بسم الله الرحمن الرحيم

Sudan University of Science and Technology

College of Graduate Studies

Enhancement of Security for Electronic Record using Virtual Local Area Networks Techniques

تحسين الأمان للسجلات الإلكترونية باستخدام تقنيات الشبكات المحلية الإفتراضية

A Thesis submitted in partial fulfillment for the requirements for the Degree of M.Sc. Information Technology

Presented by:

Mahmoud Norain Mahmoud Basi

Supervision:

Dr. Mohammed Elghazali Hamza Khalil

November 2018

Declaration

I declare that I have worked on this research independently using only the sources listed in the bibliography. All resources, sources, and literature, which I used in preparing or I drew on them, I quote in the research properly with stating the full reference to the source.

Mahmoud Norain Mahmoud basi

Acknowledgement

I would like first to thank my thesis advisor Dr. Mohammed Elghazali Hamza Khalil for granting me the opportunity to write on this topic, and for his lucid instructions and guidance. I am grateful to him for being always there to give me advice whenever I needed them, and especially for his patience with me.

I am extremely grateful for my loving family who has shown more support throughout my entire life than I could have ever wished for. My sister Dr. Tagwa Norain Mahmoud Basi has contributed immeasurably to shaping me as an individual as well as a professional; without their influence and encouragement, I would not be the person I am today. Special thanks are also extended to my dearest friends, Omran ALtigani, Musap Mohammed, Mutwakil Mohammed, Nosiba Altoom and Doaa Mohammed Osman who have granted me with their continuous guidance, mentoring, and friendship. They taught me that life has its strengths and weaknesses, but how you learn from the weaknesses and live from the strengths is what makes life's journey enriching and rewarding.

I would like finally to all my teachers from the whole studies. I thank them for creating a friendly and collegial work environment, and for their cooperation.

Abstract

Continuous development in the world of technology and diversity of data sets containing individual information is growing exponentially as the computer technology; network connectivity and disk storage space become increasingly affordable. The medical record is a record of a patient's information. Using electronic systems to store managers and share patients, healthcare-associated information. Electronic health and medical record systems supported by the use of electronic devices and communication, make health care more efficient and helpful. Remote patient monitoring is becoming more feasible as specialized sensors can be placed inside homes. The combination of these technologies will improve the quality of health care by making it more personalized and reducing costs and medical errors. Also, reduce the cost of providing health care in context. The most important challenge faced these solution is privacy and data security. Furthermore storing data in the cloud raises serious concerns. These research discuses issue related to managing and how to make data health secure. The solution provided in this research includes a set of accompanying policies for deployment and using VLAN techniques to make data secure. And the result of this research is describe how to increase the scalability and security of electronic medical records network. Finally, this research proposed a scalable and secure VLAN architecture and describe how administrators group related hosts into VLANs, and how the switches and routers forward traffic between hosts.

المستخلص

التطوير المستمر في عالم التكنلوجيا انتجت عدد متزايد و متنوع من مجموعات البيانات التي تحتوي على معلومات فردية بشكل كبير كتكنولوجيا للكمبيوتر , الاتصالات و مساحة تخزين الاقراص تصبح بأسعار مقبوله على نحو متزايد نسبة لوجود الشبكات. و السجل الطبي هو سجل لمعلومات المريض و استخدام الأنظمة الإلكترونية للتخزين , إدارة ومشاركة بيانات المرضى، والمعلومات المرتبطة بالرعاية الصحية كأنظمة السجلات الصحية والطبية الإلكترونية التي يدعمها استخدام الأجهزة الإلكترونية والاتصالات ، تجعل الرعاية الصحية أكثر فعالية ومفيدة, بالتالي أصبح رصد المرضى عن بعد أكثر جدوى حيث يمكن وضع أجهزة الاستشعار المتخصصة داخل المنازل. سيؤدي دمج هذه التقنيات إلى تحسين جودة الرعاية الصحية بجعلها أكثر تخصيصًا وتخفيض التكاليف والأخطاء الطبية .أيضا تقليل تكلفة توفير الرعاية الصحية في هذا السياق .التحدي الأهم الذي يواجهه هذا التطور هو الخصوصية وأمان البيانات .علاوة على ذلك ، فإن تخزين البيانات في الحوسبة السحابية يثير مخاوف خطيرة لوجود مخترقي البيانات و حساسية هذه البيانات هذا البحث يركز على القضية المتعلقة بالإدارة وكيفية جعل صحة بيانات المرضى آمنة .يتضمن الحل المقدم في هذا البحث مجموعة من السياسات الامنية واستخدام تقنيات الشبكات المحلية الإفتراضية (VLANs) لضمان سلامة البيانات من التسريب الداخلي و الخارجي و ابقاءها امنة. نتيجة هذا البحث توضح كيفية زيادة قابلية شبكة السجلات الطبية الإلكترونية و طريقة تأمينها.و استخدمت في هذا البحث بنية او هيكلية ال الشبكات المحلية الإفتراضية بطريقة تضمن سلامة البيانات وتوضح كيف يقوم المسؤولون بتجميع المضيفات ذات الصلة تقنية الشبكات المحلية الإفتراضية، وكيف تعمل المحولات والموجهات على توجيه حركة المرور بين المضيفين.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

LAN	Local Area Network
DES	Data Encryption Standard
HIV	Human Immunodeficiency Virus
GNS3	Graphical Network Simulator-3
EHRs	Electronic Health Records
CDP	Cisco Discovery Protocol
MAC	Media Access Control
RACLs	Router Access Lists
TCAM	Ternary Content Addressable memory
CPU	Central Processing Unit
CPMC	Columbia Presbyterian Medical Center

CHAPTER ONE

Introduction

1.1 Preface

Technological development of computers and networked campus increases in the world of today, the need for the increase and strong computer and network security also becomes increasingly necessary and important. The increase in the computer network system has exposed many networks to various kinds of internet threats and with this exposure, one can see that the need for increased network security is vital and important in every organization. The security may include identification, authentication and authorization to protect the integrity, availability, accountability, and authenticity of computer hardware or network equipment and data privacy. There is no laid down the procedure for designing a secure network. Network security has to be designed to fit the needs of one organization network.

Electronic health and medical record systems supported by the use of electronic devices and communication make healthcare more efficient and helpful. Remote patient monitoring is becoming more feasible as specialized sensors can be placed inside homes. The combination of these technologies will improve the quality of health care by making it more personalized and reducing costs and medical errors.

Also, reduce the cost of providing health care in context. The most important challenge faced these solution is privacy, data security and scalability. Furthermore storing data in the cloud raises serious concerns [1].

1.2 Research Background

This research discuses issue related to managing and how to make data health secure by using VLANs Techniques. The number and diversity of data sets containing individual information are growing exponentially as the computer technology; network connectivity and disk storage space become increasingly affordable.

The medical record is a record of a patient’s information. Using electronic systems to store managers and share patients, healthcare-associated information. Compared with the traditional based method, Electronic Health Record provide low cost, high quality and

more flexible. Medical record, transition medical information and store it in the cloud have been deployed to provide healthcare delivery service by accessing a medical record system in public network like the internet.

Enterprise networks, which connect the computers within a hospitals campus or corporate location, differ markedly from backbone networks. These networks have distinctive topologies, protocols, policies, and configuration practices. The unique challenges in enterprise networks are not well understood outside of the operator community. One prominent example is virtual LANs (VLANs) a widely-used technology that is barely discussed in networking [2].

1.3 Problem Statement

Network threats are skilled individuals who are willing to exploit the security weakness of a network in order to inflict costly damage. The challenges faced electronic medical record is sharing critical patient's data through campus sections and public internet and when load online there no protection. Unauthorized access sensitive medical data. The most important challenge is privacy, data security and scalability.

1.4 Objectives

- To investigate or to analyze VLANs a variety of goals of electronic medical record systems for the campus in their department.
- To enhance electronic medical record systems by developing a new policy solution.
- To evaluation management process by notice administration

1.5 Scope of Research

This research is the selection of a hospital campus as a case study and focuses on provide permeation's in terms of dealing between the departments, to secure communication path.

1.6 Research Solution

The solution will provide in this research includes a set of accompanying policies for

deployment in firewall and VLAN techniques that will appear in Cisco packet tracer as emulation.

1.7 Theses Layout

Selected modern technique (VLAN) for security analysis mainly at the IP layer are described in Chapter 2. Network visualization as an important part of the security analysis, gather requirements, selection of equipment and hierarchical model of campus network design is discussed in Chapter 3. Chapter 4, focus on the analysis data of hospitals topologies and implementation stage to test a design that meets these requirements are presented, even include the steps and commands demonstration in the appendix. Chapter 5 it contains conclusion of what has been achieved in this research and recommendations that help researchers in the field of data privacy and network expansion to know from where to begin or continue is the same field.

CHAPTER TOW

Literature Review

2.1 Introduction

In the growth of scientific medicine, medical records have played an important role as a tool and basis for planning patient care besides medical education, research and legal protection. By creating a virtual local area network (VLAN), broadcast domains break up in a pure switched internetwork. A VLAN is a logical group of network users and resources connected administratively defined ports on a switch. When VLANs created, it will be the ability to create smaller broadcast domains within a layer 2 switched internetworks by assigning different ports on the switch to different subnetworks. A VLAN is treated like its own subnet or broadcast domain, meaning that frames broadcast onto the network are only switched between the ports logically grouped within the same VLAN.

Network simulator is integrated and versatile package of tools that emulates network's behaviour like creating network topology, log events that occur under any load, parsing the events and understanding the network. It supports the application of various kinds of protocols in diverse types of the network with different elements and traffic models[3]. Recently, network simulators are being used extensively in different areas such as, conducting research and teaching, designing different network topologies, Quality Assurance of industrial developments for simulating, verifying, and analyzing the performance of new networking topologies and evaluating effects of the different parameters on the communication protocols that are being studied [2].

2.2 Electronic Medical Record

It's noted that users of medical records sites are exposed to the risk of confidentiality and security problems in general. Security and privacy policies developed by the Platforms are often insufficient. This is because these owners focus on functionality and ease of use. Another contributing factor to privacy and security risk is the Internet infrastructure, which does not support security enough. The consequence is that, no matter how much

the security mechanism, absolute security cannot be achieved due to there any 100% secure. Another issue is the real risk facing electronic records of satisfaction, which ensures the use of online business information and records of patients and doctors. In fact, a security and confidentiality risk.

One aspect involves observing patients' preferences through cookies without their knowledge. The other involves passing patient information to a third party without their knowledge or consent and therefore the occurrence of such data as well as another violation of privacy [2].

2.3 Virtual Local Area Network (VLAN)

One of the most popular network virtualization technologies in today's enterprise and campus networks. The VLAN in enterprise and campus networks are commonly used to group hosts in administrative domains and disregards their physical locations in the network topology. Example groups are engineers, sales, student clusters, managers, faculty clusters.

Network administrators can reduce the complexity of their management tasks, as well as provide better security and reduce costs. For example, VLAN can help network administrators create many smaller broadcast domains from a large on instead of using expensive routers. VLAN is a useful mechanism for limiting the scope of broadcast traffic, enforcing security and privacy policies, simplifying access control, decentralizing network management, and enabling host mobility [3].

Computer simulation is a technique of imitation of imaginary and actual objects on a computer such that system functions and its behaviour can be studied. The network simulation, particularly means that the computer-aided simulation techniques model the network functionality and its behaviour by determining the interaction between the different network elements (hosts/routers, etc.) using mathematical formulas, or actually monitoring and imitating experimental observations from a real network. The data from simulation experiments could be used to analyze in a series of offline test experiments to test the protocols that are supported by the network and network behaviour. Lately, application of simulation technology has been widely developed for simulating computer networks traffic [3].

VLAN need in today's world and then to conclude with the sketch of ongoing problems with desire solution and overall security techniques (Spanning Tree Protection, Enabling MAC Flooding Defense, Enabling Cisco Discovery Protocol (CDP) Protection, VLAN Hopping Defense, Dynamic Port Configuration, Double Tagging and Safe Implementation Process) with respect to different attacks on which VLAN security could be compromised.

VLAN is a group of Computers and Devices on different Local Area Networks that have the ability to communicate with each other in one network or with devices on other networks as if they were all on the same physical LAN. It manages and configured through software. Due to many Exploit techniques used by attackers now the day, our systems that operate in VLAN at risk. So if the attacker finds out the Vulnerability state of our system then our networks may suffer different exposures. So, must have to implement, ent different Security Postures in our Virtual Local Area Networks in order to protect our networks from loss of data and information. This paper will focus on techniques that can be used to increase the security of VLAN as well as it will also discuss the future of VLAN. Firstly, we will discuss different security techniques and in the end, present why these techniques are important for the future of VLAN. The Future of Virtual Local Area Network (VLAN) is wide open to companies which operate on a wide scale to small Companies. The VLAN will help reduction of traffic, increase security, cost-effective (travelling expenses while communicating another department in different cities) and make it easier for the IT department to manage better security and Management in the organization. Many companies have Installed VLAN into their networks [3].

This cost-effective solution offers a way to secure communicates with decreasing the surplus on the network. Companies cost decreased due to VLAN because now their employee doesn't have to travel to other cities which have different departments. They form a network and communicate with the rest of the departments using VLAN. The future of VLAN will grow bright, as nowadays companies are focusing on cost-effective ways and forming a VLAN is in the best interest of companies. Of course, there will be some initial cost establishing VLAN but it is in the best interest of Companies future. The MAC-based protocol will be going to implement on a wider scale because it tends to be

more protected and secure of sharing different resources on different virtual local Area networks. We will see different styles of VLAN in future due to the fastest innovations of new hardware, software, technologies [3].

Patients face the possibility of copying and keeping their electronic health records (EHRs) through portable storage media, they will encounter new risks to the protection of their private information. In this study, we propose a method to preserve the privacy and security of patients' portable medical records in portable storage media to avoid any inappropriate or unintentional disclosure. Following HIPAA guidelines, the method is designed to protect, recover and verify patient's identifiers in portable EHRs. The results of this study show that our methods are effective in ensuring both information security and privacy preservation for patients through portable storage medium [3].

Hierarchical Network Design for campus network is an enterprise network consisting of many LANs in one or more buildings, all connected and all usually in the same geographic area. A company typically owns the entire campus network and the physical wiring. Campus networks commonly consist of wired Ethernet LANs and shared wireless LANs. An understanding of traffic flow is a vital part of the campus network design. You might be able to leverage high-speed LAN technologies and “throw bandwidth” at a network to improve traffic movement. However, the emphasis should be on providing an overall design that is tuned to known, studied, or predicted traffic flows. The network traffic can then be effectively moved and managed, and you can scale the campus network to support future needs [7]. As a starting point, consider the simple network shown in Figure 2.1 A collection of PCs, printers, and servers are all connected to the same network segment and use the 192.168.1.0 subnet. All devices on this network segment must share the available bandwidth.

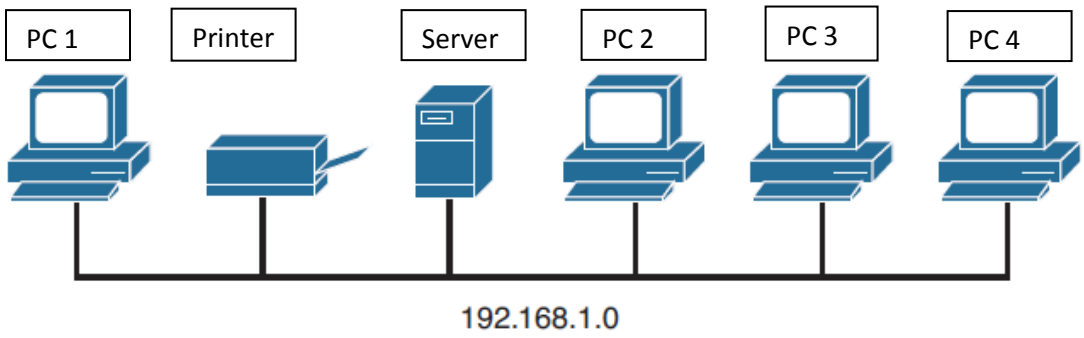

Figure 2.1: Simple Shared Ethernet Network [4]

Recall that if two or more hosts try to transmit at the same time on a shared network, their frames will collide and interfere. When collisions occur, all hosts must become silent and wait to retransmit their data. The boundary around such a shared network is called a collision domain.

In Figure 2.1, the entire shared segment represents one collision domain. A network segment with six hosts might not seem crowded. Suppose the segment contains hundreds of hosts instead. Now the network might not perform very well if many of the hosts are competing to use the shared media. Through network segmentation, to reduce the number of stations on a segment. This, in turn, reduces the size of the collision domain and lowers the probability of collisions because fewer stations will try to transmit at a given time. Broadcast traffic can also present a performance problem on a Layer 2 network because all broadcast frames flood to reach all hosts on a network segment. If the segment is large, the broadcast traffic can grow in proportion and monopolize the available bandwidth [4].

In addition, all hosts on the segment must listen to and process every broadcast frame. To contain broadcast traffic, the idea is to provide a barrier at the edge of a LAN segment so that broadcasts cannot pass or be forwarded outward. The extent of a Layer 2 network, where a broadcast frame can reach, is known as a broadcast domain. To limit the size of a collision domain, you can connect smaller numbers of hosts to individual switch interfaces. Ideally, each host should connect to a dedicated switch interface so that they can operate in full-duplex mode, preventing collisions altogether. Switch interfaces do not propagate collisions, so each interface becomes its own collision domain even if several interfaces belong to a common VLAN. In contrast, when broadcast traffic is

forwarded, it is flooded across switch interface boundaries. In fact, broadcast frames will reach every switch interface in a VLAN. In other words, a VLAN defines the extent of a broadcast domain. To reduce the size of a broadcast domain, you can segment a network or break it up into smaller Layer 2 VLANs. The smaller VLANs must be connected by a Layer 3 device, such as a router or a multilayer switch, as shown in Figure 2.1.

The simple network of Figure 2.1 now has two segments or VLANs interconnected by Switch A, a multilayer switch. A Layer 3 device cannot propagate a collision condition from one segment to another, and it will not forward broadcasts between segments [5].

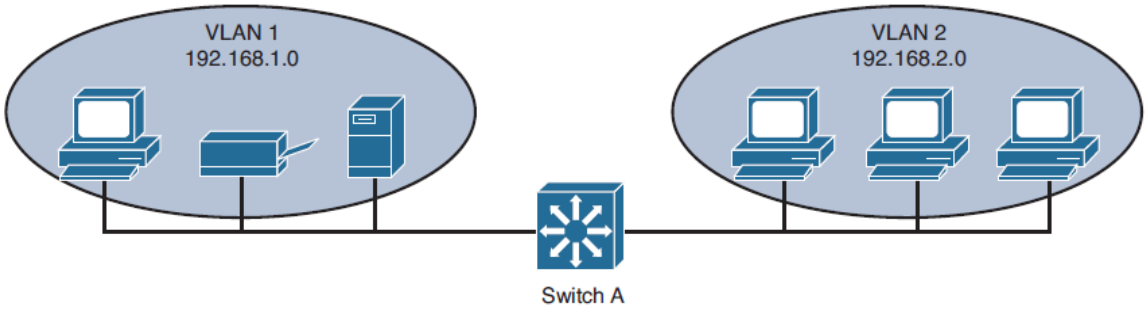

Figure 2.2: Example of Network Segmentation [5]

The network might continue to grow as more users and devices are added to it. Switch A has a limited number of ports, so it cannot directly connect to every device. Instead, the network segments can be grown by adding a new switch to each, as shown in Figure 2.3 [5].

