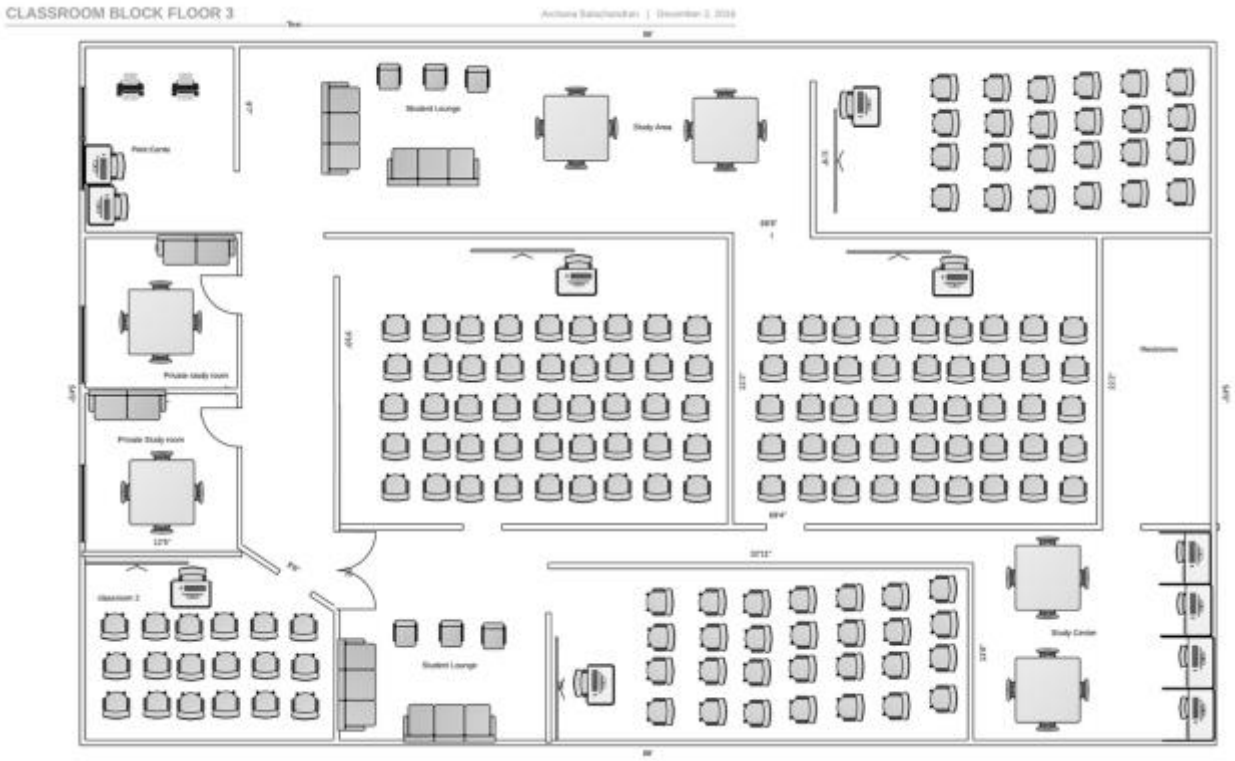
Layout of 1st floor:



Description:

This floor has only one classroom, therefore wireless access is comparatively less on this level. The devices on this floor that are connected to the network are the desktops, laptops, thin clients for student computer center with its server, projector, printer, fax and any handheld devices such as mobile phones, tablets, that will connect to the network wirelessly. 6 Wireless Access Points may be placed on this floor to accommodate all its users.

Layout of 3rd floor:



Description:

This floor will have heavy network traffic because it accommodates 160 students in 5 classrooms. Devices connected to the network are 11 desktops, 2 printers, 5 projectors, and should also accommodate the various handheld devices such as mobile phones and tablets which will connect to the network wirelessly.

4. Thus, the physical Infrastructure Requirements have been met:
    A. Organization's physical infrastructure consists of more than 8 buildings
    B. At least 3 of the organization's buildings reside on a single campus (main campus has multiple buildings). Two of these buildings are separated by at least 500 feet / 150 meters. Two of these buildings are located close together, at most 50 feet (15 m) from each other.
    C. Organization physically spans 6 campuses. Two campuses are separated by 1600 kilometers (main campus and Headquarters in India). Two of the campuses are separated by no more than 40 kilometers (main campus and regional office in Kigali is separated by 10 kilometers)

Area 2: Application Requirements

The network designed for the organization should connect the devices within the campus, and also connect campuses across the globe.

Some of the important Applications:
University Management System, to collaborate and manage the functioning of the university over a network. This platform is to be primarily made available on Main Campus.
Email systems such as Office365
Salesforce to manage the CRM of the entire organization.
AWS to host and manage the organization's websites.

