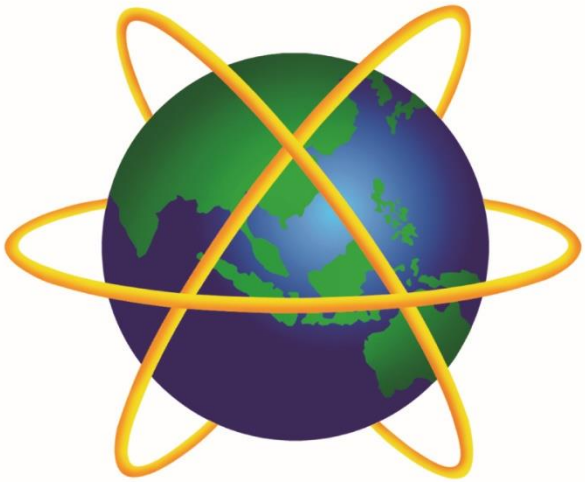

A · P · U

ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

NETWORKS AND NETWORKING

NETWORK CONFIGURATION PROPOSAL

GROUP ASSIGNMENT

TITLE: ADVERTISING FIRM: NETWORK REPORT

LECTURER NAME:	Mrs. Nurul Haniza Binti Mohtar
STUDENT NAME:	Mrisho Abeid Omary
STUDENT NUMBER:	TP033289
MODULE CODE:	AICT003-3-2-NWN
INTAKE CODE:	UCDF1310BIT
ISSUED DATE:	19th-Jun-2014
SUBMITION DATE:	04st-Sep-2015
WORD COUNT:	6853 Words

0.0 TABLE OF CONTENTS:

0.1 TABLE OF FIGURES:

0.2 ABSTRACT:

The purpose of this report is to develop and propose a network for a newly upgraded medium-size company. The proposal follows all guidelines and requirements provided by the CEO of the company. With the use of relevant research materials such as articles, websites and books, we were able to identify the information justified in the report below. The coverage of this report is based on the introduction of the company and the scope of limitation, the description of the floor plans and network diagram, description of the network topologies for both LAN and WAN networks, identification and justification of the hardware and software used, the performance and reliability issues, security issues and sustainability issues, conclusion, references and appendix.

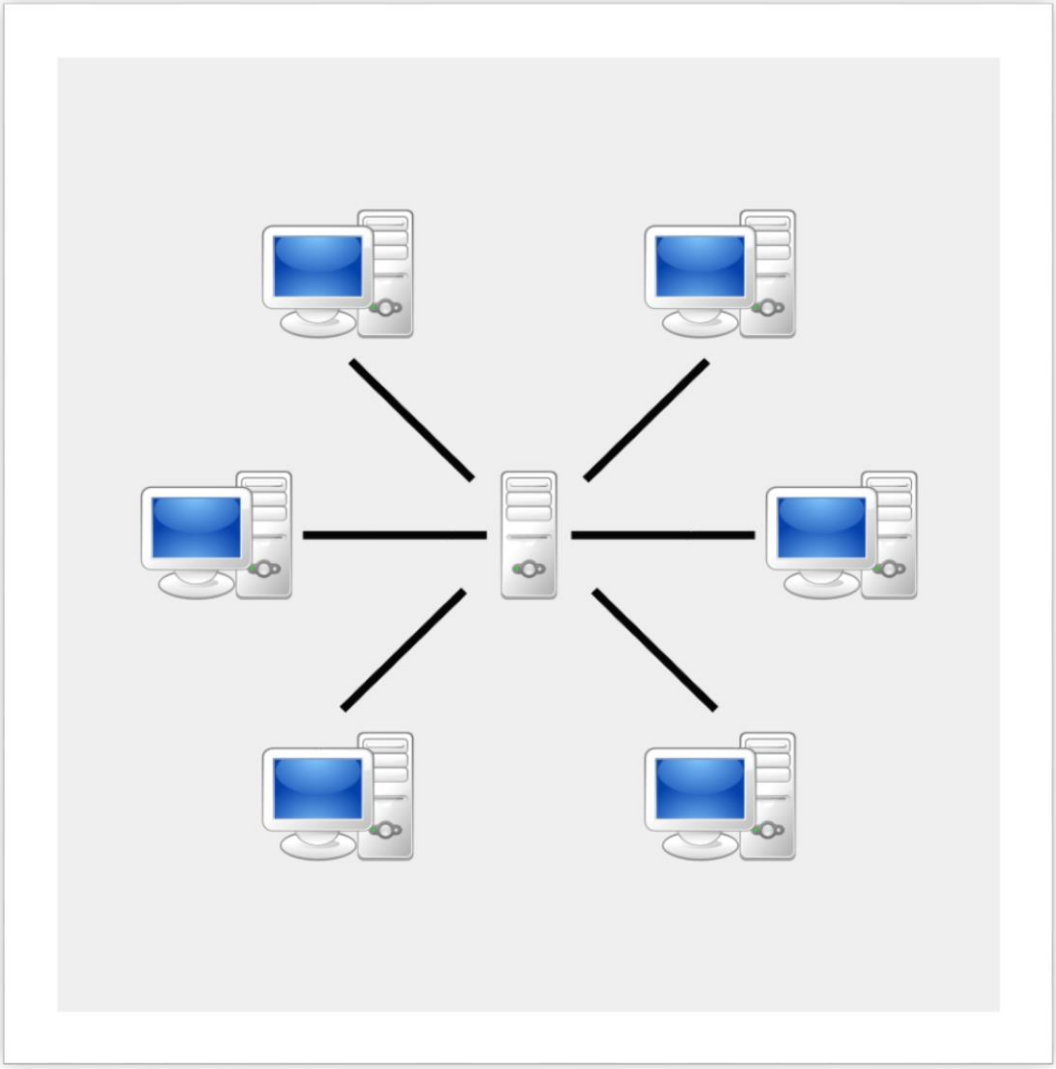

FIGURE 1: STAR TOPOLOGY LAYOUT

Source: Google Images (2015)

NETWORKS AND NETWORKING

NETWORK CONFIGURATION PROPOSAL

Mrisho Abeid Omary | Network Configuration Proposal | September 1, 2015 | Networks & Networking

1.0 INTRODUCTION:

A CEO of a newly upgraded medium-sized advertising company has requested our expertise as network consultants to accept the responsibility of proposing a network for their newly developed 5 story office building for 105 employees including himself, he also requested that we identify all necessary equipment and any other operational requirements for the proposed network.

The plan that we prepared for the company follows the guidelines identified by the CEO in his proposed document. The floor plan of the building has both specific and generic requirements. The ground/first floor should include a lobby, reception area and a cafeteria. While the second floor should have an allocated space for the server room while the third floor should be reserved for the staff recreation area and meeting rooms, where as any other relevant departments and the CEO's office together with the research and development department (R&D) can be located in of the remaining floors of the building.

Since the company designs and publishes web and printed advertisements for its customers, the CEO requested that all advertisement designs should be treated confidentially. All sensitive information is to be indicated within their correspondences through email as well as secure and monitor the designs. Also, all information in the human resources and accounts and finance departments should be secure and confidential since the company has plans to raise the number of staff in the future.

Our proposed network focuses more on the performance and reliability issues of the network. The reason why we have chosen to lean more on the performance is because we won't the connection and speed of the network to be very fast with minimal or no delay (Murdoch and Watson, 2008). Also, the reliability issues are to ensure that in case we face any problems that can cause our network to be slow or experience other network related problems, then we have ways to solve them so that the network can be fast and efficient once again. We have decided not to focus more on the security issues since if we had too much security then it would affect the performance of the network and also because it would be very expensive to incorporate a lot of security in the network.

2.0 FLOOR PLANS AND NETWORK DIAGRAM:

The following explains the distribution of the units in the floor plans of the building. Some floor plans have specific requirements of where should each particular room be located. Also, the network diagram and what type of the company is introduced.

2.1 FLOOR PLANS:

There are 5 floor plans of the new office building as seen in the images below. Following the specifications provided by the CEO, some of the rooms are located in specific floor plans only whereas others are generic.