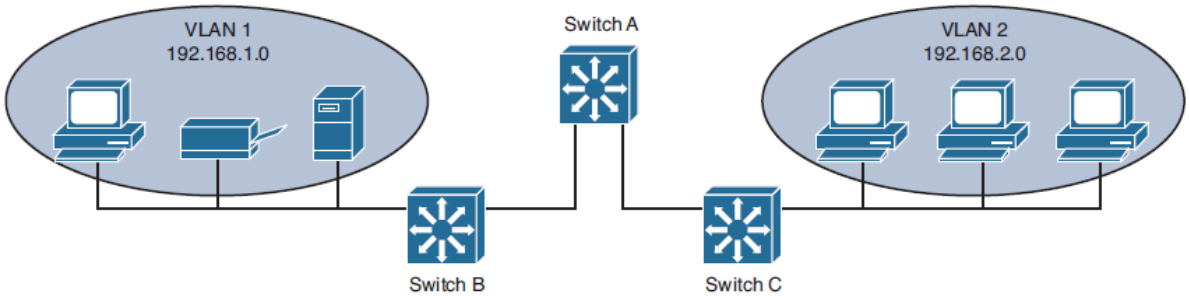

Figure 2.3: Expanding a Segmented Network [5]

Switch B aggregates traffic to and from VLAN 1, while Switch C aggregates VLAN 2. As the network continues to grow, more VLANs can be added to support additional applications or user communities. As an example, Figure 2.4 shows how Voice over IP

(VoIP) has been implemented by placing IP phones into two new VLANs (10 and 20). The same two aggregating switches can easily support the new VLANs [6].

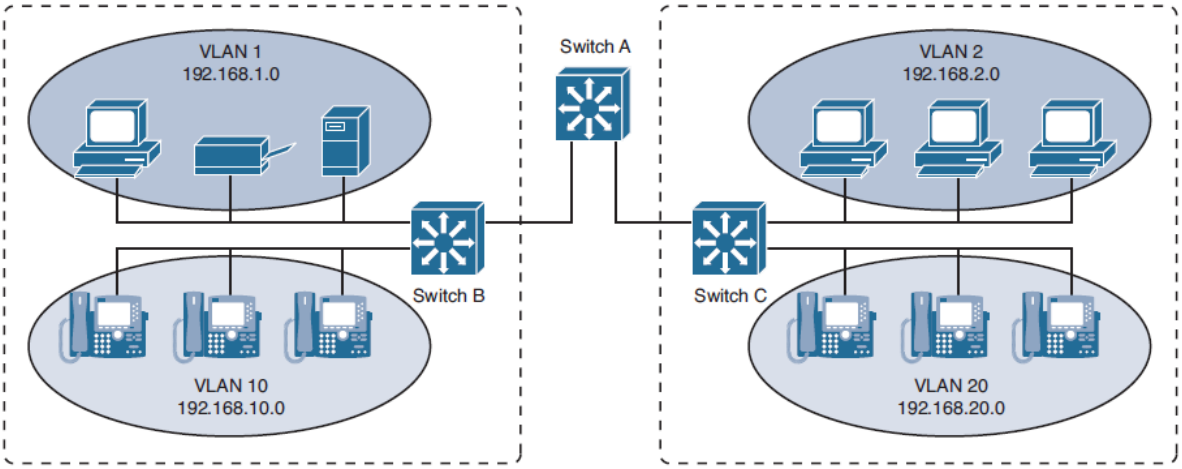

Figure 2.4: Network Growth through New VLANs [6]

2.4 Network Simulator

Network simulators can be categorized based on their futures and functionality, to very simple or complex, commercial or open source simulators. A simple simulator can imitate a small network topology by specifying the nodes, data links between those nodes and network traffic but a complex one possibly emulates many different types of network devices and communication protocols to handle network traffic. They are designed to model massive network performance with a variety of vendor's equipment to provide a facility for designing and optimization of large and complex networks.

Moreover, a powerful network simulator enhances the capability of network performance optimization. Graphical network simulators enable users to simply visualize the operation of their emulated computer network and serve them possible customization options.

The value of a simulator based on emulation of router hardware enabling the use of actual router software cannot be underestimated. Furthermore, emulation enables router virtualization such that multiple virtual machines can be implemented on a single host. The benefits of virtualization in server farms and for users desiring to run multiple operating systems on their computers are resulting in the growth of virtualization applications such as various kinds of simulators, Virtual Box and VMware [6].

2.5 Predictable Network Model

Ideally, to design a network with predictable behaviour in mind to offer low maintenance and high availability. For example, a campus network needs to recover from failures and topology changes quickly and in a predetermined manner. You should scale the network to easily support future expansions and upgrades. With a wide variety of multiprotocol and multicast traffic, the network should be capable of efficiently connecting users with the resources they need, regardless of location.

In other words, design the network around traffic flows rather than a particular type of traffic. Ideally, all end users are located at a consistent distance from the resources they need to use. If one user at one corner of the network passes through two switches to reach an email server, any other user at any other location in the network should also require two switch hops for email service.

Cisco has refined a hierarchical approach to network design that enables network designers to organize the network into distinct layers of devices. The resulting network is efficient, intelligent, scalable, and easily managed. Figure 2.4 can be redrawn to emphasize the hierarchy that is emerging. In Figure 2.5, two layers become apparent: the access layer, where switches are placed closest to the end users; and the distribution layer, where access layer switches are aggregated [7].

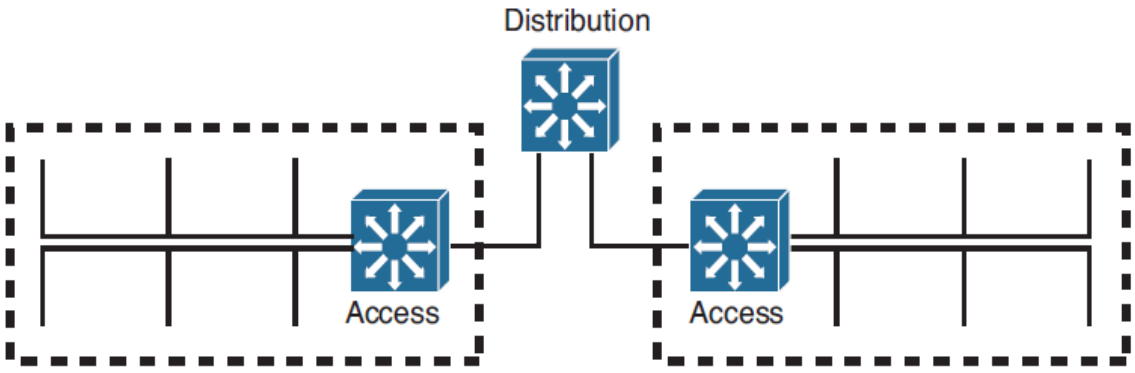

Figure 2.5: Two-Layer Network Hierarchy Emerges [7]

As the network continues to grow with more buildings, more floors, and larger groups of users, the number of access switches increases. As a result, the number of distribution switches increases. Now things have scaled to the point where the distribution switches need to be aggregated. This is done by adding a third layer to the hierarchy, the core layer, as shown in Figure 2.6.

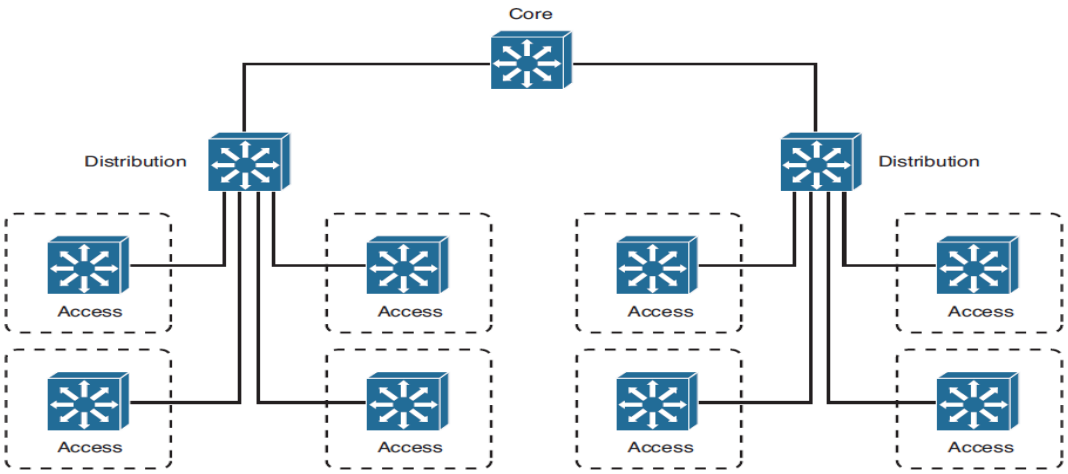

Figure 2.6: Core Layer Emerges [7]

Traffic flows in a campus network can be classified as three types, based on where the network service or resource is located in relation to the end user. Figure 2.7 illustrates the flow types between a PC and some file servers, along with three different paths the traffic might take through the three layers of a network. Table 2.1 also lists the types and the extent of the campus network that is crossed going from any user to the service.

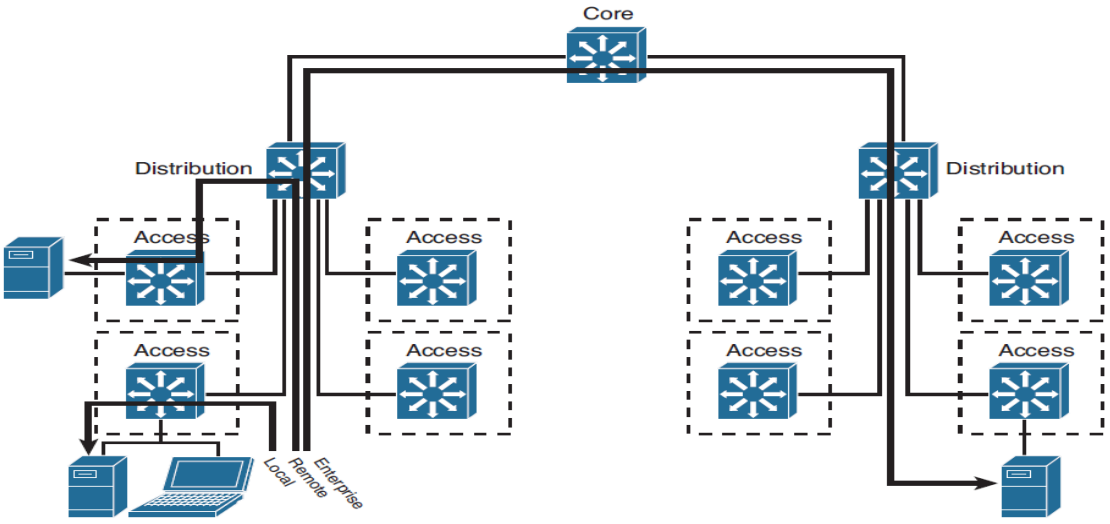

Figure 2.7: Traffic Flow Paths through a Network Hierarchy [7]

Service Type	Location of Service	Extent of Traffic Flow
Local	Same segment/VLAN as user	Access layer only
Remote	Different segment/VLAN as user	Access to distribution layers
Enterprise	Central to all campus users	Access to distribution to core layers

Table 2.1: Types of Network Services [8]

Regardless of where the user is located, the traffic path always begins at the access layer and progresses into the distribution and perhaps into the core layers. Even a path between two users at opposite ends of the network becomes consistent and predictable.

Each layer has attributes that provide both physical and logical network functions at the appropriate point in the campus network. Understanding each layer and its functions or limitations is important to properly apply the layer in the design process [8].

2.5.1 Access Layer

The access layer exists where the end users are connected to the network. Access switches usually provide Layer 2 (VLAN) connectivity between users. Devices in this layer, sometimes called building access switches, should have the following capabilities:

- Low cost per switch port
- High port density
- Scalable uplinks to higher layers
- High availability
- Ability to converge network services (that is, data, voice, video)
- Security features and Quality of Service (QoS)

2.5.2 Distribution Layer

The distribution layer provides interconnection between the campus network's access and core layers. Devices in this layer, sometimes called building distribution switches, should have the following capabilities:

- Aggregation of multiple access layer switches
- High Layer 3 routing throughput for packet handling
- Security and policy-based connectivity functions
- QoS features
- Scalable and redundant high-speed links to the core and access layers

In the distribution layer, uplinks from all access layer devices are aggregated, or come together. The distribution layer switches must be capable of processing the total volume of traffic from all the connected devices. These switches should have a high port density of high-speed links to support the collection of access layer switches. VLANs and broadcast domains converge at the distribution layer, requiring routing, filtering, and security. The switches at this layer also must be capable of routing packets with high throughput. Notice that the distribution layer usually is a Layer 3 boundary, where routing meets the VLANs of the access layer. Core Layer A campus network's core layer provides connectivity between all distribution layer devices [9].

2.5.3 The Core Layer

sometimes referred to as the backbone, must be capable of switching traffic as efficiently as possible. Core switches should have the following attributes:

- Very high Layer 3 routing throughput
- No costly or unnecessary packet manipulations (access lists, packet filtering)
- Redundancy and resilience for high availability
- Advanced QoS functions

Devices in a campus network's core layer or backbone should be optimized for high-performance switching. Because the core layer must handle large amounts of campus-wide data, the core layer should be designed with simplicity and efficiency in mind.

Although campus network design is presented as a three-layer approach (access, distribution, and core layers) the hierarchy can be collapsed or simplified in certain cases.

For example, small or medium-size campus networks might not have the size or volume requirements that would require the functions of all three layers. In that case, you could combine the distribution and core layers for simplicity and cost savings [9].

Virtual LAN A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible. VLANs define broadcast domains in a Layer 2 network. A broadcast domain is the set of all devices that will receive broadcast frames originating from any device within the set.

Broadcast domains are typically bounded by routers because routers do not forward broadcast frames. Layer 2 switches create broadcast domains based on the configuration of the switch. Switches are multiport bridges that allow you to create multiple broadcast domains. Each broadcast domain is like a distinct virtual bridge within a switch. You can define one or many virtual bridges within a switch. Each virtual bridge you create in the switch defines a new broadcast domain (VLAN). Traffic cannot pass directly to another VLAN (between broadcast domains) within the switch or between two switches. To interconnect two different VLANs, you must use routers or Layer 3 switches [9].

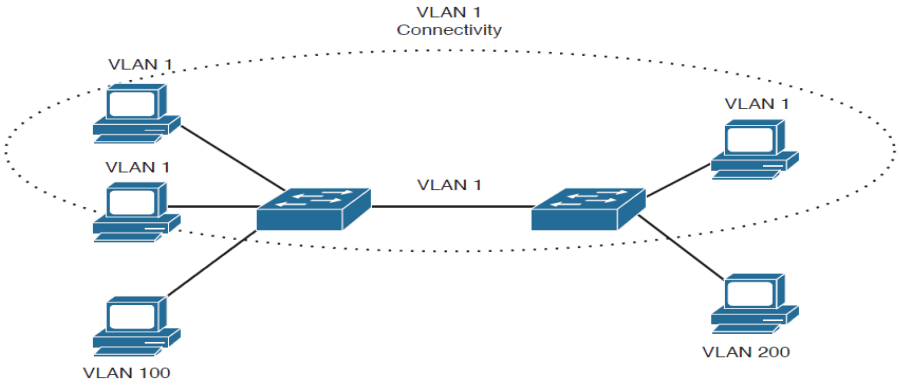

Figure 2.8: VLAN connectivity [10]

Securing VLANs traditionally, traffic has been filtered only at router boundaries, where packets naturally are inspected before being forwarded. This is true within Catalyst switches because access lists can be applied as a part of multilayer switching. Catalysts

also can filter packets even if they stay within the same VLAN; VLAN access control lists, or VACLs, provide this capability.

Catalyst switches also have the capability to logically divide a single VLAN into multiple partitions. Each partition can be isolated from others, with all of them sharing a common IP subnet and a common gateway address. Private VLANs make it possible to offer up a single VLAN to many disparate customers or organizations without any interaction between them. VLAN trunks are commonly used on links between switches to carry data from multiple VLANs. If the switches are all under the same administrative control, it is easy to become complacent about the security of the trunks. A few known attacks can be used to gain access to the VLANs that are carried over trunk links. Therefore, network administrators should be aware of the steps that can be taken to prevent any attacks [10].

Private VLANs Normally, traffic is allowed to move unrestricted within a VLAN. Packets sent from one host to another normally are heard only by the destination host because of the nature of Layer 2 switching.

However, one host broadcasts a packet, all hosts on the VLAN must listen. You can use a VACL to filter packets between a source and destination in a VLAN if both connect to the local switch. Sometimes it would be nice to have the capability to segment traffic within a single VLAN, without having to use multiple VLANs and a router. For example, in a single VLAN server farm, all servers should be capable of communicating with the router or gateway, but the servers should not have to listen to each other's broadcast traffic.

Taking this a step further, suppose that each server belongs to a separate organization. Now each server should be isolated from the others but still be capable of reaching the gateway to find clients, not on the local network. Another application is a service provider network. Here, the provider might want to use a single VLAN to connect to several customer networks. Each customer needs to be able to contact the provider's gateway on the VLAN. Clearly, the customer sites do not need to interact with each other [11].

Private VLANs (PVLANs) solve this problem on Catalyst switches. In a nutshell, a normal, or primary, VLAN can be logically associated with special unidirectional, or secondary, VLANs. Hosts associated with a secondary VLAN can communicate with

ports on the primary VLAN (a router, for example), but not with another secondary VLAN. A secondary VLAN is configured as one of the following types:

- Isolated: Any switch ports associated with an isolated VLAN can reach the primary VLAN but not any other secondary VLAN. In addition, hosts associated with the same isolated VLAN cannot reach each other. They are, in effect, isolated from everything except the primary VLAN.
- Community: Any switch ports associated with a common community VLAN can communicate with each other and with the primary VLAN but not with any other secondary VLAN. This provides the basis for server farms and workgroups within an organization while giving isolation between organizations.

All secondary VLANs must be associated with one primary VLAN to set up the unidirectional relationship. Private VLANs are configured using special cases of regular VLANs. However, the VLAN Trunking Protocol (VTP) does not pass any information about the private VLAN configuration. Therefore, private VLANs are only locally significant to a switch. Each of the private VLANs must be configured locally on each switch that interconnects them.

You must configure each physical switch port that uses a private VLAN with a VLAN association. You also must define the port with one of the following modes:

- Promiscuous: The switch port connects to a router, firewall, or another common gateway device.

This port can communicate with anything else connected to the primary or any secondary VLAN. In other words, the port is in promiscuous mode, in which the rules of private VLANs are ignored.

- Host: The switch port connects to a regular host that resides on an isolated or community VLAN.

The port communicates only with a promiscuous port or ports on the same community VLAN.

Figure 2.8 shows the basic private VLAN operation. Some host PCs connect to a secondary community VLAN. The two community VLANs associated with a primary

VLAN, where the router connects. The router connects to a promiscuous port on the primary VLAN.