Therefore, the network goals for the company can be defined as:

1. All users should have uninterrupted access (Connectivity)
2. The designed network infrastructure must be scalable to accommodate any future expansion (Scalability)
3. The network should aim for zero technical failures, and in the event of a failure, appropriate backup and recovery processes must be in place (Reliability, Redundancy)
4. The network should be safe to use for all users of the organization (Security)
5. Maintenance, repair and updates should take place with minimum cost. This can be achieved with **standardization** of all hardware and software in the organization. Repairing different types of switches, computers or software is definitely more time consuming and expensive than the maintenance of the same hardware and software components.
6. The infrastructure should be cost effective.

Network Architecture:

Since it is a university campus with multiple clients continuously requesting resources at any time of the day, a client-server based network works well. This model is selected over peer-to-peer networks because in such networks, a client cannot access a device such a printer connected to another client which has been turned off. Therefore, one server can manage all the printers in one building, since servers are rarely turned off, it ensures resource availability.

Server based networks are also scalable, thus the network's size can be easily adjusted to respond to any change in the load on the network. Sever-based networks also enhance the security, since it allows creation of accounts and enables the network administrator to set permissions for different kinds of accounts. For example, if a server hosting the software for

entry of grades is specifically designed for access only by faculty, a student cannot gain access to that server on the network.

A **3-tier architecture** is selected because it has greater degree of flexibility. This architecture also has a higher security, since security can be defined for each service at each level. Since tasks are shared between servers, this architecture demonstrates increased performance. The presentation tier at client side can cache requests, thereby reducing the network utilization. The load on the application and database server tiers thus reduces.

Typical Users of the system:
Network Administrator, Professors, Students, Administration Staff, Guests

Use case: Professors can use the Student management system to upload the student grades, and attendance. Professors can also log their working hours in the Payroll management system. These should be accessed from other systems on the network. For example, if the Dean wants to track student performance, he should be able to do so from his office in the Admin Block.

Application Requirements:

Bandwidth expectation per user:
Number of users at any given time for each location:
Bandwidth per user x Number of users =

The infrastructure must network the file/print server, mail server, web server, college management system server etc.

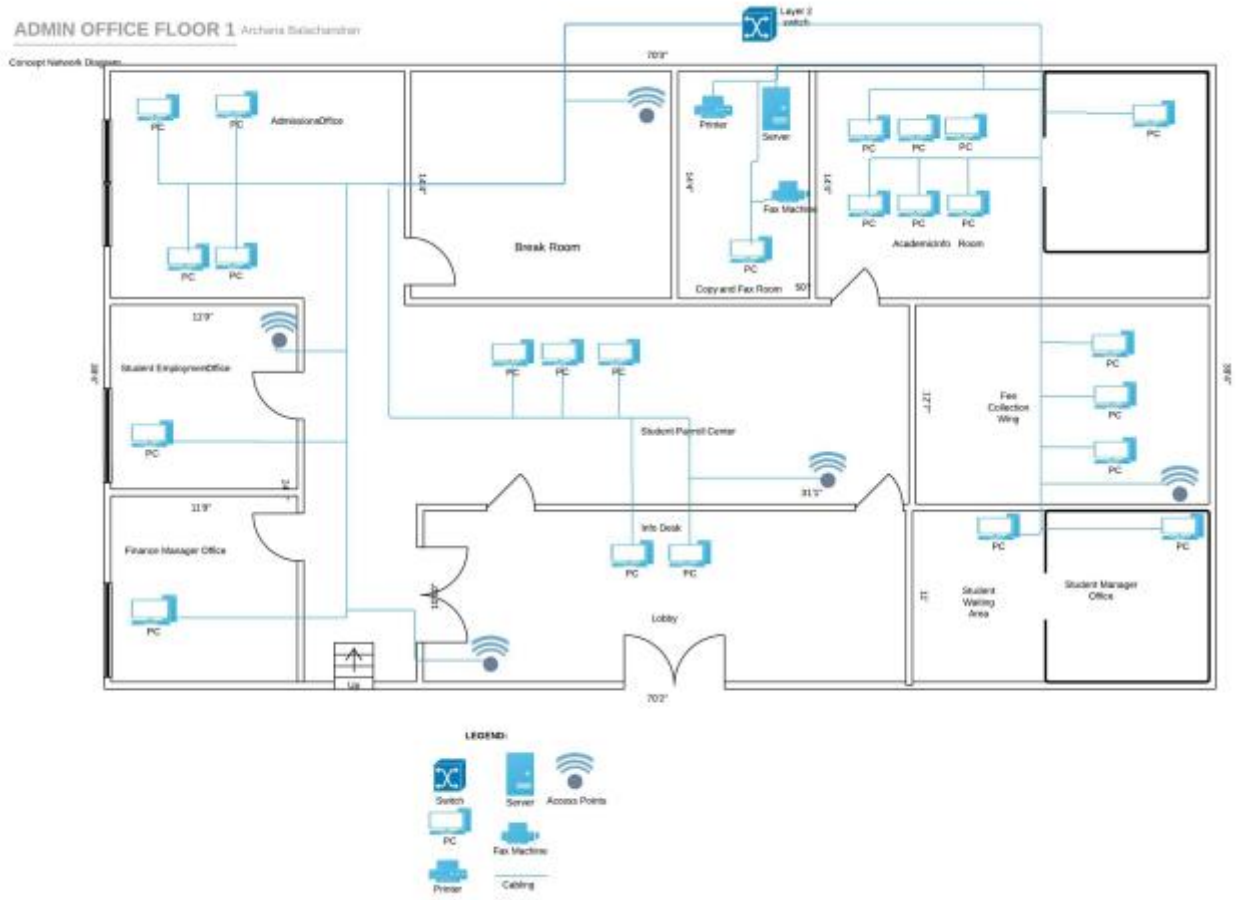
Network service details for Main Campus:

Number of networked PCs – 1000
Number of Users – 3500
Size of bandwidth – 22 Mbps
Bandwidth utilization pattern during working hours (8 am-7 pm) : 100%

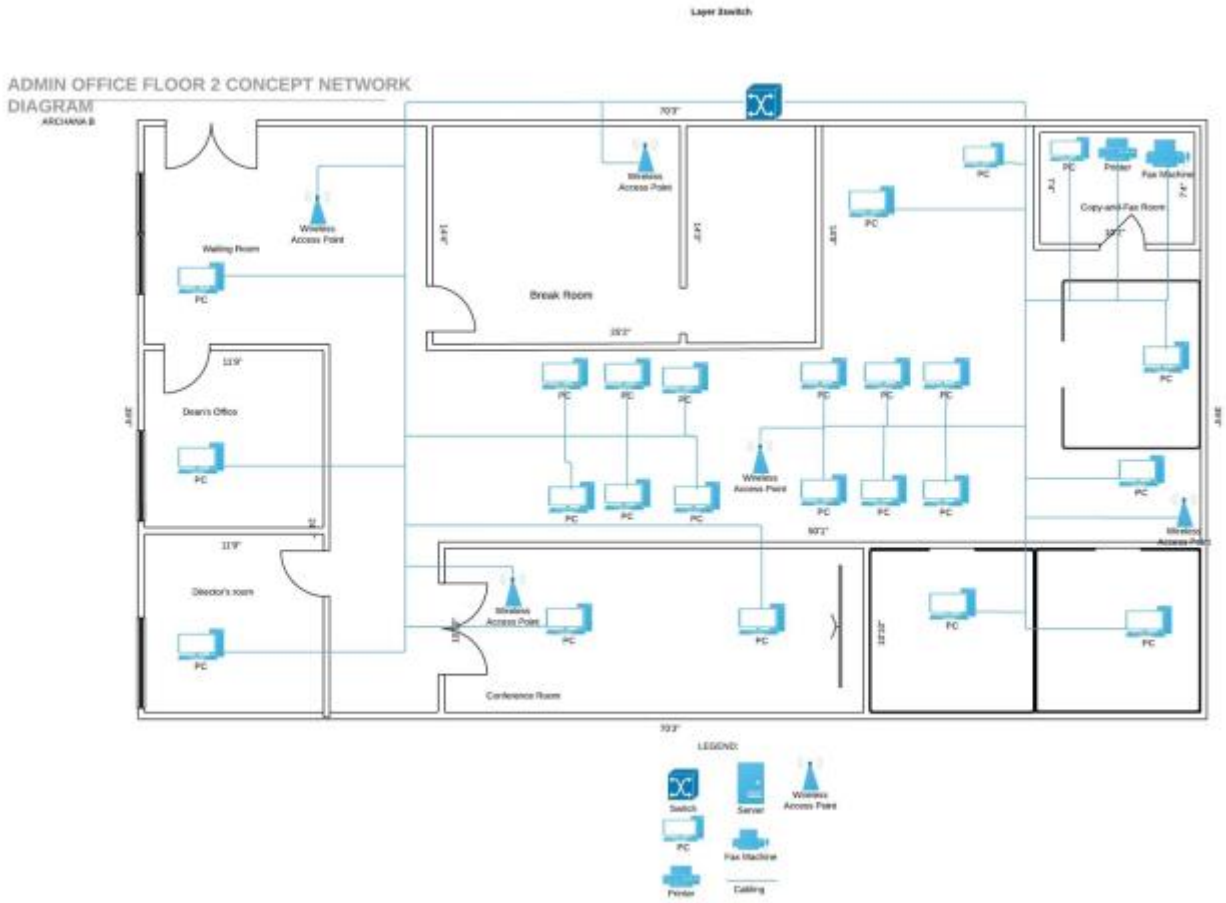
The local area network for the buildings will be a combination of Wired Ethernet and Wi-Fi. Switched Ethernet networks will be built as the primary LAN which is provided for desktop

users and Wi-Fi will be installed as overlay network to allow network access for laptop and mobile devices.

