International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V71I4P204

Volume 71 Issue 4, 29-46, April 2023

Original Article

Information Security: Proposal for a VLAN Network Model

Carmen Liliana Rodas Cortijo[1], Daniel Llallahue Callañaupa[2], Laberiano Andrade-Arenas[3], Michael Cabanillas-Carbonell[4]

[1,2]*Facultad de Ingeniería de Negocios, Universidad Privada Norbert Wiener, Lima, Perú*
[3]*Facultad de Ingeniería, Universidad Tecnológica del Perú, Lima Perú*
[4]*Facultad de Ingeniería, Universidad Privada del Norte, Lima, Perú*

[4]*Corresponding Author : mcabanillas@ieee.org*

Received: 15 October 2022 Revised: 16 March 2023 Accepted: 01 April 2023 Published: 25 April 2023

Abstract *- This article consists of the implementation of a VLAN network in the Hospital Central FAP. The objective is to increase information security, as well as to improve and optimize user data, and this is achieved through the development and use of different protocols, restrictions, and methods that helped to achieve this purpose. Likewise, the article uses the Top-down methodology, which has phases focused on analyzing, developing, and improving the different processes for designing and implementing a VLAN network topology. As a technique, an interview was conducted with the person who, through a series of questions, expressed their opinion on the hospital's problems under study. Data processing was carried out at a qualitative level using Atlas Ti22 software, which allowed the analysis of the perception of 6 people with direct knowledge of the hospital's problems. This information was used to obtain the data for the research work. The result was a high degree of deficiency and disagreement with the system they are currently using. They explained that their data were violated, generating concern among users and all the staff. In addition, the conclusion obtained was that in view of the existing problems, the experts indicated that the proposal related to the implementation of a VLAN Network would meet the desired expectations, providing security to the information, so they consider it a feasible and appropriate option that would be a great alternative for the improvement of the hospital.*

Keywords *- Atlas Ti22, Information security, Network topology, Top-down methodology, VLAN Network, VLSM.*

1. Introduction

This article used the Top-Down methodology, which consists of dividing the problem into subproblems and these, in turn, problem into subproblems and, in turn, dividing them into smaller subdivisions, which allowed them to be solved in a simpler way [1]. The use of this methodology helps to find solutions in a faster and more efficient way. Faster from the division of the smaller problem to the main problem.

The high demand for Internet use by various companies in Italy has raised concerns about data security due to the misuse of the network [2]. For this reason, a virtual LAN (VLAN) access control list has been designed, explaining that by means of this VLAN access control list, it was possible to filter and identify the users that can access the company's information and protect its data by improving security [3].

The creation of VLAN was to provide improved service and avoid local area network (LAN) traffic. Protocols were used to avoid converged connections; the aim was to create virtual VLANS networks, which allow accreditation of whether or not the user can access the network. Finally, a system was implemented to report possible threats to personnel using the network [4].

In order to share information securely or the other way around, the configuration of the LAN topology and firewall must be taken into consideration when designing the LAN topology [6], is to be able to improve the security levels of PCs when using a local network. Therefore, VLANs must be configured when connecting one computer to another [7].

The problem of cybercrime in Peru increased at the beginning of this decade. Easy access to technology and the country's socioeconomic conditions have made it an ideal place to commit cybercrime and fraud. On the other hand, the agents involved, such as the police, are often at a disadvantage, as they do not have the necessary infrastructure to combat these crimes or the capacity to use Information and Communication Technologies [8]. In Lima, communication networks are used to connect and control

computer systems. Therefore, it is inferred that using these wireless communication networks increases the vulnerability to cyber-attacks, being the servers and devices connected to the network that are exposed to these cyber-crimes. For this reason, security protocols that ensure the reliability of the data that the company wants to protect are very important [9].

Through the analysis and evaluation carried out, and seek to provide the security needed by the hospital, located in the district of Miraflores, whose problem is mainly focused on the issue of insecurity and exposure of data information. It has been analyzed that the networks they are using are not the most adequate. Therefore, have suggested the implementation of VLAN [11]considering that the data security would be more protected according to the studies carried out during the research process. At the same time, have examined the security that each area of the hospital should have in order to prevent information from being exposed to third parties [12]; have verified the vulnerability of the system currently used by the hospital and major deficiencies that have been observed over the last few years. Complaints from both staff and users, considering that the system is obsolete compared to other hospitals in Lima. In short, they do not use security protocols or topology in accordance with today's technology [13].

The objective of the work is to design the topology of the devices to be used in the VLAN network, which was to ensure and optimize both security and information, respectively, being used in the hospital under study. It is intended to achieve this improvement through the use of free software. This meant a great advance and growth of the hospital, benefiting the staff and users who come daily to this hospital—becoming an A1 hospital regarding information security levels.

The article is made up of sections. In section 2, the literature review; in section 3, the methodology was applied, in section 4 results, in section 5 discussions, and finally in section 6 conclusions and future work.

2. Literature Review

The research topic of this article aims to protect the security of the hospital's information. When detecting a network vulnerability problem, propose using free data protection software. Likewise, to be able to maintain better communication between the offices and the various areas with which it has, which are more fluid, where there is greater control and data protection of staff, users and facilities.

According to Gentile et al.[15], the current demand for the use of wireless networks used for remote work or research sites has grown. The current health problem of the COVID-19 pandemic has reflected this. This leads to the search for higher speed and higher quality broadband connections, increasing Virtual Private Network (VPN) connections and reducing costs. In addition, one must consider the problems that may arise in terms of security and must find possible solutions to these problems.

According to the author[16], the company has a clear vision of the trends in terms of technical issues and major advances, allowing people to create new environments that can access the use of technologies, either privately or at work. Through this was access to interact with others and communicate on a large scale, thanks to social networks that currently have great access. Companies must have a security system that helps them to have a plan that avoids any situation of vulnerability that could expose them. Therefore, this article tries to prioritize and clarify the concepts about security issues.

According to authors [17], it is directly focused on increasing the security levels that a network must have. For this reason, VLANs were implemented to ensure that the data can reduce the time in the file transfer process, for which equipment that meets the customer's requirements was needed. For this reason, tests were performed to ensure the information was shared between the same nodes and had the same logic. Ultimately, this led to streamlining the network.

According to Leyva et al. [18], its main objective is to observe how secure the LAN networks of the companies that provide Internet services are. By means of a study, it was possible to show the methods that access the bibliographic and statistical review of the data and those used in the survey. For the information collection, they were applied to managers of the companies that provide such services and to users. The results showed that the company complies with the established rules, following protocols in the use of firewalls, due to the fact that the main attacks produce negative effects.

According to Tareq and Muhannad [20], this research shows the characteristics a LAN should have and the operation of a VLAN. This allowed us to improve the performance and security of a company or university network. In addition, a bibliographic study was carried out to understand what the virtual local area network consists of. Also, for this study, it was necessary to use switches with VLAN support and computer equipment that works as a server. In the end, the results obtained were satisfactory both in terms of security improvements and in creating access rules for each virtual network and the Internet, all through the use of the firewall.

According to the authors [21], the company states that wireless networks bring a lot of convenience to people's daily lives, but many security problems still need to be solved. This is the most critical since it is relatively easy to breach

security and steal information from individuals and organizations. Therefore, the recommendation is to encrypt the information sent over the network by means of an algorithm, which significantly improves the user's reliability. However, it should be noted that encryption by means of algorithms in wireless networks is a somewhat costly task, depending on the level of complexity to be achieved.

The author [22] mentions that a network is of utmost importance to be able to share information from one computer to another. Those that must be connected to the same network, applying the design and structure of a VLAN to reduce traffic and insecurity in the network. It also highlights that the VLAN, being a virtual local area network, allows several networks to work with the same LAN. Therefore, to increase performance and reduce device domains. Finally, it is inferred that VLANs help manage the transit of information in a network, being seen as the division of smaller and isolated networks to ensure the reliability and security of the user with respect to the information handled within the LAN.

According to the author Fahri et al. [23], the LAN can obtain the structure of a VLAN network using virtualization, this being made possible by a certain structured configuration for this purpose. Also, this virtualized network would have several control parameters for information management, better known as protocols. Therefore, in most cases, the virtual configuration is done by means of a network controller, and the computer itself must own this controller. This would help reduce packet loss to 0% in most cases that it is used.

According to the author Silva et al. [24], before making any changes to the VLAN structure, one must first consider the configuration of both the firewall and the logical network topology. The topology is of utmost importance since it analyzes the set of characteristics and protocols to be managed on the LAN. On the other hand, networks are usually configured by means of a switch or router in order to configure the packets that users have access to at different specific points of the network. The purpose of this is to select the information and make a sub-network only able to access specific information. At the same time, the other sub-networks were only limited to working with their information.

According to the author, Ayuningtyas et al. [26] argue that VLAN is one of the environment's most valued and used technologies. Being the same possessor of a management system based on user command lines that, through a user-friendly interface, are very useful for managing a VLAN. These, in turn, have the advantage of being modified at any time for various purposes as long as they are authorized persons.

In conclusion, great contributions from the authors mentioned in the development of this article are observed. However, note certain shortcomings in the interactivity with free software, which is why want to contribute, in which through the application of the VLAN structure in the hospital network helps to collect and reinforce knowledge regarding network security.

3. Methodology

3.1. Methodological Design

The Top-Down methodology consists of modules or phasesthat allow a better interaction, obtaining a clearer and faster solution (see Figure 1).

