Wolkite University

We Strive for Wisdom!

College of computing and informatics

Department of information technology

Title: ENHANCED NETWORK DESIGN FOR WOLKITE UNIVERSITY DISTRICT AREA

By

IT fourth year students

Group Member	Id-No
1.Andualem Yenew	CIR /169/10
2.Robel Yenew	CIR /219/10
3.Natnael Alemayehu	CIR/240/09

Adviser Name: Mr. Korabza Shewarega(MSc.)

Submitted to IT Department

Submission date 14/07/2013

Wolkite University, Wolkite , Ethiopia

Contents

1 Introduction of the Project Work 5

1.1 Introduction 5

1.1.1 Background of the Organization 5

1.2 Statement of the problem 6

1.3 Objective of the project 7

1.3.1 General objective 7

1.3.2 Specific objective 7

1.4 Functional Requirement and Non-functional requirement 8

1.4.1 Functional Requirement 8

1.4.2 Non-functional requirement 8

1.5 Feasibility Study 9

1.5.1 Economic feasibility 9

1.5.2 Operational feasibility 10

1.5.3 Technical Feasibility 10

1.5.4 Political Feasibility 10

1.5.5 Schedule Feasibility ..... **Error! Bookmark not defined.**

1.6 The scope of the project 10

1.6.1 Limitations of the Project 11

1.7 Significance of the project 11

1.7.1 The beneficiary of the project 12

1.8 Methodology 12

1.8.1 Project Design Approach 12

1.8.2 Network Design Phase (PPDIOO) 14

1.9 Requirements/Data Gathering Instruments 15

1.9.1 Observation 15

1.9.2 Questionnaire 15

1.9.3 Interview 15

1.10 Project development tools 15

1.11 Team Composition ..... **Error! Bookmark not defined.**

List of Table

Table 1 cost break down analysis ..... **Error! Bookmark not defined.**
Table 2 Team Composition..... **Error! Bookmark not defined.**

WKU ……Wolkite University

ICT……..Information Communication Technology

WAN…….Wide Area Network

ACL……Access Control List

SSH……Source Socket Shale

VLAN……Virtual Local Area Network

IP……..Internet Protocol

DHCP……Dynamic Host Control Protocol

SAN……..Storage Area Network

DNZ……..Demilitarized Zone

VOIP……Voice Over Internet Protocol

VPN……..Virtual Private Network

SIMS……Student Information Management System

WLAN……..Wireless Local Area Network

ASCII……American Standard Code for Information Interchange

OSI……..Open System Interconnection

WWW……World Wide Web

PC……Personal Computer

DNS……..Domain Name System

FTP……..File Transfer Protocol

MTBF……Mean Time Between Failures

MTTF……..Mean Time To Failures

DSL ……Digital Subscriber Line

IPsec……Internet Protocol Security

NAT……Network Address Translation

PAT……..Port Address Translation

EIGRP

RIPv1…….. ……Request Information Protocol Version 2

RIPv2……..Request Information Protocol Version 1

OSPF……..Open Shortest First

CIDR……Classless Inter Domain Routing

STP……Spanning Tree Protocol

VTP…….VLAN Trunk Protocol

WPA……..WI-FI Protected Access

RJ 45……Register Jack

ARP……..Address Resolution Protocol

RADIUS……..Remote Authentication Dial-In-User Service

1 Introduction of the Project Work

1.1 Introduction

ICT refers to the communication and sharing of information and other relatively scarce (or expensive) resources. For instance, computers in a given work environment are connected to facilitate fast, accurate and timely information exchange. It also makes all resources, programs, equipment, files sharable and available to every connected computer. This takes us to the issue of designing network, which refers to a group of computers interconnected with some communication technology ether LAN, WAN ,WIFI or enterprise network .to do this Wolkite University has its own existed Local area network which is a communications network of terminals, hosts, and other devices that are located within Wolkite University for the purpose of provide service to campus community and this Network is installed from the data center (ICT) which exists in the Campus. This Local area network is installed by using different transmission medium like fiber optics cable to transfer the network from the data center (ICT) to the distribution switch. There is core switch in ICT Data Center and there are four distribution switch to provide the above idea to the campus community. Even though if there is a network in wolkite university there is some problems which needs new design for example availability, performance, security, scalability, manageability network design are main problems that needs redesign and the other is network equipment to solve these problems we make redundant link in core switch and distributed switch for availability and performance purpose and also use new security device technologies like access control list (ACL) , firewall, SSH, VLAN to solve the security problem. We use reserved DHCP(dynamic host control protocol) and reserved ports to expand the network for future use and we use the enhanced (new)devices like new router, switch, cables and so on to resolve the network equipment problems The data center (ICT) infrastructure is central to the information technology infrastructure, from which all content is sourced or passes through. Proper planning of the data center infrastructure design is critical, and performance, resiliency and scalability need to be carefully considered. Another important aspect of data center and local area network design is flexibility in quickly deploying and supporting new services. Designing a flexible architecture that has the ability to support new applications in a short time frame can result in a significant competitive advantage. Such a design requires solid initial planning and thoughtful consideration in the areas of port density, access layer uplink bandwidth, true server capacity and over subscription to name just a few. The layered approach is the basic foundation of the data center and local area network design that seeks to improve scalability, performance flexibility, resiliency, and maintenance.

1.1.1 Background of the Organization

Wolkite University (WKU) is one of the third generation higher institutions that have been founded in 2012.

It is established for the purpose of providing and promoting higher education learning, research, and outreach programs in the country to ensure the realization of the national vision of reaching the level of middle income countries by 2020.

The University is located in the Southern Nation Nationalities Regional State, in Guraghe zone, 158 km southwest of the capital city, Addis Ababa, on the way to Jima.

In November 2009 the late prime minister, his Excellency Mr. Meles Zenawi, laid the foundation stone of the University in a plain landscape which is quite ideal for academic pursuit. It is situated at Gubreye sub-city, 14 km away from Wolkite town, of the Gubrye-Butajira road.

The major link road to the University is a direct route to Wolkite-Jimma, Wolkite-Hossana and Wolkite - Butajira.

1.1.1.1 *Business Goals*

The main business goals of the wku are to perform the following LAN network:-

- **Scalable network**: wolkite university network designs can grow to include new user groups and remote sites like hospital network and the cluster campus network and can support new applications without impacting the level of service delivered to existing users so we proposed this design by set reserved IP address for future use in each subnet VLAN and by designing hierarchical network by set reserve modules and ports.
- **Available network**: a network designed for availability is one that delivers consistent, reliable performance, 24 hours a day, 7 days a week or 24 per 7. In addition, the failure of a single link or piece of equipment should not significantly impact network performance. We proposed this design by redundant link between core, distribution and access switch and by adding additional network equipment.
- **Secure network**: Security is a primary task when we stand to design the WKU network, not added on after the network is complete. Planning the location of security devices, filters, and firewall features is critical to safeguarding network resources within the WKU.We are proposed this design by configuring VLAN, ACL (access control list), SSH (secure socket shale), telnet, firewall etc.
- **Manageable network**. The proposed design for WKU network must be easily manageable by network administrator because we use hierarchical network design in order to make it easy to manageable.

1.2 Statement of the problem

In fact, Wolkite university local area network and data center (ICT) is one of the most crucial as well as backbone of the campus community by providing services but wolkite university local area network and ICT have some problems.

Generally, the current network design is expressed in terms of Network equipment, Network service, Network access, Network design and network security.

Network equipment: - wolkite university local area network has not enough network devices (router, server, switch and Access point) to provide the service to wolkite university community and also the network have no enough distribution switches to provide service to access layer there is no enough access point or wireless device for wife access.

Network service: - wolkite university local area network can't provide enough service to campus community such as IP telephony service,Demilitarized zone (DMZ) service: In cause of this service unavailability students cannot see their grade by access student information system and also lecturer cannot submit student's grade on the home and in any place,Enough internet access (service): for downloading purpose due to lack of network performance it may also cause by lack of redundant link and high traffic load.

Network access and availability: - Wolkite university network is not available all the time and places due to failure of device, power fluctuation and link, the network cover small area and the limited speed of the network the Campus community cannot access the service. In fact, wolkite university have network availability problem because of this the campus community cannot access the service.

there is no network related services like video conferencing in the college due to the lack of network performance , network equipment and also slow retrieval of data and difficult to get aggregate information and report generation due to the absence of redundant link. This makes the device have high response time (delay) so it leads to the above problem.

There is also no resource sharing between the staff like printer, copy machine because the existed network design is not considered to do resource sharing between the staff.

Therefore, we Design, implement and simulate enhanced network for wolkite university in order to optimize the Wolkite University existing or the current problem.

1.3 Objective of the project

1.3.1 General objective

The main objective of this project is to Design, implement and simulate enhanced network for Wolkite University and integrate with branches.

1.3.2 Specific objective

The specific objective of this project can be summarizing as follows:

- ✓ To Examine or study the existing network design and identify the major problems.
- ✓ To analysis and identify network protocols, standards and services requirement.
- ✓ To redesign and implement wired, wireless network.

- ✓ To provide safe and secure service for campus community.
- ✓ To provide the availability of the network.
- ✓ To support students by accessing any resource over the network.
- ✓ To design redundant link between device
- ✓ To test and optimize the network
- ✓ Document network design.

1.4 Functional Requirement and Non-functional requirement

The developed project is expected to provide the following functionalities:

1.4.1 Functional Requirement

The following Functional requirements are necessary to accomplish the objectives of the project:-

- ✓ The project should allow information and resources (printer, scanner, copy machine, etc.) sharing between staff in the college.
- ✓ The project should provide internet access on the campus that use for the Students and the staff.
- ✓ The project should Provides enough wireless and wired network connections in the campus.
- ✓ The project provide difference service such as connect user to internet, data sharing among user, accessing different web service for different functionalities.
- ✓ The project should allow to File sharing between the colleges and branches.
- ✓ The project should allow to Email service for campus community.
- ✓ The project should allow to SAN service for campus community.
- ✓ To provide VPN (virtual private network) service that is used to communicate with branches.
- ✓ To provide VOIP to the campus community.

1.4.2 Non-functional requirement

There are also non-functional requirements expected from the project and the following lists these requirements and those functional requirements are achieved by using a Top-down Network design approach, the hierarchical network design model and router, switch and Firewall configurations.

- **Security** Security is all about confidentiality, integrity, availability, and non-repudiation. The system should ensure that the network provided by subscribers and other system information is not disclosed to unauthorized processes or sites. The

system should maintain the correctness and consistency of the network it provides by configuring different security mechanisms on the firewall, switch, and router.

- **Performance** Since we use current new technologies, Hardware Devices, and Advanced Configuration mechanisms. So, this gives a high rate of performance for the network it provides.
- **Scalability** The network should scale gracefully. Scalability is a desirable property of a system or a network, which indicates its ability to either handle growing amounts of work easily. The system can maintain its availability, reliability, and performance as the amount of traffic load increases. This means it should be able to handle more subscribers and increased traffic load by designing a flexible and expandable network.

1.5 Feasibility Study

Feasibility analysis enables the system to determine either or not the project can be developed, evaluates and identifies the newly developed system. Therefore, the feasibility analysis of the proposed system involves the following feasibility:

1.5.1 Economic feasibility

The cost that we are spending while developing network infrastructure is less than the benefit. Economically this project uses much more quality network equipment with fair cost for the university.