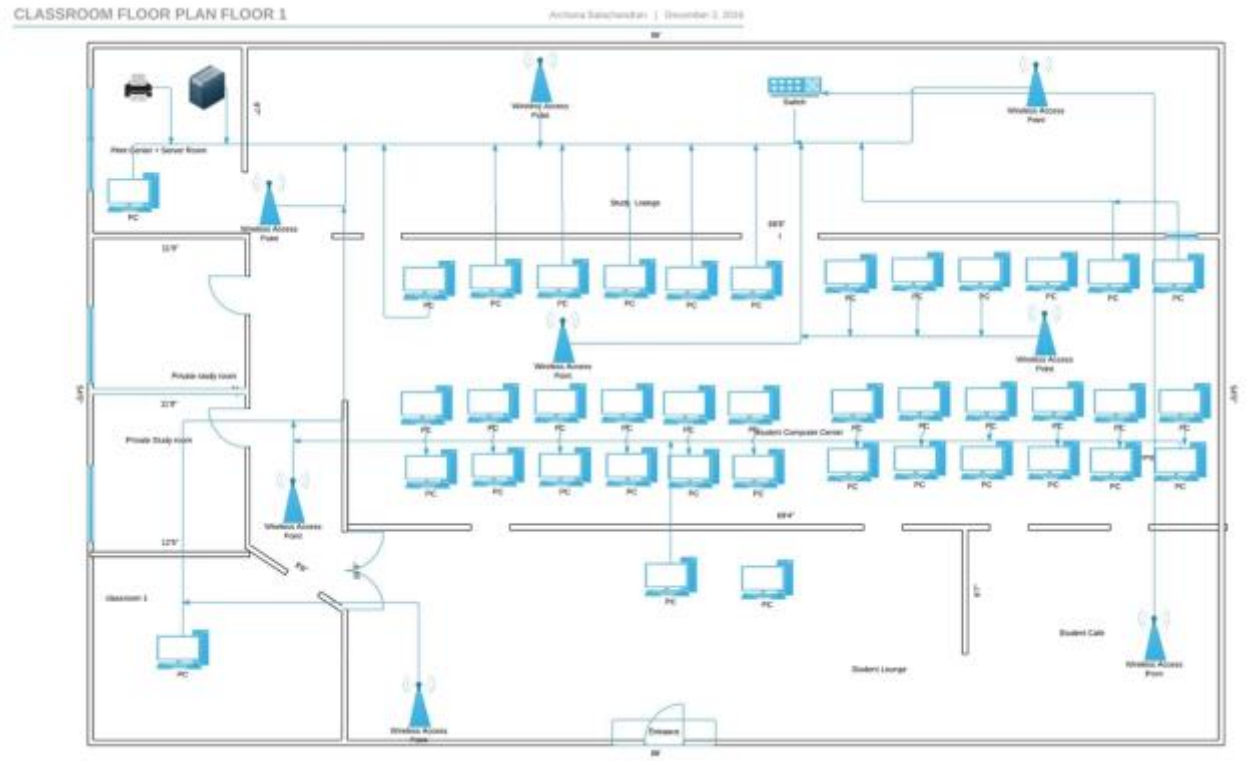
LAN design for Administration Block-floor 1



