

12-19-2016

Computer Network Design for Universities in Developing Countries

Rafid Salih Sarhan AlSarhan
Valparaiso University

Follow this and additional works at: <http://scholar.valpo.edu/itcrpr>



Part of the [Computer Engineering Commons](#), and the [Computer Sciences Commons](#)

Recommended Citation

AlSarhan, Rafid Salih Sarhan, "Computer Network Design for Universities in Developing Countries" (2016). *Information Technology Capstone Research Project Reports*. 2.
<http://scholar.valpo.edu/itcrpr/2>

This Research Project Report (Capstone) is brought to you for free and open access by the Department of Computing and Information Sciences at ValpoScholar. It has been accepted for inclusion in Information Technology Capstone Research Project Reports by an authorized administrator of ValpoScholar. For more information, please contact a ValpoScholar staff member at scholar@valpo.edu.



VALPARAISO UNIVERSITY

Computer Network Design for Universities in Developing Countries

By

Rafid Salih Sarhan AlSarhan

Master's Research

Submitted to the Graduate School of Valparaiso University

Valparaiso, Indiana

The United States of America

In partial fulfillment of the requirements

For the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY



Research Completion Form

Date: 1/16/2017

Computer Network Design for Universities in Developing Countries

by

Rafid Salih Sarhan AlSarhan

I have neither given nor received, not have I tolerated others' use of unauthorized aid.



Signature

1/16/2016

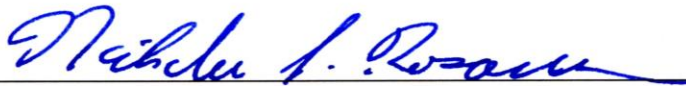
Date

This form is to certify that the above named research:

Computer Network Design for Universities in Developing Countries

has been completed by

Rafid Salih Sarhan AlSarhan



Nicholas S. Rosasco D.Sc

Assistant Professor, Computing and Information Sciences

Supervising Instructor



Valparaiso University

CERTIFICATION OF CAPSTONE PROJECT COMPLETION

The Research Project

Computer Network Design for Universities in Developing Countries

has been completed by

Rafid Salih Sarhan AlSarhan

to complete the capstone requirement for the

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

Degree Program in the Department of Computing and Information Sciences.

December 2016

Nicholas S. Rosasco

Nicholas S. Rosasco, D.Sc. Assistant Professor, Computing and Information Sciences Supervising Instructor

16 January 2017

Date

STATE OF INDIANA COUNTY OF PORTER

Subscribed and sworn to (or affirmed) before me this 16 day of January, 2017

By Nicholas S. Rosasco, personally known

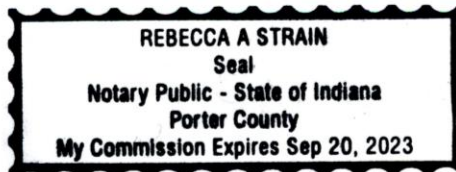
OR

produced identification. Type of identification produced

Rebecca A. Strain

Notary Public

My Commission Expires:



© Copyright

Rafid S AlSarhan, 2016

All rights reserved.

ACKNOWLEDGEMENTS

First of all, my biggest gratitude goes to God “Allah” who has consistently supported me with continued strength and knowledge all through my research studies.

Special big thanks to my supervisor, Professor Nicholas Rosasco (Ph.D.), who always educated and fed me with drops of science from his ocean of Sciences.

I want to thank my parents, especially my mother, and all my brothers and sisters, for their prayers during my entire studies in the USA. Without their support, I would not be standing where I am. Despite so many challenges, they were always there to lend me all the support that I needed.

I also would like to extend my warm appreciation to Professor Dr. James Caristi for his good direction and support. I will cherish and take them with me wherever I go.

My deepest thanks to Professor April Miller Crippliver (Ph.D.), who’s guidance and mentorship during my research never ceases to amaze me.

Finally, I say thank you to all my friends for all their love and kindness towards me, especially Mark Esiyeden, who encouraged me during my Research studies. Also, to anyone whom I might have forgotten while writing this appreciation, I want to say thanks, and I duly appreciate you all.

Table of Contents

1.	Introduction	1
2.	Objectives	2
1.1	Capacity	2
1.2	Reliability	2
3.	Challenges / Constraints	3
3.1	Implementing A Network In Developing Countries	3
3.2	Staffing Questions	4
3.2.1	Skillsets.....	5
3.3	Budget.....	5
4.	Equipment and Design Selection.....	6
4.1	Network Topology.....	6
4.1.1	Point to Point Topology.....	6
4.1.2	Bus Topology	7
4.1.3	Ring Topology.....	8
4.1.4	Mesh Topology.....	9
4.1.5	Star Topology	11
4.2	Choose the Equipment.....	12
4.2.1	Physical Connections.....	12
4.2.2	Wireless	16
4.3	Connection Setup.....	17
4.3.1	Ethernet Cable	18
4.3.2	Ethernet Straight Wired Cable.....	20
4.3.3	Wi-Fi.....	21
4.4	Devices Used	23
5.	Security.....	26
5.1	Infrastructure	26
5.1.1	Virtual Switch.....	26
5.1.2	Back-up and Recovery.	28
5.1.3	Firewall	30

5.1.4	DNS	32
5.2	Individual Systems/Components	34
5.2.1	Encryption of Passwords.	34
5.3	Individual Hosts.....	35
5.3.1	Anti-Viruses Tools.	36
5.3.2	Update and Patching Tools.....	37
5.3.3	Basic Support.....	37
5.3.4	The Server Room.....	37
6.	Background Information On TCP/IP.....	38
6.1	The Internet Protocol (IP) Address.....	38
6.2	DHCP (Dynamic Host Configuration Protocol).....	39
6.3	Static Assignment.....	40
6.4	Classful Addresses.....	40
6.5	Classless Addresses	42
7.	Implementation.....	43
7.1	Personal Computers.....	44
7.2	Switches.....	45
7.3	Routers.....	47
7.4	NAT System	54
7.5	Wireless Access Point	56
7.6	Servers	60
7.6.1	DHCP Server	61
7.6.2	DNS Server.....	62
8.	Expectations and Ongoing Challenges, Options, And Possible Future Evolution.....	64
8.1	Quality of Devices	65
8.2	Backup.....	66
8.3	Evolution/ Optional Additions	66
8.3.1	Optical Fiber.....	67
8.3.2	Firewall.....	67
8.3.3	Servers	68

8.3.4	Backup	69
8.3.5	Two Networks for Security	69
9.	Conclusion	70
9.1	Summary.....	71
10.	Reference:.....	73

LIST of Figures

Figure 1 Point to Point topology.....	7
Figure 2 Bus topology	8
Figure 3 Ring topology.....	9
Figure 4 Mesh topology.....	11
Figure 5 Star topology	12
Figure 6 Different types of wireless is used	17
Figure 7 integration network system	18
Figure 8 UTP cable Solid and striped	19
Figure 9 T-568B and T-5668A	19
Figure 10 Devices connected by straight cable	21
Figure 11 Straight cable connection.....	21
Figure 12 The access point is star topology	23
Figure 13 Virtual switche	28
Figure 14 Backup server	30
Figure 15 Firewall device	32
Figure 16 Password Creation and Encryption	35
Figure 17 standard rack for secure internet devices.....	38
Figure 18 IP address in a personal computer	45
Figure 19 Switches in the network	47
Figure 20 Hyper-star topology.....	48
Figure 21 Routers configuration.....	50
Figure 22 Static route configuration.....	51
Figure 23 Create password on a router.....	52
Figure 24 Access point connected with the router	57
Figure 25 configuration IP addresses in the router	58
Figure 26 Configuration Access point.....	59
Figure 27 Configuration IP address of a laptop computer connect to the access point.....	60
Figure 28 DHCP device configuration	61
Figure 29 DNA configuration	63

Figure 30 Check DNS from a personal computer 64

LIST of Tables

Table 1 Compares the price of the cables 14

Table 2 IP address used in the university 24

Table 3 Shows price of devices used in the network 25

Table 4 Range of IP address for each class..... 41

Table 5 Summarizes the network and host numbers for each class..... 41

Table 6 Subnet Mask 44

Abstract

The purpose of this project is to design a suitable network system for universities in developing countries. The aim was to design a network with high-quality security and low cost, in such a way that network devices of universities in developing countries, will meet standards associated with the universities in developed countries. This project will help to enhance education in developing countries.

There are many devices that were used in designing the network, such as routers, switches, backup, firewall, and servers. All devices were connected to each other to make integration network system and configured by putting IP addresses to all devices. Although the budget for this design network was low, it needed to have a high level of security. Accordingly, it incorporated several mechanisms including a firewall device that prevents any unfavorable data from entering into the network. Additionally, all devices in the network were secured by passwords, and these passwords were encrypted to be more secure. Moreover, each computer in the network was secured by antivirus programs and a backup system.

This research discussed in details the budget challenges that the network faced in developing countries. Developing countries have a limited budget that affects choosing devices in the network such as servers. The servers used for this network design are DHCP server and DNS servers. This presentation and design included additional components such as a web server, mail server, etc.

1. Introduction

Technology has reached its highest peak of development, especially in making life easier for people. Well implemented technology is faster than human in processing calculation and is more accurate. Technology has become an important concept in our life. It assists in connecting communities together. Obviously, people have started to use technology in every field of life including education, health, the military, etc.

The computer network represents a component, especially on how it enhances the functional performance in different fields and organizations, such as companies and schools. A school's computer network performs so many functions, such as connecting students with the university, faculty, and the library. Most universities today use the network to provide online education by connecting widely dispersed students with their professors directly. For this reason, computer networks play a vital role in the education area by providing efficient communications for the university environment.

However, the design of computer networks differs from one university to another. This is as a result of many factors which determine the differences. Such factors include; adaptability, integration, resilience, security, and cost. Installing networks in a university relies on the university's budget, which differs by institution and from country to country. For instance, there are many countries whose universities do not have the financial capability for designing the 'perfect' or ideal network. Yet these universities from these third world countries still need to have good quality and more secure network equipment with less cost. This is because these schools aspire to deliver capability in line with the leading prestigious universities despite low budgets. Therefore, this design will be

focusing on factors that will enhance computer network for universities in developing countries to be able to compete favorably with another computer network in modern country universities.

2. Objectives

The main goal of this project is to present a Local Area Network design suitable for universities in developing countries. Many universities in developing countries are searching for ways to integrate networks that have security, backup, and other features available in a university network in a developed country. The universities in developing countries are faced with challenges in designing a network that is equal in the standards used by developed countries. The main problem developing countries face deals with a profound budget deficit. This research will help these universities to design a network that employs low-cost solutions without unacceptable compromises in security or quality.

1.1 Capacity

This is the ability of the network to withstand intense pressure from utilization. Most times, the networks are mainly crowded by many users that the network capacity could not handle. It is very important to design a network in such a way to handle many users without failure. This network is designed for a user population of 5075. If more users access the network, it will be able to scale.

1.2 Reliability

Reliability refers to the ability of the computer network's hardware and software component to consistently perform according to its specifications. This project's network

will be highly reliable in performance because its components will be chosen from Cisco company, a major and well-regarded manufacturer.

Reliability of the security in the network is in high level. This is because there are many powerful devices used to secure data like the firewall device that is used in filtering data entering into the network. If any issue happens to the data, there is a way of restoring the data from backup servers. Each computer in the network has anti-virus to protect users' data. Also, all router and switches are protected by passwords and encryptions.

3. Challenges / Constraints

The first challenges this network design will face is economic and budget issue. The cost for designing of the network system has a limit that cannot be exceeded. This network design will be the solution for designing network in the developing countries. This is because this design can be made to be an integration network system, with good security, and quality of devices by low prices.

The availability of equipment is needed to complete the installation of all parts of the network. Developing countries do not have the complete equipment required for the local area network, such as server device, backup device, and firewall device. The provision of devices will be another challenge that will be faced when designing a network in developing countries.

3.1 Implementing A Network In Developing Countries

The proposed network will be utilized by educated minds in a university. Although educated, users are not entirely informed about network management as with their developed country counterpart. Since network technologies came at a very late time

to these countries, many users are not able to fully utilize the advantages of the system. For example, users of networks in developing countries do not have enough networking knowledge to understand the concept of connecting computers to a network such that they can share a single printer. Dedicated printers for each system are much more common, despite increased operation. Network sharing is a difficult concept for users to grasp, such as sharing files and data on connected computers. When this network is installed and utilized appropriately, users will become far more educated and knowledgeable about a network and its technologies than ever before.

Although network technicians in developing countries do not have sufficient knowledge and exposure to networking, their advanced counterparts in developed countries should endeavor to educate and share their knowledge to make the developed country's technicians to a level of self-sufficiency and independence.

3.2 Staffing Questions

The network needs a management team to manage it. These team (technicians) must have the required skills and expertise in network field. If technicians do not have the expertise about the network, they will cause more problems to the network system than resolving the problems that network system face. If a technician does not know how to fix the network or does not have enough expertise about a network, he or she will waste a lot of money fixing the network device, while the cost of that device might be less to fix. They may break down another device without fixing the devices that have problems. Additionally, many network systems have a small issue to be fixed in the system, but the inexperienced technician makes that issue very big without fixing it. The network device

may need short time for fixing, but the inexperienced technician stops network for a long time to fix it, and may not fix that issue at all thereby wasting lots of valuable time for no reason. Therefore, network system needs experience technicians who always update their knowledge base constantly.

3.2.1 Skillsets

As mentioned earlier, technicians must have enough experience to support long-term maintenance. This experience can come by employing people who have worked in the networking field. The technicians must take network courses constantly by either receiving training from certified Cisco network professionals employed locally in the university's location, or by going directly to Cisco's overseas operations in developed countries in order to acquire a wealth of knowledge on network management and operation. There are many Cisco certification exams such as CCDA, CCNP...etc. Technicians must have at least one of these certifications in order to qualify for staff positions.

3.3 Budget

Budget plays the main role in designing local area network. It can affect the choice of quality, and security of devices used in designing a network.

While expensive devices have good quality, such items may be unavailable due to cost considerations. The budget can cause changes of devices of the network system from high-quality device to very low-quality device. If there is enough budget for designing a network, a better quality of devices will be used for this network. The quality of the devices will depend on the price. For example, optical fiber cable is a faster cable used in

the internet field. However, most network projects do not use optical fiber cable because of its high price.

The budget does not only affect the quality of devices in a network design, but it also affects the quality of security. If there is a permission of using an extended budget, a new software such as a strong antivirus will be used for the devices in the network. This will make the security of the network to be stronger.

If enough budget is appropriated for designing the network, more than one backup device will be used in the network, and spare firewall device will also be used to ensure more security. Also, many servers will be added to the network system.

4. Equipment and Design Selection

4.1 Network Topology

A network topology defines how hosts are connected to a computer network. It characterizes how the PCs and other hosts are organized, and linked to each other. There are many types of network topology such as Point-to-Point, Bus, Star, Ring, and Mesh topology. Each type has a different set of advantages and disadvantages.

4.1.1 Point to Point Topology

Point to Point topologies connect two computers together with a single line connection. The advantage of Point to Point Topology is that it gives a faster connection, and it is also less expensive than other topologies. The strength of this topology is more than other kinds of connection. However, Point-to-Point topology is mainly used for small networks, and the computers must be near to each other for a better connection. However, this topology will not be useful for big networks because it does not scale

effectively. Big, in this case, includes a network of hosts such as that needed to serve a reasonable sized college or university.