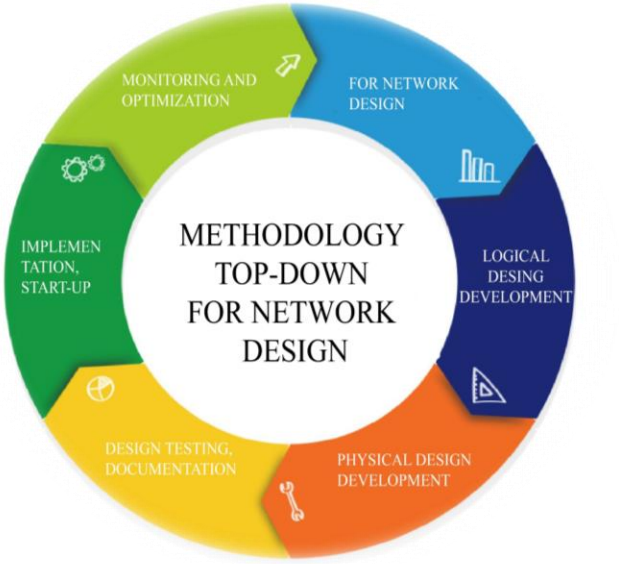

Fig. 1 Top-Down Methodology

3.1.1. Analyze Requirements

With respect to this initial phase,evaluate all the current infrastructure that presents deficiencies and poor security; this is possible thanks to the collection of information from the current network. For this, identify the objectives of the business or company and the necessary requirements of the stakeholders in the new network [27]. Likewise, it is important not to disregard the different analyses that this phase should include, such as the analysis of the network, business, goals, and information traffic, which allowed the design of the topology to be elaborated most meticulously and accurately possible for the stakeholders of the new network.

3.1.2. Develop Physical Design

For this phase,a physical and technological structure is evaluated and proposed; this refers to the equipment needed to be implemented in the design, be it brands, devices, computers, or cables, among others [28]. Likewise, the most efficient and new technology that works according to the topology and devices within the new network was considered.

3.1.3. Develop Logical Design

Regarding this phase, the logical structure of the design is elaborated here, focusing on the information obtained in the previous phase. Therefore, in this phase, the design of the network topology is presented, as well as different protocols, restrictions, and security firmware used for the correct operation and security of the actors of the new hospital network [30]. Also, some relevant aspects are appreciated in this phase, where finding the network topology design with the VLAN protocol is worth mentioning.

3.1.4. Test, Optimize, and Document Design

Network design is a process linked to the company's needs with the technology used. As it is known nowadays, the fulfillment of the objectives by employing an adequate methodology with a flexible network architecture that allows obtaining optimal results according to the needs of the company and the technology to be used [32], in which he refers that communications infrastructures are important for the correct performance and competitiveness of an organization.

3.1.5. Implement and Test the Network

As we know, the challenges when designing networks for automation generate certain problems in the implementation of the various applications or the need for networking in terms of real-time security systems, as Silva et al. [24], the generalization of protocols, the interconnections of computers, it could be observed that it did not meet the needs that were sought. That is why a series of changes have taken place that led to the technological revolution.

3.1.6. Monitor and Optimize the Network

In this phase, the aim is to ensure that each of the implemented processes works correctly, most efficiently and safely for the satisfaction of the network stakeholders according to the proposed model, as stated by Astika et al. [26], in which the result of monitoring the network was the result of integrating and performing all the evaluations and tests showing how the network was being improved and how it works over time.

4. Result

4.1. Validation by Expert Judgment

The expert judgment was applied to 4 professionals, and 8 criteria were considered, being these evaluated from 1 as deficient and 10 as excellent; in addition,1 was interpreted as 10% and 10 as 100%. Whose passing score had to be greater than 75%.

4.1.1. Criteria Analysis

For the preparation of Table 1, worked on 8 criteria, each one of which fulfills the functionality required to develop the network implementation. These were evaluated by 4 experts: the Security and Information Technology Technician, the Network and Communications Technician, the Information Technology Technician, and the Systems Engineer (See Table 1). The criteria considered are the following:

Usability

Referred to the ease with which users can securely use the network. According to the table, the average obtained by the experts was 79%.

Quality

Because it has the ability to meet the needs of both staff and patients. The overall average obtained in the table is 85%.

Scalability

It allows one to go up from an A technology and move to an A +1 technology by leveling up because it can be scalable. In this criterion, 86% was obtained.

Innovation

Considered an innovative proposal due to the advantages and benefits offered by the implementation of the VLAN. The percentage obtained is 90%.

Table 1. Expert Judgment table

Criteria	Question	Expert 1	Expert 2	Expert 3	Expert 4
Usability	Is the VLAN implementation easy to use?	80%	80%	75%	80%
Quality	Is the expected quality of the topology met?	90%	85%	90%	75%
Scalability	Is the VLAN implementation scalable?	80%	90%	90%	85%
Innovation	Do you consider VLAN to be new for HCFAP?	90%	90%	95%	85%
Technology	Does the VLAN feature quality software and hardware?	80%	86%	90%	85%
Efficiency	Does VLAN improve effectiveness and streamline processes?	90%	75%	89%	85%
Functionality	Does the implementation meet the expectations?	90%	80%	80%	90%

Technology

The tools and resources used to combine and transform the current process to an improvement after implementation. The overall average obtained by the experts is 85%.

Efficiency

When we talk about this criterion, we refer to performance. The average obtained is 85%.

Functionality

The set of features makes the VLAN implementation functional and practical. The percentage was 85%.

Authenticity

This criterion is defined as the originality and coherence of the topology design; the percentage of the total average was 85%. The average required by experts was reached, being greater than 75% of the total obtained in each of the questions asked, which were related to the criteria considered for the Topological Design of the VLAN Network.

4.2. Interview Analysis Using Atlas TI

The interview previously conducted, evaluated by means of categories, sub-categories, and indicators by means of Atlas TI software, which helped us with the qualitative analysis of the interview that was conducted with 6 people who are part of the hospital as workers as well as specialists in the field, each of them answered 7 questions related to the network they currently use and also proposing the idea of implementing a new VLAN network (see Table 2).

Innovation sub-category: On VLAN Innovation, the interviewees emphasized the deficiency in which they indicated that several inappropriate aspects should be changed for having an obsolete network that does not allow them to that several inappropriate aspects should be changed due to an obsolete network that does not allow them to carry out their daily activities. The changes made have been minimal.

The changes that have been made have been minimal [33]. Every day there are complaints, in addition to the excessive waiting time when exchanging waiting time at the moment of exchanging information, generating discomfort. Regarding viability, they are of the opinion that security would improve as well as the structure if the change were to take place. In terms of novelty, as it is a very useful idea, the new network would be beneficial because it would provide better service (see Figure 2).

4.2.1. Sub-Category Structure

Regarding the sub-category Structure, the interviewees initially mentioned security, for how vulnerable the hospital's current network is and how safe it could be with the change to a new network with more security protocols. The current network is obsolete, generating discomfort and annoyance among users; if a change were to be made, it would be efficient. They consider that, at present, they feel very insecure. In terms of feasibility, it would help provide adequate information to patients and workers who would have real-time information. The new structure would bring about a noticeable improvement for everyone. Vulnerability is an important issue because they think their data is exposed. If the network under study were implemented, they would feel more secure (see Figure 3).

Table 2. Interview Information Table

Category		Sub-category		Indicators	
Code	**Name**	**Code**	**Code**	**Code**	**Name**
1	Implementation of a VLAN network	1.1	Innovation	1.1.1	Innovative
				1.1.2	Deficiency
				1.1.3	Feasibility
		2.1	Structure	1.2.1	Vulnerability
				1.2.2	Security
				1.2.3	Feasibility
		3.1	Technology	1.3.1	Efficiency
				1.3.2	Quality
				1.3.3	Reliability
		4.1	Satisfaction	1.4.1	State of mind
				1.4.2	Productivity
				1.4.3	Comfort

