AZZAM ALWAJEEH

DESIGN IMPLEMENTATION AND PERFORMANCE INVESTIGATION OF A SCALABLE AND RELIABLE

NEU 2018

DESIGN IMPLEMENTATION AND PERFORMANCE INVESTIGATION OF A SCALABLE AND RELIABLE DATA NETWORKING PLATFORM

A THESIS SUBMITTED TO THE GRADUATE SCHOOL OF APPLIED SCIENCES OF NEAR EAST UNIVERSITY

By
Azzam Alwajeeh

In Partial Fulfilment of the Requirements for the Degree of Master of Science in Electrical and Electronic Engineering

NICOSIA, 2018

DESIGN IMPLEMENTATION AND PERFORMANCE INVESTIGATION OF A SCALABLE AND RELIABLE DATA NETWORKING PLATFORM

A THESIS SUBMITTED TO THE GRADUATE SCHOOL OF APPLIED SCIENCES OF NEAR EAST UNIVERSITY

By
Azzam Alwajeeh

In Partial Fulfilment of the Requirements for the Degree of Master of Science in Electrical and Electronic Engineering

NICOSIA, 2018

AZZAM ALWAJEEH: DESIGN IMPLEMENTATION AND PERFORMANCE INVESTIGATION OF A SCALABLE AND RELIABLE DATA NETWORKING PLATFORM

Approval of Director of Graduate School of Applied Sciences

Prof. Dr. Nadire ÇAVUŞ

We certify this thesis is satisfactory for the award of the degree of Master of Science in Electrical and Electronic Engineering

Examining Committee in Charge:

Prof. Dr. Rashad Aliyev	Department of Mathematics, EMU
Assist. Prof. Dr. Ali Serener	Department of Electrical and Electronic Engineering, NEU
Assist. Prof. Dr. Huseyin Haci	Department of Electrical and Electronic Engineering, NEU

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, last name: AZZAM. ALWAJEEH
Signature:
Date:

ACKNOWLEDGEMENTS

First, I would like to thank God for everything and for supplying me with patience and supporting me with faith.

I would like to thank Prof. Dr. Huseyin Haci for his invaluable contributions to my scientific and personal development. He always encouraged me to move forward, develop myself and take the further step. Without his comments and contributions the work of this thesis could not be achieved.

I also send my special thanks to my mother for her care, prayers and her passion. I also appreciate my father's continuous support, advice and encouragement.

Finally, I would like to thank the doctors and colleagues in the lab and school for their support and friendly environment.

ABSTRACT

Networking is an essential thing in organizations, therefore, there can never be establishment of any connection without it. Networking is irreplaceable these days, it must be considered as a very important study in scientific researches. As a result of the importance of networks in the practical life, the design, configuration and connectivity must be done carefully to produce a reliable and scalable networking system platform in a way that it would be flexible and compatible with the development of the technology that is associated with it. The consideration of the network protocols is a critical factor because it manages and organizes the behavior of networks for a specific purpose.

In this thesis, the network tier policy was innovated and created for networking design, while the binomial probability was utilized as a method to obtain the value of system failure probability for a reliable and scalable multi-tiers networking system platform. Multiple networking systems (headquarter, branch and remote home office) were configured and linked with networking protocols, these sites were connected to two internet service providers (ISPs) by fiber connection. Another aim of this thesis was to provide redundancy not only at routing layer or switching layer but also to make sure that the redundancy and the innovated design was provided at each networking tier. Multiple networking systems scenarios were applied to analyse and investigate their performance via two softwares: MATLAB and Packet Tracer. The results were shown via comparing the reliability rate and failure rate of each network systems behavior. There was also the consideration of providing a balanced and fair system in many aspects such as good reliability, economic budget and reduction in the complexity of programming, configuration, and design as much as possible.

Keywords: reliability; scalability; networking tiers; redundancy; load balancing; binomial probability; system model & performance

ÖZET

Ağ, organizasyonlarda önemli bir şeydir, bu nedenle, onsuz hiçbir zaman bir bağlantı kurulmaz. Ağ günümüzde yeri doldurulamaz, bu yüzden bilimsel araştırmalarda çok önemli bir çalışma olarak görülmelidir. Ağların pratik yaşamdaki öneminin bir sonucu olarak, tasarımın, yapılandırmanın ve bağlantının, güvenilir ve ölçeklenebilir bir ağ sistemi platformu oluşturmak için esnek ve teknolojinin geliştirilmesiyle uyumlu olacak şekilde dikkatli bir şekilde yapılması gerekir. ile ilişkili. Ağ protokollerinin değerlendirilmesi kritik bir faktördür, çünkü ağların davranışlarını belirli bir amaç için yönetir ve düzenler.

Bu tezde, ağ katmanı ilkesi yenilendi ve ağ tasarımı için yaratıldı; binom olasılığı, güvenilir ve ölçeklenebilir çok katmanlı bir ağ sistemi platformu için sistem hatası olasılığının değerini elde etmek için bir yöntem olarak kullanıldı. Çoklu ağ sistemleri (merkezi, branch ve uzak ev ofisi) yapılandırıldı ve ağ protokolleri ile bağlantılıydı, bu siteler fiber bağlantı ile iki internet servis sağlayıcısına (ISP) bağlandı. Bu tezin bir başka amacı, sadece yönlendirme katmanında veya anahtarlama katmanında değil, aynı zamanda artıklığın ve yenilik tasarımının her bir ağ katmanında sağlandığından emin olmaktır. İki yazılım üzerinden performanslarını analiz etmek ve araştırmak için çoklu ağ sistemleri senaryoları uygulandı: MATLAB ve Packet Tracer. Sonuçlar, her ağ sistemi davranışının güvenilirlik oranı ve başarısızlık oranı karşılaştırılarak gösterilmiştir. İyi güvenilirlik, ekonomik bütçe ve programlamanın, yapılandırmanın ve tasarımın karmaşıklığının mümkün olduğunca azaltılması gibi pek çok açıdan dengeli ve adil bir sistem sağlama düşüncesi de vardı.

Anahtar Kelimeler: güvenilirlik; ölçeklenebilirlik; ağ katmanları; gereksiz çokluk; yük dengeleme; binom olasılığı; sistem modeli ve performans

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 Motivation

In the coming decades, the network environment expects effective innovative technologies that will contribute to making network systems more reliable and integrated. Figure 1.1 illustrates an example of the environment of networking system reliability, which is represented by headquarter "HQ", branch, and two internet service providers "ISP1","ISP2". More than ever, most business and government organizations demand reliable and scalable connection with the corporate database. Reliability is an essential networking component, it is significant for these organizations to integrate a system that allows robust corporate steadiness approach. Redundancy technologies and protocols must be contemplated deeply and executed carefully. Network redundancy is an unpretentious notion to realize, and when a single point of access is used, it can lead to failure, and there would not be an alternative access to depend on.

Figure 1.1: Illustration of Reliability of Networking Systems Environments

If a subordinate or tertiary technique of connection is implemented, when the core access goes down, a secondary way to associate to resources and retain the connection becomes operational. The major phase in producing networking redundancy, especially in the wide area network "WAN" is to institute a scheme strategy that will consent to inspect the present architecture or infrastructure. This strategy must be able to give room for the publishing, configuration and testing of the whole redundancy networking. There should also be an establishment of policy and procedures that permit the observation of the connections in such a way that it would show signs of warning before things go down, where that proper action would be professionally taken to avoid that. The inquiry is climacteric to create a powerful redundancy strategy. Almost every network established is unparalleled in some technique and that is the reason there must by scrutinization and consideration must not only be placed on popular components that would need redundancy but also on all other classifications that have been put in place but that have not been considered to be a mainframe connection. In undergoing the investigation of a hazard, valuation must take prominence. For example, the core site "HQ" must be involved in consideration if that is the place the bulk of the database is situated or where the plurality of service connections terminates. Switching, routing, and security protocols are significant to be carefully configured to properly manipulate the parameters of the networks that will establish the reliability.

In addition, networking solutions like Cisco networking devices and systems applications must be present where exact protocols can be utilized to encompass the failover progression if executed appropriately. Load balancing, failover resolutions, and protocols are the backbone to create a reliable and integrated networking system. However, reliability should not be deemed important just at the link level of connection. Network links, networking devices such as switches, routers, firewalls, application conveyance controllers, servers, storage methods and others should be reliable. Also, constituent of network devices needs to be reliable. For instance, if the voice traffic carried over unreliable serial links probably encounter dropped packet, as a result of link fluctuation, the best method is to carry voice traffic through the low latency links which do not have packet loss and latency. In case cheaper unreliable connections were utilized,

the data traffic should be carried over them. But actually, whatsoever network device, link or component that is elected, principally they will miscarry.

The optimal and matched reliable network devices, links, component, protocols, and infrastructure must be studied deeply to deliberate and avoid the failure of connectivity. Even if there is a powerful budget capable of providing a large number of network devices and other elements, it will not make a big difference, which is intended to establish the reliability of the network if not used optimally and effectively. All of these paradoxes lead to an important and intentional goal: the reliability of network systems is not only proportional to the quality and quantity of the available network equipment but it is also a proportional factor with technology and protocols used within network devices and systems. This is the reason investigation of networking reliability performance was studied in this thesis.

The networking scalability is considered as a significant part of networking system integration, which measures and provides approbation or application that can expand to meet growing performance demands. For example, in exchanging publishing when it is applied to clustering. Scalability is the aptitude to incrementally increase the number of network clients to a present cluster, while the overall load of the cluster overrides the cluster's capability to produce sufficient performance. To meet the growing up performance requirements of the messaging infrastructure, there are two types of scalability policies that can be implemented, the scaling up and scaling out. Scaling up encompasses augmentation system resources (such as processors, memory, disks, and network adapters) to the prevailing hardware, or substituting present hardware with superior quality system resources. Scaling up is suitable to develop network host response time, such as in an exchange front-end server network load balancing “NLB” configuration. For instance, if the existing hardware is not providing satisfactory performance for network users, adding a random-access memory “RAM” is considered, and also adding central processing units “CPUs” to the servers in “NLB” cluster to meet the requirements can also be considered.

For instance, server boosts singular or several CPUs that imitate the symmetric multiprocessing "SMP" criterion. Utilizing SMP, the operating system can operate threads on any obtainable

processor, which creates its potential for applications to utilize numerous processors when supplementary processing power is necessary to grow up a system's competences. Scaling out encompasses increasing networking devices to meet requirements. In a rear-end server cluster, these leads have increased nodes to the cluster. This is the reason the network systems have been ideally created and studied in this thesis to make them flexible in terms of deployment in the future expansion at the level of users and the level of applications that contribute to the upgrading of network systems.

It should be noted that the scalability and reliability will not reach the desired level unless the networking system is designed carefully in ideal and optimal policy. Network systems must be designed to guarantee that transportation networks can regulate and scale to the requirements for new applications or services. Networking devices and information networks are climacterics to the accomplishment of organizational businesses, both huge and simple. They link network users, assist software and services, and establish access to the database that retains the businesses successively and to meet the regular demands of businesses. These networking systems must also be capable, manageable and supportive to regulate and edit traffic loads to preserve reliable service response times. It is no longer functional to institute networks by linking numerous standalone ingredients without careful strategy and design.

When the networking system is under construction, the structure and strategy of design must make provision for a significant networking factor. The network should operate up all the time, especially during the working time of network clients. Even on the occasion of unsuccessful connections, device failure, and overloaded situations, the network should reliably transport data traffic and prepare sensible response times from any client to any client connection. The networking must also ensure that security is involved in the systems platform in such a way that it will protect the database that is transferred through it and data traffic stowed on the network equipment that links to it. Modifying the network has to be easy to acclimate to system growing and overall service changes alterations. As a result of failure that sometimes happen, troubleshooting of networking issues should not be complicated, and the discovering and solving of issues should not be too time-intensive. This is the reason a new designing protocol or strategy called “networking tier design” was innovated to simplify and facilitate the designing

of networking system platforms in this thesis. The whole networking system is divided into multiple networking tiers and each networking tier consists of single or multiple networking devices.

These networking tiers represent zones that have diverse physical or logical "virtual" connectivity. They contribute in designating where various services occur in the network. This tiering supports flexibility in networking design, it eases enforcements and issues investigation. This tiering protocol has amazing advantages among which is that it establishes a deterministic networking system with obviously demarcated borders between layers. It also prepares obvious demarcation positions so that the network engineer cognizes precisely where the data traffic creates and where its inflows. It also guarantees the scalability by allowing enterprises to increase layers or networking devices easily. As a networking system platforms complication arises, the networking engineer will be able to install new application services from it and also helps the network administrator to configure networking protocols and resolutions without manipulating the underlying networking system model.

While gathering designing factors by this strategy, the network engineer classifies the problems that disturb the whole networking system and those that make issues only with specific tiers. By creating a tiering topology protocol, the network administrator can insulate networking tiers of concern and distinguish the performance of the systems. The networking tier protocol also analyzes the reliability and failure of each tier or the entire networking system to realize the effect of a specific requirement to expand beyond the original estimate of the networking system. This innovated supervision can greatly develop the performance and provide the required bandwidth where the data traffic will be transmitted through it.

1.2 Challenges

In order to have a reliable and scalable network, the security, privacy, and reliability must be established on each prime network ingredients. Therefore, the first challenge in this thesis was how to obtain the reliability, scalability and avoid the failure at all levels of networking system platforms. For example, if there is no authenticated technique to oblige security protecting each data traffic transaction on prime network ingredients, a networking system cannot be depended

on, in this kind of performance trustworthy model. The system failures are solved when the main link or networking component is down, it needs to be failover and backing up the behavior of this component before the whole connection also terminates. The most amazing thing is establishing the reliability at all layers and levels of the core network system ingredient and the standby network system ingredient. It means that providing a redundant ISP is useless unless the switching, routing, security and physical tiers do not have failover. This is the unique and innovated factor that has already been applied to the project to remedy this kind of challenge.

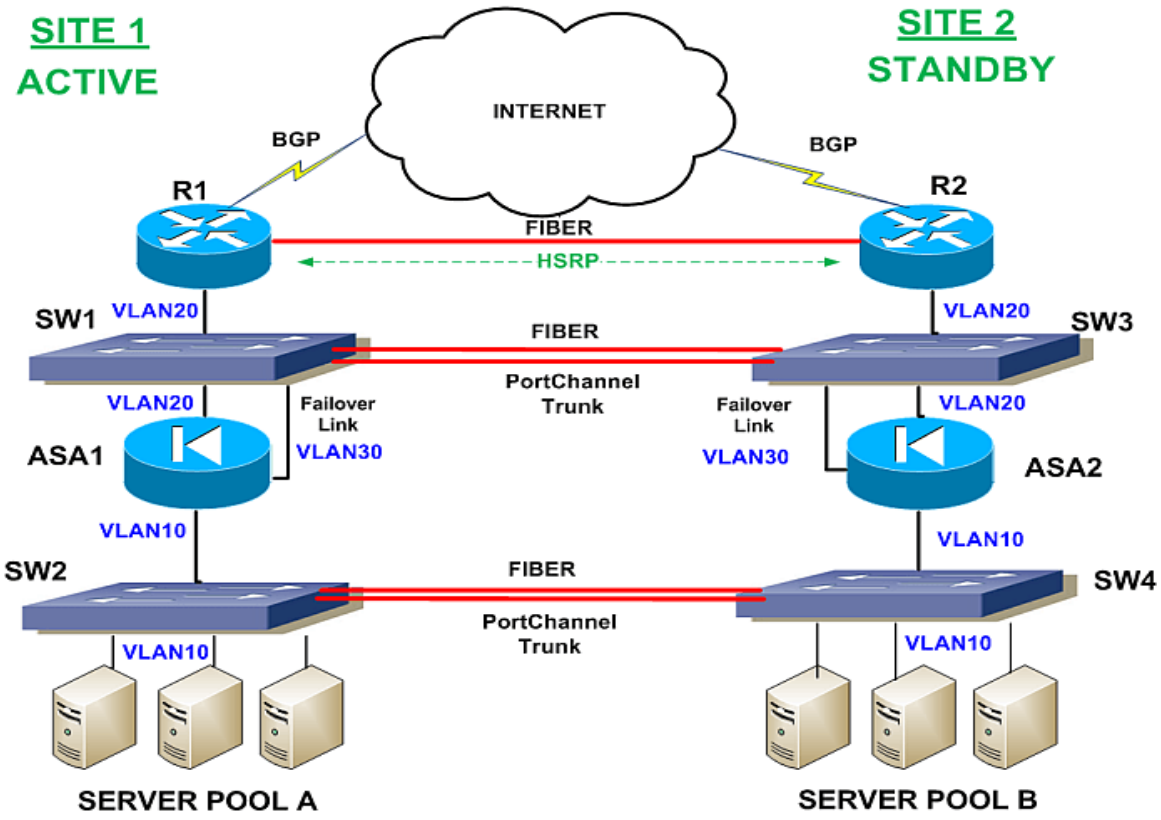


Figure 1.2: Illustration of networking reliability at the entire site level.

For instance, figure 1.2 is a clarification of networking reliability at the entire site level. Overall, the redundancy is approached through active/standby policy in all ingredients of the networking sites. Site 1 is the active networking site and site 2 is the standby networking site. During the regular process, data traffic influxes from the ISP forwards networking site 1 in order to access

“server pool A”. Where the failure of layer 3 has been dealt with by implementing Hot Standby Router Protocol “HSRP” at both routers R1 and R2. A fiber optic connection operates between the R1 and R2 to reduce certain failure situations and to contribute to better working operations of the HSRP mechanism. The switches SW1 and SW2 represent the layer 2 of the system. The failure of this layer is terminated by linking these two switches to each other with two fiber optic connections, and the two connections are configured as port-channel “EtherChannel” and trunk situation. The two networking firewalls ASA1 and ASA2 are programmed in an Active/Standby situation, while the ASA1 is in active mode, the ASA2 is in standby mode. The failure of firewalls has been handled by the failover connections between them and placed across the Layer 2 switches SW1 and SW3 and the trunked fiber optic connections (Chaturvedi, 2016).

Based on the illustration of Figure 1.2 above, both failover connections relate to VLAN30, it is as it has been directly linked in the same Layer 2 VLAN. The outside networking ports two firewalls relate to VLAN 20 and the inside networking ports relate to VLAN10 "the same VLANs on two sites". The outside and inside firewalls connections have Layer 2 connectivity, thus, the failover operation will run successfully. Analyzing and evaluating the reliability of network systems is one of the most eloquent factors that contribute to reducing failure. Thus, this analysis and study cannot reach its intended goal without the implementation of scenarios and cases of practical failures in the intended network system. The layer 3 failure represented when the router R1 is dead or down. In this issue, the HSRP will elect router R2 as the dominant router of layer 3. While the data traffic will influx as the following:

Internet ⟶ R2 ⟶ SW3 ⟶ ASA1 (via fiber optic) ⟶ server pool A.

Where the failure of layer 2 is assumed when switch SW1 is down or terminated for some reason. Router R2 and firewall ASA2 will be selected as active networking devices and the route of data traffic will flow as the next:

Internet ⟶ R2 ⟶ SW3 ⟶ ASA2 ⟶ SW4 ⟶ SW2 ⟶ server pool A.

The failure of a security layer is assumed when the firewall ASA1 is dying, then the secondary firewall will be in active mode and the data traffic flow will be as the next route:

Internet ⟶ R1 ⟶ SW1 ⟶ SW3 ⟶ ASA2 ⟶ SW4 ⟶ SW2 ⟶ server pool A.

The second challenge in this thesis is how to obtain the balance at designing the infrastructure, and integration of networking system while taking into consideration reducing the configuration complexity, enhance reliability, and fairness at the budget. The third challenge is the difficulty in analyzing and studying each networking tier accurately and carefully, otherwise, the performance of networking system will not approach the desired level, which is intended to provide and deliver network application services in a comforted and eloquent method. In this thesis, the binomial probability function was utilized to analyze and obtain the value of system failure probability for each network tier (Andrea, 2016).

1.3 Contribution of the Thesis

The objective of this thesis was to design and implement a scalable and reliable networking system platform, address its challenges and investigate its performance. The contributions of this thesis include:

1. Multiple networking protocols and technologies were proposed to perform a reliable and scalable networking system platform. The EtherChannel protocol was utilized at layer 2 switches to increase the performance of the channel capacity between networking devices and providing load balancing, scalability, and reliability. The HSRP protocol was configured at the layer 3 networking devices to provide the failover at routes of packets traffic. While the main scenario of this thesis has tunnel connection between two HQ and branch networking system, this channel was secured by the site to site VPN tunnel technology. The VLAN protocol was also implemented to make the networking more flexible, secure and private. The BGP routing protocol was established to provide magnificent functions and features, especially to optimize the load balancing and the reliability at WAN or ISP level.

2. Design a network tier by using the binomial probability to analyze and obtain the value of system failure probability. The purpose was to design and analyze a single network tier to simplify the analysis of performance and reduce the fault in networking design. An innovated tiering protocol was applied to design to provide performance analysis of a multi-tier data networking platform. The connectivity models between tiers were mentioned to show the

comparison between these modes of connection and to elucidate the pros and cons of each network tier connectivity model.

3. The performance of two tiers system was investigated. This investigation was based on the manipulation of the number of networking devices at each networking tier to reach the optimum and ideal performance of reliability. The first part of this investigation showed the effect of changing the number of ISPs on the behavior and performance of the networking system, then select the reliable and scalable system with fairness budget and less complexity. The second part of the investigation has shown that having one switch in core switch tier will be unreliable even with existing multiple ISPs (2 or 3 ISPs). Thus, it is important to have at least two or more switches at core switching level and at least two or more ISPs at WAN or ISP level. The last part of the investigation about networking system consists of 3 networking tiers. The objective of this investigation was to choose the performance of a balanced network system in several aspects such as reliability, complexity, and budget.

1.4 Structure of the Thesis

This thesis is organized into six chapters and an appendices and they are summarized as follows:

In **Chapter 1**, the motivation and challenges of design implementation and performance analyzing of scalable and reliable data networking platform were discussed. The main contributions of the thesis to address these challenges were summarized. Also, the structure of the thesis was given.

In **Chapter 2**, theoretical basis of the Layer 2 Switching and Spanning Tree Protocol (STP), the principle of Voice over Internet Protocol "VOIP" and the principle of routing were presented. Moreover, wireless networking topologies were surveyed.

In **Chapter 3**, the system model as well as overview of a multi-tier data networking platform and protocols configuration of a multi-tiers data networking platform were introduced.

In **Chapter 4**, the concept of designing a Multi-Tier Data Networking Platform was introduced and its performance analyses were given. Designing a network tier was explained to contribute to analyzing its performance. Designing of multi-tier networking platform was given to facilitate the investigation of the whole networking system performance. The connectivity models between networking tiers were given to compare the features of structure and design between them.

In **Chapter 5**, representative numerical results were shown in two parts to evaluate the performance of proposed multi-tier networking platforms. In the first part, the performance analyses of two tiers Systems were surveyed. In the second part, the performance analyses of Three Tiers Systems were shown and compared with each other to produce the optimum networking system.

In **Chapter 6**, the summary and conclusions of the thesis were given and interesting future research directions were discussed.

In **Appendices,** the analysis and source codes to obtain the reliability and failure rate of multi-tiers networking performance platforms were presented. Moreover, the source codes to configure and program all the networking device were also presented.

CHAPTER 2
BACKGROUND THEORY

2.1 Layer 2 Switching Protocols

Going back in time and taking a glance at the condition of networks before switches were introduced and how switches have helped phase the company local area network would be carried out in this section. Before local area network switch, the standard network design appeared like the network in figure 2.1. The design in figure 2.1 was referred to as a folded backbone as a result of the fact that all hosts would want to go to the company backbone to succeed in any network services, both local area network and mainframe.

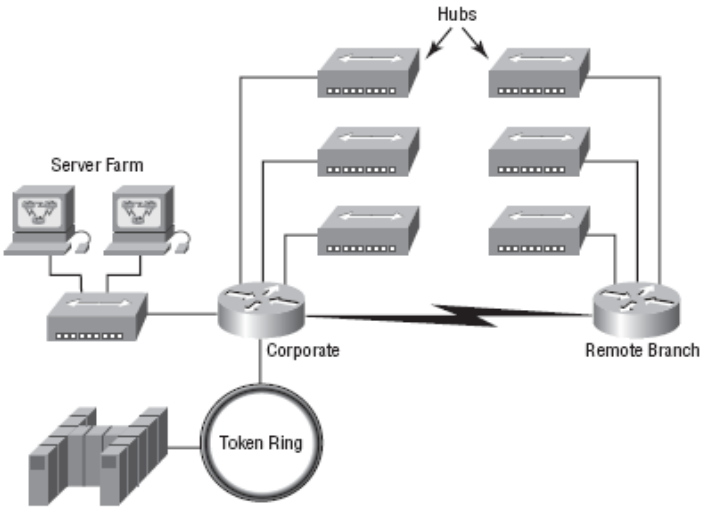


Figure 2.1: The First Switched LAN.

Each hub was placed into a switch port, associated with a degree of innovation that immensely improved the network. Now, rather than every building being crammed into identical collision domain, every hub became its own separate collision domain. However, there was a catch, switch ports were still terribly new, hence unbelievably costly. Due to that, merely adding a switch into every floor of the building just wasn't progressing to happen at least, not yet. One of the impart of these is that it has dramatically increased the possibility of these switches,

therefore, having all of network users obstructed into a switch port is now smart and possible. Hence, there is progress in the production and implementation of modern network styles to include switching services. A typical modern network style would look one thing like figure 2.2, a whole switched network style and its implementation.

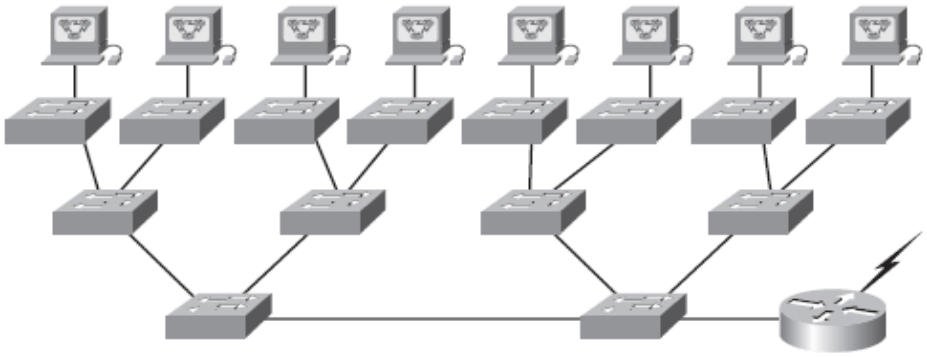


Figure 2.2: The Typical Switched Network Design

There is a router in this design but its job has been modified in such a way that rather than playing physical segmentation it currently creates and handles logical segmentation. These logical segments are known as Virtual LANs (VLANs). The VLANs will be explained thoroughly later. There are three distinct functions of layer 2 switching and these are address learning, forward/filter decisions, and loop avoidance (Bligh, 2015).

2.1.1 The Three Switch Functions at Layer 2

As stated above, there are three distinct functions of layer 2 switching: address learning, forward/filter decisions, and loop avoidance.

1. Address Learning

When a switch is initially supercharged on, the MAC forward/filter table is empty, as shown in Figure 2.3.

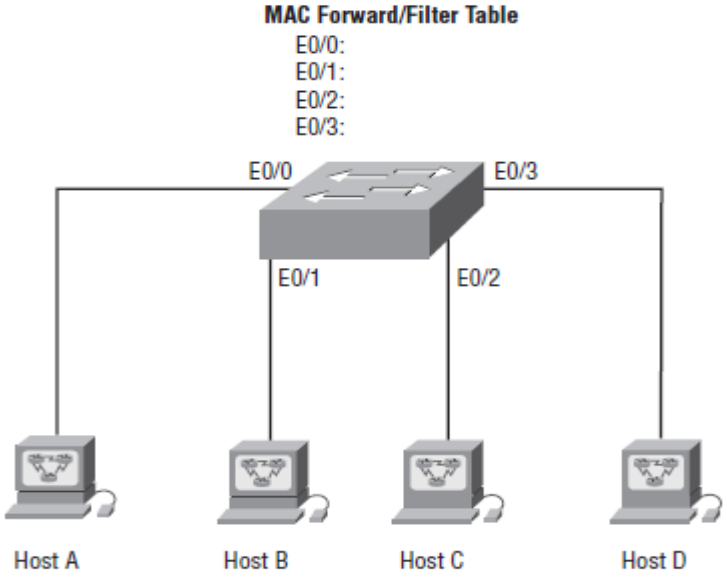


Figure 2.3: Empty Forward/Filter Table on a Switch.