A single host PC connects to a secondary isolated VLAN, so it can communicate only with the router's promiscuous port [11].

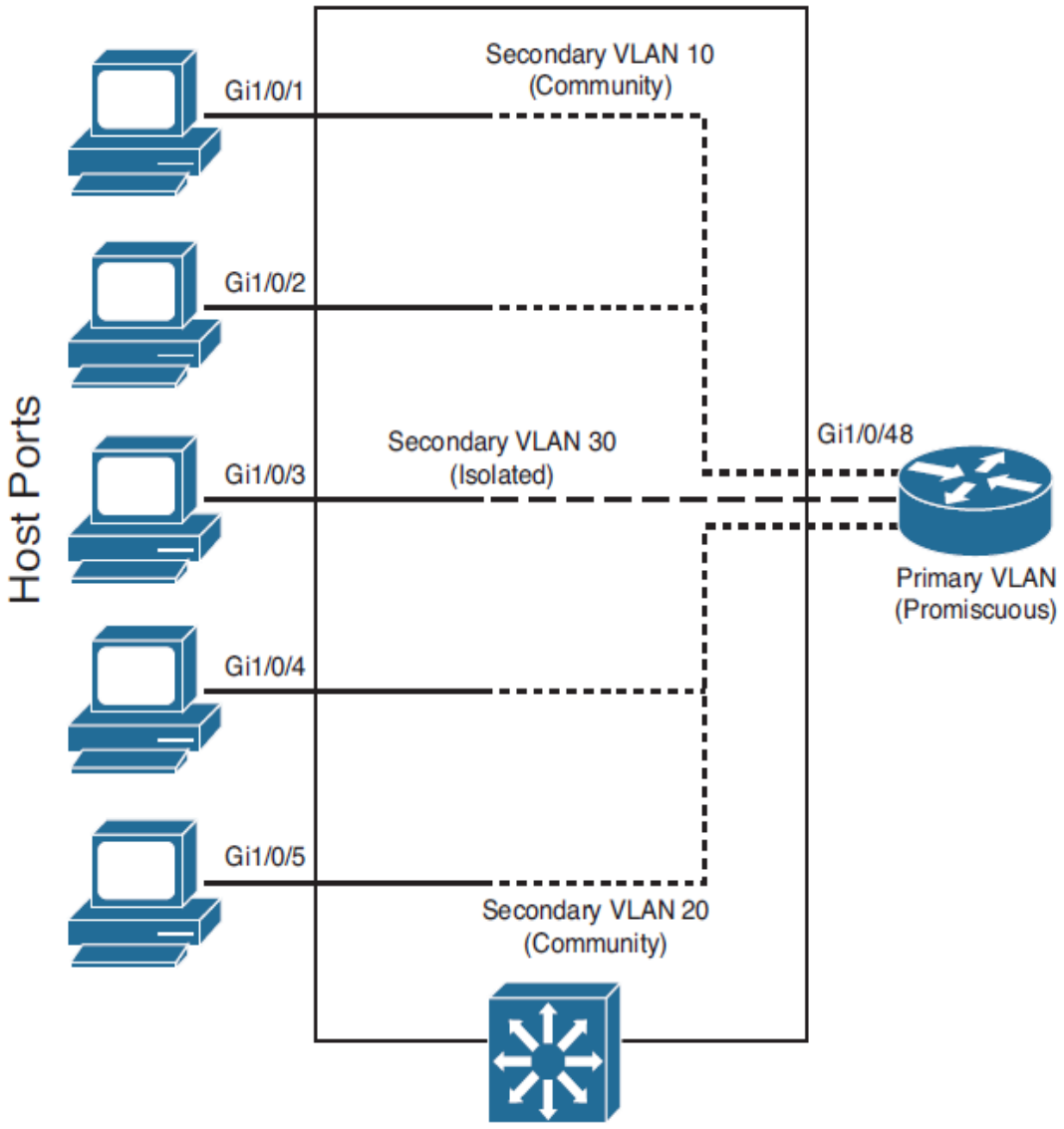

Figure 2.9: Private VLAN Functionality within a Switch [12]

2.6 VLAN Access Lists

Access lists can manage or control traffic as it passes through a switch. When normal access lists are configured on a Catalyst switch, they filter traffic through the use of the

Ternary Content Addressable memory (TCAM). “Switch Operation,” that access lists (also known as Router Access Lists, or RACLs) are merged or compiled into the TCAM. Each ACL is applied to an interface according to the direction of traffic inbound or outbound. Packets then can be filtered in hardware with no switching performance penalty. However, only packets that pass between VLANs can be filtered this way.

Packets that stay in the same VLAN do not cross a VLAN or interface boundary and do not necessarily have a direction in relation to an interface. These packets also might be non-IP or completely bridged; therefore, they never pass through the multilayer switching mechanism [12].

VLAN access lists (VACLs) are filters that directly can affect how packets are handled within a VLAN. VACLs are somewhat different from RACLs or traditional access control lists. Although they, too, are merged into the TCAM, they can permit, deny, or redirect packets as they are matched. VACLs also are configured in a route map fashion, with a series of matching conditions and actions to take.

Firewall a firewall is a system for network protection which in turn monitors and controls incoming and outgoing network traffic and is always based on the security rules specified by the network administrator. Forensic Network is a technology according to which the traffic is determined and analysis of each capture located in the package as it is also investigating and tracking attacks. This is done by collecting data and information from firewalls and intrusion detection systems, which are used to prevent malicious sites and thus, report the attack and save the system from the attackers [13].

Firewall policy, firewalls activate is controlled by the “Policy”. The policy consists of “Rules” (in context of packet routing they also often referred as “filters”). Each rule consists of a condition and action. Condition describes the criteria used to match individual packets. Action describes the activity to be performed if matches have been made. Basic conditions consist of tests, matching individual fields of the packet such as source address, destination address, packet type, etc. In the case of stateful inspection (e.g. via IP con-track module in IP tables), connection-related variables like connection state (“established”, “related”, “new”) could be checked. Finally, various system state variables like current time of day, CPU load, or system-wide configuration parameters

could be taken into account. The condition could be viewed as a predicate. Usually, for a packet to match a condition, all tests must be satisfied (logical conjunction) [13].

Security Policy The main problem with information security in healthcare is not technology, but a lack of cohesive security policy. The policy must shape technology, not vice versa. The security policy defines what is to be protected, to what reasonable degree protections will be afforded, and who is privileged to access protected items. A policy is influenced by:

- The functional requirements of an information system (what users need to accomplish from the system)
- The security requirements for the system (items that need to be protected),
- A threat model (the expected motives and resources of potential perpetrators)

The role of policy is to balance the functional and security requirements of a system, which are typically at odds. Security requirements can often be tempered by the practical concerns of a threat model because costs and user inconveniences rise sharply with harsher security implementations. "Inside attacks," the most routine kinds of security transgressions, represent one example of a threat concern. Such attacks are committed by persons who are legitimate system users with privileges but who abuse their privileges in search of gossip material, or for other personal or financial motivations.

The monetary value of health data obtainable on most individuals, however, is relatively low (unlike some financial data or military secrets), so it is reasonably safe to assume that an attacker will not spend inordinate resources (money and time) on attempting to acquire such data by computer break-m or cryptanalytic attack. Specifically, desired information, as always, might be available with less trouble and expense via "social engineering" techniques (bribery, extortion, personal misrepresentation of identity, and so forth). The health data of celebrities and other prominent persons may be of greater monetary value in certain markets, but currently available (although not necessarily implemented) security mechanisms, such as system management, access control, and encryption techniques, are sufficient to thwart or detect the covert activities of hospital employees, newspaper reporters, relatives, and other unsophisticated attackers [14].

Another example of potential threats comes from information-hungry employers, insurance companies, and managed care organizations. These organizations have greater

economic resources, along with the motivation of significant profit from what they can know about individuals.

Unethical operations in such industries could allocate a high-end computer to the task of breaking a cryptographic key used in the transmission of health data over inexpensive public channels. The 1995 cost of a machine capable of breaking a Data Encryption Standard of the U.S. government (DES) key within 1 year (with an 8% chance per month) is only $64,000.35P rofit-motivated healthcare-related organizations and unethical "private investigators" might be willing to make this investment and, for example, gather HIV data, which could be used on a covert basis to deny medical insurance coverage [15].

The above threats concern attacks on patient privacy, but threat models should also consider attacks on the integrity and availability of health data. Such threats might come from malevolent "hackers," natural disasters, or mechanical failures and could potentially cost data guardians more than any breach of confidentiality.

The Data Security Policy and Standards developed for the Mayo Clinic/Foundation provide one model example of a clear institutional security policy statement.

27 As an example of an approach to policy setting, Columbia Presbyterian Medical Center (CPMC) hired external consultants to facilitate security policy development for its Integrated Advanced Information Management System project.6 After 24 meetings with 80 people from numerous departments that spanned two institutions, 14 overlapping topic areas for which policy development was needed were identified:

- User authentication-issues relating to the identification of a user to the system and the ways in which the system might know that a user is who they claim to be.
- Physical security of data center sites-issues relating to the physical access to computer hardware; theft prevention; backup and disaster recovery; and the security of sensitive terminal locations, such as console or control, and of publicly accessible terminals.
- Access control to system resources-issues of the physical devices and logical mechanisms, such as computer programs, that control access to system resources.

- Data ownership- issues of whom own which data, the delegation of authority over data, and enunciation of the duties and responsibilities of data ownership.
- Data protection policies-issues of minimally acceptable and consistent protections to be afforded by systems crossing organizational and functional boundaries, anticipated implementation barriers to those protections, and the punitive measures for organizational members abusing system privileges.
- Building security into systems-issues of how to assure that security requirements are addressed in central and local participating systems, how to partition security responsibilities between central and local systems, and how to assure that security requirements remain satisfied as systems are modified or expanded.
- Security of hard copy materials-issues of how to prevent security breaches from paper copies of sensitive electronic documents and data.
- Systems integrity-issues related to the accuracy and reliability of system data, and the integrity and reliability of physical computer and network systems [15].

2.7 Hierarchical Model

The so-called 'hierarchical' model is to divide the complex network design into several levels, each of which focuses on certain specific functions, which can make a complex big problem into many simple small problems. Hierarchical model can be applied to both LAN design and WAN design.

In order to understand the importance of hierarchical design more clearly, it is best to understand the OSI (Open Systems Interconnection) reference, model. The OSI model simplifies the communication requirements between computers. Similarly, the use of a hierarchical model to design a network can simplify the requirements of networking [16].

2.7.1 Hierarchical Network Design:

Easy Savings

In the use of the hierarchical model, the various levels of their duties, no longer in the same platform to consider all the things. Hierarchical model the modular nature of the network to make every layer can make good use of bandwidth, reducing the waste of system resources.

Easy to Understand

The hierarchical design makes the network structure clear, can be implemented at different levels of different difficulty management, reducing management costs.

Easy to Expand

In the network design, modularity has the characteristics of network growth so that the complexity of the network can be limited to the subnet, and will not spread to other parts of the network. And if the use of flat and mesh design, any node changes will have a great impact on the entire network.

Easy to Troubleshoot

Hierarchical design can break down the network topology into easy-to-understand subnets, and network managers can easily determine the range of network failures, simplifying the troubleshooting process [16].

2.8 Summary

In this chapter present an overview electronic medical record, describes VLANs, what they are, why they were developed, and how they behave. It focuses on the general principles of VLANs, instead of describing any particular switch implementation. In addition to predictable model layers' access, distribution and core layer That includes a brief description of layers. by default, to design a network with a predictable behaviour in mind to offer low maintenance and high availability predictable model is a need. The application of VLAN technology with the creation of a large network model has been clarified the network simulator and its types this chapter presents an overview of a network simulator.

CHAPTER THREE

Methodology

3.1 Introduction

This chapter provides a full description of the complex and abstract theory of VLAN configuration can be clarified by doing some laboratories in test beds. However, it is not always possible to set up an entire test bed containing multiple computers, switches and routers to strengthen student skills for time and cost reasons. Using GUI-based applications is an alternative way to improve the understanding of the complex VLAN configuration involved in routing protocols and layer3 switches because graphics, images, diagrams and animations can be easily transformed into knowledge. With a visual didactic approach, students can understand how VLANs and routing protocols really work in a more intuitive and friendly way than using traditional approaches. In this research, we focused on the learning of VLANs, an advanced routing protocol developed by Cisco Systems, using visual educational tools. Present well-known computational tools (Packet Tracer, GNS3) [17].

3.2 Research Flow Diagram

After reviewing the previous studies, the data were collected through the questionnaire and converted to the simulation model and then compared with the proposed model, if the researcher of the required content to transfer the results and recommendations showing in Figure 3.1.

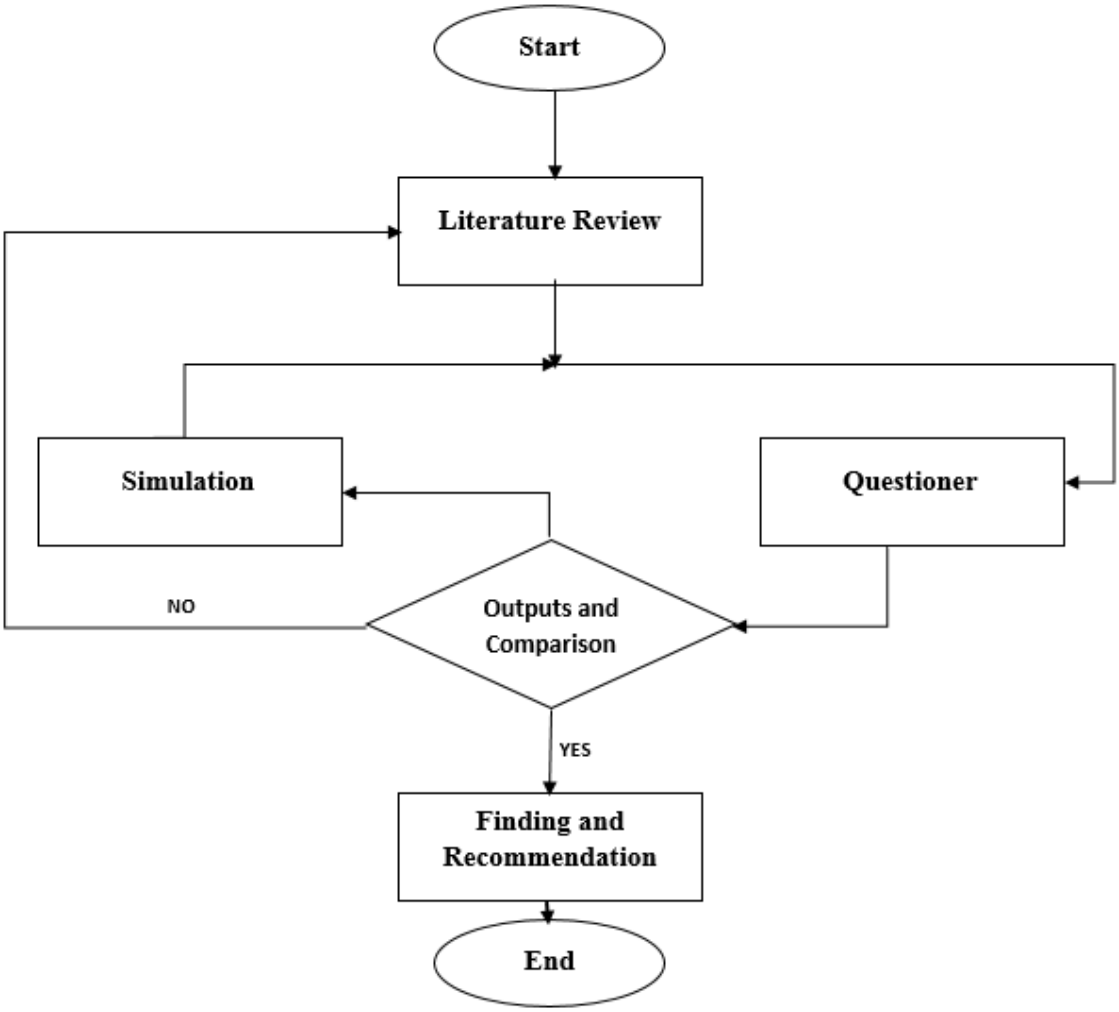

Figure 3.1: Research Flow Diagram

3.3 Gather Requirements

Define the requirements required for a research study.

3.3.1 Packet Tracer

Cisco Packet Tracer provides multiple opportunities for instructors to demonstrate networking concepts. Although Packet Tracer is not a substitute for real equipment, it allows students to practice using a command-line interface. This “re-doing” capability is a fundamental component of learning how to configure routers and switches.

Packet Tracer’s simulation mode enables instructors to demonstrate processes that were formerly hidden to students.

These simulation capabilities can help simplify the learning process by providing tables, diagrams, and other visual representations of internal functions such as dynamic data transfers and packet content expansion. The simulation model also decreases instructor presentation time by replacing whiteboards and static slides with real-time visuals. Packet Tracer helps instructors teach complex networking concepts[10]. With Packet Tracer, students can easily build their network topologies in a visual way by dragging, placing, connecting, and clustering virtual network devices such as hubs, switches, routers, workstations and servers.

Once placed in the workspace, students can customize their virtual networking devices. For example, they are allowed to add additional cards (e.g. WIC-2T, NM-1FE-TX, etc.) to modular routers such as a Cisco 2811. If a router does not allow users to add or remove extension cards while it is powered on, Packet Tracer will force the students to power off the router before performing the change, just to remind them that they can damage the router if they do not follow a strict procedure. To connect virtual networking devices, Packet Tracer offers a wide variety of connections, such as straight-through and cross-over UTP cables. If students do not use the correct connection, the experiment will not work properly and troubleshooting will be necessary. Network devices (switches or routers) can be configured by students just by double-clicking their icon and entering the commands (in the same way they will enter them in real devices) in the CLI tab of the window that will appear.

At the moment of the writing of this research, the last version of Packet Tracer supports RIP, OSPF, EIGRP and BGP. Not all the EIGRP commands are implemented in this version, but most of the usual ones are. For example, users can verify which interfaces of a router are running EIGRP (show IP EIGRP interfaces), or can see the important tables maintained by the protocol such as the neighbor table (show IP EIGRP neighbors), the topology table (show IP EIGRP topology), and the complete topology table (show IP EIGRP topology all-links). Packet Tracer also supports the customization of the K-values (metric weights 0 K1 K2 K3 K4 K5) of the metric [18].

3.3.2 Graphical Network Simulator 3

GNS3 is a very powerful graphical simulator and easy to use. It helps us to create a heterogeneous and quiet complex network, as close as a real network without any expense, GNS3 (Graphical Network Simulator 3), is an open-source graphical network simulator. However, the users have to supply a real router Internetwork Operating System (IOS) image, which means that it has to be gained directly through Cisco or from an actual router, GNS3 is a virtualization platform consisting of three software programs that run on common PC hardware and could be installed on Microsoft Windows, Linux and MAC operating systems. In order to accomplish faultless and complete network emulation.