2.1.1 1ST / GROUND FLOOR PLAN:

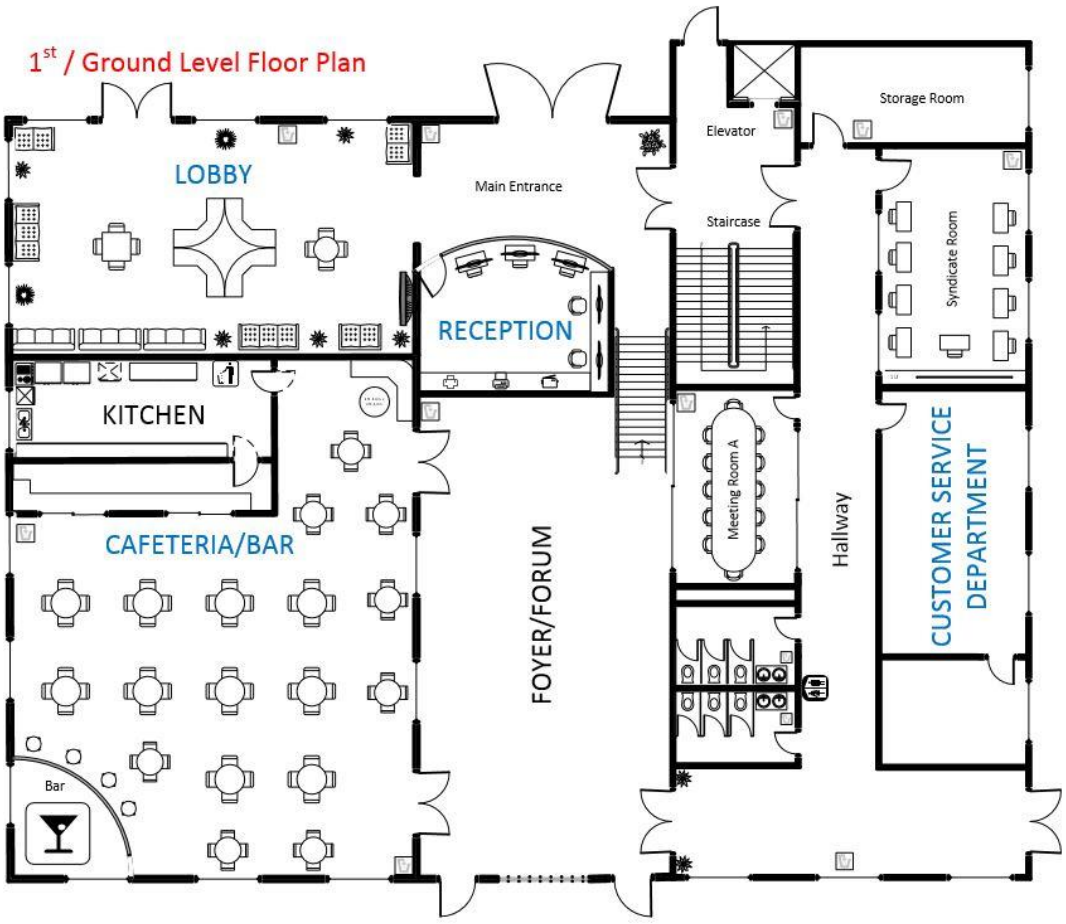

FIGURE 2: 1ST / GROUND LEVEL FLOOR PLAN

Figure 2 (above) shows the 1st/Ground level floor plan of the new office building. The allocation of the rooms and other departments as seen follow the specifications of provided by the CEO of the company. The main identified requirements for the 1st floor were to have a space for the cafeteria, lobby and reception areas. As indicated in the floor diagram, all spaces have been clearly indicated in a light blue color with a slightly larger font in capital letters, this is to show that those spaces are specified as part of the requirements to consider when developing the 1st floor plan.

2.1.2 2ND LEVEL FLOOR PLAN:

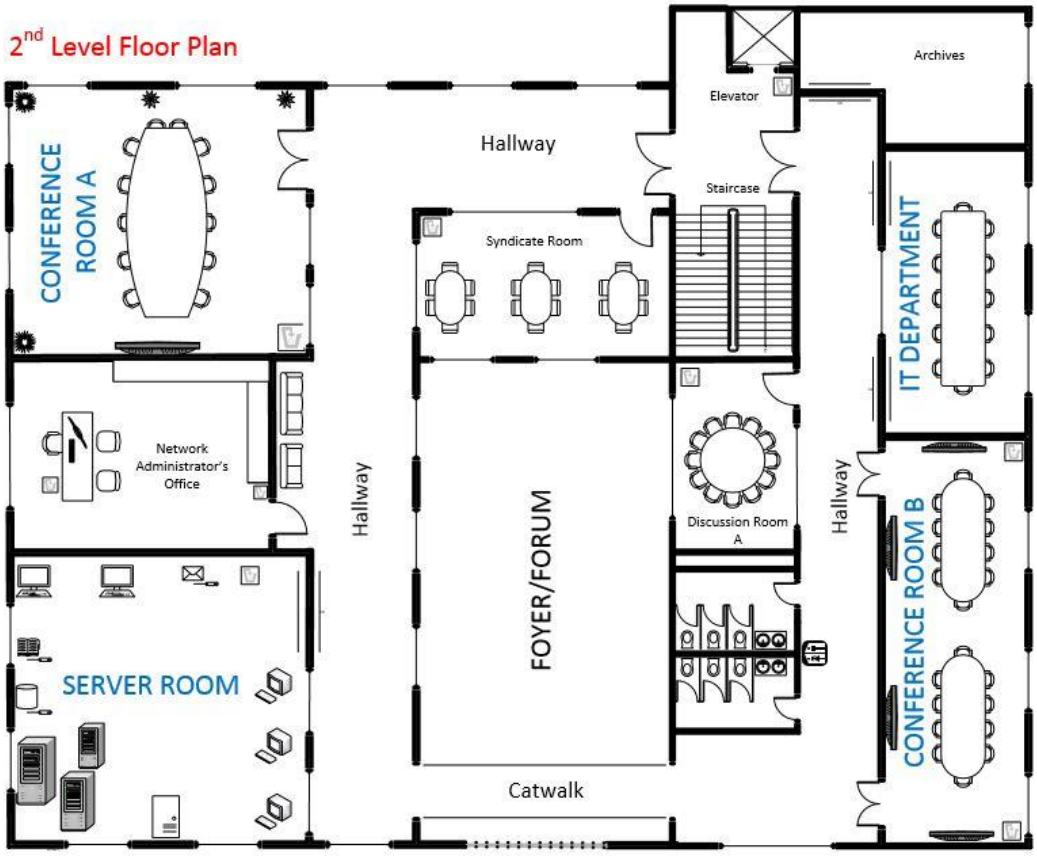

FIGURE 3: 2ND LEVEL FLOOR PLAN

The figure above illustrates the layout of the 2nd level floor plan as indicated. The figure depicts the locations the server room, conference room and the IT department of the organization as per the requirements provided. The use of access doors on the IT department and the server room to limit their accessibility. The have been implemented as a security measure to keep all unauthorized personnel and external entities from being able to access them since only authorized personnel are

allowed to access them with the use of access cards provided by the company. The only people authorized to access the server room and the IT department are the network administrator and the IT team and not anyone else.