This proposed design is economically feasible it Determine the finance, how much take cost till the whole project ended. The project, we are going to design is economically feasible than the existing network design. But there is tradeoff i.e to make it economically feasible we loss some business goals like availability, performance, scalability and others because the need additional cable, equipment, and bandwidth. When the team can be analyses the design by comparing the cost with the benefit (the enterprise can get by using the new design), surely the benefit out weight the cost. The cost of redesigning the network, including software and hardware cost for the class of application being considered should be evaluated. As part of this, the costs and benefits associated with the proposed design compared and this study classifies the cost of the project as tangible and intangible benefits.

Tangible benefits are:

Tangible cost means quantifiable cost related to an identifiable source or asset. It can be directly connected to a material item such as a network devices used to conduct operations on this project

- ✓ Using less manpower than the existing system.
- ✓ Increase the speed of activities and competitions.

- ✓ Reduce cost.

Intangible benefits are:

Intangible cost means a quantifiable cost related to maintaining or troubleshooting in the time of failure of the network is happen.

- ✓ Minimizing data redundancy.
- ✓ Better service to the student and staff members.

1.5.2 Operational feasibility

The proposed design will solve the business and time problem for the organization. Therefore the college admin staff, Academic Staff, Students, and other users can get effective and efficient service from the network, which satisfies their needs.

The proposed network:

- ➢ It offers a greater level of user satisfaction.
- ➢ Produces the best results and gives high performance.
- ➢ It can be implemented and operate easily.
- ➢ It can be solved the existing system problem and challenge.

1.5.3 Technical Feasibility

The new network design of this project is technically feasible because of harmonious communication of the device and IOS (internetwork operating system) of the device which mean that the LAN operate functionally without any problem or without any down of system by using better interaction of the user and the network.

It is a very effective tool for long term planning and troubleshooting. The technical feasibility study should most essentially support the financial information of an organization.

1.5.4 Political Feasibility

Our new network design for wku is not related to political issue. When we design proposed local area network for Wolkite University there is no any political policy unacceptability during when we done these project it is far from any crime or illegal issue so our project is acceptable by political policy. Our project is no affected by any political policy issue. Generally our project is hundred percent politically feasible from any political policy issue.

1.6 The scope of the project

The coverage area of the new local area network and datacenter design for Wolkite University and this enhanced network design will cover the whole campus area in better of the existing network.

When we design this local area network we consider the following concept

- **Wired network design and implement**:- In terms of this concept which means that the wired network the design will cover specifically at Dormitory in both female & male, Library,Academic offices**,** student cafeteria, whole colleges, student laboratory through wired cable. which means that by using wired local area network we will cover those areas listed above
- **Wireless(WI-FI) network design and implement**:- The new local area network design also use WLAN(wireless local area network) the coverage area of the network in campus via WLAN is whole area of campus at Dormitory in male or female, Library, Academic offices, student cafeteria ,in whole colleges lecturer and student launch through wireless.
- Distribute the network across the college and branches.
- Security configuration with different security technologies.
- Provide File sharing between branches.
- Provide printer sharing between branches.
- provide Email service for campus community and branches
- Connecting remote branches with VPN (virtual private network).

1.6.1 Limitations of the Project

The project that we design has the following limitation:

- There are no automation projects or systems.
- Our system does not include the physical installation of the network, the configuration of the network is done on the simulation, not on real devices.

1.7 Significance of the project

The significance of this project basically are connects the computer hardware in a localized area network such as an office, student laboratory, Dorm, guests by means of wired or wirelessly. Typically, LANs use wired connections to link the computers to each other and to a variety of peripheral devices such as printers and to communicate, to share file, information and peripheral devices between the sender and receiver basically in our campus environment. And also gained different service that provided by the designed datacenter.

The other Significance of this Project is listed as follows

- Fast data exchange and information communication,
- Reduction on the cost by sharing resources such as internet, printers, scanners
- Timely access to relevant and comprehensive information for decision-makers
- Better service and accuracy of the network that gives for the users;

- Improved communication environment,
- Facilitate the sharing of resources between institutions;
- Better information retrieval.
- Reduction in paperwork
- Ensure the organized provision of ICT training to students, teachers, and educational administrators.
- Lower operation cost.
- Reduced wastage of time.

1.7.1 The beneficiary of the project

Some users can directly or indirectly be benefited from this project some of them are

- ✓ Students: Allow college students to use internet access for reference, research, and project work.
- ✓ ICT staff: The new designs provide ICT staff easy to manage and maintain when it is failure.
- ✓ Instructors: get benefit from new design network to submit students grade to SIMS and also they can download tutorials related to these courses in their office
- ✓ Administrator staff: in the previous design there is a loss of materials like time, paper, a pen which is cost and more manpower, since there is no file and resource sharing but now the new design reduces the loss of costly materials and manpower. It has great importance for all offices to facilitate their job effectively and efficiently
- ✓ Guests also get network access by easily connect wirelessly when they enter into the campus.

1.8 Methodology

Network Methodology is a process, a set of steps to follow in network design and define the methods of how collect the data. Starting from now to precede our document we use the following methodologies to get the data.

During the data collection, this study investigated the Wolkite University ICT data center, local area network and different users in the campus for collecting the actual data by different methods such as observations, questionnaires and interview.

1.8.1 Project Design Approach

After establishing the organizational requirements and documenting the existing network, we ready to select **top- down approach design.**

Designing a large or even medium-sized network can be a complex project. Procedures have been developed to facilitate the design process by dividing it into smaller, more manageable steps. Identifying the separate steps or tasks ensures a smooth process and reduces potential risks. A top-down design allows we are to "see the big picture" before getting to the details. Top- down design clarifies the design goals and initiates the design from the perspective of the required applications. The top-down approach adapts the physical infrastructure to the needs of the applications. Network devices are chosen only after a thorough requirements analysis. Structured design practices should be integrated with the top-down approach, especially in very complex networks. In contrast to top-down design, the network design approach in which network devices and technologies are selected first is called bottom-up, or connect-the-dots. This approach often results in an inappropriate network for the required services and is primarily used when a very quick response to the design request is needed. With a bottom-up approach, the risk of having to redesign the network is high.

Guidelines for us producing a top-down design include the following:

■ thoroughly analyze the customer's requirements.

■ Initiate the design from the top of the OSI model. In other words, define the upper OSI layers (application, presentation, and session) first, and then define the lower OSI layers (transport, network, data link, and physical)—the infrastructure (routers, switches, and media) that is required.

■ Gather additional data about the network (protocol behavior, scalability requirements, additional requirements from the customer, and so forth) that might influence the logical and physical design. Adapt the design to the new data, as required.

Top-Down Approach Compared to Bottom-Up Approach

A top-down approach to design has many benefits compared to a bottom-up approach, including the following:

Incorporating the customer organization's requirements

■ providing the customer and the designer with the "big picture" of the desired network

■ providing a design that is appropriate for both current requirements and future development.

The disadvantage of the top-down approach is that it is more time-consuming than the bottom-up approach; it necessitates a requirement analysis so that the design can be adapted to the identified needs. A benefit of the bottom-up approach—selecting the devices and technologies and then moving toward services and applications—is that it allows a quick response to a design request. This design approach facilitates designs based on the designer's previous

experience. The major disadvantage of the bottom-up approach is that it can result in an inappropriate design, leading to costly redesign.

1.8.2 Network Design Phase (PPDIOO)

PPDIOO is one of the most commonly used network design phase in the top-down approach methodology

The following describes each PPDIOO phase:

- **Prepare phase:** The Prepare phase involves establishing the organizational (business) requirements, developing a network strategy, and proposing a high-level conceptual architecture, identifying technologies that can best support the architecture. Financial justification for the network strategy is established by assessing the business case for the proposed architecture.
- **Plan phase:** This phase involves identifying the network requirements, which are based on The goals for the network, where the network will be installed, A project plan helps manage the tasks, responsibilities, critical milestones, and resources required to implement the changes to the network. The project plan should align with the scope, cost, and resource parameters established in the original business requirements. The output of this phase is a set of network requirements.
- **Design phase:** The initial requirements determined in the Plan phase drive the network design specialists' activities. These specialists design the network according to those initial requirements, incorporating any additional data gathered during network analysis and network.
- **Implement phase:** Implementation and verification begins after the design has been approved. The network and any additional components are built according to the design specifications, with the goal of integrating devices without disrupting the existing network or creating points of vulnerability.
- **Operate phase:** Operation is the final test of the design's appropriateness. The Operate phase involves maintaining network health through day-to-day operations, which might include maintaining high availability and reducing expenses. The fault detection and correction and performance monitoring that occur in daily operations provide initial data for the network lifecycle's Optimize phase.
- **Optimize phase:** The Optimize phase is based on proactive network management, the goal of which is to identify and resolve issues before real problems arise and the organization is affected. Reactive fault detection and correction (troubleshooting) are

necessary when proactive management cannot predict and mitigate the failures.

1.9 Requirements/Data Gathering Instruments

1.9.1 Observation

Observation is one of our data collection methods and it is more accurate than the other methods because during observation we can observe everything available in our campus related with network by our eye. And also this method helps us to make the decision on our own way.

When we observing or seeing the designed data center and installed local area network exist in the Wolkite University we observed that the data center and the installed Local area network is giving service for the users and we observed that they used different network devices to design the data center and to install Local area networks such as layer3 switch, layer2 switch, Data cable, server etc.

1.9.2 Questionnaire

In this data collection method we can get different idea about the local area network and datacenter design we asked different open end and closed end questions to the datacenter administrator and the campus community such as .

Is there information and resource sharing between the staff?

Is there automation project or system is existing inside the college?

What types of service provided to user?

What are the constraints/ problems that are available in existing network?

1.9.3 Interview

In this data collection method we get some answer what we before asked about local area network and datacenter design by directly communicate with the person who works in network area and knows about networking.

We interpreted and analyzed their opinion and answer even during the interview what they want to say Also we interviewed the data center(ICT) administrator and the campuses community orally, and they answered Most of our question Based on the way we want.

1.10 Project development tools

- Cisco Packet Tracer: for simulation
- Microsoft Visio Setup: for design
- E-draw max

CHAPTER TWO

NETWORK NEEDS ANALYSIS

The goal of network need analysis is to understand why the network is being built and what users and applications it will support. In many cases, the network is being designed to improve poor performance or enable new applications to be used.

Designing network needs analysis in order to create new network or to upgrade existing network. So in this chapter we are going to define data types, next to this data sources, number of user are discussed. This chapter also includes storage, transmission speed, security and reliability requirement of existing and proposed network infrastructure, finally, the chapter discussed about load variation estimation and description of existing network infrastructure.

Data Types

The types of data served by the WKU network will be reports, bulletins, accounting information, personnel profiles, and web page, very frequent letters, purchase huge request data, student data, cafeteria data, hospital data (patient).

The majority of the data will be text (ASCII and non-ASCII), but there will be some still graphics and possibly a large amount of video conferencing and distance learning (primarily for PC-based teleconferencing).

The organization has the following data sources for the enterprise network in the organization vicinity:

- Detail WKU client's information (i.e. business requirements, term of agreements, contract letter and others).
- Human resource information of the WKU.
- Previous developed software to different organizations.
- Inventory information of the WKU.
- Materials that support software development (audio files, textbooks, web files, video files and other files: - The future automation systems web pages and databases).

Data Sources

Data will be created and used at all end stations on the network. The data will be produced by software applications in Windows 10, primarily and Office 10 Professional (Word, Excel, Access, PowerPoint, and Outlook). Other data sources to be supported on at least a limited

basis will Windows 10 Accessories (Paint, Notepad, etc.), NetMeeting, Media Player, and Photoshop.

Numbers of Users and Priority Levels

In the WKU, the users will be administrators (i.e. president, college dean, department head, coordinators, directors, team leaders, secretaries, teachers, students, and other workers.