Network virtualization refers to the process of simulating network infrastructure and their functionality into a single, logical software-based administrative entity, a "Virtual Network". Virtualized network can be set up either by using virtual devices (such as a virtual machine inside a hypervisor) or creating protocol-based virtual networks (such as VLANs, VPNs and etc.) Network simulators can be categorized based on their futures and functionality, to very simple or complex, commercial or open source simulators. A simple simulator can imitate a small network topology by specifying the nodes, data links between those nodes and network traffic but a complex one possibly emulates many different types of network devices and communication protocols to handle network traffic. They are designed to model massive network performance with a variety of vendor's equipment to provide a facility for designing and optimization of large and complex networks. Moreover, a powerful network simulator enhances the capability of network performance optimization. Graphical network simulators enable users to simply visualize the operation of their emulated computer network and serve them possible customization options.

The value of a simulator based on emulation of router hardware enabling the use of actual router software cannot be underestimated. Furthermore, emulation enables router virtualization such that multiple virtual machines can be implemented on a single host. The benefits of virtualization in server farms and for users desiring to run multiple

operating systems on their computers are resulting in the growth of virtualization applications such as various kinds of simulators, Virtual Box and VMware [19].

3.4 Equipment Selection

To select and define campus network devices.

3.4.1 Switches

The campus network uses Gigabit Ethernet switching network. Configure a central switch and seven secondary switches. Each switch supports Gigabit Ethernet expansion ports with expansion module slots. Campus network backbone for the Gigabit network, Fast exchange to the desktop, to protect all users at the same time call the service resources can be fast and smooth, give full play to the role of patients record; at the same time to ensure that all users at the same time smooth Internet, the campus network function most vividly. The Catalyst 2948G-L3 switch is a three-tier L3 Ethernet switch that provides wire-speed switching for IP protocols, Internet packet-switched protocols, IPX, and IP multicast. This new Catalyst switch provides the required high performance for a medium-sized park backbone with the appropriate port density [20].

3.4.2 Router

Routers are devices on the interconnected networks that forward packets between networks based on Layer 3 addresses. Routers are able to choose the best path in the network for data transmission. Operating at the Layer 3 of the OSI model, the router can make decisions based on network addresses instead of using individual second-layer MAC addresses. Routers are also able to interconnect networks with various second-layer technologies, such as Ethernet, Token Ring and Fiber Distributed Data Interface (FDDI). Typically, routers also connect networks that use asynchronous transfer mode (ATM) and serial connections.

Due to its ability to forward packets based on information of the third layer, routers have become the main backbone of the global Internet and use them

IP protocol [20].

3.4.3 Firewall

The firewall as a term originates from a fireproof wall made of stone or metal that stopped the fire flames to spread across the area. Later, the term was adopted to represent a metal sheet between the vehicle's engine compartment and the passenger compartment. Eventually, the term firewall became widely used in the computer network's terminology: like a wall, it prevents harmful and undesirable traffic to pass into the secured network.

A firewall is a single or a group of systems that enforces an access control policy between networks. Firewalls can be as a standalone hardware, embedded in the network devices or be a software on the host computers [21].

3.5 Campus Network Structure

The construction of the campus network will design based on the actual situation and characteristics of the hospital. Design of very complex and high quality network topology, Emulation of several Cisco routers, platforms and firewalls using GNS3 and packet tracer, Simulation of a common network, switches such as Ethernet and Multilayer switches.

The hospital network needs to complete, including the health record information, hospital administrative office and other integrated business information management system for the majority of doctors, patients and other hospital staff to provide a network environment for providing treatment and research work of the advanced platform. The campus network covers the entire campus, and the network design follows the following five basic principles:

Reliability and high-performance networks must be reliable, including network-level reliability such as routing, switching aggregation, link redundancy, and load balancing. The network must be of sufficient performance to meet the needs of the business.

Scalability and scalability of the system to be scalable and scalable, with the business growth and application level, the network of data and information flow will grow exponentially, the need for good network scalability, and can continue to upgrade with the development of technology. Equipment should be used in line with international standards of systems and products to ensure that the system has a long vitality and scalability to meet future requirements of the system upgrade.

Easy to manage, easy maintenance as the campus backbone network system is a large, rich and complex application, the need for network management system has good manageability, network management system with monitoring, fault diagnosis, fault isolation, filtering settings and other functions to facilitate the management of the system and maintain.

To choose a high degree of integration, the module can be a common product for easy management and maintenance. Here we use the equipment is Cisco switches, firewalls.

Security, confidentiality of the network system should have good security. As the campus backbone network for multiple user intranet to provide interconnection and support a variety of business, requiring flexible and effective security control, but also should support the virtual private network to provide multi-level security options. In the system design, not only consider the full sharing of information resources but also pay attention to the protection and isolation of information, so the system should be different for different applications and different network communication environment, take different measures, including system security mechanisms, data access the authority of the control. In this campus network erection, it will be through subnet and the switch of VLAN to achieve network security.

Through the use of structured, modular design forms with flexibility and comprehensive, to meet the system and difference needs from users to adapt to changing requirements. To meet the system goals and functions as the goal, to ensure that the overall program design is reasonable to meet the needs of users while maintaining the use of the system maintenance, as well as the future system of secondary development and transplantation [12].

3.6 Summary

In this chapter provide a full description of the research methodology. And the techniques have been applied in the research by gathering requirements and give a full description of the campus network structure and hieratical design. In this section explain equipment selection by gives an overview of the devices that are used to build modern networks. At this moment the most popular are switches, routers and firewalls.

CHAPTER FOUR

Finding and Discussion

4.1 Introduction

Network architecture and its security are important any organization. If we follow the hierarchical network design, the network will be scalable, performance and security will be increased, and the network will be easy to maintain. In this work, we proposed a compact cost-effective secure campus network design based on the work environment and required scalability, security and other aspects. Depending on the data and requirements collected from different cases and organizations to analyze until there are results that help in the development of protected areas, especially in the field of medical records.

It's easy to see why virtual LANs have become extremely popular on networks of all sizes. In practical terms, multiple VLANs are pretty much the same as having multiple separate physical networks within a single organization without the headache of managing multiple cable plants and switches. Because VLANs segment a network, creating multiple broadcast domains, they effectively allow traffic from the broadcast domains to remain isolated while increasing the network's bandwidth, availability and security.

4.2 Performance Analysis

This research will simulate network architecture in a packet tracer (Show in figures 4.1 to 4.20) simulation to compare and explain the performance and security between hospitals, the architectures were implemented in a testbed to analyze the performance of the data plane between hospitals architectures to compare it with other secure VLANs.

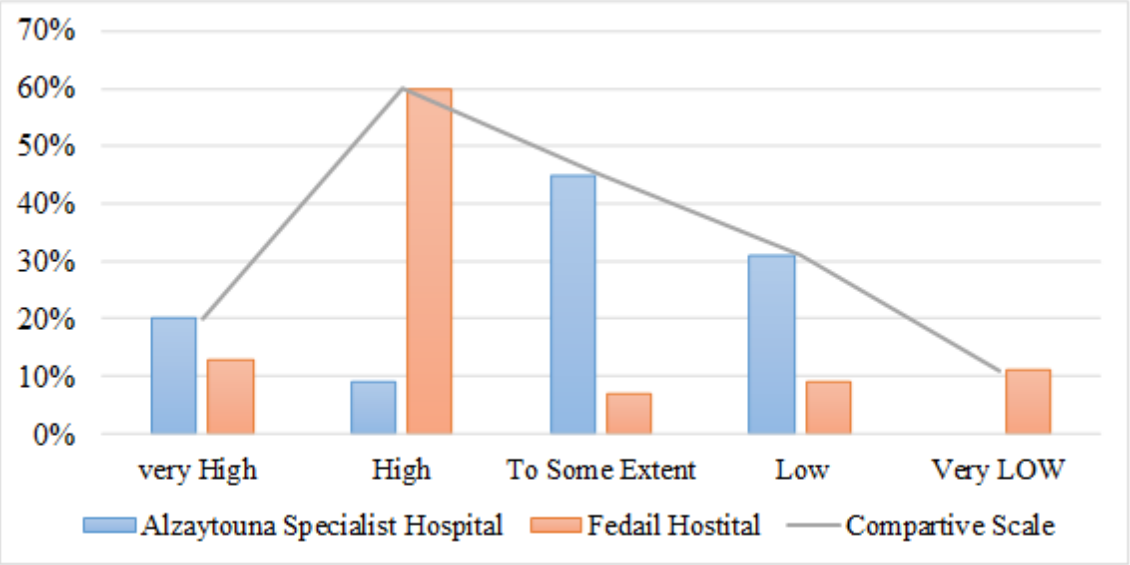

Figure 4.1: System knowledge Ratio

Figure (4.1) show the extent to which employees are aware of all the electronic services provided by the institution through the percentages shown in the table, which contains an analysis of data collected from Fedail Hospital and Alzaytouna Hospital.

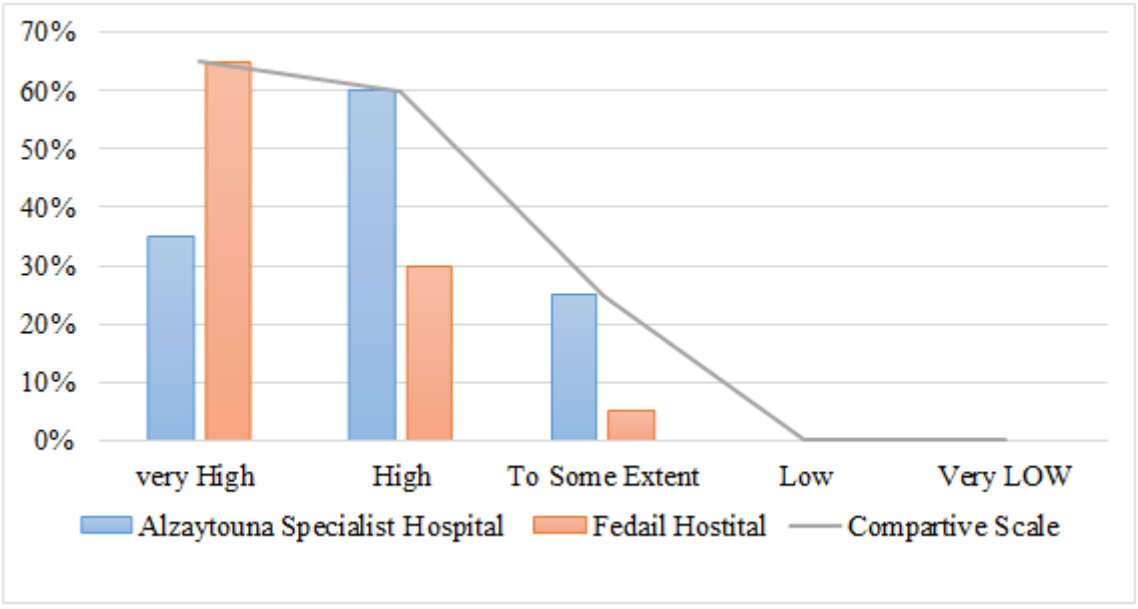

Figure 4.2: Data Confidential Ratio

Figure (4.2) It describes and measures the extent to which the institution is keen to maintain the confidentiality of patient data until completion of treatment.

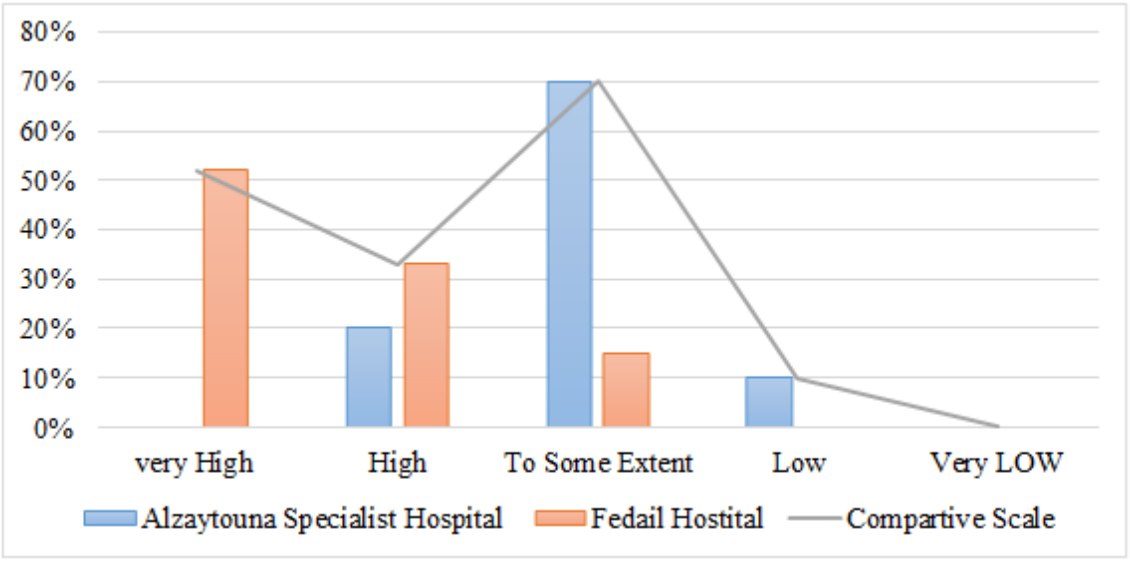

Figure 4.3: Data Communicate Ratio

Figure (4.3) show extent of how Members of the Foundation or organization and their colleagues communicate with through mobile chatting and email is effective and good.

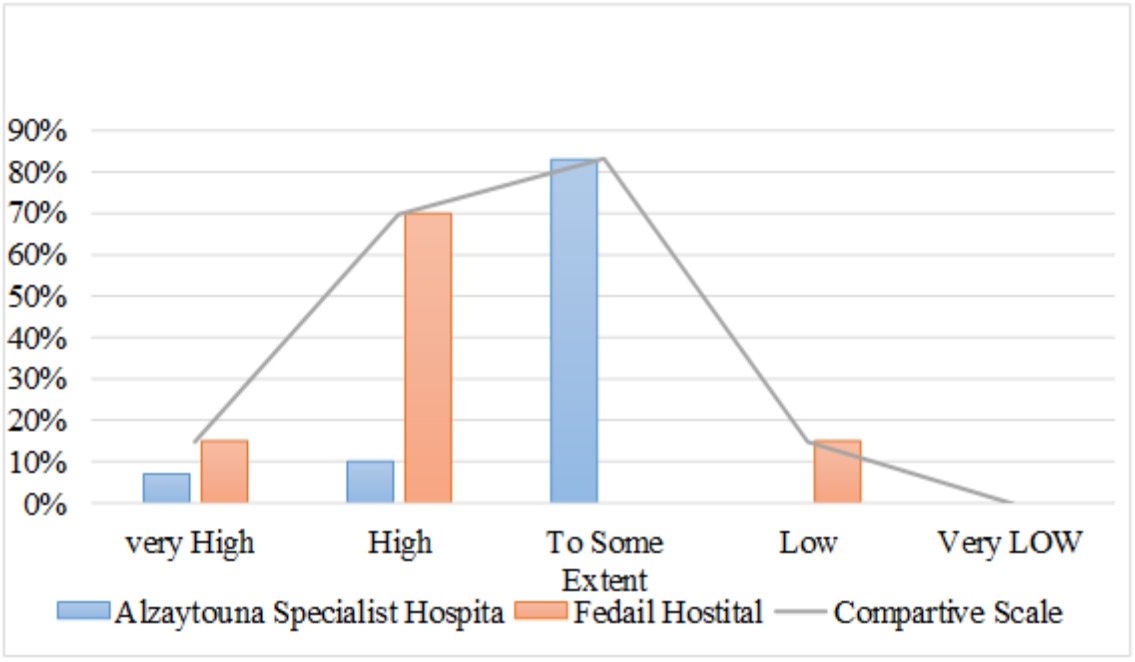

Figure 4.4: Visibility Ratio of Medical Menus

Figure (4.4) shows visibility ratio of electronic forms for follow-up patients required to be packaged easy and clear.

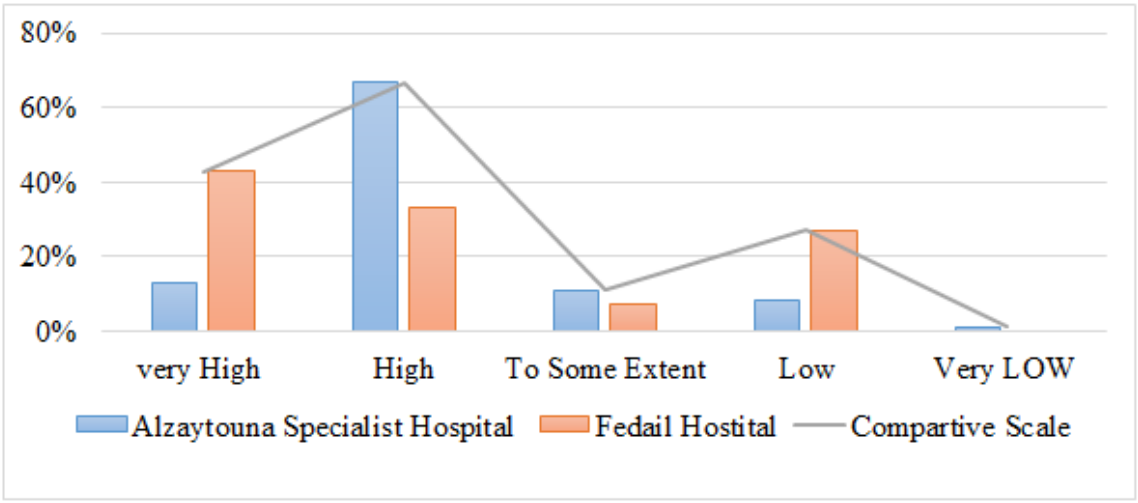

Figure 4.5: System and Network Response Rate

Figure (4.5) demonstrates data analysis to measure system and network responsiveness to meet all requirements system and network response to meet all requirements.

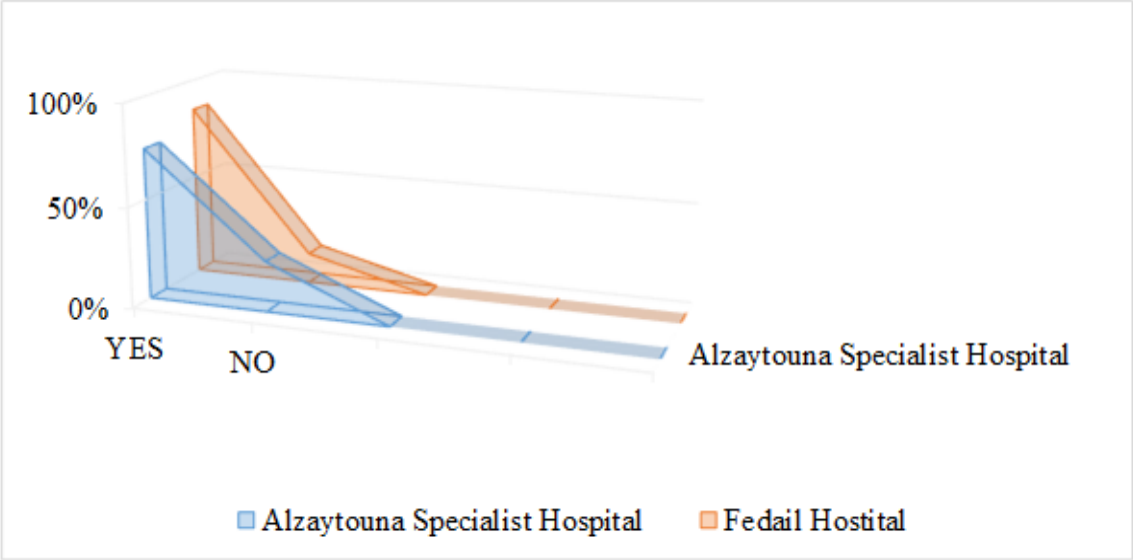

Figure 4.6: The Possibility of a Privacy Policy

Figure (4.6) Contains the answer to does the institution provide a privacy policy to protect patient records.