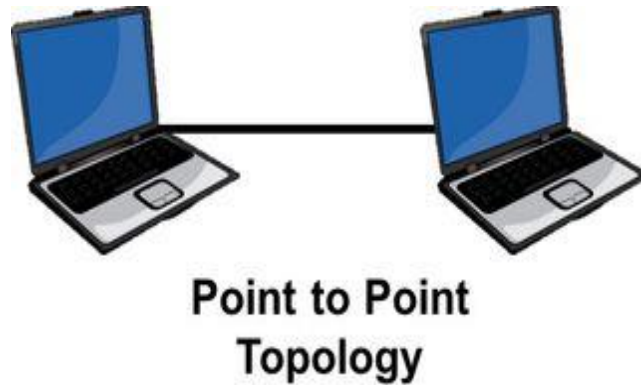


Figure 1 Point to Point Topology

4.1.2 Bus Topology

Bus topology, with the inexpensive configuration, many computers are connected by a single line of cable. Each side of the main cable must be connected to terminals. This type of network topology is small and very easy to connect devices together to making the network. The bus topology uses one main cable for all the connection, and it's usually seen in smaller networks. If the main cable is broken, there will be a network failure such as that seen at a local office level. Due to the disadvantages of this small network, it cannot be suitable for universities, which usually requires large and robust network connections. It is also very slow for sending and receiving data because all information is transmitted only in one cable, and that cable can create performance issues. "Heavy network traffic can slow a bus considerably because any computer can

transmit at any time. But networks do not Coordinate when information is sent. Computer interrupting each other can use a lot of bandwidth.”¹(Pandya, Kartik 23)

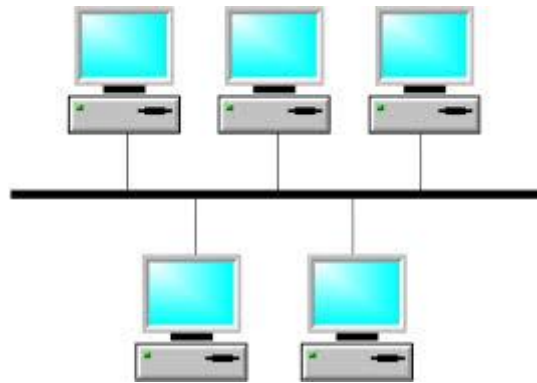


Figure 2 Bus topology

4.1.3 Ring Topology

Another topology is the ring topology, which uses a connecting computer in a circle shape. The source computer sends information to the cable ring, and this information searches for its destination by accessing each computer on the ring until it gets its destination node. According to the article “A review of Network Topology” by Jiang, “Adjacent pairs of workstations are directly connected. Other pairs of workstations are indirectly connected, the data passing through one or more intermediate nodes.”² (Jiang 1175). This topology is used for LAN (Local area network) and WAN (Wide Area Network) networks. It is very easy to install but difficult to expand and maintain. The ring topology is very slow to send and receive data. According to Yurcik.” This topology provides inherent reliability since a signal from a source travels around the ring to the

¹ Pandya, Kartik. "Network Structure or Topology." International Journal of Advance Research in Computer Science and Management Studies 1.2 (2013).

² Jiang, Ruoqing. "A review of Network Topology." (2015).

destination and back to the source as an acknowledgement. Least-cost rings may approach the cost of a least-cost tree but are generally more expensive and have more delay.”. This is because the information does not go to the computer destination directly but passes all computers between the source and destination. A drawback of this topology is that if one host shuts down or breaks down, the whole network will go down. Also, the hardware used for connecting each device for this topology is very expensive. This kind of topology is not useful for universities in developing countries because those universities do not have the resource to purchase such computers. Especially given that the probability of network failure is very high.

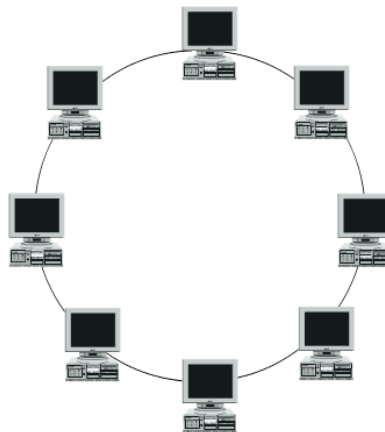


Figure 3 Ring topology

4.1.4 Mesh Topology

The mesh topology requires each computer to be connected directly to multiple computers, with more than one line connecting all computers to each other. One good thing about this topology is that if one line fails or cut, it will use the other paths to send information to the destination. This reduces the probability of a total network failure.

Mesh topology is faster compared to other kinds of topology, but it is very expensive.

According to the Clarke “A disadvantage of a mesh topology is the cost of the additional cabling and network interfaces to create the multiple pathways between each system.”³

(14). This is because of its high number of Network Interface Cards (NIC)s and connections. When each computer connects to all computers in the network (one to all), each computer needs more than one NIC. For example, if mesh topology network device is connected to six computer devices together, each computer in the network must have five NIC devices to connect to all other computers, and the number of connections will be 15 connections. It is calculated by the following formula: $n(n-1)/2$ (n represent the number of computer in the figure below). According to the article “Fully-connected networks with local connections” by Kornilovitch said “The main disadvantage of fully-connected networks is complexity. A N node network needs at least $N(N - 1)/2$ individual pair-wise links to be fully connected.”⁴(Kornilovitch 999). According to the formula above, when connecting six computers together, the network needs 15 connections. Moreover, the network in mesh topology is very difficult to maintain, setup, and manage.

³ Clarke, Glen E. CompTIA Network+ Certification Study Guide. McGraw-Hill, 2012.

⁴ Kornilovitch, P. E., R. N. Bicknell, and J. S. Yeo. "Fully-Connected Networks with Local Connections." Applied Physics A, vol. 95, no. 4, 2009., pp. 999-1004doi:10.1007/s00339-009-5124-3.



Figure 4 Mesh topology

4.1.5 Star Topology

The star topology is generally used for all networks whereby each device or computer is connected to a center hub by a direct line. The center hub can be a switch, router, or server. Each computer connects directly to the center device such as the hub, router, and server. "A star topology is designed with each node connected directly to a central network hub, switch, or concentrator"⁵ (Jiang, Ruoqing 1174). It is easy to add and remove a computer from the network without affecting the network. Pandya, Kartik mentioned in their article, "It is easy to replace, install or remove hosts or other devices, the problem can be easily detected-It is easier to modify or add a new computer without disturbing the rest of the network by simply running a new line from the computer to the central location and plugging it to the hub."⁶(Pandya, Kartik 25). Also, the cost of this network topology is less. If a computer shut or breaks down, it will not affect other devices in the network. However, if the center device (hub) breaks down, it will affect all the computers connected with it. This topology will be used for this design because each

⁵ Jiang, Ruoqing. "A review of Network Topology." (2015).

⁶ Pandya, Kartik. "Network Structure or Topology." International Journal of Advance Research in Computer Science and Management Studies 1.2 (2013).

computer is independent of other computers in the network, and it is less expensive than mesh and ring topology and easy to install.

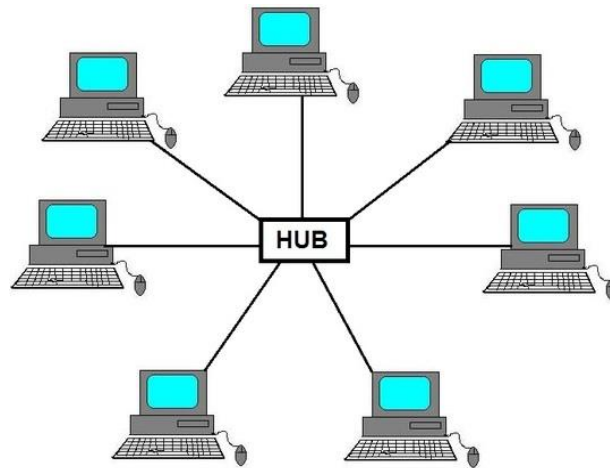


Figure 5 Star topology

4.2 Choose the Equipment

Each network must have a media for transferring information from one node to another, or from one device to other devices. These media play a significant role in determining the transmission speed of the network, maximum distance, shielding against interference, and the cost of the network. There are two options for general use: One of them is a physical connection, and the other one is wireless.

4.2.1 Physical Connections

Cable networks are hardware materials used for connecting network devices together such as routers to switches, computers to switches...etc. There are many kinds of network cables used to connect devices. Such cables include optical fiber, coaxial and twisted pair cable. These cables differ from each other in terms of cost of the network, way to install, the distance between devices, and speed.

The optical fiber cable is a link containing one or more optical strands that are utilized to convey light instead of electricity. So, this type of cable is the fastest type of cabling for transferring information from one node to another, because the speed of this kind of wire is equal to the rate of the light which is approximately 3×10^8 . According to the article "A good performance watermarking LDPC code used in a high-speed optical fiber communication system" by Zhang, Wenbo, et al., "A main limitation for nearly all recent high-speed optical transmission systems is that the uncoded bit-error-rate (BER) is only around 10^{-3} even for back-to-back [2]."⁷ However, the optical fiber cable installation is very expensive because it requires a specialized technician to properly install it, and another specialized technician for fixing it. Unfortunately, the developing countries do not typically have enough financial resources to employ the services of these special technicians in the installation and fixing of the optical fiber. Also, the tools and components used with a class of cable are also high cost. According to JAN, EDWIN "Fiber optic - consists of a center glass core surrounded by layers of protective material. Of the given cables, this is the most high speed and the most expensive."⁸ (34) However, developing countries have a limited economy, and it makes more sense to use the less expensive option. Therefore, the optical fiber is not suitable for this network. The table below compares the price of the optical fiber and other cables such as coaxial cable and twisted pair cable. All prices are taken from the Amazon website.

⁷ Zhang, Wenbo, et al. "A Good Performance Watermarking LDPC Code used in High-Speed Optical Fiber Communication System." *Optics Communications*, vol. 346, 2015., pp. 99-105 doi:10.1016/j.optcom.2015.02.023.

⁸ Jan, Edwin. "A Protocol for Authoring Curricula for Technology Education. Diss. University of Manitoba.

Cable	Type	length	price
Optical Fiber	ST/ST single mode	100 feet	\$81.3
Coaxial cable	BNC-100	100 feet	\$30.41
Twisted pair cable	CAT5e	100 feet	\$7.99

Table 1 Compares the price of the cables

Coaxial cable is a networking cable usually used for cable TV signals. It has many layers within the internal conductor that encompass a tubular protection layer, surrounded by a directing shield. Coaxial cable transfers data using electrical signals, whereas fiber transfer data using light. The speed of this kind of cable is slower than the optical fiber, and the material inside the cable sends information slower than the optical fiber as well. Although coaxial cable is cheaper than fiber because “In fiber, the equipment cost is higher because it requires to get all signal formats on and off the fiber”⁹ (Babani, S., et al. 60). Also, coaxial cable is much slower than fiber, and therefore still not the optimum choice for networks.

The most logical choice would be to use twisted pair cable, as twisted pair cable is the customary choice for local area network (LAN). Often abbreviated as UTP for the unshielded twisted pair, UTP is composed of eight wires that have been twisted into four pairs. The twists reduce the crosstalk and electromagnetic enlistment, while contorted pair link is utilized by more established networks. The category of cable that will be used for this network design is CAT-5e. The CAT-5e is rated to 350 Mhz. CAT-5e has 100-

⁹ Babani, S., et al. "Comparative Study Between Fiber Optic and Copper In Communication Link."

ohm impedance and electrical attributes supporting transmissions up to 100 MHz.

According to Eastman, Mark, and Gregory K. Sherrill. "As described above, Cat 5e cable is an enhanced version of Cat 5 for use with 1000BASE-T (gigabit) networks, or for long-distance 100 Base-T links (350 m, compared with 100 m for Cat 5)."¹⁰ (2). Thus, the maximum distance length of CAT-5e cable is 100 meters.

CAT 5e which is officially called ANSI/TIA/EIA 568A-5 or just Cat-5e (the e stands for 'enhanced'), has parts composed of high-speed gigabit Ethernet, while CAT-5 segments may have a capacity to some degree in a gigabit Ethernet.

The improved electrical execution of CAT-5e guarantees that the link will bolster applications that require extra transmission bandwidth.

Also, this cable has a high-frequency signal for sending and receiving data.

According to the article "Twisted pair cable" by Siekierka, "A twisted pair cable which is exceptionally suitable for high-frequency signal transmission. One embodiment provides a twisted pair cable having two conductors with a foamed dielectric surrounding each conductor, and having a center-to-center conductor spacing at any point along a 1000 ft."¹¹ (1). Installation of this kind of link is easier comparing with optical fiber and coaxial cable. Also, this cable type has the lowest cost see Table 1 (page 14 for pricing information). The UTP cable has many characteristics comparing with other kinds of cable. For example, according to Engebretson "The UTP/balun method of analog CCTV transmission is a fast-growing segment of our industry. Distances up to 12,000 feet to a

¹⁰ Eastman, Mark, and Gregory K. Sherrill. "Category 5e compliant patch panel." U.S. Patent No. 7,354,316. 8 Apr. 2008.

¹¹ Siekierka, Thomas J., and Robert David Kenny. "Twisted pair cable." U.S. Patent No. 6,222,129. 24 Apr. 2001.

camera can be achieved; UTP cabling is lighter and easier to install than RG-59U, with UTP cabling being less expensive to purchase than comparable lengths of RG-59U.”¹² (Engebretson 65). Therefore, this network design will make use of this kind of cable.

4.2.2 Wireless

Wireless is used to depict media communications in which electromagnetic waves transfer the sign over part or most of the transmission path, so there is less need for cable. There are many advantages in wireless transmission when compared to wire. This includes the easy network installation with less time because "Wireless networks save money on cabling costs and are easier than wired networks to install, operate, and maintain (Tao, 2003)."¹³ (Brubaker 8). The wireless that will be used in this network design is (802.11). The 802.11 is an advance group of details for WLANs developed by a group working in the Institute of Electrical and Electronics Engineers (IEEE). According to the "A survey of quality of service in IEEE 802.11 networks." by Zhu, Hua, et al. "IEEE 802.11 is designed for best effort services only".¹⁴ (Zhu, Hua, et al. 6) Mobility is less limited, and it can provide wide coverage over a long distance. According to "Method and system for managing data traffic in wireless networks." by Juitt, David et al., "Such wireless network technology can provide LAN and/or WAN service to

¹² Engebretson, David J. Designed for Distance: Coaxial Cable, UTP Category Cable, Fiber Optic Cable--each can Work Flawlessly when Properly Planned and Installed, and each Technology Serves Different Distance Requirements, vol. 39, BNP Media, 2009.

¹³ Brubaker, Aaron T. "Faculty perceptions of the impact of student laptop use in a wireless internet environment on the classroom learning environment and teaching." Unpublished MS thesis, School of Information and Library Science, University of North Carolina, Chapel Hill, NC (2006).

¹⁴ Zhu, Hua, et al. "A survey of quality of service in IEEE 802.11 networks." IEEE Wireless Communications 11.4 (2004): 6-14.

enterprises' authorized users without wire installation and without tethering users to network connections." Thus, making use of wireless will be of great benefit to users of this network design. In this network design, different types of wireless are used as shown in the figure below.

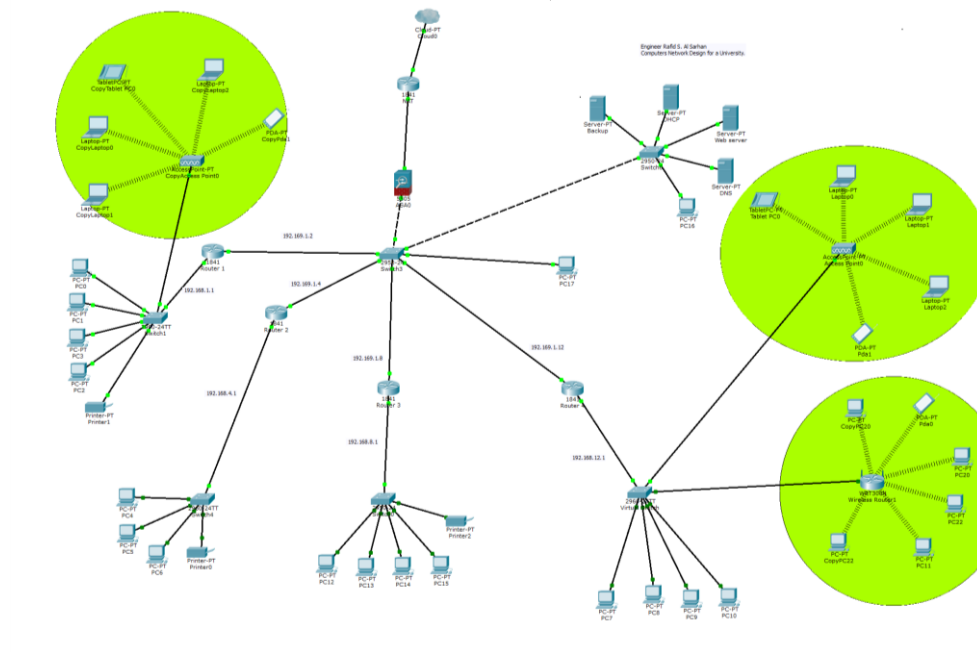


Figure 6 Different types of wireless is used

4.3 Connection Setup

The obvious way, given the constraints, to connecting devices together, all computers must be connected to switches then switches must be connected to the routers. After that, all routers connect to the last switch in order to link with edge switch, in which various servers such as DHCP server and DNS server are connected. The last switch is also connected to a firewall device. The firewall device links to the NAT router, and then

to the external networks or internet. The figure below shows the connection setup of all devices.