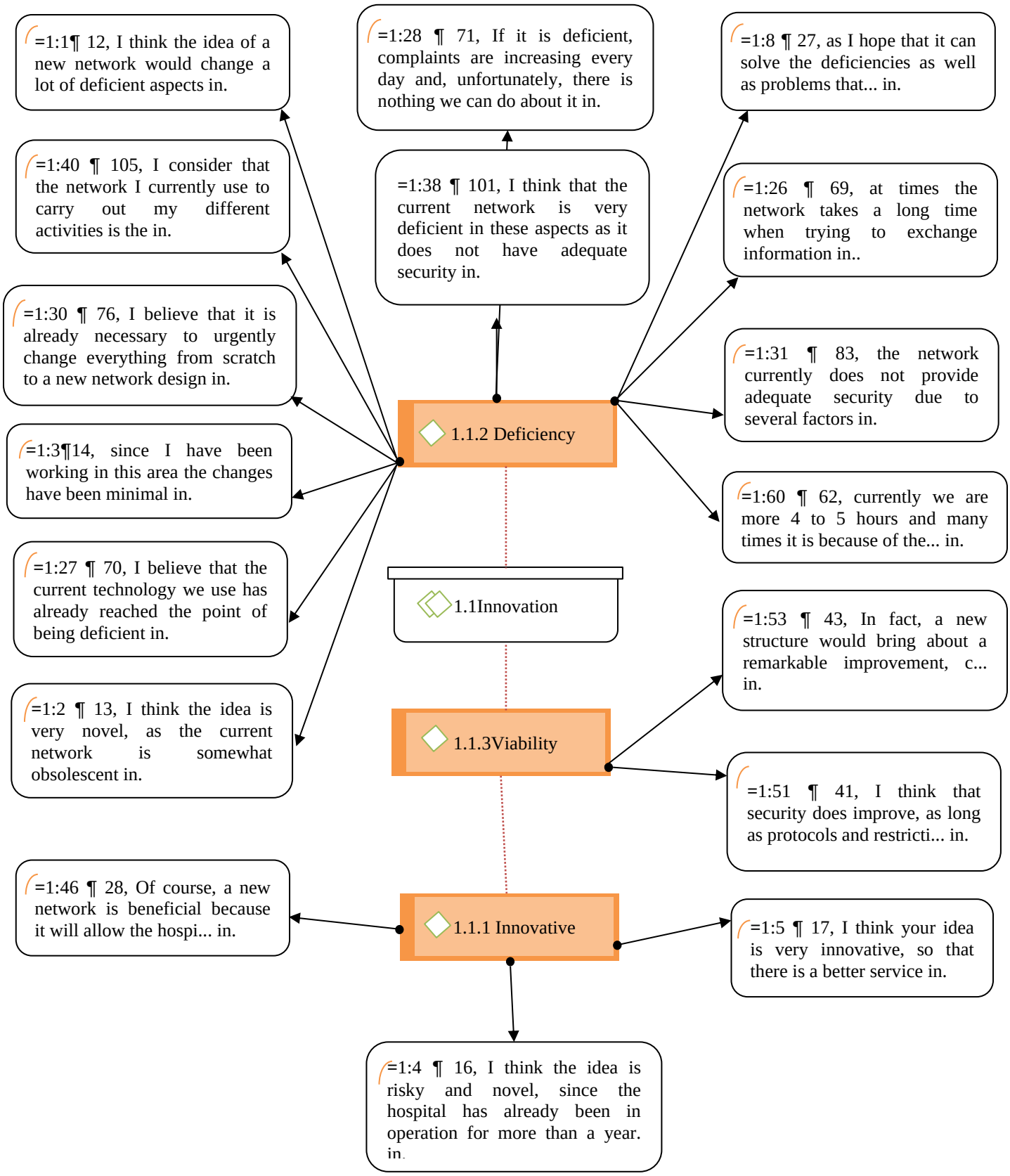

Fig. 2 Innovation sub-category

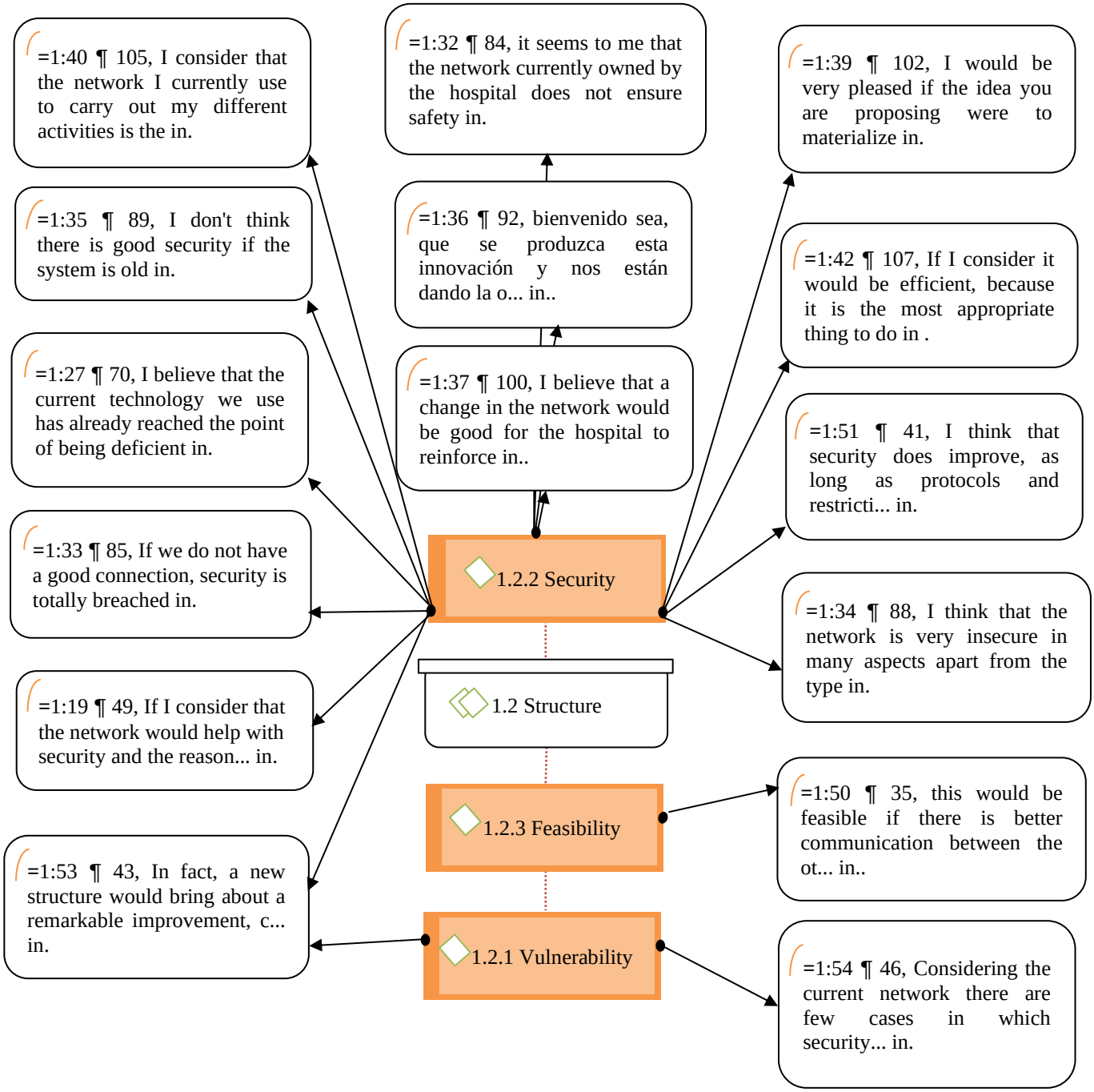

Fig. 3 Sub-category Structure

4.2.2. Technology Sub-Category

The analysis of the Technology sub-category is composed of three indicators, efficiency because it would streamline activities and information in the hospital environment, this being the most appropriate. Therefore, based on this interview can affirm that the hospital must take on the challenge of a new implementation with a new network which has the protocols and other parameters that ensure the comfort and integrity of the hospital's users reliability [34], is an important point to mention because nowadays security is very necessary, it is also worth mentioning that the indicator for the quality allows to leave aside the slow and obsolete system, to opt for a new one that allows to carry out the activities in a more efficient way. Activities in a more efficient, safer, and less error-prone way (see Figure 4).

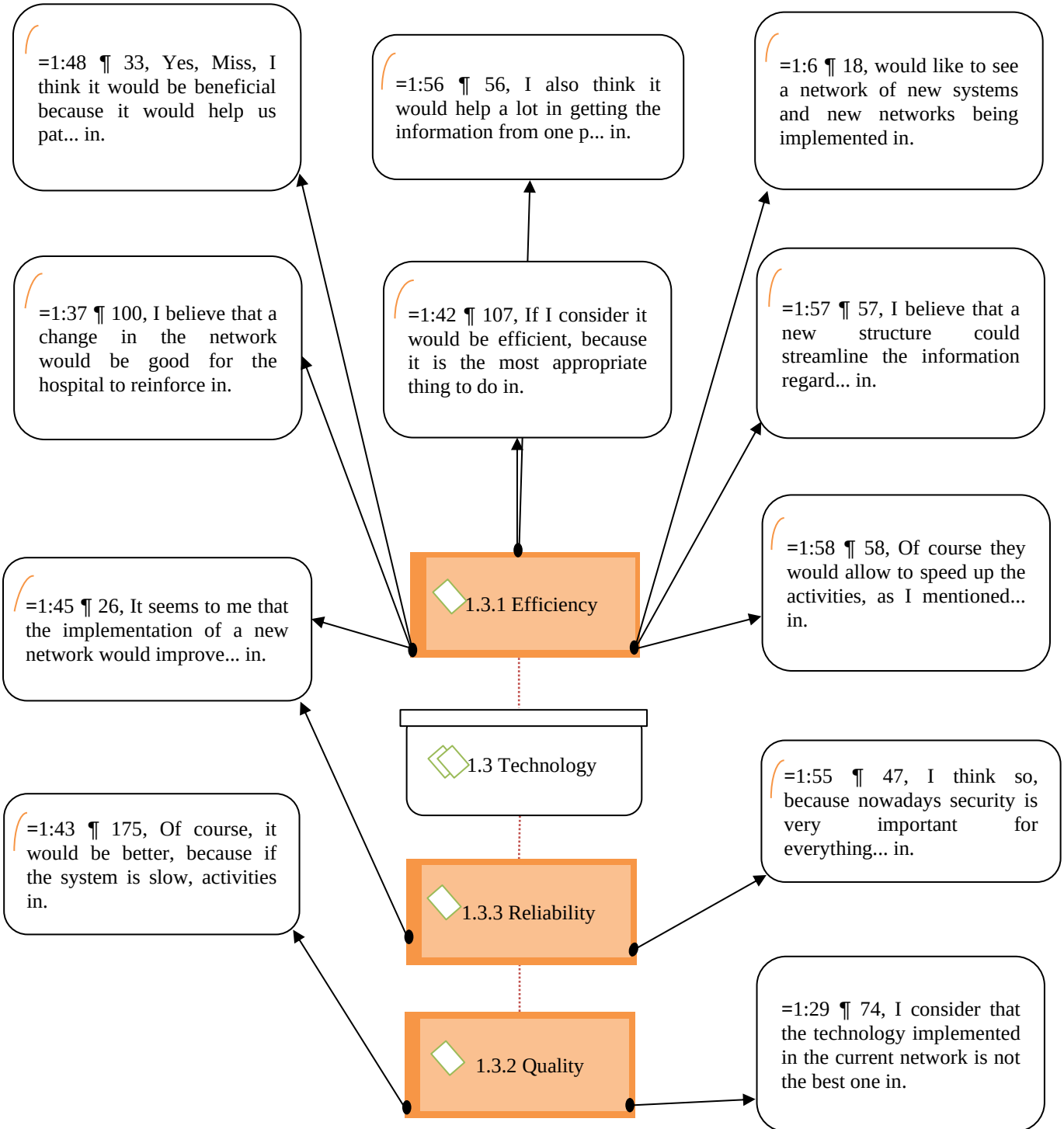

Fig. 4 Technology sub-category

4.2.3. Sub-category Satisfaction

Regarding the Satisfaction analysis, the interviewees indicated that the new proposal is ideal because the current system is slow. It is a good proposal, which would improve the attention and work of both staff and users. The mood would improve notably; there would be no more annoyances or complaints, as is the case daily. Finally, the productivity indicator would contribute to speeding up information times and performance (see Figure 5).