The Priority is derived from the impact and the urgency of accessing information in the network, based on the context of an organization. The allocation of a priority code determines how the user is being taken care of by the tool, the support staff and access to different services in the WKU network. Therefore, the team can categorize users of the infrastructure into different groups based the rules and regulations of the organization and define their priority based on the organization structure, privilege level and resources in the organization.

Three priority levels will be supported: administrators (top priority), academic staff (medium priority) and students and other workers (low priority). Note that these designations do not correspond to administrative levels in the school; rather, they are network service levels (i.e. services delivered to the staff and students). Network management processes (packages in Simple Network Management Protocol) will receive top priority service; most network processes will receive medium-priority service; a few processes (e.g., e-mail transfers, backup, web access (WWW), FTP, etc.) will be given low-priority service. It should be noted that network management will usually consume a small amount of the available bandwidth; this means that management and user processes will usually enjoy identical support. Background processes will also usually receive more than adequate service, but they will be delayed as needed to maintain support for management and user services.

Transmission Speed Requirements

The network is to be transparent to the users. Thus, remotely executed applications, file transfers, and so forth should ideally appear to operate as quickly as processes executed within an end-station. Interviews with users to ascertain their needs and expectations indicate that an average throughput of 100mbps per user within each LAN and 55mbps per user between LANs will more than support the needed performance in most cases (teleconferencing being the possible exception).

The network infrastructure in the WKU (suppose the university has 12,000 students, 3000 both academic and administrative). The WKU could provide email, video and audio file accesses, web accesses, social network sites accesses, communication, application download, uploads, and accesses the WKU-specific system and other services.

After the end of the design network, the outcome is to provide applications like mail service, FTP, video conferencing, DNS, WEB, VOIP. We are intended to design and agreed with the WKU that the network will support the following application:

- FTP (for allowed traffic flow): the WKU allows giving service of file transfer securely with fast speed.
- Web server: that helps to deliver Web content that can be accessed through the Internet. By considering the number of staff and students of the university and services that are delivered to them, the capacity of the sole internet service provider in the country and budget of the university.

Load Variation Estimates

Load forecasting (estimation) plays a key role in helping the WKU to advance a network service and to make important decision on network users and its priority, load balancing, network reconfiguration, infrastructure development, purchasing and installing new hardware and software to enhance network service to its clients. In order to determine the network load, it is better to study long period i.e. to know the network access history, access the university ICT policy to know the current stand and to propose the future network (bandwidth) requirement of the university. So, we can define the network load (usage) variation in the university in different day and time interval.

- The data indicate that the highest average traffic volume will occur from 8:30 am to 5:00p.m, Monday to Friday (since it is normal work hour of the WKU).
- The network traffic reaches a peak volume at two time during the working day of the WKU: 8:30a.m to 10:00p.m and 2:30p.m to 5:00p.m

The data indicates the following network design parameters

- The average required throughput on any LAN during working hour (3:00a.m to 6:00p.m) will be only about 2Mbps.
- The average required throughput on any WAN during working hour (3:00a.m to 6:00p.m) will be only about 1Mbps.
- The peak expected traffic load on any LAN would be about 1Mbps

Storage Requirements

Storage requirement all knows determining the requirements or making best educated guesses when we cannot know for sure. Factor to consider include potential data storage requirements

of the future projects and tries of storage. Tiered is a way to assign different categories of data to various types of storage media with the objective of reducing the total cost of storage. Tired storage architecture places data in a hierarchy according to its business value. Considering the network infrastructure in each branch, the storage requirements need to be large enough to store all WKU community information, employee, and other required data (web access file, email and any backup). Memory technologies that we are going to use in proposed network are:

DDR4memory standard: provide up 50% increase performance and bandwidth while decrease the power consumption of your overall computing environment. It also provides cyclic redundancy checks (CRC) for improved data reliability.

Solid state drive (SSD): is high performance plug and play storage device that contains no moving parts. Because they contain their own CPUs to manage data storage, they are a lot faster than conventional rotating hard disk: therefore they produce highest possible I/0 rates.
Two tiered storage architecture is used in proposed network infrastructure in order to enhance performance of network service through using tiered architecture
And also we use A Storage Area Network (SAN) is a specialized, high-speed network that provides block-level network access to storage. Increase storage utilization and effectiveness (e.g., consolidate storage resources, provide tiered storage, etc.), and improve data protection and security.

Reliability requirements

Is the ability of a device or a system to perform its function without failure when increasing MTBF(mean time between failure) or decrease MTTF(mean time to failure):- it is possible to decrease this time through eliminating single point of failure, fast convergence time to enable and disable path link.
Reducing server in different location: - we can use storage replica to configure two servers sync data so that each has an identical copy the same value. Storage replica supports synchronous and asynchronous replication. Synchronous replication mirrors data within a low latency network site with crash consistent volumes to ensure zero data loss at the file system level during a failure.
Asynchronous replication mirrors data across sites beyond metropolitan ranges over network links with higher latencies, but without a guarantee that both sites have identical copies of the

data at the time of failure so synchronous replica is best to make as replication policy since low latency and no guarantee that sites have same copies of data to use this storage replica we use those technologies such as Windows Server 2019, Windows Server 2016, Windows Server.

Software can also play a major role in overall network availability at a higher level than with in individual devices. Cisco recently announced the globally resilient IP initiative to help ensure that software and design protocol deliver zero packet loss end to end across an entire network. Hot stand by router protocol (HSRP) and virtual router redundancy protocol (VRRP) are two other examples of cisco IOS software features that enhance reliability at the network level. These protocols enable a set of routers to work together to present the appearance of a single virtual router or gateway to a set of IP hosts. By sharing an IP address and media access control(MAC)address, two or more routers acting as a single virtual router are able to transparently continue the routing function in case of a router failure, a power failure, scheduled maintenance .The main purpose is for availability and performance, to decrease latency.

The minimum network requirement is needed to meet WKU communities need through considering affecting factors of reliability requirements.

- The LAN are expected to operate at 95% and the WAN is expected to operate at 90% uptime and an undiscovered error rate of 5% and 10% for LAN and WAN respectively
- The network could have replica server in WKU in addition to ICT to keep the university data server and reliance to any kind of catastrophes.
- Both LANs and WAN network could work properly in the organization working hours.

Security Requirements

Existing network has low security measure since there is no firewall between the organization network and external network(internet) and the other security problem is no VLAN and ports are not secure mean that anybody can connect to the network simply using laptop this should be protected. So, in our proposed network design we are going to address that security measure in order to increase network security. Some the security measure that will be used in the proposed network infrastructure:

Security measure can physical or logical, physical security for data center (ICT) there should be special room that unauthorized person could not enter as well as the place should be free

from any natural disaster other device router, cable, and switch are attached on the wall in order to secure core service from any kind of physical security challenges.

A firewall will be configuring at the branches to control threats from the outside world; therefore, the internal network is entirely secure from some unauthorized users (i.e. hackers and crackers). So, firewall will be either hardware or software but, in our case, we will use software or router with access control list to deny and permit user according to their privilege and to protect out network from external or unauthorized traffic.

Configure VLAN for different department in order to separate and secure network as well as decrease broadcast domain on each LAN. Give password and user name for network device router:-in order to access the router user will have asked to fill username and password so unauthorized use can be protected from accessing router.

Create: DMZ or demilitarized zone is physical or logical sub network that contain and exposes an organization external facing service such as internet.
Create VPN: virtual private network is a way to create secure connection between the remote computers and present the connection as if it were a local private network. This provides a way to configure service that run on WKU network as if they were on a private network and connection remote servers over secure connection.

Existing Network

Currently the WKU district includes Wolkite University, Wolkite University specialized Hospital and cluster campus branches. Wolkite University and WKU specialized Hospital uses from the only internet service provider Ethiotelecom through DSL of 600Mbps bandwidth since for Wolkite University 400Mbps for Wolkite University specialized Hospital 200Mbps. At recent time wolkite university consists 1 core router and 4 distribution switches of 48 port and Wolkite university specialized Hospital consists a 1 distribution switches of 48 port and it uses cat 5 unshielded twisted pair(UTP) as connecting cable. Cluster campus contains 1 router 2 switches and it uses a DSL technology to be connected with internet service provider with 150Mbps. existing network uses centralized cabling topology in each branch local area network (LAN) and cable type is cat 5.

The functions of this existing WKU network infrastructure are:

- ✓ For internet purpose
- ✓ For digital library
- ✓ For E-Learning purpose
- ✓ For mailing purpose
- ✓ For FTP purpose
- ✓ DNS purpose
- ✓ Student information management purpose

Why network design is required?

- ➢ To make the network more available than the existing by using redundant link and additional devices.
- ➢ To provide file and resource sharing between the main campus and the cluster campus.
- ➢ To share applications between the cluster campus and the main campus.
- ➢ To make the network more secure than the existing by configure software firewall and also hardware devices.
- ➢ To increase the performance of the existing network by using enhanced devices.