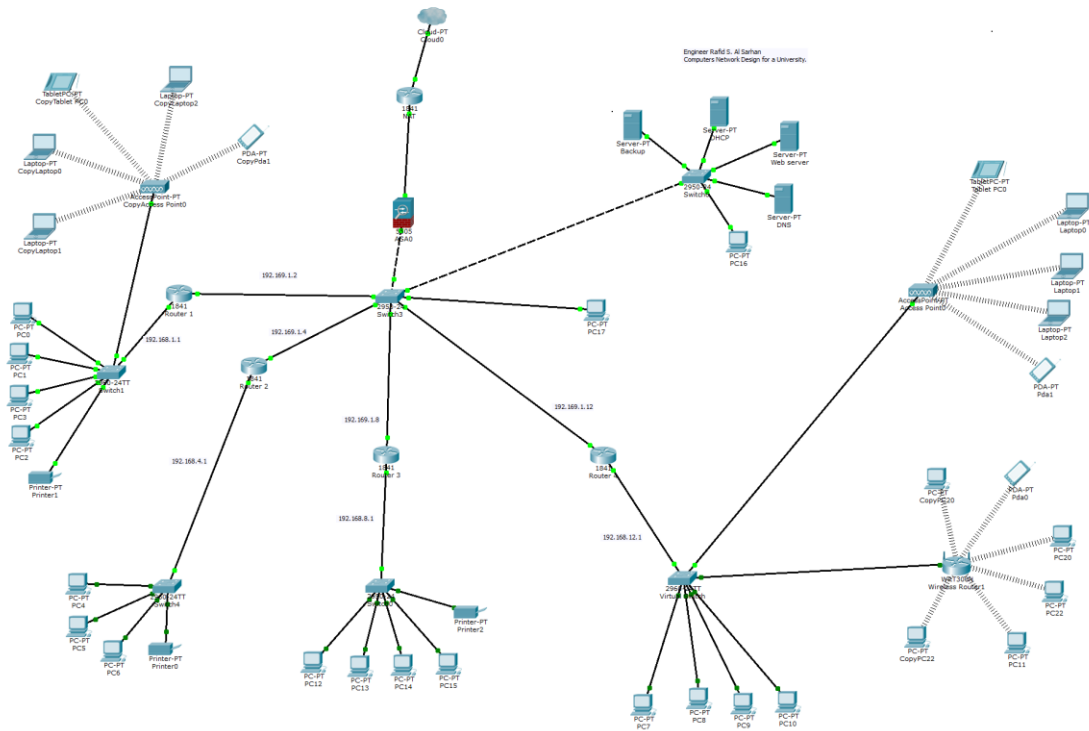


Figure 7 Integration network system

4.3.1 Ethernet Cable

Ethernet is a way to connect devices together that is usually used for installing connected Local Area Network(LAN). For connecting twisted pair cable between computers and Switches, each computer must have Network Interface Card (NIC). The cable used is UTP because it is the cheapest. UTP cable has eight wires inside of it. Each two wires are twisted with each other making it four twisted pairs altogether. Each wire

has a different color. The twisted pair of wire has two different colors. One of them is a solid color, and another one is striped color, as shown in the figure below.

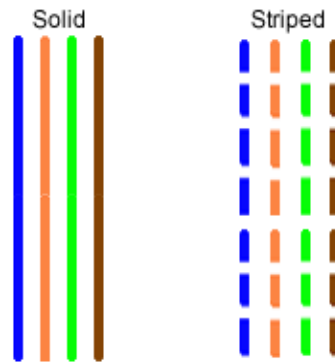


Figure 8 UTP cable Solid and striped

To connect the cable with Network Interface Card (NIC), the cable must first be connected with a Registered jack-45 (RJ45) connector. There are two standard ways to connect the wire to the RJ45. One of them is T568A standard or A, and another one is T568B standard or B. The figure below shows T568A and T568B.

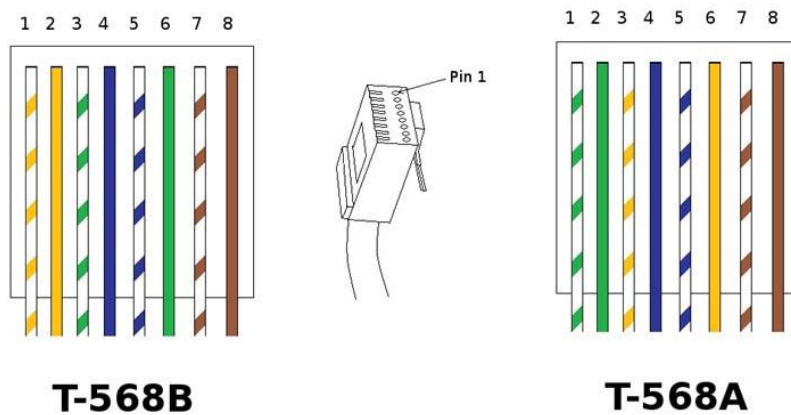


Figure 9 T-568B and T-568A

The T-568b standard is used on one side of the cable for connecting the wire to RJ45, and T-568A standard is used on another side of cable when the type of connection is a crossover. However, when connecting straight wired cables T-568B or T-568A standard, the cable must be connected to RJ45 from both sides. The cable for connecting a computer with a switch will utilize 10BaseT/100BaseT Ethernet using only two pairs of orange and green color. In other words, using pin number (1, 2, 3, 6) and other unused colors can be used for phone connection, or can be used as spare. However, other unused wires help the connected twisted pair to avoid noise on the connection.

There are three kinds of connection used for connecting devices together. The connection depends on the nature of device used. One of these connection is Ethernet crossover wired cables; another is Ethernet straight wired cable connection, and the last one is Ethernet rollover wired cable connection. However, the Ethernet crossover wired cable and Ethernet rollover wired cable connection will not be used for this network design because they do not have the required devices to connect each other.

4.3.2 Ethernet Straight Wired Cable

The straight wire cable usually connects different devices together. The devices use straight cables to connect the computer to the switches, the switch with the router, and server with the switch, etc. The figure below shows the devices connected by straight cable

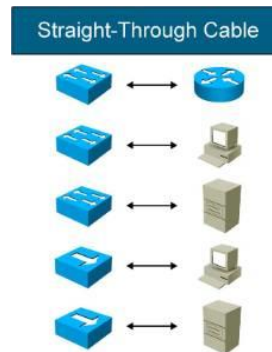


Figure 10 Devices connected by straight cable

In order to connect straight cable for both sides, each pin is connected to the same pin on the other side. For example, connecting pins (1, 2, 3, 4, 5, 6, 7, 8) to the same pins numbers (1, 2, 3, 4, 5, 6, 7, 8). The figure below describes a straight cable connection.

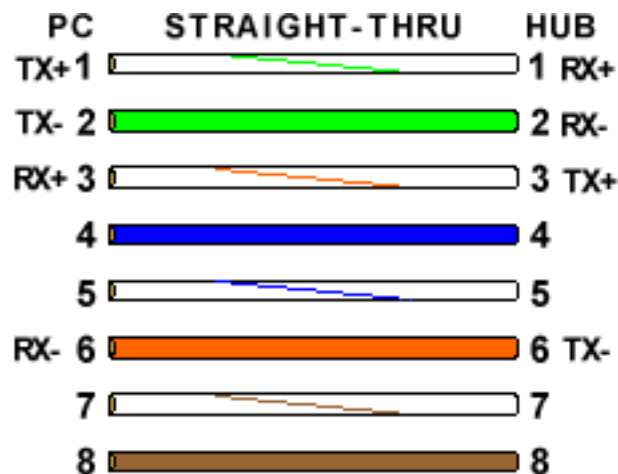


Figure 11 Straight cable connection

4.3.3 Wi-Fi

The Wi-Fi is one type of wireless communication device used for connecting to a network. It is imperative for daily life's communication. Wi-Fi signal must be made available to connect inside all buildings at the University. This is because all students and

faculties make good use of the Wi-Fi connection with their tablets, phones, and laptops, etc. The wireless local area network (WLANs) that will be used in this project network design is (802.11). The 802.11 is an advance group of details for WLANs developed by a group, working in the Institute of Electrical and Electronics Engineers (IEEE). The 802.11 is an open design, and it is also less expensive. According to Leung, Kin K., and B-J. Kim, Frequency assignment for IEEE 802.11 wireless networks, "In addition, the cost of 802.11 equipment is much lower than that for 3G equipment because of the simple and open design of the former networks, coupled with competition among WLAN vendors."¹⁵ (1)

All Wi-Fi devices must be secured by a password. The password prevents unauthorized user to connect to the Wi-Fi network. This is because the network could easily be hacked when it is open to all users, especially unauthorized users who can overcrowd the network, making it work very slowly. Also, a limited number of IP addresses that are reserved for the real users of the network can be taken by unauthorized users. To connect the wireless, Cisco access point is used, and at least one access point is installed in each building. The numbers of access point Installation depends on the size of the building. A Bigger building can have more than one access point installed in it. The access point usually makes use of the star topology network connection, as shown in the figure below.

¹⁵ Leung, Kin K., and B-J. Kim. "Frequency assignment for IEEE 802.11 wireless networks." Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th. Vol. 3. IEEE, 2003.

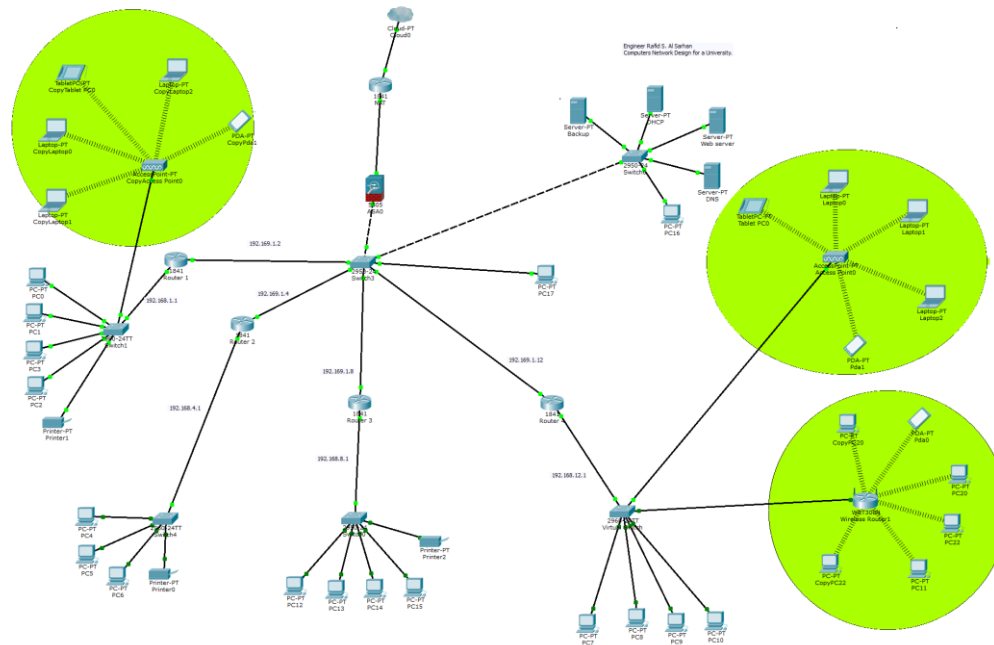


Figure 12 The access point is star topology

4.4 Devices Used

All devices to be used, such as routers, switches, servers, etc, in this network design, will be chosen from the Cisco company. This is because the quality of Cisco devices is much better than other devices. According to Cisco website, “With Cisco network systems, intelligent network services, such as quality of service (QoS) and encryption, are consistently supported and preserved across the entire network, enabling the same secure, high-quality service delivery regardless of whether the user is at headquarters or in a local branch.”¹⁶. The number of hosts to be used is 5075 for the network and is distributed among various sections or colleges in a university.

¹⁶ "Why Use Cisco Network Systems? - Cisco." Insert Name of Site in Italics. N.p., n.d. Web. 16 Nov. 2016.

The table below shows the numbers of IP address and hosts that will be used for each college at the university.

Subnetting Successful

Major Network: **192.168.0.0/19**
 Available IP addresses in major network: **8190**
 Number of IP addresses needed: **5075**
 Available IP addresses in allocated subnets: **7142**
 About **88%** of available major network address space is used
 About **71%** of subnetted network address space is used

Subnet Name	Needed Size	Allocated Size	Address	Mask	Dec Mask	Assignable Range	Broadcast
College of Engineering	700	1022	192.168.0.0	/22	255.255.252.0	192.168.0.1 - 192.168.3.254	192.168.3.255
library	700	1022	192.168.4.0	/22	255.255.252.0	192.168.4.1 - 192.168.7.254	192.168.7.255
College of Basic Education	450	510	192.168.8.0	/23	255.255.254.0	192.168.8.1 - 192.168.9.254	192.168.9.255
College of Arts	400	510	192.168.10.0	/23	255.255.254.0	192.168.10.1 - 192.168.11.254	192.168.11.255
College of Medicine	400	510	192.168.12.0	/23	255.255.254.0	192.168.12.1 - 192.168.13.254	192.168.13.255
College of Science	400	510	192.168.14.0	/23	255.255.254.0	192.168.14.1 - 192.168.15.254	192.168.15.255
College of Pharmacy	375	510	192.168.16.0	/23	255.255.254.0	192.168.16.1 - 192.168.17.254	192.168.17.255
College of Humanities	350	510	192.168.18.0	/23	255.255.254.0	192.168.18.1 - 192.168.19.254	192.168.19.255
College of Administration and Economics	300	510	192.168.20.0	/23	255.255.254.0	192.168.20.1 - 192.168.21.254	192.168.21.255
College of Nursing	300	510	192.168.22.0	/23	255.255.254.0	192.168.22.1 - 192.168.23.254	192.168.23.255
Union	300	510	192.168.24.0	/23	255.255.254.0	192.168.24.1 - 192.168.25.254	192.168.25.255
College of Education	200	254	192.168.26.0	/24	255.255.255.0	192.168.26.1 - 192.168.26.254	192.168.26.255
College of Law and Political Sciences	200	254	192.168.27.0	/24	255.255.255.0	192.168.27.1 - 192.168.27.254	192.168.27.255

Table 2 IP address used in the University

The design will need 13 Cisco routers, 100 switches, three computer servers, 20 access points, one firewall device, one backup device, one rack, 50 boxes of twisted pair cable, 150 boxes of RJ 45 connectors and approximately 5000 terminals.

The table below shows the equipment, quality, number of the device, price for each device, the price of quantity, and the total price of all quantity of equipment. All prices are taken from the Amazon website

Equipment	Quality	Numbers	Price for each	The price of quantity
IP address	192.168.0.0 255.255.224.0	8190	\$8	\$65,520
Router	Cisco Systems Gigabit Dual WAN VPN 14 Port Router (RV325K9NA)	13	\$229	\$2,977
Switches	Cisco SF200-48 SLM248GT-NA 48 10/100 Port 2 Combo Mini-GBIC Smart Switch	100	\$205	\$20,500
Access point	Cisco Aironet 340 Series 11Mbps Wireless LAN Access Point (Capt Antennas)	20	\$60	\$1,200
Servers	PREGDD-APLNC-K9 ¹⁷	1	\$ 16999.00	\$16,999
Rack	22U Network Server Rack Cabinet	1	\$ 537	\$537
Cable	1,000 ft bulk Cat5e Ethernet Cable / Wire UTP Pull Box 1,000ft Cat-5e Style Grey ~ VIVO (CABLE-V001)	50	\$ 41	\$2,050
RJ-45	Cybertech Cat6, Cat5e crimp connectors pack of 100	150 box	\$ 9	\$1,350
Firewall	ASA5505-SEC-BUN-K9 and unlimited users ¹⁸	1	\$ 645	\$645
Total price of all quantity of equipment's				\$111,778

Table 3 Shows price of devices used in the network

¹⁷ <http://itprice.com/cisco-gpl/PREGDD-APLNC-K9>

¹⁸ <http://www.cisco.com/c/en/us/support/security/asa-5505-adaptive-security-appliance/model.html>

5. Security

Due to the constant development of software programs which has led to the increase in the theft and the number of cyber security attacks, security has become important for all hosts on a network. Network security must protect all information and users supplied by a network. Security involves a pro-active prevention process to avert any danger or attack in a network. A computer administrator must be present in order to enforce the security of data access in the network. In terms of securing the network, there are three major aspects to consider. These include Infrastructure, Individual Systems/Components, and Individual Hosts:

5.1 Infrastructure

Infrastructure powers all functions on the network. They include all base devices in the network. When all base devices are protected, the network system will be secured. This is because the data passing from the outside of the local network must pass through those devices into the local network. The devices used for infrastructure in this network design are a virtual switch, back-up systems, firewall, and DNS.