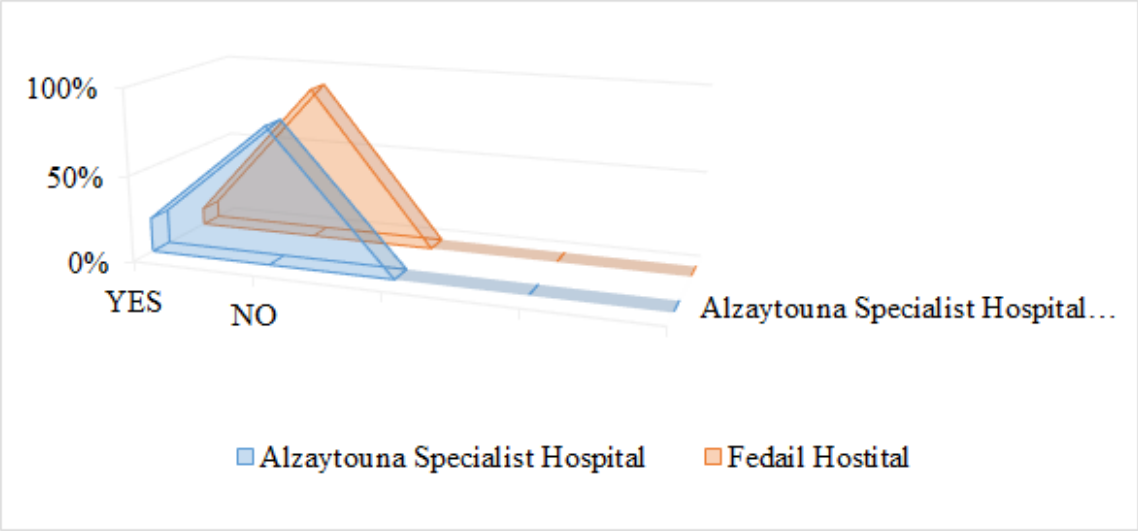

Figure 4.7: The Possibility of Using Medical Records

Most hospitals in the world use patient records for scientific research purposes, but the patient must choose to obtain his consent. Thus, the format shows a comparison between the hospital that uses the records for research purposes and which you do not use the shown Figure (4.7).

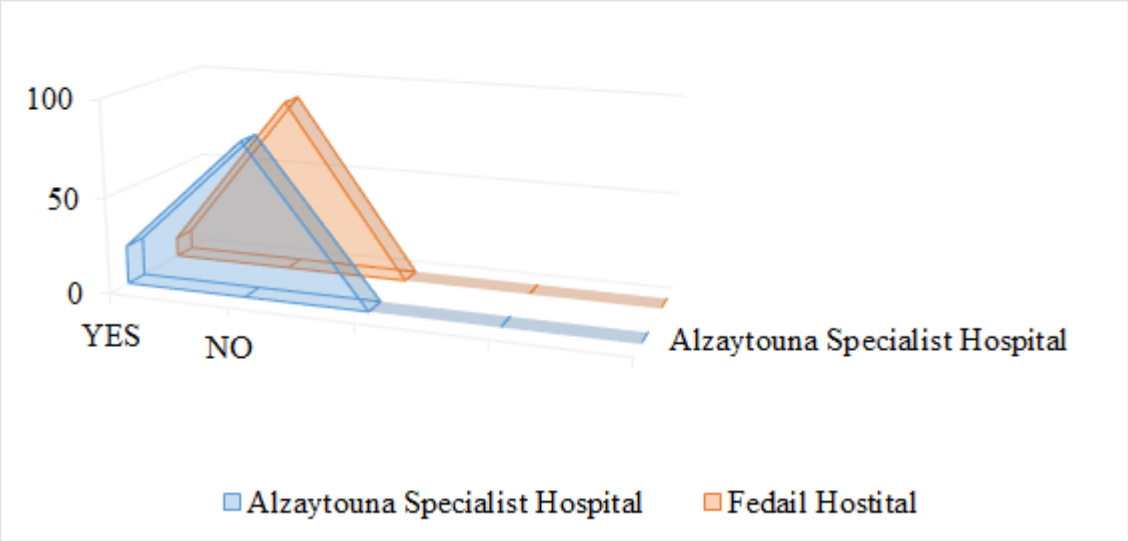

Figure 4.8: Probability of Consultation with Patients

Figure (4.8) explain the possibility of consultation with patients before using their records or disposing of them for any purpose.

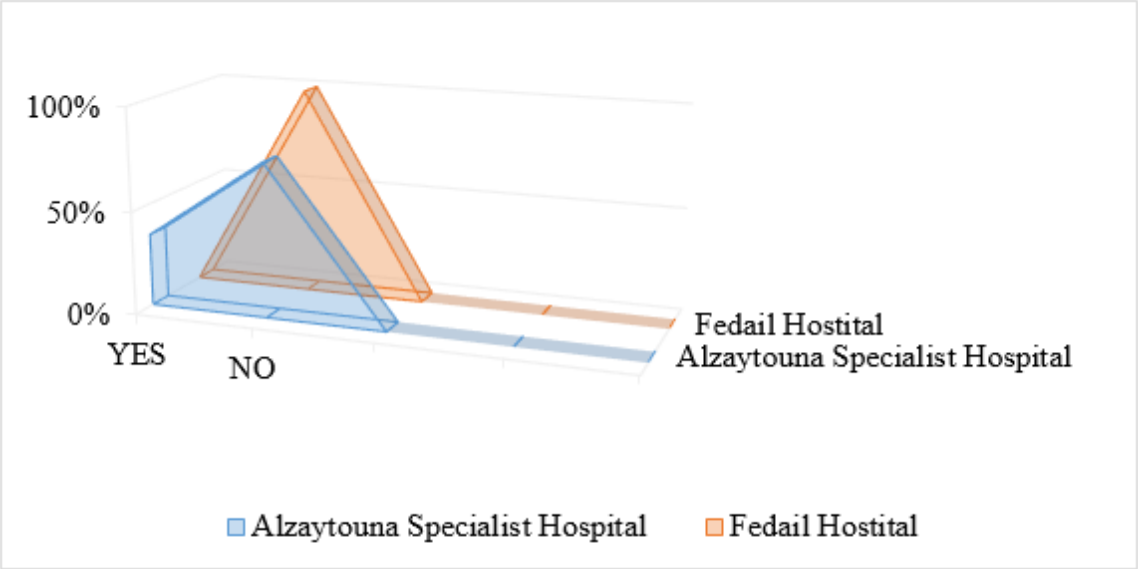

Figure 4.9: Possibility of Using VLAN Technology

Figure (4.9) show Possibility of using VLAN technology in campuses, after data collection and analysis, it was ascertained that the hospitals that collected the data were using the technique poorly and the other did not use the technology.

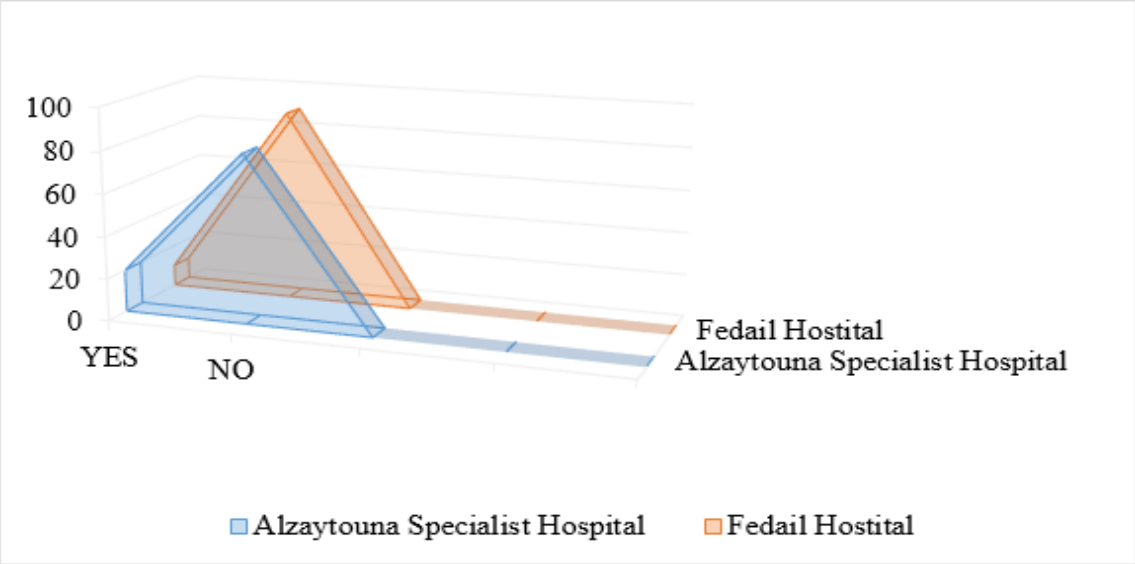

Figure 4.10: Probability of Training Courses

figure 4.10 show the availability of the institution courses and training courses for the workers in the institution and their development with modern technology.

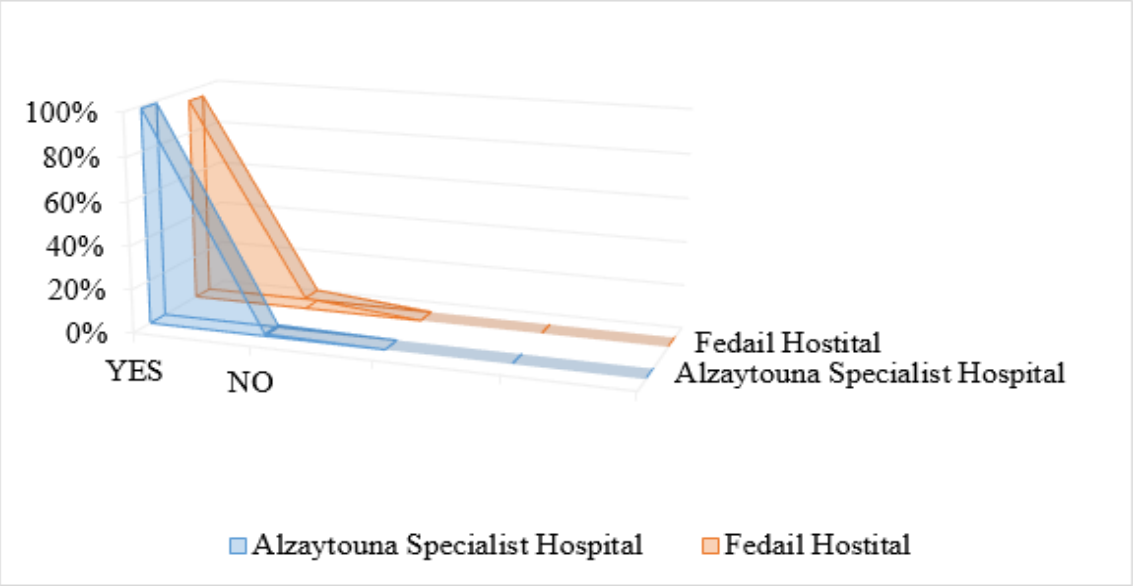

Figure 4.11: Possibility of Backup

The effects of the forces of nature from fires, floods, earthquakes and thefts also lead to damage and loss of files, and thus the permanent backup of data is very important, figure 4.11 show the extent to which the availability backup in hospitals.

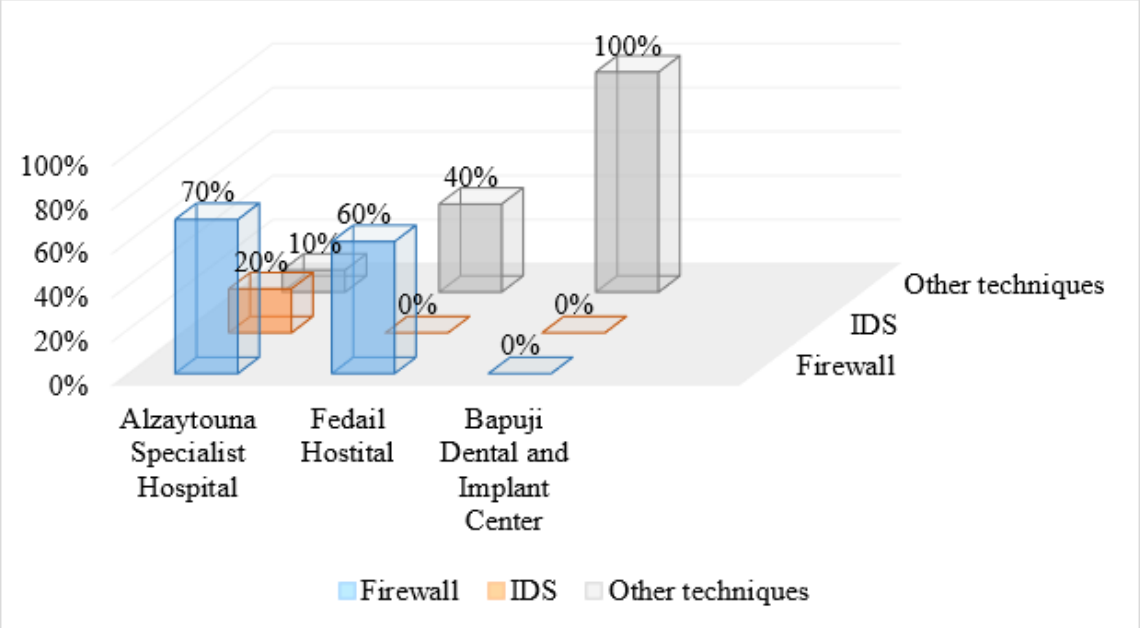

Figure 4.12: kind of Protection Technologies

Figure 4.12 show the type of protection technologies degree are currently used campuses.

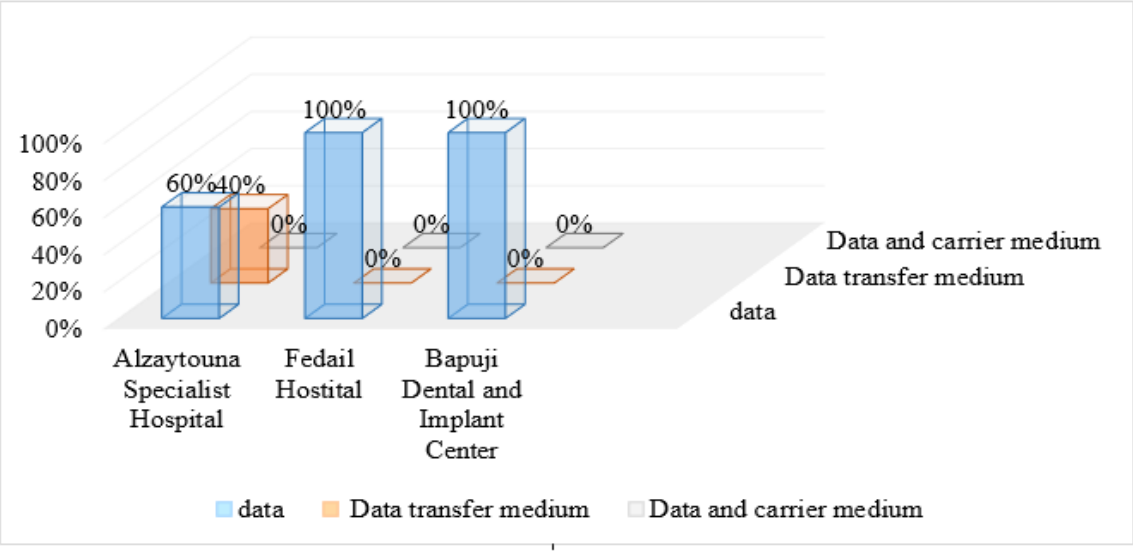

Figure 4.13: The Foundation Protects

Figure (4.13) show the concentration of the institution on the protection of patient data in terms of media carrier or data itself or both.

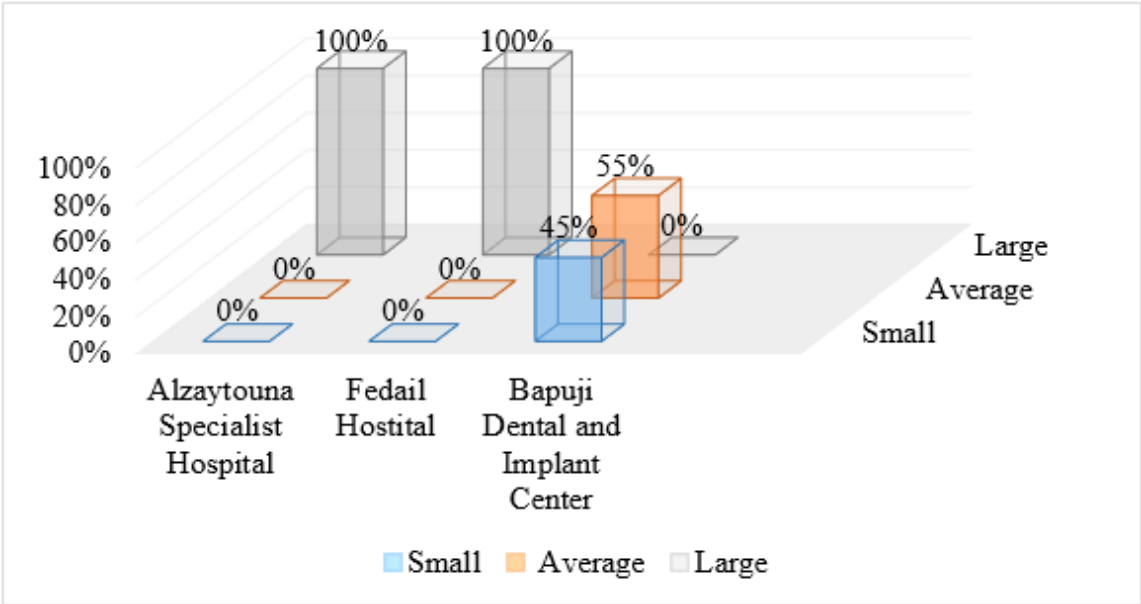

Figure 4.14: Percentage of User's Size

Measuring the size of users depends on the size of the organization and the number of devices used by servers and switches figure 4.14 show Percentage of user's size.