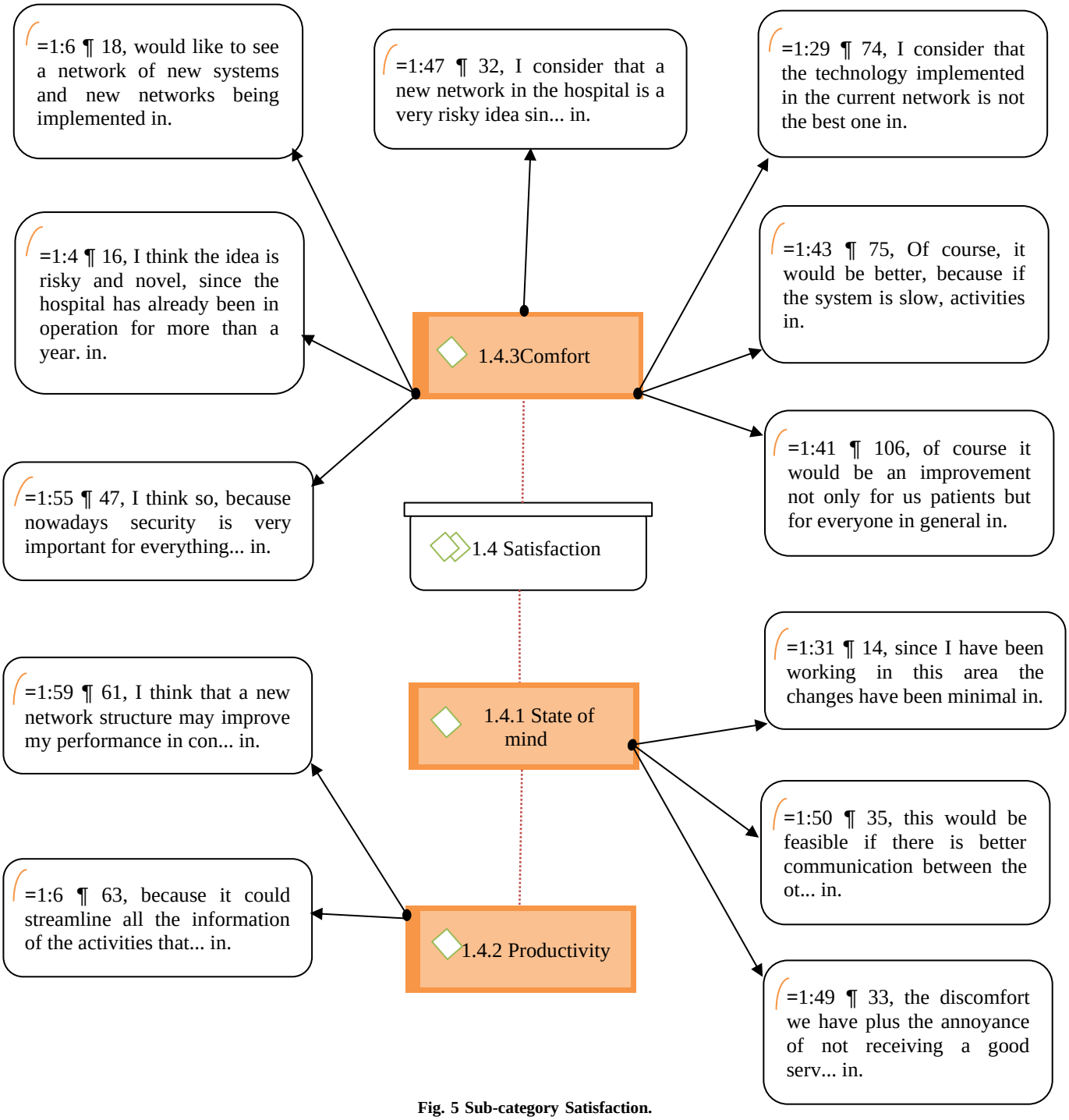

Fig. 5 Sub-category Satisfaction.

4.3. About Methodology

4.3.1. Physical Design Development

Based on the second phase, where the physical topology was designed, following up on that phase, we designed the logical topology in which we evaluated the needs and advantages of using a VLAN network, so we designed a topology according to those requirements and design of the hospital because it has 4 main areas, which are distributed on different floors. Therefore, the topology includes the customer service nursing, medical staff, and pharmacy areas (see Figure 6).

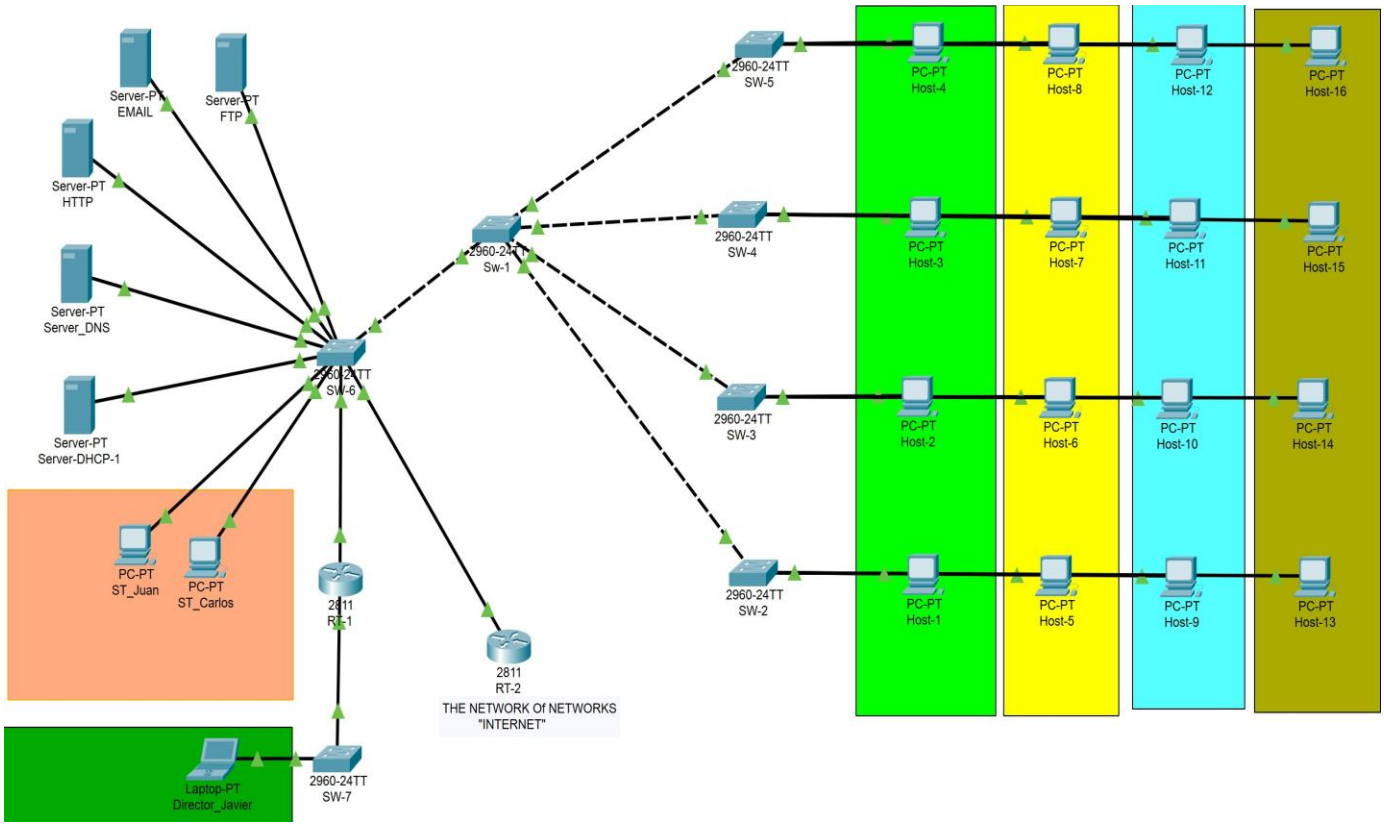

Fig. 6 Physical Design of The Topology

Logical Design Development

Based on the first phase, where the requirements were analyzed, it was possible to evaluate the needs and advantages of using a VLAN network; that is why a topology was designed according to the devices, switches, and routers that were be interconnected in the network, as well as the different servers and types of cables that was be needed for the interconnection of the network(See Figure 7).

Design Documentation Development

In this case, we are using the Canvas Model as a tool that allows us to capture the idea of a model, which is validating as developing the ideas and suggestions that customers have, who are contributing their ideas according to the needs of the company or organization. Each Canvas Model element contains enough information to bring the company to life in simple terms that make it easy to understand. This method allows us to speak the same language clearly and precisely. Each of the steps allows us to develop visual techniques. Finally, this was allowed to create opportunities and new challenges (see Figure 8).

Network Implementation and Testing

Having already designed and implemented the VLAN network in the hospital, proceed to test the different servers and the connectivity and functionality of the connected devices. Also, appreciate the different parameters that work as well as the configuration that it has. On the other hand, the servers are worked individually by default in this case, since to save costs could use several services on the same server. This could happen if the server in the hospital does not handle so much information or work with so many services simultaneously. It is advisable to establish these factors to consider not to have any inconvenience when using the topology (See Figure 9, Figure 10, Figure 11, and Figure 12).