5.1.1 Virtual Switch

A virtual switch or (vSwitch) is a software application that permits correspondence between virtual machines. A virtual switch accomplishes more than simply forward information bundles. It keenly coordinates the correspondence on a network by checking information parcels before moving them to a destination.

In this network design, the vSwitch is used between the access point and the personal computers as shown in figure 13. Virtual switches are generally inserted into an

installed software. However, they may likewise be incorporated into a server's equipment as a component of its firmware. A virtual switch is entirely virtual and can associate with a Network Interface Card (NIC). The virtual switch combines physical switches to a separate intelligent switch. This expands transmission capacity and makes a dynamic work amongst server and switches.

Virtual switches are also used for protecting networks system. Cisco switches have the ability to do the configuration. Usually, the switch has many ports. Each of those ports must be connecting to a terminal. In a normal way, all the terminal devices have the same network address; that is the 23.24 in the IP address 23.24.25.26 for the class B. However, when configuring the switch by virtual switches, the network address will be different from a terminal to another in the same switch device. For example, if one port has the IP address 23.24.25.26, the other one must be 23.25.25.26. Therefore, each port will have a different network IP address. This factor makes it difficult for a hacker to hack other devices when compromising the one device. Ultimately, a virtual switch helps to protect devices from hackers and also prevents hackers from accessing all devices.

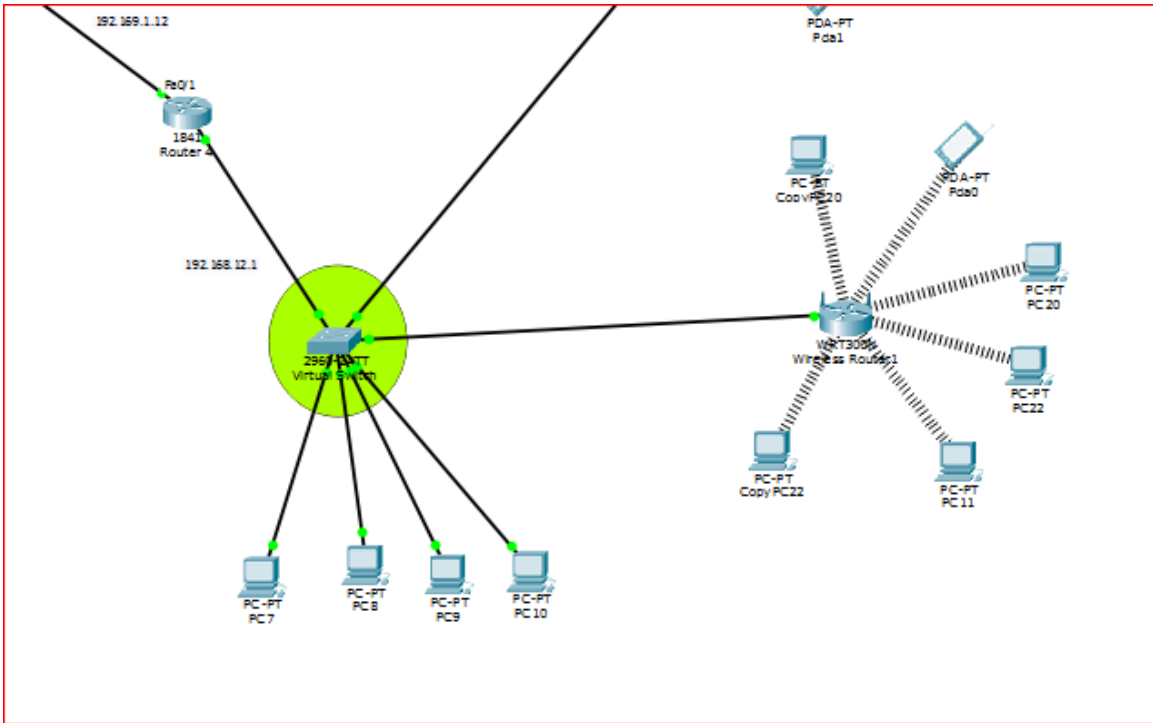


Figure 13 Virtual Switch

5.1.2 Back-up and Recovery.

Despite numerous security precautions that may follow to protect data, it is likely there may be the occurrence of any damage or distortion or loss of data. So, it is necessary to secure a way for which damaged, lost or distorted data can correctly provide a strong level of protection for the system to be restored. Backup creates duplicates, and this is a greater degree of protection. It is through creating backup copies saved both in the same workplace or another location, updated on a regular basis, that ensure the least amount of losses in the case of the original data loss. According to White, Paul

“Data Security: The Backup Backdoor”, by White “Backing-up data is essential for any business, in case the original information is destroyed. The very nature of back-up is to copy data from live

systems to contingency systems, whether they are secondary servers or storage mediums such as tape or optical. However, many organizations overlook the security vulnerabilities introduced by the back-up software, procedures and the location of the data, in their disaster recovery plans.”¹⁹.

However, backup device will be in the same place because of the financial limitation. Backing up of data depends on the degree of protection to be achieved, how to use the network, and as well as on the degree of importance of the data stored on the file server. The backup must determine what it should reserve as copy and when it should be copied. The figure below shows the position of the backup server in the network.

¹⁹ White, Paul. "Data Security: The Backup Backdoor." *Network Security*, vol. 2002, no. 2, 2002., pp. 8-9doi:10.1016/S1353-4858(02)00213-1.

The firewall consists of software and hardware. These walls act as a filter or strainer to check all connection attempts to the local network. It allows only useful and safe communication to pass through while prohibiting every other information perceived to be dangerous, such as viruses. If a network connects to the internet, it must connect to its firewall to protect the network from attacks and viruses outside that network. The firewall that will be used in this research will be “ASA5505-SEC-BUN-K9” (www.cisco.com)²⁰. This type of firewall provides an unlimited usage which will secure the local network from very large numbers of networks. The figure below shows the location of the firewall in the network.

²⁰ <http://www.cisco.com/c/en/us/support/security/asa-5505-adaptive-security-appliance/model.html>

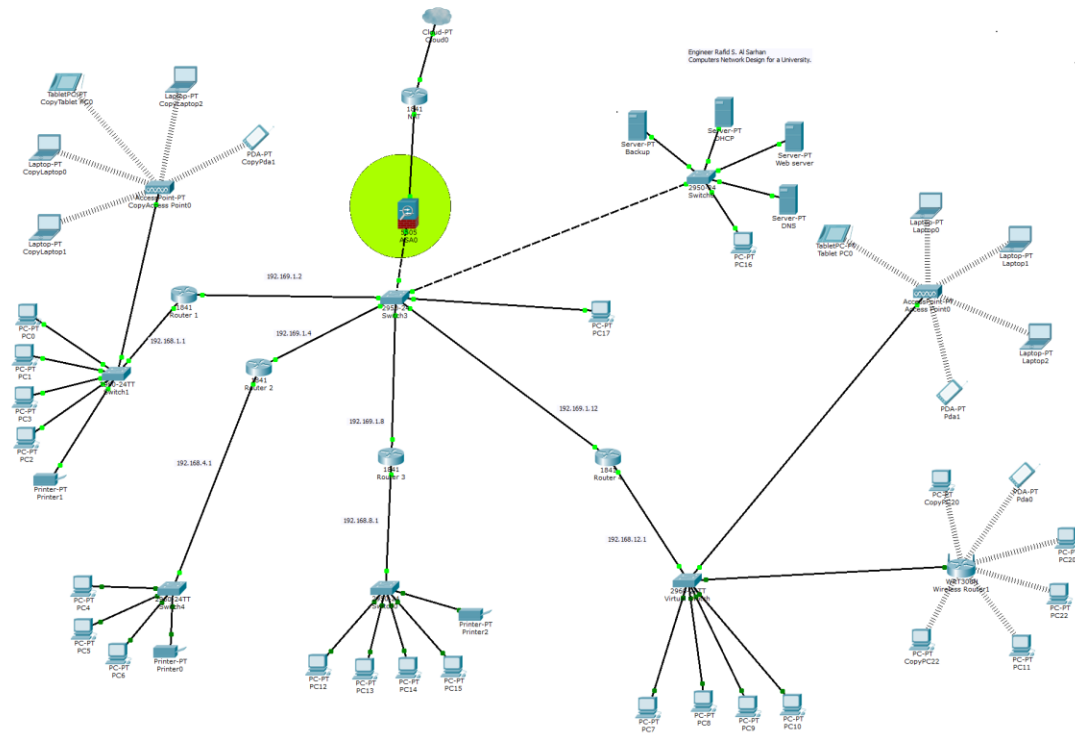


Figure 15 Firewall device

5.1.4 DNS

It is hard for people to remember numbers or the normal form of IP addresses easily. Human readable host name, be that as it may, are much less demanding to utilize, yet require a technique to take steps to the genuine address of the server or remote computer. The Domain Name System (DNS), was produced to direct local and Internet movement to the proper goal by performing real-time look-ups of Internet address with different DNS servers situated on the Internet. Prior to a local computer to sending a DNS server, it will ask the DNS server for the local network. Notwithstanding, the host's record contains pairings of IP addresses alongside one or more host names and is overhauled much of the time in light of predefined conditions on the local computer.

Prior to the creation of DNS, there was a solitary hosts file that was shared over the network. This solution did not scale.

DNS 'lookups' constantly occur on the Internet. The two most normal exchanges are DNS zone exchanges and DNS inquiries/reactions. A DNS zone exchange happens when the auxiliary server upgrades its duplicate of a zone for which it is definitive. The auxiliary server makes utilization of data it has on the zone, in particular, and verifies whether the essential server has a later form. On the off chance that it does, the auxiliary server recovers another duplicate of the zone.

A DNS reaction replies a DNS query. Resolvers utilize a limited rundown of name servers, generally not more than three, to figure out where to send inquiries. The main name server in the review is accessible to answer the question than the others in the rundown, and are never directed. For some reason when its inaccessible, every name server in the rundown is directed until one is found that can give back a response to the question. The name server that gets a question from a customer can follow up for the benefit of the customer to determine the inquiry. At that point, the name server can initiate inquiry from other name servers each one in turn, with every server directed being apparently nearer to the reply. The name server that has the answer sends a reaction back to the first name server, which then can reserve the reaction and send the reply back to the customer. Once an answer is stored, a DNS server can utilize the cached data when reacting to ensuing questions for the same DNS data. Reserving makes the DNS more productive, particularly when under the overwhelming burden. This proficiency pickup

has its tradeoffs. The most prominent are in security. Therefore, DNS will be used for safety in the network system.

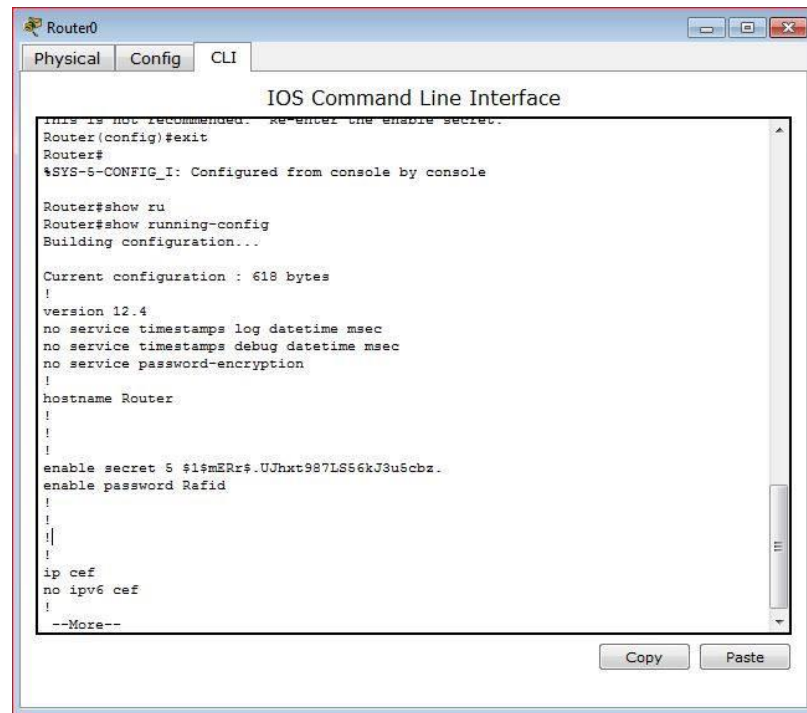
5.2 Individual Systems/Components

All devices in the network system must have a tool for security. This is because each device has an important data. When some devices in the network do not have any tools of security, that device will affect other devices in the network. This is because all devices are connecting to each other.

5.2.1 Encryption of Passwords.

Each host must have its own password for authentication control. This is the only authorization process to gain access to the information in the network. The password must be different from a device to another, depending on the user of the devices. However, for network devices such as routers and switches, the password is not enough for their security. The password for each device must be encrypted. The encryption of passwords or hashing of the password involves converting passwords to symbols. For instance, if a programmer wants to use a password such as 'Rafid', it will convert that name or word to a unique code such as "\$1\$mERr\$.UJhxt987LS56kJ3u5cbz". This is done so that no one can recognize the main password from the encrypted code. The reason for encrypting is that if a hacker or any other person gain access to one device, they cannot see the password of that device. This is because some people use the same passwords for all devices. In this case, the hacker will access all devices together by one password. However, even if the hacker gains access to one device, the encryption of the password will hinder them from seeing the original password. For this reason, encryption

will secure all devices on the local network. The figure below shows a password that is created and encrypted in the router.



```
Router0
Physical Config CLI
IOS Command Line Interface
THIS IS NOT RECOMMENDED. Re-enter the enable secret.
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ru
Router#show running-config
Building configuration...

Current configuration : 618 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
enable secret 5 $1$mERr$.UJhxt987LS56kJ3u5cbz..
enable password Rafid
!
!
!
ip cef
no ipv6 cef
!
--More--
Copy Paste
```

Figure 16 Password Creation and Encryption

5.3 Individual Hosts

The number of attacks in the world has risen today due to the constant development of sophisticated software. Each person or hosts must have his/her security to protect their data from hackers. Every host must secure their data from attack and protect their information from being stolen. For a professor preparing questions for an exam to administer to his students, should be able to assure the exam remains confidential on the network under consideration. If the exam questions are not private, all students will see the exam questions. This will cause a serious academic integrity problem. So, each professor must secure their data. Also, students must secure their grades and assignments

from other students. Security is very important in preventing others from seeing their personal information. There are many software to secure each host device such as anti-viruses, update and patching tools, basic support and server room.

5.3.1 Anti-Viruses Tools.

A Computer Virus is a small piece of programming code that insidiously attacks network systems and computer through infected, virus data files, introduced into a system by internet or flash memory. A virus program affects some files' system in the operating system or the performance of computer or device in the network. Some virus influences the system by copying itself in the system or by deleting some files in the operating system. For instance, when a virus copies itself inside the victim device system, it will affect the data operation process and the memory, making the device work very slowly.

The virus applications and other malicious programs also cause inconvenience to computer users by causing outages and breakdowns, thereby negatively impacting the services the computer can deliver. Malicious programs can become a network security problem when it attacks other hosts, or obtain and transmit personal information from users emails and other data stored in the device.

Each computer in the network must be protected by using appropriate programs to combat unwanted malicious programs. The antivirus will not allow viruses to be active in computers in the network in order to make the network become fully protected from threats.

5.3.2 Update and Patching Tools

All devices in the network are programmed by software such as operating system (OS). Over time, this software loses some characteristics which make it vulnerable to attacks. Sometimes, companies make software for devices. Then that company might want to develop that software or test to see if there are some problems with that software. If there is any problem with the software, the company will publish new or higher version of the software, usually with a patch to fix the old problems in order to make it more secure. The important thing that companies focus on is the security when updating the software to a new version. All devices in the network need a software update for the security of the network devices and data.

5.3.3 Basic Support

All universities have specialized technicians for managing the network devices. Universities in developing countries must have specialized technician for managing the network devices. Those specialists must have skills in networking. If they do not have experience, it will affect the whole network system. For example, when a device such as a router does not work or break down, and if a person does not have enough experience to fix that problem, it may affect the whole network. So, network technicians must take networking courses to gain enough experience on how to fix the problem of the network system.

5.3.4 The Server Room

All major devices (servers, routers, firewall, DNS...etc.) must be secured and be placed in the particular room. The devices must be placed in a standard way by putting all

devices in the rack (shown in figure 16 below) with a lock to become more secure. The rack will use 22U Network Server Rack Cabinet (see price in page 25). No one must touch the rack or even enter into the rack room except the authorized personnel who has permission for maintaining, installing, protecting, securing, designing, and monitoring network devices. This is because an unauthorized person who has experience of a network system can enter to that room, break the password for the devices, and hack all the networks system. This hacking can be done when the person plugs wire from a computer directly to any device.