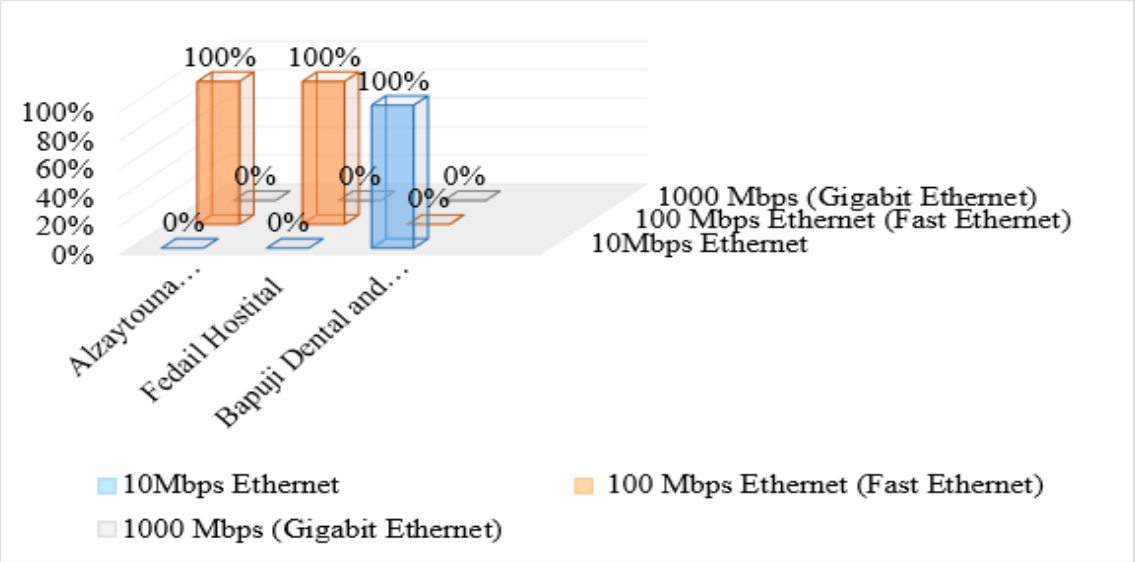

Figure 4.15: Kind of Internet Connection

Figure 4.15show witch internet connection cable used by organization depending on Mbps Which passes through the carrier medium.

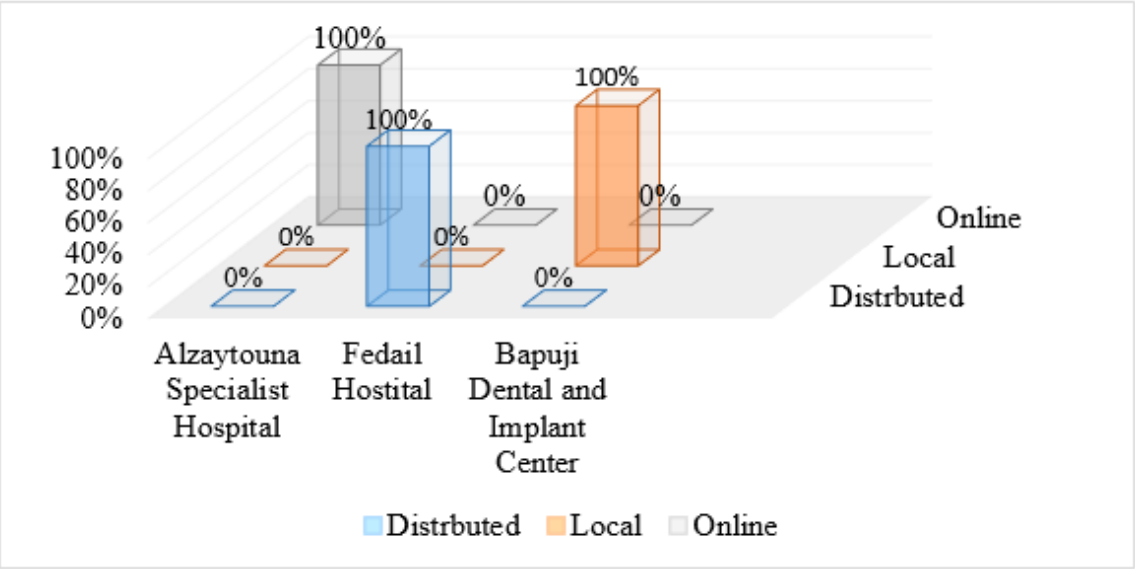

Figure 4.16: Type of Server Used

Figure 4.16 show percentage type of storage used to depend on server type for each campus.

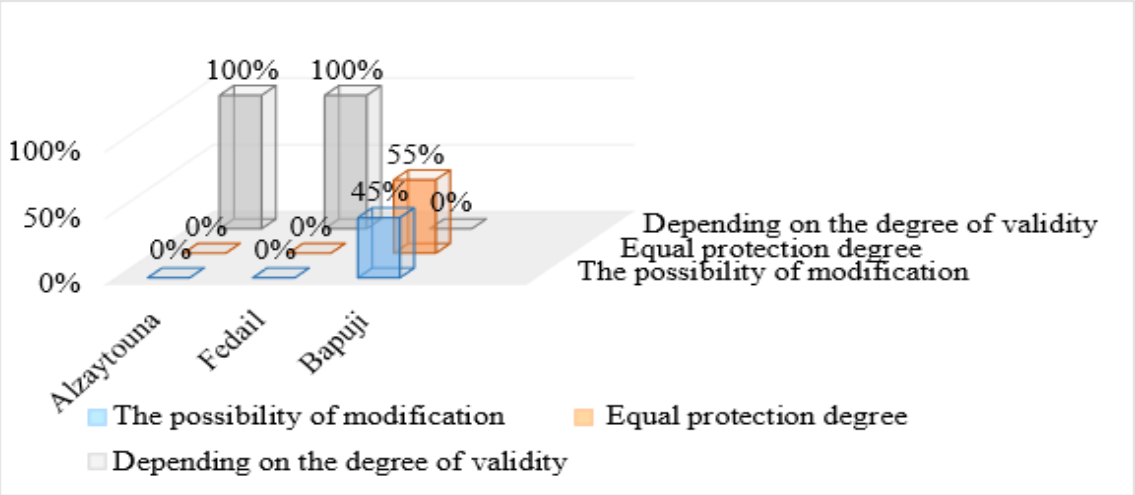

Figure 4.17: Method of The Division of Permissions

Figure 4.17 show the method of dividing the degree of protection depending on the sensitivity of data and security statements in the organization

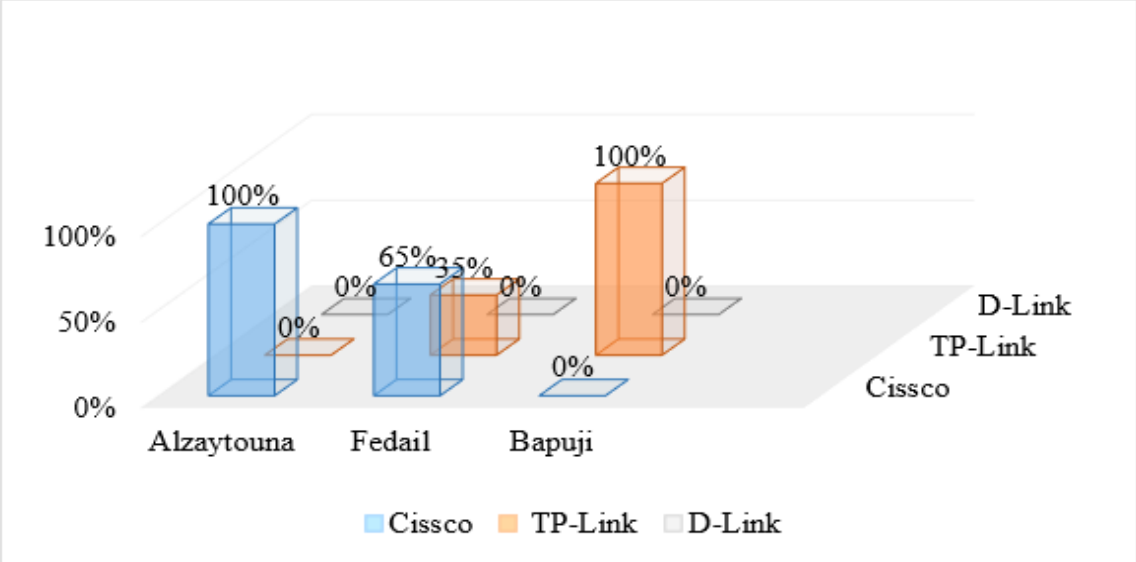

Figure 4.18: Kind of Switches Used

Figure 4.18 shows the percentage which kind of switches used depend on manufacturer company because the method of configuration varies from company to company.

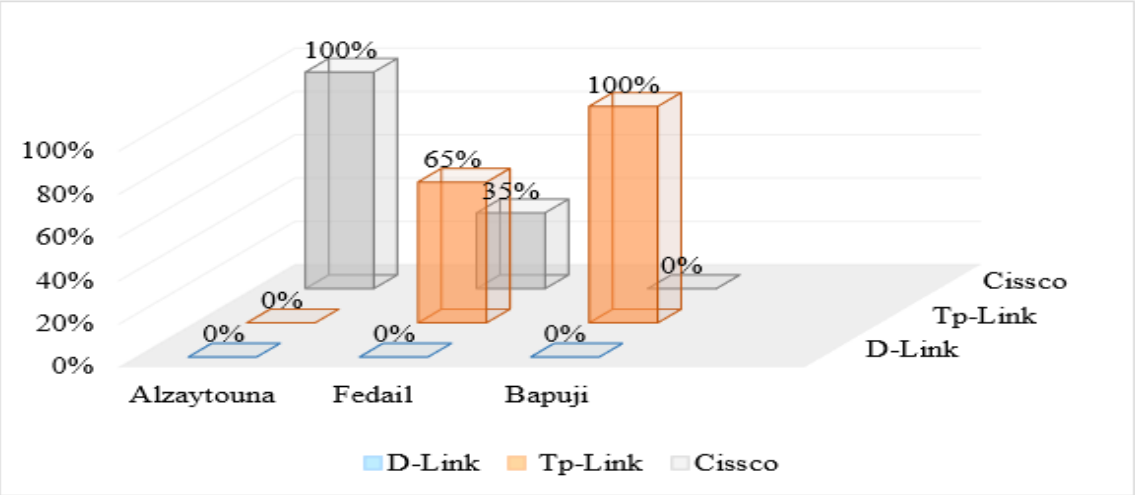

Figure 4.19: Type Routers Used

Figure 4.19 displays the percentage of which kind of routers used to depend on manufacturer company because the method of configuration varies also from company to company.

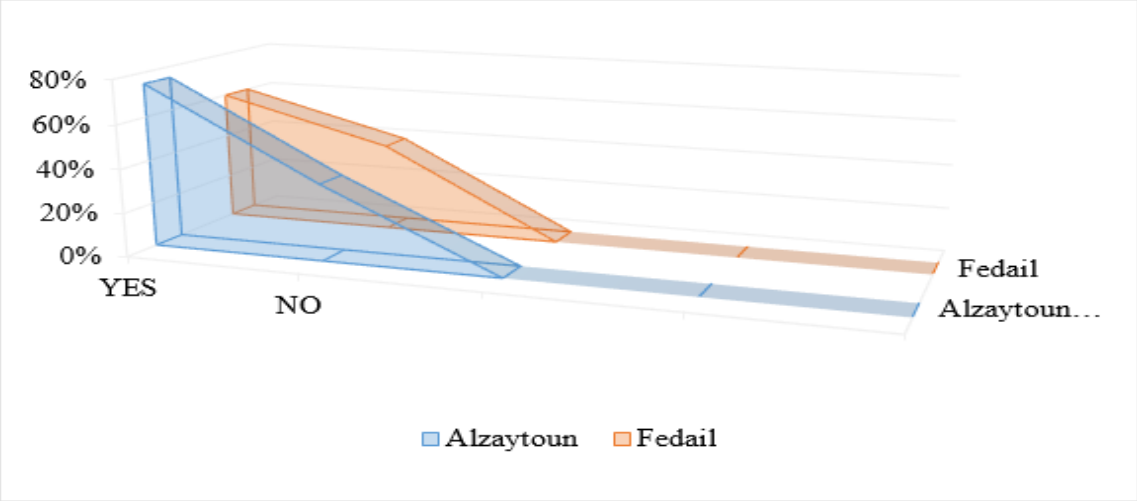

Figure 4.20: Employees' Approval to Use Their Data

During the data collection, a question was asked at the end of the questionnaire about the possibility of putting the name and telephone number as a reference in our scientific research Figure 4.20 shows the ratio of employees' approval to use their data as a reference.

4.3 Analysis Current Campus Network Topologies:

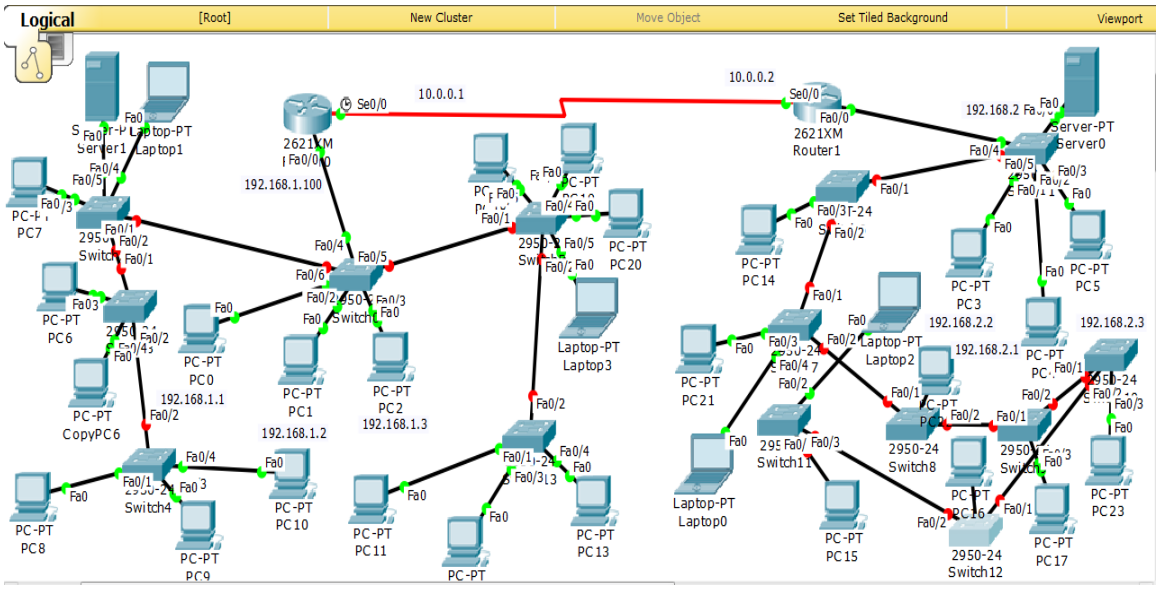

Figure 4.21: Alzaytouna Specialist Hospital Network Topology

Figure 4.21 shows analysis of network typology currently used in Alzaytouna Hospital, which this research is developing and adding the VLAN technology to protect its records.

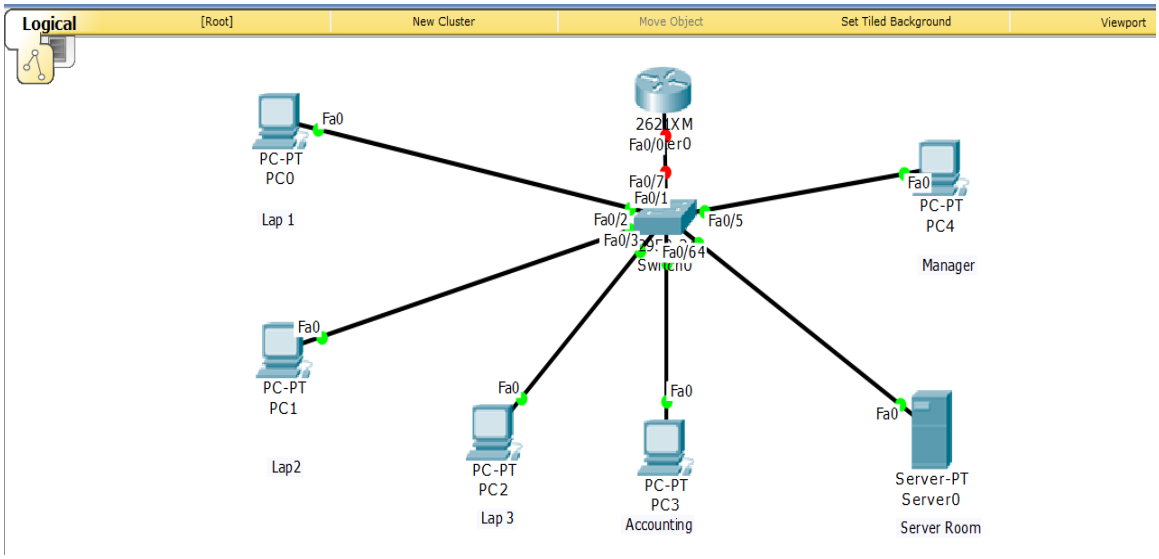

Figure 4.22: Fedail Specialist Hospital Network Topology

Figure 4.22 shows the analysis of network typology currently used in Fedail Specialist Hospital.

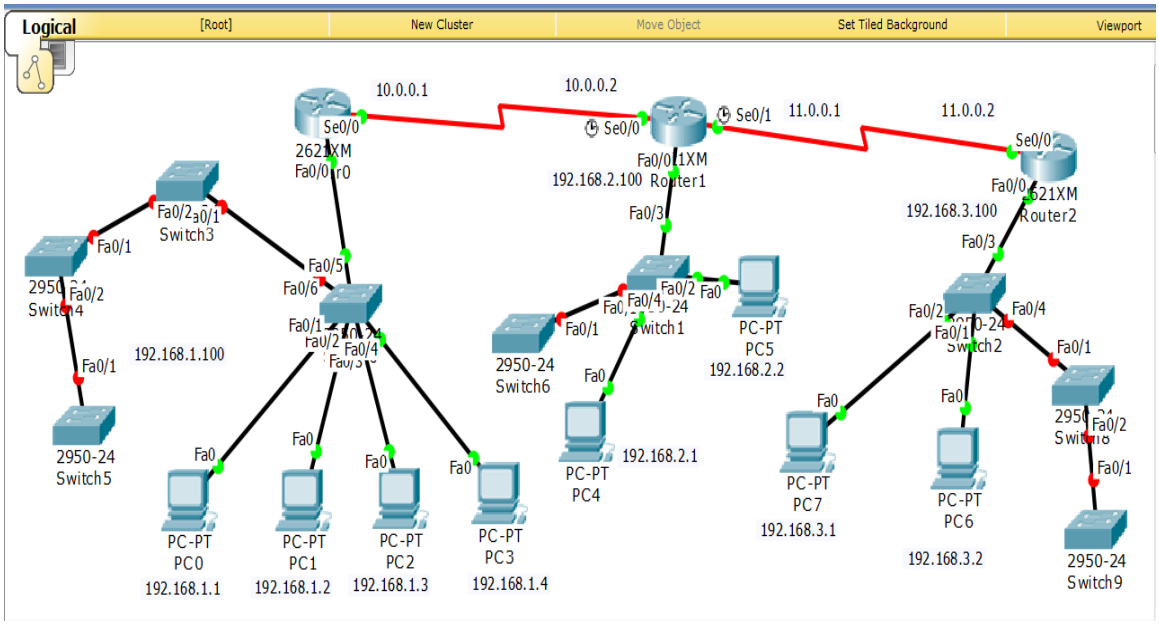

Figure 4.23: Bapuji Dental and Implant Center Network Topology

Bapuji Dental and Implant Center is a small dental clinic with a small network and a local server and a small percentage of users, Figure 4.23 shows analysis of network typology currently used in Bapuji Dental and Implant Center.