Regarding security, the topology uses the VLAN protocol, which allows for isolating and disabling ports that were not used to prevent possible intruders from entering the network. On the other hand, the administrator is the only one in charge of the configuration who could disable and enable the ports considered necessary. Another security aspect that is provided is related to the configuration of users and passwords, thus preventing the entry of any person who is not authorized by the administrator and restricts any type of access to the configuration information and code (see Figure 13, Figure 14, Figure 15, Figure 16).

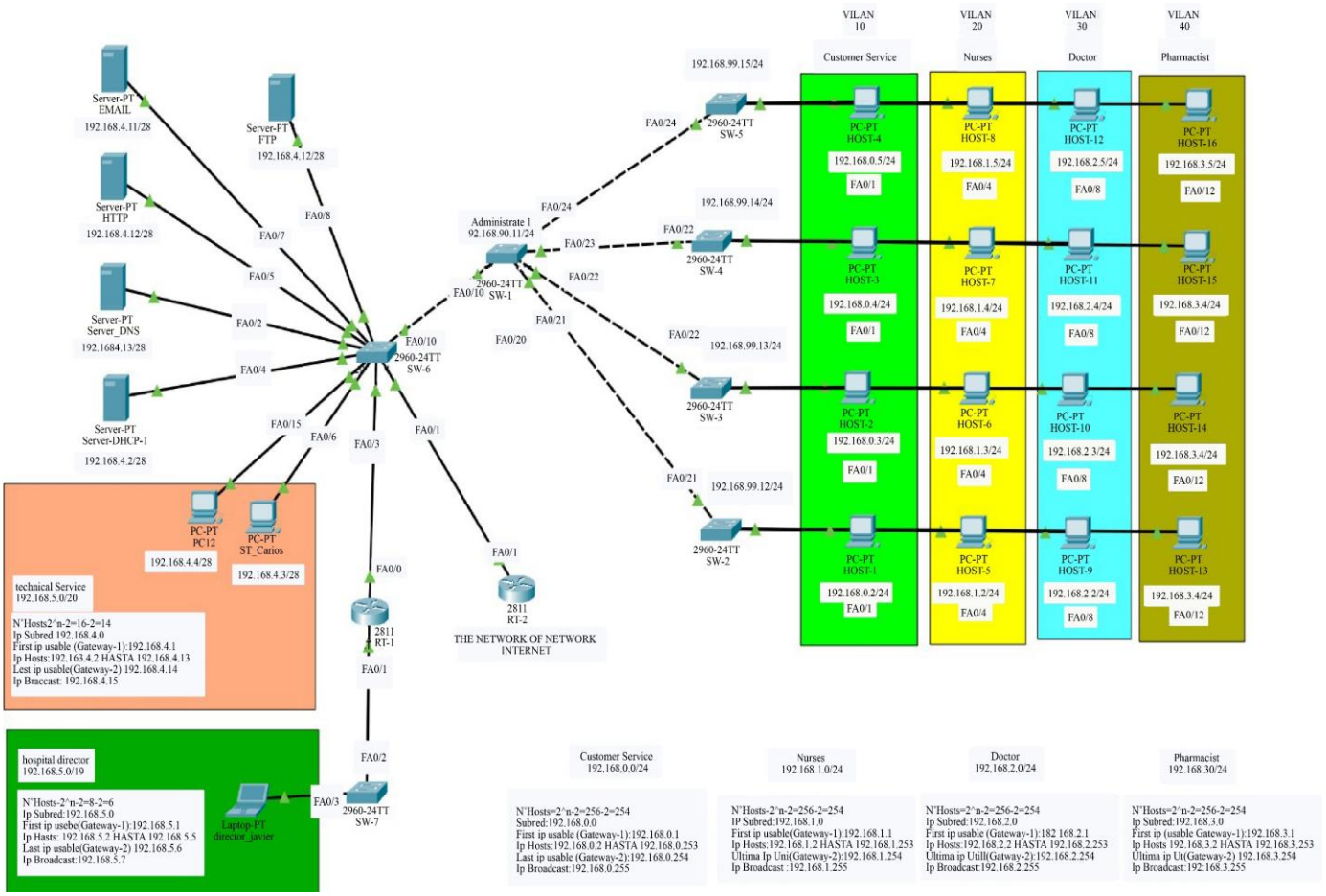

Fig. 7 Logical Design of The Topology

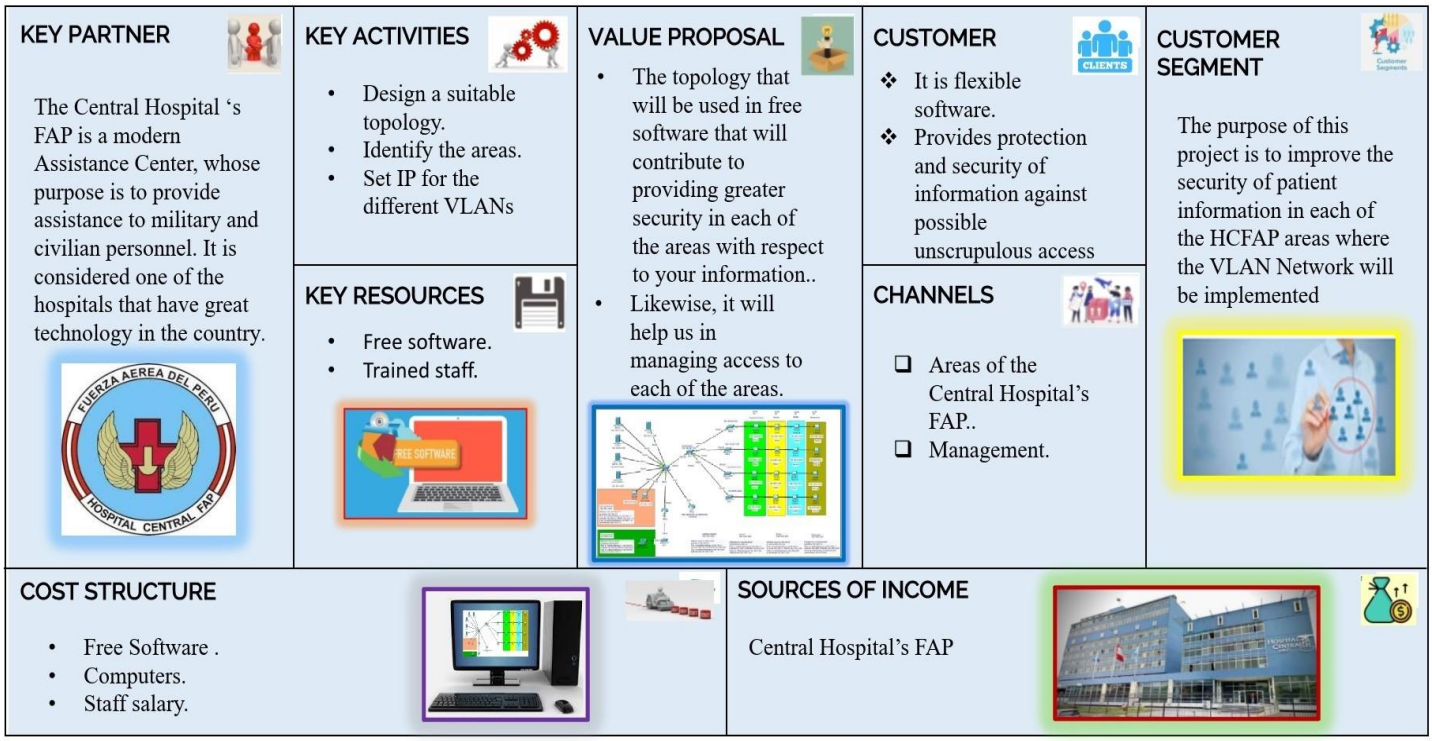

Fig. 8 Canvas Model

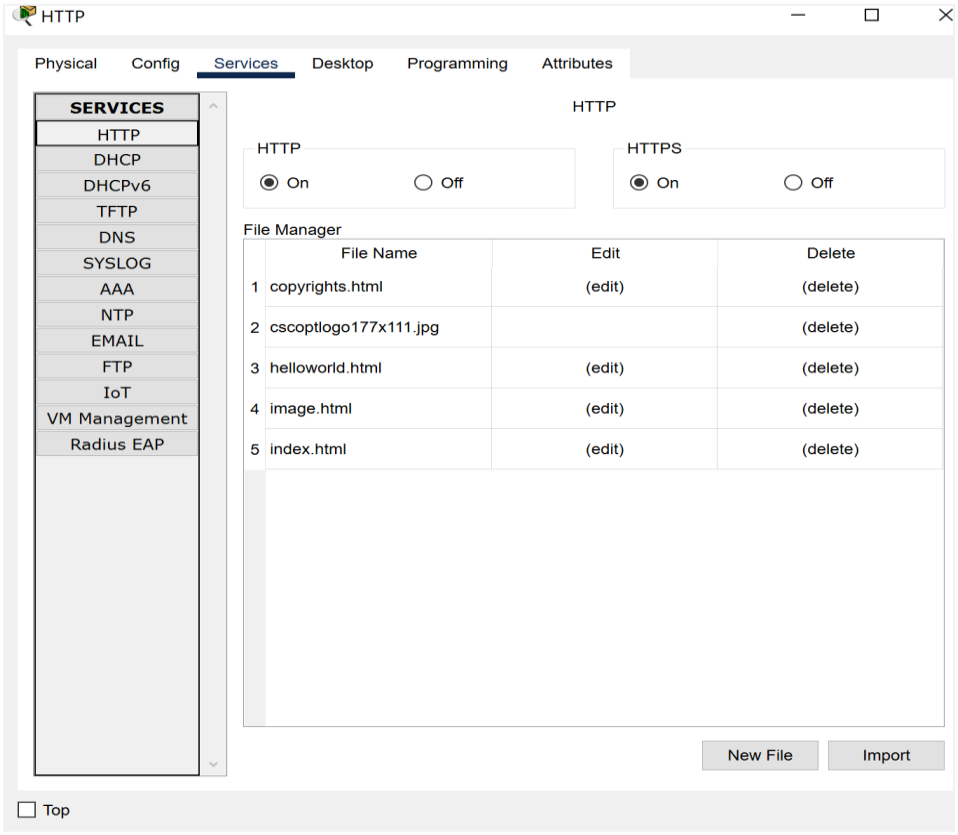

Fig. 9 Web Site Configuration.