Figure 17 standard rack for secure internet devices

6. Background Information On TCP/IP

6.1 The Internet Protocol (IP) Address

The internet protocol (IP) address is a 32-bit number. It is divided into two components. The first one is a network address, and the other one is a host address. The name of this division is called subnet mask or slash (/ + number) such as this IP

255.255.224.0/19 which has subnet mask (/19). When changing the subnet from decimal numbers (Human numbers) to binary numbers (Machine numbers), it will become 11111111.11111111.11100000.00000000. The numbers of "1"s in the previous example is 19. This operation is called subnet mask because the subnet mask is used to classify network address of an Internet protocol address by implementing a bitwise AND operation on the mask. The network bits in the Subnet Mask are indicated by all the "1"s, and the host bits are indicated by all the "0"s. In the network system, there are two bits which are reserved for the particular purpose such as "0" address and "1" address. The "0" address is not used for the host address because it is reserved for the network address, and the "255" address also is not used because it is reserved or allocated for the broadcast address. This subnet mask can be found in the third column of Table 4. (see page number 44). There are two ways to manage configuring the IP address for these computers: (1) Using DHCP (Dynamic Host Configuration Protocol) and (2) Static assignment.

6.2 DHCP (Dynamic Host Configuration Protocol)

DHCP allows each computer to get its IP address automatically from a pool of addresses with said pool being established by the network administrator and managed by a DHCP server. Companies and organizations use this kind of IP configuration most often due to the ease of setup. For example, according to Mentze “Most network devices available today default to dynamic host configuration protocol (DHCP). In many commercial environments, network devices are configured via DHCP and this default setting is maintained when the network devices are installed. In other commercial network environments, experienced network administrators override the default DHCP

and assign a static Internet Protocol (IP) address, subnet mask, and default gateway.”²¹

This kind of IP address may change over a period of time. The lease for DHCP configuration will be for seven days. When the computer requests an IP address, it must do so from a DHCP server device within the network. However, employing a DHCP server device increases the cost of the network. This protocol requires a server (hardware). A knowledgeable administrator is required to setup, operate and maintain that server. In the case of a large network, using a DHCP server is all but required since maintaining a static configuration would be counterproductive (see below).

6.3 Static Assignment

The second way to configure IP addresses on a client computer is through static addressing. This type of IP address is constant or static. This means that the IP address for that computer never changes. The alternative, static addressing, has inherent problems as computers rarely stay in the same network and rarely need an IP address 24 hours a day. When a computer has been assigned a static IP address, that address is permanently reserved; if that computer is powered off, that IP address is not available for use.

6.4 Classful Addresses

An IP address can be classified as classful or classless. The first octet, which is number 23 in this IP address 23.24.25.26 can determine the class of an IP address. The following table shows the range of numbers that can be in the first octet for each class.

²¹ Mentze, Duane, and David McAnaney. "Automatic networking device configuration method for home networking environments." U.S. Patent Application No. 09/969,248.

Class	Range in the first octet
Class A	0 to 126
Class B	128 to 191
Class C	192 to 223
Class D	224 to 239
Class E	240 to 255

Table 5 Range of IP address for each class

Notice that 127 is missing from the above table. This is a Class A number but is reserved for the loopback address. The loopback address is used to test the local NIC (Network Interface Card). The 127 loopbacks were designated by IANA in 1981 when the use of IP addressing was in its infancy. Unfortunately, IANA's decision to reserve a Class A number as the loopback wasted 16,777,214 possible addresses on the 127 network. This is why the IPv6 loopback wastes only one, and it is::1.

The class of a network will also determine the number of hosts. The following table summarizes the network and host numbers for each class:

Class	Networks	Hosts	Private address range
A	126	16777214	10.0.0.0 through 10.255.255.255
B	16384	65534	172.16.0.0 through 172.31.255.255
C	2097152	254	192.168.0.0 through 192.168.255.255
D			Not applicable
E			Not applicable

Table 6 Summarizes the network and host numbers for each class

Class A, B, and C addresses are frequently used while class D and E are not commonly used. This is because class D is for multicasting (distribution of information from one source to many receivers [such as cable television] or many sources to many receivers [such as group collaboration]) and Class E is reserved for research or government use.

As the above chart shows, Class A has few number of networks but a large number of hosts. Likewise, Class C has a large number of networks but few hosts. Class B, being in the middle of these two, has approximately the same number of networks and hosts. "Class A represented large national scale networks (small number of networks with large numbers of hosts); Class B represented regional scale networks; and Class C represented local area networks (large number of networks with relatively few hosts).²²" (Leiner et al. 26).

The downside of using Classful Addressing is the waste of host addresses. For instance, the proposed network only needs 19 number of networks and 8190 number of hosts. If Class C is used, there will be a waste of 532,668,418 addresses, causing more collisions on the network and more difficulty in managing the network. To counter this, the proposed network will use a classless addressing scheme.

6.5 Classless Addresses

Recall that an IP address can be classified as classful or classless. Classless addressing, otherwise called CIDR (Classless Inter-Domain Routing), is intended to

²² Leiner, Barry M., et al. "A brief history of the Internet." ACM SIGCOMM Computer Communication Review 39.5 (2009): 22-31.

assign IP addresses as efficiently as possible. Like Classful addressing, CIDR subnets also separate the network from the host, but this time the network portion of the subnet mask borrows bits from the host portion, allowing a division, of sorts of Classes A, B, and C. For instance, if an organization needs more than 254 hosts but far less than the 65,533 hosts that a typical Class B would allow, then this is not possible with Classful addressing. With Classless, an organization can choose anywhere between 254 and 65,533, allowing other organizations to use those addresses. Thanks to NAT (see Page 54), an IPv4 addressing scheme can be used instead of moving to an IPv6 scenario. One organization might need only 1000 IP hosts. With Classful, this organization would need to use Class B, wasting 64,533 addresses ($65533-1000=64533$). With Classless addressing (CIDR), this same organization can retain the use of IPv4 addresses and secure only what it needs, wasting no IP addresses. CIDR successfully tackles the issue by giving another and more adaptable approach to arranging addresses. Therefore, the Classless addressing system will be used for this research with IP address 192.168.0.0 and subnet mask 255.255.224.0.

7. Implementation

Implementation is the carrying out or completing of a network project. This paper will design a project involving a computer network that will be implemented in a developing country.

7.1 Personal Computers

The first step is to configure all the personal computers. Each personal computer must be connected to a switch. Each computer needs a unique Internet Protocol (IP) address (see page number 38).

The table below shows how IP address can be applied more efficiently by using Classless (CIDR) than with Classful. See page 42 for an explanation of how CIDR is expressed by using the slash (/) notation as shown in the third column below.

Allocated Size	Address	Mask	Dec Mask	Assignable Range
1022	192.168.0.0	/22	255.255.252.0	192.168.0.1 - 192.168.3.254
1022	192.168.4.0	/22	255.255.252.0	192.168.4.1 - 192.168.7.254
510	192.168.8.0	/23	255.255.254.0	192.168.8.1 - 192.168.9.254
510	192.168.10.0	/23	255.255.254.0	192.168.10.1 - 192.168.11.254
510	192.168.12.0	/23	255.255.254.0	192.168.12.1 - 192.168.13.254
510	192.168.14.0	/23	255.255.254.0	192.168.14.1 - 192.168.15.254
510	192.168.16.0	/23	255.255.254.0	192.168.16.1 - 192.168.17.254
510	192.168.18.0	/23	255.255.254.0	192.168.18.1 - 192.168.19.254
510	192.168.20.0	/23	255.255.254.0	192.168.20.1 - 192.168.21.254
510	192.168.22.0	/23	255.255.254.0	192.168.22.1 - 192.168.23.254
510	192.168.24.0	/23	255.255.254.0	192.168.24.1 - 192.168.25.254
254	192.168.26.0	/24	255.255.255.0	192.168.26.1 - 192.168.26.254
254	192.168.27.0	/24	255.255.255.0	192.168.27.1 - 192.168.27.254

Table 7 Subnet Mask

The IP addressing scheme for this research will use CIDR (Classless Inter-Domain Routing) with a Class B subnet. For instance, the IP address of the first device on a /22 network is 192.168.4.52 when using a subnet mask of 255.255.252.0. This will ensure that the IP addresses used by this research will not conflict with the university IP address scheme, thereby ensuring no overlaps in subnets. With Classful addressing, the subnet

mask of 255.255.0.0 can accommodate roughly 65,534 addresses. Since this research project only requires roughly 5,075 IPs, the major network address will be 192.168.0.0/19. This means the subnet mask of 255.255.224.0 will be used.

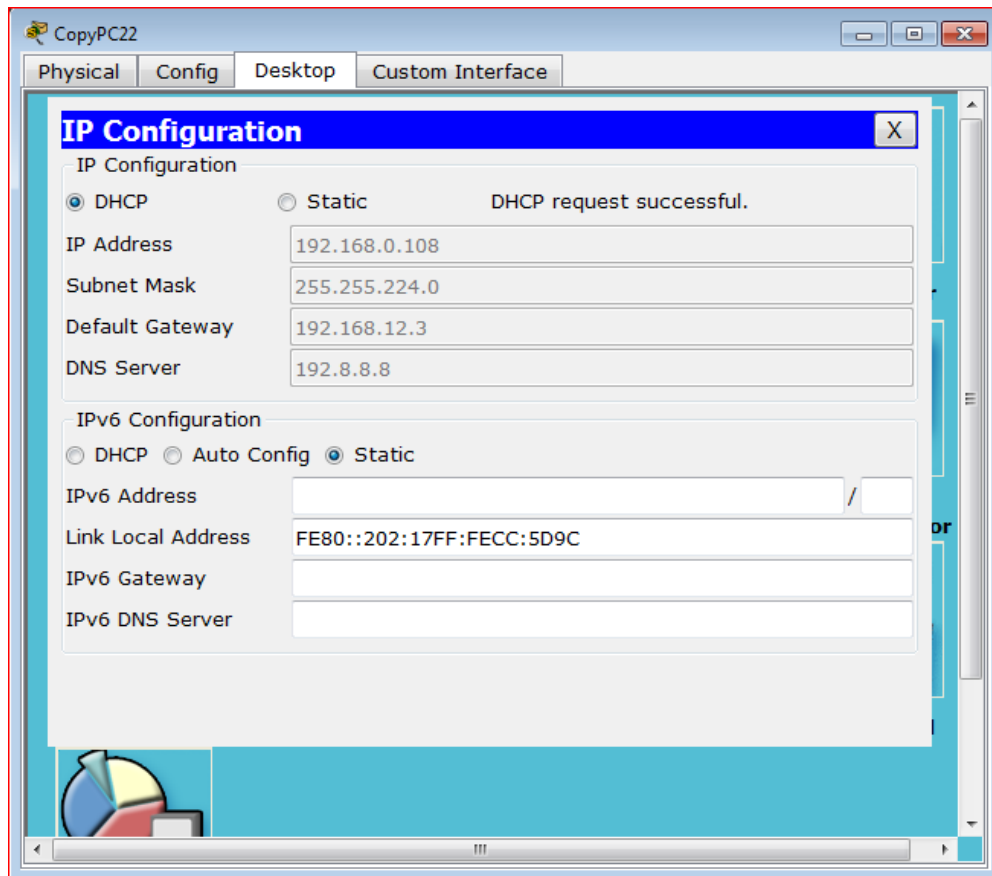


Figure 18 IP address in a personal computer

7.2 Switches

Switches are devices used on the network to transmit and receive data from one device to another or to many devices depending on the message intended. A switch provides the full bandwidth of the network to each port, thereby reducing collisions on the network. Switches also perform functions from the Data Link Layer (Layer 2 on the

OSI [Open Systems Interconnection] Model). If the switch also performs routing capabilities, then it is considered to be a Layer 3 switch. In strict terms, however, switches are Layer 2 devices. According to “Cisco router configuration” by Leinwand, “A Cisco switch is essentially a multiport bridge that runs the IOS. A switch, which functions at the data link layer, performs the same basic functions as a bridge.” (11)²³ Each switch will be connected to many personal computers. Most switches have a capacity of 16, 24, 32 or 48 ports. Rather than purchasing several switches with fewer ports, it would be less expensive to purchase fewer switches. This network will need a 48-port switch, so the Cisco (Cisco WS-C2960S-48TS-S 2960 48 10/100/1000 Port Gigabit Switch) switch would be a good choice for this implementation (see page 25 for pricing information). The name of each port is FastEthernet, and the numbering of ports begins at 0/1 and ends at 0/48. The personal computer connects from FastEthernet 0/2 to 0/48 while 0/1 will connect to the router. The Cisco switch is able to configure each port with a specific IP address, or a default will be provided by the router.

The virtual LAN will be used for connecting access point device from one side, and personal computers from another side. This helps to separate wireless from the personal computers in the network. The reason for this separation is that people outside the university will use external wireless devices. These personal devices may bring the virus to the network inside the university. Thus, isolating the wireless devices from the network will prevent viruses that come from any external wireless device to personal

²³ Leinwand, Allan, Bruce Pinsky, and Mark Culpepper. Cisco router configuration. Cisco Press, 1998.

computers inside the university. The following figure shows the switches' positions in the network design.

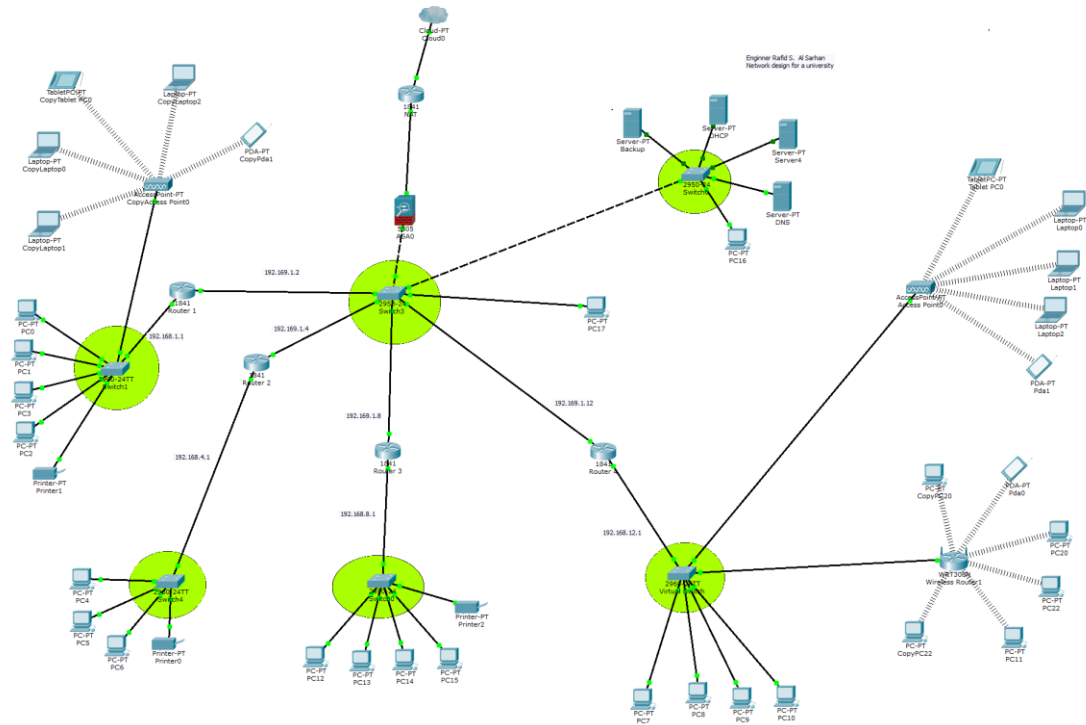


Figure 19 Switches in the network

7.3 Routers

A router is a networking device that forwards data packets between computer networks. The router chooses the best path to transfer data packets to their destination in the most efficient manner. Think of a router as a traffic cop at a busy intersection. This traffic cop makes determinations on which vehicles get through, which vehicles are not permitted on the path and the destination that the vehicles may take. The best kind of router for this endeavor is made by Cisco²⁴ because of its high standards of reliability and

²⁴ Id page 18

technical support. Since the proposed network must connect many computers to many switches, the router is an important component of the network. The router will control switches in a hyper-star topology and computer as shown in the Figure A below.