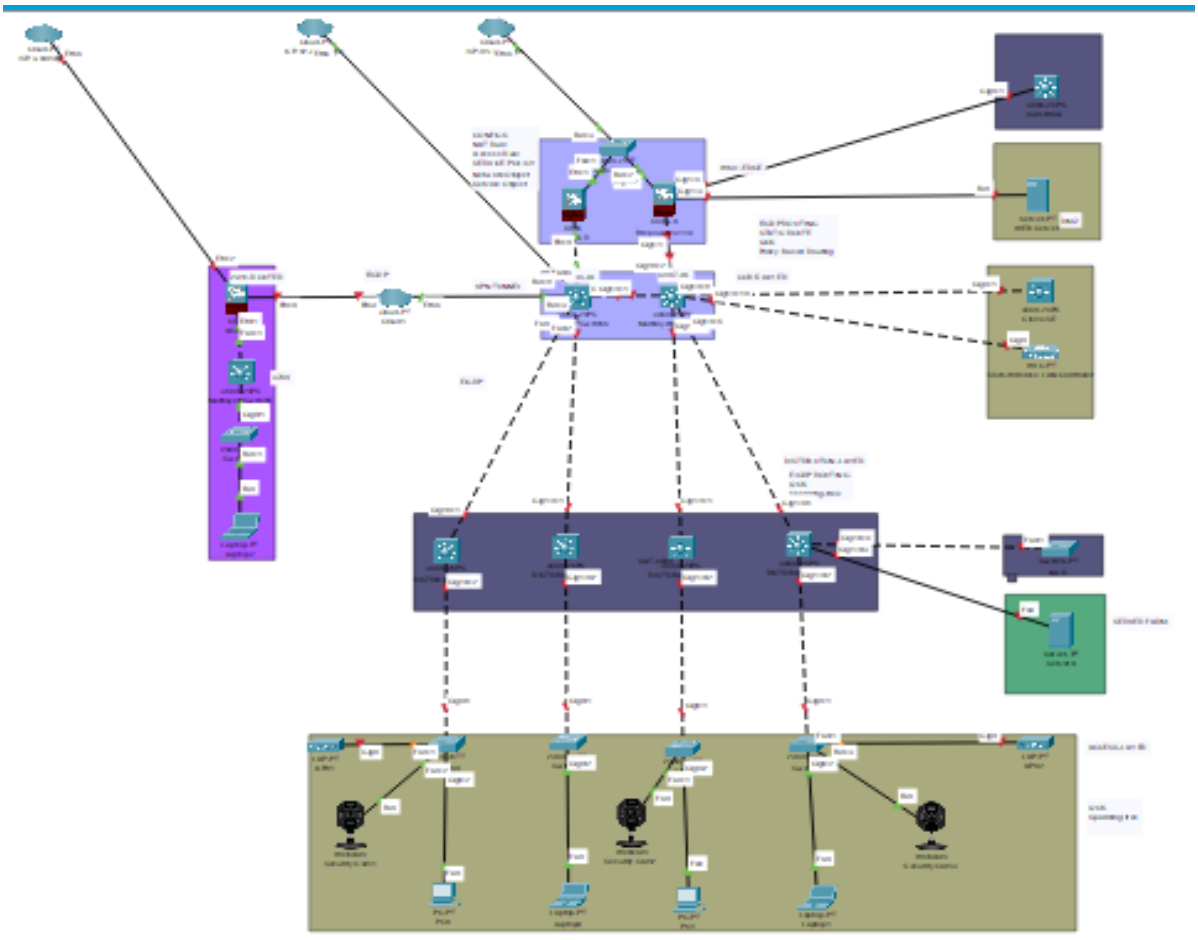


Figure 1 existing network design for WKU

CHAPTER THREE

Logical Network Design

Logical Network Topology

An internetwork's topology is a diagram that shows network segments, interconnection points, and user communities. The logical design process of the top down network design approach begins with the development of a network topology. We define logical subnet works and interconnection points, the size and complexity of networks, and the types of internetworking devices that will be needed during the topology design phase, but not the actual devices, during the topology design phase. We design the logical topology of the network before choosing devices and technologies in order to achieve the organization's goals in terms of scalability and adaptability. We use hierarchical network architecture to meet WKU's business and technological goals in the proposed network design. Each layer may be based on a single application, allowing us to select the appropriate systems and features for each layer. Another issue is how WKU's branches can interact with one another, given that each branch office is located in a different geographic area. Owing to the high cost of fiber optics cable, connecting various branches over a private wide area network will be difficult. To link branch offices, we suggest using virtual private network (VPN) technology from an internet service provider. VPN is currently the best option for safe communication between branches over an untrustworthy public network.

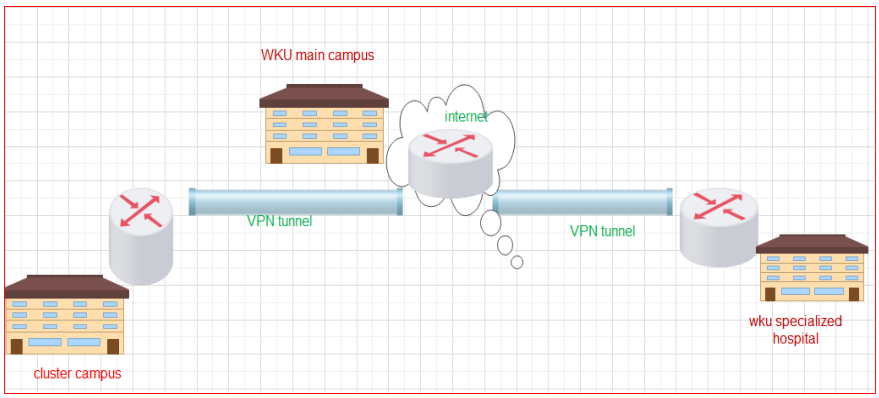
To link several branch office workers at the same time, all office locations must have access to the same network infrastructure. The most popular method is to use a centralized location to building the network's core resources, such as servers and databases, at the head office. Branch offices, on the other hand, do not need such infrastructure. Remote offices connect to the central office through a special VPN connection.

To communicate securely, WKU branches are linked to the the main campus through a public network or the internet through VPN technology. VPN allows organizations to create stable, end-to-end private network connections over service provider networks using advanced encryption and tunneling. When your users send a message, all data is encapsulated to protect

your sensitive information. When your users send and receive data. Tunneling is a method of encapsulating packets from one protocol within packets from another protocol. a logical point-to-point connection across a connectionless IP network, enabling! Application of advanced security features

the proposed design we are going to use Site-to-site VPNs are a relatively costly way for a business to link geographically scattered branch offices through a service provider in the proposed design. Among the available topologies, a site-to-site VPN is a more cost-effective and manageable solution. To build a site-to-site VPN, we use Hub and spoke topologies. When there is a single regional or headquarters with several remote offices, and the majority of traffic is between the remote sites and alters, a hub-and-spoke topology is used. By providing a single IPsec link from each remote location back to the headquarters location of the main campus at gubrye, this design reduces configuration complexity. As a result, the hub and spoke topology is appropriate for our proposed design because WKU has one central site, which is situated on the main campus, and some distant branches, such as the WKU specialized Hospital and cluster campus

Figure proposed network WAN topology for WKU



In our proposed enterprise network design, we use a VPN link with a hub and spoke topology, which follows the steps below:

Any source computer c1 from each branch wishes to send the packet PI to the computer C2's destination IP address. For example, the router at the cluster branch receives packet P1 and uses IPsec to encrypt the entire packet.

- After encrypting the packet, router at cluster campus encapsulates the whole packet to form a new packet NPI. This packet has IP address of router at cluster campus as

source IP and the IP address of the router R2 (the router placed at the WKU data center) as the destination IP.

- The router R1 then forwards the packet NPI to the IP address of R2 using the Internet.
- The destination router R2 receives the packet.
- The router R2 encapsulates the NPI to get the original packet Pl.
- The router R2 decrypts the packet Pl using the appropriate algorithm
- The router R2 then forwards the packet Pl to the destination computer C2, where the packet was actually supposed to reach.

WKU benefits from IPsec VPN site-to-site tunnels in a variety of ways. Some of them are: The need to purchase private dedicated costly Incase lines to link branches to the head office is completely eliminated because data is transmitted over public telecommunication lines. Both the participating networks' and nodes' internal IP addresses are shielded from each other and from external users. The entire communication between the source and destination sites remains encrypted which means that chances of information theft are extremely low. Hierarchical topology most of the time has three discrete layer for large organization. The primary goal of the collapsed core design is to reduce network infrastructure costs while retaining the majority of the advantages of the three-tier hierarchical model.

The hierarchical topology of our design consists of the following layer:-

A core layer of high-end routers and switches optimized for network availability and performance. We implement NAT and firewall at the core layer router in order to secure internal network from attack. To access the Internet, one public IP address is needed for the branches and private IP address can be used in our private network.

IP address can be assigned to internetworking devices using statically and dynamically for users. On the proposed design DHCP server is configured at core layer router to assign IP address dynamically and it provide additional information for hosts rather than IP address like address of default gate way and different server address. DHCP is a good way of assigning address. Since public IP addresses are allocated by service providers for a fee, each device has a high cost. So, to solve the problem of each device needing a public IP address, we'll configure NAT (network address translator) at the core layer, which is the process of mapping a group of IP addresses or a single IP address on the internet-facing interface to the local area network (LAN). Among available of NAT types that suit for our WKU is PAT types of NAT

because this NAT type maps many local (private) IP address to single public IP address. The reason why we have chosen this NAT type is effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

The other layer of the proposed design is an access layer which provides connection to the LAN via switches, or access point for Wi-Fi access. We separate different departments by grouping them in different subnet at layer 3. There are departments in each branch of WKU and there is also guest user, so we will configure VLAN for each department and for guests.

Designing Models for Addressing and Numbering

Assigning address number for the devices on the network should be in structured model means that addresses are meaningful, hierarchical, and should be planned in order to leave room for growth in address. In proposed design we are assigning address in hierarchical model because it facilitates hierarchical routing, permits the summarization (aggregation) of network numbers. A clearly documented structured model for addressing facilitates management and troubleshooting. Structure makes it easier to understand network maps, operate network management software. Block of an IP number is provided by internet service to WKU and each branch network needs one public IP in order to join an internet, so we subnet a given IP number to different logical sub networks for the department of each branches in order to conserve IP number. Structured model for network layer addressing and naming is very important because without structure, it is easy to run out of addresses, waste addresses, introduce duplicate addresses and names, and use addresses and names that are hard to manage. Network layer addresses should be planned, managed, and documented before assigning IP number for any device. To maximize flexibility and minimize configuration, we use dynamic addressing through DHCP for end systems. With dynamic addressing, a station can automatically learn the network segment to which it is currently attached, and adjust its network layer address accordingly. DHCP server provides additional information more than only IP address like, a subnet mask, a default gateway. Structured model for WKU is shown below on table.

Ip schema for wolkite main campus

VLAN	VLAN name	Host	Network id	Subnet mask	Broadcast id	Usable

NO		requirement				host
1	ENG1	250	10.194.0.0/24	255.255.255.0/24	10.194.0.255/24	254
2	ENG1	250	10.194.1.0/24	255.255.255.0/24	10.194.1.255/24	254
3	ENG1	250	10.194.2.0/24	255.255.255.0/24	10.194.2.255/24	254
4	ENG1	250	10.194.3.0/24	255.255.255.0/24	10.194.3.255/24	254
5	ENG1	250	10.194.4.0/24	255.255.255.0/24	10.194.4.255/24	254
6	ENG1	250	10.194.5.0/24	255.255.255.0/24	10.194.5.255/24	254
7	ENG1	250	10.194.6.0/24	255.255.255.0/24	10.194.6.255/24	254
8	ENG1	250	10.194.7.0/24	255.255.255.0/24	10.194.7.255/24	254
9	ENG WIFI	250	10.194.8.0/24	255.255.255.0/24	10.194.8.255/24	254
10	COMPUT1	250	10.194.9.0/24	255.255.255.0/24	10.194.9.255/24	254
11	COMPUT2	250	10.194.10.0/24	255.255.255.0/24	10.194.10.255/24	254
12	COMPUT3	250	10.194.11.0/24	255.255.255.0/24	10.194.11.255/24	254
13	COMPUT4	250	10.194.12.0/24	255.255.255.0/24	10.194.12.255/24	254
14	COMPUT WIFI	250	10.194.13.0/24	255.255.255.0/24	10.194.13.255/24	254
15	CNS1	250	10.194.14.0/24	255.255.255.0/24	10.194.14.255/24	254
16	CNS2	250	10.194.15.0/24	255.255.255.0/24	10.194.15.255/24	254
17	CNS3	250	10.194.16.0/24	255.255.255.0/24	10.194.16.255/24	254
18	CNS WIFI	250	10.194.17.0/24	255.255.255.0/24	10.194.17.255/24	254
19	SOCIAL1	250	10.194.18.0/24	255.255.255.0/24	10.194.18.255/24	254
20	SOCIAL2	250	10.194.19.0/24	255.255.255.0/24	10.194.19.255/24	254
21	SOCIAL3	250	10.194.20.0/24	255.255.255.0/24	10.194.20.255/24	254
22	SOCIAL WIFI	250	10.194.21.0/24	255.255.255.0/24	10.194.21.255/24	254
23	AGRI1	250	10.194.22.0/24	255.255.255.0/24	10.194.22.255/24	254
24	AGRI1	250	10.194.23.0/24	255.255.255.0/24	10.194.23.255/24	254
25	AGRI1	250	10.194.24.0/24	255.255.255.0/24	10.194.24.255/24	254