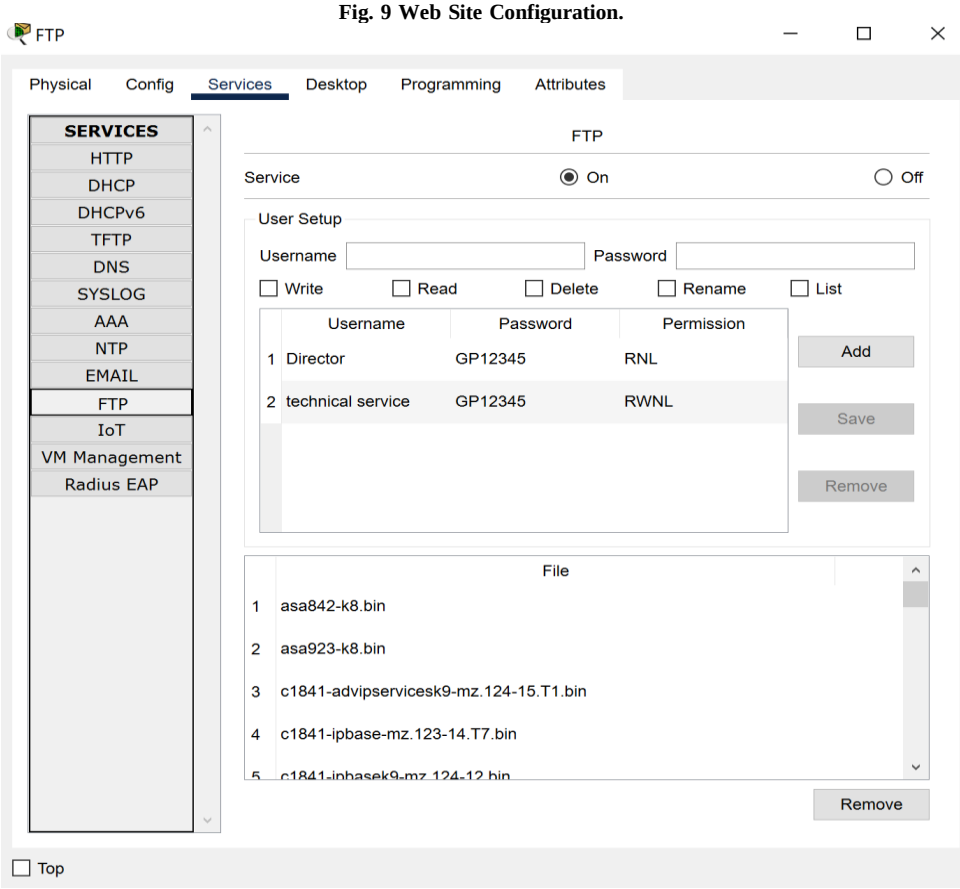

Fig. 10 FTP Server Configuration

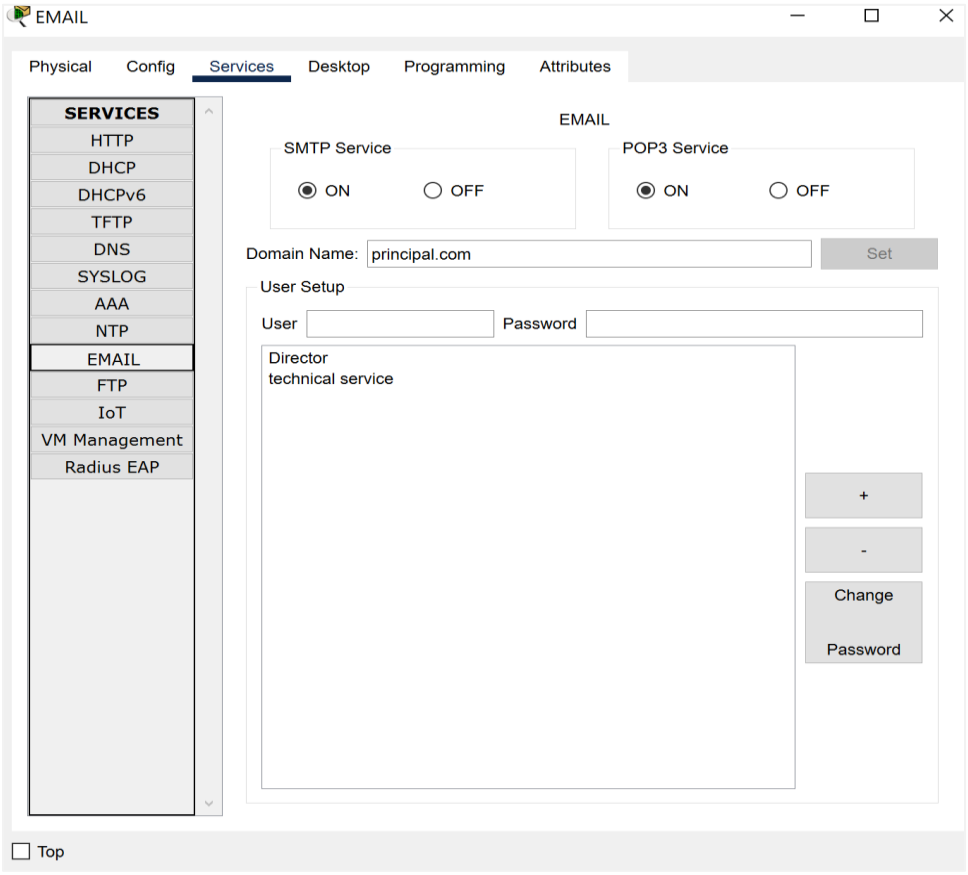

Fig. 11 Email Server Formatting.