When a tool transmits and the port receives a frame, the switch puts the frame's origin address within the media access control address forward/filter table, permitting it to save which port the causation device is found on. The switch then has no selection, however, to flood the network with this frame out of each interface except the source interface as a result of its no plan on where the destination device is really placed. If a tool answers this flooded frame and sends the frame again, then the switch can take the origin address from that frame and place that media access control address in its info, moreover, associating this address with the interface that received the frame. Since the switch currently has each of the relevant media access control addresses in its filtration table, the 2 tools will create a point-to-point communication. The switch doesn't have to be compelled to flood the frame because it did at the initial stage and the frames will be forwarded just between the 2 devices. This can precisely be the factor that brings about the production of a level 2 switches that are higher than hubs. In an exceedingly hub networking, all frames area unit forward all ports out in each time no matter what. Figure 2.4 shows the processes involved in building a media access control info.

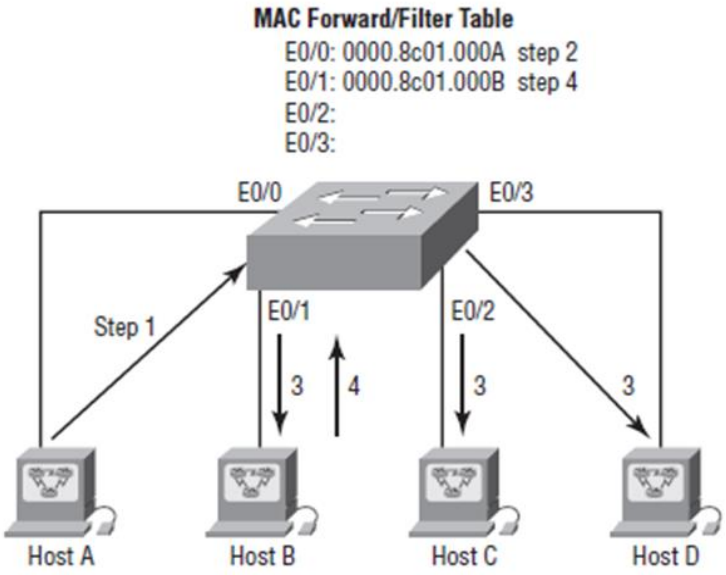


Figure 2.4: How Switches Learn Hosts' Locations.

In Figure 2.4, four clients hooked up to a switch. Once the switch is supplied by power, it has nothing in its media access control address forward/filter table, even as in Figure 2.4. However, once the clients start communication, the switch places the origin address of every frame inside table along with the interface that the frame's address is compatible with. An example about how a forward/filter table is populated will be explained. The first procedure, Client A sends a frame to Client B. Client A's MAC address is 000A, Client B's media access control address is 000B. The second step, the switch takes the frame on the port e0/0 and put the source address in the media access control address table. When the wanted address is not in the media access control database, the frame is directed out on all ports except the origin port. Then client B take the frame and send response to Client A. The switch takes the frame on port e0/1 and put the origin address in the media access control database. In the last step, both Clients A & B can now make a point-to-point communication and just the 2 tools will take the frames. Client C and D can't see the frames, nor are their media access control addresses found in the database as they didn't send a frame to the switch (Lammle, 2013).

2. Forward/Filter Decisions

When Client A's media access control address does not exist in the forward/filter list, the switch will take in the origin address and interface to the address list and then redirect the frame to

Client D. If Client D's media access control address did not exist in the forward/filter list, the switch would have filled the frame out on all interface except interface fa0/3. Assuming the previous switch got a frame with these media access control addresses: S.MAC: 0005.dccb.d74b and D.MAC: 000a.f467.9e8c. How will the switch treat this frame? The solution is that the wanted media access control address will be caught in the media access control address list and the frame will be redirected out through fa0/3. If the wanted media access control address is not caught in the forward/filter list, it will redirect the frame out on all interfaces of the switch searching for the wanted device. For this, the ability to access the media access control address list and the switches is possible, but more Clients addresses must be put into the forward filter list (Odom, 2013).

3. Loop Avoidance

Additional links via switches are a useful idea since they support the prevention of failure of all network in case one link failed to work. But even additional links cannot be completely helpful, they almost make more issues than they solve them. The reason is that there is possibility that frames can be completely down as well as all additional links at the same time, thereby creating network loops as well as other dangers. Some of the worst issues include a case where there is no placement of loop dodging schemes in the original position, the switches can flood broadcasts infinitely throughout the internetwork. This often indicate a broadcast storm. Figure 2.5 shows clearly that a broadcast will be widespread in all of the internet-work in such situation. It is important to ensure that a frame is always being flooded through the internetwork's physical network media (Shooman, 2003).

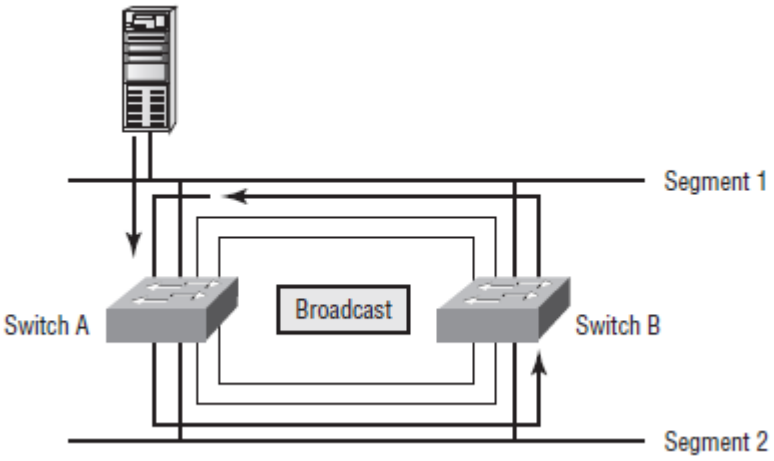


Figure 2.5: Broadcast Storm

A tool can take multiple copies of the same frame when that frame can reach from different sections at the same time. Figure 2.6 explains how all the bunch of frames can reach from multi-sections at the same time. The server in the figure gives a unicast frame to the Router C. While it's a unicast frame, switch A redirects the frame and switch B supply the same service and it redirects the broadcast. It is considered not to be good because the Router C takes that unicast frame two times, making the extra load on the internetwork.

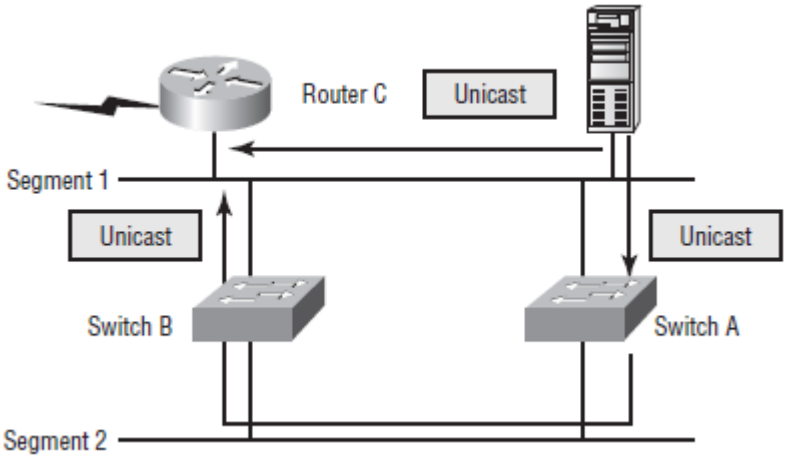


Figure 2.6: Multiple frame copies

The media access control address filter list might be wholly confused regarding the tools' location as a result of the switch getting the frame over one link. In addition, the bemused switch may get trapped in perpetually changing the media access control filter list with origin address

locations that it will fail to redirect a frame. This can be referred to as thrashing the media access control table. The deepest things that can happen is that there is going to be generation of multiple loops throughout an internetwork. These leads loops can happen inside another loop, in case a broadcast storm was to happen, the internetwork would not be ready to provide frame switching period. These issues spell disaster (or a minimum of something near it) and there are a lot of evil things that must be avoided. That is where the Spanning Tree Protocol gets into the game. It was developed to resolve each of all the issues that may arise in the network.

2.1.2 Spanning Tree Protocol (STP)

The main goal of using STP is to prevent internetwork loops from happening on both of bridges and switches in your layer two level internetwork. It watchfully observes the network to see the whole links, and to ensure that there are no loops happening by turning off any additional links. STP operates the spanning-tree algorithm (STA) first to initially produce a topology InfoBase and then find out and destroy additional links. When we run the STP, frames will be redirected just to the premium.

STP operates 3 procedures to produce a loop-free network topology.

1. Elects 1 root bridge.
2. Choose 1 root port per Non-Root Bridge.
3. Choose 1 selected port on every network phase.

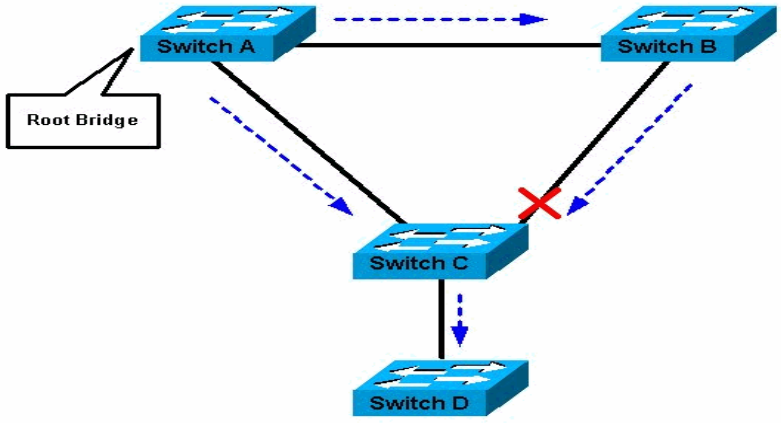


Figure 2.7: Regular STP Operation

Convergence, in case of spanning tree protocol, happens once all the interfaces on bridges and switches have moved to either redirecting or blocking cases. No data is redirected till

convergence is completely done, therefore, the time for convergence, once the configuration changes, are extremely vital. Quick convergence is extremely fascinating in giant networks. The traditional convergence time is fifty seconds for 802.1D spanning tree protocol (which is very slow), however, the timers will be connected. Since spanning tree protocol is activated, each switch within the network goes via the case of block and also the transient cases of both listening & learning. And the interfaces become stable to the redirecting or block situation.

Table 2.1: Explain Briefly the STP Port States

State	Can forward data?	Learn MAC?	Timer	Transitory or Stable State?
Blocking	No	No	Max Age (20 sec)	Stable
Listening	No	No	Forward Delay (15 sec)	Transitory
Learning	No	Yes	Forward Delay	Transitory
Forwarding	Yes	Yes		Stable

2.1.3 EtherChannel Protocol

This section will present the approach of an EtherChannel technique for three major switches supporting our "HQ" network. Every two switches have one EtherChannel port channel connection between them, while our purpose for using the EtherChannel protocol in this thesis was to provide redundant links between switches and increase the performance of the channel capacity of the network device. In addition to that, the most important characteristics of EtherChannel were to provide load balancing, scalability, and reliability. The next advanced explanations will show how the EtherChannel provided these awesome features in the network environment of this thesis. Scalability of EtherChannel protocol usage in the thesis by the scenario which has two switches connected together through the link (100MBps) inside the organization as shown in Figure 2.8.

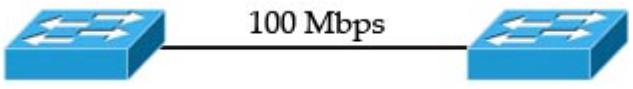


Figure 2.8: Normal Channel between 2 Switches

Suppose in the future the number of hosts inside the organization increases more and more so that the channels or ports between the switches would have a lot of loads and pressure to transfer the data to these hosts. While the ports or interfaces will not handle these huge loads at the same time but what will happen if we connect the additional link between them. Of course, the additional link will not work and it will be blocked by Spanning Tree Protocol "STP" to prevent the loop from happening as shown in Figure 2.9.

Figure 2.9: STP Block the Additional Channel

In this situation, the network was not designed and implemented for scalability in the future. The solution of scalability in this thesis was an EtherChannel protocol that was utilized to merge multiple physical ports into one logical port or one port and consider them as one connection. In this case, the bandwidth of the channel would increase to support more hosts. In addition to that, the "STP" would not block the EtherChannel because "STP" would see it as one logical port as shown in Figure 2.10.

Figure 2.10: EtherChannel Technique

The EtherChannel protocol provides high reliability and load balancing inside networking system platform. Based on the EtherChannel technique that was operated and working very well between the two previous switches that connected to each other via EtherChannel in this scenario. One would be wondering what would happen if suddenly one of the two links broke down for some reasons as shown in Figure 2.11.

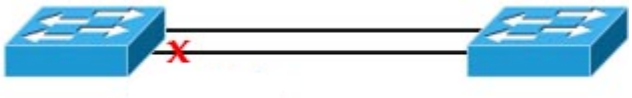


Figure 2.11: One Link of EtherChannel Failed

Has the connection between two switches stopped? Of course no, if at least one of the two links is working fine, the communication would still be alive even if one link failed. This awesome feature provided for load balancing in this thesis. When the EtherChannel is utilized, EtherChannel can be more than two links to establish the connection. EtherChannel is capable of maximizing the capacity of communication up to eight Gigabit Ethernet ports merged together to represent the EtherChannel. This point indicates that when the number of the merged ports of EtherChannel is increased the reliability will increase inside the networking system as shown in Figure 2.12.

Figure 2.12: Reliability & Load Balancing of EtherChannel

2.1.4 Virtual Local Area Network (VLAN)

This section explains more details about VLAN and show the advantages and the main purpose of utilizing this protocol. The VLAN is considered as a logical grouping of network clients and network resources inside one broadcast domain. It means that networking devices which exist in the same VLAN are separated from the other VLANs or other LANs. The main concept of VLAN is to divide the main LAN into multiple VLANs and multiple broadcast domains because each VLAN acts as one broadcast domain for the whole networking system. Where the data traffic will be switched just between interfaces or ports that are related to the same VLAN. Understanding the VLAN based on advanced example will clarify the benefits of VLAN suppose the networking system platform consists of multiple departments.

One department is called ‘Sales’ and has its own resources, the second department is named ‘Technical’ also with its own resources. Since each department has its resources, they are separated from each other. Applying this scenario without using VLANs will be easy. The two networks will be assigned to these two departments and utilize the ACLs to control who will access the networking resources of each department. The sales department will be configured with network 192.168.1.0/24, while the technical department will be configured with network

192.168.2.0/24. The Figure 2.13 includes and describes the example of configuring networking system platform without utilizing VLANs.

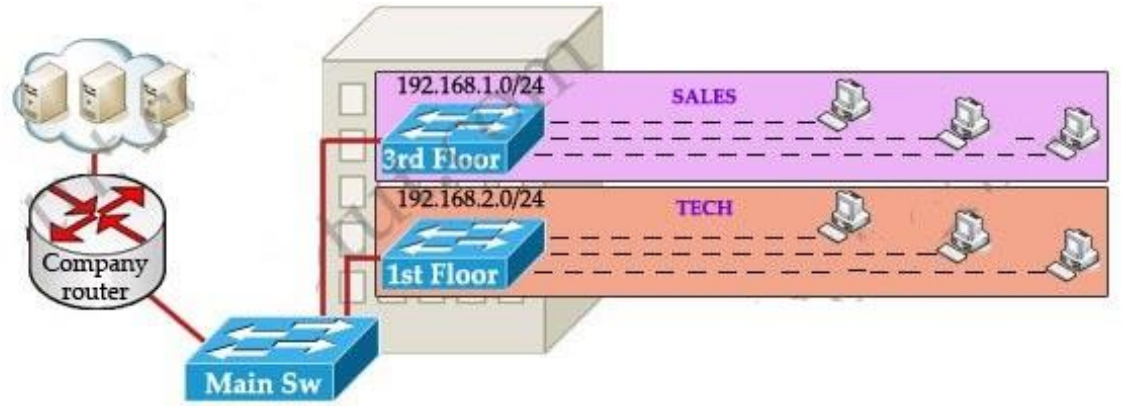


Figure 2.13: A Topology of Networking System Platform without VLANs

The configuration of networking system seems good, but on the other hand, it has a lot of disadvantages. In this case, the leaders or some staffs need more privileges to access a credential database, while some other staffs are not allowed to access it. Suppose the number of technical staffs increased and the first floor is full, they must sit on the sales floor, then they will have access to the resources of sales staffs which only sales staffs are allowed to access. In the same vein, creating the ACLs for each leader is so sophisticated to be implemented. All these networking issues can be solved by using the VLANs instead of LANs because VLANs recognize the logical groups of networking users, while it does not care about the physical network or locations. The VLANs provide the flexibility by letting the network users use the networks from several locations. After configuring VLANs inside the whole networking system, awesome features are added.

For example, the network users can share the database from any desired location. The VLANs enhance the performance of the networking system because it reduces sending the data traffic inside the network to unwanted destination. Suppose there are 50 users per one broadcast domain in the network, after applying VLANs, each 25 network users can be in separate VLAN. In this case, the broadcast traffic is reduced to 50 percent, hence the performance of the network will be better. VLANs simplify the administration because the users in organizations always try to move from location to another but with the use of VLANs there is no need for that. A lot of

physical things should also be provided like new cabling, new hardware, and reconfiguration of the routers. VLANs avoid all these points and provide a perfect management for the network environments. VLANs provide security since each VLAN has network IP, it reduces the confidential data traffic from broadcasting by managing each VLANs and apply rules on it like access list.

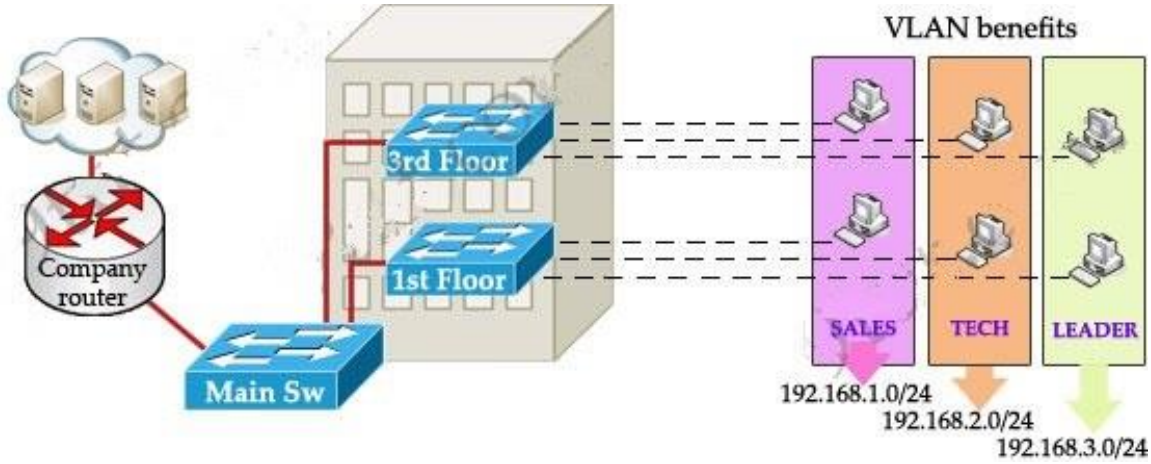


Figure 2.14: A Topology of Networking System Platform with VLANs.

When the VLANs are configured inside the networking system which has multiple switches, the link between the switches must be programmed as a VLAN trunk link. The switches put a tag on each frame sent across these switches. And the receiver's switches will identify the VLAN and that the frame is special and related to it. The tag is called VLAN ID, which is indicated by a number to represent it. Figure 2.15 represents an example of a trunk link between switches.

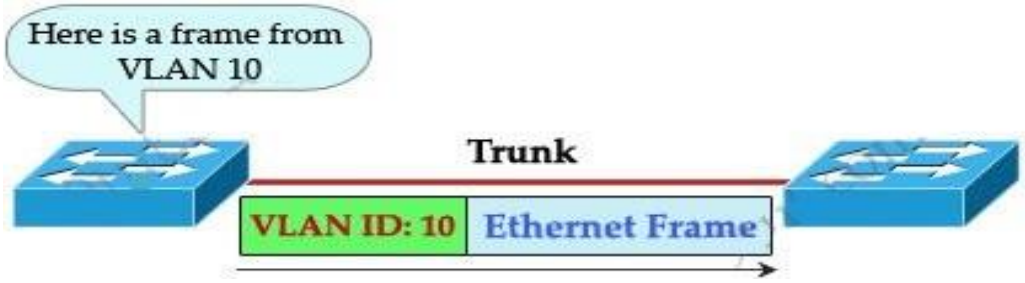


Figure 2.15: An Example of VLAN Trunking between Switches.

The sender switch adds the tag to the frame, then the receiver switch removes the tag from this frame that is sent via a trunk link. While the network clients do not have any idea or background about all these operations. Figure 2.16 clears and explains these operations.

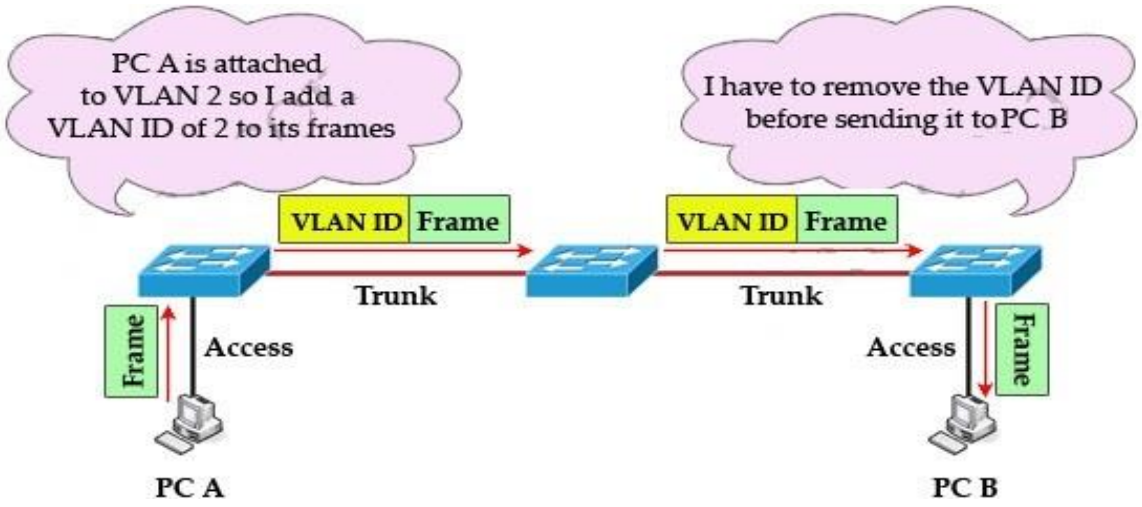


Figure 2.16: An Example of Trunking by Adding and Removing Tag.

2.2 The principle of Voice over Internet Protocol (VoIP)

The telephone system is utilized (referred to as a Private Branch Exchange "PBX") each day, therefore, the information that telephone systems handle include the control of call and the management of the communication to the telephone company supplier. VoIP could be modified and upgraded to creating calls across (LAN) and/or (WAN). The technology behind VoIP converts analog voice into digital packets that area unit then sent across a network (IP) to their final destination. VoIP is most typically related to the creation of calls across the (IP). Since a VoIP communication system uses Voice over IP that is connected to the local area network, most voice technology will be linked to the Public Switched Telephone Network. This provides the flexibility to utilize each VoIP technology and, therefore, the PSTN technology for business.

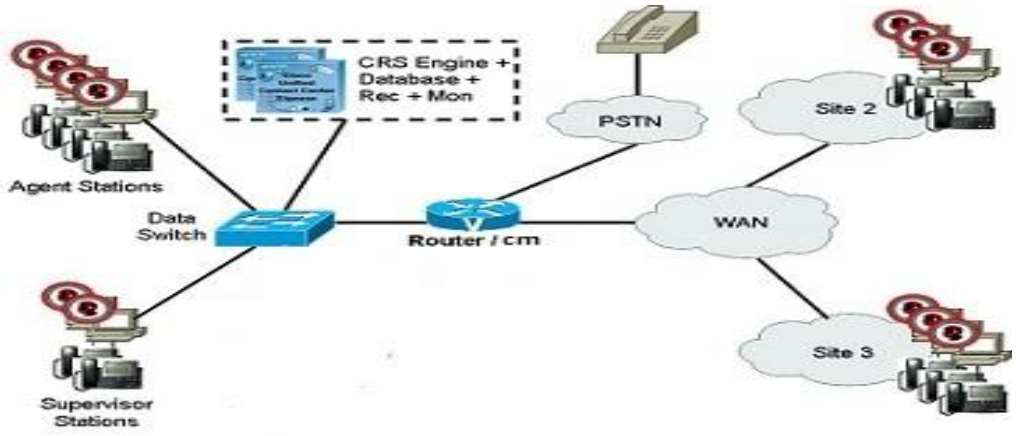


Figure 2.17: Represent the VoIP Connection Across WAN & LAN

2.2.1 The Common Methods of Using VoIP Technology

The most pressing issue concerning the use of VoIP is that there is no one method to make a service. There are three totally different methods of VoIP technology in common usage in contemporary time. The first method is the use of Analog Telephone Adaptor "ATA" which is a simple and common approach. The Analog Telephone Adaptor permits the linking of a regular phone to a pc or network communication to be used within VoIP. The analog signal is being transformed to a digital signal by the use of analog telephone adapter. ATA gets the analog from our normal phone and converts the signal to digital information to be sent across the network. Suppliers such as Vonage and AT&T CallVantage ensure that they combine ATAs without cost with their service. They crack the analog telephone adapter far off the box, connect the cable from the phone which may usually get into the electric outlet into the ATA, and ability to build VoIP calls. Some ATAs could be shipped with further package that is loaded onto the host PC to put it together. However, in any case, it is a terribly simple setup (Cioara and Valentine, 2011).

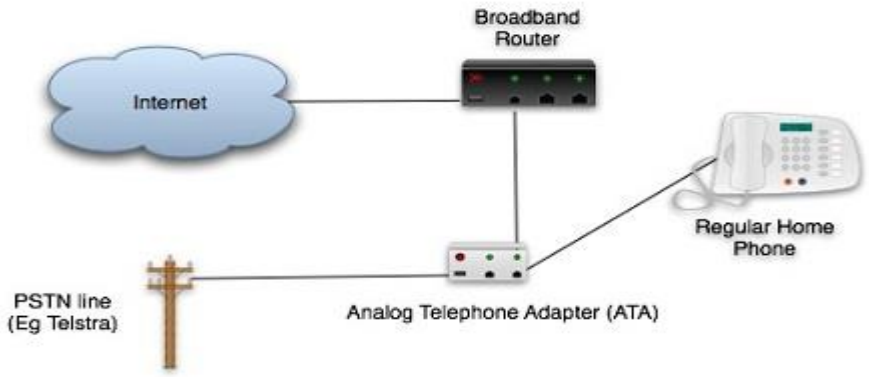


Figure 2.18: Example for ATA Method

The IP phone is the second method of using VOIP technology. The IP phones are customized and more advanced phones though they seem a bit similar to regular phones, they have extra features and hardware equipment like buttons, headsets, and cradle that differ them from the regular phones. However, rather than having the head RJ-11 phone connectors, phones over IP have associate RJ-45 local area network linker. The phones over IP have direct connections with the router, in addition to that they have hardware and software systems that make them treat calls over IP. Phones over Wi-Fi enable subscribers of this service to create calls over IP via Wi-Fi hotspot.