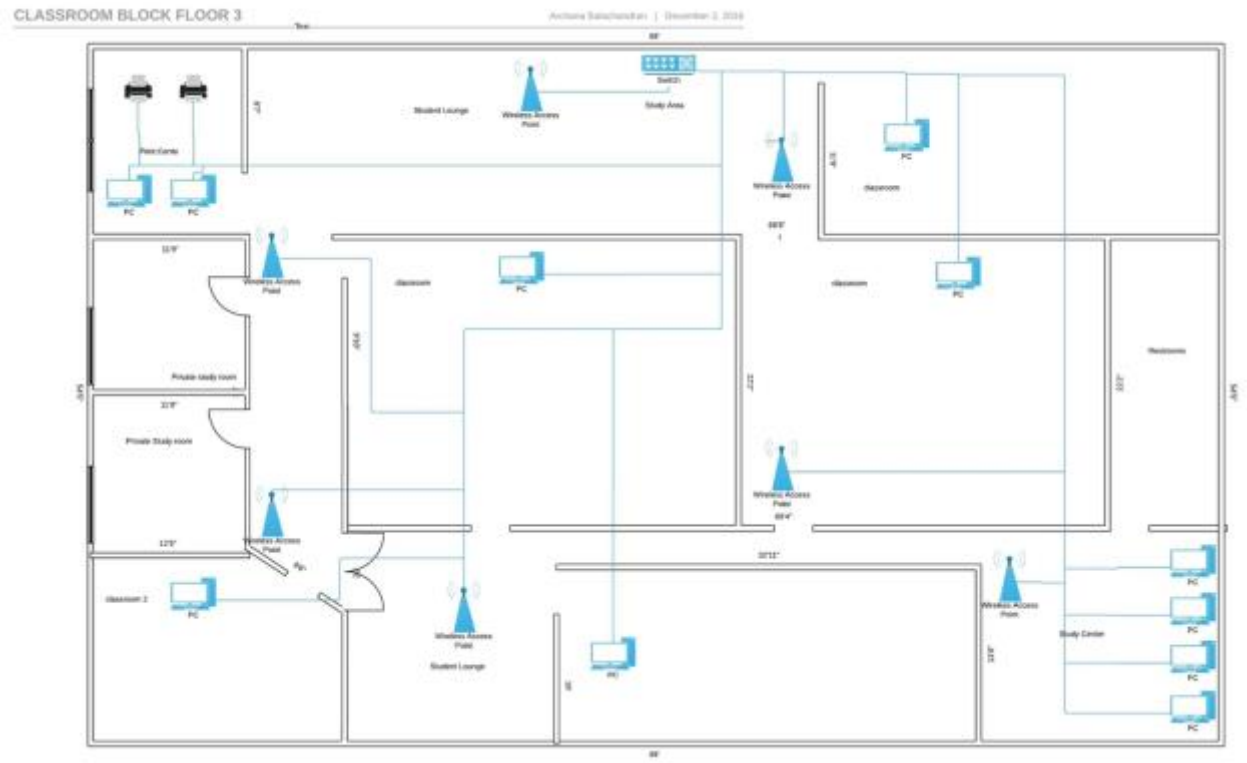
LAN design for Administration Block-floor 2



LAN design for Classroom Block Floor 1



LAN design for Classroom Block Floor 3



Description of LAN Design:

The LAN design uses Ethernet cables, gigabit Ethernet switches, NIC installed on nodes in the network, WAPs to provide an infrastructure for data transfer. In order to preserve bandwidth and reduce broadcast, a maximum of 50 workstations are included in one network. Since the network will have internet access, we will also need to consider firewall or packet filtering to prevent unauthorized access. Ports and preserved in the switches to accommodate future expansions. Each LAN design allows scalability, reliability and can also be implemented cost effectively, which is aligned with the network goals and requirements of the organization.

Technology Used:

Since the Administration building has very limited wired connections (24 desktops on the first floor,25 desktops on second floor, approx. 5 WAP on each floor and 3 other devices such as printer), we can use one 1000 Base-T Ethernet switch with 48 ports over category 5e wiring on each floor. The wiring for 1000 Base-T Ethernet has a 100 meter limitation, which is not a problem in our case (The wires shown in the diagrams are gathered along the walls, and bundled around the switch before connection). The media selected consists of 4 twisted pairs