2.1.3 3RD LEVEL FLOOR PLAN:

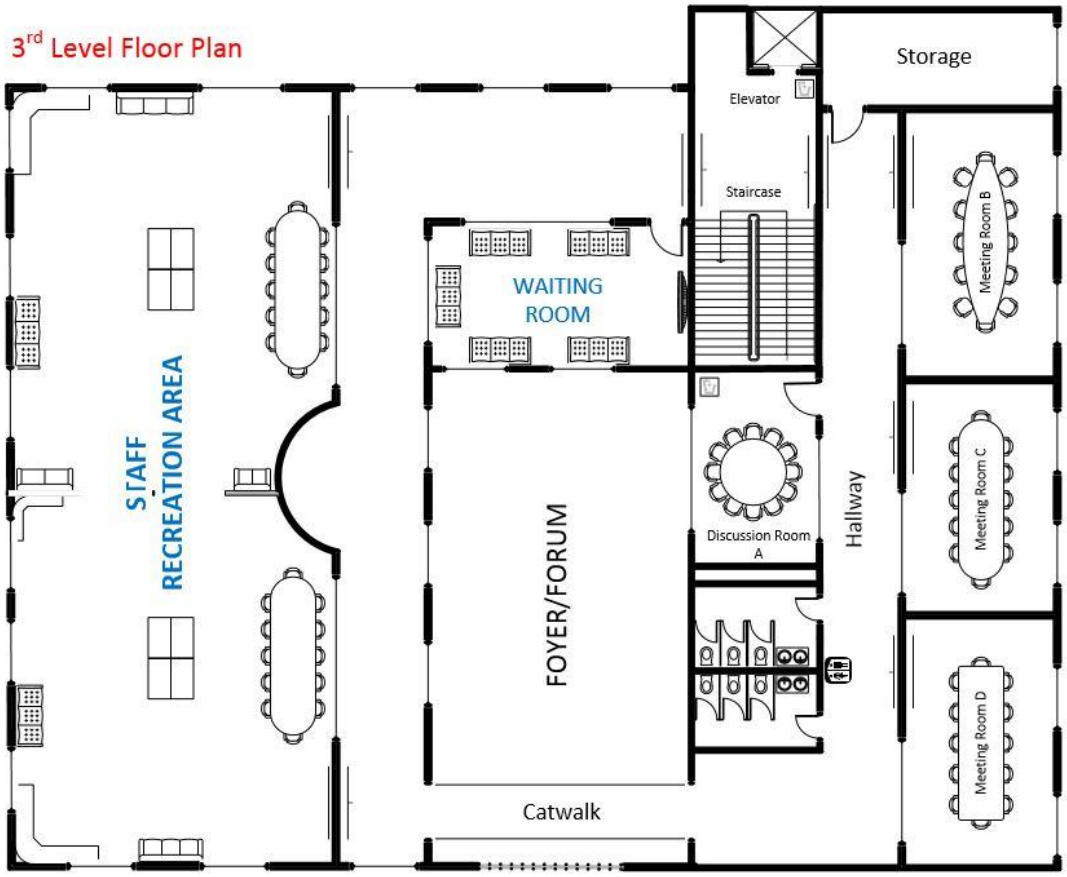

FIGURE 4: 3RD LEVEL FLOOR PLAN

The 3rd level floor plan as seen in the figure above shows the locations of the staff recreation area and other meeting rooms of the organization. In addition to that, eh figure also shows the use of access doors for the entire floor and its rooms since only authorized personnel are allowed to access this floor. The permissions of those who can access this floor are granted to the employees of the company unlike other floors such as the 2nd floor were only the IT team, and the network administrator are allowed to access both the IT department and the server room. (Refer to figure 3 above.)

2.1.4 4TH LEVEL FLOOR PLAN:

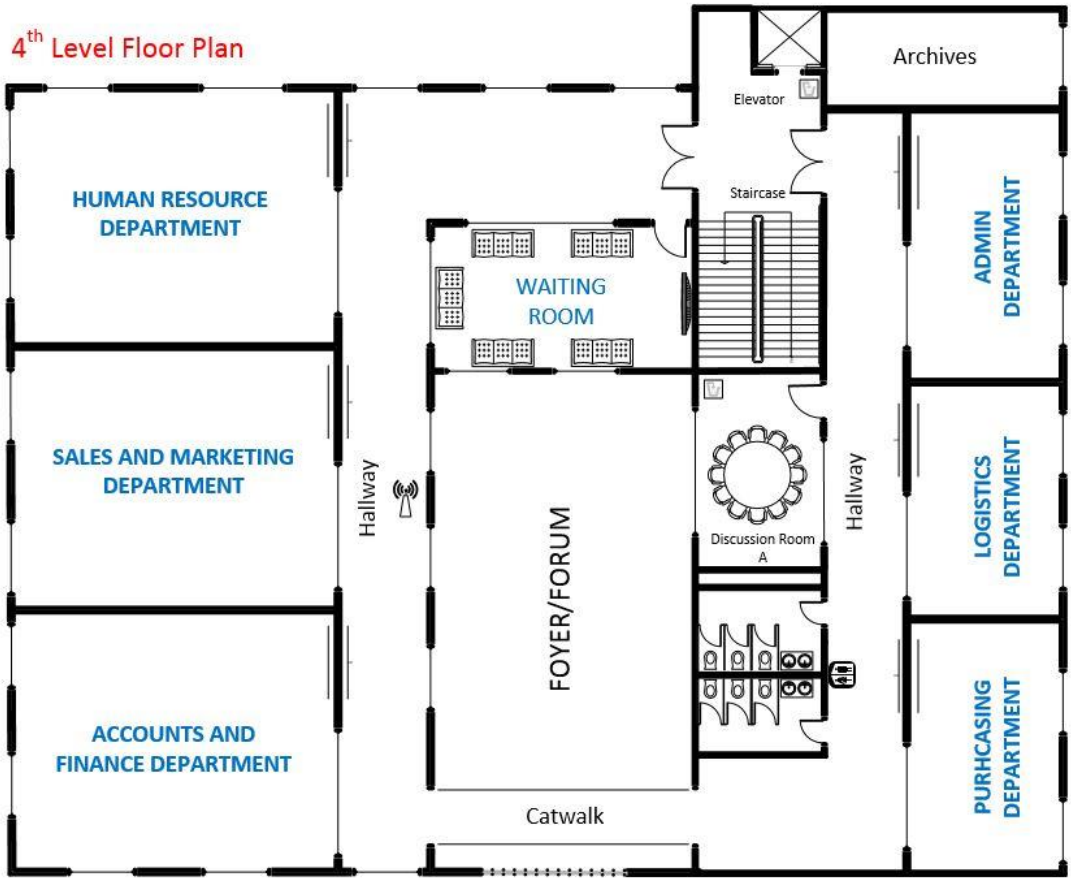

FIGURE 5: 4TH LEVEL FLOOR PLAN

In the 4th floor as seen in the figure above, all rooms are reserved for the rest of the departments within the organization apart from the research and development (R&D) which is located of the 5th floor instead. The application of access doors can also be clearly seen on this floor are well since there are some of the employees in other departments who are not permitted to access other departments. However, for the matter of some departments that have a relation where their employees may need to work together from time to time, those departments can be accessed by employees from the other department provided that the correlation of those two departments can be seen. For instance, employees in the Accounts & Finance Department may need to collaborate with those from the Sales and Marketing and Purchasing Departments directly since these two have a direct connection with their customers and suppliers of the company, hence the employees from these departments can access each other's departments.

2.1.5 5TH LEVEL FLOOR PLAN:

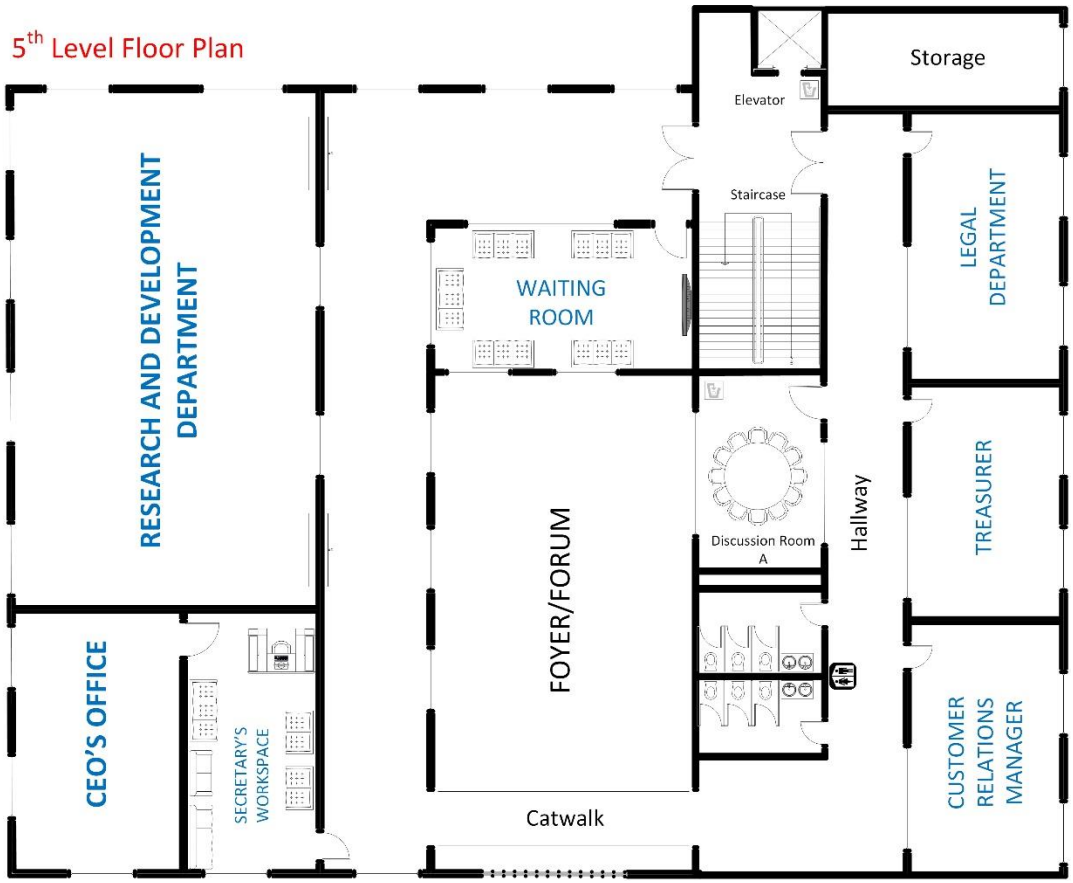

FIGURE 6: 5TH LEVEL FLOOR PLAN

The 5th level floor plan as seen in the figure above will have the CEO's office together with the secretary's office, the research and development (R&D) department together with the customer relations department, legal department and the treasurer's office will also be located on the same floor. We have added more physical security at the R&D department because only authorized personnel are allowed to see the designs and any other ideas developed by the R&D department.

2.2 NETWORK DIAGRAM:

In this section, we will discuss on the network diagram design, the IP addressing plan and the location of the core and distribution layer devices.

2.2.1 NETWORK DIAGRAM AND IP ADDRESSING TABLE:

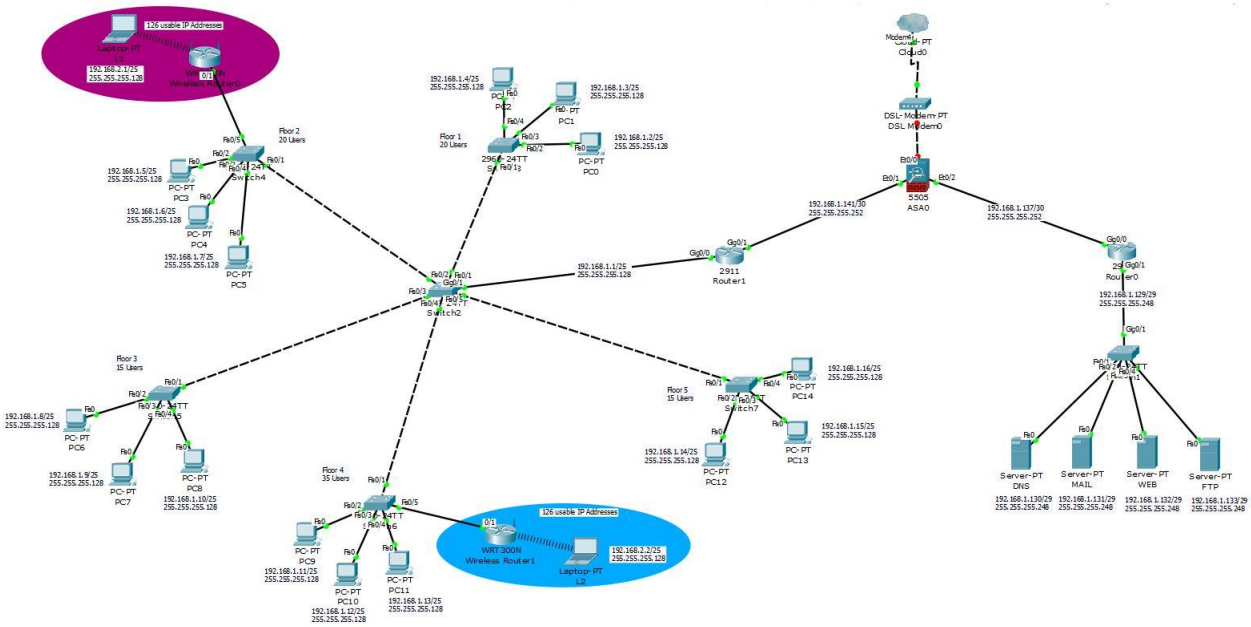

FIGURE 7: NETWORK DIAGRAM OF THE COMPANY

SUB-NETWORKS IN THE NETWORK DIAGRAM							
Sub-Network	**Net ID**	**CIDR Notation**	**Net Mask**	**Available Hosts**	**First IP**	**Last IP**	**Broadcast Address**
1	192.168.1.128	/29	255.255.255.248	129 - 134	192.168.1.129	192.168.1.134	192.168.1.135
2	192.168.1.136	/30	255.255.255.252	137 - 138	192.168.1.137	192.168.1.138	192.168.1.139
3	192.168.1.140	/30	255.255.255.252	141 - 142	192.168.1.141	192.168.1.142	192.168.1.129
4	192.168.1.0	/25	255.255.255.128	1 - 126	192.168.1.1	192.168.1.126	192.168.1.127
5	192.168.2.1	/25	255.255.255.128	1 - 126	192.168.1.1	192.168.1.126	192.168.1.127
6	192.168.2.2	/25	255.255.255.128	129 - 254	192.168.1.129	192.168.1.254	192.168.1.255

TABLE 1: SUB-NETWORKS IN THE NETWORK

As seen in the Sub-netting table above (table 1), there are 6 sub-nets in the network. Sub-network 1 is dedicated for the interface Gig0/ of router 0 to the Servers of the network (see figure 7). The idea of using /29 for this subnet is to provide 6 usable IP addresses to assign to the available servers and the remaining IP addresses to be used as extras in case the company needs to add more servers in the future. Since sub-networks 2 and 3 are both point to point connections, we have implemented /30 for these networks so that we can obtain a total number of 2 usable IP Address for each (see figure 7).

On the other hand, sub-network 4 which covers the rest of the network has a larger number of users, 105 in total. Hence, we have implemented a /25 notation in order to obtain a total number of 126 usable IP Address for each pc in this sub-network. The left over 21 IP Addresses are purposely kept for the future in case the company expands to add more employees in the department. The Wi-Fi connections both have 126 usable IP Addresses that were derived from a different network of 192.128.2.

3.0 STAR TOPOLOGY:

The following is the discussion on the type of network topology that we have proposed for the network and the reasons why we have chosen it.

3.1 JUSTIFICATION OF STAR TOPOLOGY:

Topology refers to the logical or physical layout of computers or nodes in a network. The topology chosen to be implemented in this network is a star topology which is a network topology that needs a central high-end device (such as hub, router, pc or a simple switch) on which others nodes within the network are connected to (Forouzan, 1998). The messages in a star topology are sent by either being broadcasted to all nodes in the network or sent only to the intended receiver depending on whether the central device is of high fidelity or not (Meador, 2008). Within this topology, every device is considered to be a personal area network (PAN) coordinator through which communications take place on a given radio channel (Cho et al., 2007). There is fast transmission of information in the network through a star topology since all devices are connected together to a central device. This makes it easier for the information to be received at any given time since all

devices on the same network can get the information on the central device (Yawut and Kilaso, 2011).

3.2 REASONS AND ADVANTAGES OF USING STAR TOPOLOGY:

There are numerous reasons of why we decided to implement a star topology for this network which can be explained by the advantages of using star topologies in a network. The following are a few of the main advantages of Star topology.