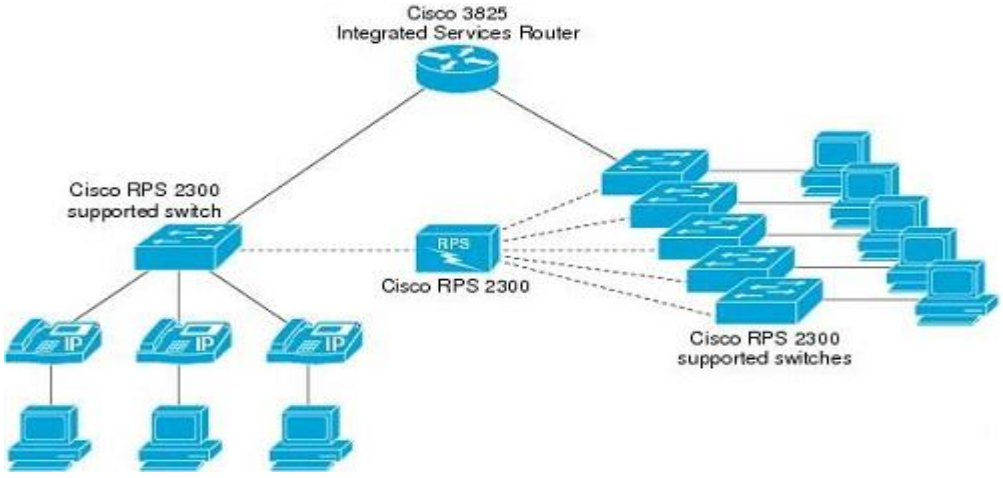


Figure 2.19: IP Phones Systems Method

Computer to computer method is considered as the simplest method to use the technology of voice over IP where there is no cost for calls made to distances that are very far. Many

organizations providing no-cost calls or terribly low-priced package make use of this kind of voice over IP. The package includes audio speaker, sound card and a network communication, and it is ideally a quick one such as you would have through the use of Digital Subscriber Line modem "DSL" and cable. Apart from your regular periodic money payment for internet service provider "ISP", there is almost no charge if the calls are created from PC to PC, irrespective of the space in-between them (VoIP Supply, 2014).

2.2.2 The Features & Benefits of VoIP Phone System

1. Flexibility & integration of VoIP phone system

Despite the fact that there are various services technology that could be implemented such as the use of network and basic voice technology, Voice over IP phone system stands out because of its flexibility and the ease with which it could be integrated into the network of an organization. This flexibility and the ease with which it could be integrated give room for sales expansion, productivity and efficiency in an organization (Crubsy, 2017).

2. Supporting power over Ethernet "PoE"

VoIP phones support and are compatible with Power over Ethernet "PoE". This means that the phones can be fed power through the switch that supports Power over Ethernet rather than through the use of an energy adapter. That factor decreases muddle on our table and facilitates management of inventory. This feature keeps your budget economic since the people typically buy adapters of energy individually from the phones.

3. Supporting HD Voice

HD voice is supported and can be produced by utilizing VoIP phones, whereas alternative commercial phones do not support HD Voice. It is an established fact that the propagation of voice over a regular landline is at a quality of 3.4KHz, the propagation of audio to be in High Definition is believed to be around 7KHz. It can, therefore, be concluded that since VoIP phones support HD voice, one VoIP phone would propagate twice better than a regular phone.

2.3 General Wireless Networking Topologies

In explanation of wireless network topologies, it is important to note that there are many parts to the concept. Therefore, there is complete difference between a wireless local area network and a wireless personal area network. The subsequent sections explain the characteristics of each of these networks, what they intend to perform, and varieties of wireless network technologies associated with each of them. Figure 2.20 shows clearly the different wireless networks topologies.

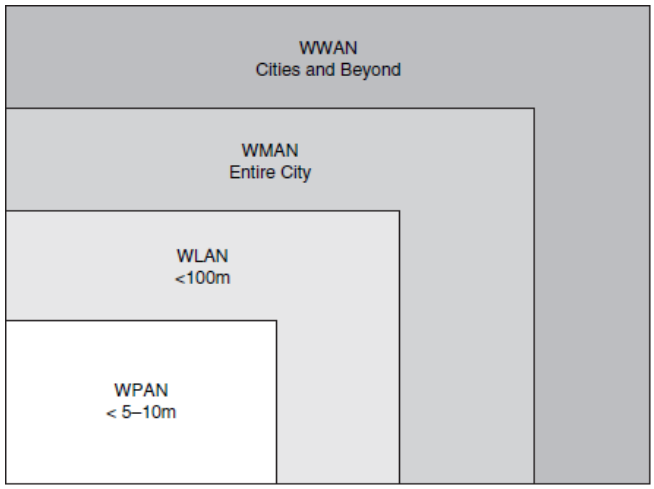


Figure 2.20: Wireless Networks Topologies

2.3.1 Wireless Personal Area Network (WPAN)

WPAN is considered as a wireless network which is created to work within the area of a 20-foot band. The most common form of WPAN is a bluetooth. When a network of bluetooth is utilized, the communication spectrum should be at a range of 2.4 GHz. The network of bluetooth piconets can include up to 8 activated end-point devices, however, it can be able to include several inactive devices. The wireless network WPANs is typically considered with the unlicensed 2.4-GHz frequency range where WPANs are standardized by the workgroup of 802.15 IEEE. The area of WPAN is considered to be as short as 5-10 meters when compared with other technologies. WPAN is also known as “piconet”.

Figure 2.21: WPAN Topology

2.3.2 Wireless Local Area Network (WLAN)

WLAN is considered as a wireless network which is created to work for a wider range when compares to the range of WPAN. It has the ability of extending from terribly small houses and offices to giant organizations networks. Organizations can be said to be in a local area when they conjointly manage their wireless network or when they have the same instrumentation. Therefore, the characteristics of WLAN include the fact that WLAN is unlicensed and can communicate on 2.4 GHz or 5 GHz frequency range. The area of WLAN is considered as bigger than WPAN near to 100 meters from access Point (AP) to the host. To perform further space, additional output of energy is needed. WLAN cannot be treated in the same way as personal network, therefore, there is a prospect of having additional hosts on its network (Carroll, 2008). One of the advantages of WLAN is that it is so flexible to the extent that there is possibility of allowing more than 8 active hosts to be added to the WLAN. This shows that WLAN is more flexible than WPAN. As the wireless networks WLAN operate bigger areas, the networks need an additional output of energy when compared with WPAN. In addition to that, the energy output must be monitored to ensure that it does not reach the power limit for overloads. WLAN also has the ability of sharing the network database on mobile hosts and that is the reason it is possible to see multiple users on a WLAN. In addition, the WLAN allows for some other wireless devices on its network such as storage devices, print server, presentation servers and all other devices that support wireless. The access points (APs) and hosts support dual-band feature inside WLANs.

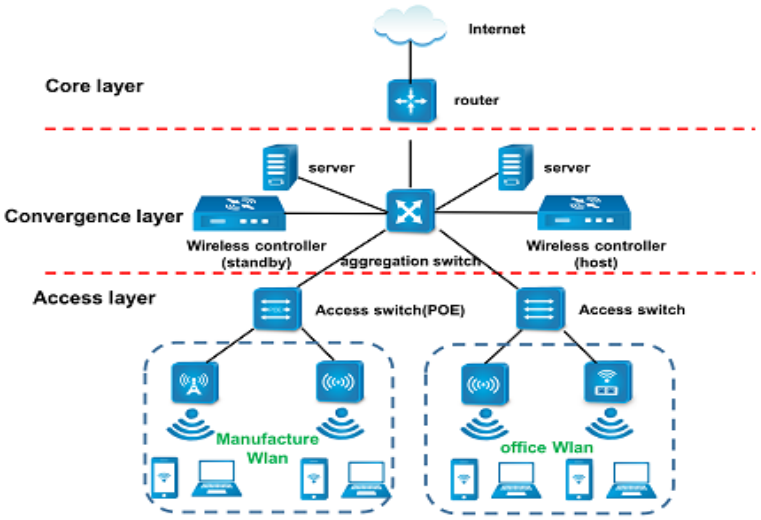


Figure 2.22: WLAN Topology

2.3.3 Wireless Metropolitan Area Network (WMAN)

WMAN is considered to be a wireless network that is created to operate on wide range of spaces. The characteristics of WMAN include the fact that the Speed of WMAN decrease as a result of the increment in the space it covers. WMAN is closer to the speed of broadband than the speed of Ethernet. WMAN operates like a backbone, peer to peer, and also as a point to multipoint. WMAN is also popularly known as WiMax. WMAN sometimes utilize unlicensed frequencies, but it is not recommended as a desirable solution, because it is possible that other users maybe using the same range of frequency and this would result in wireless interference. WiMax technology is considered to be very good since spaces are limited. To operate the WiMax we must pay to the service supporter to enable it, and the cost of establishment is so expensive.

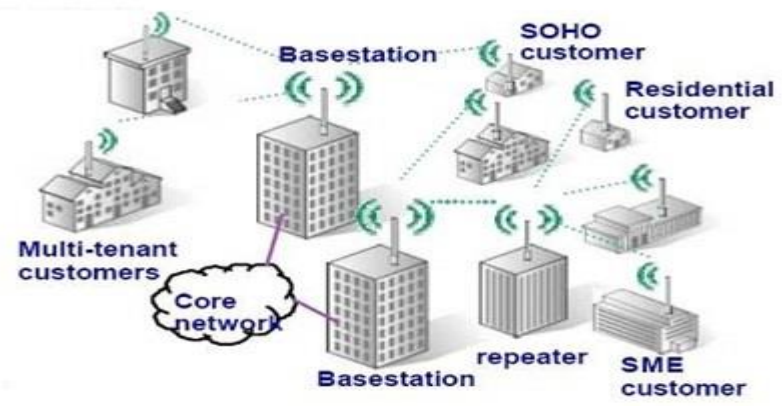


Figure 2.23: WMAN Topology

2.3.4 WLAN Topologies.

WLAN has two main topologies which are created by the 802.11 organization and they are Ad Hoc mode and Infrastructure mode.

1. Ad Hoc Mode

The ad hoc network happens when 2 PCs need to share data directly with each other. To create an ad hoc network there is no need of a network device to connect the two PCs together. Ad-hoc network is also called "IBSS" Independent Basic Service Set because the two PCs do not require any network device to connect with each other. Every PC has his own radio. As a result of the existence of just one radio for every PC so the capacity is weaker, and this indicates that the PC will be in the half-duplex transmission mode because the two PCs would be unable to get and give data simultaneously.

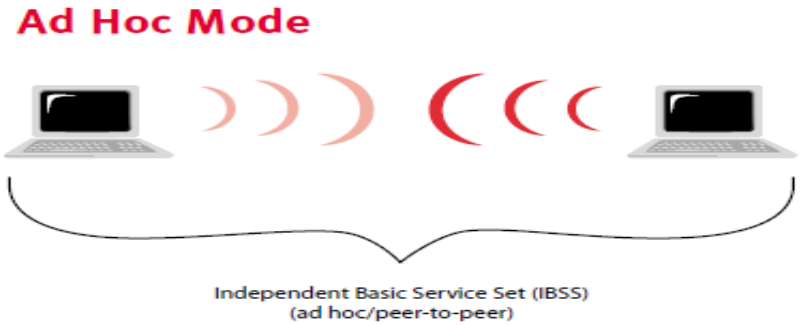


Figure 2.24: Ad-Hoc Mode

2. Infrastructure Mode

The infrastructure mode is seen when wireless PCs and other wireless devices communicate with each other via the access point (AP). In this case, the established communication starts from wireless radio spectrum and they are linked to the wired local area network. The function of AP, in this mode, is to convert the wireless packets 802.11 to Ethernet LAN packet 802.3. The packets of data move from the wired network to the wireless network by getting converted, through the use of AP, to radio signal then move out to the air. There are two type of infrastructure mode, the first one is known as the regular infrastructure mode and it happens with only one access point (AP) known as "BSS" Basic Service Set. The second one happens when there are at least two access points which are connected and linked to the LAN to create a single sub network known as "ESS" Extended Service Set. Also, the specification of 802.11 includes roaming abilities which permit the host PC to move between multiple APs across various frequency channels, where the movement of host PCs with low radio signals leads them to link themselves to another APs with better radio signals. When multiple APs are established to include the exact range and utilizing various non-interfering frequencies the capacity of host network device will be balanced very well. The Wireless NIC can choose to reconnect itself with another AP inside the area because the load on its present AP is too big for perfect execution (USR, 2015).

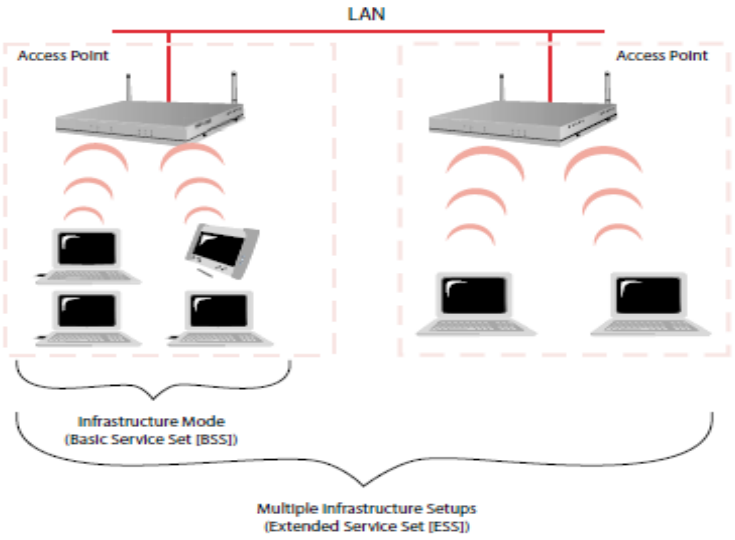


Figure 2.25: Infrastructure Modes

2.4 The Principle of Routing

When a network is established so as to link WANs and LANs to a router, the logical network addresses should be considered, like "IP" Internet Protocol addresses, when connected to any hosts inside the network in order to share data via that network. The expression of routing is used when transmitting a packet from one network device across the internet-work to the correct network device which exists in another network. Generally, the routers do not take into consideration the clients inside the network, routers take into consideration just the network in addition to the optimal path of the networks. The IP addresses of the intended client is utilized to take the packets into network across network managed by a router, hence, the MAC address of the client is utilized to reach packets from the router into the right client.

2.4.1 Routing Information Protocol (RIP)

The RIP protocol is considered to be the routing protocol over a distance vector. Routing Information Protocol transmits full routing list outside to the whole activated ports periodically for thirty seconds. To choose the perfect path to other networks RIP utilizes a technique called a ‘hop count’ which can be defined as routers number. RIP is classified into two and they are RIPv1 and RIPv2. RIP version (1) is considered as a classful routing protocol and this means that the subnet mask of the network address is not involved in the routing list. This classful routing protocol will lead us to issues related to discontinuous subnets.

Table 2.2: RIP version (1) vs. RIP version (2)

RIPv1	RIPv2
Distance vector	Distance vector
Maximum hop count of 15	Maximum hop count of 15
Classful	Classless
Broadcast based	Uses multicast 224.0.0.9
No support for VLSM	Supports VLSM networks
No authentication	Allows for MD5 authentication
No support for discontiguous networks	Supports discontiguous networks

RIP version (2) is considered as a classless routing protocol which means that the subnet mask of the network address is involved in the routing list, that is why the RIP version (2) is more flexible and has advanced routing networks (CCNA Tutorial 9tut, 2011).

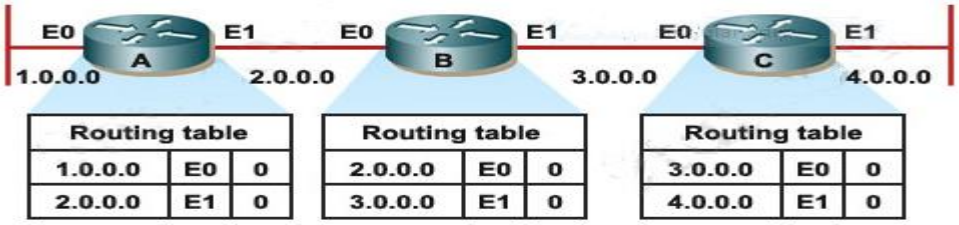


Figure 2.26: RIP Topology

2.4.2 Open Shortest Path First Protocol (OSPF)

The OSPF protocol is known to be the extremely utilized routing protocol of interior gateway protocol in the network environment as a result of this it is considered as a public routing protocol whereas EIGRP is the best competitor for OSPF. The OSPF is classified as a routing protocol of complicated connection state protocol. The routing protocol of connection state create updates related to the routing just at the time of amendment happens inside the topology of the network. When a connection is in amendment state, the network device that reveals the amendment generates a thing that is called "LSA" Link State Advertisement. This LSA connects and transmits to neighbor network devices utilizing a particular address of multicast. Every router copies the Link State Advertisement and generates updates related to what is known as "LSDB" Link State Database then redirect the Link State Advertisement into whole neighbor network devices.

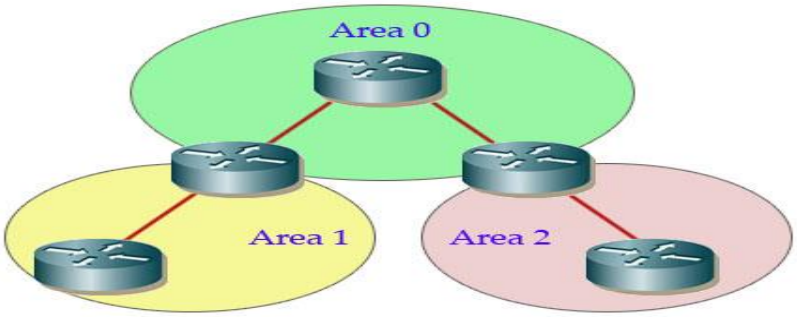


Figure 2.27: OSPF Topology

Open Shortest Path First links state protocol handle with 5 kinds of packets. "Hello Packets" are utilized to create and preserve the adjacency with other routers that operate the OSPF protocol. The packets are also utilized to vote and select the "DR" Designated Router & "BDR" Backup Designated Router on networks as Ethernet networks. Database Description “DBD” Packets includes a brief listing of transmitting router "LSDB" Link State Database and it is also utilized by getting routers to test the local "LSDB" Link State Database. “LSR” packet is another type of OSPF packets and it is utilized by getting routers to order extra data concerning any entree in-side "DBD". Link-State Update “LSU” packets are utilized to answer to link state advertisements "LSRs" likewise to advertise new data. "LSUs" have 7 various kinds of "LSAs" Link-State Advertisements. Link-State Acknowledgement “LSAck” packets are used for emphasizing the reception of the "LSU" letter (CCNA Tutorial 9tut, 2010).

2.4.3 Enhanced Interior Gateway Routing Protocol (EIGRP)

The EIGRP protocol is considered as a classless type of routing protocol. This EIGRP transmits the subnet mask of the network to the same router ports inside the routing table, EIGRP utilizes a complicated metric by calculating both delay and bandwidth. The EIGRP can be represented by mixed or hybrid routing protocol because EIGRP has the features of two type of routing protocols. These two types of routing protocols are Link State Routing Protocol and Distance Vector Routing Protocol, however, giant organizations like "Cisco" indicates the EIGRP like an advanced distance vector protocol. It is important to note that EIGRP calculates the metric based on all of band-width, delay, reliability and load and that both bandwidth and delay are already activated on the EIGRP router as default. Every routing protocol must have communication packets to talk with the neighbors, the EIGRP have 5 kinds of packets to discover and talk with the EIGRP neighbors. “Hello packets” is utilized to discover the EIGRP neighbors, and the packets are transmitted like multicast, periodically. “Update packets” are utilized to declare the paths, where the packets are transmitted like multicast if several things are changed.

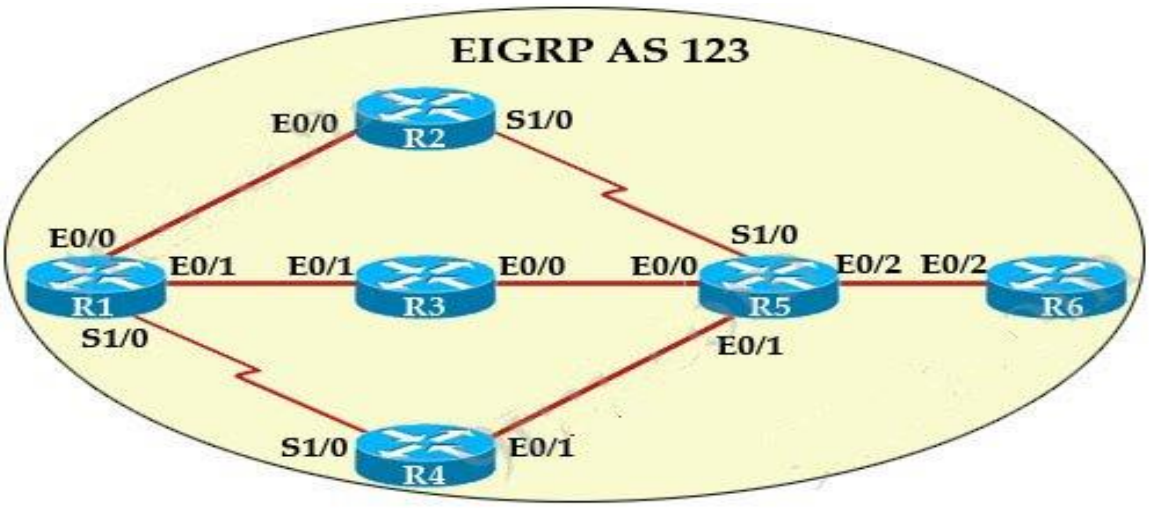


Figure 2.28: EIGRP Topology

The “Ack packets” reveals the reception of updates. The truth is that Ack packets could be considered as hello packets but without data. Ack packets are unicast permanently and it utilizes "UDP" in its operation. The “Query packets” is used to look up alternative routes if all routes that lead to the destination have failed. “Reply packets” is transmitted based on query packets to guide the founder not to recalculate the path due to the existence of appropriate successors. The reply packets is considered as a unicast to the query founder.

2.4.4 Border Gateway Protocol (BGP)

BGP is a very important routing protocol in our network environment and this section will describe why it is significant. Understanding the main mechanism of BGP or at least the basic things are required. The first thing is to differentiate between the two types of “BGP”. They are Interior Gateway Protocol “IGP” and Exterior Gateway Protocol “EGP”.

1. Interior Gateway Protocol "IGP" is a routing protocol that is working inside the famous system known as "AS" autonomous system. IGP is similar to both "EIGRP" & "OSPF". Commonly, IGP routers are operated beneath the same network domain, for example, individuals, association, and company.
2. Exterior Gateway Protocol "EGP" is a routing protocol that is working in the midst of two various "AS". The down topology will show that routers 1, 2 & 3 have to operate with "IGP" to talk to each other. The reason they are placed at the "AS 1" is to link them with other

routers that are placed in a different "AS". In this case, both routers 1 and 3 must operate with EGP.

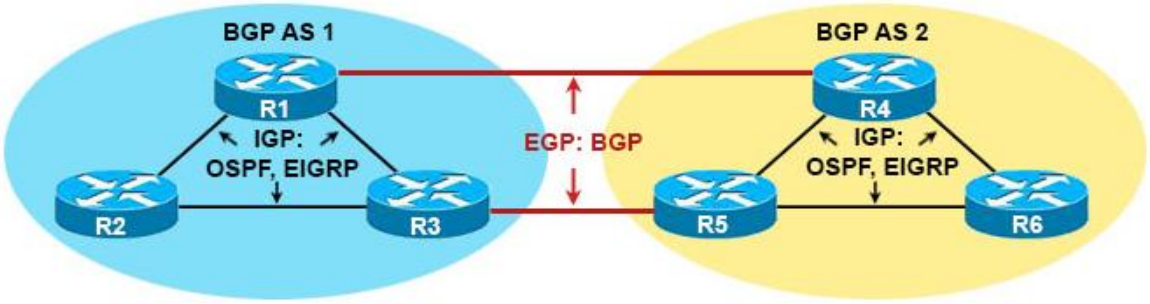


Figure 2.29: BGP = (IGP&EGP) Topology

We may be wondering why “EIGRP" or "OSPF" is not utilized instead of BGP. It is because, in this thesis, the basic goals of using the BGP was to provide “Path control”. In addition to that BGP provides three essential awesome features: scalability, reliability, and load balancing. While both OSPF & EIGRP are focusing on the best and the optimal route to the destination, this thesis considered the operating with internet service provider “ISP" level. Thus, the best route or path is not concerned to the destination, even though, the route is not considered as the best path to our destination. For example, this scenario will clarify the purpose of using BGP in this thesis based on the next figure. Assuming that our source is "AS1" and our destination is "AS3". What is the selected path that has to be selected? Assuming that the protocol which was selected to use is IGP (similar to OSPF) to choose our path to the destination, then the configurations are already programmed like bandwidth and other parameters of the interfaces. OSPF was selected to go from "AS1" to "AS2" then "AS3". After 3 months for some reasons, a new update happened, the modifications of the path and editing of the bandwidth are required. In this case, configurations of the bandwidth and other parameters must be changed at each router placed on the edge of the AS. But in BGP case defining the desired path to the destination will be done easily. Where the access from "AS1" into "AS3" will be via "AS2" to "AS4" then "AS5". In addition to that, the manipulation of the rate of data via every link can be done easily.

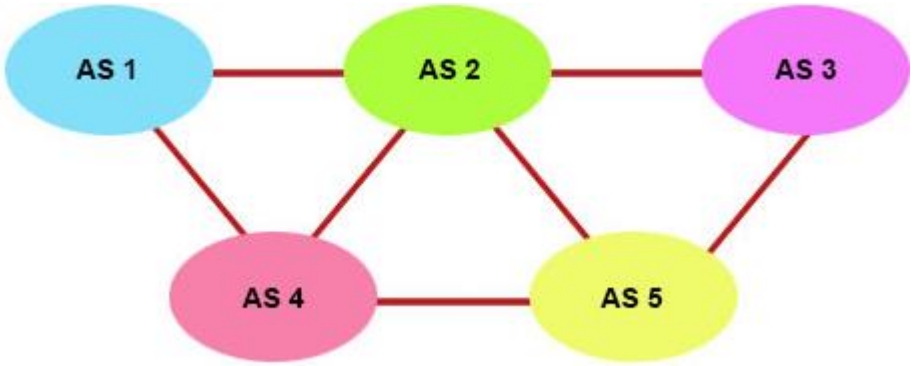


Figure 2.30: Scalability, Flexibility and Path Control of BGP

The truth is that the BGP is considered as a path vector protocol and the meaning of the path vector is based on the autonomous system number that has to transfer through. A great way to utilize the BGP is by using it with large numbers of paths or routes where OSPF or EIGR are helpless to treat this very big number of routes. In this thesis, we utilized two routers of "HQ" connected to multiple ISPs to provide a high level of redundancy and load balancing. In sharing the routing data traffic between the routers of the company and those of the ISPs routers in this design and during the implementation of the data networking platform, BGP is utilized to provide magnificent functions and features especially to optimize the load balancing and the reliability. All these previous features shows that BGP provides a high level of scalability, reliability, flexibility, path control and load balancing.

Figure 2.31: Load Balancing and Reliability of BGP

2.4.5 Hot Standby Router Protocol (HSRP)

All organizations, these days, must have a connection to the ISP for specific purposes. Figure 2.32 is an obvious example of a simple networking system that can be used in a small organization. To establish this kind of network system, the two interfaces of the router must be configured by IP addresses. The LAN interface of the router is represented by fa0/0 which has an IP address of 192.168.1.1 and linked to the switch. Then the IP addresses, Domain Name

System “DNS” and default gateway must be assigned to the network users. All the configurations for the network users can be done manually or automatically by Dynamic Host Configuration Protocol *“DHCP”*. After a while, the organization may decide to create a redundant connection to the ISP, and the network clients have a connection to the ISP, even if the main router fails, automatically and no manual configuration must be added.