4.3 Implementation Stage

Define implementation steps and its requirements.

4.3.1 Requirements

The network should cover the area of a built-in-nearest future production plant which will include the main office, a warehouse, a security office (central entrance) and two workshops. It should support around 500 users and IP telephony.

The main office is a three-floor building with a server room located in the basement. There are several departments in the company: sales department, logistics department, call center, technical support and accounting department.

All of the departments will share the same Office VLAN. The server part is not covered in this thesis work, but for network planning, it is assumed that Active Directory Domain

Controller, DHCP, NTP, applications and databases servers, as well as web-server for the company's Intranet will be running on the network.

The warehouse is a separate building to store produced goods before its transportation. This part of the network relates to the main office and needs to be placed in the same VLAN. Warehouse Wi-Fi is needed for the use of barcode scanners and their connectivity with warehouse employees' portable devices.

Even though Wi-Fi technologies and its configuration are not covered in this work, Wi-Fi VLANs are mentioned and created. Workshops must be protected from any intrusions, traffic needs to be isolated inside each of the workshops. For this purpose, firewalls will be placed to border workshops' parts of the network.

After considering the approach to design the campus network discussed in the second chapter I developed a plan of the network that will fit the company's needs. The design was clearly separated into core, distribution and access

layers. The functionality of the implemented devices will be separated so the main features are distinguishable and met. As defined with the company's engineers there must be:

1. the network device that will connect the LAN to the Internet (WAN) should be a Layers 3 device to be able to perform routing. At this point (endpoint between our LAN and WAN) the security must be implemented.
2. a switch stack that will be capable of connecting users in the main office, server room and be connected to the rest of the network.
3. Distribution and access switches for connecting workshops, warehouse and the security office. Based on the requirements the network plan, shown in Figure 14, is designed and accepted by the company's engineers.

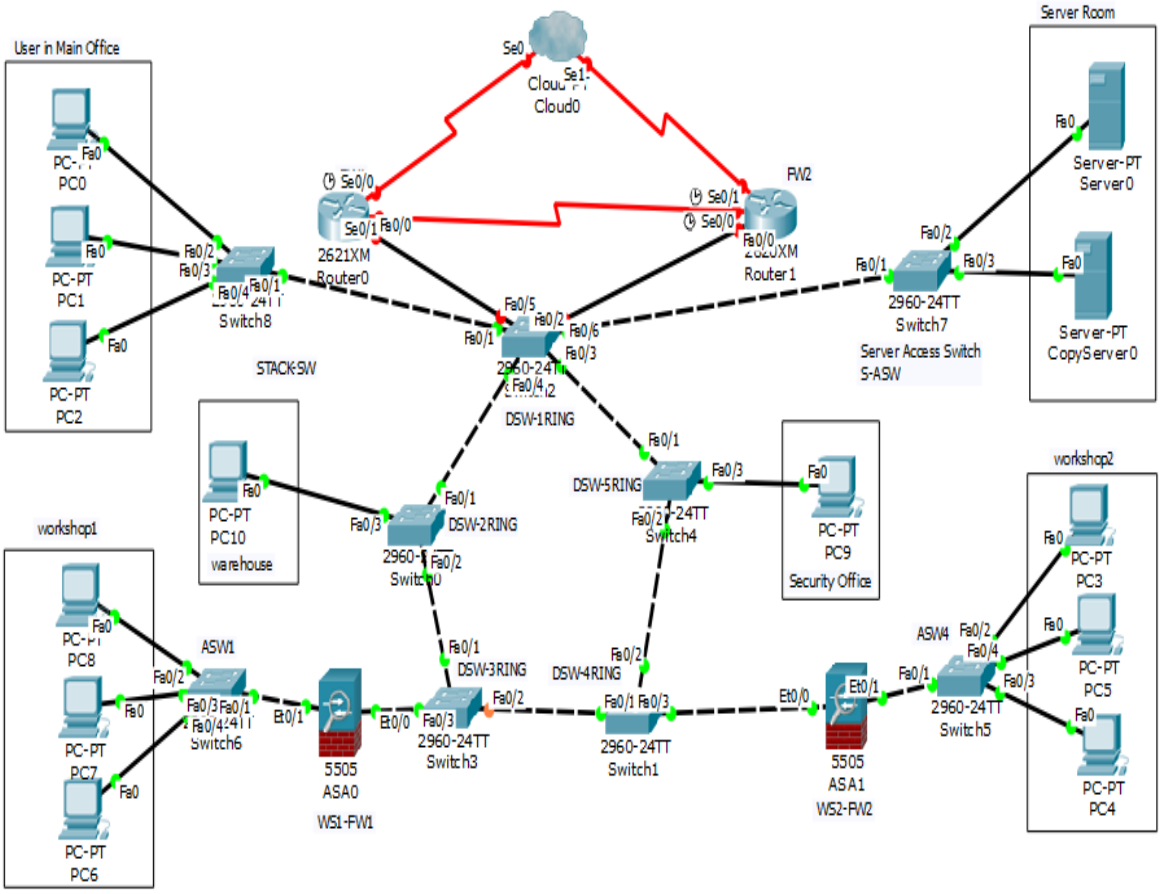

Figure 2.24: Solution Topology

The network design created according to the Campus needs and approval, Figure 2.24 illustrates the network's characterization, which has been designed and contains the means and protection policies required to protect patients' records, all of which have been attached to the appendices. To learn the steps and commands see appendix.

4.4 Summary

This section provides a comprehensive analysis of the data collected through the questionnaire, which in turn contain different types of questions and then compare the results between the various Hospitals from which data were collected (Alzaytouna Specialist Hospital, Fedail Hospital and Bapuji Dental and Implant Center) using Microsoft Office (Excel) 2016, shown in Figures (2.1 – 2.20). In this chapter, applied gathered knowledge into the configurations and commands that are needed to be conducted on the devices in the network show appendix for commands

CHAPTER FIVE

Conclusion and Recommendation

Conclusion

This research presented the main contributions of how to increase the scalability and security of electronic medical records network. First, this research proposed a scalable and secure VLAN architecture and describe how administrators group related hosts into VLANs, and how the switches and routers forward traffic between hosts. In this research work, the study on hierarchical network design approach was carried out.

Hierarchical design allows separating levels and provides better management and scalability opportunities. The final design plan of the hospital new plant network was built following the three-layer hierarchical design model. The necessary technologies and protocols were investigated and sample configurations that are needed to be performed were listed. Some of them were tested using the equipment in Virtual Laboratory, some of them were tested using Cisco Packet Tracer.

The design and configuration of a big enterprise network is a time-demanding, careful process and every little detail was hard to cover in this work. I prepared sample configurations, but it is obvious that in a scale of such a big network there are a lot of things to consider and more technologies must be implemented. I think that there are important issues that need to be reconsidered before implementing the network in real life. Following prepared configurations, the network can be set up and running, but to be reliable in a production, future developments and improvements are needed. The most important thing to reconsider is that DSW-RING1 switch is a single point of failure for the entire network. I recommend adding redundancy at this point.

Recommendations

Due to high operating costs and compatibility issues in L3VPNs, L2VPNs (Layer 2 Virtual Private Networks) such as VPLS are now becoming popular We are witnessing and recommending use VPLS to increase the scalability, flexibility and compatibility of secure VPLS networks. because scalable secure flat-VPLS architecture based on Host

Identity Protocol (HIP) increase the forwarding and security plane scalability and a secure hierarchical-VPLS architecture has been proposed by extending the previous proposal to achieve control plane scalability as well. To solve the compatibility issues of Spanning Tree Protocol (STP) in VPLS networks, a novel Distributed STP (DSTP) is proposed. and to achieve better results use OMNET++ simulator.

Reference

1. Zhang LP, Zhu SH, Tang S, Member S. Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme. 2016;(January):1-11.
2. Yu M, Rexford J, Sun X, Rao S, Feamster N. A survey of virtual LAN usage in campus networks. *IEEE Commun Mag*. 2011;49(7):98-103. doi:10.1109/MCOM.2011.5936161
3. DAYANAND LAL N BG& SV. a Survey on the Use of Gns3 for Virtualizing Computer Networks. *Int J Comput Sci Eng*. 2016;5(1):49-58. http://www.iaset.us/view_archives.php?year=2016&jtype=2&id=14&details=archives.
4. Chowdhury NMMK, Boutaba R. A survey of network virtualization. *Comput Networks*. 2010;54(5):862-876. doi:10.1016/j.comnet.2009.10.017
5. Akram J, Akram N, Mamoon S, Ali S, Naseer N. Future and Techniques of Implementing Security in VLAN. 2017;7(5):14-17.
6. Huang LC, Chu HC, Lien CY, Hsiao CH, Kao T. Privacy preservation and information security protection for patients' portable electronic health records. *Comput Biol Med*. 2009;39(9):743-750. doi:10.1016/j.compbiomed.2009.06.004
7. Hucaby D. *CCNP Routing and Switching SWITCH 300-115 Official Cert Guide*.; 2014.
8. Barrows C. Randolph, Jr PDC. Privacy, Confidentiality : and Electronic Medical Records Abstract The enhanced Goals of Informational Security In Health Care. *J Am Med Inf Assoc*. 1996;3(2):139-148.
9. Expósito J, Trujillo V, Gamess E. Using Visual Educational Tools for the Teaching and Learning of EIGRP. *Proc World Congr Eng Comput Sci*. 2010;

I:169-174.

10. Systems Cisco. Cisco Packet Tracer - Networking Academy. *Cisco Press*. 2010;1(2):1-3. doi:C78-552124-01.
11. Spitzner, L. (2002). Honeypots: Tracking Hackers.US: Addison Wesley. pp 1-430.
12. L. Sweeney k-anonymity: a model for protecting privacy International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002; 557-570.
13. L. Nguyen, E. Bellucci, "Electronic health records implementation: An evaluation of information system impact and contingency factors", Int. J. Med. Inf., vol. 83, no. 11, pp. 779-796, 2014.
14. IJCSI International Journal of Computer Science Issues, Volume 13, Issue 2, March 2016 ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784 www.IJCSI.org
15. L.p.Zhang, S.H Zhu,S. Tang*, Senior Member, IEEE Journal of Biomedical and Health Informatics (Volume: PP, Issue: 99),12 January 2016
16. Provos, N and Holz, T (July 26, 2007). Virtual Honeypots: From Botnet Tracking to Intrusion Detection. US: Addison-Wesley Professional.
17. Mikhail Afanasyev , Tadayoshi Kohno, Justin Ma, "Privacy-Preserving Network Forensics", Communications of ACM, Vol. 54 (5), pp – 78-87, 2011.
18. Vadim Zaliva, Firewall Policy Modeling, Analysis and Simulation May 9, 2008.
19. Oluwafemi Osho, Christopher I. Onuoha, Joel N. Ugwu, A Survey of Security Awareness, CoRI'16, Sept 7–9, 2016, Ibadan, Nigeria
20. Legal Medical Record Standards, Policy No. 9420, Policy Dated 05/01/2008
21. Vadim Zaliva, Firewall Policy Modeling, Analysis and Simulation, May 9, 2008.

Appendix One

1. Questioner

The data was collected through questionnaire questions and contained three types of questions yes or no questions, Multichoice questions and Degree of Availability questions. The questionnaire is divided into two parts, one for the medical staff and one for the technical and administrative staff

First: Basic Data: Name: (optional) .....

Table 2: Basic Data

Foundation	□ ……			
Gender	□ Male		□ Female	
Job	Engineer	programmer	Network Technician	□ Other
Age	□ 5 years and less	□ 25-45	□ more than 10 years	
Years of Experience	□ Less than 25	□ 6-10	□ more than 45	
Do you own a laptop / PC	□ Yes	□ No	□ Other	
How much do you use the Internet?	□ Daily □ Day-3 Days	□ Once a Week □ Once a Month	□ If necessary □ I do not use	
Educational qualification	□ Graduate □ Undergraduate □ Postgraduate			
Email/Telephone (optional)	……			

Second: Services Provided by the Foundation:

Table 3: Services Provided by the Foundation

N	Phrases	Degree of Availability				
		Very high	High	To some extent	Low	Very low
1	I have knowledge of all the electronic services provided by the institution					
2	The Foundation is keen to keep patient data confidential until the completion of treatment					
3	Your organization and colleagues communicate with you through mobile messaging - email and email is effective and good					
4	Electronic forms for follow-up patients required to be packaged easy and clear					
5	System and network response to meet all requirements					

Does the institution provide a privacy policy to protect patient records?

Yes ☐ No ☐

Are you using patient records for scientific research?

Yes ☐ No ☐

Does Foundation consult patients for their consent to use their records for other purposes?

Yes ☐ No ☐

Does the organization provide training courses to improve the quality of performance in the use of the system and the network?

Yes ☐ No ☐

Has the organization used VLAN technologies before?

Yes ☐ No ☐

1- What type of protection techniques are currently used and the level of protection?
   - Firewall
   - Another technique?

     …….

2- Institution protects:
   - Data
   - Data transfer medium
   - Data and carrier medium

3- Users size?
   - Small
   - Average
   - Huge

4- Type of Internet connection cable used
   - 10Mbps Ethernet
   - 100 Mbps Ethernet (Fast Ethernet)
   - 1000 Mbps (Gigabit Ethernet)

5- The server type used
   - Local server
   - Online server

6- Number of switches and type used?

   ……..

7- Number of Routers and Type Used?

……

Appendix Tow

1. IP Addressing of VLAN and Devices

Table 4 provides the IP addressing plan for VLANs and devices.

Table 4: IP-addressing plan for the network

Network, ip address	**VLAN name**	**VLAN number**	**Interface on the device**
172.16.2.0	**MNGT**	**2**	
172.16.2.1	FW1, FW 2		int g0/1.2
172.16.2.2	STACK		vlan 2
172.16.2.3	S-ASW		vlan 2
172.16.2.4	DSW1-ring		vlan 2
172.16.2.5	DSW2-ring		vlan 2
172.16.2.6	DSW3-ring		vlan 2
172.16.2.7	DSW4-ring		vlan 2
172.16.2.8	DSW5-ring		vlan 2
172.16.2.9	WS1-FW1, WS1-FW2		int g0/0.2
172.16.2.10	WS2-FW1, WS2-FW2		int g0/0.2
172.16.2.13	ASW1		vlan 2
172.16.2.14	ASW2		vlan 2
172.16.2.15	Administrator's PC		NIC
172.16.3.0/24	**SERVERS**	**3**	
172.16.3.1	FW1, FW 2		g0/1.3
172.16.3.2-254	Servers' pool		
172.16.100.0	OFFICE 100		
172.16.100.1	FW1, FW 2		int g0/1.100
172.16.100.1	FW1, FW 2		int g0/1.100
172.16.100.2	WS1-FW1, WS1-FW2		int g0/0.100
172.16.100.3	WS2-FW1, WS2-FW2		int g0/0.100

172.16.100.4-254	Users' pool		
172.16.108.0	**WIFI**	**108**	
172.16.108.1	FW1, FW 2		int g0/1.108
172.16.108.2 172.16.108.3	WS1-FW1, WS1-FW2 WS2-FW1, WS2-FW2		int g0/0.108 int g0/0.108
172.16.108.4-254	Users' pool		
172.16.109.0	**WAREHOUSEWIFI**	**109**	
172.16.109.1	FW1, FW 2		int g0/1.109
172.16.109.2	WS1-FW1, WS1-FW2		int g0/0.109
172.16.109.3	WS2-FW1, WS2-FW2		int g0/0.109
172.16.109.4-254	Users' pool		
172.16.110.0	VOICE 110		
172.16.110.1	FW1, FW 2		int g0/1.110
172.16.110.2	WS1-FW1, WS1-FW2		int g0/0.110
172.16.110.3	WS2-FW1, WS2-FW2		int g0/0.110
172.16.110.4-254	Users' pool		
172.16.111.0	PRINTERS 111		
172.16.111.1	FW1, FW 2		int g0/1.111
172.16.111.2	WS1-FW1, WS1-FW2		int g0/0.111
172.16.111.3	WS2-FW1, WS2-FW2		int g0/0.111
172.16.111.4-254	Users' pool		
172.16.112.0	**WS1**	**112**	
172.16.112.1	WS1-FW1, WS1-FW2		int g0/1.112
172.16.112.2-254	Users' pool		
172.16.113.0	**WS1WIFI**	**113**	
172.16.113.1	WS1-FW1, WS1-FW2		int g0/1.113
172.16.113.2-254	Users' pool		
172.16.114.0	**WS1PRINTERS**	**114**	
172.16.114.1	WS1-FW1, WS1-FW2		int g0/1.114

172.16.114.2-254	Users' pool		
172.16.115.0	**WS2**	**115**	
172.16.115.1	WS1-FW1, WS1-FW2		int g0/1.115
172.16.115.2-254	Users' pool		
172.16.116.0	**WS2WIFI**	**116**	
172.16.116.1	WS1-FW1, WS1-FW2		int g0/1.116
172.16.116.2-254	Users' pool		
172.16.117.0	**WS2PRINTERS**	**117**	

For the network of the factory, the following VLANs listed in Table 2 are going to be implemented.

Table 5: VLANs of the hospital.

Number	**Name**	**Purpose**
1	default	Not used
2	MNGT	Device management
3	SERVERS	For servers
100	OFFICE	For the rest of office employees
108	WIFI	For guests and personnel, only Internet access
109	WAREHOUSEWIFI	Warehouse Wi-Fi for barcode scanners
111	PRINTERS	Printers
112	WS1	Workshop 1
113	WS1WIFI	Workshop 1 Wi-Fi
114	WS1PRINTERS	Workshop 1 printers
115	WS2	Workshop 2
116	WS2WIFI	Workshop 2 Wi-Fi
117	WS2PRINTERS	Workshop 2 printers

2. Configuring Switches

The approximate configuration on the example of the stack switch that connects users of the main office are as follows:

Set up a password for privileged EXEC mode on the switch:

Switch> enable

Switch# configure terminal

Switch(config)# enable password 1234

Turn on password encryption so that the passwords are not shown in clear text in the configuration:

Switch(config)# service password-encryption

Set up the unique device name:

Switch(config)# hostname STACK-SW

Configure an IP address for the device. Address is needed for management purposes. IP address can be found in Table 1 in Chapter 2. For the stack switch it is 172.16.2.2 and it is in the VLAN 2.

STACK-SW(config)# interface vlan 2

STACK-SW(config-if)# ip address 172.16.2.2 255.255.255.0

STACK-SW(config-if)# exit

Disable the domain lookup feature so that the device does not start searching for a match whenever a typing mistake occurs:

STACK-SW(config)# no ip domain-lookup

Define the Domain Name:

STACK-SW(config)# ip domain-name my-domain.ru

Set up the current time by defining the NTP server. NTP server resides in the server farm.

STACK-SW(config)# ntp server 172.16.3.6 version 2 source vlan 2

STACK-SW(config)# ntp clock-period 36029056

STACK-SW(config)# ntp max-associations 1

Disable web-interface:

STACK-SW(config)# no ip http server

Set up default gateway:

STACK-SW(config)# ip default-gateway 172.16.2.1

Configure SSH connection to the device. RSA key needs to be generated, user has to be created, assigned with AAA model and SSH needs to be enabled on virtual terminal lines:

STACK-SW(config)# crypto key generate rsa

STACK-SW(config)# username user privilege 15 password 7 1234

STACK-SW(config)# aaa new-model

STACK-SW(config)# line vty 0 15

STACK-SW(config)# transport input ssh

STACK-SW(config)# logging synchronous

Define Access List to access the switch only from specific IP-addresses:

STACK-SW(config)# ip access-list standard SSH

STACK-SW(config-std-nacl)# permit 172.16.2.15

STACK-SW(config-std-nacl)# exit

Apply the Access List:

STACK-SW(config)# line vty 0 15

STACK-SW(config-line)# access-class SSH in

Set up timeout of inactivity in the SSH session. When the time is exceeded and

no actions were taken, the telnet session will be closed.