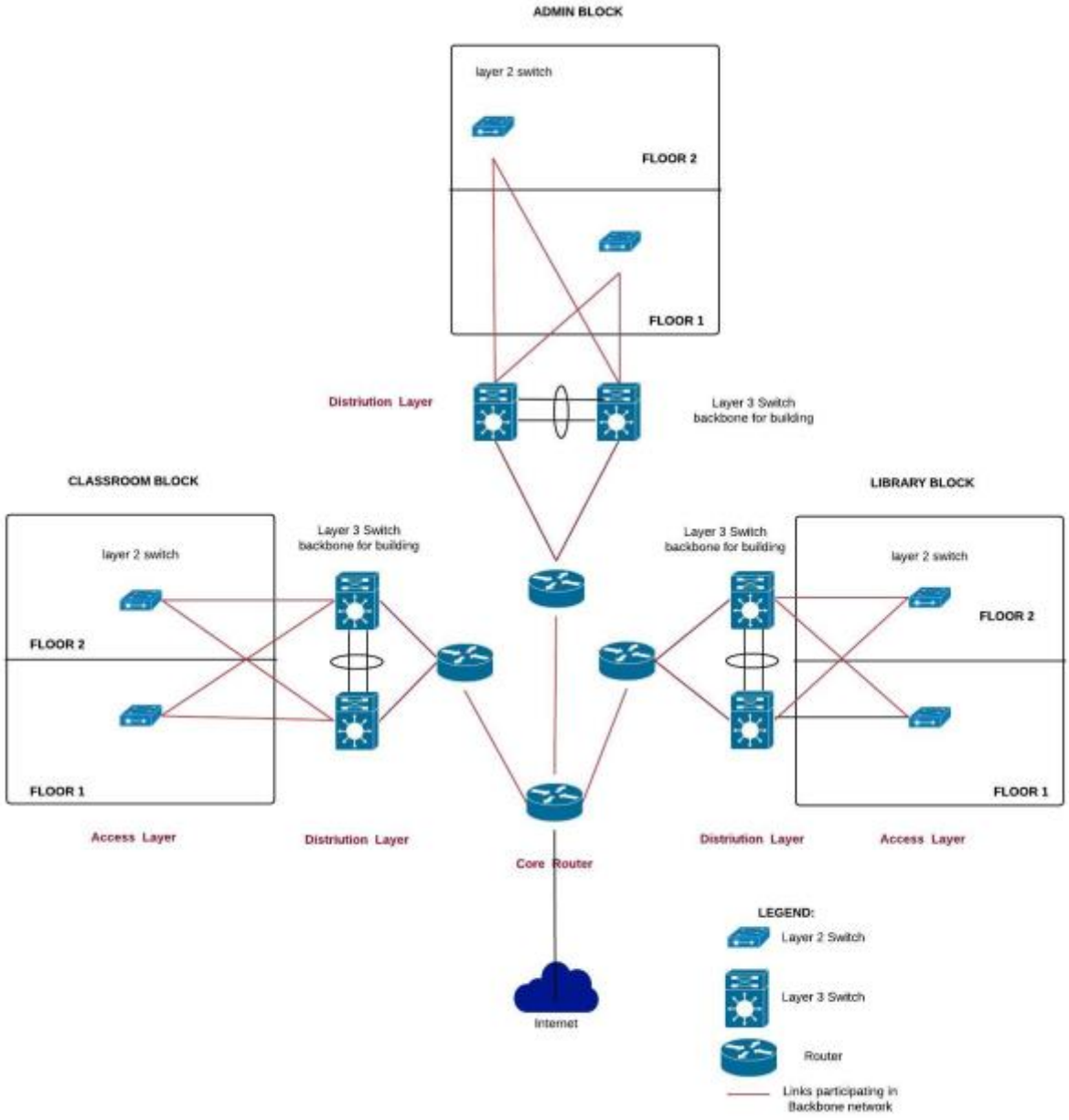
of copper wire, that is terminated by RJ45 connectors and supports a data rate of 1000 Mbps. Cat 5e cables are used to allow flexibility for using 100Base-T or 1000 Base T, in case there arises a situation to reduce bandwidth for certain networks on the campus.

This can be implemented with low cost and has high speed. We are not using a 24-port switch because it would not allow us to scale easily in the event of a future expansion. We will also need additional ports to connect multiple WAP. This floor also contains a 1 GbE Router and a 1 GbE central switch used in the backbone network (not shown in figure). The workstations in the Transceivers (which are used to connect nodes to Ethernet media) such as NIC are installed on computers. Gigabit Ethernet NICs that are 10/100/1000 capable are selected for the organization. Tree topology is used to form the LAN. The same configuration and technology is implemented in the Classroom block as well with slight modifications in technology used. Since this building has a much higher student population, thereby increasing the network traffic, to accommodate this demand, more access points are included in locations with anticipated high traffic such as classrooms, student lounges and study areas, etc.

For high speed, high volume data transfers (between the backbone devices, which is explored later), 10GbE fiber is used. Switches between each floor is connected by a fiber optic cable.

For Wireless Ethernet, 802.11n standard is used. For WAP, we are using Cisco 351 Access points due to its low cost. In the Admin Block, since the number of wireless users are comparatively less, we will use 5 access points. However, in the classroom block, due to large volume of traffic and users, we will need at least 8 access points on each floor. It allows a cost-effective 802.11n connectivity and also comes with a 5 10/100/1000 Ethernet Ports. This is also compatible with our selected Cat 5e cabling. In the Administration Block's video conference room, an exclusive WAP is included to reduce network interference.