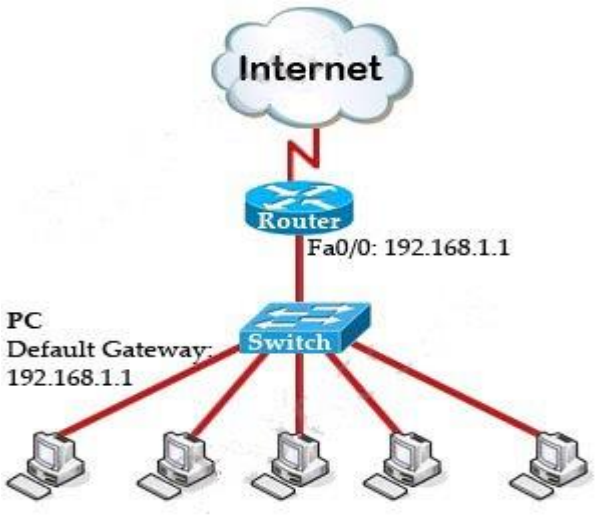


Figure 2.32: A General Example of Simple Networking System

In this case, an additional router is required to establish this method of connection as shown in Figure 2.33. But there are a lot of issues that would be faced after implementing this type of scenario. The network user will not be able to accommodate two default gateways at the same time. When the router (1) is in failure status and the hosts want the connection to the ISP through a router (2), the default gateway has to be modified and assigned manually to IP address 192.168.1.2. Also, if after a while, the main router (1) becomes active, then the default gateway must be modified to the IP address of the router (1). At this time none of the network users have a connection to the ISP. All these issues can be avoided by utilizing Hot Standby Router Protocol "HSRP".

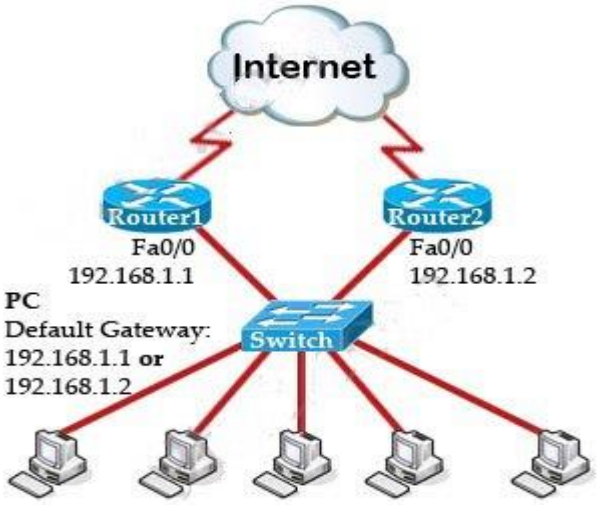


Figure 2.33: A Simple Networking System with Redundant Router

When the HSRP is implemented inside both router (1) and router (2), it will represent the two routers as one virtual router. This virtual router has one virtual MAC address and one virtual IP address to represent the router (1) and router (2) like one default gateway for network users. The virtual IP is supposed to be 192.168.1.254, where the MAC address is represented with "0000.0C07.AC0A". Now each network will take into consideration the new virtual default gateway to have access to the networking system via these virtual addresses. Figure 2.34 shows the situation of the network system after deploying the HSRP on both router (1) and router (2).

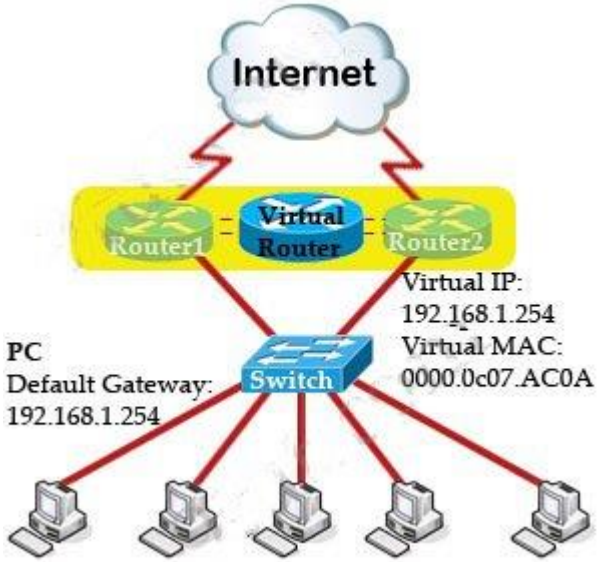


Figure 2.34: Implementation of HSRP inside Routers

Based on an Election Operation, one of the routers would be selected to be the "Active Router" while the second router would become the "Standby Router". At that instance, the two HSRP routers are in listening status but only the router selected as "Active Router" is transmitting and forwarding the packets traffic to the whole networking system while the other standby router would stay as a backup router. In case, the active router failed through periodic checking of the hello packets transmitted by the active router to identify the failure of the active router. Figure 2.35 describes the operations of when the active router is not in failure mode, while the standby router acts as a backup router.

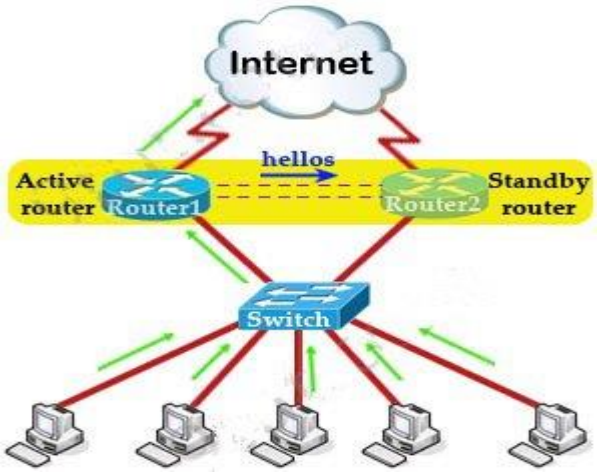


Figure 2.35: Communication between HSRP Routers

If the active router gets to failure mode, the backup router undertakes the functions of transmitting and forwarding the packets traffic. Because the group of HSRP routers is sharing the same virtual IP address and virtual MAC address, the network users will not lose the connection to the whole networking system and a new active router is elected from the group of the HSRP routers. The group of HSRP routers communicates with each other via hello packets. The hello packet timer inside the HSRP is considered to be 3 seconds while the dead timer is considered by default to be 10 seconds. This means that at every 3 seconds the group of HSRP routes communicates with each other via hello packets. Therefore, if the group of standby routers does not receive a hello packet from the active router for 10 seconds, one of the standby routers is elected as a new active router as shown in Figure 2.36.

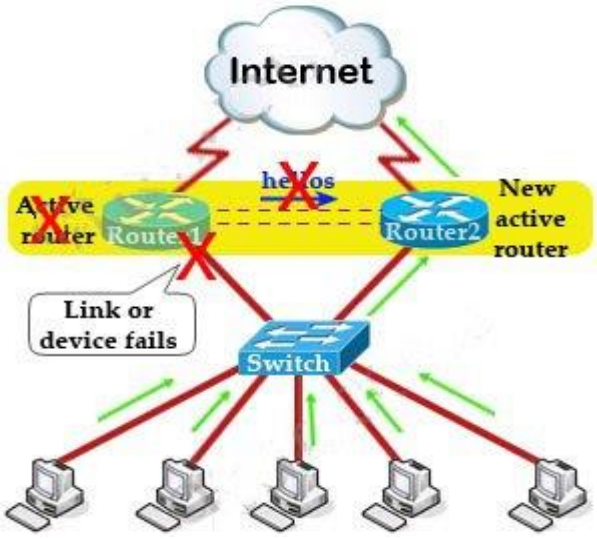


Figure 2.36: An Election Operation of a New Active Router

2.5 IPsec VPN Tunnel

This part will clarify how the IPsec VPN tunnel is integrated into the security system and how it can support other protocols. This VPN tunnel would provide the security, scalability, and reliability. In this thesis, the whole networking system platform has an HQ networking system and a branch networking system ,the VPN utilized Site to Site IPsec VPN tunnel. The function of VPN tunnel is to establish optimized security between sites, hence, the reliability and scalability are related to the establishment of security. The details given next show how the IPsec VPN tunnel provided these awesome features in the network environment of this thesis. IPsec protocol is a security protocol utilized to establish powerful and secure connections called VPNs. IPsec secures the site to site VPNs virtually, where it is implemented by IPsec (Santos and Stuppi, 2015). The function of IPsec Protocol is to secure and protect the transmitted packets between the source and destination and this is established by an IPsec framework, this framework has three major functions and they are as follows (Cisco, 2016):

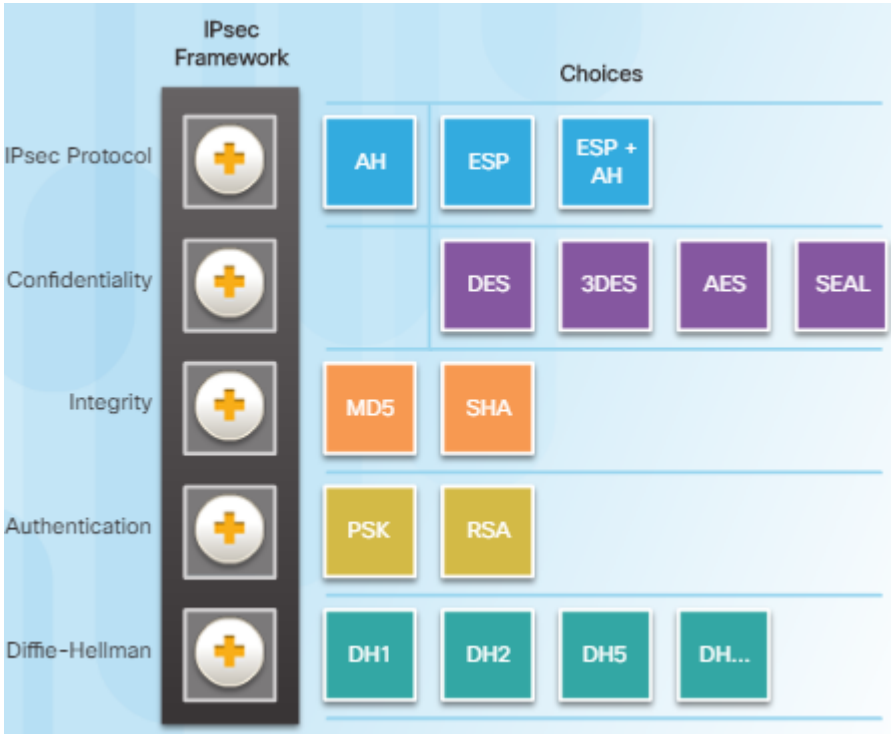


Figure 2.37: The IPsec Technologies & the Structure of its Framework

IPsec protocol provides a high level of scalability as shown Figure 2.37. above. The IPsec is not restricted to any specific principles or technologies that are related to the secure connection. This scalability and flexibility of the framework will allow an IPsec to easily integrate new security technologies in the future without updating the existing IPsec standards. This awesome feature leads the IPsec to be considered as high scalability. The framework of IPsec has three essential functions to work as follows.

1- Confidentiality is shown inside the framework of IPsec. The framework accomplished the confidentiality when the transmitted data is encrypted as described in next Figure 2.38. The length of the key that is utilized in the algorithm encryption decide the security level. The shortest key length, the easiest to be broken. To break the key with length 64 bits. It needs almost one year via a very high level of PC, hence to break a key with 128 bits. It needs nearly 10^{19} year to break it. The encryption algorithms are all symmetric key cryptosystems.

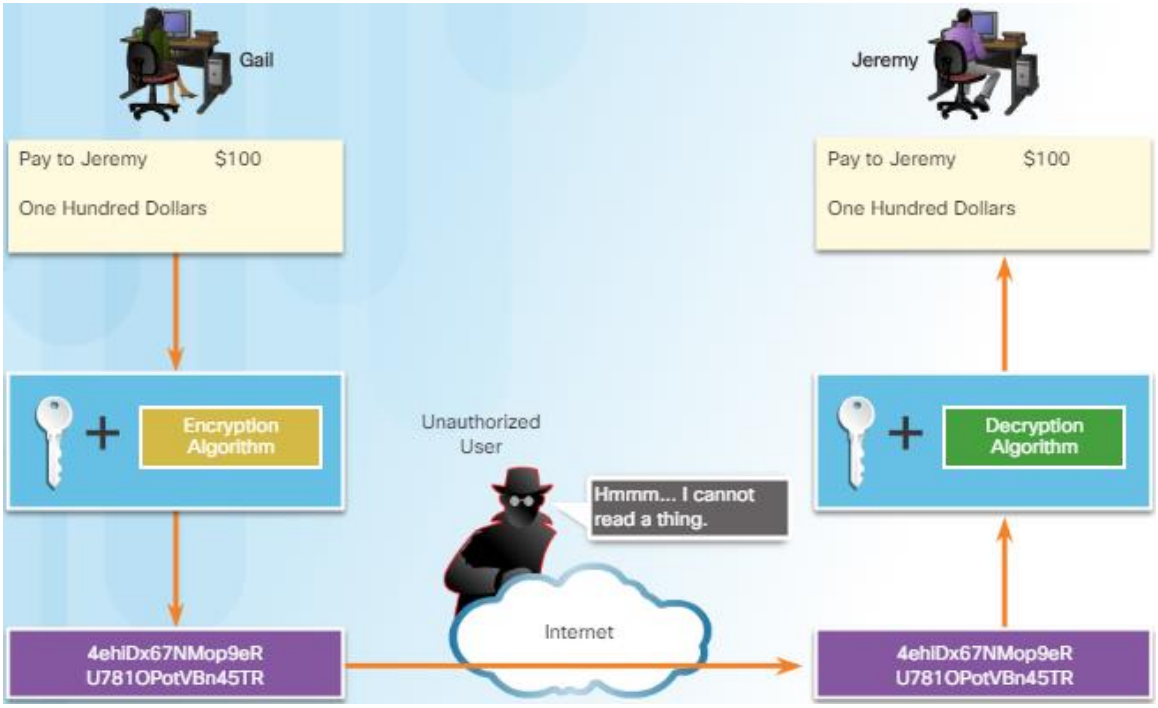


Figure 2.38: Confidentiality with Encryption

2- Integrity is accomplished to guarantee the transmitted data exactly matching the received data. Probably, the sent data are exposed and edited as described in Figure 2.39. Because the VPNs connection occurs via the public internet this is the reason for using the integrity technique of the VPN connection. The algorithm of integrity is known as "HMAC" Hashed Message Authentication Code. And the two most famous hashing algorithms are MD5 and SHA. MD5 is not recommended anymore because it is already broken by the attacker , the recommended algorithm now is a Secure Hash Algorithm "SHA".

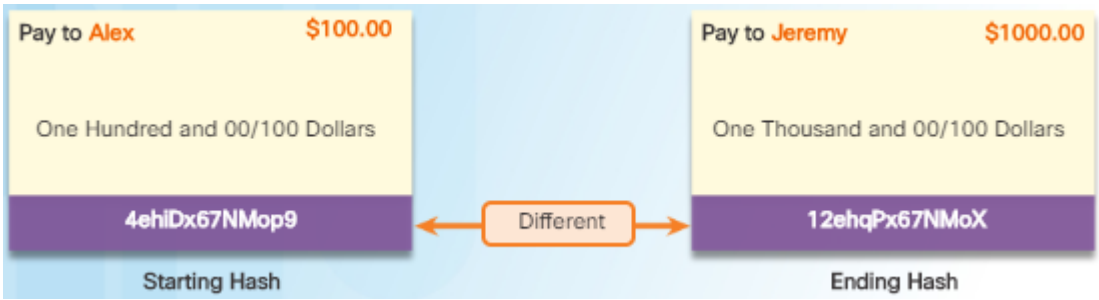


Figure 2.39: Intercepted and Modified the Received Data

3- Authentication is very important when we are transmitting data from the source host to the destination host. It is very important to authenticate the ID of the destination host before establishing any transmission. That is why we use this technology to authenticate the destination of communication before transmitting anything to it. There are two types of authentication, Pre-Shared Secret Key Algorithm “PSK” and Rivest Shamir Adleman Algorithm “RSA”.

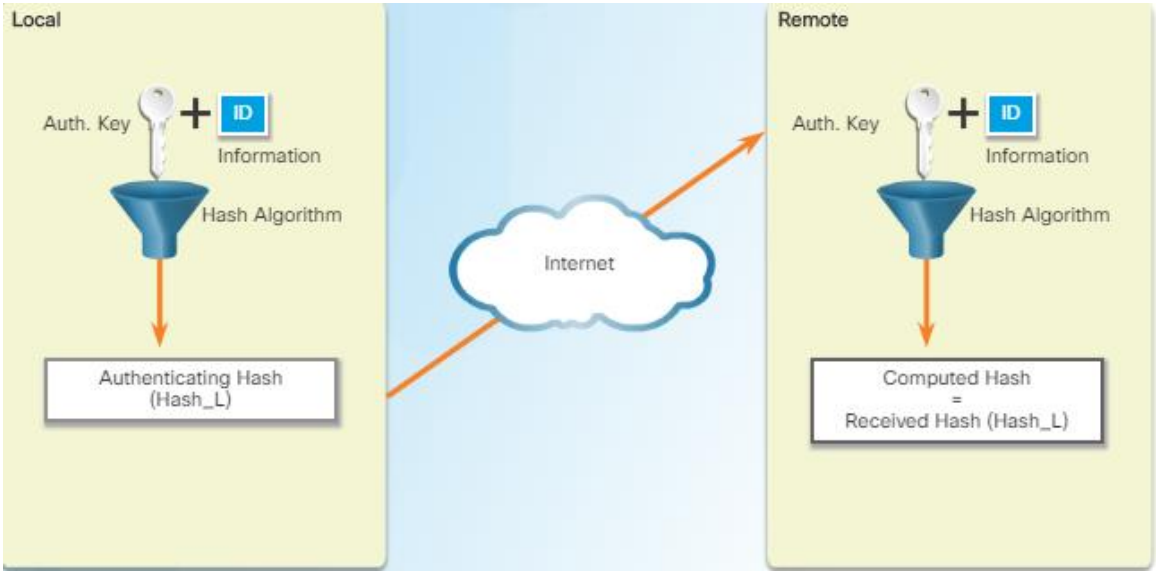


Figure 2.40: PSK Algorithm

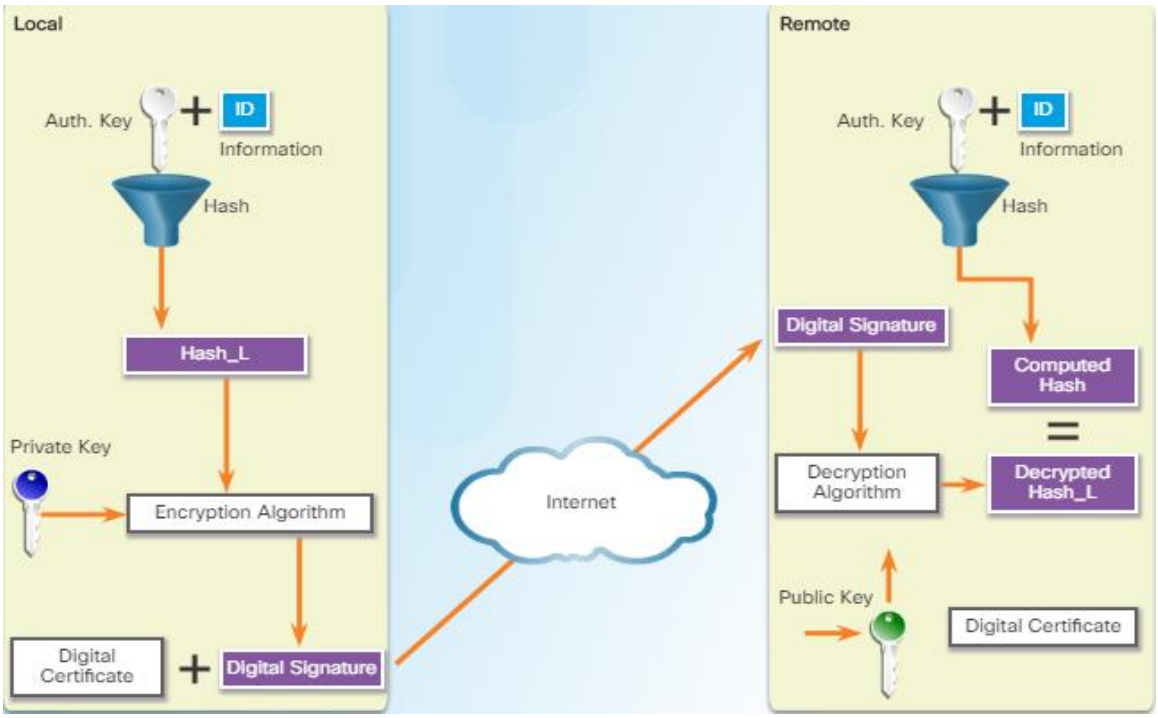


Figure 2.41: RSA Algorithm

This part will clarify the operation of IPsec VPN via organized structure. When the framework of IPsec is already created and done, there is Internet Key Exchange "IKE" which is utilized to provide the negotiation of Security Associations "SAs" as shown in Figure 2.42.

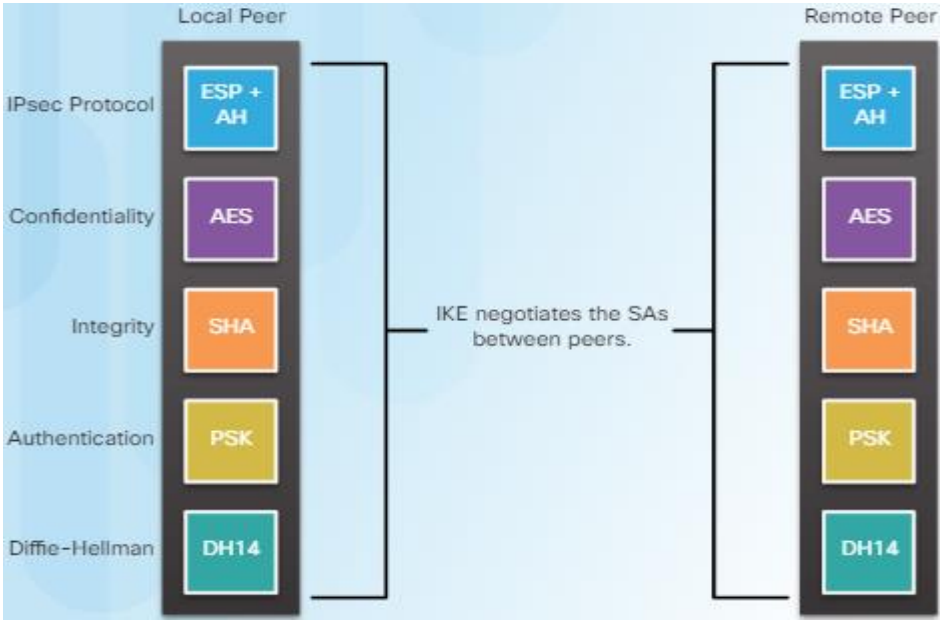


Figure 2.42: Internet Key Exchange "IKE"

This negotiation will happen in the middle of both local and remote peer. IKE does more functions, it activates and operates the IPsec communication, and makes an enhancement for IPsec. It also makes the configuration easier to do and a lot of useful features and functions that are related to this key also support its effectiveness. The IKE has two different phases, phase 1 and phase 2 and each phase has its own functions as shown in Figure 2.43.

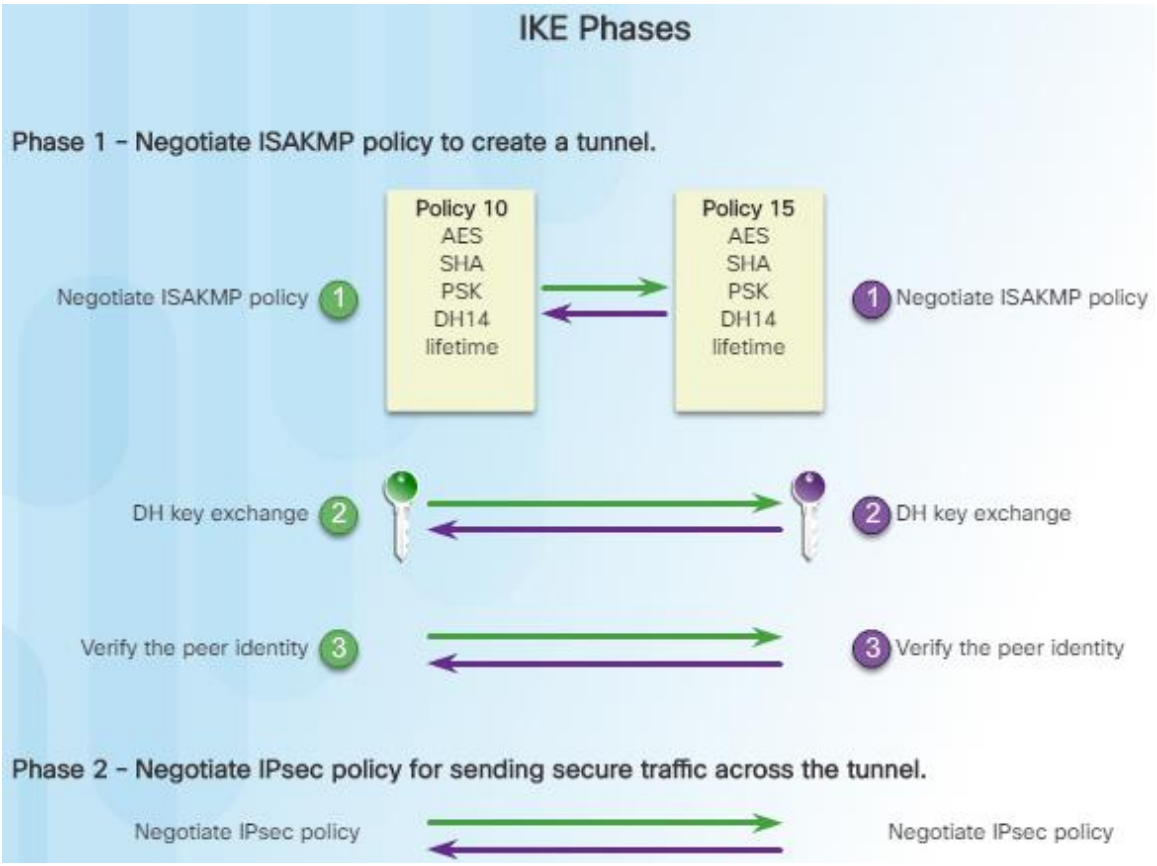


Figure 2.43: IKE Phases

In the IKE operation stage, the "ISAKMP" is utilized in both phase (1) and phase (2). In phase (1), the IPsec of both local and remote peers is executing basic SAs negotiation. The main goal of Phase 1 is to make sure one hundred percent that the policy of ISAKMP is negotiated. In addition to providing the authentication for both local and remote peers, it establishes a powerful secure communication tunnel. In phase 2, the secure communication tunnel subscribes and supports the negotiation of IPsec as shown in the following flowchart.