26	AGRI WIFI	250	10.194.25.0/24	255.255.255.0/24	10.194.25.255/24	254
27	HEALTH1	250	10.194.26.0/24	255.255.255.0/24	10.194.26.255/24	254
28	HEALTH2	250	10.194.27.0/24	255.255.255.0/24	10.194.27.255/24	254
29	HEALTH3	250	10.194.28.0/24	255.255.255.0/24	10.194.28.255/24	254
30	HEALTHWI	250	10.194.29.0/24	255.255.255.0/24	10.194.29.255/24	254
31	FBE1	250	10.194.30.0/24	255.255.255.0/24	10.194.30.255/24	254
32	FBE2	250	10.194.31.0/24	255.255.255.0/24	10.194.31.255/24	254
33	FBE WIFI	250	10.194.32.0/24	255.255.255.0/24	10.194.32.255/24	254
34	LOW1	250	10.194.33.0/24	255.255.255.0/24	10.194.33.255/24	254
35	LOW2	250	10.194.34.0/24	255.255.255.0/24	10.194.34.255/24	254
36	LOW WIFI	250	10.194.35.0/24	255.255.255.0/24	10.194.35.255/24	254
37	ART1	250	10.194.36.0/24	255.255.255.0/24	10.194.36.255/24	254
38	ART2	250	10.194.37.0/24	255.255.255.0/24	10.194.37.255/24	254
39	ART WIFI	250	10.194.38.0/24	255.255.255.0/24	10.194.38.255/24	254
40	LIBERARY1	250	10.194.39.0/24	255.255.255.0/24	10.194.39.255/24	254
41	LIBERARY2	250	10.194.40.0/24	255.255.255.0/24	10.194.40.255/24	254
42	LIBERARY WIFI	250	10.194.41.0/24	255.255.255.0/24	10.194.41.255/24	254
43	CAFTERIA	250	10.194.42.0/24	255.255.255.0/24	10.194.42.255/24	254
44	ADMIN	250	10.194.43.0/24	255.255.255.0/24	10.194.43.255/24	254
45	MANAGER	250	10.194.44.0/24	255.255.255.0/24	10.194.44.255/24	254

As we see from the above we created many subnets at WKU according to host requirement by considering future scalability. We have taken 10.194.0.0 IP block for the main campus since it have many devices which requires IP to communicate with a network so we assign the above network which have 65,534 usable host by considering for future use or scalability and we calculated variable length subnet mask (VLSM) for each VLANs with in the campus and the other is for wireless network. VLSM allows us to divide an IP address space into a

hierarchy of subnets of different sizes, making it possible to create subnets with very different host counts without wasting large numbers of addresses. More than conserving of IP addresses subnetting increase network performance through dividing entire network in different logical networks.

Ip schema for the cluster campus

VLAN no	VLAN name	Host require ment	Network id	Subnet mask	Broadcast id	Usable host
VLAN 1	college	500	192.168.0.0/23	255.255.254.0/23	192.168.1.255/23	510
VLAN 2	wifi	250	192.168.2.0/24	255.255.255.0/24	192.168.2.255/24	254
VLAN 3	library	150	192.168.3.0/24	255.255.255.0/24	192.168.3.255/24	254
VLAN 4	cafeteria	50	192.168.4.0/26	255.255.255.192/26	192.168.4.63/26	62
VLAN 5	administr ator	2	192.168.4.64/30	255.255.255.252/30	192.168.4.67/30	2
VLAN 6	manager	1	192.168.4.68/30	255.255.255.252.30	192.168.4.71/30	2

As we have seen from the above table we assign 192.168.0.0 IP for cluster campus since it needs one public IP to communicate with internet and we subnet it to assign IP address to its internal devices

IP schema for WKU hospital

VLAN no	VLAN name	Host requirement	Network id	Subnet mask	Broadcast id	Usable host
Vlan 1	Patient room	1500	194.172.0.0/21	255.255.248.0/21	194.172.7.255/21	2046
Vlan 2	Doctor	500	194.172.8.0/23	255.255.254.0/23	194.172.9.255/23	510
Vlan 3	wireless	250	194.172.10.0/24	255.255.255.0/24	194.172.10.255/24	254
Vlan 4	Manager	1	194.172.11.0/30	255.255.255.252/30	194.172.11.3/30	2

IP schema table for Wolkite University which is located in gubrye. We have created 36 wired logical networks of VLAN and there is 9 wireless VLANs for wireless network. Separating the network is important for network performance through decreasing network traffic. There is one public IP for each branch and all the device on the LAN that require access to internet is mapped to the public IP.

While subnetting takes some planning and can be time consuming, it's well worth the effort many benefits can be gained from subnetting. Those are improving network performance and speed since a single broadcast packet sends out information that reaches every device connected to that network only rather than other subnet this means the other subnets are not disturbed by broadcast come from other subnet. For example, any traffic from cluster branch does not disturb wolkite main campus since both branches are on different sub networks. Subnetting enables us to ensure that information remains in the subnetted network or broadcast domain, which allows other subnets to maximize their speed and effectiveness. Subnetting also divides our network's broadcast domains, enabling us to better control traffic flow, thus increasing network performance! The other importance of subnetting is reducing network congestion. Subnetting ensures that traffic destined for a device within a subnet stays in that subnet, which reduces congestion. We can also control network growth through subnetting. when we are planning and designing a network, size is something that needs to be taken into consideration. One of the key benefits of subnetting is that it enables us to control the growth of network through limiting size of subnets. Subnetting can boost our network security through implementing ACL on router in order to protect resource of one's subnet from the other.

Selecting Routing and Switching Protocols

Understanding the switching and routing protocols that a switch or router must support would aid us in selecting the right product for the job, and making sound protocol and technology decisions is an important network design skill. The switching section covers transparent bridging, multilayer switching, spanning-tree algorithm enhancements, and switching protocols for transporting virtual LAN information. A routing protocol follows the bridging section. A routing protocol lets a router dynamically learn how to reach other networks and exchange this information with other routers or hosts. All routing protocols have the same general goal: to share network reachability information among routers. In the proposed project we will select routing protocols that is suitable for our design. So firstly, we configure EIGRP

protocol on the core router because of its high advantage over others protocols. It has the following advantages: -

- ❖ Since EIGRP's default administrative distance is lower than RIP's, it has a stronger algorithm for advertising and choosing a default route than RIP does. It also has a load balancing option for specific traffic types.

  It reduces convergence time through triggered update mean that it only advertises neighboring router table if and only if there is change on network topology. This reduces bandwidth and resource consumption An EIGRP router develops a topology table that contains all destinations advertised by neighboring routers. And then a router computes its own "metric for the destination by using each neighbor's metric in combination with the local metric the router uses to reach the neighbor. However, since this routing protocol is proprietary to Cisco, it can only be used on Cisco devices. Because all of the internetworking devices in our project are Cisco products, there is no problem. OSPF is the routing protocol that we will configure. OSPF is an open standard that several vendors support. It has the following characteristics that are appropriate for our design.

- ➢ It converges quickly
- ➢ OSPF authenticates protocol exchanges to meet security goal.
- ➢ OSPF supports discontigous subnets.
- ➢ It supports VLSM through advertising subnet mask information when advertising routing table information.
- ➢ OSPF does not use a lot of bandwidth since it propagates only there are changes in topology. And we will implement OSPF in our project to gain the above advantages.

  Generally The table below shows characteristics of some routing protocols

Routing protocol	Adaptability	Must Scale to large	Not create lot of traffic	Run on inexpensive	Easy to configure and manage	Link state	Automatic router summarization	Distance vector	Convergence time
OSPF	✓	✓	✓	✓	✓	✓			Fast
IS-IS	✓	✓	✓	✓	✓	✓			Fast

IRGP	✓	✓					✓	✓	slow
EIRGP	✓	✓					✓	✓	Very fast
RIP	✓						✓	✓	Fast

The last routing protocol we'll set up is RIPv2, which supports classless Inter Domain Routing (CIDR) and can carry subnet information. Its metric is hop count, and its maximum hop count is 15, which is the same as RIP version 1. It allows you to advertise routing table information and multicast it to nearby routers using authentication. It has the following benefits that are appropriate for our university network. It is a structured protocol that is VLSM compliant, allows for quick convergence, and sends triggered updates when the network changes. We are configuring several routing protocols in one to improve routing protocol efficiency, and the router selects one of the routing protocols for them based on their administrative needs.

Switching protocols

Layer 2 switching is the process of using the hardware addresses of devices on a LAN to segment a network in order to breaks up large collision domains into smaller ones and that a collision domain is a network segment with two or more devices sharing the same bandwidth. This is all good, but we have redundant physical links between your switches, routing protocols won't do a thing to stop loops from occurring at the Data Link layer. Redundant connections between switches may be beneficial because they help avoid total network failures in the event that one connection fails. That's why the Spanning Tree Protocol was created: to prevent loops in a Layer 2 switched network. However, it appears that there is often a drawback: while redundant links can be extremely useful, they often create more problems than they solve. This is due to the fact that frames can be flooded down all redundant links at the same time, causing network loops and other problems. Here are a few examples of issues that may arise: If no loop avoidance schemes are put in place, the switches will flood broadcasts endlessly throughout the internetwork. This is sometimes referred to as a broadcast storm. This means loops occurring within other loops, and if a broadcast storm happened at the same time, the network wouldn't be able to perform frame switching at all its toast! To begin with. STP's main task is to stop network loops from occurring on your Layer 2 network (bridges or switches). It achieves this feat by vigilantly monitoring the network to find all links and making sure that no loops occur by shutting down any redundant ones. STP uses the spanning-tree algorithm (STA) to first create a topology database and then search out

and destroy redundant links. Switches running STP will build a map or topology of the entire switching network. STP will identify if there are any loops, and then disable or block as many ports as necessary to eliminate all loops in the topology. A blocked port can be reactivated if another port goes down. This allows STP to maintain redundancy and fault-tolerance. The other protocol that should be configured at layer two is VLAN trunk protocol (VTP) because VTP manages the addition, deletion, and renaming of VLANs on an enterprise network without requiring manual intervention at each switch. VTP also reduces manual configuration by automatically configuring a new switch or router with existing VLAN information when the new switch or router is added to the network.

When VLANs are implemented in a switched network, the switches need a method to make sure intra-VLAN traffic goes to the correct interfaces. To benefit from the advantages of VLANs, the switches need to ensure that traffic destined for a particular VLAN goes to that VLAN and not to any other VLAN. The proposed project consists of many VLAN and when there is traffic between them there should be clear header information. This can be accomplished by tagging frames with VLAN information using the IEEE 802.1Q standard

Developing Network Security Strategies

Security is fundamentally about protecting assets. Assets may be tangible items, such as a web page or our customer database or they may be less tangible, such as our company reputation Security is the biggest issues that should be carefully considered because if the network Security is not protected the functionality of network service may dis functioned Security issues that can encounter the WKU can either from inside or outside of an organization. Security threats to the WKU may come from both within and outside an organization. Some employees can snoop data packets using various tools; users may download files from unsecure websites or (virus-infected files); and some employees may lack security knowledge and therefore use poor passwords, posing a security threat to the enterprise network. The other is security issues that is from outside to enterprise network are denial of service attack, hostile intruders can steal data when data packets transmitted over internet and the router may update its routing table information from any neighbor router without authenticating. Lastly security issues can be seen from physical level. The datacenter infrastructure and network connecting devices can be placed somewhere unsecured place. We have listed some security risk that may encounter an organization and now we are going to

discuss how the proposed design overcome those security risks or issue listed on the starting section of this paragraph. To give solution for security problems we should have to develop security plan that consists different security policies. So, in order to create security plan for WKU to achieve security requirements we have to see the case from different angle mean that from inside threats and outside. The proposed design will overcome security threats that encounter from inside of the organization or from the user of WKU. The university should have to give short training for its employee on how to securely perform their work and how to browse the internet.

- The WKU should have to hire skilled network administrator.
- An employee should not download application and data from internet on their desktop since Holstein may spread malware virus and virus affected software over the internet.
- Each employee should be required to install antivirus software on their workstation (desktop), and any employee who installs prohibited software such as Wire shark on their workstation should be disciplined. Finally, an employee can use a secure password and keep their username and password confidential.

The security concerns that rise from outside is big factor can harm internal network Functionalities. As a result, in the proposed design, a firewall is configured on the router to protect the internal network from external attacks and untrustworthy sites.