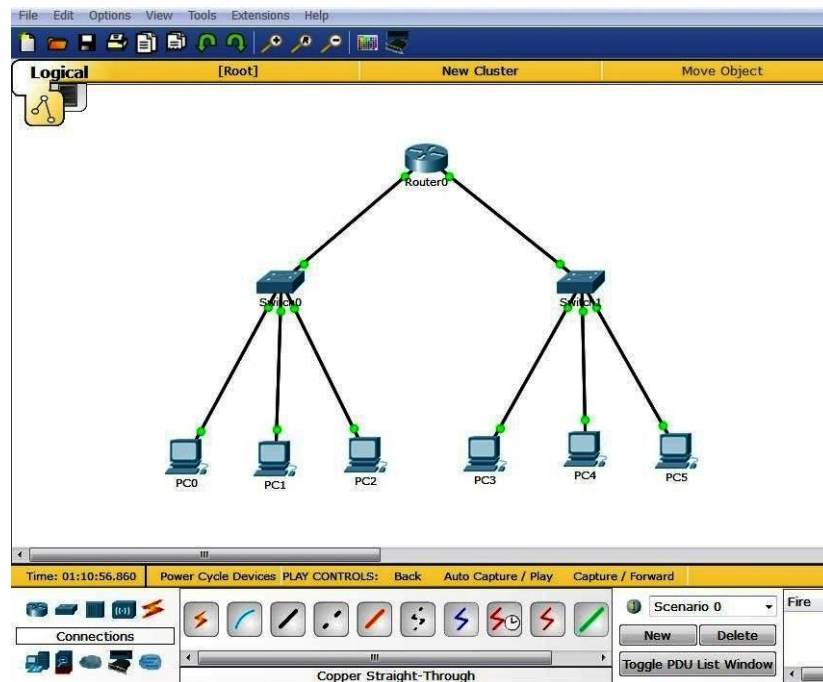


Figure 20 Hyper-star topology

The configuration of the Router starts with many steps. These steps are as follows:

Router>Enable

Router # Configure Terminal

Router(config)# hostname Router2

Router2 (config)# banner

In the first step, The **Enable** command must be entered to turn on privileged command mode (#). The second step is to enter the configuration mode by using **Configure Terminal** command. Optionally, to change the name of the router, the

hostname command is used. Also, comments are written on the router by using the **banner** command. These comments appear when the router starts configuration and also helps the programmer to figure out the exact router before entering into the router's configuration. When there are many routers, comments usually come in handy by making the router programmer's job easy in identifying each single router. After that, IP address can be configured for the network by using **IP address** command or **IP DHCP excluded-address** command. For static IP, the IP address command must be entered, then follow by the value of IP and subnets mask directly. Whereas, for DHCP a range of IPs must be entered. For instance, the range will be 192.168.1.2 to 192.168.1.200.

The IP address used for network design is Classless class B 192.168.0.0 and subnet mask 255.255.224.0. However, the IP address for the computers will start from 192.168.1.1. While connecting routers together, IP address 192.169.x.x. is used. For configuring static IP address, the following commands are used:

```
Router2# Configuration terminal
```

```
Router2 (config)# interface FastEthernet 0/0
```

```
Router2 (config-if)# IP address 192.168.1.1 255.255.224.0
```

```
Router2 (config-if)#no shut
```

```
Router2(config-if)# exit
```

For DHCP, IP address configuration for the following commands will be used

```
Router2(config)# interface FastEthernet 0/0
```

```
Router2 (config)# IP dhcp excluded-address 192.168.1.10 192.168.1.200
```

```
Router2 (config)# IP dhcp pool employ
```

```
Router2 (dhcp-config)# network 192.168.1.0 255.255.224.0
```

```
Router2 (dhcp-config)# default-router 192.168.1.1
```

```
Router2 (dhcp-config)# exit
```

While when configuring the router port with other routers' ports, the following commands are used.

```
Router2# Configuration terminal
```

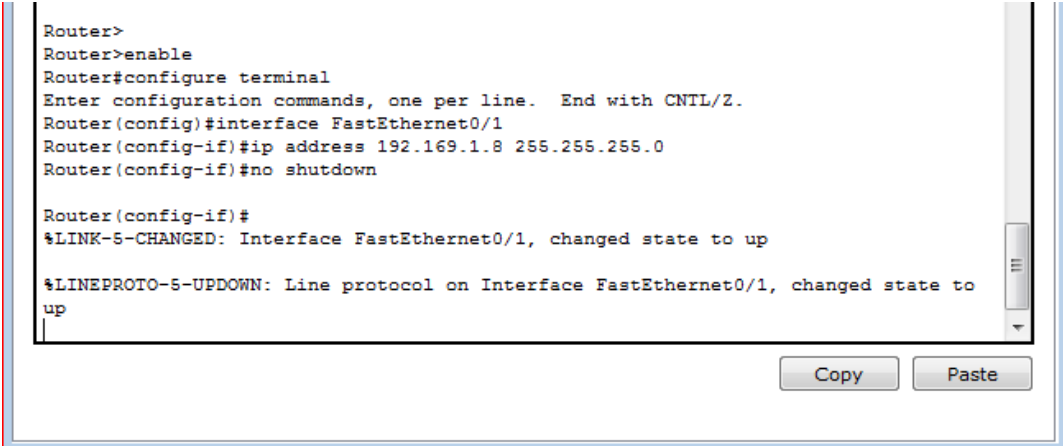
```
Router2 (config)# interface serial 0/0/0
```

```
Router2(config-if)# ip address 192.169.1.2 255.255.224.0
```

```
Router2(config-if)#no shut
```

```
Router2(config-if)# exit
```

The figure below clearly shows the Routers configuration



```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 192.169.1.8 255.255.255.0
Router(config-if)#no shutdown

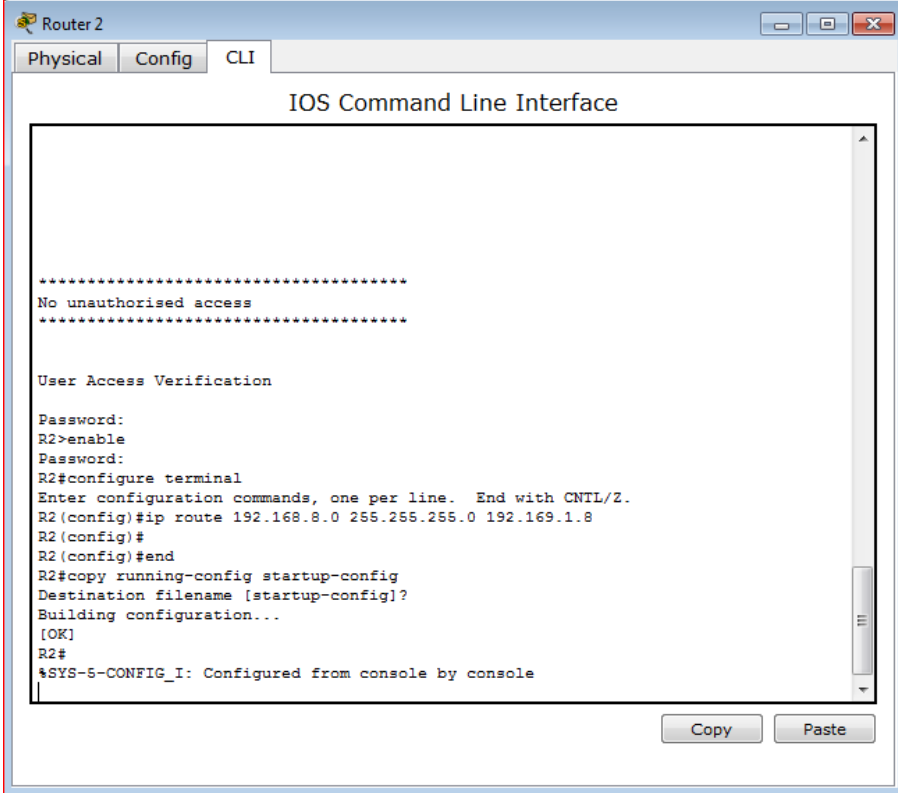
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
```

Copy Paste

Figure 21 Routers configuration

Static routing is a kind of routing that occurs when a router uses a physically configured routing entry, as opposed to information from a dynamic routing traffic.

Information will not pass through the router to outside the network until the router is configured as a static route. The figure below shows the static route configuration.



```
Router 2
Physical Config CLI
IOS Command Line Interface
.....
No unauthorised access
.....

User Access Verification

Password:
R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip route 192.168.8.0 255.255.255.0 192.169.1.8
R2(config)#
R2(config)#end
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 22 Static route configuration

The router is an essential device on the network. It manages the IP address of the computers and also controls all computers connected to it. The information inside the router is very significant. Router is encrypted with a password request which is paramount because it must always be secured in order to prevent unauthorized access. The first step to configuring the password on the router is by using **Enable Password** command, then inputting the desired password thereafter. However, this password is not yet encrypted. To encrypt the password, the **Enable Secret** command is entered with the

Router# Configuration terminal

Router(config)# line console 0

Router(config-line)# password cisco

Router(config-line)# login

Router(config-line)# exit

Furthermore, the router has another port called VTY port, which stands for Virtual Teletype. This port is a standard name for telnet and SSH connection. The range of VTY port starts from 5 to 1000. Five initial ports i.e. port 0 – 4, are enabled for VTYs connections. The following commands show how to protect the VTY port by password.

Router(config)# line vty 0 4

Router(config-line)# password cisco

Router(config-line)# login

Router(config-line)# exit

The auxiliary port also needs password protection. The Auxiliary port is the remote access to the router. According to the article “Cisco router configuration” by Leinwand, “These modems may be either integrated into the product, as with the Cisco AS5200 AccessServer and 3600 routers, or attached externally, as with the 2511 AccessServer and the auxiliary port of most Cisco routers. Figure 4-9 shows a typical dial-up scenario for a remote workstation user accessing a network via an access server

with external modems."²⁶. The auxiliary port on this model must also be protected; the following commands will enable that:

Router(config)# line aux 0

Router(config-line)# password cisco

Router(config-line)# login

Router(config-line) # exit

7.4 NAT System

NAT is the last router device in the local area network that is directly connected to the external networks (Internet). NAT stands for Network Address Translation. It is a software tool that translates numerous private IP addresses from the LAN to one public IP address that is required for access to the Internetwork (Internet or WAN: Wide Area Network). According to Srisuresh, Pyda, and Matt Holdrege "Traditionally, NAT devices are used to connect an isolated address realm with private unregistered addresses to an external realm with globally unique registered addresses."²⁷(1). This allows a single public IP address to be used for multiple hosts within a LAN, thus saving precious public IP addresses. It is NAT that has allowed IPv4 to operate beyond the end of its normal address range. A NAT router is a good example of the virtualization of Internet Protocol (IP) addresses. It also decreases the number of IP addresses for any network. NAT operates at the Transport Layer in OSI Model.

²⁶ Leinwand, Allan, Bruce Pinsky, and Mark Culpepper. Cisco router configuration. Cisco Press, 1998.

²⁷ Srisuresh, Pyda, and Matt Holdrege. "IP network address translator (NAT) terminology and considerations." (1999).

The NAT router has a table for saving IP addresses and port numbers. When the host in the local area network requests data from the Internet and has an IP address such as 12.13.14.15, the IP address of the host will be saved in that NAT table with a port number such as Port 51383. Then NAT changes that IP address to the public IP address such as 20.19.18.17, with the same port number. When data comes back from the Internet, NAT will return the IP address from public with the port number (20.19.18.17:51383) to the private address and port number combination that requested the data, such as 12.13.14.15:51383. This operation makes information arrive safely to the exact host which requested the information from the Internet. This process is named Port Address Translation (PAT).

NAT also helps improve the security of the network by adding an additional layer between intruders and hosts. This is because the external users of the local network cannot see the private IP addresses inside the local network. Instead, it only sees one IP address which is public. Each computer inside the network has its own IP address which allows each host to see the other hosts. Thanks to NAT, it is possible to conserve the supply of 'public' IP addresses.

NAT configuration can be classified as Static NAT, Dynamic NAT, and PAT NAT. Static NAT uses one-to-one address mapping. It also gives each host an IP address. While dynamic NAT uses many-to-many address mapping, it still also uses one-to-one addressing as well. Dynamic NAT gives each host a unique IP address. NAT PAT uses many-to-one address mapping where all hosts on the local network get only one IP

address from the NAT router. For this design, NAT PAT will be utilized. The configuration for NAT PAT will be as follows:

Nat inside local network

```
Router (config) # interface fa0/0
```

```
Router (config-if) # ip nat inside
```

```
Router (config-if) # exit
```

Nat outside local network

```
Router (config) # interface fa0/1
```

```
Router (config-if) # ip nat outside
```

```
Router (config-if) # exit
```

Translated network

```
Router (config) # ip access-list standard clint-list
```

```
Router (config-std-nacl) # 192.168.0.0 0.0.31.255
```

Nat overload

```
Router (config) # ip nat inside source list clint-list interface fastethernet0/1 overload
```

7.5 Wireless Access Point

An access point is a wireless service device used for networks. Wireless access point service plays a significant role in this design and is very important for educational institutions. The universities must have a wireless network available. This is because it is an important part of communication in education. Students, staff, and faculty make use of wireless services such as the Internet for their laptops, printers, tablets, and smartphones, in a bid to support effective learning and better communication. Also, wireless service

has many advantages in a university setting. One of this is the low-cost effectiveness, and another is the very broad coverage area of service it offers. “According to Swett (2002), more than 90% of public universities and 80% of private universities in the US have some level of mobile wireless technologies, such as mobile wireless devices and networks. One such institution is Louisiana State University (LSU), which implemented Cisco CTE 1400, an application enabling the transformation of the web page into a format appropriate for mobile wireless devices.”²⁸. The access point device must be connected to the router by cable, as shown in the figure below.

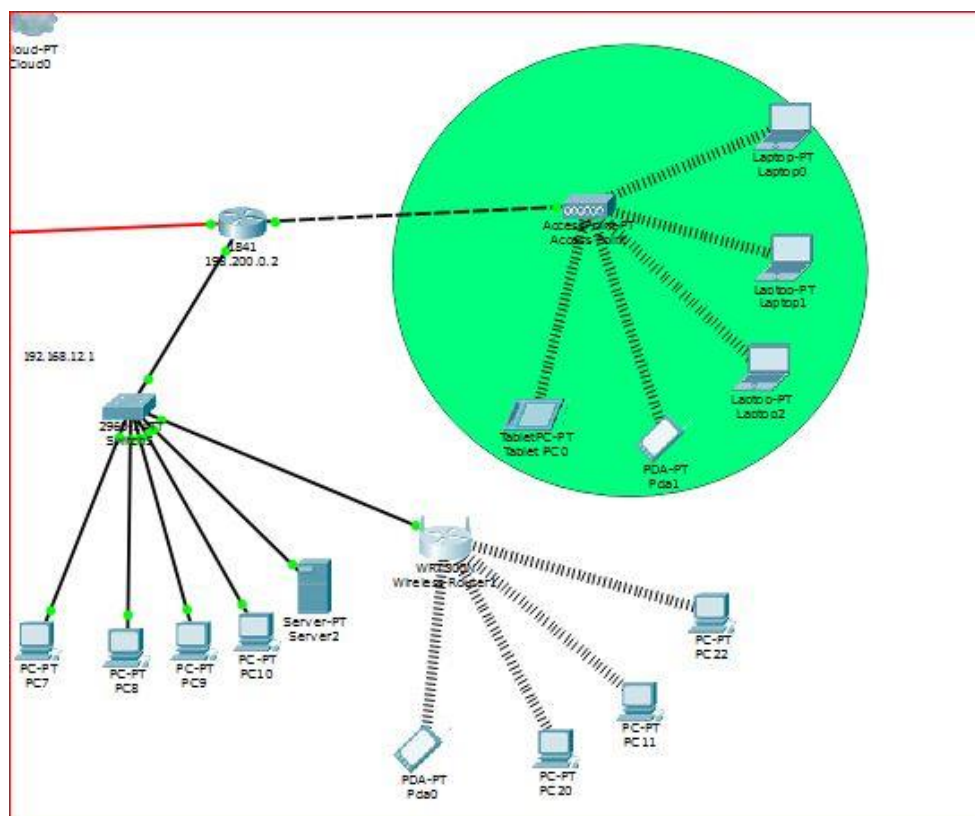


Figure 24 Access point connected with the router

²⁸ Kim, Sang Hyun, Clif Mims, and Kerry P. Holmes. "An introduction to current trends and benefits of mobile wireless technology use in higher education." AACE journal 14.1 (2006): 77-100.

For this configuration, access point device is connected to the router. This network configuration will also make use of classless class B. The IP address for fastEthernet0/0 line in the router is 192.168.12.1, and fastEthernet0/1 is 193.168.12.1. The subnet address is 255.255.224.0 because classless class B will be used for this design. The figure below shows the configuration of the router.