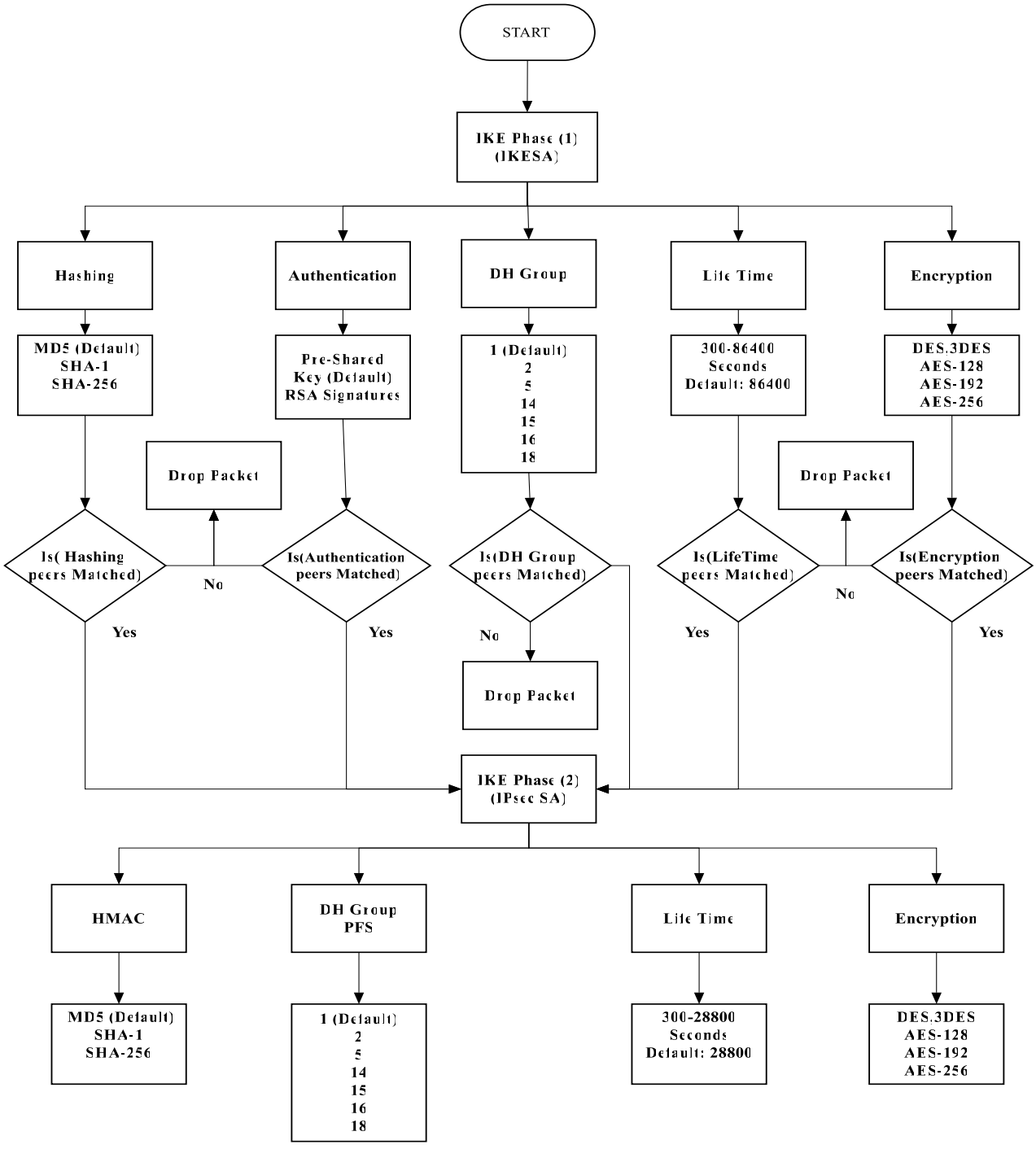


Figure 2.44: Flowchart of IPsec VPN Algorithms & Technologies

CHAPTER 3
SYSTEM MODEL

3.1 General Overview of a Multi-Tier Data Networking Platform

In this thesis, a networking data platform system was designed, configured and implemented to provide the reliability, scalability and load balancing. This system was completely integrated, flexible and compatible with the development of the technology that is associated with it. Figure 3.1 describes an overview of data networking platforms that have major network systems. These systems consist of headquarter "HQ" networking system, branch networking system, remote home office system and multiple internet service providers "ISPs". Both headquarter system and branch system were connected to each other via multiple ISPs. The remote home office system has a connection to both of headquarter network and branch network remotely via Digital Subscriber Line "DSL" connection. All these sites were integrated, secured, optimized and flexible. The networking systems were supported with routing, switching, voice, wireless and security protocols. All connections to the ISPs were done via fiber optic technology.

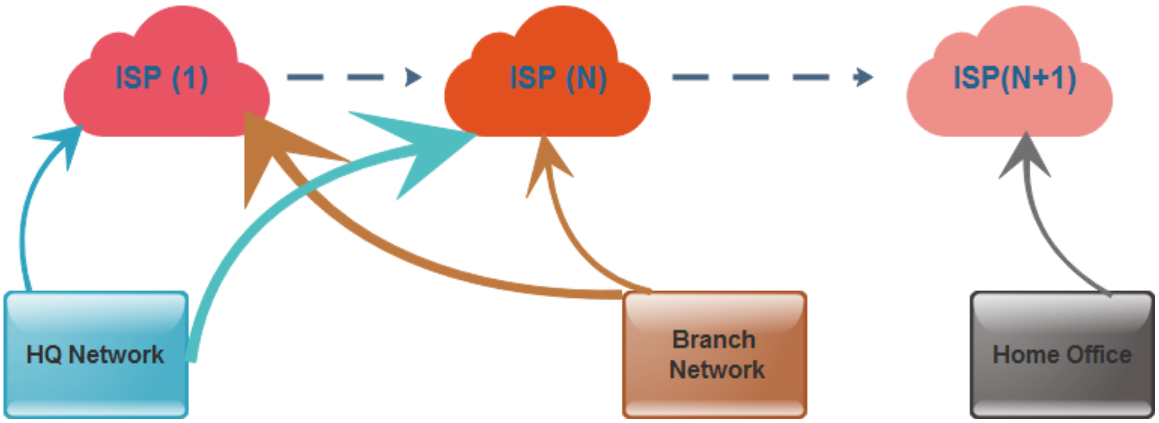


Figure 3.1: An Overview of Data Networking Platform

Figure 3.2 represents the networking structure of HQ and branch systems. These networking systems consist of an edge router, network firewall, intranet router, core switches, distribution switches, servers, and end-user's equipment. As shown in Figure 3.2 all networking devices

were sorted sequentially because each network device has specific features, functions, and protocols. The first network device as shown in Figure 3.2 is known as edge router. This router is a featured router existing at the edge or border of the network.

It provides the connection with ISPs, external networks, and autonomous systems "ASs". The edge router uses "BGP" Border Gateway Protocol, which it utilized extensively via ISP to create the connection with other networks. Edge routers are sometimes combined with firewalls, “NATs” Network Access Translation, and Virtual Private Network “VPN”. Edge router can also be called core router or access router.

The second device is represented by the network firewall device to protect the whole networking system. The software on the firewall provides the visibility into all traffic that is natively integrated in such a way that no gaps exist and the context is delivered. Thus, it reacts to the threats that are critically important to remove the attack. The network firewall has significant features to mitigate the attacks. It identifies and accesses all traffic, blocks known threats, sends the unknown threats to cloud and it is extensible to mobile and virtual networks. The firewall is designed to safely enable applications and prevent modern threats and attacks. It identifies all the network traffic and provides the protection using “multi-method prevention” to stop the malware and threats.

The threat intelligence cloud is established by powerful firewall through multiple features. The first thing it does is the gathering of potential threats from network and endpoints. The second is analyzing and correlating the threats intelligence of the network. While the third feature is the dissemination of the threats intelligence to network and endpoints. The intranet router is considered as the third network device after the network firewall as shown in Figure 3.2. The main purpose of this network device is to operate all the routing functions on all internal data traffic. While the internal network consists of multiple “VLANs" Virtual Local Area Networks, each VLAN must have a unique default gateway.

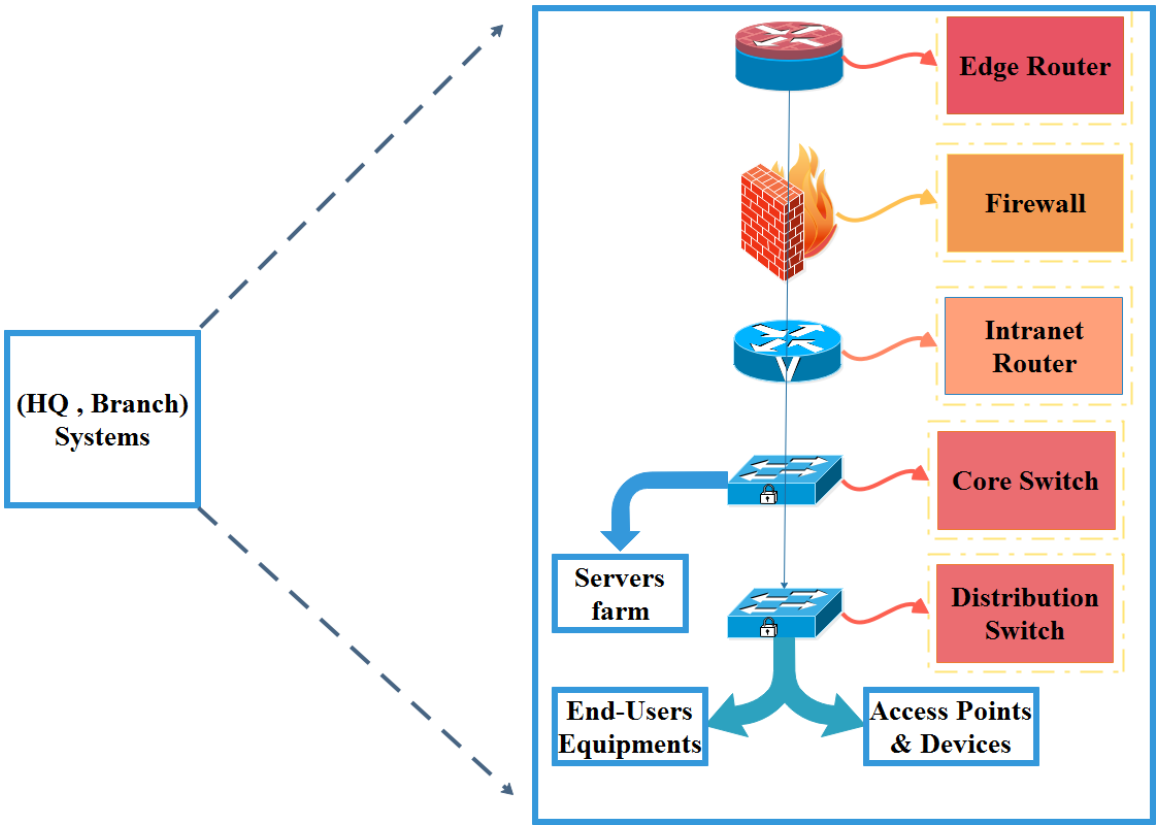


Figure 3.2: Networking Blocks of HQ and Branch Systems

As a result of existing multiple VLANs, the one physical interface is divided into multiple sub-interfaces or virtual interfaces to support the multiple VLANs. The Router on Stick technology is programmed inside the intranet router to create sub-interfaces of VLANs. Also, this router acts like "CUCM" Cisco Unified Communications Manager. A voice over IP "VoIP" technology feature applied inside the intranet router to establish a voice connectivity via call manager and IP phones. These network devices are programmed with each other to support the end-users. The Hot Standby Router Protocol "HSRP" is applied inside the intranet router to provide a fault-tolerant default gateway for all VLANs.

The Core Switch is a powerful networking device which has a high Central Processing Unit "CPU" performance with high capacity, it is also called a backbone switch. The main purpose of core switch is to create a reliable connectivity and establish a networking negotiation between the routers, servers and distribution switches. The servers linked directly to the core switches, and the function of the network servers is to provide all the services that are requested from the

hosts of the network. The Distribution Switch exists after the Core Switch as shown in Figure 3.2. The essential function of the Distribution Switches is to provide the connection between the core switches, access devices, access points and end-users equipment. All the VLANs are programmed inside both core switches and distribution switches to establish the negotiation of data traffic that are related to these VLANs. The Wireless Access Points "WAPs" are linked and configured by the controller with specific parameters to cover the whole networking system. Figure 3.3 gives an overview of a complete example of a networking system model. Where the notation "SW" indicates the switch, the notation "R" indicates the router and "WAP" indicates the wireless access point. The HQ networking system consists of four routers, two servers, firewall, Intrusion Prevention System "IPS", four switches, two wireless access points and end-users networking equipment. The four routers are distributed into two internal routers and two external routers, the two internal routers are denoted by R1 and R2. These R1 and R2 are configured and programmed to route, manage and control the data, voice and wireless traffic for servers, computers, IP phones and access points. R1 is in operational status as default and the R2 is in a standby situation to provide the redundancy and load balancing. The two external routers represented by R3 and R4 are considered as secure edge routers. R3 and R4 are placed at the edge of the network to provide the protection against threats. Also, they perform the functions of firewall and IPs, and connect the whole network with the outside. R3 is operational by default and R4 acts as a redundant router.

The four switches consist of 2 core switches and 2 distributed switches, the core switches are represented by SW1 and SW4. While the distributed switches are SW2 and SW3. The two servers virtualized into many servers as Hypertext Transfer Protocol "HTTP" server, Domain Name System "DNS" server, Domain Controller "DC" server and Email Exchange server. The main server is in operational status as default and the redundant server is in standby mode to provide the reliability. The Wireless Access Points "WAPs" are distributed to the coverage area of HQ to provide a wireless connection to the whole system.

The first Internet Service Provider "ISP1" contains Wide Area Network "WAN" cloud, ISP server and ISP router is R5. The remote access "home" network includes laptop, modem and wireless router that are connected to the internet to provide the remote access to both the HQ

and the branch. The ISP2 has WAN cloud, ISP server and ISP router represented by R6 and which is considered as the public default gateway for specific organizations.

The branch networking system is designed with four routers, three switches, one main server, firewall, IPS, one WAP and clients networking devices as shown in Figure 3.3. The four routers are represented by R7, R8, R9 and R10, both R7 and R8 are secure edge routes while routers R9 and R10 act like intranet routers. The routers R9 and R10 work to support each other, R9 is in operational status since R10 is in standby mode. Also, the routers R7 and R8 take the same approach, R7 is working as main intranet router while R8 is kept as a redundant router to support R7. The three switches are represented by SW5, SW6, and SW7 while SW5 is the core switch, SW6 and SW7 are distributed switches. Designing a networking system model must be done carefully by considering the advantages that come with it and they can be summarized as follow:

- It makes the network simpler, easier to troubleshoot and easy to investigate in case there is any networking issue.
- It makes the operation of scalability simpler when the network system is under extension.
- The regular maintenance of networking devices become more organized because all network devices are related to each other.
- It makes the controlling and management of networking devices as well as the addition of features and protocols more effective and eloquent.

All the aforementioned network devices are programmed to work harmoniously with each other. As a result of the fact that the network devices are related to each other despite the fact that they have different mechanism and specific purpose to deliver their services.

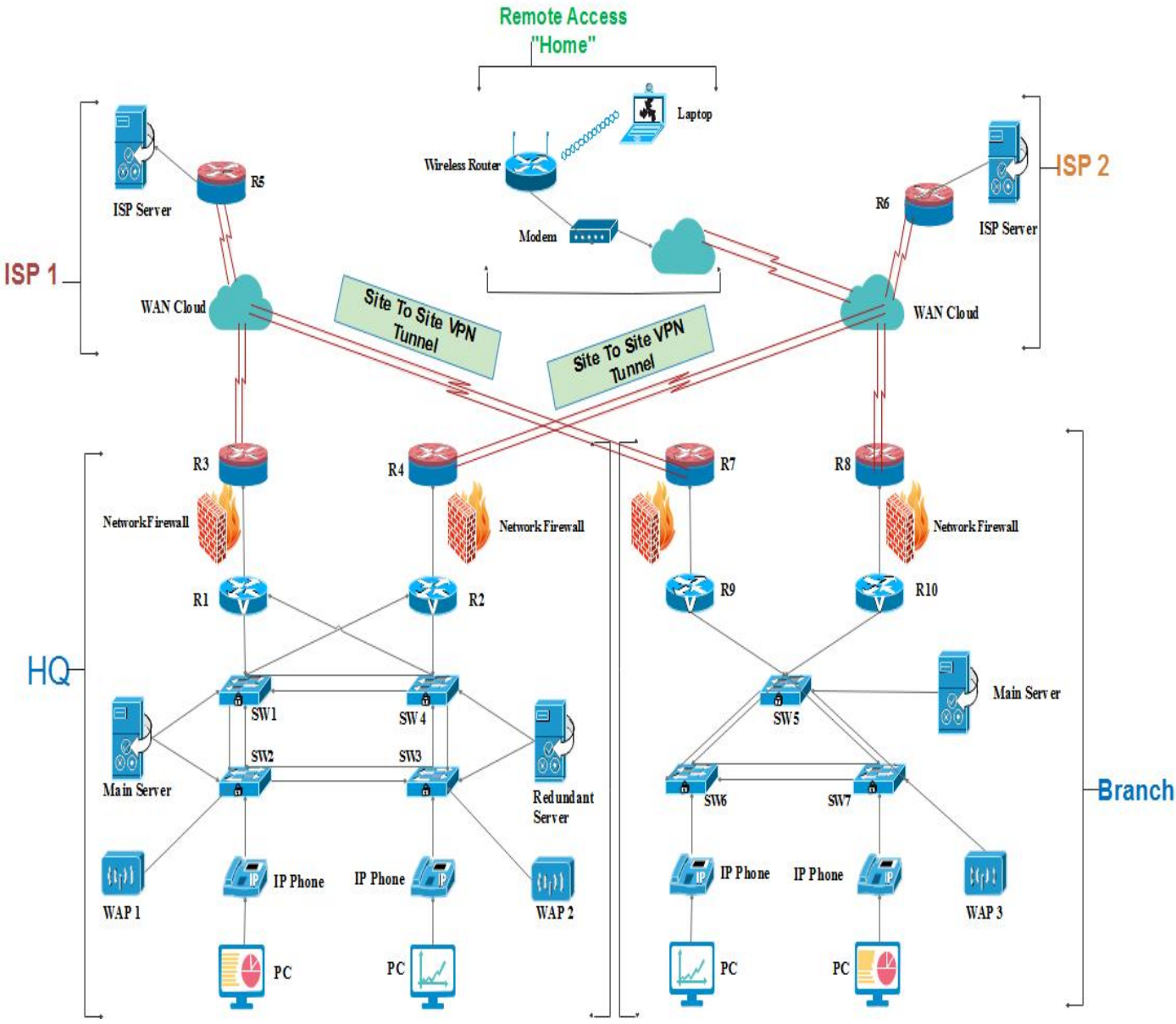


Figure 3.3: An Overview of a Complete Example Networking System Model

3.2 Protocols Configuration of a Multi-Tiers Data Networking Platform

In this section, the protocols configuration of the designed data networking platform is presented. An illustration of the protocols configuration is provided in Figure 3.4. With reference to the Figure 3.3 that shows an overview of the networking system model of this thesis. The HQ includes 4 switches connected to each other via a protocol known as "EtherChannel".

As a result of the existing four switches, a four Etherchannels are configured between them. One EtherChannel is programmed between two switches connected to each other. The purpose of using the EtherChannel protocol in this thesis is to provide redundant links and enhance the performance of the channel capacity of the networking device. In the previous section, more advanced details about EtherChannel are explained. The Virtual Local Area Network VLAN protocol is also configured into these four switches.

VLANs consist of logical LANs, it means the physical LAN is segmented into multiple logical LANs called VLANs. The target of utilizing the VLANs is to provide high performance of data traffic, simplify the administration, reduce the cost and provide the security. The VLAN Trunking Protocol "VTP" is a protocol created by Cisco organization. This protocol is applied inside the switches to share the VLANs information which exists inside the switches. This information is represented by "VLAN name" and "VLAN ID". The Spanning Tree Protocol "STP" is considered as a significant switching protocol. STP presents a fault tolerance per port or per link. The main purpose of using STP is to prevent the switching loop increasing when applying redundant channels between two physical ports.

Border Gateway Protocol "BGP" is one of the routing protocols and it is considered as a dynamic routing protocol. The main goal of using BGP is to manage and control the paths of packets traffic for a specific purpose. It routes and controls the packets between systems known as Autonomous Systems "ASs". BGP is a powerful routing protocol, especially when the networking platform systems work with ISPs levels to control the paths. Access Control List "ACL" is applied to most of the networking devices (switches, routers, and firewalls) for packet filtration. It is considered to be a deep customization to permit the network administrator to deny or permit specific packets from passing through desired ports or interfaces. ACL is termed a deep customization due to its flexibility to determine the source IP, destination IP, and the source or destination port ID and the ability to deny or permit the passing packets traffic.

The Secure Shell "SSH" protocol is utilized for securing remote access to the networking devices. The purpose of using SSH is to establish a strong encryption and authentication for the communication between the network engineer and the network device. Also, SSH prevents the man in the middle to capture the data traffic session that related to the logging in. Inside every

networking firewall, IPS or router the security Group Policy “GP” must exist. The GP is a combination of multiple secure protocols and rules that are integrated together to provide a powerful security. As mentioned in Figure 3.3 the HQ has 4 routers, two intranet routers and two external “edge” routers. In this thesis, the voice dial from site to site was configured via intranet routers that are working as Call Manager “CM” router. The CM router provides all the telephony services that are related to the VoIP to support the IP phones and make them operational with a special configuration.

Since the physical LAN is divided into multiple VLANs so that each VLAN requires a separate default gateway to support it. In this case, multiple default gateways were required per one interface where it is impossible physically but it is possible logically. In this thesis, the router on stick configuration was used to solve this issue but what will happen if this router got failed, and the network clients do not know the default gateway of the redundant router? The Hot Standby Router Protocol “HSRP” was used in the two intranet routers. The purpose of utilizing HSRP was to make the two intranet routers act like one virtual router with “one logic IP” and “one logic MAC”. Where all networking hosts would not care about the real IPs and MACs of routers. They would recognize only the "virtual IP" and "virtual MAC" of the HSRP.

Figure 3.4 contains multiple networking tiers where each tier has unique and integrated combinations of networking protocols. The edge routers tier combination has BGP, site to site VPN, SSH and “ACL”. BGP was selected as a result of having integration and flexibility with other protocols and routers. BGP can be transformed into two types, it can establish internal routing peering sessions when the connections with other routers inside the organization as Internal Border Gateway Protocol “iBGP”.

Where it can be as External “eBGP” when the connection is needed to external organizations or ISPs. These external routing sessions will not be reliable and secure without implementing a powerful secure protocol. Which is the role of virtual private networks "VPN" to make it integrated with BGP to ensure absolute protection and reliability of data traffic from a perspective, effective routing of data traffic from another perspective. Since internal networks are always vulnerable to expansion, BGP can be used to administrate the complicated networks by integration with iBGP. It can solve troubles such as scaling the internal network to correspond

the data traffic purposes while keeping networking efficiency. The Access Control List “ACL” contribute to manage and secure the whole networking system by filtering the data traffic per network device interfaces for many purposes such as permit or deny specific network users, subnets and zones to access some features or connections. ACL is useful to isolate some network devices from the whole network due to some updates or maintenance where it will be integrated with other switching and routing protocols.

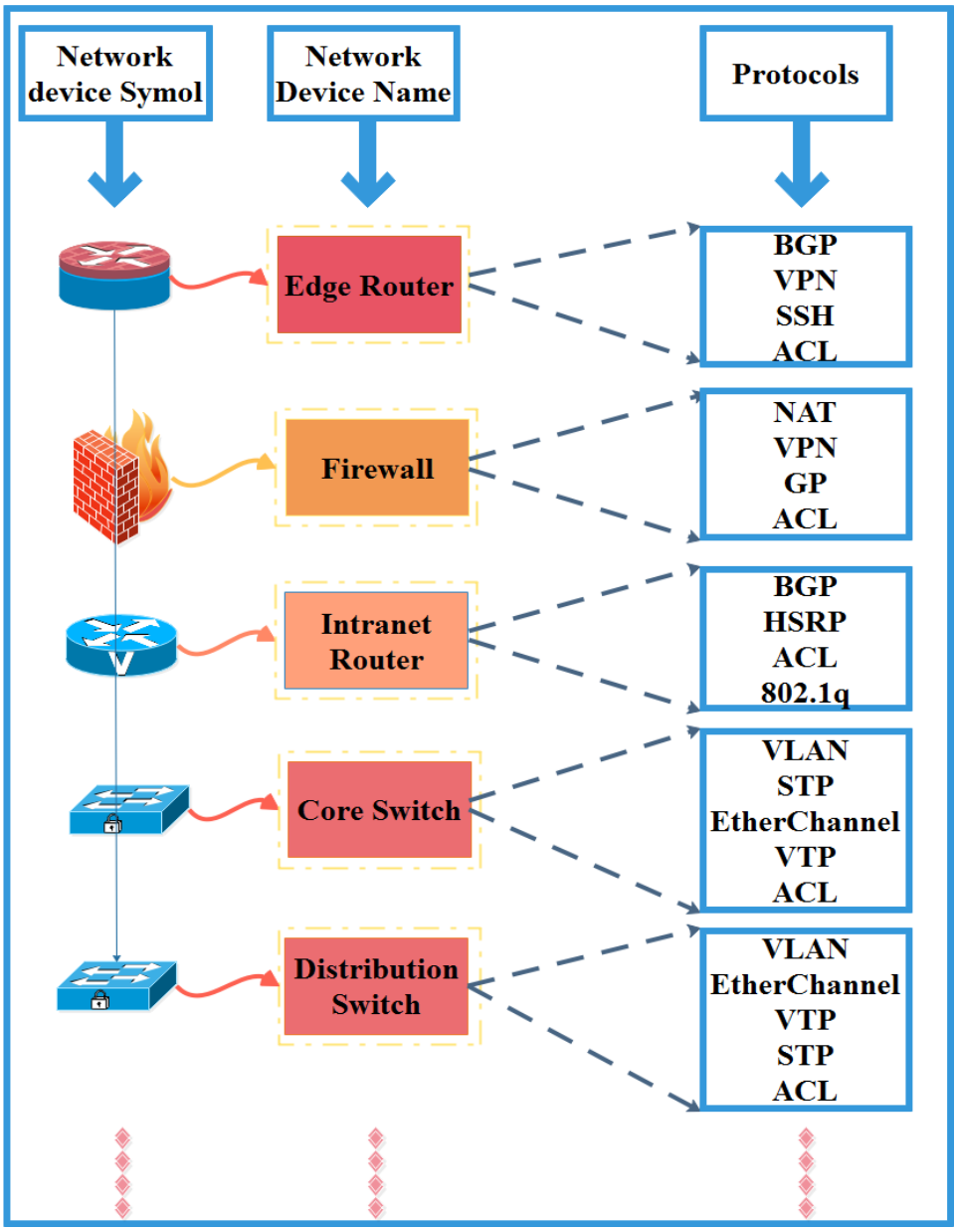


Figure 3.4: An Illustration of Protocols Configuration

Updating and maintaining the networking devices almost are done through encrypted communication tunnels between the administrator and network devices. These secure remote sessions are established by Secure Socket Shell protocol “SSH”. Where it contributes to complete the integration with BGP, VPN, and ACL. The network protocols of edge router tier are selected and configured to operate and support each other as a harmony cooperation.

The firewall tier has a significant combination of protocols such as Network Access Translation “NAT”, VPN, Group Policy “GP” and ACL. The behavior of firewall tier is specialized for deep security. The source packets traffic that is going to the destination “ISP” can’t be routed directly without network access translation. NAT performs two types of translations for IPs, forward translation and reverse translation. It translates the Private IPs of the whole network to public IPs to access the internet and apply reverse network translation for the public IPs. While the VPN supports the access to the external networks by performing the strongest secure technologies for packet traffic. The group policy plays the core roles inside the firewall tier, it includes multiple management and security protocols such as ACL, AAA, NAT, SSH, security zones levels and security object for the whole network. The purpose of combining all these secure protocols to operate in a harmonious system to adopt security and management integration at the level of firewall tier.

The intranet router tier has some difference in combination of protocols because the core responsibility of this tier to provide the intranet routing for all VLANs. The protocols combination of this tier consists of BGP, HSRP, ACL, SSH and 802.1q protocol. BGP inside the intranet router tier has a different behavior compared with edge router tier. It is working just as “iBGP” to establish peering routing sessions with edge router. 802.1q protocol contributes to create logical or sub-interfaces to support the VLANs which have been created in each switch. Each sub-interface related to unique VLAN to provide switching sessions between network devices, these switching sessions were privileged and managed by ACL. The remote access channels between network devices and administrator are encrypted by SSH. While the HSRP provide the reliability per layer 3 and virtualize the IP and MAC of each sub-interface of intranet router as fault tolerance.