- To improve physical protection, the proposed network architecture would position different servers in a hidden location and replicate them in order to recover from failure.
- Security is especially important in wireless networks because data is transmitted using radio signals that can easily be intercepted without the use of specific data encryption mechanisms. WPA (Wi-Fi Protected Access) should be set up with WPA as the strong encryption protocol.
- In the proposed design, any ports that are not in service will be turned off.
- To access routers and switches, log in IDs and passwords should be needed.
- There should be risk preventing mechanism while there are disasters like fire

damage is happen and to protect from denial of service attack appropriate protection tools must be installed for both networks and applications that run on the network. This includes such key tools as firewalls, network monitoring software, anti-virus and anti-malware programs, as well as threat monitoring systems. With these, we can monitor network baseline traffic and set up alerts for behavior that is out of the ordinary

WAN (wide area network) protection: All organizations should protect their WAN to ensure that communications between all of their branches are protected, and that all transmitting data reaches the intended recipients in safe hands. WKU's external network, as well as its virtual private network, should be safe and well-secured. A virtual private network (VPN) is a good way to arrange safe remote access to an internal network. The VPN in the proposed design is equipped with IPsec (internet protocol security) to provide greater WAN security. Encryption is a good way to keep communication confidential by encrypting it with a private key. It has a significant benefit in terms of protecting the network from external attacks and maintaining data integrity.

Developing Network Management Strategies

Network management is one of the most important aspects of logical network design. A good network management design can help an organization achieve availability, performance, and security goals. Effective network management processes can help an organization measure how well design goals are being met in the working environment and adjust network parameters if these goals are not being met.

Network management also facilitates meeting scalability goals because it can help an organization analyze current network behavior, apply upgrades appropriately, and troubleshoot any problems with upgrades. Most clients need to develop network management processes (it also true for the team network project) that can help them manage the implementation and operation of the network, diagnose and fix problems, optimize performance, and plan enhancements. The International Organization for Standardization (ISO) defines five types of network management processes, which are often referred to with the FCAPS acronym:

This proposed network design will have remotely network management mechanism to monitor the enterprise network by using remote management technique such techniques are:-

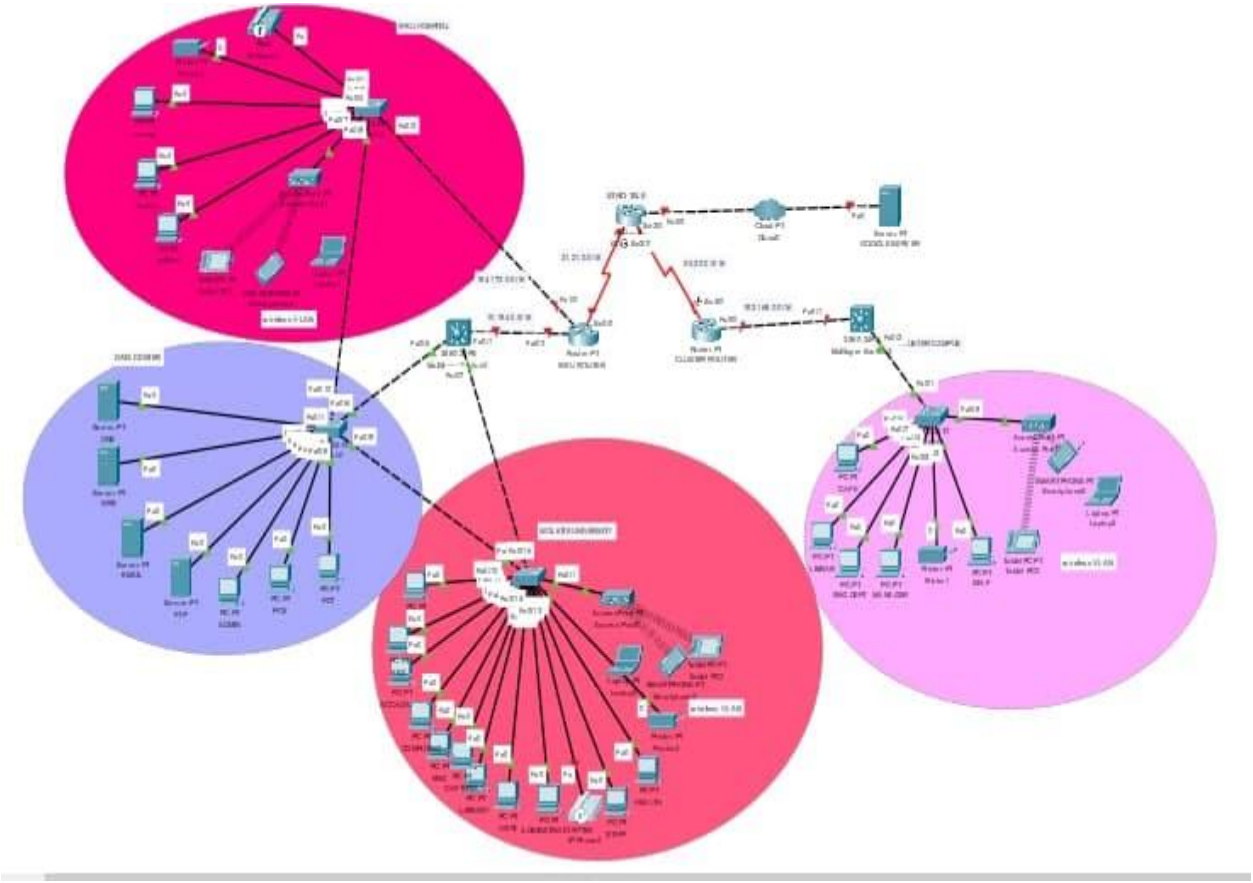
- **Fault management**: is managing the network by using proactive fault monitoring and notification, fault detection and troubleshooting of the network. It also refers to detecting, isolating, diagnosing, and correcting problems. It also includes processes for reporting problems to end-users and managers, and tracking trends related to problems. In some cases, fault management means developing work arounds until a problem can be fixed. Monitoring tools are often based on the Simple Network Management Protocol (SNMP) and Remote Monitoring (RMON) standards.

- **Configuration management**: helps a network manager keep track of network devices and maintain information on how devices are configured. With configuration management, a network manager can define and save a default configuration for similar devices, modify the default configuration for specific devices, and load the configuration on devices. It also lets a manager maintain an inventory of network assets and do version logging. So, we will document every configuration that is implemented on the network and prepare a configuration manual and guideline for the proposed network.
- **Accounting management**:-facilitates usage-based billing, whereby individual departments or projects are charged for network services. Even in cases in which there is no money exchange, accounting of network usage can be useful to catch

  Departments or individuals who "abuse "the net intentional or unintentional.
- **Performance management**:-mange network via performance monitoring and analysis the network performance it also allows the measurement of network behavior and effectiveness. It includes examining network application and protocol behavior, analyzing reachability, measuring response time, and recording network route changes. It facilitates optimizing a network, meets service-level agreements (SLA), and planning for expansion.
- **Security management**: - monitor the network through security protocols like SSH and SNMP(simple network management protocols). Let's a network manager maintain and distribute passwords and other authentication and authorization information. It

includes processes for generating, distributing, and storing encryption keys. It can also include tools and reports to analyze a group of router and switch configurations for compliance with site security standards. It is a process for collecting, storing, and examining security audit logs. Network management tools should provide an intuitive user interface that can react quickly to user input. In many cases, having both a browser interface and a command-line interface (CLI) is beneficial.

Proposed logical design for WKU



CHAPTER FOUR

Physical Network Design

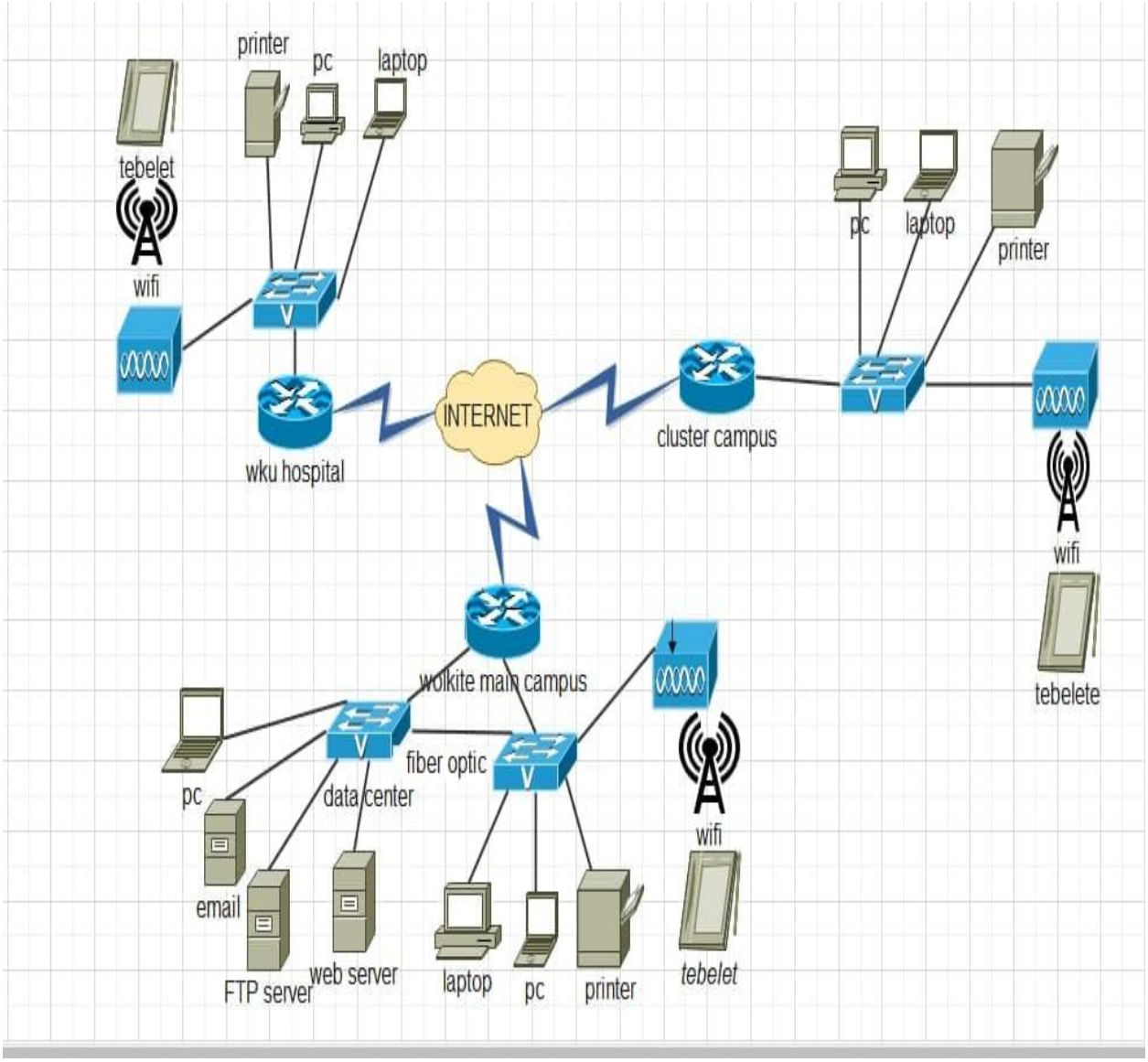
The selection of LAN and WAN technologies for the WKU proposed network design will be discussed in length in this chapter. In addition, we will choose cabling, physical and data connection layer protocols, and internetworking devices in this chapter (such as switches, routers, and wireless access points). The development of organization network solutions comes first, followed by remote access and WAN solutions in a good design process.