Cost: In comparison with other topologies such as the Mesh topology, the expense in creating a star topology is very little (Forouzan, 1998). This can be seen in the use of expense money to buy extra devices to connect a new network or expanding an existing one. In the case of the Mesh topology, if one wants to connect 8 computers in the network then he/she would require a total of 7 individual network cards for each and every computer and 7 network cables to be connected directly from that computer to the rest in the network where the applications of this would be both chaotic and troubling when it comes to troubleshooting especially if the cables are not arranged properly or color coded. On the hand, a star topology would only require a single central device to connect all other computers together through it. Which saves a lot of costs, expenses and time for the company.

Connectivity or implementation: In a star topology, all devices have one I/O port and one link that connects it to a number of others. Due to this reason, a star topology is easy to configure and reconfigure compared to a mesh topology for instance (Forouzan, 1998). Since the mesh topology requires each device in the network to have the same number of I/O ports as the number of devices in the network so that each computer can be connected with each by one link, this makes it very hard, confusing to connect a large number of devices together and sometimes impossible to connect a network of many devices at the same time.

Expansion or increase: Another one of the advantages of star topology is the expansion. When expanding a star topology, other different topologies can be derived from the process. For instance: adding new central devices such as hubs, routers or switches, the network can expand to be a cluster-tree topology (Cho et al., 2007).

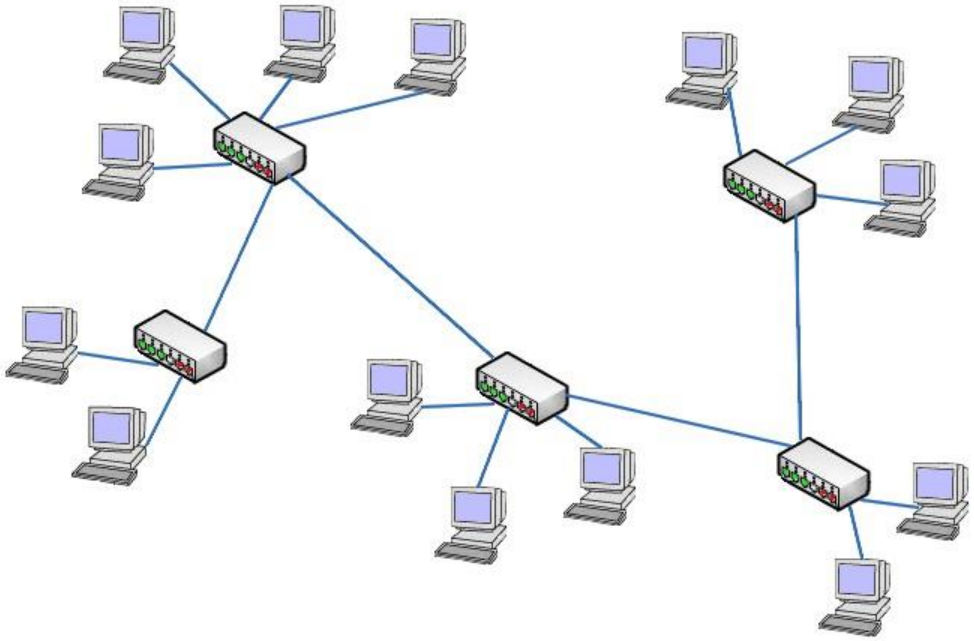

FIGURE 8: CLUSTER-TREE TOPOLOGY

Device compatibility: This refers to the network devices used in a network to connect the computers to each other. With networks such as Bus, Mesh or Ring, these networks cannot connect to network devices such as hubs, routers because of their compatibility with network devices. With the use of a star topology in a network, one can connect different network devices such as routers, switches and hubs to expand the network and easily connect the computers together so that all users in the network can communicate with each other. Each one of the devices in the network have a dedicated point-to-point connection to the central device or controller (Forouzan, 1998).

Robustness: A star network is very robust in terms of robustness. If a link in a star topology fails, the only link that will be affect would be itself. This also helps in fault isolation and identification. Due to the use of a hub for instance, as long as it is still on and working, it can be used in monitoring problems of links and even bypass any defective ones (Forouzan, 1998). Unlike other network such as Bus which have a difficulty in reconfiguration and fault isolation since it is designed to have optimum efficiency in installation, it would not be conducive to be implemented for such a network. Also, another issue with the bus topology is that if the bus has a problem (such as a fault or break), this will discontinue all communications even among devices on the same side of the problem.

3.3 DISADVANTAGES OF USING STAR TOPOLOGY:

The following are the disadvantages of using a star topology that may cause problems to the proposed network of the company.

One of the main disadvantages of using a star topology is the dependency on the central device. In a star topology, all nodes or computers are connected together to one single central device such as a switch, hub or router (Forouzan, 1998). Hence, in uncontrolled situations where the network is disorganized, or the cabling in the network is messy, it creates chaos and sometimes unmanageable cases where it becomes hard for the network administrator to conduct troubleshooting procedures. However, in order to be able to solve the problems caused by such situations and preventing them from happening, implementing the use patch panels to help properly align the cabling and arranging the network is one of the ways to solve such a problem.

Another one of the major problems is a failure in the central device. In cases where such a situation occurs, the whole network will be affected. Due to the dependency of the central device as the main communication channel from one node to another, it makes it the major disadvantage of the network because all the computers and devices in the network will be disconnected if central device fails. Hence, the failure of the central device results to an inoperable network (Santra and Acharjya2, 2013). In order to make sure that such a problem should not occur, we have implemented a redundant device which will communicate the operating device so that in case the operating device fails then the redundant central device will take over the network operations immediately.

4.0 HARDWARE AND SOFTWARE:

The following are the discussions on the proposed hardware and software to be used in the network.

4.1 HARDWARE:

The following discussion below is dedicated to the types of network devices (such as routers, switches, servers and more) and also non network devices (such as access cards for added security) that we have implemented in this company network.

4.1.1 ROUTERS:

These are sophisticated devices that can execute specific tasks and have access to the addresses at the network layer. They also have software that makes them capable of determining which among several paths between addresses is the best for a particular transmission (Forouzan, 1998).

The two routers that we will implement in our design (see figure 7) will be Cisco 3800 Series integrated service routers. This router is very good for medium-sized (such as this company) to large businesses and enterprise branch offices. It simplifies deployment and management and also lowers costs and any complexities of the network. With the availability of a total of 20 staff where 2 of them are the Network Administrators who will be directly involved with monitoring as well as maintaining the network, they do not need extensive training to manage this router due to its ease of configuration and use. In case the current Network Administrators were to resign from the company, it would not be difficult for any of the new staff to assume the role in maintaining the network. It also supports critical business applications by providing a secure platform with concurrent T3/E3 wire-speed delivery of data, security, video, voice and wireless (Cisco.com, 2014).

It also has other features such as Cisco Router and Security Device Manager (SDM) which can be used to simply management, built-in security to limit or stop external and internal intruders from accessing the system, support for wireless LAN standards 802.11a/b/g, built-in redundant power supply (on 3845 model) which can be used in case the organization has problems with its power and also up to two 10/100/1000 Mbs built-in ports among others. These features and more are what led us to choose this specific model for two routers used in the organization (Cisco.com, 2014) (see figure below).

FIGURE 9: CISCO 3800 INTEGRATED SERVICES ROUTER

4.1.2 SWITCHES:

The choices of the switches to be used differ depending on the number of users on each floor. Since one of the main concerns of the organization is the use of power due to electricity costs and the sustainability of the network, we have decided to opt for switches that use less power and still provide good performance for the network.

Since we have a total of 35 users on the 4th floor (see figure 7), we have decided to use a 48 ports switch so that each node can be connected and we can have a few extra ports which can be used for expansion purposes in the future in case the company would like to add more employees. The switch that we will use for this flow is the ERS 3549GTS (see figure 10) that has the 48 10/100/1000BASE-T ports with 2 shared SFP ports, 1SFP+ (1Gig or 10Gig) up link port that we can use to connect this switch to the main switch, RJ-45 Console ports that provide industry standard serial port connectivity. Apart from all those features and many more, it also consumes only 65 Watts of power maximum compared to the ERS 3549GTS-PWR+ which uses 484 Watts of power, hence this makes it environmentally and cost friendly in terms of electricity (Avaya.com, 2015).