The protocols combination of core and access switch tiers contents VLAN, STP, VTP, EtherChannel and ACL. VLAN protocol provides security, management, and customization for frames traffic through segmentation process the physical LAN to Virtual LAN. The switching sessions will not be established unless the connected interfaces between the switches or between switch and router configured as a trunk link. Then VTP assists the VLANs by organizing the frames traffic through tagging them with unique information as a kind of categorization. While the core function EtherChannel protocol is creating layer 2 reliability and redundancy at each trunk interface. In case the Etherchannel got down, the STP protocol will prevent the phenomenon of loop avoidance. And customization of management and access the VLANs to each other will be done though ACL.

The beauty and difference of these combinations from other protocols combinations are to make these protocols work regularly and cohesively in a harmonious system.

CHAPTER 4
DESIGN AND PERFORMANCE ANALYSIS OF A MULTI-TIER DATA NETWORKING PLATFORM

4.1 Design of a Network Tier

This section is about the design of a network tier. The most important issue that could be faced in the design of a network tier is the number of network devices inside the tier and how they would be located and linked because these devices would be utilized for redundancy, backup and load balancing. When a network tier (level) consists of just one network device such as a single switch, the tier would work properly but once this switch stops working suddenly all the tier would fail, therefore, the whole network system would be in a failure mode because the tier is linked as a series connection with another network tier, the use of this network tier is not recommended because it is an unreliable tier.

In another case where a network tier has multi-network devices (three devices), it is considered as a highly reliable network tier and provide a very good load balancing. The load balancing is provided by existing three network devices so that the data traffic is not transferred only via one device, the load is shared via these three devices. Once one of these three network devices is in a failure status, the other devices operate to transmit the data traffic normally to provide the reliability in this tier. This type of network tier has a high reliability and load balancing, but on the other hand, it has a high complexity and needs high budget to establish. When the number of network devices increase the reliability will increase, but the complexity and cost will also increase. Therefore the ideal number of networking devices at a tier should be studied very carefully. In this research, a network tier was designed and programmed due to existing two network devices per tier. This type of network tier provides the reliability of the whole network system and has a fair complexity and budget to establish it. During the designing stage of a network tier, it is very important to obtain the system failure probability.

Figure 4.1: A Network Tier with 1 Network Device.

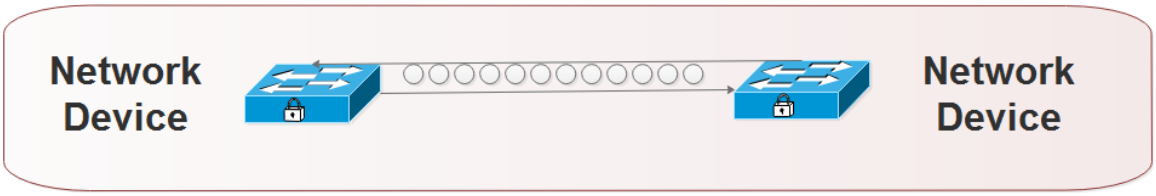


Figure 4.2: A Network Tier with 2 Network Devices.

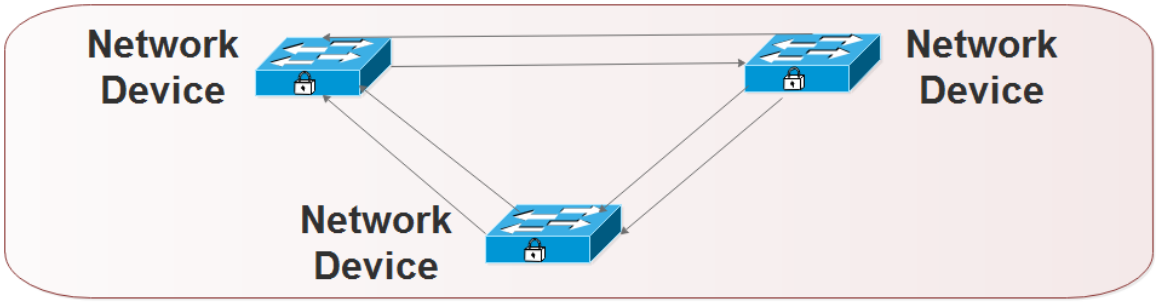


Figure 4.3: A network Tier with 3 Network Device

This subsection provides the mathematical analysis to obtain the system failure probability for a network tier to fail and to work successfully. In this research, the binomial probability was utilized to obtain the value of system failure probability for a tier network and it is represented by the following formula.

$$b(x, n, P) = {}^{n}C_{x} \times P^{x} \times (1 - P)^{n-x} \quad (4.1)$$

$$Q = b(x, n, P) \quad (4.2)$$

Where:

$${}^{n}C_{x} = \{ n! / [x! (n - x)!] \} \quad (4.3)$$

$$P = 1\text{-}Q \quad (4.4)$$

Before starting with an example that is related to this formula, the notation of the previous binomial formula is described as follows:

- x: Indicates the number of the successes that are related to the event.
- n: Indicates the number of trials that are used in the event.

- P: Represents the probability of success in a specific event or system.
- Q: Represents the probability of failure in a specific event or system.
- ${}^{n}C_{x}$: Indicates the number of combinations.

Table 4.1: One Tier System Status

Tier Status	System Status
F	F
W	W

Where the notation "F" indicates that the networking system is in failure status and the notation "W" indicates that the networking system is in successfully working status.

Assuming that the network system has just one tier. Thus, to obtain the value of probability of success for one tier and to obtain the value of whole system failure probability there are two steps.

- ❖ Step (1): The probability of failure for one level "tier" must be obtained by using the formula (4.1) which is: $b(x, n, P) = {}^{n}C_{x} \times P^{x} \times (1 - P)^{n-x}$.
- ❖ Step (2): The probability of success for one level "tier" must be obtained by using the formula (4.4): $Pn = 1 - b(x, n, P)$.

4.2 Design of Multi-Tier Networking Platform

Multi-Tier data networking means that the network consists of multiple levels (Tiers), where each tier has different roles and characteristics. For example, tier "1" is responsible for internet connectivity, link the HQ with the outside networking environments (outside networks), and protects the internal network by integrating secure devices and technologies such as utilizing a VPN tunnel to establish powerful secure communications with the outside side networks like a branch. Tier"1" make filtration to the data via access list and apply for inbound role and outbound role, and make group policies inside the Intrusion Prevention Systems "IPS" and firewall to establish a full control of data flow traffic. In addition to that, it establishes the intra-domain routing to route all the kind of data to the wanted destinations like servers, hosts. Tier "2" consists of core switches, these switches are considered as edge switches to provide the

connectivity between tier 1 and tier 3. Tier 3 is represented by 2 distribution and access switches, at the same time, it is utilized to connect the hosts or end-users of the network to the network devices (servers, routers) to have access to the desired features and resources as shown in Figure 4.4. The Figure 4.4 shows that the reliability and efficiency of the network do not depend only on a single tier but on the operation of all tiers together. Therefore, it is very important to consider and design each tier of the networking platform as well as the platform as a whole to get reasonable and useful reliability analysis. The contribution of this thesis was to design and provide performance analysis for a multi-tier data networking platform.

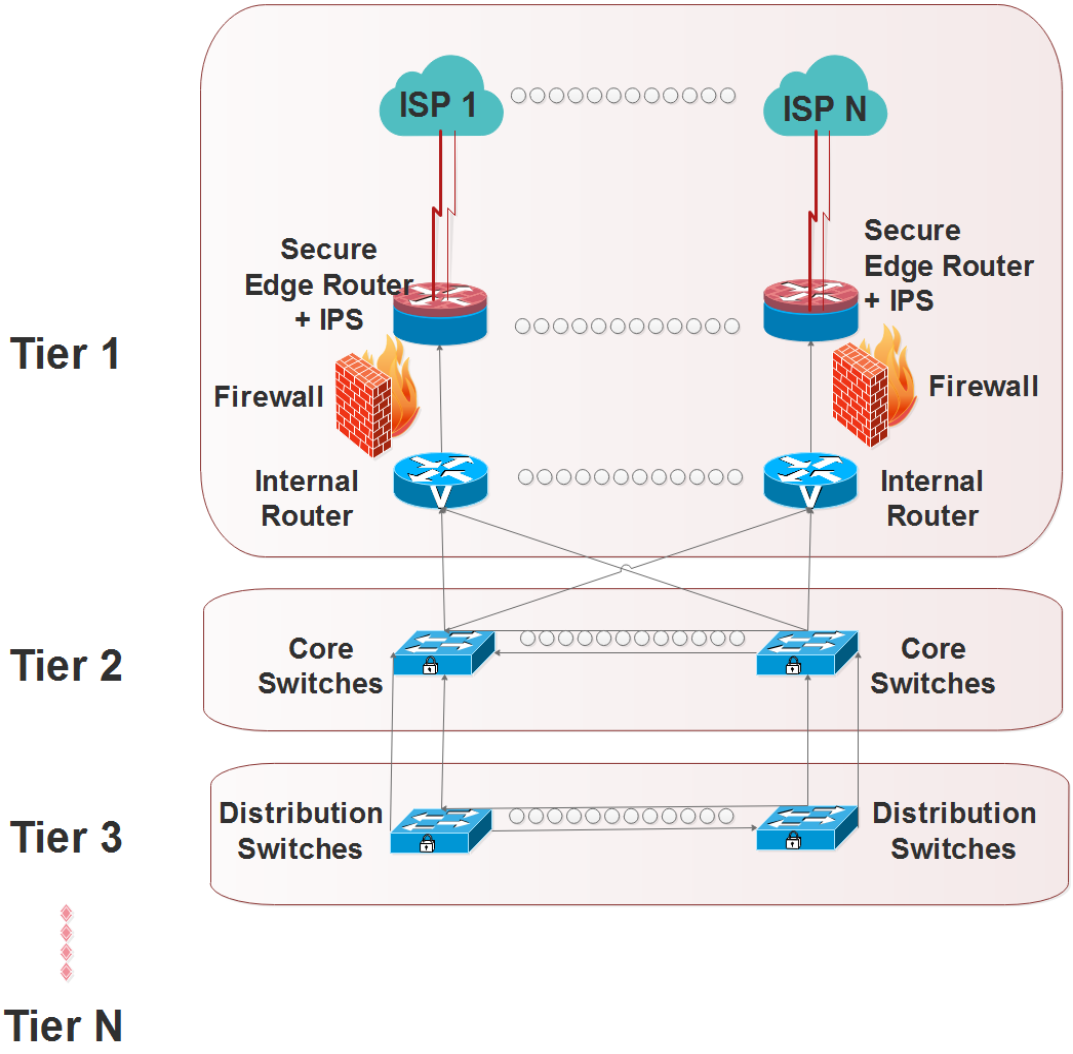


Figure 4.4: An Illustration of Multi-Tier Data Networking Design.

When the network system is under design, the most important idea that should be noted is that the network system is working because all the tiers are working simultaneously in harmony. It means that if one of the tiers fails, the whole system would be in failure status so each tier is very important to operate the system. When the network system has 1 ISP and 2 core switches, it is considered as a two tiers (multi-tiers) example of obtaining the system failure probability because 1 ISP is placed in the first tier and the other core switches are placed in the second tier. The next tables represent all the probability of system status that has multi-tiers and they are shown as follow.

Table 4.2: 2 Tiers System Status

Tier (1) Status	Tier (2) Status	System Status
F	F	F
F	W	F
W	F	F
W	W	W

Table 4.3: 3 Tiers System Status

Tier (1) Status	Tier (2) Status	Tier (3) Status	System Status
F	F	F	F
F	F	W	F
F	W	F	F
F	W	W	F
W	F	F	F
W	F	W	F
W	W	F	F
W	W	W	W

Assuming that the network system has two tiers, the probability of success for tier 1 that has 1 ISP is W1=0.9 and the probability of success for tier 2 that has 2 core switches is W2=0.9. The value of whole system failure probability is obtained by following these four steps:

- Step (1): The probability of failure for each level "tier" must be obtained by using the formula (4.1) which is: $b(x, n, P) = {}^{n}C_{x} \times P^{x} \times (1 - P)^{n-x}$.
- Step (2): The probability of success for each level "tier" must be obtained by using the formula (4.4): $P_n = 1- b(x, n, P)$.
- Step (3): The probability of success for the whole system for all levels combined is obtained and represented by formula (4.5):

$$P_{total} = P1 \times P2 \quad (4.5)$$

- The probability of failure for the whole system must be obtained by using the formula (4.6):

$$Q_{total} = 1 - P_{total}. \quad (4.6)$$

Where the notation "P1" indicates the probability of success in the tier (1), also the "P2" indicates the probability of success in the tier (2), "P_{total}" represents the probability of success for the whole system for all tiers (levels) combined together and "Q_{total}" represents the probability of failure for the whole system.

A system that has two tiers with the first tier being 1 ISP and the second being 2 core switches are considered as an unreliable system because once the ISP stops working the whole system will not work. The same result is also seen when the system has two tiers of 2 ISPs and 1 core switch. The two systems that have 3 ISPs and 3 core switches or 3 ISPs and 2 core switches have high reliability but on the other hand, they require a high budget to create in addition to the complexity that would be ecountered in the configuration and programming of these network devices. Based on the previously mentioned points this research recommeded a system that is consisted of 2 ISPs and 2 core switches because such a system provides reliability and is considered to be economical at the same time.

4.3 Connectivity Models Between Tiers

This section shows the types of connectivity models available and the benefit of each of them. The number of networking device that is utilized is not the only most important factor in the design of multi-tiers in a network environment. The design also depends on the location and connectivity of network devices in each network tier. The proper, optimal connectivity and the organized position of devices of network tiers make the troubleshooting of the whole networking system easier if something wrong happened. The optimal connectivity and organized position ensure perfect utilization of each of the devices on the network and also make all the protocol and functions more integrated with each other. This design makes the network system understandabe and more simple, otherwise, the other network systems would be complex. Each connectivity model has its own characteristics and specific purpose in order to make effective use of them.

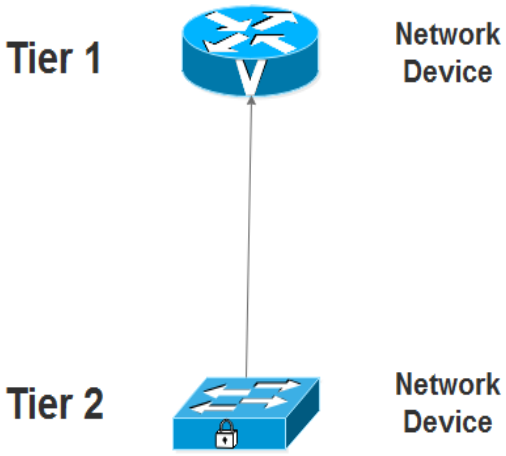


Figure 4.5: One to One Tiers Connectivity

Figure 4.5 shows one type of connectivity model between tiers and this is known as one to one tier connectivity. In this model of connectivity, each network tier has one network device that is connected to another peer network device within the different network tier. The main goal of utilizing this model is to share information and support the other devices to work collaboratively. In addition to that, it helps to establish the desired features or operate a specific mission that is limited due to the network bandwidth but as shown in Figure 4.5 when one network device tier fails, the whole networking system would be in a failure mode since there is no redundant

device.“one to one” tier connectivity is considered as an unreliable connectivity model, therefore, it can only be used in a simple and small network with a poor budget.

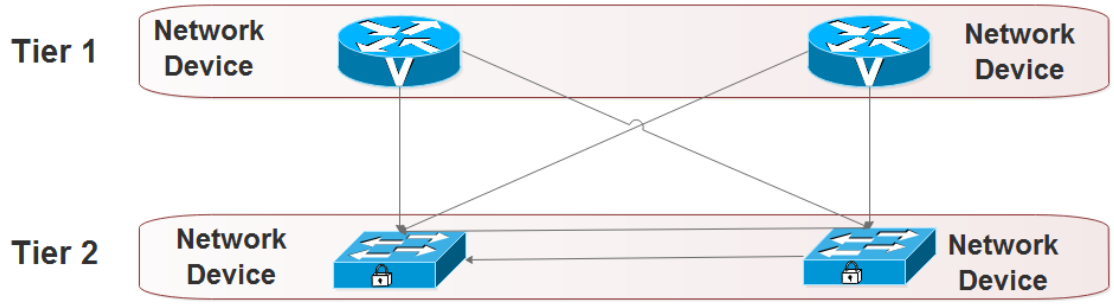


Figure 4.6: Two By Two Tiers Connectivity

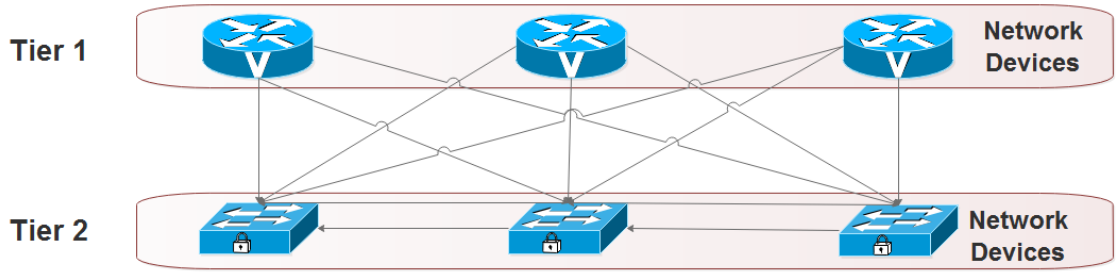


Figure 4.7: Three By Three Tiers Connectivity

Figure 4.6 describes another type of connectivity models between tiers which is “two by two” tiers connectivity. This model has a different connectivity compared to “one to one tier connectivity” because in this case every network tier has two network devices that are connected to other two network devices. Two by two tiers connectivity is considered as a reliable model and at a fair cost, it is recommended when reliability, load balancing, and fair cost are required. Figure 4.7 shows the third type of connectivity models between tiers which is the “three by three” tiers connectivity model. In this model, each network tier has three network devices that connected to another network tier by its three network devices. “Three by three” tiers connectivity provide a high reliability and high load balancing when compared to the other connectivity models but on the other hand, it requires a high complexity and high budget to establish and operate it. When the system is in design connection status, the most important idea that must be noted is that every network device has a specific task, functions, and features which is different from another network device.

Assuming that the network has a firewall, the network firewall uses the concept of zones to secure and manage the network systems, the systems with similar security levels are grouped into zones. For example, the network administrator would expect to see the traffic initiated from the internet making a connection into a demilitarized zone “DMZ” network but do not expect to see the internet traffic going into a data center network. To enforce this behavior, the DMZ network can be placed in one zone and the data center network can be placed in another zone. Then different firewall configuration security policy rules would be applied to control the traffic to and from each zone. The previous practical scenario shows that the placement and connectivity of each networking device must be done very carefully.

CHAPTER 5
NUMERICAL RESULTS & PERFORMANCE INVESTIGATION

5.1 The Performance Analysis of Two Tiers System

This chapter discusses multiple scenarios with multiple numbers of tiers and to investigate the performance of each system that have been suggested. The purpose of these investigations and analysis was to produce optimal, integrated and reliable system. The first scenario based on Figure 5.1 shows a network system that has two levels (tiers). The first tier is considered as 1 ISP and the second tier is considered as three situations: 1 core switch or 2 core switches or 3 core switches. Investigating and analyzing these three situations as represented in Figure 5.1 shows that the system with 1 ISP and 3 core switches provide the highest reliability when compared to systems utilizing 1 switch or 2 switches. However the system of two tiers with 1 ISP and 3 switches is still not considered as a reliable system due to the existing one ISP. In case the ISP got disrupted then the whole system would be in a failure situation, thus it is an unreliable system.

Table 5.1: Results of System Failure Probability for "1 ISP"

	System Failure Probability							
1 ISP / 1 SW	0.1450	0.1900	0.2350	0.2800	0.3250	0.3700	0.4150	0.4600
1 ISP / 2 SWs	0.1023	0.1090	0.1202	0.1360	0.1563	0.1810	0.2103	0.2440
1 ISP / 3 SWs	0.1001	0.1009	0.1030	0.1072	0.1141	0.1243	0.1386	0.1576

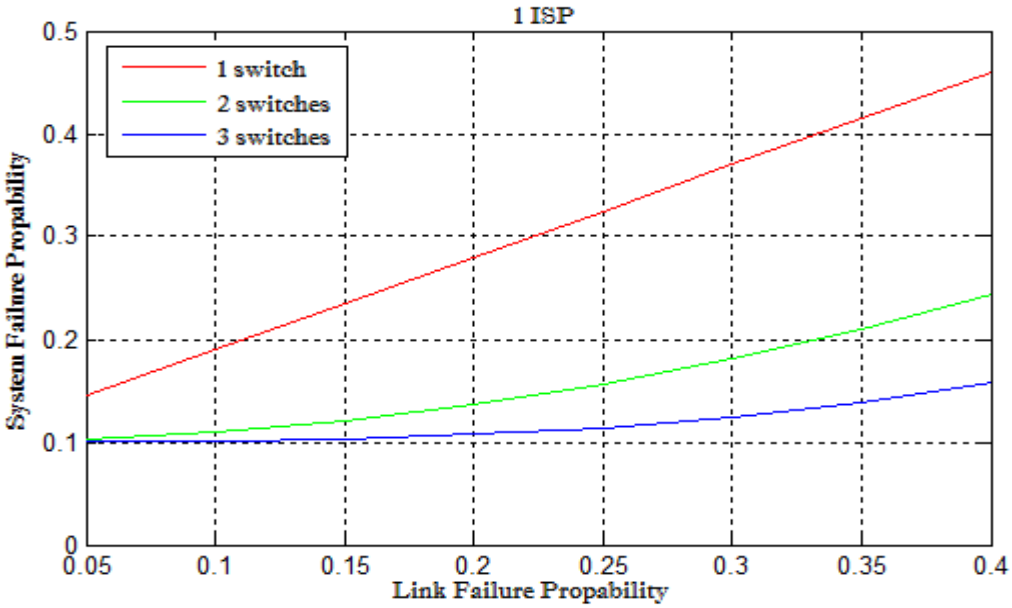


Figure: 5.1: System failure probability for "1 ISP"

Figure 5.2 indicates the second scenario that has a network system of two tiers, but the first tier has 2 ISPs and the second tier has three cases: 1 core switch, 2 core switches and 3 core switches. In the first case, the network system consists of 2 ISP and 1 core switch and the system is considered as unreliable. The reason being that when utilizing one core switch, then this switch suddenly got disrupted, the whole system would be in a failure situation. The result of the investigation and analysis of the performance of the system failure probability gives a very bad curve performance compared with the performance of 2 and 3 core switches as shown in Figure 5.2. The performance result of using the network system that has the first tier 2 ISP and second tier 3 core switches gives the best curve reliability performance compared with utilizing 1 or 2 core switches. However, it is not classified as an optimal system due to the high cost needed to establish it. All previous points in this thesis and in the networking environment indicated that the networking system that has tier of 2 ISP and another tier of 2 switches is a reliable system and with a fair cost to establish it as shown in Figure 5.2.

Table 5.2: Results of System failure probability for "2 ISP"

	System Failure Probability							
2 ISP / 1 SW	0.0595	0.1090	0.1585	0.2080	0.2575	0.3070	0.3565	0.4060
2 ISP / 2 SWs	0.0125	0.0199	0.0323	0.0496	0.0719	0.0991	0.1313	0.1684
2 ISP / 3 SWs	0.0101	0.0110	0.0133	0.0179	0.0255	0.0367	0.0524	0.0734

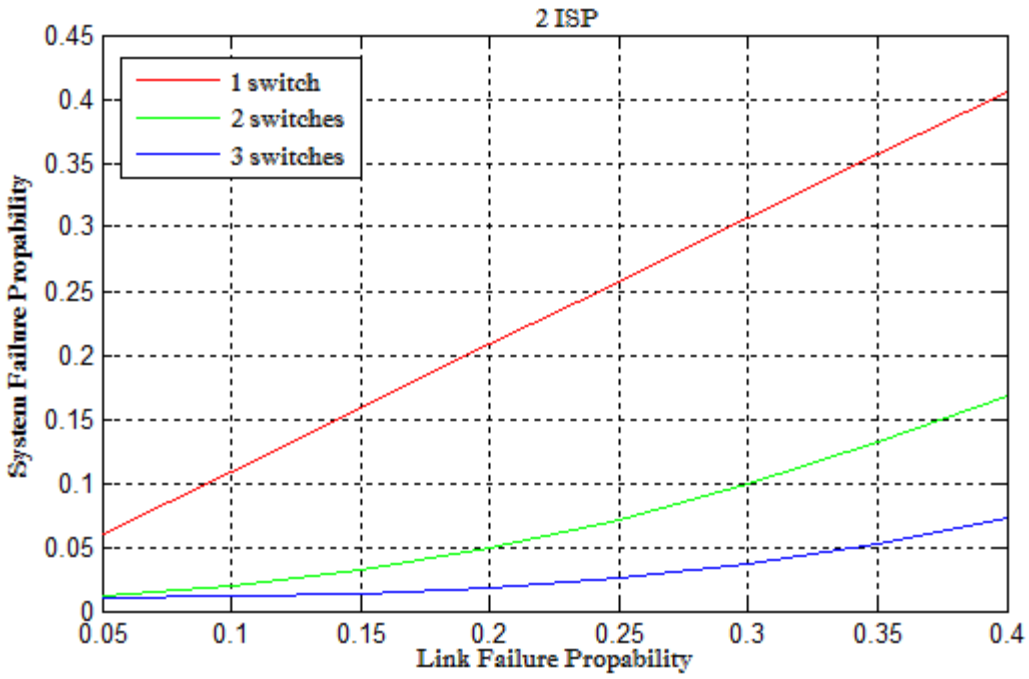


Figure: 5.2: System failure probability for "2 ISP"

The third scenario is represented by existing network system that has a two-tier of network devices. The first tier is 3 ISPs and the other tier has three cases: 1 core switch, 2 switches and 3 core switches. The first case of existing one core switch is considered as an unreliable system because there is no redundant core switch to provide the reliability. The performance result of the network system that consists of 3 ISPs and 2 switches has a high curve of reliability, but on the other hand, a high cost is needed to create it. As shown in Figure 5.3 the best performance result of reliability is accorded to the system that has 3 ISPs and 3 core switches, it has the lowest curve result of failure probability but the system with 3 ISPs and 3 switches needs a very high

budget to establish it. It is complicated to configure and program it as a result of the high number of network devices that are required to establish and publish it, the system requires high cost and high complexity to provide it.

Table 5.3: Results of System failure probability for "3 ISP"

	System Failure Probability							
3 ISPs / 1 SW	0.0510	0.1009	0.1509	0.2008	0.2508	0.3007	0.3507	0.4006
3 ISPs / 2 SWs	0.0035	0.0110	0.0235	0.0410	0.0634	0.0909	0.1234	0.1608
3 ISPs / 3 SWs	0.0011	0.0020	0.0044	0.0090	0.0166	0.0280	0.0438	0.0649

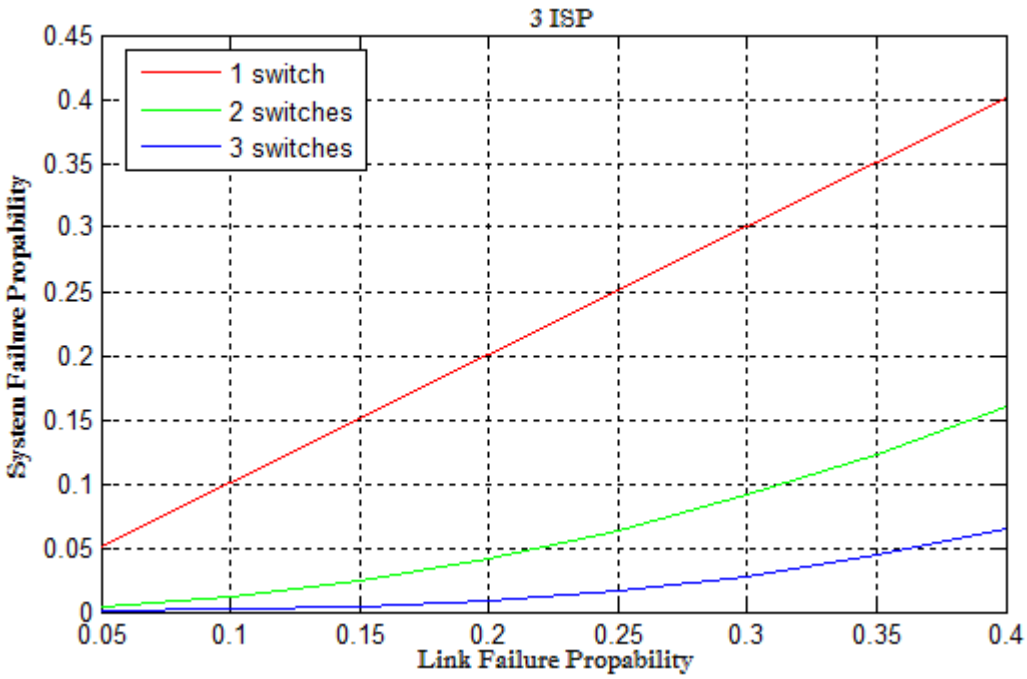


Figure: 5.3: System Failure Probability for "3 ISP"

This research suggested that having one switch in core switch tier would be unreliable even with existing multiple ISPs (2 or 3 ISPs). Thus, it is important to have at least two or more switches at core switching level. Figure 5.4 shows the result of analyzing the performance and reliability of utilizing 2 core switches with 2 and 3 ISPs, also using 3 core switches with 2 and 3 ISPs.