LAN Cabling Plant Design

Twisted pair unshielded copper wire is used in this project to link computers and switches, as well as switches with routers, since it is the cheapest option and is sufficient to support the bandwidth requirements of each branch. Among available category of UTP cable proposed design will be built by cable types cat 6e because Cat 6e support faster, more reliable data transmission through networks than the previous cat 5 . Cat 6e cable allows 10 Gigabit Ethernet over 100 m of copper cabling. This cable type is enhanced one and it is good for most small networks and improved crosstalk characteristics of other cat of UTP cable.

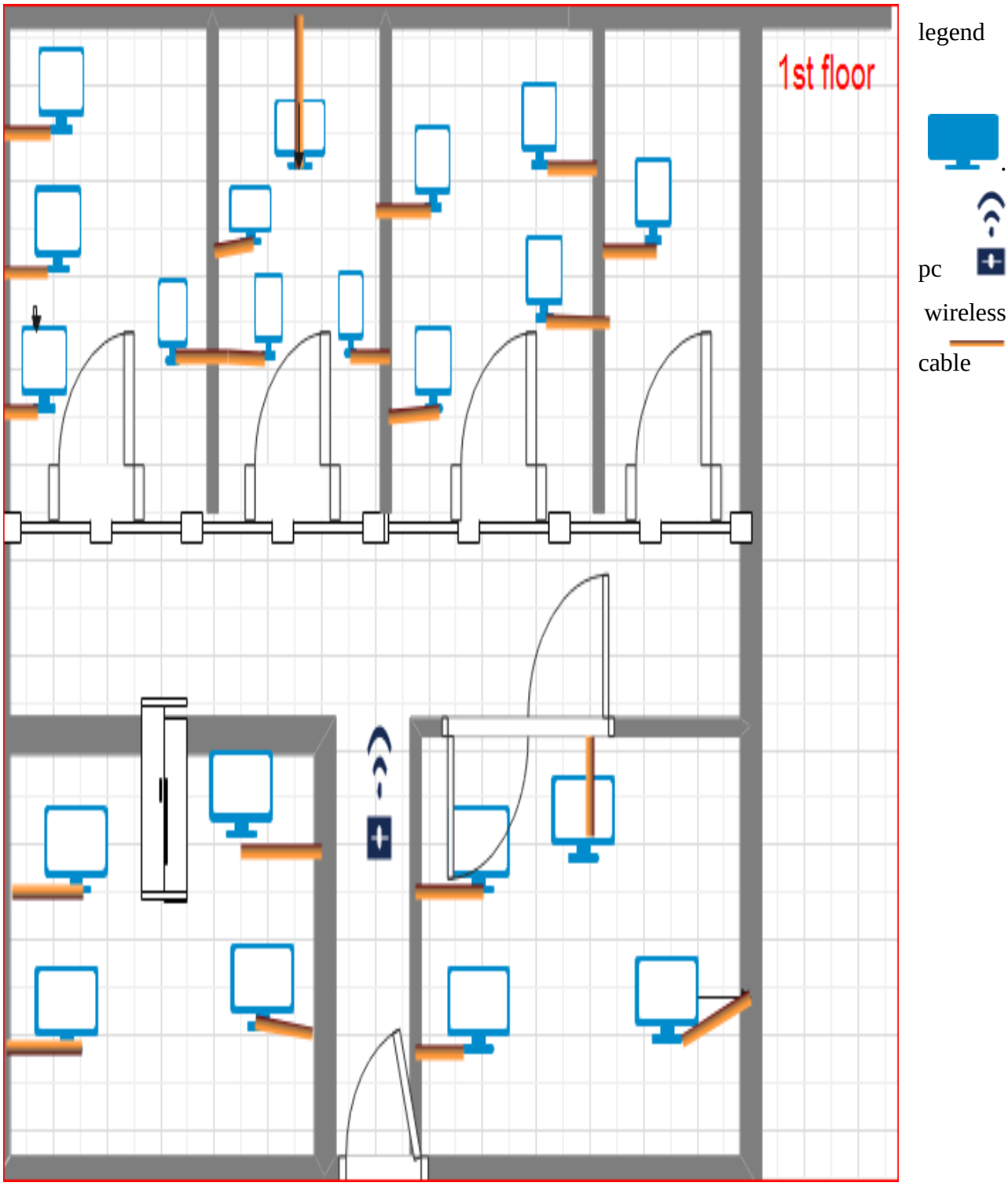
We used RJ 45, a type of cable that you are familiar with, since the cable requires a connector. The proposed design's cabling topology is a centralized cabling scheme. For wired network, there is a switch at the central location, and nodes on the network are linked to it. Because centralized cabling is easy to management and it is suitable for small network for wireless LAN, there is a switch at the central location, and wireless devices would be connected to it.

As we see in figure below the topology of proposed design is star topology



As we see from the above figure 4 the entire network of every WKU branches of the University are located in separate location and each branch are connected with other datacenter in order to give its service since datacenter and server are located at datacenter which is located at WKU main campus. The connection between hospital and datacenter is through direct connection with cable not with dedicated private line this is difficult because of current political situations, cost, and distance between them it is not feasible to the organization so to connect them using private line we use the new technology that is feasible to WKU to integrate branch with head quarter is VPN as we discussed previously. So, in proposed design each branch has on cisco 1941 integrated service router at core layer that is capable enough to support VPN device is switch at access layer to connect device at access layer. The topology of proposed design is hierarchical topology and most of the time hierarchical topology has three layers And wireless network deployed in each branch to

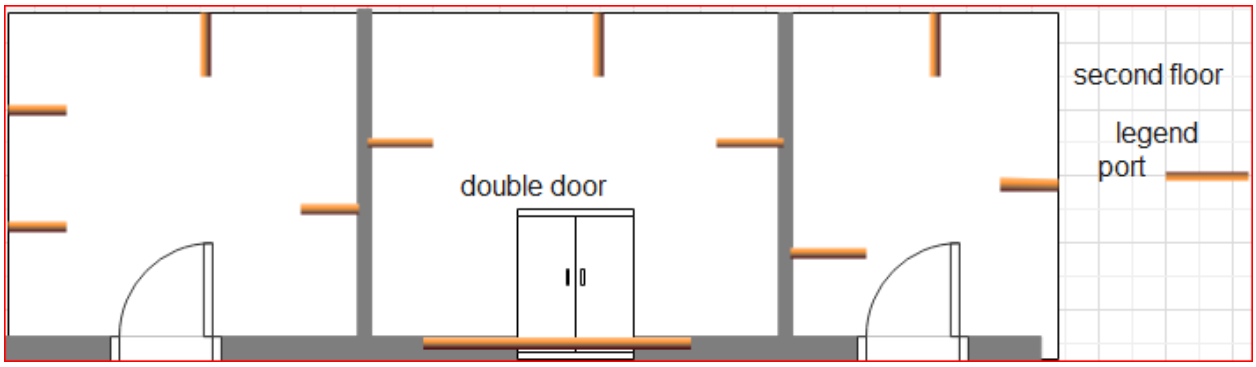
provide wireless network access to guest user who may be visiting around the university as well as for the employee of the university. In each branch printer will be shared using one desktop as server that the printer is connected on it. The main office is designed with redundant at distribution layer to protect single point of failure and to increase availability.



Proposed physical design for main campus and hospital

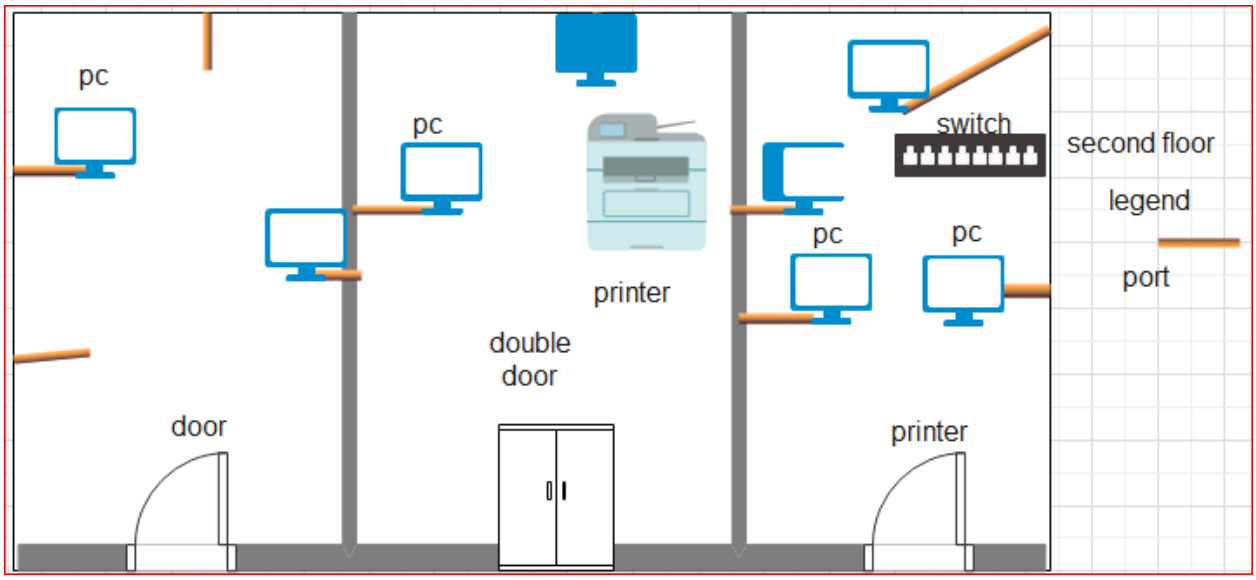
As we discussed previously in each branch there are many network users. All office of work area is at the first and second floor for both hospital and Wolkite main campus. Vertical distance of cabling is about 8 meter in each floor and horizontal distance is around 30-40

meters. One access point is deployed at first floor to provide wireless LAN and it is located at entrance point. Printer sharing is provided in each LAN by using the desktop as server.



Proposed physical design for second floor

On the second floor there is instructor office in wolkite main campus and cluster but for the future case we designed network port at this floor.



Proposed physical design for Wolkite main campus and cluster on floor 3

On the third floor there is DSL modem from ethiotelecom only internet service provider in Ethiopia to enable internet access and there is router to forward packets with in entire network and outside its own network. The other networking device at this floor is switch that is used connect the switch at first floor and to connect nodes at access layer. There is patch panel used to accommodate Ethernet cables in an enterprise network. In an enterprise network

Cabling for Wolkite main campus and cluster Branch

rooms	Cable length (in metter)		No of connectors(RJ45)
	horizontal	vertical	
Head office	30	8	4
Instructor office	40	8	10
Admin office	30	7	6
Student lab room	40	10	60
Data center room	30	7	4

Hospital branch is also one branch of WKU in gubrye . All office of hospital are on first and second floor.

Table below shows cabling information inside each rooms of hospital branch.

rooms	Cable length (in matter)		No of connectors(RJ45)
	horizontal	vertical	
Doctors room	30	7	4
Diagnosis room	40	8	15
Manager room	30	7	6
Patient room	40	10	15
Data center room	30	7	4

table below shows cabling of computing college in wolkite main campus district office

Floor no	Room no	cabling length in matter		No connector(RJ)
		horizontal	vertical	
Floor 1	Lab 01	40	10	60
Floor2	03	30	7	35
Floor3	Lab 06	40	10	60

LAN Technologies

A local area network (LAN) is a data communication network that connects multiple terminals or computers inside a single building or geographical area. In our instance, however, each branch's geographical area is primarily contained within one structure. For university

personnel, communication between devices might be wired, while for guests and workers of the university, it might be wireless.