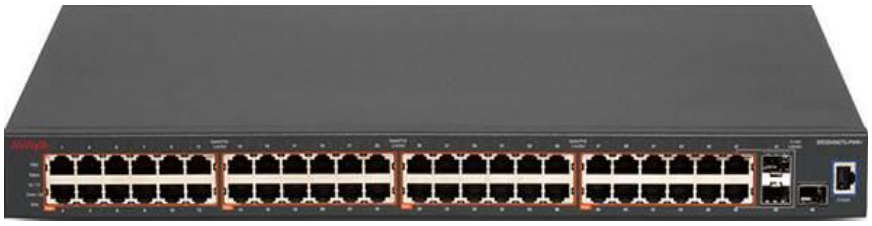

FIGURE 10: ERS 3549GTS SWITCH

On the 1st, 2nd, 3rd and 4th floors (see figure 7) we have 20 users and 15 users respectively hence we have implemented the use of the ERS 3524T switch that has 24 10/100Base-TXports plus 2 combo 10/100/1000BASE-T ports switches for both floors (see figure 11). These switches have 400MHz of system speed and 32MB flash 128MB DRAM system memory. They also have industry standard RJ-45 console ports that provide serial port connectivity. On top of that, they only consume 28.5 Watts of electricity maximum and input 100 to 240 VAC of voltage unlike the ERS 3526T-PWR+ which consumes 500 Watts of electricity maximum. Due to the fact that they use less power we have decided to use this model of switches since they will help us save electricity costs and also build a sustainable network (Avaya.com, 2015). The reason why we are using 24

ports switches for all these floors is so that we can have extra ports for expansion in the future. This is important because it will save the company some costs when they plan to expand their network.

FIGURE 11: ERS 3524T SWITCH

4.1.3 MODEM:

Since our network depends on the cloud which is located in the servers of another company since we are outsourcing from them, we need to have internet available so that we can access the cloud in order to retrieve the information that we need for decision making purposes hence we need a modem for that reason (see the figure below).

FIGURE 12: MODEM

4.1.4 SERVERS:

These are super computers that are specifically optimized to provide software and other resources to other computers or clients over a network upon request (Forouzan, 1998). They are capable of managing large numbers of computers at the same time.

The servers implemented in this network are IBM zEnterprise BC12 servers (see figure 12 below) which are built for medium-sized companies like this one because they can be used to handle 50 to 5000 users with ease. These were and excellent choice because they have many features necessary for this network and its design as well as additional features. They contain redundant array of independent memory (RAIM) of up to 496GB that help in full memory fault-toleration for increased durability. They also have special software and hardware that can perform early detections of vulnerabilities in order to reduce risks, they protect the data with high speed encryption and centralized management. They also have a structure that allows easy air flow to help cool the components faster and efficiently. In addition to that, they are designed to support raised floor designs for server rooms which is very convenient since our server room design has such a feature. With all these main qualities, these servers are indeed the best to be implemented in this network as all of their features and functionalities are the reasons why we chose them.

FIGURE 13: IBM ZENTERPRISE BC12 SERVER

4.1.4 NETWORK LAYERS AND DISTRIBUTION OF DEVICES:

This section describes the three layers (core, distribution and access layers) in a network. It also show the allocation of the core and distribution layer devices of the network in the organization building.

There are three layers in a network which are core layer, distribution layer and access layer. The core layer or the backbone and main access of the network is the main layer in which provides for high capacity transport between the attached distribution blocks. This layer uses Layer 3 routing (switching) to provide the necessary scalability, sharing of load, fast convergence and high speed capacity (Cisco Systems, 2005). The core layer devices in this network are the cloud, modem, firewall and the routers which are all located in the server room in the 2nd floor of the organization building (see the figure below). The distribution layer on the other hand, this layer provides policy-based connectivity, the best balance for the distribution block design and also the fastest restoration of voice and data traffic flows (Cisco Systems, 2005). In this network, the distribution layer devices are the main switch located in the Staff recreation area on the 3rd floor that distributes the network to the other switches in the network and the servers which are located in the server room in the 2nd floor (see figure 14 below).

It also includes the two wireless access points in the logistics department in the 4th floor and the IT department in the 2nd floor and the other switches in 5th floor in the R&D department, 4th floor in the sales and marketing, 3rd floor in the meeting room C, 2nd floor in the IT department and 1st floor in the reception area. Lastly, the access layer is the one that provides local and remote workgroup or user access to the network. The devices in the access layer include all kinds of end user devices such as laptops, computers, mobile phone etc. In this network design, the access layers will be located on their relevant floors depending on the departments in the organization. They will be connected to the distribution layer directly so that they can provide access of the network to the users (see figure 14 below).

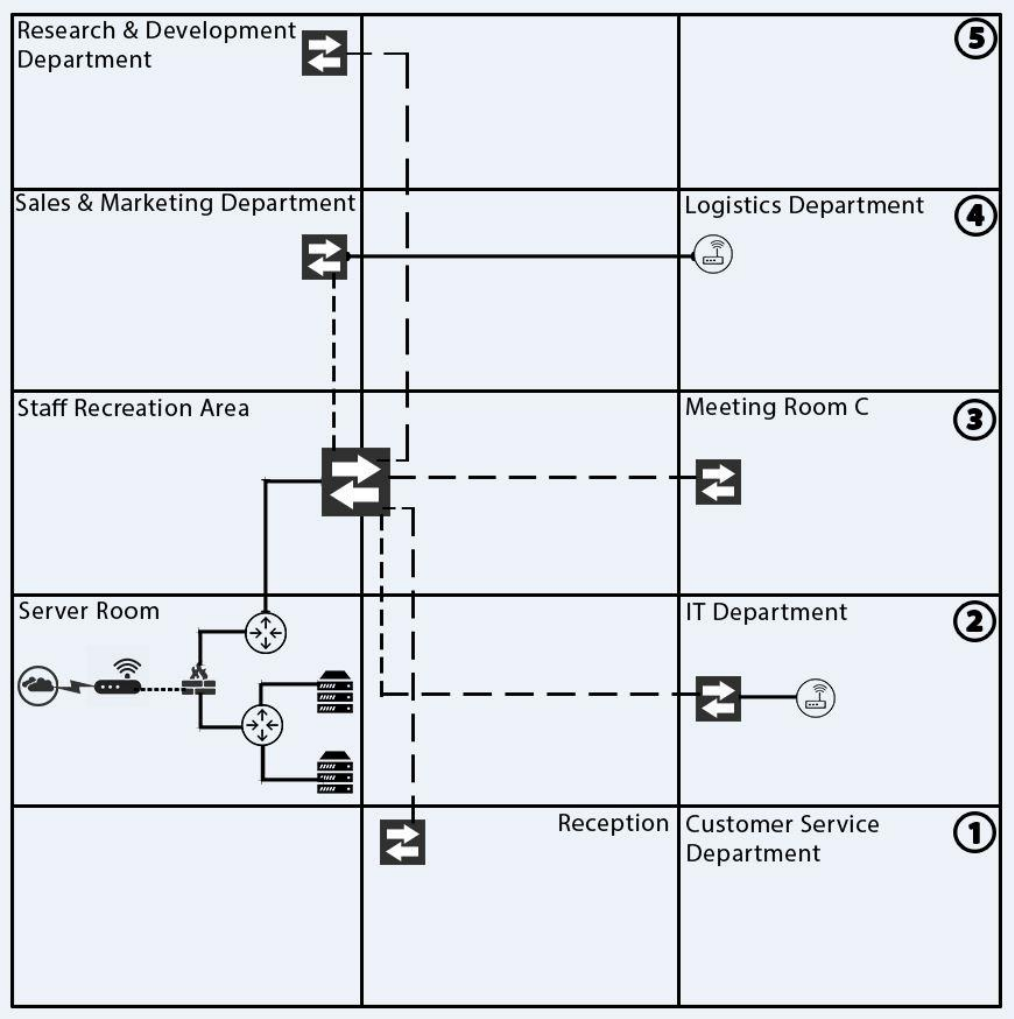

FIGURE 14: NETWORK LAYERS AND DISTRIBUTION OF DEVICES

4.2 SOFTWARE:

In this section we will discussing about the type of server operating system that we will use in this network.