Based on the analyses that are shown in Figure 5.4 , when the value of link failure probability is equal or less than 0.15 using 2 core switches, it is considered as an optimal networking system. When the value of link failure probability is bigger than 0.15 it is recommended to use 3 core switches in the networking system.

As shown in Figure 5.4, there is little improvement in performance when the number of ISPs is increased from 2 ISPs to 3 ISPs. However, the system that contains 3 ISPs will cost too much and it leads to using more network devices resulting in more complexity to the configuration, programming and handling of the system in general. This study suggests and recommends the utilization of 2 ISPs because of its advantages.

Table 5.4: System Failure Probability for 2 SWs & 3 SWs

	System Failure Probability							
2 SWs / 2 ISPs	0.0125	0.0199	0.0323	0.0496	0.0719	0.0991	0.1313	0.1684
2 SWs / 3 ISPs	0.0035	0.0110	0.0235	0.0410	0.0634	0.0909	0.1234	0.1608
3 SWs / 2 ISPs	0.0101	0.0110	0.0133	0.0179	0.0255	0.0367	0.0524	0.0734
3 SWs / 3 ISPs	0.0011	0.0020	0.0044	0.0090	0.0166	0.0280	0.0438	0.0649

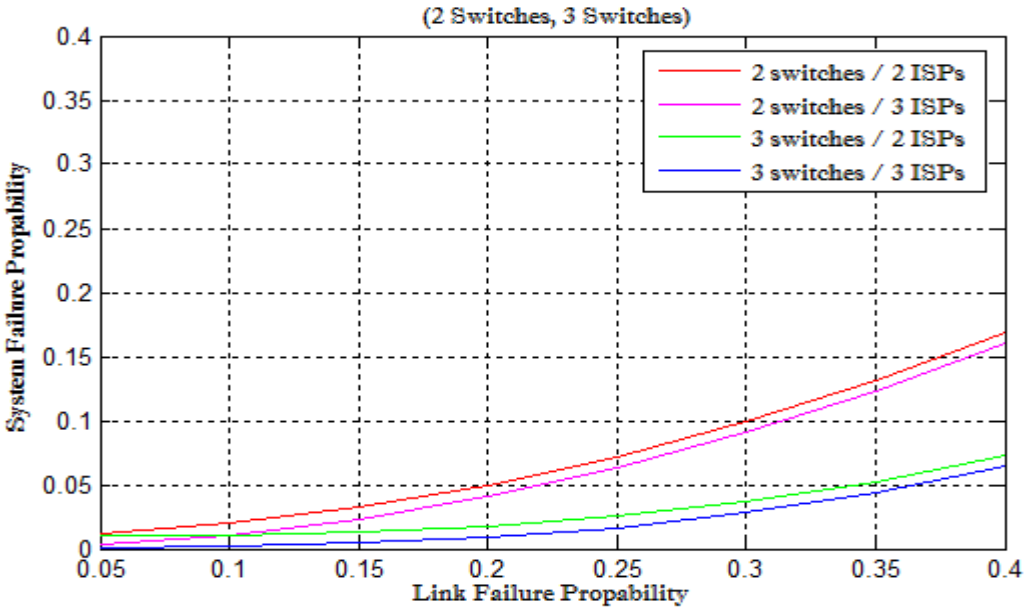


Figure 5.4: System performance for 2 SWs & 3 SWs

5.2 The Performance Analysis of Three Tiers System

This section describes and analyzes the performance of multiple scenarios of the networking system platform. This system consists of 3 networking tiers which are ISP, core switch, and distribution switch "DS". Based on the previous analyses of networking systems performance, there is a little improvement when the number of ISPs at ISP networking tier increase from 2 ISPs to 3 ISPs inside the networking system, consequently, in the three tiers investigations and analysis, the number of ISPs is assumed to always be equal to 2 in all scenarios. The first networking system consists of 3 tiers, the first tier represented the 2 ISP, the second tier has 2 core switches and the third tier has 2 distribution switches. Figure 5.5 shows the system failure probability of the first networking system while Table 5.5 shows the results of this networking system performance. This networking system platform is a reliable system due to the existence of redundant networking device for each networking tier. It is recommended to be utilized as a result of the fair requirements needed to establish, design and configure it.

Table 5.5: Results of System performance for 2 Core Switches, 2 DS switches, 2 ISPs

System Failure Probability For 2 Core, 2 DS, 2 ISP							
0.0149	0.0224	0.0347	0.0520	0.0742	0.1014	0.1334	0.1705
0.0224	0.0297	0.0420	0.0591	0.0812	0.1081	0.1400	0.1767
0.0347	0.0420	0.0540	0.0710	0.0928	0.1194	0.1508	0.1871
0.0520	0.0591	0.0710	0.0876	0.1090	0.1351	0.1660	0.2017
0.0742	0.0812	0.0928	0.1090	0.1299	0.1554	0.1856	0.2204
0.1014	0.1081	0.1194	0.1351	0.1554	0.1802	0.2095	0.2432
0.1334	0.1400	0.1508	0.1660	0.1856	0.2095	0.2377	0.2703
0.1705	0.1767	0.1871	0.2017	0.2204	0.2432	0.2703	0.3015

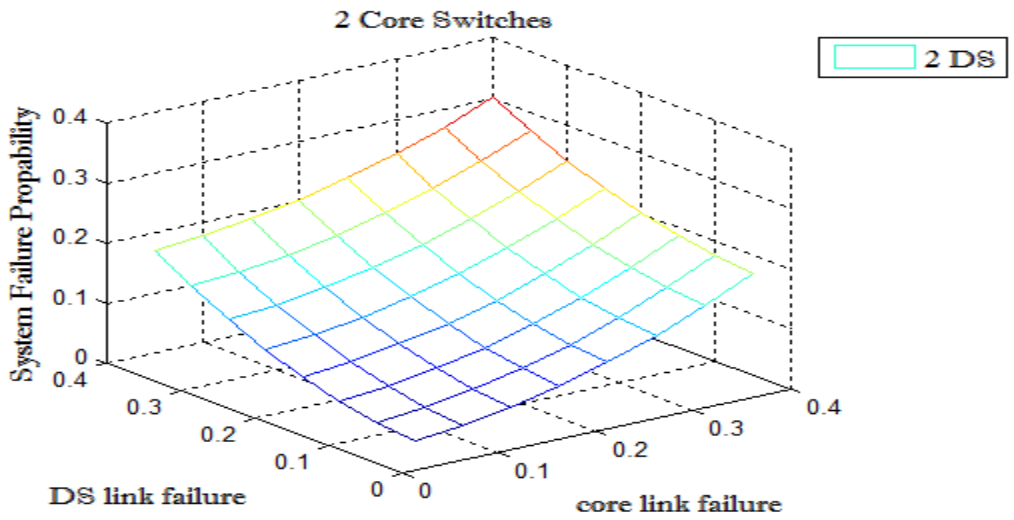


Figure 5.5: System Failure Probability For 2 Core switches, 2 DS switches, 2 ISP

While the second networking system includes 3 tiers also, ISP tier has 2 ISP, core switch tier has two core switches and the distribution switch tier has 3 DS. The Figure 5.6 shows the results of system performance for this second networking system. This system is more reliable compared with the previous system as a result of the existence of 3 distribution switches but it is more complex to create and publish and also needs a higher budget to provide it. The analyses of performance of these two networking systems indicate that when the value of system failure probability is less or equal to 0.2 it is recommended to utilize the first networking system which has 2 core switches and 2 distribution switches. In case the values of system failure probability became bigger than 0.2, the second system which has 2 core switches and 3 distribution switches should be selected to serve the network clients.

Table 5.6: Results of System Performance for 2 Core Switches, 3 DS switches, 2 ISPs

System Failure Probability For 2 Core, 3 DS, 2 ISP							
0.0126	0.0135	0.0158	0.0204	0.0279	0.0391	0.0548	0.0757
0.0200	0.0209	0.0232	0.0277	0.0352	0.0464	0.0619	0.0826
0.0324	0.0332	0.0355	0.0400	0.0474	0.0584	0.0738	0.0942
0.0497	0.0506	0.0528	0.0572	0.0645	0.0753	0.0903	0.1104
0.0720	0.0728	0.0750	0.0793	0.0864	0.0969	0.1117	0.1313
0.0992	0.1000	0.1021	0.1063	0.1132	0.1234	0.1377	0.1568
0.1314	0.1321	0.1342	0.1382	0.1448	0.1547	0.1685	0.1869
0.1685	0.1692	0.1712	0.1751	0.1814	0.1909	0.2041	0.2216

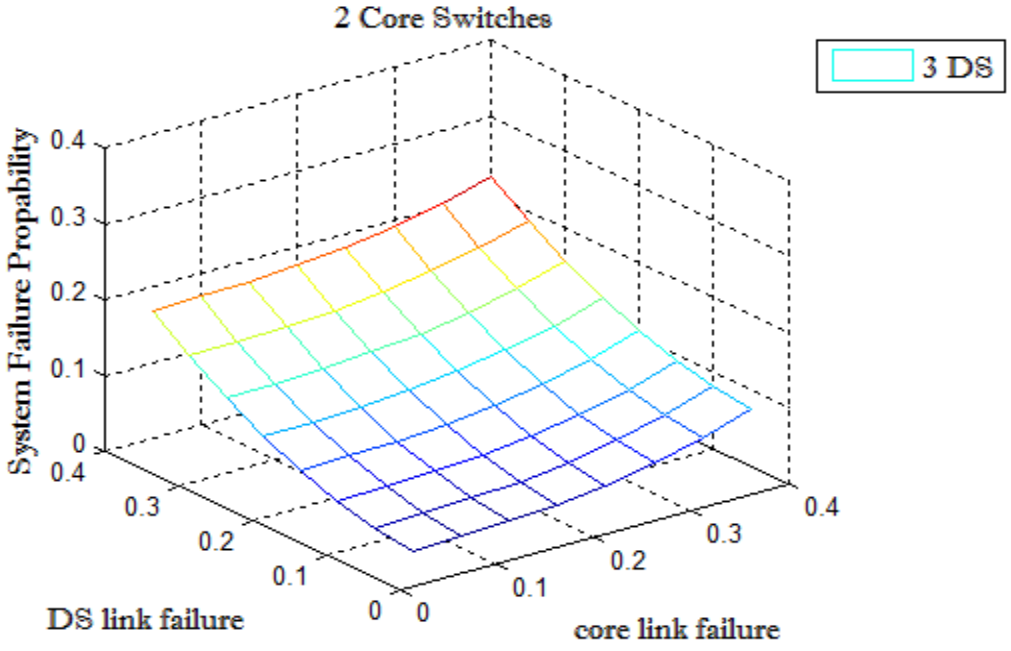


Figure 5.6: System Performance for 2 Core Switches, 3 DS Switches, 2 ISPs

Figure 5.7 represents the performance analysis of networking system of 3 networking tiers, which has 3 core switches, 2 distribution switches, and 2 ISPs. This system is recommended when a high pressure exists on the networking core tier. For example, if the number of servers inside the servers farm increases more and more due to increasing number of applications and services, the networking devices around the core switches also increase due to the increase in

the number of network users, so, the networking system must be extended. This system is used when a very high reliability is wanted. As a result of existing multiple redundant networking devices in each networking tier especially the core network tier, it has a higher reliability compared with the two previous systems.

Table 5.7: Results of System performance for 3 Core Switches, 2 DS Switches, 2 ISPs

System Failure Probability For 3 Core, 2 DS, 2 ISP							
0.0126	0.0200	0.0324	0.0497	0.0720	0.0992	0.1314	0.1685
0.0135	0.0209	0.0332	0.0506	0.0728	0.1000	0.1321	0.1692
0.0158	0.0232	0.0355	0.0528	0.0750	0.1021	0.1342	0.1712
0.0204	0.0277	0.0400	0.0572	0.0793	0.1063	0.1382	0.1751
0.0279	0.0352	0.0474	0.0645	0.0864	0.1132	0.1448	0.1814
0.0391	0.0464	0.0584	0.0753	0.0969	0.1234	0.1547	0.1909
0.0548	0.0619	0.0738	0.0903	0.1117	0.1377	0.1685	0.2041
0.0757	0.0826	0.0942	0.1104	0.1313	0.1568	0.1869	0.2216

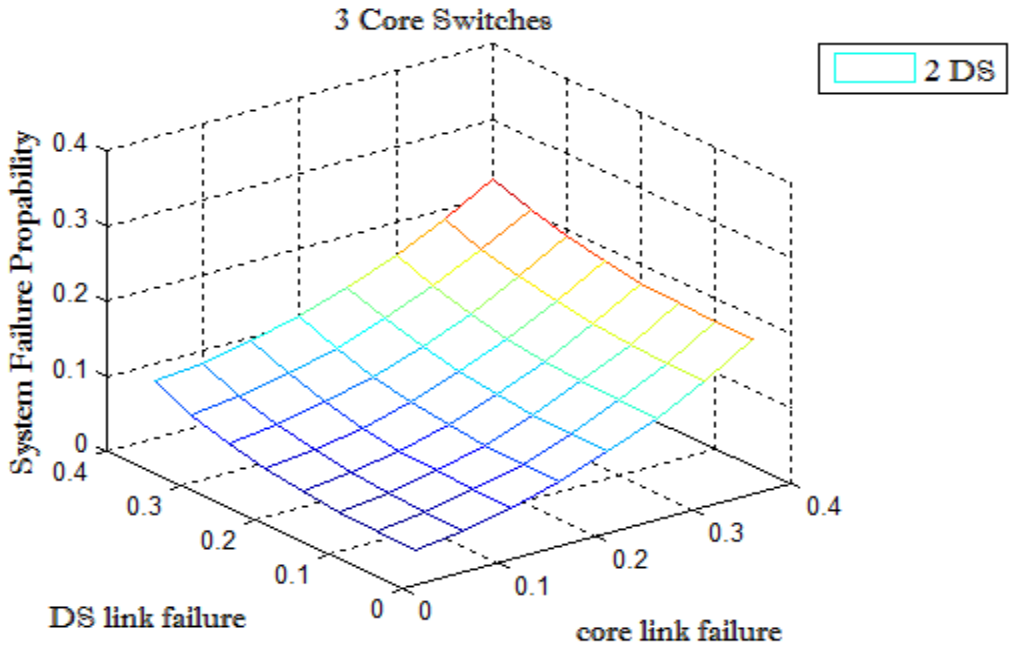


Figure 5.7: System Performance for 3 Core Switches, 2 DS Switches, 2 ISPs

Figure 5.8 shows the performance analysis of networking system of 3 tiers also. It has 3 core switches, 3 distribution switches, and 2 ISPs. This system is more preferred compared to the previous system. The previous system that is shown in Figure 5.7 has a very weak and sensitive point. It has 3 core switches inside the core tier and 2 distribution switches inside distribution tier. In this case, the 2 distribution switches would not be able to accommodate the data traffic that is coming from the 3 core switches, consequently, the system that is shown in Figure 5.8 which has 3 core switches and 3 DS is more recommended because it has the highest reliability compared to all the previous networking systems. On the other hand, this type of networking system platform request a very high budget to be established and it is considered to be sophisticated to design and configure.

Table 5.8: Results of System performance for 3 Core Switches, 3 DS Switches, 2 ISPs

System Failure Probability For 3 Core, 3 DS, 2 ISP							
0.0102	0.0111	0.0135	0.0180	0.0256	0.0369	0.0526	0.0735
0.0111	0.0120	0.0143	0.0189	0.0264	0.0377	0.0534	0.0743
0.0135	0.0143	0.0167	0.0212	0.0288	0.0400	0.0556	0.0765
0.0180	0.0189	0.0212	0.0258	0.0333	0.0444	0.0600	0.0808
0.0256	0.0264	0.0288	0.0333	0.0407	0.0518	0.0673	0.0878
0.0369	0.0377	0.0400	0.0444	0.0518	0.0627	0.0780	0.0984
0.0526	0.0534	0.0556	0.0600	0.0673	0.0780	0.0931	0.1131
0.0735	0.0743	0.0765	0.0808	0.0878	0.0984	0.1131	0.1327

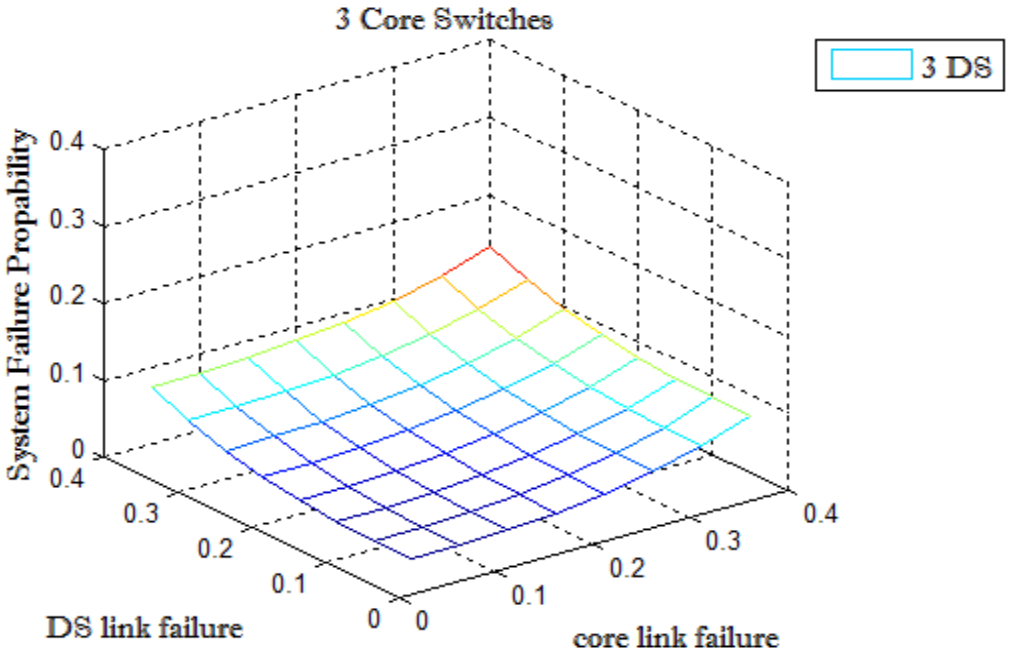


Figure 5.8: System Performance for 3 Core Switches, 3 DS Switches, 2 ISPs

CHAPTER 6
CONCLUSIONS AND FUTURE RESEARCH

6.1 Summary and Conclusions

The design, implementation and configuration of a scalable and reliable networking system platform is full of many obstacles and these obstacles can be overcome by many innovated methods and protocols which have been proposed in this thesis. A new networking tier design protocol was executed to enhance and develop the networking design as a physical enhancement. Diversified networking protocols were utilized to lead the networking system to the reliability and scalability as much as possible where it is considered as a logical development. The performance of two tiers networking systems and 3 tiers networking systems were investigated and analyzed by using the binomial probability function with multiple scenarios. The following conclusions were drawn:

1. It is very important to consider and design each tier separately from the networking platform as well as the design of the platform as a whole to get reasonable and useful reliability analysis.
2. When the network system is under design, the most important idea that should be noted is that the network system is working with all the tiers working simulatenously in harmony. It means that if one of the tiers fails, the whole system would be in failure status, therefore, each tier is very important to operate the system.
3. Increasing the number of network devices will not increase the reliability and scalability level of networking system and it is useless unless it is put in an appropriate place for each networking tier.
4. It is not recommended to implement or apply a networking system that has one network device per one network tier due to the vulnerability in the reliability and redundancy level. Example of this is a two tiers network system, the first tier has one router where the second tier contains 2 switches.

5. This study suggests and recommends the utilization of 2 ISPs instead of 3 ISPs per network tier, because there is little improvement in performance when the number of ISPs is increased from 2 ISPs to 3 ISPs. Otherwise, the networking system platform which has 3 ISPs requests a very high budget and is sophisticated to design and configure without any advantageous services.
6. Increasing the network device per network tier depends on the pressure of data traffic that passes through it but at the same time, the matching of accommodating devices in transferring the data traffic between network tiers is very important to be in the consideration of the process.

6.2 Future Research Directions

The research presented in this thesis showed an awesome enhancement and development of design, reliability and scalability level of networking system platform. Yet, for the practical realization of the networking system still much research effort is needed to develop an advanced networking system platform. Following are a number of interesting research directions that the focus of this research can be extended to:

- **Extend the Scalability and Reliability with Virtualization and Flexibility of Networking System Platform.** In a dynamic networking environment, the challenge with flexibility is about how massive clusters of networking nodes will be synchronized together. The key of virtualization and flexibility is to keep easiness and simplicity by removing intricacy, simplifying the process, and integrating automation to ensure a dynamic and responsive networking infrastructure. The other goal of flexibility is to virtualize the logical and physical networking components, such as servers, storage, switching operations, routing processes, and bandwidth then merge them virtually due to the need to provide integrated network services, load balancing, fault-tolerant, and so on. Figure 6.1 is an illustration of virtualization and flexibility of the networking system platform that consists of multiple network tiers. These virtual network tiers are shown below:

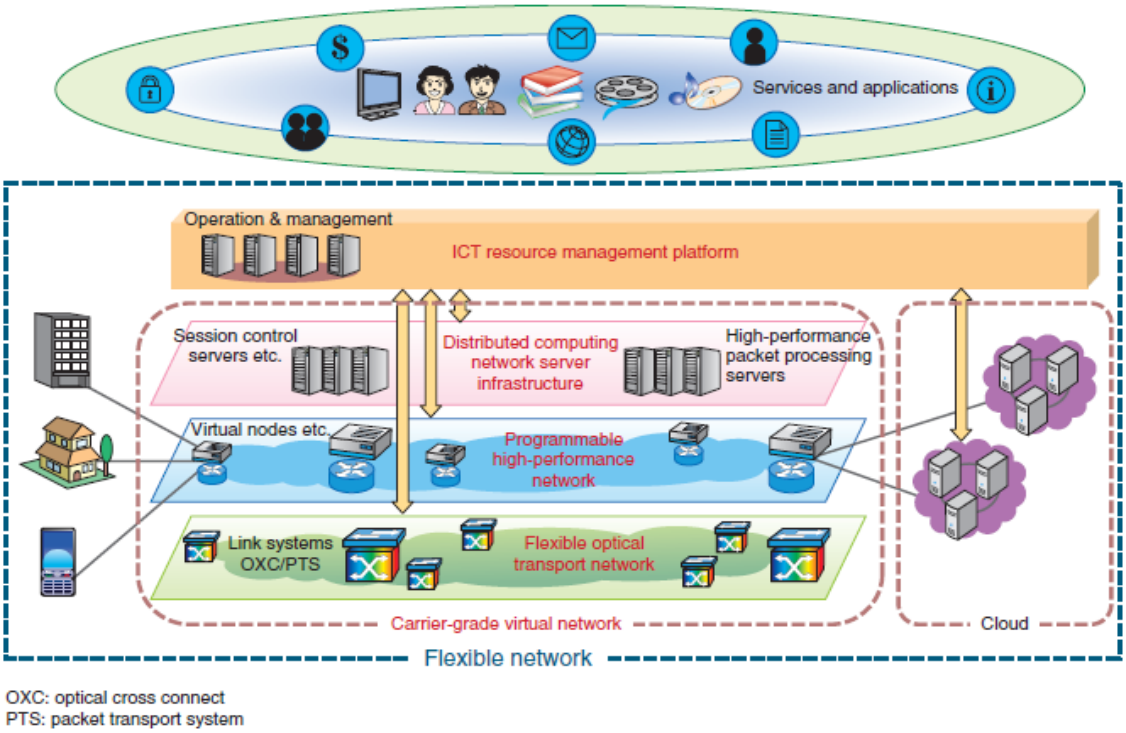


Figure 6.1: A Model of Virtualization and Flexibility of Networking System Platform

The lowest tier is known as a Flexible Optical Transport networking "FOT", while the second tier is a Programmable High Performance network "PHP". The third virtual tier is the Distributed Computing Network Server infrastructure "DCS", and the highest tier is "ICT" resource management platform. All these virtual and flexible tiers are examples, and can be enhanced and developed in the future scientific research as an extension of scalability and reliability of this thesis.

- **Network Functions Virtualization "NFV", and Network Virtualization "NV".** NFV and NV are providing an innovated methods to layout, construct and operate networks. Through the last decades, the environment of networking has seen a huge number of innovations in network devices to reach the networks, software solutions, and network services that operate in the area of networking and also in storage resolutions and computing that has to do with handling "huge database". However, the implicit network that links all of these devices has stayed virtually without alteration. The actuality is that

instances of the extended quantity of network user and their devices utilizing the network have extended its limits to guarantee that the network is able to integrate and assist with the requests of virtualized architectures, especially with multi-tenancy necessities.

- **Analysis and Investigation of the Virtualization and Flexibility of Networking System Platform.** The network infrastructure must operate in an orchestrated method to handover the network services in an ideal way. This means that computers, network protocols, applications of production, and all the surrounding systems must have the ability to coordinate without confliction. Widely, the virtualized and flexible network has to be capable to adapt with various network behaviors through strategy and has the capability to appropriate the resources of the network dynamically to the maximum significant organization requirements. All of these requirements are to be well-done via deep careful analysis and investigations with methods that can simply be automated (Blenk et al., 2016).

The output of this thesis and future research contributes to the state-of-the-art on uplink networking, and can be used by industries to design, optimize and investigate the performance of future networking systems platforms.

REFERENCES

Andrea, H. (2016). Network Failover Redundancy Scenario, two sites with two ASA firewalls. Retrieved February 15, 2018 from https://www.networkstraining.com

Blenk, A., Basta, A., Reisslein, M., & Kellerer, W. (2016). Survey on network virtualization hypervisors for software defined networking. IEEE Communications Surveys & Tutorials, 18(1), 655-685.

Bligh, A. (2015). Network Scalability, Layer 2 Issues. Retrieved February 29, 2018 from https://www.flexiant.com/2015/01/22/network-scalability-layer-2-issues/

Carroll, B. (2008). CCNA Wireless Official Exam Certification Guide (CCNA IUWNE 640-721). Pearson Education.

CCNA Tutorial 9tut. (2010). CCNA Knowledge, Open-Shortest-Path-First "OSPF". Retrieved January 05, 2018 from http://www.9tut.com/ospf-routing-protocol-tutorial

CCNA Tutorial 9tut. (2011). CCNA Knowledge, Routing Information Protocol "RIP". Retrieved January 01, 2018 from http://www.9tut.com/rip-routing-protocol-tutorial

CCNA Tutorial 9tut. (2011). CCNA Knowledge, Virtual Local Area Network VLAN Concepts. Retrieved January 21, 2018 from http://www.9tut.com/virtual-local-area-network-vlan-tutorial

CCNA Tutorial 9tut. (2013). CCNA Knowledge, Hot Standby Router Protocol "HSRP". Retrieved February 29, 2018 from http://www.9tut.com/hot-standby-router-protocol-hsrp-tutorial

CCNA Tutorial 9tut. (2014). CCNA Knowledge, EtherChannel Protocol. Retrieved November 20, 2017 from http://www.9tut.com/etherchannel-tutorial

CCNA Tutorial 9tut. (2016). CCNA Knowledge, Border Gateway Protocol "BGP". Retrieved February 01, 2018 from http://www.9tut.com/border-gateway-protocol-bgp-tutorial

Chaturvedi, S. K. (2016). Network reliability: measures and evaluation. John Wiley & Sons.