Area 4: Local Backbone Network Design



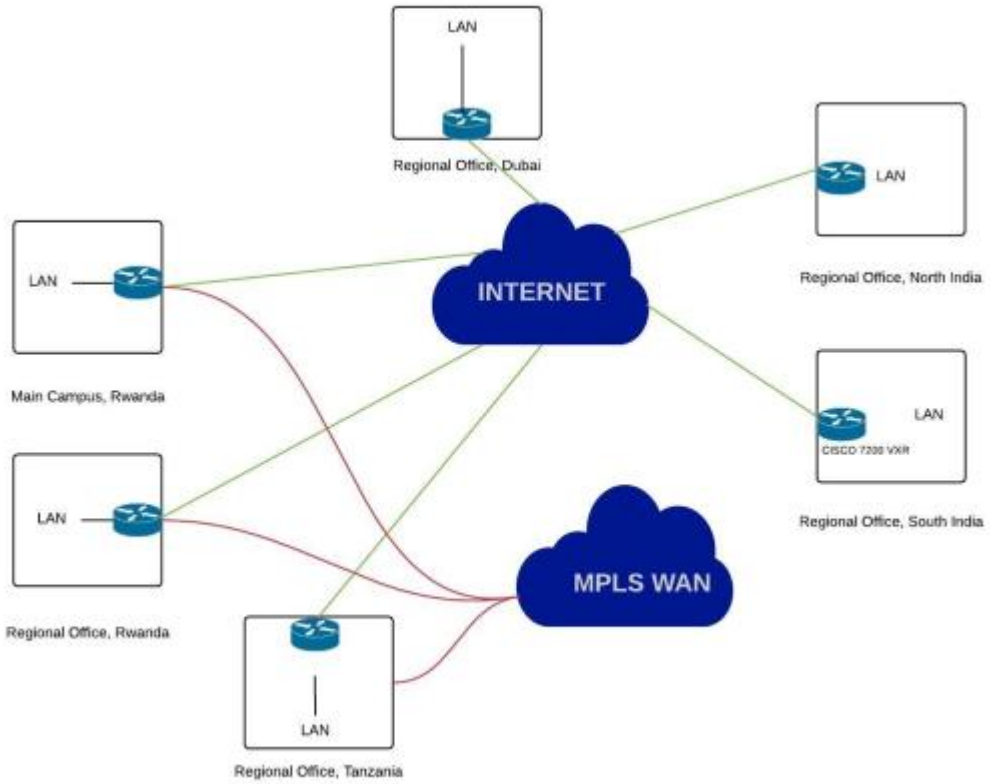
Description and Technology:

The building is connected to the campus backbone using fiber optic cables. Hierarchical design model is utilized in the design, where network devices are divided into discrete layers, each with a specific purpose. This makes the design modular, thus making maintenance and repair easier. A hybrid of switched backbone and routed backbone architectures are used. On each

floor, there is a 1000 Base-T layer 2 Ethernet switch connecting all client nodes, thereby forming the switched backbone and therefore, the Access Layer. Cat 5e cables are used to allow flexibility for using 100Base-T or 1000 Base T, in case there arises a situation to reduce bandwidth for certain networks on the campus. Connecting all the layer 2 switches on each floor are two Layer 3 switches that forms the switched backbone for the entire building, and which are typically stored in the basement for convenience. These layer 3 switches have a failover link for backup and recovery in the event of network failures. The redundant layer 3 switches provide good reliability, since the failure of either one switch does not affect the operation of the backbone. This forms the Distribution Layer. This building backbone is usually a higher speed network running over 1 GbE fiber optic cable. The layer 3 switches, is connected to high-speed, 1GbE router that leads to the campus backbone. Therefore, the building backbone(in distribution layer) is a switched backbone architecture, and the campus backbone is a routed backbone architecture(core layer).

The switched backbone in distribution layer reduces cost. Distribution layer connects to access layer via 1000 Base T switches running on Cat5e cables. The core layer uses routers running 10 GbE over optical fibers.

Area 4-1 WAN Backbone Design



The primary goal of the WAN design is to provide common resource access experience to all users regardless of location. Factors considered are data rates, cost, reliability.

The business activity intense locations (Main Campus and Regional Offices in Rwanda and Tanzania) are connected via an MPLS WAN as well as over the internet. In order to provide greater capacity and flexibility, the main campus and regional offices in Tanzania and Kigali are connected to each other in a full mesh using OC-3 circuits. Common carrier's network using SONET or Ethernet is selected.

The MPLS is used to improve the QoS and movement of packets through the TCP/IP networks. Label Switching Routers(LSRs) are used for MPLS. Network manager has to define a series of Forwarding Equivalence Classes(FEC) through the networks of LSRs, and each FEC has a reserved data rate and its own QoS. MPLS easily accommodates layer 2 protocols, and has better traffic management since the network manager defines FEC based on IP address and source or destination port. MPLS is primarily used for data transfer between these locations, in order to efficiently operate the organization's various cloud based applications (Office365, AWS for web sites management, CRM, and other management ERPs) because there is better traffic control, and higher availability of dedicated bandwidth. The other locations are connected to the to each other via the internet over fiber cables.