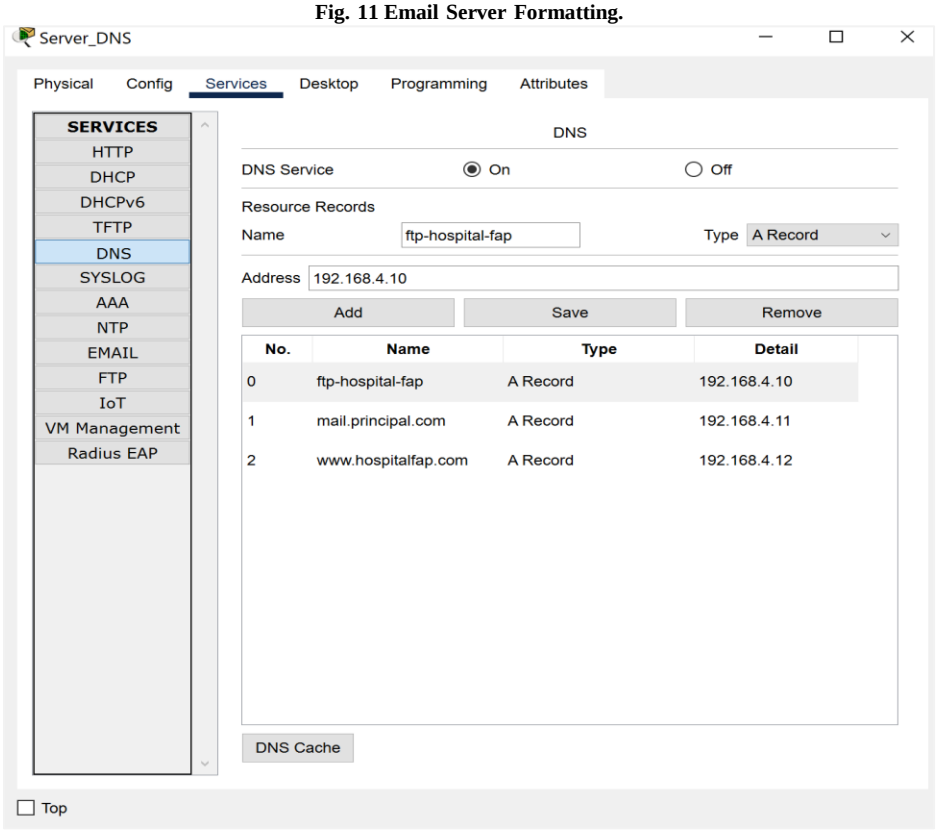

Fig. 12 DNS Server Configuration

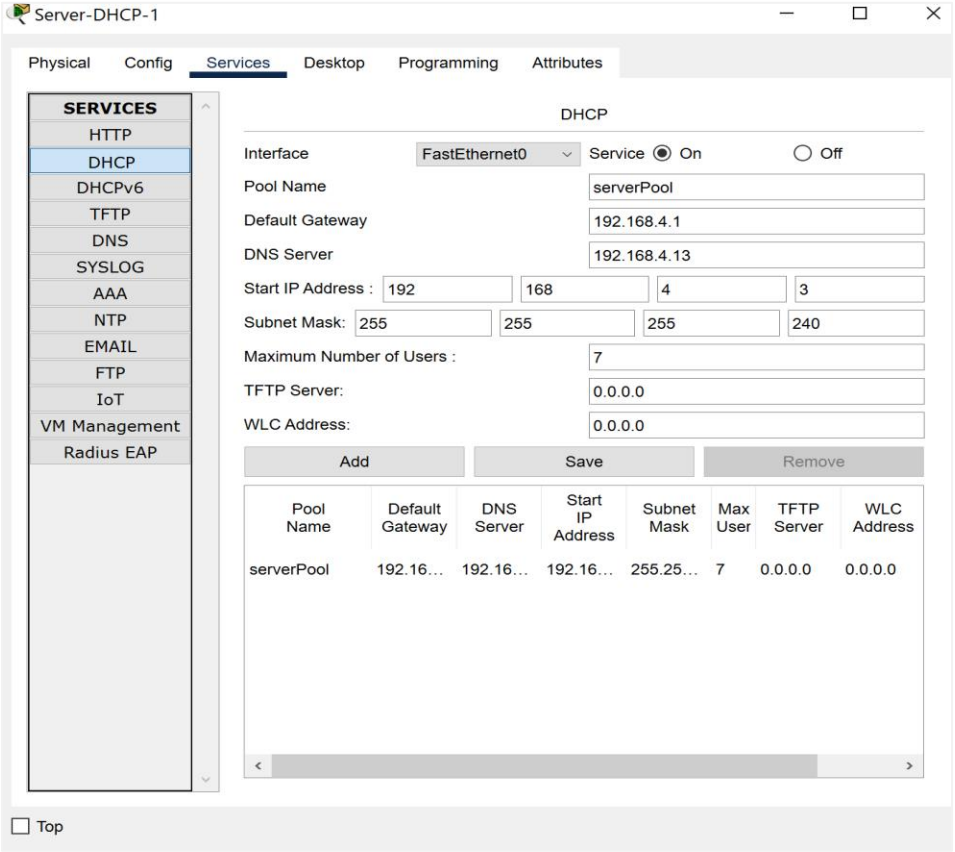

Fig. 13 DHCP Configuration

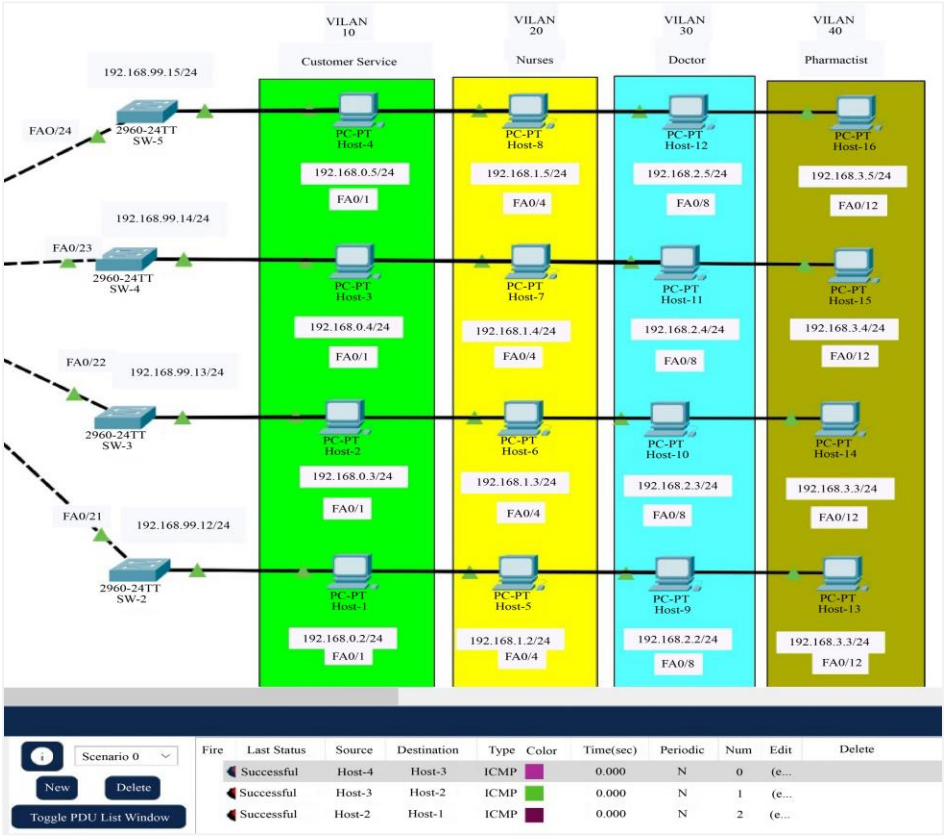

Fig. 14 VLAN Network Connectivity

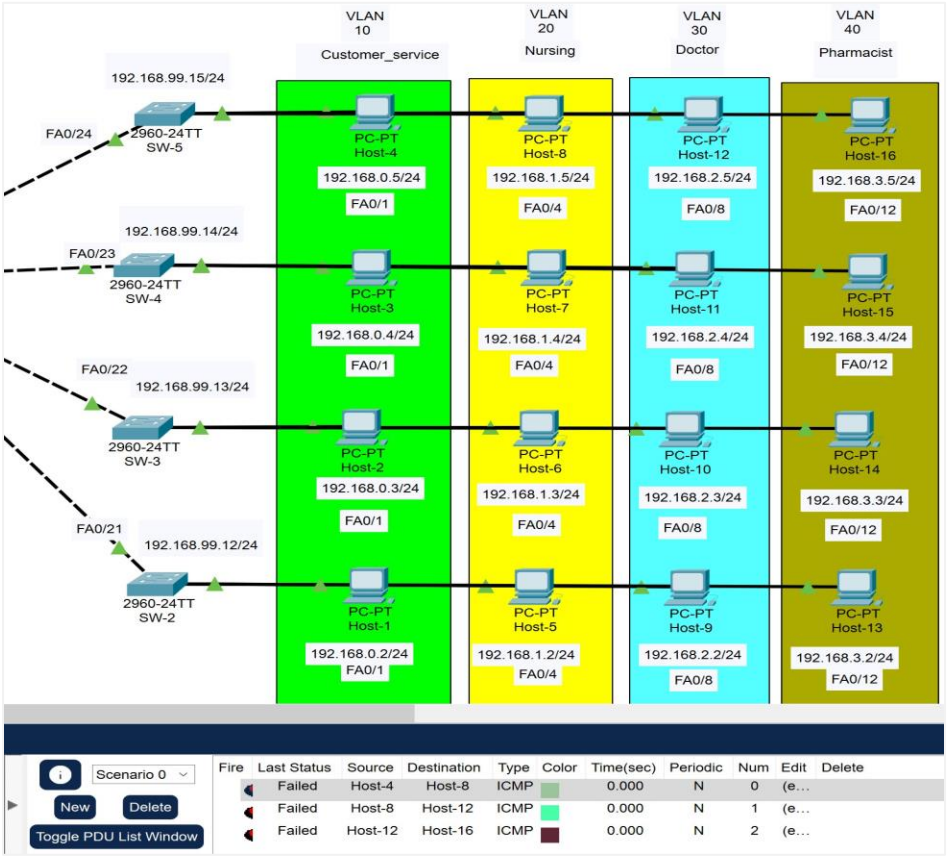

Fig. 15 Security Testing

```
Device Name: SW-2
Custom Device Model: 2960 IOS15
Hostname: SW-2

Port                Link   VLAN   IP Address         MAC Address
FastEthernet0/1     Up     10     --                 0060.47D1.1601
FastEthernet0/2     Down   10     --                 0060.47D1.1602
FastEthernet0/3     Down   10     --                 0060.47D1.1603
FastEthernet0/4     Up     20     --                 0060.47D1.1604
FastEthernet0/5     Down   20     --                 0060.47D1.1605
FastEthernet0/6     Down   20     --                 0060.47D1.1606
FastEthernet0/7     Down   20     --                 0060.47D1.1607
FastEthernet0/8     Up     30     --                 0060.47D1.1608
FastEthernet0/9     Down   30     --                 0060.47D1.1609
FastEthernet0/10    Down   30     --                 0060.47D1.160A
FastEthernet0/11    Down   30     --                 0060.47D1.160B
FastEthernet0/12    Up     40     --                 0060.47D1.160C
FastEthernet0/13    Down   40     --                 0060.47D1.160D
FastEthernet0/14    Down   40     --                 0060.47D1.160E
FastEthernet0/15    Down   40     --                 0060.47D1.160F
FastEthernet0/16    Down   1      --                 0060.47D1.1610
FastEthernet0/17    Down   1      --                 0060.47D1.1611
FastEthernet0/18    Down   1      --                 0060.47D1.1612
FastEthernet0/19    Down   --     --                 0060.47D1.1613
FastEthernet0/20    Down   --     --                 0060.47D1.1614
FastEthernet0/21    Up     --     --                 0060.47D1.1615
FastEthernet0/22    Down   --     --                 0060.47D1.1616
FastEthernet0/23    Down   --     --                 0060.47D1.1617
FastEthernet0/24    Down   --     --                 0060.47D1.1618
GigabitEthernet0/1  Down   1      --                 0060.47D1.1619
GigabitEthernet0/2  Down   1      --                 0060.47D1.161A
Vlan1               Down   1      <not set>          000D.BDB0.A165
Vlan99              Up     99     192.168.99.12/24   000D.BDB0.A101

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > SW-2
```

Fig. 16 Switch Configuration

Network Monitoring and Optimization

The implementation of this VLAN model helped to improve the security of patient information. The creation of the design has allowed us to group users by area, which made access easier for the hospital staff. This VLAN model helps to reduce possible overloads for each host on the network. It also reinforced the security of the data in a different VLAN, giving it stability and strength. Therefore, this VLAN can be considered more secure and independent in each of the sectors where it is being developed.

Network Optimization Using VLSM

VLSM (Variable Length Subnet Mask) is a method by which a network is divided into smaller and smaller subnets whose masks are different according to the needs of the hosts. VLSM allows the hospital to use more than one mask within the same network addressing space. The implementation of VLSM maximizes efficiency in the subnet division. Likewise, its implementation avoids unnecessary configurations with respect to the use of IPv4 addresses and improves the use and optimization of the addresses avoiding that only a few are wilted. As have developed throughout the work, we can affirm that the VLSM technique is of great help to et al. [27] and proposes a more suitable solution in terms of saving IP addresses (Internet Protocol address). The implementation and creation of the presented prototype were to allow control and efficiency that can be adapted in the future.