STACK-SW(config-line)# exec-timeout 5 0

STACK-SW(config-line)# exit

Save the Configurations:

STACK-SW# copy running-config startup-config

Or

STACK-SW#write

Configure SSH connection to the device. RSA key needs to be generated, the user has to be created, assigned with AAA model and SSH needs to be enabled on virtual terminal lines:

STACK-SW(config)# crypto key generate rsa

STACK-SW(config)# username user privilege 15 password 7 1234

STACK-SW(config)# aaa new-model

STACK-SW(config)# line vty 0 15

STACK-SW(config)# transport input ssh

STACK-SW(config)# logging synchronous

Define access-list to access the switch only from specific IP-addresses:

STACK-SW(config)# ip access-list standard SSH

STACK-SW(config-std-nacl)# permit 172.16.2.15

STACK-SW(config-std-nacl)# exit

Similar configurations are applied for all the devices.

3. Virtual Local Area Network

VLANs and their description need to be configured on every switch. For easy management, the VTP (VLAN Trunking Protocol) can be configured. DSW-RING1 will be defined as a VTP server, while other switches are defined as clients.

All the VLANs need to be created on the VTP server as follows:

DSW-RING1# configure terminal

DSW-RING1(config)# vlan 2

DSW-RING1(config-vlan)# name MNGT

DSW-RING1(config-vlan)# vlan 3

DSW-RING1(config-vlan)# name SERVERS

DSW-RING1(config-vlan)# vlan 100

DSW-RING1(config-vlan)# name OFFICE

DSW-RING1(config-vlan)# vlan 108

DSW-RING1(config-vlan)# name WIFI

DSW-RING1(config-vlan)# vlan 110

DSW-RING1(config-vlan)# name VOICE

DSW-RING1(config-vlan)# vlan 111

DSW-RING1(config-vlan)# name PRINTERS

DSW-RING1(config-vlan)#vlan 109

DSW-RING1(config-vlan)#name WAREHOUSEWIFI

DSW-RING1(config-vlan)#vlan 112

DSW-RING1(config-vlan)#name WS1

DSW-RING1(config-vlan)#vlan 113

DSW-RING1(config-vlan)#name WS1WIFI

DSW-RING1(config-vlan)#vlan 114

DSW-RING1(config-vlan)#name WS1PRINTERS

DSW-RING1(config-vlan)#vlan 115

DSW-RING1(config-vlan)#name WS2

DSW-RING1(config-vlan)#vlan 116

DSW-RING1(config-vlan)#name WS2WIFI

DSW-RING1(config-vlan)#vlan 117

DSW-RING1(config-vlan)#name WS2PRINTERS

The next thing is to actually define DSW-RING1 as a VTP server with the following commands:

DSW-RING1(config)# vtp domain MY

DSW-RING1(config)# vtp password MY

DSW-RING1(config)# vtp mode server

and to configure other switches as clients:

DSW-RING2(config)# vtp domain MY

DSW-RING2(config)# vtp password MY

DSW-RING2(config)# vtp mode client

4.1 Configuring Interfaces

As soon as all VLANs are created, the interfaces can be configured to either be in access mode and to belong to a specific VLAN or to operate in trunk mode and pass tagged traffic.

Access ports Interfaces, that connect PCs and phones to switches will be configured in access mode.

The VLAN to which a PC relates as well as Voice VLAN must be specified on the interface. It was decided to implement the Layer 2 security. The number of possible MAC addresses on the interface is restricted to two and in case of violating this rule, the port must become disabled. An example configuration of an access port that needs to apply to the main office access switch STACK-SW is the **following:**

```
STACK-SW(config)# switchport access vlan 100
STACK-SW(config)# switchport mode access
STACK-SW(config)# switchport voice vlan 110
STACK-SW(config)# switchport port-security maximum 2
STACK-SW(config)# switchport port-security
STACK-SW(config)# switchport port-security violation shutdown
```

Similar commands are needed to be applied to other ports and o other devices. Trunk ports in order to pass traffic from different VLANs, Trunking protocol needs to be configured on the interfaces that are pointing to neighbor switches. Configuration for DSW-RING1 on the interface GigabitEthernet 0/0–the one that points to FW1– is the **following:**

```
DSW-RING1(config)# interface GigabitEthernet 0/0
DSW-RING1(config-if)# switchport trunk encapsulation dot1q
DSW-RING1(config-if)# switchport trunk native vlan 2
DSW-RING1(config-if)# switchport mode trunk
DSW-RING1(config-if)# switchport nonegotiate
```

Similar configurations are needed for connections between DSW-RING3 and DSW RING4 and firewalls clusters. To configure Trunking between switches in the ring, e.g. between DSW-RING1 and DSW-RING2 and DSW-RING1 and DSW-RING3, the configuration is applied on the port channel interfaces. The configuration of port channels is described later in this section. Actually, it does not differ much from the one applied to a single port:

```
DSW-RING1(config)# interface port-channel 1
 DSW-RING1(config-if)# switchport trunk encapsulation dot1q
```

DSW-RING1(config-if)# switchport trunk native vlan 2

DSW-RING1(config-if)# switchport mode trunk

DSW-RING1(config-if)# switchport nonegotiate

Following the same manner, Trunking is needed to be configured on the links between all the switches in the ring and between DSW-RING1 and STACK-SW and S-ASW.

4.2 Stacking

Stacking possibility with Cisco FlexStack modules allows unifying up to four devices with the 20 Gbps stack throughput. If a new switch is added to the stack, its software will be automatically upgraded and the switch will become a member of the stack transparently. Switches, that are part of a stack, behave as a single device which reduces maintenance costs and eases its management. Cross-stack features, such as Etherchannel, can be highlighted as an advantage of creating a stack.

Each member of the stack is identified with a stack member number. If the number a switch was assigned is already taken, it will select the lowest available in the stack number. After changing the member number, the member must be reset. The higher the priority number of a stack member, the higher the chance this switch will be chosen as a stack master. Stack master operates the stack and all configurations applied to a stack master are later replicated to stack members. The MAC address of the stack determined is the same as the master switch has. The stack MAC persistency can be configured. It ensures that, if a master switch fails, the MAC address will still be the same during the persistency timer and, if the same switch becomes the master again; it will not change. If another switch becomes master, the MAC address will be inherited from it. (Cisco Systems Inc. 2016.)

Global configuration commands are the following:

STACK-SW(config)# switch 1 renumber 1

STACK-SW(config)# switch 1 priority 10

STACK-SW(config)# stack-mac persistent timer 0

For verifying the configurations of the switch the show switch command is issued.

4.3 Spanning Tree and its Features

By default, the switches have PVST+ spanning tree protocol enabled. Automatically, the root switch is selected based on its bridge identifier which is summed from switch priority and the MAC address.

DSW-RING1 switch is chosen to be the root switch in the network and in order to accomplish it, its priority will be manually lowered with the command:

DSW-RING1(config)# spanning-tree vlan 1-4096 root primary

In order to protect the root switch, the root guard will be enabled on its interfaces that are pointing to other switches in the topology:

DSW-RING1(config-if)# spanning-tree guard root

For all access interfaces that point to end clients/devices the portfast and bpduguard features are enabled:

DSW-RING1(config-if)# spanning-tree portfast

DSW-RING1(config-if)# spanning-tree bpduguard enable

For the port-channels, the following command will enable additional protection in **the case of misconfiguration:**

DSW-RING1(config)# spanning-tree etherchannel guard misconfig

4.4 Etherchannel

Link aggregation allows increasing bandwidth and also adds redundancy, if the port goes down, cable is harmed or unplugged, etc. The configuration of the aggregation is simple, but in order to aggregate several ports they have to have identical characteristics such as:

- the same speed;
- same duplex settings;
- same VLAN settings.

For the network I am working on, the links between switches in a ring are aggregated (GigabitEthernet interfaces g0/0-1 to one neighbor switch and g0/2-3 to another) using the LACP protocol. The following introduces an example configuration on a DSW-RING2:

DSW-RING1(config)# interface range GigabitEthernet 0/0-1

DSW-RING1(config-if)# description * to DSW-RING1*

DSW-RING1(config-if)# channel-group 1 mode active

DSW-RING1(config)# interface range GigabitEthernet 0/2-3
DSW-RING1(config-if)# description * to DSW-RING3*
DSW-RING1(config-if)# channel-group 2 mode active

5. Configuring Edge Device

The edge devices in this thesis mean the ones that separate production LAN from the Internet – FW1&FW2 and also failover clusters of WS1FW1-WS1FW2 and WS2FW1 WS2FW2 firewalls that separate Workshops from LAN. In this section configuration examples for interfaces, routing, network address translation and access control lists are presented.

5.1 Failover Clustering

For each firewall presence, the Active/Standby failover needs to be configured.

Configuring primary unit:

WS1FW1(config)# failover lan unit primary

This command assigns an interface that points to a standby device:

WS1FW1(config)# failover lan interface FAILOVER GigabitEthernet0/3

This command assigns an IP address to a failover interface:

WS1FW1(config)# failover interface ip FAILOVER 10.10.10.1
255.255.255.0 standby 10.10.10.2

Enable the interface:

WS1FW1(config)# no shutdown

Assign the same interface to be a stateful failover link. There is no need to specify IP address because it was already configured:

WS1FW1(config)# failover link statelink GigabitEthernet0/3

enable the failover:

WS1FW1(config)# failover

Configuring the secondary unit takes place as follows: WS1FW2(config)#failover lan unit secondary WS1FW2(config)#failover lan interface FAILOVER gigabitEthernet0/3 WS1FW2(config)#failover interface ip FAILOVER 10.10.10.1
255.255.255.0 standby 10.10.10.2
WS1FW2(config)#failover link statelink GigabitEthernet0/3
WS1FW2(config)#failover
Following the same manner, the failover clusters for FW1-FW2 and WS2FW1-WS2FW2 are configured.

5.2 Interfaces, Subinterfaces

On Cisco ASA firewalls the interface that points to the ISP will be configured as OUTSIDE interface with the IP address defined by the Internet provider. The security-level of outside interface by default is 0. So, until it is necessary, there is no need to change it.

FW1(config)#interface GigabitEthernet 0/0
FW1(config-if)#nameif outside
FW1(config-if)#security-level 0

The interface that points to DSW-RING1(and connects the whole Local area network) will be INSIDE interface, but to perform inter-vlan routing, the configurations are not applied on the physical interface itself. Sub interfaces are created and assigned with IP addresses which are default gateways for specific VLANs.

FW1(config-if)#interface GigabitEthernet 0/1
FW1(config-if)#no name
FW1(config-if)#no ip address
FW1(config-if)#interface GigabitEthernet 0/1.3
FW1(config-if)#nameif SERVERS
FW1(config-if)#ip address 172.16.3.1 255.255.255.0
FW1(config-if)#security-level 100
FW1(config-if)#interface GigabitEthernet 0/1.2
FW1(config-if)#nameif MNGT
FW1(config-if)#ip address 172.16.2.1 255.255.255.0

FW1(config-if)#security-level 100

FW1(config-if)#interface GigabitEthernet 0/1.100

FW1(config-if)#nameif OFFICE

FW1(config-if)#ip address 172.16.100.1 255.255.255.0

FW1(config-if)#security-level 100

FW1(config-if)#interface GigabitEthernet 0/1.108

FW1(config-if)#nameif WIFI

FW1(config-if)#ip address 172.16.108.1 255.255.255.0

FW1(config-if)#security-level 100

FW1(config)#interface GigabitEthernet 0/1.109

FW1(config-if)#nameif WAREHOUSWIFI

FW1(config-if)#ip address 172.16.109.1 255.255.255.0

FW1(config-if)#security-level 100

FW1(config-if)#interface GigabitEthernet 0/1.110

FW1(config-if)#nameif VOICE

FW1(config-if)#ip address 172.16.110.1 255.255.255.0

FW1(config-if)#security-level 100

FW1(config-if)#interface GigabitEthernet 0/1.111

FW1(config-if)#nameif PRINTERS

FW1(config-if)#ip address 172.16.111.1 255.255.255.0

FW1(config-if)# security-level 100

Similar configurations are applied to the second member of the failover cluster.

5.3 Configuring Workshops

The configuration of the workshop border firewalls is similar, but considering that WS1-FW1 and WS1-FW2 are implemented to protect production areas not only from outside intruders, but also from the possible harm or data leakage in the local network, the interfaces on this firewalls are as follows: the inside interface points to workshop network and the outside interface connects the factory LAN.

Based on this, the outside interface is configured and divided into subinterfaces for each VLAN in the network, and the inside interface is configured for VLANs used inside workshop area. The configuration is as follows:

```
WS1-FW1(config)# interface GigabitEthernet 0/0
WS1-FW1(config-if)# no name
WS1-FW1(config-if)# no ip address
WS1-FW1(config-if)# interface GigabitEthernet 0/0.3
WS1-FW1(config-if)# nameif SERVERS
WS1-FW1(config-if)# ip address 172.16.3.2 255.255.255.0
WS1-FW1(config-if)#
WS1-FW1(config-if)# interface GigabitEthernet g0/0.2
WS1-FW1(config-if)# nameif MNGT
WS1-FW1(config-if)# ip address 172.16.2.2 255.255.255.0
WS1-FW1(config-if)# security-level 80
WS1-FW1(config-if)# interface GigabitEthernet g0/0.100
WS1-FW1(config-if)# nameif OFFICE
WS1-FW1(config-if)# ip address 172.16.100.2 255.255.255.0
WS1-FW1(config-if)# security-level 80
WS1-FW1(config-if)# interface GigabitEthernet 0/0.108
WS1-FW1(config-if)# nameif WIFI
WS1-FW1(config-if)# ip address 172.16.108.2 255.255.255.0
WS1-FW1(config-if)# security-level 80
WS1-FW1(config-if)# interface GigabitEthernet g0/0.109
WS1-FW1(config-if)# nameif WAREHOUSEWIFI
WS1-FW1(config-if)# ip address 172.16.109.2 255.255.255.0
WS1-FW1(config-if)# security-level 80
WS1-FW1(config-if)# interface GigabitEthernet 0/0.110
WS1-FW1(config-if)# nameif VOICE
WS1-FW1(config-if)# ip address 172.16.110.2 255.255.255.0
WS1-FW1(config-if)# security-level 80
WS1-FW1(config-if)# interface GigabitEthernet 0/0.111
```

WS1-FW1(config-if)# nameif PRINTERS

WS1-FW1(config-if)# ip address 172.16.111.2 255.255.255.0

WS1-FW1(config-if)# security-level 80

The interface that point to Workshop LAN are configured using the following **commands:**

WS1-FW1(config)# interface GigabitEthernet 0/1

WS1-FW1(config-if)# no name

WS1-FW1(config-if)# no ip address

WS1-FW1(config-if)# interface GigabitEthernet 0/1.112

WS1-FW1(config-if)# nameif WS1

WS1-FW1(config-if)# ip address 172.16.112.1 255.255.255.0

WS1-FW1(config-if)# security level 100

WS1-FW1(config-if)# interface GigabitEthernet 0/1.113

WS1-FW1(config-if)# nameif WS1WIFI

WS1-FW1(config-if)# ip address 172.16.113.1 255.255.255.0

WS1-FW1(config-if)# security level 100

WS1-FW1(config-if)# interface GigabitEthernet 0/1.114

WS1-FW1(config-if)# nameif WS1PRINTERS

WS1-FW1(config-if)# ip address 172.16.114.1 255.255.255.0

WS1-FW1(config-if)# security level 100

Almost the same configurations are applied for WS-FW2 firewall cluster, but there the device addresses on the subinterfaces pointing to factory LAN end with three as in the example:

WS2-FW1(config)# interface GigabitEthernet 0/0.3

WS2-FW1(config-if)# nameif SERVERS

WS2-FW1(config-if)# ip address 172.16.3.3 255.255.255.0

WS2-FW1(config-if)# security-level 80

The subinterfaces that point inside Workshop 2 LAN are configured for its VLANs: WS2, WS2Wifi and WS2Printers.

5.4 Routing

For inter-vlan routing, so that the traffic can pass between different VLANs configured on the subinterfaces on a single physical port, the following commands are issued:

WS1-FW1(config-if)# same-security-traffic permit interinterface

WS1-FW1(config-if)# same-security-traffic permit intrainterface

For the FW1-FW2 cluster, the default route to the Internet is configured. Also, routes towards Workshop 1 and Workshop 2 LANs are statically defined.

The default route on FW1-FW2 cluster towards the Internet is:

FW1(config-if)# route OUTSIDE 0.0.0.0 0.0.0.0 229.10.105.1

where 229.10.105.1 is the address on the ISP device that faces this network.

Static routes to declare how to reach WS1 and WS2, their Wi-Fi and printers networks are the **following:**

WS1-FW1(config)# route OFFICE 172.16.112.0 255.255.255.0 172.16.100.2

WS1-FW1(config)# route OFFICE 172.16.113.0 255.255.255.0 172.16.100.2

WS1-FW1(config)# route OFFICE 172.16.114.0 255.255.255.0 172.16.100.2

WS1-FW1(config)# route OFFICE 172.16.115.0 255.255.255.0 172.16.100.3

WS1-FW1(config)# route OFFICE 172.16.116.0 255.255.255.0 172.16.100.3

WS1-FW1(config)# route OFFICE 172.16.117.0 255.255.255.0 172.16.100.3

Default routes are configured for WS1 and WS2 firewalls as follows:

WS1-FW1(config)# route OFFICE 0.0.0.0 0.0.0.0 172.16.100.1

Similar configurations are needed to be applied to all other firewalls of the network.

5.5 Access Control List

For testing and planning environment, a rule that allows a host in the main office

with IP address 172.16.100.48 to have RDP access to a server (172.16.112.22) in workshop 1 was configured on the WS1-FW1 in the following way:

WS1-FW1(config)# access_list RDP_IN extended permit TCP host 172.16.100.48 host 172.16.112.22 eq 3389

The access list is applied to the Office interface as follows:

WS1-FW1(config)# access-group RDP_IN in interface OFFICE

Following the same manner, access lists are needed to be configured for WS1-FW2.

5.6 Network Address Translation

Nat rules are applied only on FW1-FW2 in order to provide Internet access.
For each subnet a network object needs to be created. As an example
configuration for Office and Wi-Fi subnets is the following:

```
WS1-FW1(config)#object network OFFICE
WS1-FW1(config-object-network)# subnet 172.16.100.0
255.255.255.0
WS1-FW1(config-object-network)#nat (OFFICE,OUTSIDE) dynamic interface
WS1-FW1(config)#object network WIFI
WS1-FW1(config-object-network)#subnet 172.16.108.0
255.255.255.0
WS1-FW1(config-object-network)#nat (WIFI,OUTSIDE)
```

dynamic interface Similar configurations are needed to be performed for other subnets