```
Router>enable
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.12.1 255.255.224.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fastethernet 0/1
Router(config-if)#ip address 193.168.12.1 255.255.224.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#
Router#
```

Figure 25 configuration IP addresses in the router

The Access point devices connect to the router directly. Each access point device is placed in an area to distribute the internet for that particular area. The configuration of the access point is very easy. The first step in the configuration of an access point is inserting the access point name to know which access point is to be used. The name entered in the SSID field is used to identify the network, as shown in the figure below.

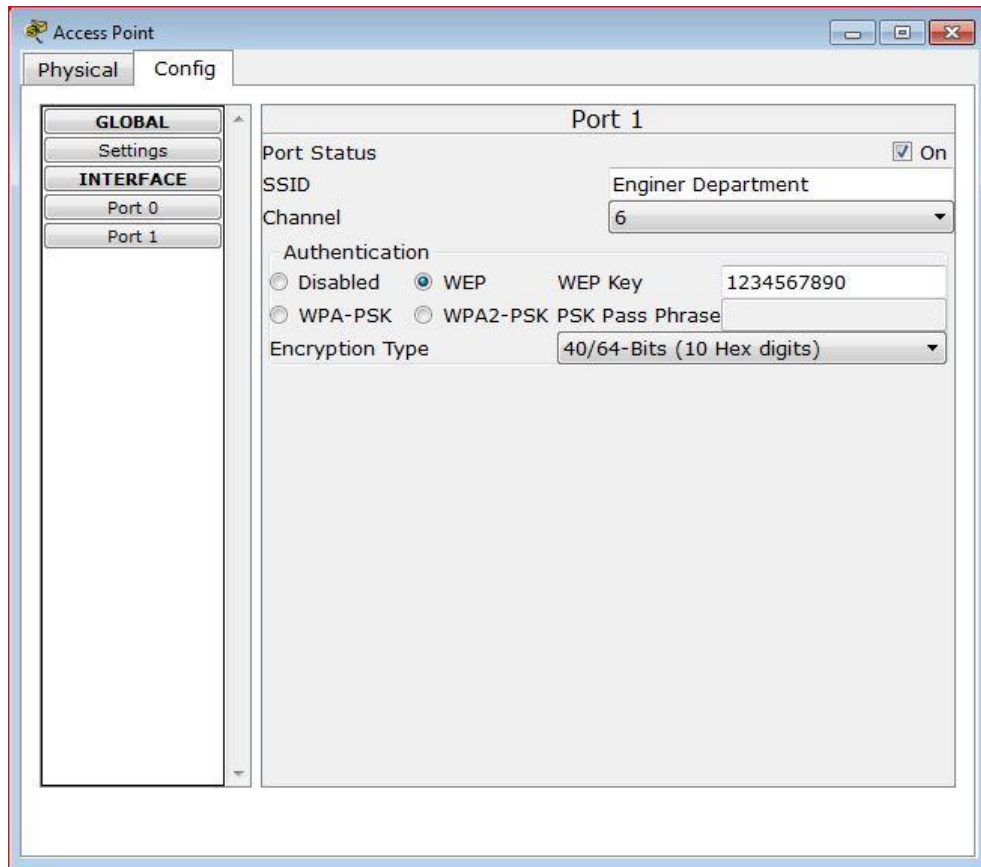


Figure 26 Configuration Access point

After that, each access point must be protected by password and also have encryption enabled. The key prevents an unauthorized user from connecting to the network. They will use their laptops or any smart devices to connect to the access point by changing their configuration settings. For example, to connect a laptop computer to the access point, the SSID of the laptop must be changed to the same SSID of the access point. Then put IP address for each computer on the same network, or to the same network used to connect the access point to it. The router IP is 192.169.12.1, while

computer IP address is 192.168.0.118. The image below shows the configuration IP address of one of the laptop computer.

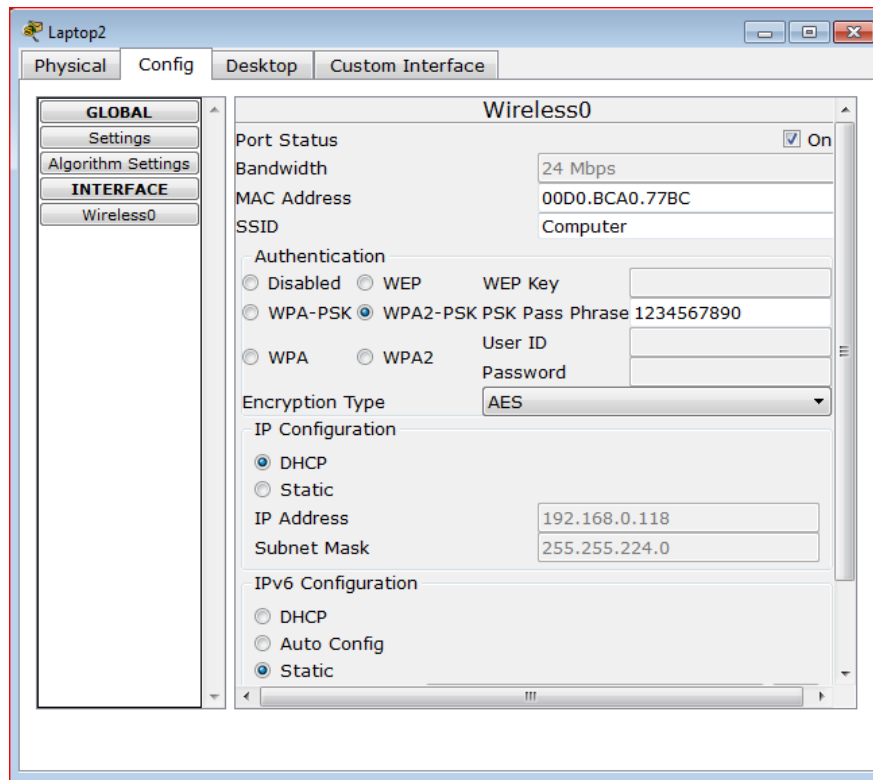


Figure 27 Configuration IP address of a laptop computer connect to the access point

7.6 Servers

The term server refers to a device or a computer program that supports other devices or programs which are called clients. This is known as the client-server model; one server can support many clients and can give different functionalities or characteristics to different clients.

The cost of purchasing many servers is very high, and institutions in developing countries cannot afford such high-priced systems. According to Jan, "The server is

usually the most expensive computer on the network.”²⁹ (26). As a result, few servers will be used for this project’s network design. The few servers that will be used in this project are DHCP server and DNS server.

7.6.1 DHCP Server

Dynamic Host Configuration Protocol (DHCP) server will be connected to the switch device in order to connect to many computers. Each computer that is connected to the network needs an IP address. The DHCP will distribute the IP address to each computer (see page 39). Cisco DHCP server is used because it is easy to configure the DHCP device using packet tracer simulation program, as shown below in figure below.

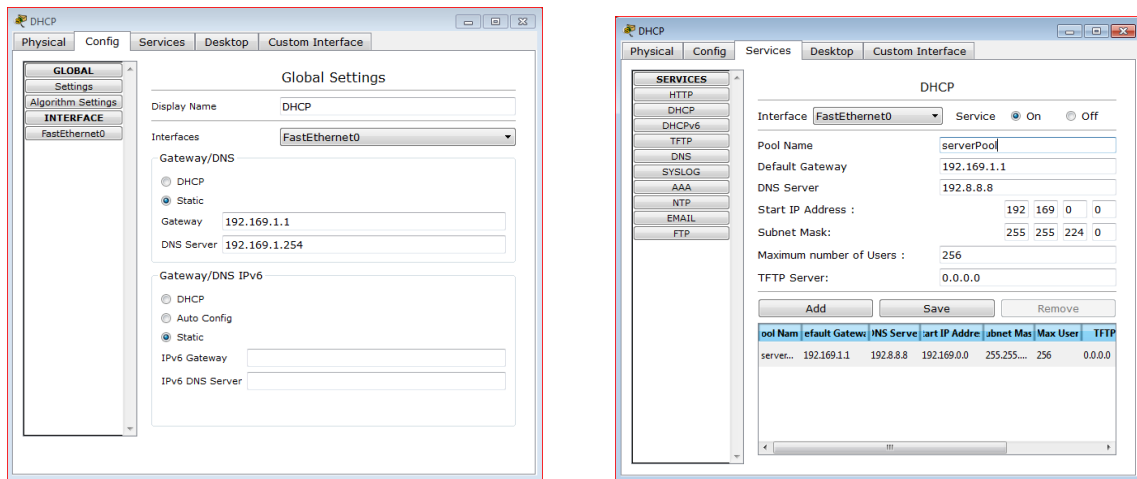


Figure 28 DHCP device configuration

After configuring DHCP server, all hosts on the local area must change the IP configuration option from static to DHCP to get the IP address automatically. The figure 18 shows how a computer gets IP address from DHCP server.

²⁹ Idel page 11.

7.6.2 DNS Server

The Domain Name System (DNS) is a server service that maps a domain name to IP addresses. DNS server translates a domain name to the IP address. IP address contains 32 bit. Since people cannot easily memorize all numbers of IP addresses, it is easier for them to memorize domain names of IP addresses. For instance, it is easier to memorize “www.Cisco.com” website, but difficult to memorize the IP address “72.163.4.161” for requesting Cisco site. It is easy for a computer to understand numbers, and in reverse to a human who prefers text to the numbers. For example, when a user requests “www.Cisco.com” page, the computer host does not understand the request “www.Cisco.com.” The Computer needs to know the IP address of “www.Cisco.com” site. The Computer host will send a request to the DNS servers to request the IP address of the Cisco site. The DNS server will then translate “www.Cisco.com” to “72.163.4.161”. With this, the computer host can get information from the Cisco site.

If a network does not have DNS servers, making use of computers in surfing the internet will be complicated. Humans have to memorize all IP address, or must make a note for each IP address. Without DNS servers, the internet will be very much complex or nearly impossible to use.

The DNS server will be connected to the switch then to the router. The IP address for the DNS server must be static, and IP address used is 199.8.8.8. The configuration of the DNS server is shown in the figure below.

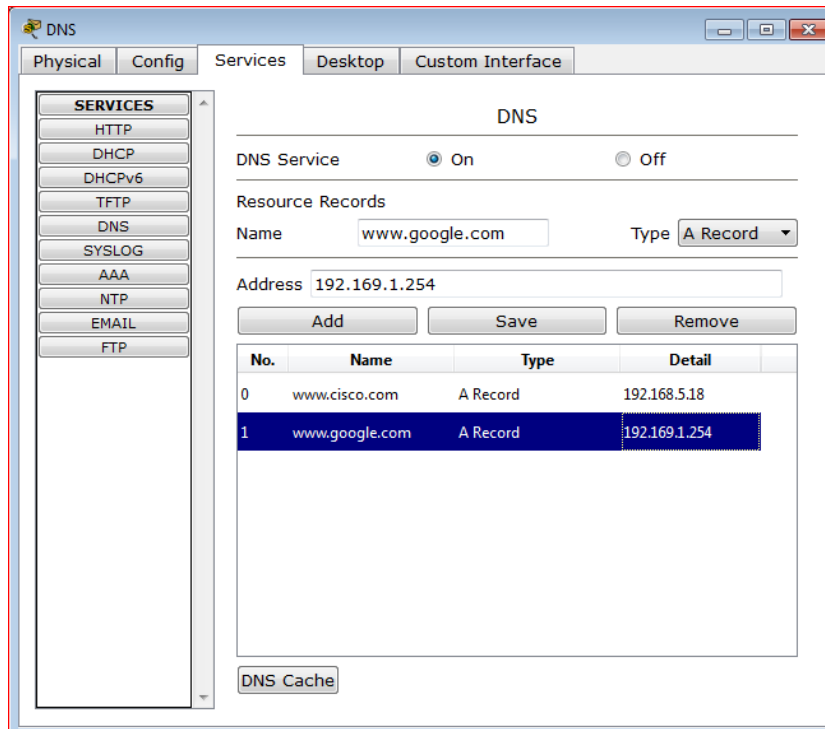


Figure 29 DNA configuration

DNS can be obtained from any personal computer. The figure below shows “www.google.com” DNS obtained from a personal computer.

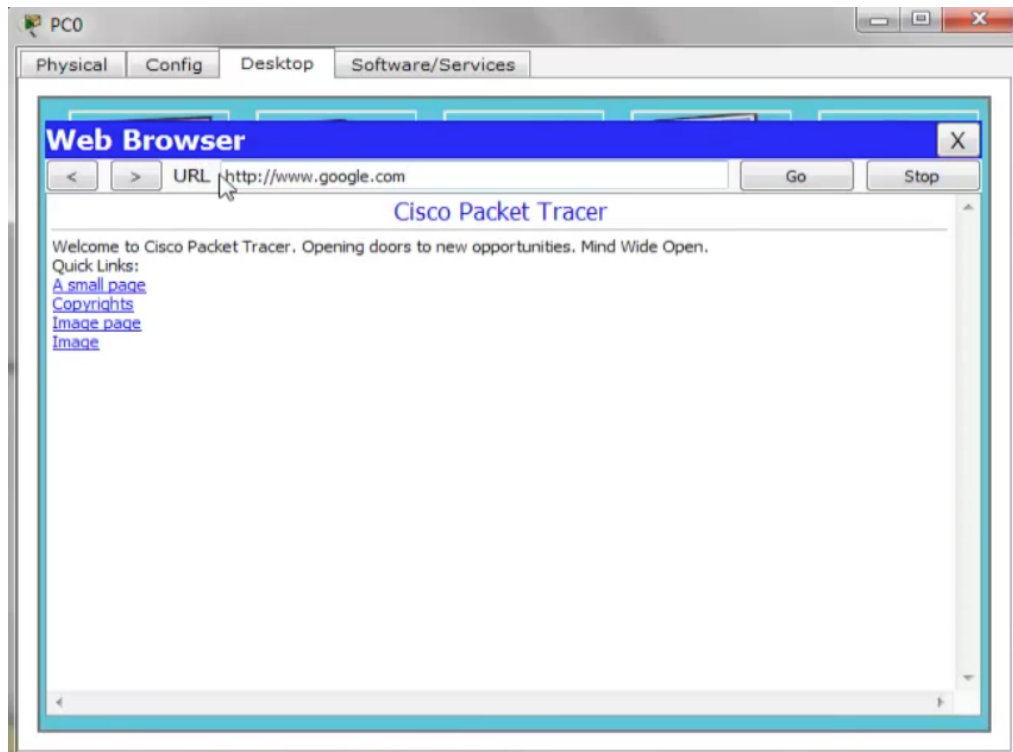


Figure 30 Check DNS from a personal computer

8. Expectations and Ongoing Challenges, Options, And Possible Future Evolution

An operating network will face challenges over its lifespan. One big challenge this design will face is economy problems. This is because a key requirement has been cost on making reduction suitable for developing countries. As a result, robust materials and less numbers of complex devices such as servers will be used. If there are improvements in the economy later in the future, the network materials and a number of devices used will be upgraded or extended. For example, in the future, more servers can be added to the already existing three servers as a form of system-wide upgrade. Furthermore, more than one backup device can also be added to save the network's data.

Accordingly, it is necessary to include room for future development plans. For instance, this project's network design has an extra number of IP addresses for the future. The network needs 5075 hosts while it has 8190 hosts. In the future, the universities in developing countries can connect 3115 additional hosts which can be included without exhausting available and IP address.

A number of issues and scenarios that should be considered.

8.1 Quality of Devices

The quality of the network device is vital for the network. When the device has good quality, the number of issues in the network will be reduced. Cisco company is known for their good quality network devices. According to Cisco website "With Cisco network systems, intelligent network services, such as quality of service (QoS) and encryption, are consistently supported and preserved across the entire network, enabling the same secure, high-quality service delivery regardless of whether the user is at headquarters or in a local branch." As a result, all devices used for this research are Cisco devices, such as routers, switches, access point, servicers, and firewall. One reason for patronizing Cisco devices is for the high protection service that its devices provides, which will be of high relevance to important information of the University. It is important for a network to continue working all the time and should never stop for any reason. A network failure can cause a disruption of academic activities. All staff, professors, and students need the network most of the time. For example, if a network stops for any reason, the students cannot submit their assignments, exams can be halted, and every other student academic activities that make use of the network will be stopped. Also,

professors will not be able to attend online class sessions until the network starts working again. Cisco devices are very strong at withstanding such network failures. Therefore, using Cisco devices will minimize possible network failures for this project's network implementation.

8.2 Backup

As a form of best practice, organizations and companies always place Backup server offsite. A backup system is a mechanism for storing data in the network, allowing restoration and recovery if needed. Those data in the backup are updated periodically depending on how the backup schedule is configured. The data stored in this platform are very important and must be protected from any loss. To protect these data, more than one backup server is strongly preferred, and the location of the backup server must be far away from the location of the original data. However, the cost will be high when the backup device is placed in another location. If a budget allows, more than one backup server devices and the backup server will be placed in other continents, separate from the location of the local area. As an extreme example, if the local area network is in the Asian continent, the backup device can be placed in another continent such as the North or South America continent, or the Australian continent. This is because if natural disasters such as earthquakes, floods, hurricane, volcanoes, etc. occur in the location of the local network, the backup data will not be affected since its location is far away from the disaster.

8.3 Evolution/ Optional Additions

Budget plays a significant role in the design of the network in terms of quality,

device selection, and network security. The budget for this network design is limited (see page 5). When the budget is limited for designing the network, the designer must utilize specific devices that the available budget can afford. Therefore, if the budget is high, devices that will be used includes optical fibers, firewalls, backup devices two networks for security and many servers.

8.3.1 Optical Fiber

Optical fiber cable is a medium for transferring information. This kind of cable is more expensive than other cable types, less noisy than twisted pair cable, faster, and mostly used for long distance transmissions. According to the “However, from around 2005, we began to develop the continuous extrusion method in earnest, and by 2008 succeeded in 40-Gb transmission. This was the world’s fastest transmission speed, surpassing the GI-type silica optical fiber. We achieved these results through joint research with Asahi Glass.”³⁰(Koike XI) Optical fiber require a special fiber optic technician for fixing any issue facing the cable. Since universities in developing countries have a limited budget, they cannot afford to use this cable. However, if these universities have a good budget plan, optical fibers will be their best bet due to its high qualities.

8.3.2 Firewall

Budget impacts greatly on the security of a network. If the budget is favorable, two firewalls devices will be used and placed between LAN and WAN. This is because if one of the firewalls breaks down, the other one will continue to work without affecting the network. However, making use of two firewalls requires special timing configuration in

³⁰ Koike, Yasuhiro. Fundamentals of Plastic Optical Fibers, Wiley-VCH, DE, 2015;2014;.

the OS because each firewall works differently in a timely manner. For example, when two Firewall is connected, one of them must function as spare. There are two ways to connecting two firewalls. The first one works automatically. This kind of connection is named Active-Active. When the first firewall breaks down, the OS automatically gives notification to the second or spare firewall to start working in replacement of the first firewall. Also, According to Jiang, Dongyi, et al. "Techniques are described to enable two or more layer two (L2) firewall devices to be configured as a high availability (HA) cluster in an active-active configuration."³¹ (1). Thus, high availability (HA) involves the configuration of connecting two firewall devices together.

The second way for connecting two firewall devices is called Active-Standby. This sort of connection is less expensive than the first one. When the firewall breaks down in this connection, a technician manually replaces the failed firewall, and switches to the second(spare) firewall.

8.3.3 Servers

All networks need servers in order to provide a range of functionality. A server is a host whose work involves providing services to other computers. The servers used in this research project are DHCP servers and DNS server. If budget permits, this network can be expanded to include many additional servers such as Mail Server, Application Server, Server Platforms, Web Server, Real-Time Communication Server, FTP Server, Collaboration Server, Open Source Server, Virtual Server, List Server, and Telnet Server. Each of these servers serves the hosts on the local area network in different ways,

³¹ Jiang, Dongyi, et al. "Layer two firewall with active-active high availability support." U.S. Patent No. 7,941,837. 10 May 2011.

depending on the kind of servers. For instance, Web servers manage and serves web browsers for the clients. It loads data from disk and serves that data to the user's web browser. The main function of the web server involves storing, processing and transferring web pages to the users. Without the web server, internet security becomes vulnerable. This is because web server provides some security and reliability to the network.

8.3.4 Backup³²

8.3.5 Two Networks for Security