We have decided to use Windows Server 2012 because of the features that it provides us, the advantages that it has and because of its availability and ease of deployment. Some of the features that it offers which are suitable for this network are a complete platform for virtualization with increased performance and scalability features, cloud services connectivity which can be used to connect and access the cloud storage that we have in the network. Also, with constant availability of new and improved features which offer cost-efficiency with the use of commodity storage and

improved acquisition, we can efficiently manage the network with full automation by using a set of broad management tasks that are simplified for deployment and virtualization (Microsoft, 2011). It also provides us with a flexible environment to build on-premises and in the cloud which can be used by developers to build symmetrical or hybrid framework applications between the datacenter and cloud. Compared to other server operating systems such as the Linux or UNIX server operating systems, Windows Server offers this network all reliable and efficient tools and features that we can use to implement for this network. On top of that, it offers an easy platform form deployment and management (Microsoft, 2011).

On the other hand, the Windows Server 2012 is one of the bestselling server operating systems (Tanenbaum, 2009). Due to this reason, we can be fairly certain to say that there are many network consultants available who are capable of properly monitoring and managing the Windows Server 2012, hence, in case we dace problem with the network because of the server software, we can be sure that we can quickly find a network consultant to help us fix the problem. Also, the decision of using this particular OS for our network is also based on the fact that there are a lot of articles and tutorials that talk about deploying, monitoring, handling, and managing the Windows Server 2012 hence if we cannot find a network consultant to help us fix the problem in our network, we can be able to review the articles and get a good understanding on how we can go about fixing the problem with the network.

5.0 PERFORMANCE AND RELIABILITY ISSUES:

The following below are the discussions of both performance and reliability issues of the company network.

5.1 PERFORMANCE ISSUES:

The performance of a network can be measured in different ways including transmit and response time. The performance of a network depends on the different factors such as number of users in the network, transmission medium, hardware (see hardware section) and its capabilities and the software's (see software section) efficiency.

The number of users in a network is a high factor that the network performance depends on because too many users concurrently using the network can slow the response time if the network is not designed to accommodate and coordinate heavy traffic loads (Forouzan, 1998). When designing a network, one needs to take into account the number of users who will be using the network so that he/she can develop a network that is capable of maintaining large numbers of users at the time. Due to this reason, we have decided to use an efficient network design by implementing hardware (IBM zEnterprise server) that is capable of handling large numbers of users at the time so that the response time of the network will not be affected hence making the network performance slow.

The media that we are using for thins network are both cable and wireless connectivity (see figure 7). The cables will be Fast Ethernet cables which will be connected from the end user devices to the switches to the distribution switches and from the distribution switches to the main switch we will use Gigabit Ethernet cable for faster transmission of data. Also, we will implement Wi-Fi as identified above. This is will be good and beneficial for mobile users who work with laptops and mobile phones. They also add an advantage for this network because many users will be able to access the internet through the computers connected to the network directly as well as through the use of Wi-Fi.

5.2 RELIABILITY ISSUES:

The reliability of a given network is defined by the number of times it fails (frequency of failure), the time of which it takes to recover from a failure (recovery time) and catastrophes (Forouzan, 1998). The proposed network for this company has alternative options which can be used in the case of network failure, disasters or unavailability of the cloud by implementing a Disaster Recovery Plan (DRP). A DRP is an ongoing process of creating testing and maintain the policies and procedures an organization will follow should a disaster occur (SunGuard Recovery Systems Inc., 1995, p.7).

The information that we will backup includes the product designs, accounts information such transaction details, payroll records, employee details, customers and suppliers information. In the case of a disaster or failure to the network, we want to make sure that the information stored is safe and available upon request. Due to the fact we have implemented an outsourcing strategy for the cloud in which we will be saving our information, we have also derived other ways in which

we can ensure the available of the network and the information in the case disaster. One of the activities that we have planned to execute are backups of the information. On a daily basis we will conduct a scheduled backup where we will save all of the information which we have gathered for a particular day in the cloud. On the hand, we will also implement a weekly backup from the cloud to an external storage that we will have in the company. This external storage will not be connect to the network in order to protect it from internal or external attacks in the network is corrupted. Furthermore, we will perform a final backup on a monthly basis where all the information saved in the external backup that we gathered during the end of each week will be saved. This is already practiced by the Central Washington University (2012) hence we can be sure that it is a good practice to implement for our network. The weekly and monthly backups will be manual while the daily backup will be automatic since it will scheduled.

Within the company network itself, some problems may occur such as faulty hardware that may cause a problem in accessing the network. Based on the network diagram plan (see figure 7), if either router 1 fails, we will face problems accessing the network from router 0 to the servers. In case we face such a problem, we will pull the cable of the main switch, and connect it to router 0 directly so that we can keep working with no problems. If the affected devices are the switches connecting from the main switch to the uses in each floor, then we will distribute the PCs of that department to the other departments throughout the building so that the communication and work processes continue.

6.0 SECURITY AND SUSTAINABILITY ISSUES:

The following below are the security and sustainability issues of the proposed network for the company;

6.1 SECURITY ISSUES:

The security issues of this company discuss or talk about the problems that are likely to happen in case we do not use or implement the security measures in this organizations network. We have implemented both physical and network security for the company.

Firewall: This was not identified as a requirement but we have implemented it for an added layer of security to help external and internal attacks. The allocation of the firewall to be the bridge of the network connecting the servers, main network and the cloud (see figure 7) was to make sure that all packets transmitted from either side are checked so that we can prevent internal attacks from the user's side to the servers and external attack from the cloud to the servers or the user's sides. In the cisco packet tracer file, the use of the firewall has prevented the server side and the user's sides to communicate since it is not possible to ping from either side. But that should not be identified as a problem with the network.

FIGURE 15: CISCO ASA 5505 FIREWAL

Email security: As identified by the CEO of this company, the emails are their main communications channel with their customers and suppliers hence they need to make sure that their email server and services are secure. In order to achieve this, we have implemented a few measures as follows; relaying protection to the SMTP access control, this is where the administrator is required to know all authorized users in order to configure the mail server so that only those approved may be able to relay. Another measure is to block hostile addresses from the SMTP access control, this will enable the mail server to be able deny incoming emails from specific email and IP addresses. Encrypting all webmail access by adding a secure socket layer (SSL) to the login page at least. We will also add encryption to the content of data being transmitted by using public key encryption which is provided by applications such as Pretty Good Privacy (PGP). Finally, we will set a maximum message size allowed for the emails so that we can prevent the situations where the server crashes due to large content contained in the email messages (Takamura, 2003). The practice of setting a maximum size for the message is done by companies such as Google where they permit only 25MB.

Policies: Due to malicious threats and other viruses, we have decided to protect this company network by implementing a few policies that can reduce or stop these threats. The policy that we have implemented for this network is to use and automated software to clear all files, documents and any other resource in all of the computers in the company so as we delete any infected files in the computer systems hence protecting the network. Such soft-wares like COMODO are used by many organizations and institutions for the purpose of reducing virus threats or attacks to the network. This software has been implemented and currently used in Asia Pacific University computers located in the lab environment. By using the COMODO software, one can create a scheduled task to restore the computer system once the computer is shutdown. The advantage of this policy is that, any files saved in the computers of the company whether they are affected or not will be deleted so that the computer can be restored to its previous state without any viruses or malicious software to harm the network.

Physical security: The physical security used in this company is managed by the door access systems that permit access to authorized personnel only (Honeywell Security System, 2011). In order to access certain levels or rooms in the company such as the server room, IT, sales and marketing, human resource and R&D departments, the authorized personnel are required to use the access card provided to the by the company in order to unlock the doors. Since it is possible for an employee to lose his/her access card, we have added another layer of security which requires the employees to add a passcode after having flashed their accessed cards. These codes will be updated to the authorized personnel on a weekly basis so that only they can know them and not anybody else.

6.2 SUSTAINABILITY ISSUES:

In this network, we have implemented the use of different techniques in order to ensure that it is sustainable and efficient enough to be used with damaging or threatening the environment. One of the main aspects that we looked at is the significant reduction of power usage and reduction in producing greenhouse gases (GHGs) that cause problems in the environment including climate change. The following are the strategies used in this network in order to ensure its sustainability for use.