5. Discussions

In the research carried out, a high degree of agreement was obtained with the authors [15] because his study was based on the security that companies must have when protecting their data, which may be exposed to any situation of vulnerability that may affect the information of both personnel and patients. Likewise, also agree with the authors [17] in his article refers to the importance of the characteristics that a VLAN network must have, which improves the company's performance. The study agrees with the author because the project is taking one of the evaluation criteria, efficiency, which provided satisfactory results, improving security. On the other hand, we have taken these two authors because we consider that they are more related to the work of study. The others also possess a degree of similarity in the treated subject but have considered citing these two authors in particular.

6. Conclusion

According to the qualitative study, the stakeholders' opinions regarding implementing a VLAN network could be appreciated, which met the desired expectations and solved the old network's deficiencies. This is with reference to the topology design, which aims to provide security and efficiency with respect to the management of information within the Central Hospital FAP. On the other hand, consider that the TOP-DOWN methodology has contributed to the development of this project because it allowed us to analyze the deficiencies of the old network and evaluate possible actions to help us improve security and efficiency. Finally, it allowed us to design a suitable topology for the hospital. However, the topology can consider using only one server to manage all the services to reduce costs and make the network implementation in the hospital more feasible, possible if considering that the information to be stored in this server is not relatively large. Finally, suggest that this project should have new studies with respect to IPv6 since it works even better with the topology because it has better network identifiers. It also gives the host a unique address, among other positive aspects.

References

[1] Shamimul Islam et al., "Threat Minimization by Design and Deployment of Secured Networking Model," *International Journal of Electronics and Information Engineering*, vol. 8, no. 2, pp. 135-144, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[2] Fairriky Rynjah, Bronson Syiem, and L. Joyprakash Singh, "Investigating Khasi Speech Recognition Systems using a Recurrent Neural Network-Based Language Model," *International Journal of Engineering Trends and Technology*, vol. 70, no. 7, pp. 269–274, 2022. [CrossRef] [Publisher Link]

[3] Tareq Al-Khraishi, and Muhannad Quwaider, "Performance Evaluation and Enhancement of VLAN Via Wireless Networks Using OPNET Modeler," *International Journal of Wireless & Mobile Networks*, vol. 12, no. 3, pp. 15–30, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Madjed Bencheikh Lehocine, and Mohamed Batouche, "Flexibility of Managing VLAN Filtering and Segmentation in SDN Networks," *2017 International Symposium on Networks, Computers and Communications, ISNCC 2017*, pp. 1-6, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[5] Ahmed Y. Mahmoud, "A Novel Hash Functions for Data Integrity Based on Affine Hill Cipher and Tensor Product," *International Journal of Engineering Trends and Technology*, vol. 70, no. 11, pp. 1-9, 2022. [CrossRef] [Publisher Link]

[6] Holden Gordon et al., "Securing Smart Homes Via Software-Defined Networking and Low-Cost Traffic Classification," *Proceedings - 2021 IEEE 45th Annual Computers, Software, and Applications Conference, COMPSAC 2021*, pp. 1049–1057, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[7] P. Sindhu, and G. Indirani, "Equilibrium Optimizer with Deep Convolutional Neural Network-based Squeeze Net Model for Grape Leaf Disease Classification in IoT Environment," *International Journal of Engineering Trends and Technology*, vol. 70, no. 5, pp. 94–102, 2022. [CrossRef] [Publisher Link]

[8] Ricardo Flores Moyano et al., "NFV-based QoS Provision for Software Defined Optical Access and Residential Networks," *2017 IEEE/ACM 25th International Symposium on Quality of Service, IWQoS 2017*, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[9] Sesha Kethineni, "Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms," *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, pp. 305–326, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Swetha Gadde, J. Amutharaj, and S. Usha, "A Hybrid Cryptography Technique for Cloud Data Security," *International Journal of Engineering Trends and Technology*, vol. 70, no. 11, pp. 258-267, 2022. [CrossRef] [Publisher Link]

[11] Kumaresh Sheelavant, R. Sumathi, and Charan K V, "Optimal Routing and Scheduling for Cognitive Radio Sensor Networks Using Ensemble Multi Probabilistic Optimization and Truncated Energy Flow Classification Model," *International of Engineering Trends and Technology*, vol. 69, no. 9, pp. 168–178, 2021. [CrossRef] [Publisher Link]

[12] Dhurgham Abdulridha Jawad, and AL-Khaffaf, "Improving LAN Performance Based on IEEE802.1Q VLAN Switching Techniques," *Jthenal of University of Babylon for Engineering Sciences*, vol. 26, no. 1, pp. 286–297, 2018. [Google Scholar] [Publisher Link]

[13] M. Ogar-Abang, G. A. Fischer, and E. J. Akpama, "Evaluation of Network Performance for Single VLAN and Six VLANS Network," *2nd International Conference on Electrical Power Engineering*, pp. 20-24, 2021. [Google Scholar]

[14] Neha Priya, "Cybersecurity Considerations for Industrial IoT in Critical Infrastructure Sector," *International Journal of Computer and Organization Trends*, vol. 12, no. 1, pp. 27-36, 2022. [CrossRef] [Publisher Link]

[15] Antonio Francesco Gentile, Peppino Fazio, and Giuseppe Miceli, "A Survey on the Implementation and Management of Secure Virtual Private Networks (VPNs) and Virtual LANs (VLANs) in Static and Mobile Scenarios," *Telecom 2021*, vol. 2, no. 4, pp. 430–445, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] J. A. Figueroa-Suárez et al., "Computer Security and Information Security," *Pole of Knowledge*, vol. 2, no. 12, pp. 145–155, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[17] Ammar. O.Hasan et al., "A Simulation of Wireless Computer Network Salahaddin University Campus of FTP Using OPNET Simulator," 2017. [Google Scholar]

[18] Nelly Victoria Ley Leyva et al., "Effectiveness and efficiency of LAN network security. Cantón Pasaje," *Society & Technology*, vol. 4, no. 2, pp. 205–222, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] Vencelin Gino V, and Amit KR Ghosh, "Enhancing Cyber Security Measures for Online Learning Platforms," *SSRG International Journal of Computer Science and Engineering*, vol. 8, no. 11, pp. 1-5, 2021. [CrossRef] [Publisher Link]

[20] Tareq Al-Khraishi, and Muhannad Quwaider, "Implementation of VLAN via Wireless Networks Using Opnet Modeler," *Computer Science & Information Technology*, pp. 57–72, 2019. [CrossRef] [Google Scholar]

[21] Chen Liang et al., "Research on Neural Network Chaotic Encryption Algorithm in Wireless Network Security Communication," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–10, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[22] Bruno Carneiro da Rocha et al., "Preventing APT Attacks on LAN Networks with Connected Iot Devices Using a Zero Trust Based Security Model," *2021 Workshop on Communication Networks and Power Systems, WCNPS 2021*, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[23] Muhamad Fahri, "*Simulation of a Virtual Local Area Network (VLAN) Network Using a POX Controller*," Faculty of Science and Technology Syarif Hidayatullah State Islamic University Jakarta, 2017. [Publisher Link]

[24] Marcio Silva Cruz, Ferrucio de Franco Rosa, and Mario Jino, "A Study on Ontologies of Vulnerabilities and Attacks on VLAN," *Advances in Intelligent Systems and Computing*, pp. 115–119, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[25] Sivathas P, "Emerging Information Technology in Indian Banking Sector and its Cyber Security," *SSRG International Journal of Economics and Management Studies*, vol. 5, no. 2, pp. 16-22, 2018. [CrossRef] [Publisher Link]

[26] Astika Ayuningtyas, Sudaryanto Sudaryanto, and Deno Daseftra Cessara, "Virtual Local Area Network (VLAN) Management System on Web-Based Cisco Catalyst 3750," *Symmetris: Journal of Mechanical Engineering, Electrical and Computer Science*, vol. 11, no. 1, pp. 297–306, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[27] Māris Jurušs, Baiba Šmite-Roķe, and Līga Gasūne, "Excise Duty Gap on Cigarettes," *Engineering Economics*, vol. 29, no. 4, pp. 419–423, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[28] Namra Abid et al., "Synthesis of Nanomaterials Using Various Top-Down and Bottom-Up Approaches, Influencing Factors, Advantages, and Disadvantages: A Review," *Advances in Colloid and Interface Science*, vol. 300, p. 102597, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[29] V.Usha Bala, and B.D.C.N.Prasad, "Steering the Enterprise's Information System Security Risks in Relation with Uncertainty (Information System, Risks)," *SSRG International Journal of Computer Science and Engineering*, vol. 5, no. 2, pp. 5-8, 2018. [CrossRef] [Publisher Link]

[30] David C. Wynn, and P. John Clarkson, "Process Models in Design and Development," *Research in Engineering Design*, vol. 29, no. 2, pp. 161–202, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[31] I.Lakshmi, "A Review on Security in Mobile Cloud Computing," *SSRG International Journal of Mobile Computing and Application*, vol. 6, no. 2, pp. 4-11, 2019. [CrossRef] [Publisher Link]

[32] Annika E. Nilsson et al., "Towards Extended Shared Socioeconomic Pathways: A Combined Participatory Bottom-Up and Top-Down Methodology with Results from the Barents Region," *Global Environmental Change*, vol. 45, pp. 124–132, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[33] Igor Saenko, and Igor Kotenko, "A Role-Base Approach and a Genetic Algorithm for VLAN Design in Large Critical Infrastructures," *Proceedings of the Genetic and Evolutionary Computation Conference Companion*, pp. 1643-1650, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[34] Tianjiao Chen et al., "Virtual Network Embedding Algorithm for Location-Based Identifier Allocation," *IEEE Access*, vol. 7, pp. 31159–31169, 2019. [CrossRef] [Google Scholar] [Publisher Link]