Because future network services such as Voice over IP and video conferencing will be adopted and demand high bandwidth, we will adopt 1000-Mbps (1-Gbps) Ethernet established by the IEEE 802.3ab standard as a LAN technology in our proposed architecture. We recommended gigabit Ethernet because it transmits data through unshielded twisted pair (UTP) cable and does not necessitate the installation of new infrastructure, making it cost-effective. Interconnecting high performance switches, routers at the core layer of our network, and servers with switches is faster and more critical, and it provides full duplex operation at data.

Users in a wireless LAN can roam around freely within the coverage region. Because we propose one access point per branch, the access point we choose should be able to provide wide coverage. The 802.11ac wireless local area network (WLAN) will be employed in this project's network design. The 802.11ac is a set of advanced WLAN features produced by a team at the Institute of Electrical and Electronics Engineers (IEEE). It supports simultaneous connections on both the 2.4GHz and 5GHz Wi-Fi bands thanks to dual band wireless technology. It can connect wireless devices at the quickest maximum speed and with the best signal range. Cisco access points are used, and each building has at least one access point. The number of access points installed is determined on the building's size. More than one access point can be established in a larger structure.

Selecting Internetworking Devices

Our suggested design is not just a local area network since it includes a wide area network with VPN technology to protect packet delivery across the internet. As a result, when selecting internetworking devices, we must consider a number of criteria. The router we chose must support the VPN in order to provide services. We advocate using one of the Cisco 1900 integrated service (ISR) series routers, the Cisco 1941 integrated service router, as a core router for all branches due to its many benefits. The following are some of the benefits of this router. This are

Agility: New services can be activated fast, and licenses can be simply updated, thanks to ubiquitous IOS. Because the Cisco 1941 integrated service router features a built-in Cisco wireless access point for corporate Wi-Fi, it also provides integrated enterprise Wi-Fi.

WAN flexibility: - It connects the organization to the internet service provider using a variety of options, including WLAN with 802.11a/g/n, T1/E1, T3/E3, 4G/LTE, and fibre Gigabit Ethernet. Since it has various interfaces that support wired and wireless network networks, it can provide both.

Secure communication of file sharing - this router has ability to support high level or advanced security encryption like IPsec, Flex VPN, SSL VPN, intrusion prevention, next generation encryption and firewall. It offers highly integrated security through offering a comprehensive suite of VPN technology with IPsec and SSL VPNs and WLAN security support for 802.11i. Get threat defense support through firewall and IPS options, and support for encryption and cloud-based security.

High performance: The 1900 series includes multicore processors that are both powerful and energy efficient, a multigigabit fabric, and high-performance services modules that can run multiple concurrent services at high throughputs in a scalable manner. This router provides top benefits to the enterprise, including efficient service delivery, investment security through previous generation interface support, and the ability to reuse modules across platforms, as well as being energy efficient. It supports video and voice data, as well as the EIGRP routing protocols, which we chose as routing protocols because they are Cisco-developed device. The other internetworking devices are switch which is data link layer device. We recommend Cisco Catalyst 2960-S Series Switches at all branches of the WKU to connect different nodes on access layer. They enable reliable and secure business operations with lower total cost of ownership through a range of innovative features including Flex Stack, Power over Ethemet Plus (PoE), and Cisco Catalyst Smart Operations (tools that simplify deployment and reduce the cost of network administration). Let see the specification of the product it has USB interfaces for management and file transfers.

The Cisco Catalyst 2960-S Series Switches provide a range of security features to limit access to the network and mitigate threats, including: threat defense features including Port Security, Dynamic ARP Inspection, and IP Source Guard and features to control access to the network, including Flexible Authentication, 802.1x Monitor Mode. The Cisco Catalyst 2960-S Series Switches offer a superior CLI for detailed configuration and administration. 2960-S switches are also supported in the full range of Cisco network management solutions. It has 64 MB Hash memory and 128 MB DRAM. 24 Ethernet port is enough for proposed design.

Our project's last internetworking equipment is a wireless access point that provides a wireless network to the branches and visitors. The Cisco Small Business 500 wireless access point is a

high-performance, easy-to-deploy, and secure business-class wireless network connection that we suggest.it Provides cost-effective selectable or concurrent dual-radio Wireless network connectivity for high capacity and additional users. It supports Gigabit Ethernet LAN interfaces with Power over Ethernet (PoE) support flexible installation and reduces cabling and wiring costs. Intelligent quality-of-service (QoS) features let us prioritize bandwidth-sensitive traffic for voice over IP (VOIP) and video applications, Smart Signal Antenna technology enables us to extend the reach of wireless network by optimizing coverage, reception, and performance. To provide secure guest access to visitors and other users, the Cisco 550 access points support a captive portal with multiple authentication options and the ability to configure rights, roles, and bandwidth. A customized guest login page lets you present a welcome message and access details, and reinforces your brand with company logos.

To enhance reliability and safeguard sensitive business information of the institution, the Cisco 350/560 access points support both Wi-Fi Protected Access (WPA) Personal and Enterprise, encoding all wireless transmissions with powerful encryption. In addition, 802.1 X RADIUS authentications helps keep unauthorized users out. It supports VLAN, load balancing and access control list (ACL) plus MAC ACL.

Selecting Devices for the Central Site

WKU's central site or datacenter connects remote users or branches of the organization via VPN software to the corporate network. Users connect to a VPN via a service provider's local area network and send data across encrypted tunnels to a VPN firewall or concentrator in the datacenter. Both routers and firewalls at the central site can act as the termination point for VPN tunnels. A generic router can become overwhelmed if a network supports many tunnels. Since a peak number of simultaneous users reach 100, a dedicated firewall or VPN concentrator should be deployed at the main office.

(A VPN concentrator is a standalone hardware platform that aggregates a large volume of simultaneous VPN connections from each branches of WKU.) Generally, the VPN firewall placed between a router that has access to the VPN and a router that forwards traffic into the corporate network. Hence, the firewall should support at least two Ethernet interfaces of the flavor used in this module of the network design (Fast Ethernet, Gigabit Ethernet, and so on). The VPN firewall at the central site should be interoperating with the VPN client software on remote the users systems. The VPN firewall that we are going to select for central site should have a fast processor, high-speed RAM, and support for redundant power supplies and

hardware-assisted encryption since it must support a number of simultaneous tunnels and the amount of traffic it can forward.

It should also support the following software features:

- ✓ Tunneling protocols, including IPSec, PPTP, and L2TP
- ✓ Encryption algorithms, including 56-bit DES, 168-bit Triple DES, Microsoft Encryption (MPPE), 40- and 128-bit RC4, and 128-, 192-, and 256-bit AES.
- ✓ Authentication algorithms, including Message Digest 5 (MDS), Secure Hash Algorithm (SHA-1), Hashed Message Authentication Coding (HMAC) with MDS, and HMAC with SHA-1
- ✓ Network system protocols, such as DNS and DHCP
- ✓ routing protocols

Because every branch of the WKU should be connected to the datacenter in order to provide service, the router at the central site should have high performance and enable numerous VPN tunnel connections to numerous branches of the organization. So, we recommend the cisco 1941 series integrated service router for the head office branch because of its benefit and it is suitable to the university. It has High-performance Gigabit Ethernet ports, enabling branch of the institution to transfer large file rapidly to datacenter. The cisco 1941 series integrated service router Dual Gigabit WAN VPN Routers is the choice for any network in which performance, security, reliability, and adaptability top the list of requirements and high-capacity virtual private networks (VPNs) connect multiple offices and enable dozens of employees to access the information they need from any branch just as securely as if they were working at main office. It is modular platform device mean that the Cisco 1941 Series ISR are highly modular platforms with multiple module slots to provide connectivity and services for varied branch network requirements. The ISRs offer an industry-leading breadth of LAN and WAN connectivity options through modules to accommodate field upgrades to future technologies without requiring replacement of the platform. The Cisco 1941 Series uses high-performance multicore CPUs to meet the expanding demands of branch office networks, including high-throughput WAN applications. It also supports a variety of routing protocols, which we'll set up in our network architecture. Cisco 1900 Series Integrated Services Routers also support multiple network monitoring protocols like SNMP, Remote Monitoring (RMON) and Network Flow.

branches	WKU	WKU hospital	Cluster campus	Price per unit	Total price
Router	1	1	1	120,000	360,000
switch	4	1	2	160,000	1,120,000
Access point	1	1	1	80,000	240,000
RJ-45 connecter	5000	2000	3000	30	300,000
UTP cable in roll	50	20	30	2000	200,000
Total cost					2,220,000

Table cost of project

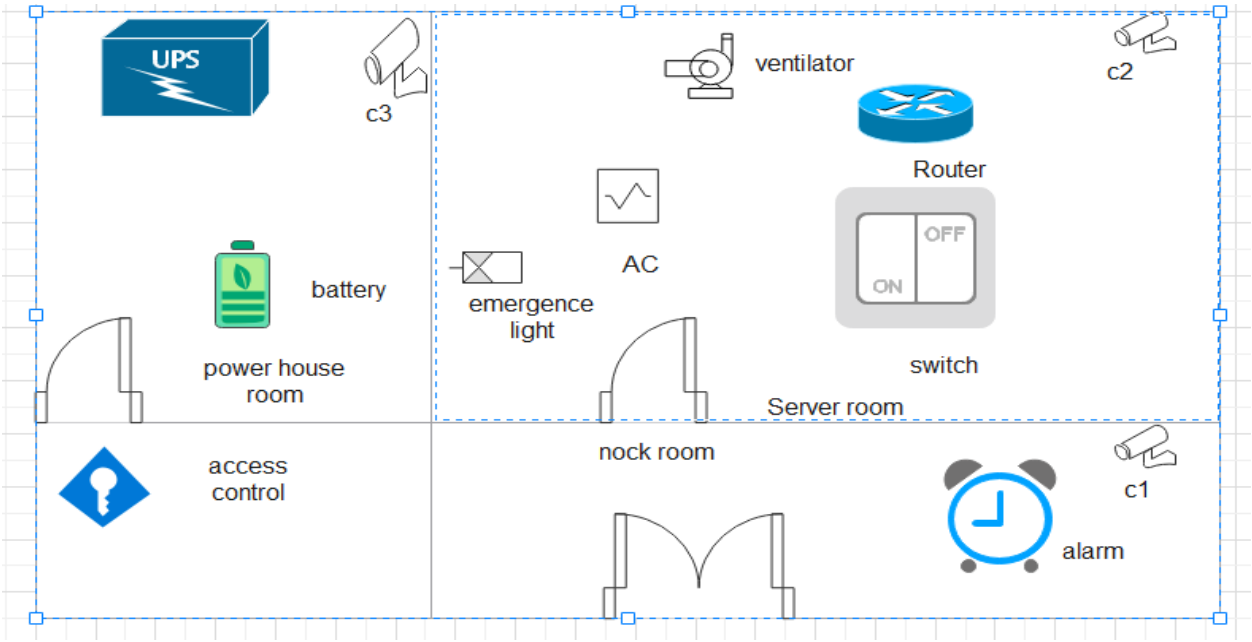


Figure Main data center design

Table Description of main data center

Access control	Biometric device to control outdoor
Alarm	Device used to detect fire extingusher
AC	Air conditioner used to control server room
Emergence light	Device used to detect any contact between electric
C1	Indicate security camera in power house room
C2	Indicate security camera in server room
C3	Indicate security camera in nock room
Switch	To connect device on computer network by packet switching to retrieve, process and forward data to destination
Router	Connect multiple networks from branches in VPN tunnel mode and forward packet destined for its own network or other network
UPS	Un interrupted power supply
Battery	Indicate storage in order to store power supply