Area 5 Network Security and Management

Network Security:

Two Important assets that are part of the network:

1. The university's research LAN file servers
2. The Employee database

The university's research lab's **LAN file servers** contains highly sensitive information of public interest, which can be illegally retrieved from the database and replicated outside the university. The network in the research lab is designed in a 3-tier architecture fashion in order to improve security. In addition to this, the LAN architecture is in such a way that the switches segment the network. However, if the hacker can hack into the network device, they can easily cause a security breach.

The hacker may be someone who is from a different university, trying to reveal the research documents to sell them to third party institutions or independent researchers.

If the attack is successful, and if the intent of the hacker is what is was stated above, then the research findings will be published under another institution or individual, and the university will lose its credit and it affects the university's overall rank for research in the country.

Solutions to mitigate the threats against this includes:

Implement additional layers within network architecture at each layer (data, application, etc), keeping in mind that this addition is also manageable from operations viewpoint.

Segmentation of information based on the sensitivity of information also makes it difficult for a hacker to penetrate. Make the access very restricted for high sensitive information.

The names, uses and locations of the network components should not be publicly available. Restrict the access to this information only for authorized network personnel in the organization.

Policies such as Account access request policy, information sensitivity policy, remote access policies, Router and Switch security policy may be used.

The Employee database contains the Social Security Numbers and Credit card information of all employees. This database may be attacked by anyone who is interested in obtaining the credit card information for personal gains. One common way the database can be attacked is by obtaining the database password from someone in the organization who may have access to it,

by means such as phishing emails. The success of such attacks lead to excessive monetary loss of employees and also the loss of credibility of the IT infrastructure in the organization.

Security solutions that mitigates or eliminates the threats against the assets include:

Provide employees with education and training on how to avoid phishing attempts.
Implement Document Retention polices, password policy, information sensitivity policy etc.
Encourage database users to create hard-to-crack passwords.

Network Management:

Common Network Issues:

1.Cable Problem: When cables are cut and lose their transmission capabilities. Network Infrastructure management policies should be in place where network engineers are given a timeline to identify and fix the issue.
2. Connectivity Problem: A connectivity problem with one or more devices in a network can occur after a change is made in configuration or by a malfunction of a connectivity component, such as hub, a router or a Switch. Connectivity policies should state that the network managers should monitor network devices and trace any irregularities and made appropriate fixes.
3. Excessive Network Collisions: which leads to slow connectivity. This happens due to poor network set up, or if a user transfers a lot of information on the network or the network card is damaged and is in transmit mode. This can be handled by proper Capacity management policies where the network manager constantly monitors the traffic levels on the network devices.
4, Software Problem: Software configuration(such as DNS configuration) leads to network problems. Network Software engineers should be included in the policy which requires them to identify and fix the issue.
5. Duplicate IP Addressing: A common problem in many networking environments occurs when two machines try to use the same IP address. This can result in intermittent communications.

Personnel to maintain and manage the network:

The main campus requires:
Network Manager
Telecom Manager
LAN Administrator
WAN Administrator
Network Designer (for initial phases)
Network Technician
Technical Support staff

All other Regional offices only requires Network Manager, Network Designer(initial phase), network technician and technical support staff.

Managed Devices:

1. Managed switch is capable of detecting faulty transmissions from a malfunctioning network card and it also disables incoming circuit to prevent receipt of more messages and finally alerts the network manager via an alarm. This simplifies network hardware management.
2. Managed Router provides maintenance, continuous monitoring, and fault management, and also help reduce capital expenditure and alleviate IT staff's burden of day-to-day system management. If a router is receiving an overwhelming traffic, the network manager is alerted.
3. Managed Hubs: Hubs, along with routers are ideal places to gather information since all traffic must pass through both devices. This device also simplifies network hardware management by alerting the nwtrok manager in case of irregular traffic flow.

References:

http://www.smallbusinesscomputing.com/ProductReviews/Networking/networking-a-small-business-office-from-scratch.html
http://www.ciscopress.com/articles/article.asp?p=2189637&seqNum=4
http://www.conceptdraw.com/diagram/campus-network-design-project-pdf
http://what-when-how.com/data-communications-and-networking/backbone-network-architectures-data-communications-and-networking-part-1/
http://www.mcmcse.com/cisco/guides/hierarchical_model.shtml
http://docwiki.cisco.com/wiki/Internetwork_Design_Guide_--_Designing_Switched_LAN_Internetworks
http://smallbusiness.chron.com/five-things-considered-designing-network-35911.html
http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Oct2016/CVD-IWANDesign-2016OCT.pdf
http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Oct2016/CVD-IWANDesign-2016OCT.pdf
https://www.youtube.com/watch?v=6Ny7kKtbPEE
http://www.jidaw.com/itsolutions2.html