Cloud storage: As pointed out by Dahan (2014), the use of leverage of environmental reference whenever possible and acceptable by implementing a cloud storage from external an provider in order to significantly reduce the production of GHGs and energy consumption in an enterprise is highly imperative. In this company, we have implemented a cloud storage which we are hosting from a different external provider so that we can reduce the consumption of energy and power. The use of cloud storages is very productive because it saves the organization costs of buying its own storage device (such as server), less power will be used to run the network especially in cooling the servers and most importantly, we will reduce the emission of GHGs which pollute the environment and causing climate change.

Virtualization: Is a very broad concept that generally refers to as a techniques for hiding physical characteristics of computing resources for the way in which other systems, applications or end users interact with those resources (IBM, 2007, Tebbut, Atherton and Lock, 2009). The impacts of virtualization on energy consumption are a lot but the two main reasons as to why we implemented this to our network are as follows; in a given situation where there is a large traffic load, minimizing the energy consumption can be achieved by launching an optimum number of virtual machines (Jin, Wen and Zhu, 2013), hence, in order to increase the performance of the network by increasing the response time of the network due to traffic load, we have implemented virtual servers in order to take of that. Another impact of virtualization on energy consumption is due to the fact that a substantial amount of energy is consumed when a server is idle, reducing the number of servers by virtualizing them helps at cost reduction, reduction of greenhouse gases (GHGs) hence saving the environment (EEA, 2008c).

Use of server racks with pre-installed built-in fans: An overheating server or computer for that matter can be very dangerous for a user's health or the environment all together. Due to this reason, servers need to be kept in a cool room in order to reduce the heat as it is running. The problems of implementing high-end technology in cooling systems in that it can very expensive at it can also create other environmental problems caused by too much use of power and electricity. In order ensure that the heat of the servers is not too high and that we do not use too much power in running the cooling systems for the server room, we have implemented the use server rack that have built-in fans (see figure 15 below) that can help cool the server as they are still in operation. The use of these racks will not increase the costs of power for the organization because the built-in fans a

large enough the use less energy to cool the servers. They can also be powered by an external power supply such as a small generator since they use a maximum of 30 Watts at full speed. This will help the company save their usage of electric energy and also reduce costs, as a result, the servers will not harm the environment due to over consumption of power (Macworld.co.uk, 2012).

FIGURE 16: SERVER RACK WITH BUILT-IN FANS FOR COOLING

Raised floors in the server room: One of the main advantages of raising server room floors is that is helps in distribution of cold air throughout the room for efficient and easy cooling. With the increasing in advancement of data center technologies, heat densities have increased as well to as high as 10KW per rack (Ctrl Tech, 2015). This can lead to overheating and damage to the servers if not cooled properly. By implementing raised floors, we can seamlessly distribute cool throughout the server room or to specific areas in order to cool the server from bottom-side up since in most server design, the main processing components of the servers are located at the bottom. With the added advantage of using less power for air conditioning and even lesser power to run the built-in fans in the racks (see figure 14 above), we can quickly cool the servers with lesser costs and damage to the environment since there will not be too much use of power and emission of heat causing environmental problems.

7.0 CONCLUSION:

Conclusively, with the available reasons and justifications explained above together with the supporting evidence and critical analysis, it is clear that this network is cost efficient, sustainable, manageable and profitable for the environment and the company. Also, due to the fact we have implemented latest technology that is cost effective and efficient for the company, if they were to deploy this given network proposal, we can be sure that they will face less to no problems and incur more profits because they will not spend too much money in designing and maintaining it because of its efficiency and sustainability.

8.0 REFERENCES:

Avaya.com. (2015). *Avaya Ethernet Routing Switch 3500 Series.* Available at: http://www.avaya.com/usa/documents/avaya-ethernet-routing-switch-3500-series-lb7028.pdf. Last Accessed: 31st August 2015.

Central Washington University, (2012). Information Technology Service: Disaster Response and Recovery Plan – PL408.0

Cisco.com. (2015). *Cisco 3800 Series Integrated Services Routers.* Available at: http://www.cisco.com/c/en/us/products/routers/3800-series-integrated-services-routers-isr/index.html. Last Accessed: 31st August 2015.

Cisco Systems. (2005). *High Availability Campus Network Design— Routed Access Layer using EIGRP or OSPF*. Available at: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/ccmigration_09186a00805fccbf.pdf. Last Accessed: 02nd September 2015.

Cho, H., Kang, M., Park, J., Park, B., & Kim, H. (2007, May). Performance analysis of location estimation algorithm in ZigBee networks using received signal strength. In *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on* (Vol. 2, pp. 302-306). IEEE.

Ctrl Tech. (2015). *Server Room Raised Floor*. Available at: http://www.raisedflooruae.com/server-room-flooring. Last Accessed: 02nd September 2015.

Dahan, U. (2014). *The Architecture Journal: Green Computing.* Available at: http://research.microsoft.com/pubs/78813/aj18_en.pdf. Last Accessed: 01st September 2015.

EEA, (2008c). Impacts of Europe's changing climate — 2008 indicator-based assessment. EEA Report No 4/2008, European Environment Agency. Available at: https://www.energy.eu/publications/THAL08006ENC_002.pdf. Last Accessed: 01st September 2015.

Forouzan, B. A. (1998). Introduction to Data Communication and Networking. Singapore: WCB/McGraw-Hill. (Pp. 18-24).

Honeywell Security Systems. (2011). *Access Systems.* Available at: https://www.security.honeywell.com/me/documents/Access_Systems2011.pdf. Last Accessed: 02nd September 2015.

IBM. (2014). *IBM zEnterprise BC12.* Available at: http://www-03.ibm.com/systems/z/hardware/zenterprise/zbc12.html. Last Accessed: 02nd September 2015.

IBM (2007). *Virtualization in Education.* Available at: http://www-07.ibm.com/solutions/in/education/download/Virtualization%20in%20Education.pdf. Last Accessed: 01st September 2015.

Jin, Y., Wen, Y., Chen, Q., & Zhu, Z. (2013). An empirical investigation of the impact of server virtualization on energy efficiency for green data center. *The Computer Journal*, bxt017. Available at: http://www.ntu.edu.sg/home/ygwen/Paper/JWZC-TCJ-13.pdf. Last Accessed: 01st September 2015.

Macworld.co.uk. (2012). *The 160 Mac mini server rack.* Available at: http://www.macworld.co.uk/news/mac/160-mac-mini-server-rack-3416223/. Last Accessed: 02nd September 2015.

Meador, B. (2008). A Survey of Computer Network Topology and Analysis Examples. *Washington University in St. Louis*.

Microsoft. (2011). *Evaluation Guide Windows Server 2012.* Available at: http://download.microsoft.com/.../WS%202012%20Evaluation%20Guide.pdf. Last Accessed: 03rd September 2015.

Murdoch, S. J., & Watson, R. N. (2008). Metrics for security and performance in low-latency anonymity systems. In *Privacy Enhancing Technologies* (pp. 115-132). Springer Berlin Heidelberg.

Santra, S and Acharjya, P. P. (2013). *A Study and Analysis on Computer Network Topology for Data Communication.* Available at: http://www.ijetae.com/files/Volume3Issue1/IJETAE_0113_84.pdf. Last Accessed: 29th August 2015.

SunGard Recovery Services Inc. (1995). Action Plan for Disaster. Pennsylvania.

Takamura, E. (2003). *Securing Mail Servers.* Available at: http://muspin.gsfc.nasa.gov/download/docs/technical_guides/securing_mail_servers.pdf. Last Accessed: 02nd September 2015.

Tanenbaum, A. S. (2009). *MODERN OPERATING SYSTEMS.* Available at: http://stst.elia.pub.ro/news/SO/Modern%20Operating%20System%20-%20Tanenbaum.pdf. Last Accessed: 03rd September 2015.

Tebbutt, D., Atherton, M. and Lock, T. (2009). *Green IT for Dummies.* Available at: http://www.hp.com/hpinfo/globalcitizenship/environment/productdesign/GreenITforDummiesSpecialEdition.pdf. Last Accessed: 01st September 2015.

Yawut, C., & Kilaso, S. (2011). A wireless sensor network for weather and disaster alarm systems. In *Proc. International Conference on Information and Electronics Engineering, IPCSIT* (Vol. 6).