Choi, B. Y., Zhang, Z. L., & Du, D. H. C. (2011). Scalable Network Monitoring in High Speed Networks. Springer Science & Business Media.

Cioara, J., & Valentine, M. (2011). CCNA Voice 640-461 Official Cert Guide. Cisco Press.

Cisco networking Academy. (2016). Virtual Private Network "VPN". Retrieved December 20, 2017 from https://www.netacad.com/courses/ccna-security

Cisco. (2018).The future of networking, a guide to the intelligent network. Retrieved March 03, 2018 from https://www.cisco.com/c/en/us/solutions/enterprise-networks/future-of-networking.html

Crubsy. (2017). Advantages of VoIP phone system. Retrieved January 20, 2018 from http://crubsy.com/voip-phone-system-advantages-for-small-business

Empson, S., Gargano, P., & Roth, H. (2014). CCNP routing and switching portable command guide. Pearson Education.

Enterprise Networking Planet. (2015). Characteristics of the Network. Retrieved February 01, 2018 from http://www.enterprisenetworkingplanet.com

Harris, R. (2015). Network Reliability. Retrieved December 20, 2017 from http://seat.massey.ac.nz/143465/Lectures/Network%20Reliability_2_1s.pdf

HowStuffWorks. (1998). The mechanism of VoIP. Retrieved January 15, 2018 from https://computer.howstuffworks.com/ip-telephony.htm

Lammle, T. (2013). CCNA Routing and Switching Study Guide: Exams 100-101, 200-101, and 200-120. John Wiley & Sons.

NNT. (2012). Flexible Virtualized networking system. Retrieved February 02, 2018 from https://www.ntt-review.jp

Odom, W. (2013). CCNA Routing and Switching 200-125 Official Cert Guide Library. Cisco Press.

Santos, O., & Stuppi, J. (2015). CCNA Security 210-260 Official Cert Guide. Cisco Press.

Scalable Network Technology. (2015). Network Design Services. Retrieved January 06, 2018 from https://web.scalable-networks.com/network-design-services

SDxCentral. (2017). Network functions virtualization, network virtualization. Retrieved March 01, 2018 from https://www.sdxcentral.com/sdn/definitions/why-sdn-software-defined networking-or-NFV-network-functions-virtualization-now/

Shooman, M. L. (2003). Reliability of computer systems and networks: fault tolerance, analysis, and design. John Wiley & Sons.

StatTrek. (2016). Binomial Probability Distribution. Retrieved December 23, 2017 from http://stattrek.com/probability-distributions/binomial.aspx

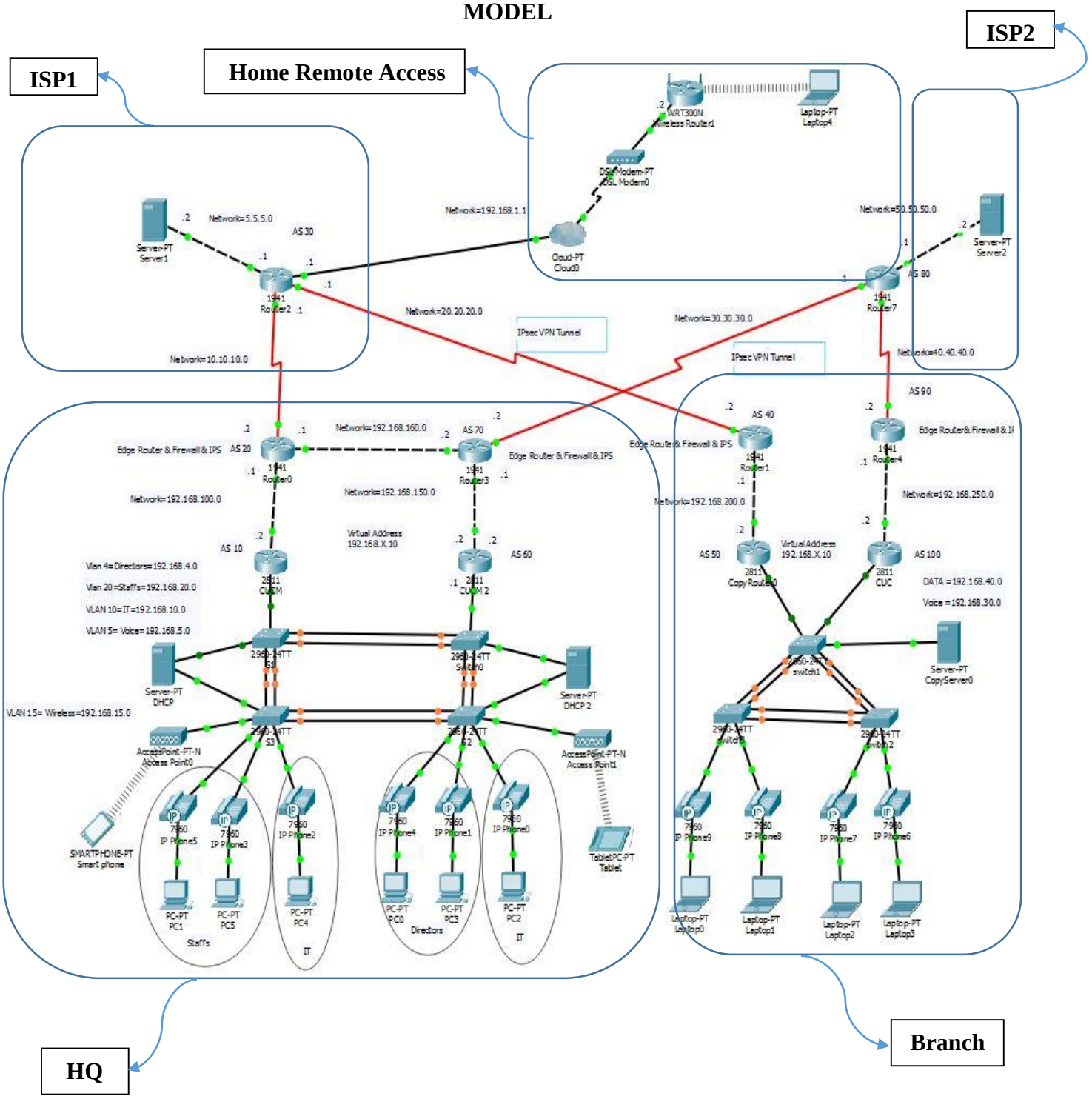
USR. (2015). Wireless LAN Networking, WLAN topologies, Ad Hoc Mode, Infrastructure Mode. Retrieved December 23, 2017 from http://support.usr.com/download/whitepapers/wireless-wp.pdf

VoIP Supply. (2014). VoIP Phone System Overview. Retrieved January 01, 2018 from https://www.voipsupply.com/voip-phone-system-overview

APPENDICES

APPENDIX 1

AN OVERVIEW OF A COMPLETE PACKET TRACER NETWORKING SYSTEM MODEL



APPENDIX 2

PACKET TRACER SOURCE CODES

- Intranet Router

conf t

security passwords min-length 10

enable secret ciscoenapa55

service password-encryption

line console 0

password ciscoconpa55

exec-timeout 15 0

login

logging synchronous

banner motd $Unauthorized access strictly prohibited and prosecuted to the full extent of the law!$

conf t

username **** privilege 15 secret *****

```
aaa new-model

aaa authentication login default local enable


conf t

ip domain-name ccnasecurity.com

crypto key generate rsa 1024

ip ssh version 2

line vty 0 4

transport input ssh


conf t

login block-for 60 attempts 2 within 30

login on-failure log

interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.4
encapsulation dot1Q 4
ip address 192.168.4.1 255.255.255.0
```

```
ip helper-address 192.168.10.2
standby 3 ip 192.168.4.10
standby 3 priority 107
standby 3 preempt
standby 0 track FastEthernet0/1
!
interface FastEthernet0/0.5
encapsulation dot1Q 5
ip address 192.168.5.1 255.255.255.0
ip helper-address 192.168.10.2
standby 2 ip 192.168.5.10
standby 2 priority 106
standby 2 preempt
standby 0 track FastEthernet0/1
!
interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
ip helper-address 192.168.10.2
standby 1 ip 192.168.10.10
standby 1 priority 105
standby 1 preempt
standby 0 track FastEthernet0/1
!
interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
ip helper-address 192.168.10.2
standby 4 ip 192.168.20.10
```

```
standby 4 priority 108
standby 4 preempt
standby 0 track FastEthernet0/1
!
interface FastEthernet0/1
ip address 192.168.100.2 255.255.255.0
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
router bgp 10
bgp log-neighbor-changes
no synchronization
neighbor 192.168.100.1 remote-as 20
network 192.168.4.0
network 192.168.20.0
network 192.168.10.0
network 192.168.5.0
!
ip classless
!
ip flow-export version 9
!
dial-peer voice 100 voip
destination-pattern 4...
session target ipv4:192.168.200.2
```

```
!
telephony-service
max-ephones 20
max-dn 20
ip source-address 192.168.5.1 port 2000
!
ephone-dn 1
number 5001
!
ephone-dn 2
number 5002
!
ephone-dn 3
number 5003
!
ephone-dn 4
number 5004
!
ephone-dn 5
number 5005
!
ephone-dn 6
number 5006
!
ephone 1
device-security-mode none
mac-address 0001.4315.1862
type 7960
button 1:1
```

```
!
ephone 2
device-security-mode none
mac-address 0001.63B8.021D
type 7960
button 1:2
!
ephone 3
device-security-mode none
mac-address 0001.438E.507B
type 7960
button 1:3
!
ephone 4
device-security-mode none
mac-address 0060.7099.6E49
type 7960
button 1:4
!
ephone 5
device-security-mode none
mac-address 00E0.F963.0C9A
type 7960
button 1:5
!
ephone 6
device-security-mode none
mac-address 0050.0F58.C6C8
type 7960
```

button 1:6

!

line con 0

!

line aux 0

!

line vty 0 4

password admin@1234

logging synchronous

login

- **Core Switch**

hostname S1

!

conf t

security passwords min-length 10

enable secret ciscoenapa55

service password-encryption

line console 0

password ciscoconpa55

exec-timeout 15 0

login

logging synchronous

banner motd $Unauthorized access strictly prohibited and prosecuted to the full extent of the law!$

conf t

username Admin01 privilege 15 secret Admin01pa55

aaa new-model

aaa authentication login default local enable

conf t

ip domain-name ccnasecurity.com

crypto key generate rsa

1024

ip ssh version 2

line vty 0 4

transport input ssh

conf t

login block-for 60 attempts 2 within 30

login on-failure log

spanning-tree mode pvst

spanning-tree extend system-id

conf t

interface FastEthernet ***

switchport mode trunk

switchport trunk native vlan ****

switchport nonegotiate

!

interface Port-channel1

 switchport mode trunk

!

interface Port-channel3

 switchport mode trunk

!

interface FastEthernet0/1

```
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/3
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/4
 switchport mode trunk
!
interface FastEthernet0/5
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/6
```

```
 switchport mode trunk
 channel-group 3 mode desirable
!
interface FastEthernet0/7
 switchport mode trunk
 channel-group 3 mode desirable
!
interface FastEthernet0/8
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access
```

```
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/15
```

```
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 10
 switchport mode access
```

```
!
interface FastEthernet0/20
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/24
```

```
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
```

line vty 5 15

login

- Access Switch

hostname S3

!

conf t

security passwords min-length 10

enable secret ciscoenapa55

service password-encryption

line console 0

password ciscoconpa55

exec-timeout 15 0

login

logging synchronous

banner motd $Unauthorized access strictly prohibited and prosecuted to the full extent of the law!$

conf t

enable secret ciscoenapa55

line vty 0 4

password ciscovtypa55

exec-timeout 15 0

login

conf t

interface FastEthernet ***

switchport mode trunk

switchport trunk native vlan ****

switchport nonegotiate

spanning-tree mode pvst

spanning-tree extend system-id

!

conf t

username Admin01 privilege 15 secret Admin01pa55

aaa new-model

aaa authentication login default local enable

conf t

```
ip domain-name ccnasecurity.com

crypto key generate rsa

1024

ip ssh version 2

line vty 0 4

transport input ssh

conf t

login block-for 60 attempts 2 within 30

login on-failure log

interface Port-channel2

 switchport mode trunk

!

interface Port-channel3

 switchport mode trunk

!

interface FastEthernet0/1

 switchport access vlan 10

 switchport mode access
```

```
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/4
 switchport mode trunk
 channel-group 2 mode desirable
!
interface FastEthernet0/5
 switchport mode trunk
 channel-group 2 mode desirable
!
interface FastEthernet0/6
```

```
 switchport mode trunk
 channel-group 3 mode desirable
!
interface FastEthernet0/7
 switchport mode trunk
 channel-group 3 mode desirable
!
interface FastEthernet0/8
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 5
!
interface FastEthernet0/9
 switchport access vlan 20
 switchport mode access
 switchport voice vlan 5
!
interface FastEthernet0/10
```

```
 switchport access vlan 20
 switchport mode access
 switchport voice vlan 5
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 10
```

```
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 10
 switchport mode access
!
```

```
interface FastEthernet0/19
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 10
```

```
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan4
 mac-address 0003.e4d8.1501
 no ip address
!
```

```
interface Vlan20
 mac-address 0003.e4d8.1502
 ip address 192.168.20.2 255.255.255.0
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
```

- Edge Router

```
hostname Router
!
no ip cef
no ipv6 cef
!
license udi pid CISCO1941/K9 sn FTX1524XU26
```

!

conf t

security passwords min-length 10

enable secret ciscoenapa55

service password-encryption

line console 0

password ciscoconpa55

exec-timeout 15 0

login

logging synchronous

banner motd $Unauthorized access strictly prohibited and prosecuted to the full extent of the law!$

conf t

username **** privilege 15 secret ****

aaa new-model

aaa authentication login default local enable

spanning-tree mode pvst

conf t

ip domain-name ccnasecurity.com

crypto key generate rsa

1024

ip ssh version 2

line vty 0 4

transport input ssh

!R1

conf t

login block-for 60 attempts 2 within 30

login on-failure log

conf t

access-list 101 permit ip **** **** **** ****

crypto isakmp policy 10

encryption aes 256

authentication pre-share

hash sha

group 5

lifetime 3600

exit

crypto isakmp key ciscovpnpa55 address ****

crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac

crypto map CMAP 10 ipsec-isakmp

set peer ****

set pfs group5

set transform-set VPN-SET

match address 101

exit

interface ****

crypto map CMAP

zone security IN-ZONE

zone security OUT-ZONE

access-list 110 permit ip **** **** any

access-list 110 deny ip any any

class-map type inspect match-all INTERNAL-CLASS-MAP

match access-group 110

exit

policy-map type inspect IN-2-OUT-PMAP

class type inspect INTERNAL-CLASS-MAP

inspect

zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE

service-policy type inspect IN-2-OUT-PMAP

exit

interface ****

zone-member security IN-ZONE

exit

interface ****

zone-member security OUT-ZONE

mkdir ipsdir

conf t

ip ips config location flash:ipsdir

ip ips name IPS-RULE

ip ips signature-category

category all

retired true

```
exit

category ios_ips basic

retired false

exit

exit

<Enter>

interface ****

ip ips IPS-RULE in

!

interface GigabitEthernet0/0

 ip address 192.168.100.1 255.255.255.0

 duplex auto

 speed auto

!

interface GigabitEthernet0/1

 ip address 192.168.160.1 255.255.255.0

 duplex auto

 speed auto
```

```
!
interface Serial0/0/0
 ip address 10.10.10.2 255.255.255.0
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router bgp 20
 bgp log-neighbor-changes
 no synchronization
 neighbor 10.10.10.1 remote-as 30
 neighbor 192.168.100.2 remote-as 10
```

```
 neighbor 192.168.160.2 remote-as 70
 network 192.168.100.0
 network 192.168.160.0
!
ip classless
!
ip flow-export version 9
!
line con 0
!
line aux 0
!
line vty 0 4
 login
```

- Configure Security and Firewall Settings

enable

<Enter>

conf t

interface vlan 1

nameif inside

security-level 100

ip address **** ****

interface vlan 2

nameif outside

security-level 0

no ip address dhcp

ip address **** ****

exit

hostname Firewall

domain-name ******

enable password *****

username admin password *****

aaa authentication ssh console LOCAL

ssh **** **** inside

ssh **** **** outside

ssh timeout 10

dhcpd address **** **** inside

dhcpd enable inside

route outside **** ****

object network inside-net

subnet **** ****

nat (inside,outside) dynamic interface

exit

conf t

class-map inspection_default

match default-inspection-traffic

exit

policy-map global_policy

class inspection_default

inspect icmp

exit

service-policy global_policy global

APPENDIX 3
MATLAB SOURCE CODES

```
link_failure = 0.05:0.05:0.4;


%% 1 ISP

isp1_failure = binopdf(0,1,0.9);

isp1_success = 1-isp1_failure;


% 1 switch

sw1_failure=binopdf(0,1,1-link_failure);

sw1_success=1-sw1_failure;


 % The Whole System failure

isp1_system_success_sw1=isp1_success*sw1_success;

isp1_system_failure_sw1=1-isp1_system_success_sw1


% 2 switch

sw2_failure=binopdf(0,2,1-link_failure);
```

```
sw2_success=1-sw2_failure;
  % The Whole System failure
isp1_system_success_sw2=isp1_success*sw2_success;
isp1_system_failure_2sw=1-isp1_system_success_sw2

% 3 switch
sw3_failure=binopdf(0,3,1-link_failure);
sw3_success=1-sw3_failure;
  % The Whole System failure
isp1_system_success_sw3=isp1_success*sw3_success;
isp1_system_failure_3sw=1-isp1_system_success_sw3

figure
plot(link_failure, isp1_system_failure_sw1, 'r', link_failure, isp1_system_failure_2sw, 'g', link_failure, isp1_system_failure_3sw, 'b')
title(' 1 ISP ')
legend('1 switch', '2 switches', '3 switches')
xlabel('Link Failure Propability')
```

```
ylabel('System Failure Propability')

grid on


%% 2 ISP

isp2_failure = binopdf(0,2,0.9);

isp2_success = 1-isp2_failure;


% 1 switch

sw1_failure=binopdf(0,1,1-link_failure);

sw1_success=1-sw1_failure;


  % The Whole System failure

isp2_system_success_sw1=isp2_success*sw1_success;

isp2_system_failure_sw1=1-isp2_system_success_sw1


% 2 switch

sw2_failure=binopdf(0,2,1-link_failure);

sw2_success=1-sw2_failure;
```

```
  % The Whole System failure
isp2_system_success_sw2=isp2_success*sw2_success;
isp2_system_failure_2sw=1-isp2_system_success_sw2

% 3 switch
sw3_failure=binopdf(0,3,1-link_failure);
sw3_success=1-sw3_failure;
  % The Whole System failure
isp2_system_success_sw3=isp2_success*sw3_success;
isp2_system_failure_3sw=1-isp2_system_success_sw3

figure
plot(link_failure, isp2_system_failure_sw1, 'r', link_failure, isp2_system_failure_2sw, 'g', link_failure, isp2_system_failure_3sw, 'b')
title(' 2 ISP ')
legend('1 switch', '2 switches', '3 switches')
xlabel('Link Failure Propability')
ylabel('System Failure Propability')
```

```
grid on


%% 3 ISP

isp3_failure = binopdf(0,3,0.9);

isp3_success = 1-isp3_failure;


% 1 switch

sw1_failure=binopdf(0,1,1-link_failure);

sw1_success=1-sw1_failure;


  % The Whole System failure

isp3_system_success_sw1=isp3_success*sw1_success;

isp3_system_failure_sw1=1-isp3_system_success_sw1


% 2 switch

sw2_failure=binopdf(0,2,1-link_failure);

sw2_success=1-sw2_failure;

  % The Whole System failure
```

```
isp3_system_success_sw2=isp3_success*sw2_success;

isp3_system_failure_2sw=1-isp3_system_success_sw2



% 3 switch

sw3_failure=binopdf(0,3,1-link_failure);

sw3_success=1-sw3_failure;

  % The Whole System failure

isp3_system_success_sw3=isp3_success*sw3_success;

isp3_system_failure_3sw=1-isp3_system_success_sw3



figure

plot(link_failure, isp3_system_failure_sw1, 'r', link_failure, isp3_system_failure_2sw, 'g',
link_failure, isp3_system_failure_3sw, 'b')

title(' 3 ISP ')

legend('1 switch', '2 switches', '3 switches')

xlabel('Link Failure Propability')

ylabel('System Failure Propability')

grid on
```

```
link_failure = 0.05:0.05:0.4;



%% 2 Switches


sw2_failure=binopdf(0,2,1-link_failure);

sw2_success=1-sw2_failure;

% 2 ISP

isp2_failure = binopdf(0,2,0.9);

isp2_success = 1-isp2_failure;

  % The Whole System failure

isp2_system_success_sw2=isp2_success*sw2_success;

isp2_system_failure_2sw=1-isp2_system_success_sw2


% 3 ISP

isp3_failure = binopdf(0,3,0.9);
```

```
isp3_success = 1-isp3_failure;

% The Whole System failure

isp3_system_success_sw2=isp3_success*sw2_success;

isp3_system_failure_2sw=1-isp3_system_success_sw2


%% 3 switch

sw3_failure=binopdf(0,3,1-link_failure);

sw3_success=1-sw3_failure;


% 2 ISP

isp2_failure = binopdf(0,2,0.9);

isp2_success = 1-isp2_failure;

  % The Whole System failure

isp2_system_success_sw3=isp2_success*sw3_success;

isp2_system_failure_3sw=1-isp2_system_success_sw3


% 3 ISP

isp3_failure = binopdf(0,3,0.9);
```

```
isp3_success = 1-isp3_failure;

% The Whole System failure

isp3_system_success_sw3=isp3_success*sw3_success;

isp3_system_failure_3sw=1-isp3_system_success_sw3




figure

plot(link_failure, isp2_system_failure_2sw, 'r', link_failure, isp3_system_failure_2sw, 'm',
link_failure, isp2_system_failure_3sw, 'g',link_failure, isp3_system_failure_3sw, 'b')

title(' (2 Switches, 3 Switches)')

legend('2 switches / 2 ISPs', '2 switches / 3 ISPs', '3 switches / 2 ISPs','3 switches / 3 ISPs')

xlabel('Link Failure Propability')

ylabel('System Failure Propability')

grid on
```

```
%% 2 ISPs 2 Core Switches 2 DS Switches
```

```
clc

clear all

core_link_failure = 0.05;

core_vector = zeros(1,8);

ds_vector = zeros(1,8);

arr=zeros(8,8);

DS_link_failure = 0.05;




% 2 ISp

isp2_failure = binopdf(0,2,0.9);

isp2_success = 1-isp2_failure;


for k=1:8

    % 2 Distribution Switches

    DS_Sw2_failure=binopdf(0,2,1-DS_link_failure);

    DS_Sw2_success=1-DS_Sw2_failure;

    ds_vector(k)=DS_Sw2_success;
```

```
    DS_link_failure = DS_link_failure+0.05;
end



for j=1:8
    % 2 Core Switches
    core_2sw_failure=binopdf(0,2,1-core_link_failure);
    core_2sw_success=1-core_2sw_failure;
    core_vector(j)=core_2sw_success;

    for i=1:8
        % The Whole System failure
        isp2_system_success_2core_2DS=core_2sw_success*ds_vector(i)*isp2_success;
        isp2_system_failure_2core_2DS=1-isp2_system_success_2core_2DS;
        arr(j,i)=isp2_system_failure_2core_2DS;
    end

    core_link_failure=core_link_failure+0.05;
```

```
end


disp(ds_vector)

disp(core_vector)

disp(arr)


%% 2 ISPs 2 Core Switches 3 DS Switches


ds_vector3 = zeros(1,8);

arr2=zeros(8,8);

DS_link_failure = 0.05;

for k=1:8

    % 3 Distribution Switches

    DS_Sw3_failure=binopdf(0,3,1-DS_link_failure);

    DS_Sw3_success=1-DS_Sw3_failure;

    ds_vector3(k)=DS_Sw3_success;

    DS_link_failure = DS_link_failure+0.05;
```

```
end
core_link_failure = 0.05;
for j=1:8

   for i=1:8
      % The Whole System failure
      isp2_system_success_2core_3DS=core_vector(j)*ds_vector3(i)*isp2_success;
      isp2_system_failure_2core_3DS=1-isp2_system_success_2core_3DS;
      arr2(j,i)=isp2_system_failure_2core_3DS;
   end

   core_link_failure=core_link_failure+0.05;

end

disp(ds_vector3)
disp(core_vector)
disp(arr2)
```

```
figure


x = 0.05:0.05:0.4;

z = 0.05:0.05:0.4;


mesh(x,z,arr);

title('2 Core Switches')

legend('2 DS ')

xlabel('core link failure')

ylabel('DS link failure')

zlabel('System Failure Propability')


figure

x = 0.05:0.05:0.4;

z = 0.05:0.05:0.4;

mesh(x,z,arr2);

title('2 Core Switches')
```

```
legend('3 DS')

xlabel('core link failure')

ylabel('DS link failure')

zlabel('System Failure Propability')
```

```
%% 2 ISPs 3 Core Switches 2 DS Switches

clc

clear all

core_link_failure = 0.05;

core_vector = zeros(1,8);

ds_vector = zeros(1,8);

arr=zeros(8,8);

DS_link_failure = 0.05;



% 2 ISp

isp2_failure = binopdf(0,2,0.9);
```

```
isp2_success = 1-isp2_failure;


for k=1:8
    % 2 Distribution Switches
    DS_Sw2_failure=binopdf(0,2,1-DS_link_failure);
    DS_Sw2_success=1-DS_Sw2_failure;
    ds_vector(k)=DS_Sw2_success;
    DS_link_failure = DS_link_failure+0.05;
end



for j=1:8
    % 3 Core Switches
    core_3sw_failure=binopdf(0,3,1-core_link_failure);
    core_3sw_success=1-core_3sw_failure;
    core_vector(j)=core_3sw_success;

    for i=1:8
```

```
        % The Whole System failure
        isp2_system_success_3core_2DS=core_3sw_success*ds_vector(i)*isp2_success;
        isp2_system_failure_3core_2DS=1-isp2_system_success_3core_2DS;
        arr(j,i)=isp2_system_failure_3core_2DS;
    end

    core_link_failure=core_link_failure+0.05;

end

disp(ds_vector)
disp(core_vector)
disp(arr)

%% 2 ISPs 3 Core Switches 3 DS Switches

ds_vector3 = zeros(1,8);
```

```
arr2=zeros(8,8);
DS_link_failure = 0.05;
for k=1:8
    % 3 Distribution Switches
    DS_Sw3_failure=binopdf(0,3,1-DS_link_failure);
    DS_Sw3_success=1-DS_Sw3_failure;
    ds_vector3(k)=DS_Sw3_success;
    DS_link_failure = DS_link_failure+0.05;
end
core_link_failure = 0.05;
for j=1:8

    for i=1:8
        % The Whole System failure
        isp2_system_success_3core_3DS=core_vector(j)*ds_vector3(i)*isp2_success;
        isp2_system_failure_3core_3DS=1-isp2_system_success_3core_3DS;
        arr2(j,i)=isp2_system_failure_3core_3DS;
    end
```

```
    core_link_failure=core_link_failure+0.05;


end
disp(ds_vector3)
disp(core_vector)
disp(arr2)
figure
x = 0.05:0.05:0.4;
z = 0.05:0.05:0.4;
mesh(x,z,arr);
title('3 Core Switches')
legend('2 DS ')
xlabel('core link failure')
ylabel('DS link failure')
zlabel('System Failure Propability')
figure
x = 0.05:0.05:0.4;
```

```
z = 0.05:0.05:0.4;

mesh(x,z,arr2);

title('3 Core Switches')

legend('3 DS')

xlabel('core link failure')

ylabel('DS link failure')

zlabel('System Failure Propability')
```