Less budget affects the security of the network. If budget allows for designing the network, two separate networks can be used. One network for network devices inside the university such as public computers, and another network for wireless devices such as personal laptops and smart phones.

The network devices inside the university can be secured by using antivirus and automatic cleaning and re-imaging software. The automatic cleaning and re-imaging software prevents computer devices from saving virus in their storage. When a user uses a computer device and then store some information or install any program on it, the information stored or installed program will be gone after the computer device is restarted. This is because automatic cleaning and re-imaging software will remove any new installed programs and files that may or may not contain virus saved on that computer. Therefore making use of the automatic cleaning and re-imaging software will ensure that network devices inside the university are well protected.

³² See page 5 in this chapter (7.3 Backup Server- offsite backup/disaster recovery)

The second network which is the wireless network will be an individual network. This network must have public IP address different from the network inside the university, and must not have any connection with the devices inside the University. It must have different servers, NAT, routers, etc. In other words, the wireless network will be an independent network. When a user uses their own device with the network and may have a virus on their device, it will not affect the network inside the university. As a result, the network will be more secure.

The wireless devices is very tough to secure. This is because each user has its own device that may contain a virus, especially when they make use of the network. As an illustration, when a user connects to the network, the virus will pass from the user's device to the network, and can cause traffic to that network. Consequently, when budget allows, it is a good idea to separate the network into two networks: physical network connection and wireless network connection.

9. Conclusion

This project has proven that a standard network system can be designed with less cost. Although we used the cheapest devices in designing the network, the security of this network turned out to be very strong. This is because the firewall and backup devices used in this network are of good quality.

All networks need many servers for doing their work. For this research, we did not use all servers because of cost, but we used some important servers such as DNS and DHCP. These servers help the network to perform their functions in a smooth way.

It can be seen in this research that various costs were minimized in order to maximize the quality of the designed network. Although there may have been some challenges in this project due to some financial constraints, at the end our aim was achieved by designing a network for developing countries with minimal cost. For example, we made use of some cheap devices for the network security, but the most interesting part is that, at the end of the day, all challenges and constraints were overcome.

This research has also demonstrated that economy problems of a country cannot hinder the success of a technological invention. Many developing countries who aspire to be in the same technological league as the developed countries, will be very hopeful. This is because this project has deeply provided a way to adopt a cheap and effective solution to designing a standard network, especially when a budget is not favorable.

Lastly, as cheap and effective as the methods of designing a network in this research are, it is not limited to only developing countries. Developed countries that are trying to cut cost in any of their network design projects can also adopt the methods used in this research.

9.1 Summary

In this network design, an integrated network design for universities in the developing countries has been presented. This network design is composed of many sections. First, we started to explain the design constraints. Many universities in the developing countries are eager to design a network that meets standards of developed

countries but has always been faced with cost implementation barrier. Secondly, this design accounts for challenges that will be faced when designing network in developing countries due to the lack of a rich economy like developed countries. Another challenge that developing countries have is equipment availability, requiring careful selection of components. Also, security is an important section in this network design. Strong security solutions are detailed including as firewall, backup, virtual switch and DNS server options. This configuration includes some software applications, such as antivirus, password, and encrypted passwords.

This design allows for future expansion, as universities using this design can connect 3115 additional hosts, allowing for per host costs, like cabling. The additional hosts can be included without exhausting the available IP address. Also, if there are high budget, they can develop the network system to become more powerful, have a high level of security and many servers can be added to the network.

Lastly, as cheap and effective as the methods of designing a network in this research are, it is not limited to only developing countries. Developed countries that are trying to cut cost in any of their network design projects can also adopt the methods used in this network design.

10. Reference:

- Babani, S., et al. "Comparative Study Between Fiber Optic and Copper In Communication Link."
http://s3.amazonaws.com/academia.edu.documents/34322554/comparative-study-between-fiber-optic-and-copper-in-communication-link.pdf?AWSAccessKeyId=AKIAJ56TQJRTWSMTNPEA&Expires=1481706535&Signature=3RrOr%2F6wEQt%2BVtvIU8vGD1cX0A%3D&response-content-disposition=inline%3B%20filename%3DComparative_Study_Between_Fiber_Optic_An.pdf
- Bakkal, Ahmet Emre. "IP PBX STATIONS.", Istanbul Arel University (2013).
<http://www.hasanbalik.com/projeler/bitirme/44.pdf>
- Brubaker, Aaron T. "Faculty perceptions of the impact of student laptop use in a wireless internet environment on the classroom learning environment and teaching."
Unpublished MS thesis, School of Information and Library Science, University of North Carolina, Chapel Hill, NC (2006).
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.95.6765&rep=rep1&type=pdf>
- Eastman, Mark, and Gregory K. Sherrill. "Category 5e compliant patch panel."
U.S. Patent No. 7,354,316. 8 Apr. 2008.
<https://docs.google.com/viewer?url=patentimages.storage.googleapis.com/pdfs/US7354316.pdf>
- Clarke, Glen E. CompTIA Network+ Certification Study Guide. McGraw-Hill, 2012.
http://s3.amazonaws.com/academia.edu.documents/35436829/CompTIA_Network_Plus_Certification_Study_Guide_Fourth_Edition_Glen_Clarkewww.ebook-dl.com.pdf?AWSAccessKeyId=AKIAJ56TQJRTWSMTNPEA&Expires=1481619248&Signature=n%2BbG4gb%2B36gWD4mlegizaWyyVuc%3D&response-content-disposition=inline%3B%20filename%3DRrjeta_Kompjuterike.pdf
- Engebretson, D. J. (2009). Designed for Distance. Sdm, 39(7), 64-67. Retrieved from
<http://ezproxy.valpo.edu/login?url=http://search.proquest.com/docview/228454153?accountid=14811>.
<http://www.cisco.com/c/en/us/support/security/asa-5505-adaptive-security-appliance/model.html>
<http://itprice.com/cisco-gpl/PREGDD-APLNC-K9>
- Jan, Edwin. "A Protocol for Authoring Curricula for Technology Education. Diss. The university of Manitoba.
<http://www.collectionscanada.gc.ca/obj/s4/f2/dsk2/ftp01/MQ32930.pdf>.
- Jiang, Dongyi, et al. "Layer two firewall with active-active high availability support."
U.S. Patent No. 7,941,837. 10 May 2011.
<https://docs.google.com/viewer?url=patentimages.storage.googleapis.com/pdfs/US20030200463.pdf>

- Jiang, Ruoqing. "A review of Network Topology." (2015).
http://scholar.googleusercontent.com/scholar?q=cache:flAST4TFFz8J:scholar.google.com/&hl=en&as_sdt=0,15
- Kim, Sang Hyun, Clif Mims, and Kerry P. Holmes. "An introduction to current trends and benefits of mobile wireless technology use in higher education." *AACE journal* 14.1 (2006): 77-100.
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.532.9058&rep=rep1&type=pdf>
- Koike, Yasuhiro. *Fundamentals of Plastic Optical Fibers*, Wiley-VCH, DE, 2015;2014;
<https://books.google.com/books?hl=en&lr=&id=yjb-CAAQBAJ&oi=fnd&pg=PA79&dq=Koike,+Yasuhiro.+Fundamentals+of+Plastic+Optical+Fibers,+Wiley-VCH,+DE,+2015%3B2014&ots=6b4QH7srTn&sig=Iovn21atmmuPZwa60D12187uvo#v=onepage&q&f=false>
- Kornilovitch, P. E., R. N. Bicknell, and J. S. Yeo. "Fully-Connected Networks with Local Connections." *Applied Physics A*, vol. 95, no. 4, 2009., pp. 999-1004doi:10.1007/s00339-009-5124-3.
http://download.springer.com/static/pdf/0/art%253A10.1007%252Fs00339-009-5124-3.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Farticle%2F10.1007%2Fs00339-009-5124-3&token2=exp=1480439417~acl=%2Fstatic%2Fpdf%2F0%2Fart%25253A10.1007%25252Fs00339-009-5124-3.pdf%3ForiginUrl%3Dhttp%253A%252F%252Flink.springer.com%252Farticle%252F10.1007%252Fs00339-009-5124-3*~hmac=3a5f9e1f700852abbad213d784ae6556c87a9814c69e2e65b260596ea14350fa
- Leiner, Barry M., et al. "A brief history of the Internet." *ACM SIGCOMM Computer Communication Review* 39.5 (2009): 22-31.
<http://www.isoc.org/oti/printversions/0797prleiner.html>
- Leinwand, Allan, Bruce Pinsky, and Mark Culpepper. *Cisco router configuration*. Cisco Press, 1998.
http://ptgmedia.pearsoncmg.com/imprint_downloads/cisco/1578702410.pdf
- Leinwand, Allan, Bruce Pinsky, and Mark Culpepper. *Cisco router configuration*. Cisco Press, 1998.
http://ptgmedia.pearsoncmg.com/imprint_downloads/cisco/1578702410.pdf
- Leung, Kin K., and B-J. Kim. "Frequency assignment for IEEE 802.11 wireless networks." *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th. Vol. 3. IEEE, 2003.*
http://www.ics.forth.gr/netgroup/mobile/Bibliography/LoadBalancing/LB/Channel_Assign_80211_MultiCell.pdf
- Mentze, Duane, and David McAnaney. "Automatic networking device configuration method for home networking environments." U.S. Patent Application No. 09/969,248.

- http://www.dut.edu.ua/uploads/n_2205_50283608.pdf#page=79
- Pandya, Kartik. "Network Structure or Topology." *International Journal of Advance Research in Computer Science and Management Studies* 1.2 (2013).
<http://ijarcsms.com/docs/paper/volume1/issue2/V1I2-0006.pdf>
- Siekierka, Thomas J., and Robert David Kenny. "Twisted pair cable." U.S. Patent No. 6,222,129. 24 Apr. 2001. <https://www.google.com/patents/US6222129>
- Srisuresh, Pyda, and Matt Holdrege. "IP network address translator (NAT) terminology and considerations." (1999). <https://tools.ietf.org/html/rfc2663.html>
- Teare, Diane. *Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide: Foundation learning for the ROUTE 642-902 exam*. Pearson Education, 2010.
[https://books.google.com/books?hl=en&lr=&id=f5KssgEfd1IC&oi=fnd&pg=PR10&dq=Teare,+Diane.+Implementing+Cisco+IP+Routing+\(ROUTE\)+Foundation+Learning+Guide:+Foundation+learning+for+the+ROUTE+642-902+exam.+Pearson+Education,+2010&ots=8NpOgMCDas&sig=ZUpIzzYiXFMrOPPX8Jwv-US5NTE#v=onepage&q=Teare%2C%20Diane.%20Implementing%20Cisco%20IP%20Routing%20\(ROUTE\)%20Foundation%20Learning%20Guide%3A%20Foundation%20learning%20for%20the%20ROUTE%20642-902%20exam.%20Pearson%20Education%2C%202010&f=false](https://books.google.com/books?hl=en&lr=&id=f5KssgEfd1IC&oi=fnd&pg=PR10&dq=Teare,+Diane.+Implementing+Cisco+IP+Routing+(ROUTE)+Foundation+Learning+Guide:+Foundation+learning+for+the+ROUTE+642-902+exam.+Pearson+Education,+2010&ots=8NpOgMCDas&sig=ZUpIzzYiXFMrOPPX8Jwv-US5NTE#v=onepage&q=Teare%2C%20Diane.%20Implementing%20Cisco%20IP%20Routing%20(ROUTE)%20Foundation%20Learning%20Guide%3A%20Foundation%20learning%20for%20the%20ROUTE%20642-902%20exam.%20Pearson%20Education%2C%202010&f=false)
- White, Paul. "Data Security: The Backup Backdoor." *Network Security*, vol. 2002, no. 2, 2002., pp. 8-9doi:10.1016/S1353-4858(02)00213-1.
<http://www.sciencedirect.com/science/article/pii/S1353485802002131>
- "Why Use Cisco Network Systems? - Cisco." *Insert Name of Site in Italics*. N.p., n.d. Web. 16 Nov. 2016
 <<http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-s>>.
- Yurcik, William J. "Network Topologies." *Computer Sciences*, edited by K. Lee Lerner and Brenda Wilmoth Lerner, 2nd ed., Macmillan Reference USA, 2013. *Science in Context*,
link.galegroup.com/apps/doc/CV2642250100/SCIC?u=valpo_main&xid=cc7ad170. Accessed 6 Dec. 2016.
- Zhang, Wenbo, et al. "A Good Performance Watermarking LDPC Code used in High-Speed Optical Fiber Communication System." *Optics Communications*, vol. 346, 2015., pp. 99-105doi:10.1016/j.optcom.2015.02.023.
<http://www.sciencedirect.com/science/article/pii/S0030401815001133>
- Zhu, Hua, et al. "A survey of quality of service in IEEE 802.11 networks." *IEEE Wireless Communications* 11.4 (2004): 6-14.
https://www.cse.iitb.ac.in/~varsha/allpapers/wireless/kiran/surveyofQoSin802_11.pdf